

NCS TIB 05-01



NATIONAL COMMUNICATIONS SYSTEM

TECHNICAL INFORMATION BULLETIN 05-01

VoIP/E9-1-1 for NS/EP

March 2005

**NATIONAL COMMUNICATIONS SYSTEM
Technology and Programs Division (N2)
PO Box 4052
Arlington, Virginia 22204-4052**

VoIP/E9-1-1 for NS/EP



**Office of the Manager
National Communications System**

March 2005

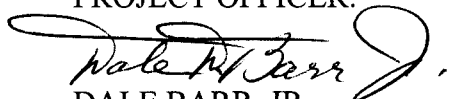
Communication Technologies, Inc.
14151 Newbrook Drive, Suite 400
Chantilly, Virginia 20151
703-961-9080 (Voice)
703-961-1330 (Fax)
<http://www.comtechnologies.com>

NCS TECHNICAL INFORMATION BULLETIN 05-1

VoIP/E9-1-1 for NS/EP

March 2005

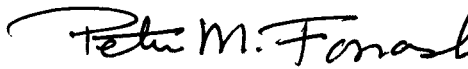
PROJECT OFFICER:



DALE BARR, JR.

Chief, Advanced Technology
Technology and Programs Divisions

APPROVED FOR PUBLICATION:



PETER M. FONASH, Ph.D.

Deputy Manager
National Communications System

FOREWORD

Among the responsibilities assigned to the Office of the Manager, National Communications System (NCS) is the management of the Federal Telecommunications Standards Program. Under this program, the NCS, with the assistance of the Federal Telecommunications Standards Committee, identifies, develops, and coordinates proposed Federal Standards which contribute either to the interoperability of functionally similar Federal telecommunications systems or to the achievement of a compatible and efficient interface between computer and telecommunications systems. In developing and coordinating these standards, a considerable amount of effort is expended in initiating and pursuing joint standards development endeavors with appropriate technical committees of the International Organization for Standardization, the International Telecommunication Union-Telecommunications Standardization Sector, and the American National Standards Institute. This Technical Information Bulletin presents an overview of an effort that contributes to the development of compatible Federal and national standards in the area of E9-1-1 response capabilities in light of the nationwide deployment of Voice over Internet Protocol (VoIP) services. This TIB is meant to inform interested Federal and industry parties. Any comments, inputs, or statements of requirements which could assist in the advancement of this work are welcome and should be addressed to:

National Communications System
Technology and Programs Division (N2)
PO Box 4052
Arlington, Virginia 22204-4052

VoIP/E9-1-1 for NS/EP

Abstract

Voice over Internet Protocol, or VoIP, is a technology that is becoming widespread in industry as an alternative to traditional telephone service. Traditionally, circuit-switched networks for voice comprise Signaling System 7 (SS7) standards compliant technologies, which provide a Connection Oriented Network Service (CONS). A number of changes are occurring to this infrastructure due to the convergence of Internet and Voice technologies. The Internet provides Connection Less Network Service (CLNS) by means of the Internet Protocol (IP) layer. Additionally, VoIP systems are introducing a number of technical challenges to Public Safety Organizations that are responsible for providing Enhanced 9-1-1 (E9-1-1) operations. VoIP and the network convergence technologies present the NCS with a number of technical, policy, and economic challenges regarding the support infrastructure for handling National Security/Emergency Preparedness (NS/EP) traffic. These challenges can be extended to include E9-1-1 services.

This Technical Information Bulletin (TIB) examines the present day state of VoIP technologies, with the caveat that the area is rich in experimental scientific research that may yield substantial changes within the next week, the next decade, and beyond. If convergence predictions prove to be accurate, profound changes in the core infrastructure that supports NS/EP operations, including E9-1-1 emergency services, is likely. Also, this report examines existing and emerging VoIP and Internet network technology and support for E9-1-1 emergency traffic, identifies current issues associated with their deployment, and discusses their applicability within the overall NS/EP environment. Finally, this TIB provides recommendations for NCS activities to track these technologies, to influence the development of standards designed to minimize the impact of VoIP implementations, and to enhance NS/EP communications in the future. This document was developed by the Scientific, Research, and Development (R&D) Department staff at Communication Technologies, Inc. in association with Mr. Jason Canon.

Table of Contents

1 Introduction.....	1
1.1 VoIP Background and Introduction	3
1.2 Advantages and Disadvantages of VoIP.....	5
1.3 NS/EP use of VoIP.....	6
2 VoIP/E9-1-1 Emergency Communications Transition.....	9
2.1 Legacy 9-1-1 Call Flow	10
2.2 VoIP E9-1-1 Transition Issues.....	11
2.3 Operational Issues with Current VoIP/E9-1-1 Deployments.....	13
2.3.1 Requirements for a Local Voice Trunk in E9-1-1 Tandem Switches.....	13
2.3.2 Separation of Emergency Location Identification Number (ELIN) from DID Public Number Space.....	14
2.3.3 Standardized ALI Records	15
2.3.4 VoIP/E9-1-1 Deployment Considerations	15
2.4 VoIP/PSN Gateway E9-1-1 Limitations	16
2.5 Quiet VoIP	16
2.6 Network Address Translation (NAT) Issues.....	16
2.7 Database Issues	18
2.7.1 MSAG Database	19
2.7.2 TN Database.....	19
2.8 Power for VoIP/E9-1-1 Interoperability	20
2.9 VoIP Congestion Control Concerns.....	20
3 VoIP Standards and Technologies	23
3.1 Packet-based Multimedia Communications Systems	24
3.2 H.323 Entities	24
3.2.1 H.323 Call Priority.....	25
3.2.2 H.323 URI Addressing and Resolution	27
3.2.3 H.323 Internet Service Registration.....	28
3.3 H.245 Non Standard Identifier.....	28
3.4 Internet VoIP.....	29
3.4.1 SIP.....	29
3.4.2 SIP Messages	34
3.4.3 SIP Resource Priority Mechanisms	34
3.4.4 E.164 to URI DDDS ENUM	37
3.4.5 ENUM Service Registration for SIP.....	38
3.4.6 IETF Emergency Services for Internet Telephony Systems.....	38
3.4.7 VoIP over WiFi.....	38
3.4.8 P2P	40
4 VoIP Research and Regulatory Efforts	41
4.1 IETF Research and Development Efforts	41
4.2 General Requirements for ETS.....	41
4.3 IP Telephony Requirements For ETS	42

4.4 Technology Leveling	43
4.5 International vs. National Standards Groups	43
4.6 FCC Activities	44
4.7 CALEA	44
4.8 Legislative Action.....	45
5 Observations and Conclusions.....	47
6 Recommendations	49

Figures

Figure 1 E9-1-1 Public Safety Answering Point.....	9
Figure 2 ANI transmission Format	10
Figure 3 VoIP/PSN Convergence	23
Figure 4 H.323 Terminal Configuration	25
Figure 5 ASN.1 Call-Priority	26
Figure 6 H.323 DNS Zone Record	28
Figure 7 H.245 Non Standard Parameter.....	29
Figure 8 SIP Addressing	30
Figure 9 SIP Entities	32
Figure 10 SIP Redirection.....	33
Figure 11 SIP Resource Priority Header.....	37

Tables

Table 1 ITU-T H.323 Registration for the Service field of the RFC 2782 SRV Record.	27
Table 2 ITU-T H.323 Registration for the Proto field of the RFC 2782 SRV Record....	27

Appendices

Appendix A: Acronyms	51
Appendix B: Bibliography.....	57
Appendix C: NS/EP Requirements and Operational Assets.....	59
Appendix D: VoIP QoS Issues	67

1 INTRODUCTION

The National Communications System (NCS) was established through a Presidential Memorandum signed by President John Kennedy on August 21, 1963. The memorandum assigned the NCS the responsibility of providing necessary communications for the Federal Government under national emergency conditions by linking together, improving, and expanding the communication capabilities of the various agencies.

In April 1984, President Ronald Reagan signed Executive Order (E.O.) 12472, Assignment of National Security and Emergency Preparedness (NS/EP) Telecommunications Functions,¹ which broadened the mission and focus. Since that time, the NCS has been assisting the President and the Executive Office of the President (EOP) in exercising wartime and non-wartime emergency telecommunications and in coordinating the planning for, and provisioning of, NS/EP communications for the Federal Government under all circumstances. In this regard, the Office of the Manager, NCS (OMNCS) continually seeks to improve the Federal Government's ability to respond to the telecommunications requirements to support national security and emergency situations. Among these responsibilities, the NCS seeks to ensure that a national telecommunications infrastructure is developed that "is capable of satisfying priority telecommunications requirements under all circumstances." The OMNCS is the appropriate body to communicate NS/EP requirements to standards bodies and participate in related standards activities.

As part of this mission, the N2 division identifies new technologies that enhance NS/EP communications capabilities and ensures key NS/EP features, such as priority, interoperability, reliability, emerging standards support, availability, and security. In concert with this approach, the N2 manages the Federal Telecommunications Standards Program (FTSC). Additionally, the N2 division directs efforts in both NS/EP management and applications services.

Further, on July 16, 1996, President Bill Clinton signed Executive Order 13010 Critical Infrastructure Protection (CIP),² which recognized that "...certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government." On September 11, 2001, terrorists struck both towers of the World Trade Center in New York, the Pentagon in Washington, DC, and a remote site in Pennsylvania by using commercial aircraft as flying missiles. On October 4, 2001, Kenneth C. Watson, President, Partnership for Critical Infrastructure Security reported to Congress that:

- Verizon's switching office at 140 West St. in Manhattan, supporting 3.5 million circuits, sustained heavy damage. Verizon Wireless lost 10 cellular transmitter sites.
- AT&T lost fiber optic equipment in the World Trade Center and had switching equipment damaged in a nearby building.

- Sprint PCS wireless network in New York City lost four cells.
- Cingular Wireless lost six Manhattan cell sites.
- WorldCom lost service on 200 high-speed circuits in the World Trade Center basement.³

On March 1, 2003, President George W. Bush transferred the NCS from the Department of Defense (after nearly 40 years of serving as the NCS's Executive Agent) to the Department of Homeland Security (DHS). The NCS was one of 22 Federal agencies transferred to the Department in accordance with Executive Order 13286.⁴ A revised Executive Order 12472 reflects the changes of E.O. 13286. Today, the NCS is part of the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate. The DHS Assistant Secretary for Infrastructure Protection now serves as the NCS Manager.

This Technical Information Bulletin (TIB) examines Voice over Internet Protocol (VoIP) and Enhanced 9-1-1 (E9-1-1) services. VoIP, as the name suggests, is voice traffic that has been digitized for transmission over Internet Protocol (IP) based networks and represents a true integration of voice and data services. VoIP offers substantial cost savings and a wide-range of potential new technology applications for NS/EP systems. E9-1-1 is an enhanced 9-1-1 capability present at some community-based Public Safety Answering Point (PSAP) call centers that provides caller ID and caller location information for both cellular and landline emergency calls. The ability to automatically redial an emergency call or locate an emergency caller greatly decreases the response time to that emergency and provides the first responders with important knowledge about the emergency.

Portions of this TIB are presented in [AbstractSyntaxNotation 1](#)⁵ for technical precision and to serve as a visual aid. The goals of this TIB are to:

- Present an introduction to VoIP technologies.
- Describe technical issues related to VoIP/E9-1-1 for NS/EP.
- Identify the potential benefits of VoIP/E9-1-1 for NS/EP applications in support of Critical Infrastructure Protection (CIP) requirements.
- Identify emerging NS/EP VoIP/E9-1-1 emergency service requirements and existing capabilities.
- Identify areas for further development of the technology which would enhance the governments NS/EP mission performance capabilities.

This VoIP/E9-1-1 TIB incorporates by reference the President's National Security Telecommunications Advisory Committee (NSTAC) report, *Information Technology Progress Impact Task Force Report (ITPITFR) on Convergence*,⁶ dated May 2000. Moreover, this TIB accepts and concurs with the conclusions of the ITPITFR contained within the report. The ITPITFR report states: "The potential implications of Convergence and the Next Generation Network (NGN) for GETS services include new blocking sources, lack of ubiquity and interoperability, lack of access to GETS features, disparate congestion handling, and a lack of commensurate network reliability and security."

Throughout this report industry standard notation practices are used when referring to E9-1-1. That is, consistent with recommended safety practices, when discussing the E9-1-1 emergency system a reference is never made to “nine-eleven” in recognition of the fact that a child could easily become confused during an emergency because there is no number “eleven” on a telephone.

For additional background information, it is recommended that the reader refer to the NCS TIB 00-8, dated September, 2000, *The Convergence of Signaling System 7 and Voice-over-IP*.⁷ TIB 00-8 provides an introduction and background material that serves as a useful basis for understanding VoIP convergence.

1.1 VoIP Background and Introduction

Providing high quality isochronous⁸ (audio/video) communications was the dominant challenge for Telecommunications companies during the 19th and 20th centuries. Voice communications has stringent Quality of Service (QoS) parameters and technical requirements in terms of delay, jitter, and echo suppression. Conventional circuit-switched networks have been fine tuned to handle voice communications. A voice call on the circuit-switched telephone network is typically engineered to have an average delay of 25 milliseconds. The International Telecommunications Union – Telecommunications (ITU-T) sector G.114 *One-way transmission time*⁹ recommends that one way end-to-end delay for high-quality voice transmission should have an upper limit of no more than 150 milliseconds. The performance characteristics of circuit-switched voice communications are highly refined and of very high quality - anything less is unacceptable for human communications.

During the last quarter of the 20th century, data networks and computer-to-computer communications began an explosive growth period. The greater flexibility in performance requirements for data communications made it possible for telecommunications carriers to simply “add-on” data communications to the existing high-performance voice networks. One problem, however, was that the Telecommunications business model did not adequately address the inherent service level and cost differences between voice and data communications. The result is the cost for many data communications applications and services was found to be disproportionate to the requirements.

Advanced Research Projects Agency (ARPA) funded research went into the design and engineering of technologies specifically intended to solve data communication issues. ARPA network (ARPAnet) packet switching and the Internet Protocols were created and evolved over a period of almost 25 years, during which many new interoperable computer networking applications were developed. As the capabilities of the Internet expanded, the circuit-switched networks became increasingly suboptimal for Internet Protocol (IP) based data communications. On the other hand, IP networks designed to provide “best effort” service were not engineered to satisfy the stringent technical requirements of real-time applications, such as voice and video communications. The inherent flexibility in packetized IP networks makes it substantially more difficult to provide QoS to a large set of users and applications. The result was that the divergence of voice and data communications networks continued until the last decade of the 20th century.

The advancement of personal computers (PCs), Internet Service Providers (ISPs like AOL), and the availability of high speed, broadband access brought an unprecedented explosion in the popularity of the Internet. This created demand for faster connections that could deliver improved data communications performance. As a result, a growth in bandwidth capacity and broadband access became affordable for millions of Internet users.

In 1995, hobbyists in Israel designed the first implementation of Voice over IP (VoIP). VoIP was created as a software application that digitized and compressed analog voice signals and could run on a home PC. The limited design of this application required the sender and receiver to use the same VoIP software and hardware components. The sound was not “telephone industry standard toll quality” voice, but it did represent the beginnings of a new Internet application. The design approach of placing voice application services and processing directly in the hands of end users of the network was a noteworthy departure from the existing telephone networks, which centralized application services.

Today, there are two standards for implementing VoIP that have been widely deployed: The ITU-T H.323 *Packet-based multimedia communications systems Recommendation*¹⁰ and Internet Request For Comments (RFC) 3261 *SIP: Session Initiation Protocol*¹¹ (SIP). They are the two dominant technical standards used to build VoIP products.

One additional noteworthy change occurred during the same decade that VoIP was created: the popularity of cellular telephones changed the consumer expectations regarding what constituted “acceptable” quality voice services. Cell phone users began to experience call fadeouts, disconnects, service unavailable locations, and power (e.g., battery) outages. The deployment of cellular technology also created new difficulties for E9-1-1 PSAP operations personnel who, in many cases, could no longer automatically receive location information about emergency callers.

Packet switched communications provided by the Internet has always operated as an unregulated, “best effort” entity driven by technology and free market demands. Analog-based voice communications, traditionally provided by the “Baby Bell” companies, has long been a regulated application due to the vital public and national security requirements that it satisfies. Since the introduction of VoIP technologies, a number of new technical mechanisms have been proposed by the Internet Engineering Task Force (IETF). These facilitate the evolution of the Internet’s “best effort” service model and render it capable of providing guaranteed services for real-time applications, such as voice and video. They include, among others:

- QoS enhancements
- Internet Standard 0064 *RTP: A Transport Protocol for Real Time Applications*¹²
- RFC 2205 *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*¹³
- RFC 3006 *Integrated Services in the Presence of Compressible Flows*¹⁴
- RFC 2475 *An Architecture for Differentiated Services*.¹⁵

Due in part to the current oversupply of USA telecommunications fiber capacity, it has been suggested that real-time applications can be supported simply by over provisioning

IP networks such that delay, jitter, and other performance considerations are no longer a concern. These new mechanisms for handling VoIP/E9-1-1 application requirements are examined in subsequent sections.

Today, VoIP can be observed in four distinct deployment scenarios, which operate in static or mobile configurations. First, VoIP can be deployed via cable or Digital Subscriber Loop (DSL) technologies, remain at a fixed location (e.g., a home), and employ the common North American Numbering Plan. Second, campus or enterprise VoIP can be established in the traditionally static configuration, with the additional benefit that the end user can easily move his telephone anywhere within the enterprise. Third, an Internet Service Provider (ISP) or carrier offering is expected to support highly mobile VoIP such that the user can plug into any Internet-based connection to obtain voice telecommunications service. Fourth, Wireless Fidelity (WiFi) or Worldwide Interoperability for Microwave Access (WiMAX) VoIP provides a mobile telephony configuration that allows the user to take a VoIP connection and roam within a wireless interconnected data network, in a manner similar to cellular telephony technologies.

The ability to identify the location of an emergency caller is the key element necessary for building an emergency response system. The legacy SS7 based 9-1-1 emergency services system was built on the premise that the telephone equipment was in a fixed location. Every telephone number had a billing address that was associated with the physical address of the device. Community emergency response systems were designed on the basis that the county, or similar government authority, assigned street names and street numbers and maintained this information in a database. When a 9-1-1 emergency call is placed, the phone company sends the calling telephone number information to the emergency response center as caller identification. The emergency response system was designed to associate the phone number with the officially assigned address. Since all phone locations are static, synchronization of both phone company and local community address databases can be batch processed on a regular (e.g., daily) basis. The anticipated mobility capabilities of VoIP E9-1-1 technologies mean that it will no longer be possible to associate the calling device with a fixed location. The requirement to constantly update the equipment location information in real time also creates a major challenge that the legacy SS7 based system was not designed to handle.

It is important to recognize that VoIP is a relatively young technology still on the cutting edge of innovation. VoIP holds great promise for the development of new and beneficial applications that can save lives during emergencies, enhance the competitiveness of global business, improve the quality of life, and help preserve national security.

1.2 Advantages and Disadvantages of VoIP

VoIP enables individuals and/or organizations to avoid long distance telephone toll charges and this reduction has been the motivation for early VoIP adopters. The ISPs offer flat rate pricing, which provides considerable long distance cost savings for both voice and facsimile. The sharing of telecommunications equipment and operational costs for both data and voice users can also improve network efficiency by creating savings through economies of scale. Deloitte Touche Tohmatsu¹⁶ has predicted that “by 2006

more than two-thirds of the largest global 2000 companies will have started deployment of VoIP to the desktop.”

The benefits of VoIP are not limited to cost cutting. VoIP enables a modernization of voice communications, productivity improvements, and opportunities for transforming the way that business is conducted. VoIP offers opportunities to combine operations; reduce network staff; reduce the impact of network points of failure; and to reduce management complexity, by employing the Internet Simple Network Management Protocol (SNMP) for both voice and data communications. VoIP will enable new voice features to be added by software upgrades without changing the networks lower layers IP infrastructure. The promise of VoIP is that it can be applied to almost any voice communications requirement, ranging from a simple inter-office intercom system to complex multi-national teleconferencing with shared screens. A simplified and integrated infrastructure that supports voice, data, video, and other applications can also reduce the total equipment costs through the use of standardized products, and VoIP is designed to support equipment mobility – telephones, and their numbers, move with the staff.

Major disadvantages of VoIP today are:

- Emergency services (E9-1-1) and directory services (411) are not universally available.
- The two widely deployed standards (H.323 and SIP) used to build VoIP systems are not interoperable.
- Implementations of the same VoIP standard from different vendors may not interoperate.
- Enterprise level VoIP typically requires initial equipment purchase and setup investments.
- Data and voice communications are both terminated if the Internet connection is lost.
- Transmission of VoIP calls may not have a consistent QoS.
- A wideband connection is usually recommended and adds to the costs.

1.3 NS/EP use of VoIP

The private networks and technologies deployed by the 23 member agencies of the NCS include those of the Federal Emergency Management Agency (FEMA), the Department of Defense, and others. These networks employ a wide-range of advanced technologies including:

- Multi Level Precedence and Preemption (MLPP) capabilities for both voice and data applications
- Radio frequency networks with and without preemption capabilities, such as the Wireless Priority Service (WPS) and SHARED RESOURCES SHARES
- The Government Emergency Telecommunications System (GETS).

The scale of the emergency directly affects the impact on communications networks. Natural disaster events, such as earthquakes, can quickly exceed the demands for communications that far outpaces the capacity. Thus, the heart of any technical

examination of emergency communications is focused on the available means to handle network congestion – whether voice (PSN) or data networks (Internet).

When fire engines are rushing to a fire, most people consider it a civic duty to clear even very congested roadways so that emergency responders can provide critical services. Preemption of normal traffic flows by emergency service responders on public highways is universally accepted. In the communications world, any suggestion that emergency responders be provided with the capability to preempt traffic on public voice or data communications networks has historically sparked cost, technical, first amendment, and other social concerns.

VoIP use in support of NS/EP will not be limited to E9-1-1 scale emergencies. In addition to the resources associated with E9-1-1, the emergency services assets that comprise the NCS will also incorporate VoIP. Annex C contains a brief overview of select NCS network assets that are likely candidates for early adoption of VoIP technologies for use in NS/EP situations.

2 VoIP/E9-1-1 EMERGENCY COMMUNICATIONS TRANSITION

Existing E9-1-1 emergency services networks comprise three distinct elements:

- The telephone SS7 network element
- The PSAP element
- The Data Base Management Systems (DBMS) element.

Today's E9-1-1 emergency services network can be viewed as a closed information system that provides a limited set of services due to its dependency on outdated technology systems and protocols. These systems are severely constrained with regards to supporting the mobility aspects of VoIP. Thus, the existing E9-1-1 networks are referred to as legacy systems. It also is widely accepted that transitioning to IP technologies will not only significantly reduce the costs associated with E9-1-1 operations, but will also enable the infusion of new emergency service capabilities.

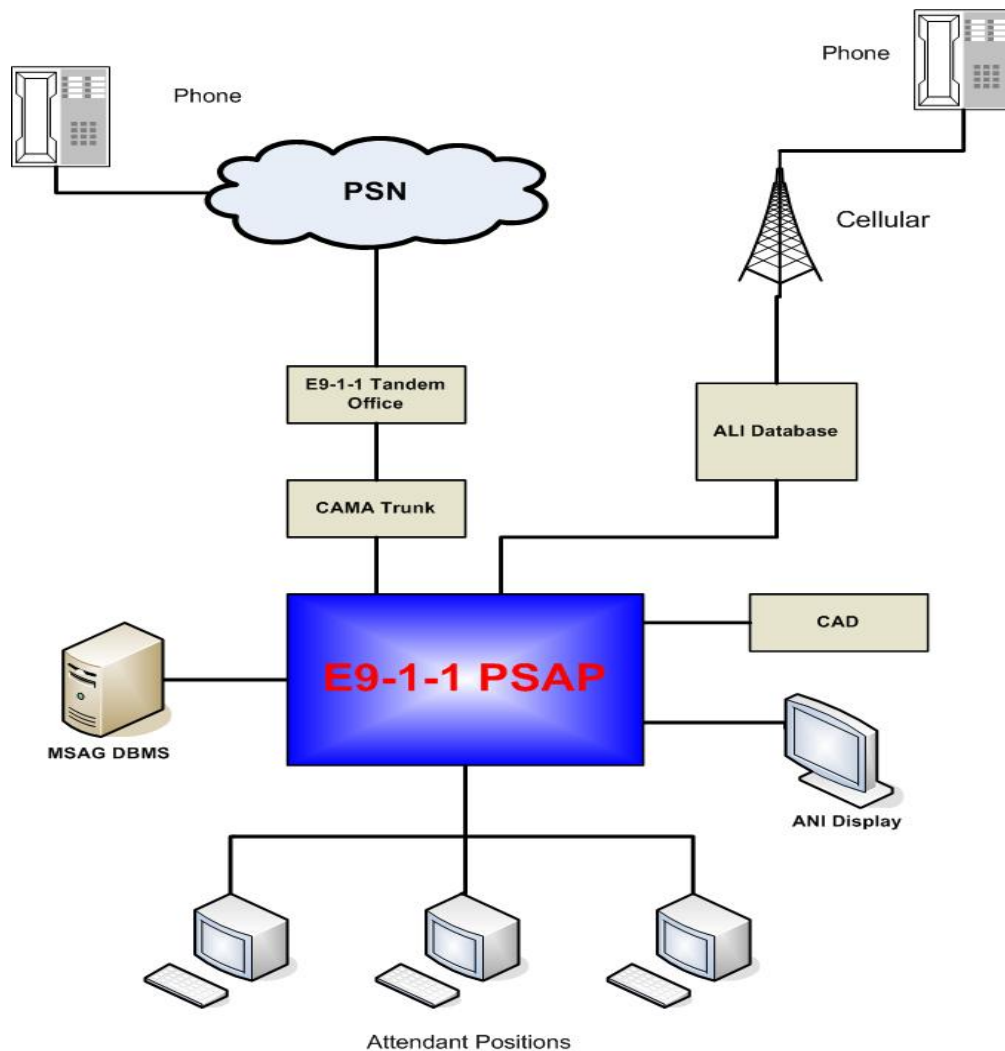


Figure 1 E9-1-1 Public Safety Answering Point

Figure 1 depicts an example of a PSAP connected to the PSN via a local Tandem Office switch. The trunk used between the PSAP and the Tandem switch is known as a Centralized Automatic Message Accounting (CAMA) trunk. Incoming 9-1-1/E9-1-1 calls from either the PSN or cellular networks trigger a lookup in the Automatic Location Identification (ALI) database. The figure also depicts the Master Street Address Guide (MSAG) database, Computer Aided Dispatch (CAD), Automatic Number Identifier (ANI) Display, and attendant positions. The actual ANI transmission format differs slightly from carrier to carrier, but the general form is depicted in **Figure 2**:

<p>T-1 (in-band):</p> <p style="padding-left: 40px;">KP + I + 7 or 10 digits + ST</p> <p style="padding-left: 40px;">where</p> <p style="padding-left: 80px;">KP = key pulse</p> <p style="padding-left: 80px;">I = information digit</p> <p style="padding-left: 40px;">7 or 10 digits = calling party station directory number</p> <p style="padding-left: 80px;">ST = start signal</p>

Figure 2 ANI Transmission Format

The ANI call setup information is provided in the Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) out-of-band signal. The ANI displays both ANI (wire line) and pseudo ANI (pANI wireless) 10-digit numbers.

2.1 Legacy 9-1-1 Call Flow

The following sequence illustrates the legacy 9-1-1 emergency call process:

1. A county resident requires emergency aid and dials 9-1-1.
2. The digits are received in the central office serving the exchange from which the user is dialing.
3. The central office sends the 10-digit ANI to the 9-1-1-tandem office.
4. The tandem office finds the associated Emergency Service Number (ESN) for the calling telephone number (TN) via the TN/ESN table. An ESN is a number associated with the geographical area served by the same fire, police, and ambulance districts.
5. Based on the ESN, the call is switched, via a dedicated trunk, to the appropriate PSAP.
6. The ANI is displayed at the PSAP.
7. The ANI information is sent to the ALI database for retrieval.
8. The ALI searches and retrieves the ALI data from the database.
9. The ALI computer returns the ALI to the PSAP.
10. The data is received at the PSAP and the information is displayed.
11. The PSAP attendant verifies the telephone number and the street address that has appeared on the screen and obtains information as to which emergency service is needed.

The attendant may transfer the call to the required agency (e.g., fire or ambulance) and/or stay on the line for additional assistance.

12. The details for each call (calling number, answering attendant's number, time of answer, time of transfer and/or disconnect, and the trunk number) are printed following disconnect on a printer at the PSAP, as a record of the transaction.

2.2 VoIP E9-1-1 Transition Issues

Three aspects of an emergency call must be maintained in order to transition to VoIP/E9-1-1 services. First, the user must be able to signal the network that the call is an emergency, so that it can be transferred to the correct PSAP. Rather than dialing 9-1-1 on a telephone, the user can enter (by typing, speaking, etc.) "sip: sos@city.state.us" or similar semantics into any computerized device that supports VoIP.

Second, it is necessary to determine the caller's location. This is currently accomplished using the ALI and MSAG databases, but in a VoIP environment there is no standard method. It could be accomplished using the Internet Domain Name System (DNS).

The third major required capability is that the PSAP must be furnished with the information necessary to reconnect to the caller should the call be disconnected. The user location was never an issue in wire-line systems because every call coming into the PSAP was associated with a stationary communications device that had a readily identifiable physical address. An underlying assumption in the design of VoIP is that every device is mobile.

Various paths are possible for transition emergency services from today's PSN centric networks to the next generation, IP-based networks. For example, a three-phased approach has been identified within the Internet community, as described below:

- The first phase, known as I1, is in existence today and requires no modification to the current E9-1-1 system. It consists of gateways between the Internet and the PSN. The gateways provide translation between IP and SS7 protocols. However, this configuration provides no enhanced services and VoIP sets must be static rather than nomadic.
- The second phase, known as I2, is intended to provide support for both stationary and nomadic VoIP configurations. It will provide caller location information to the called PSAP, but requires modifications to the XML ALI database format.
- The third phase, known as I3, is intended to replace ALI with DNS. New services, such as multimedia, international number support, and Global Network Positioning (GNP), will become available.

Foreign visitors present E9-1-1 problems even with the legacy PSN-based system. As shown in **Figure 2**, each PSAP is connected to the PSN by means of the Local Exchange Carrier (LEC) tandem switch using a Centralized Automatic Message Accounting (CAMA) trunk. CAMA trunks are limited to supporting no more than four area codes. CAMA trunks pulse out the ANI over analog trunks, thereby introducing 10-15 second delays. They are limited to providing no more than 10 digits, so longer international cell phone numbers that are used by foreign visitors to the U.S. are not fully supported. Even if a foreign visitor dials the correct emergency number (9-1-1) within the U.S., the PSAP

cannot call the visitor back should the call be disconnected because the equipment displays only the first 10 digits of the number.

The introduction of wireless mobile cellular telephones created E9-1-1 emergency location identification challenges that have not yet been fully resolved. Approximately 25% of CONUS-based PSAPs are equipped to handle the Federal Communications Commission (FCC) mandated phase II for wireless cellular deployment.¹⁷ Phase II of wireless introduced the use of Emergency Service Routing Digits (ESRD) and the Emergency Services Routing Key (ESRK), as defined in Telecommunications Industry Association (TIA) TR45 standard, J-STD-036. The routing information (ESRD/ESRK) is passed from the cellular provider's Mobile Switching Center (MSC) to the tandem switch in the ISDN User Part (ISUP). Routing to the correct PSAP is based on the ESRD/ESRK value. Unfortunately, there are locations where cellular boundaries span more than one PSAP boundary and the ESRD/ESRK is not sufficient to prevent misrouted calls in such situations. To reduce misrouted calls, the American National Standards Institute (ANSI)-41¹⁸ standards defined a Coordinate Routing Database (CRDB) that can be consulted by the network and returns the appropriate routing value to ensure that the call goes to the correct PSAP.

VoIP technology today is complicating the work of PSAPs beyond the challenges they face in achieving wireless Phase II capabilities. As discussed in section 1.1 of this report, four distinct deployment scenarios for VoIP must be addressed. In the case of VoIP home services, cable or Digital Subscriber Loop (DSL) providers that elect to offer E9-1-1 services to their customers must request that customers provide their home address. Only then can providers associate locations and the Media Access Control (MAC) address to the providers Ethernet port attachments. It should be noted that the MAC address is preferred, because IP address assignments are often dynamically allocated. This information enables a VoIP service provider to perform an association based automated retrieval of the required location data and pass it along to the appropriate PSAP when an E9-1-1 call is processed. It has been suggested within the Internet community that this information be published, without discrimination. This would enable all VoIP service providers to populate their databases.

In a conventional PSN-based enterprise or campus environment, a typical configuration includes a local Private Branch eXchange (PBX), which may be tied to other site PBX systems. Phone locations are fixed and tied to a specific PBX port. Changes to this system are made by physically moving the connection from one port to another. VoIP in a campus or enterprise environment identifies a user's VoIP phone by assigning the phone's MAC address to a port in the VoIP switch. The user may move the phone from office to office; by simply plugging the phone into an available switch Ethernet port, the new user location is automatically updated.

PSN connectivity from an enterprise system may be centralized in such a manner that E9-1-1 calls originating in one location are passed to the PSN in another location, because that is the PSN interconnect point. This situation applies to PBX systems with remote instruments connected via private tie lines, Digital PBX systems that connect remote locations via digital tie lines or VPNs, and VoIP systems that connect over the Internet. A VoIP enterprise client may be connected to the network in another city, state, or even

country than the one in which the client's VoIP server is located. Enterprise VoIP networks may have an insufficient number of trunks from which to allocate VoIP numbers. Further, the Internet is dynamic, thereby requiring real-time location information updates, whereas traditional PBX updates are most commonly performed daily.

For campus or smaller enterprise environments, the challenge is passing the PBX station's unique ANI information to the PSAP. This may involve either the PBX or a third-party application terminating CAMA trunks. These special trunks deliver the 9-1-1 call to the E9-1-1 Tandem switch. This will include either sending the Direct Inward Dialing (DID) number of that PBX station or inserting the telephone number of the nearest DID-serviced telephone to the E9-1-1 caller. Software capable of providing the required information to the correct PSAP is available. The enterprise is responsible for updates to the PBX database and for transmitting directly to the ALI database.

2.3 Operational Issues with Current VoIP/E9-1-1 Deployments

The National Emergency Number Association (NENA)¹⁹ has numerous technical committees actively working with recognized standards bodies (e.g., ANSI, TIA, etc.) and the Internet community, to identify requirements associated with providing emergency services to VoIP/E9-1-1 callers. The NENA currently has an identified work item to complete a VoIP technical requirements document.²⁰ Meanwhile, the NENA has identified a number of operational issues that have been experienced based on early VoIP/E9-1-1 deployed products. Some of the operational issues are very similar to those experienced with wireless configurations. For example, a VoIP device isn't necessarily E9-1-1 ready upon delivery. It may be necessary to follow the providers' instructions for "setting up" E9-1-1 service before emergency calls that provide location information may be placed. The following subsections highlight issues that have been documented by the NENA.

2.3.1 Requirements for a Local Voice Trunk in E9-1-1 Tandem Switches

The NENA has described an example scenario where a telecommuter in Boise, Idaho has a VoIP phone connected through an IP PBX in San Jose, California. When the Boise telecommuter makes a 9-1-1 call, it is processed through the IP PBX in San Jose. The range of IP gateways (to the PSN and E9-1-1 networks) that the enterprise owns determines the possible egress points from the IP network into the PSN E9-1-1 network. The 9-1-1 emergency call could be passed to the PSN in San Jose if the enterprise has voice trunks in that city. Today, there is no standard way of routing emergency calls across a long-distance provider backbone to reach the E9-1-1 tandem switch near Boise.

The challenge from a VoIP provider's perspective is that the current E9-1-1 network requires the provider to have a point of presence for each central office switch territory within the U.S. in which it offers VoIP services and to be registered as a Competitive Local Exchange Carrier (CLEC). For many would-be VoIP providers this may be cost prohibitive. Their only viable short-term solution is to not offer E9-1-1 services.

2.3.2 Separation of Emergency Location Identification Number (ELIN) from DID Public Number Space

In basic wire line 9-1-1 in North America, a caller dialing 9-1-1 is routed to a PSAP. The 9-1-1 operator in the PSAP is responsible for talking to the caller and arranging the appropriate emergency response, such as sending police, fire, or ambulance teams.

E9-1-1 extends these requirements as follows:

- The emergency call must be routed to the local PSAP based on the location of the caller. Basic 9-1-1 service simply routes the call to some PSAP, not necessarily the local one.
- The caller's location information must be displayed at the emergency operator's terminal. This information is obtained by querying an ALI database.

The location of an E9-1-1 caller is determined by the emergency location identification number (ELIN), which is a phone number the PSAP can dial to reconnect to the emergency caller if the call is disconnected for any reason, or if the PSAP needs to contact the caller again. The emergency call is routed to the PSAP based on the location information associated with this number. The ELIN can be associated with more than one telephone in multi-line phone systems, such as an office system, by grouping the phones into an emergency response location (ERL). In this case, the PSAP receives the address of an office building as the emergency location. The location information in multi-line phone systems would include data to identify the floor or a region on a floor. Each ERL requires a unique ELIN. Each locality can further extend or limit these requirements. For example, a city ordinance might include specific limitations on the size of an ERL (e.g., no larger than 1,000 square feet), or on the number of phones that can be included in an ERL (e.g., no more than 48 phones).

The NENA has summarized a problem where the ANI is a single key that serves two purposes in E9-1-1 networks. The ANI serves as the callback number when a PSAP needs to return a call to an emergency caller, and it also serves as a key into the ALI database. This connectedness was not a problem when Time Division Multiplexing (TDM)-based PBXs were the norm and location databases were manually updated after scheduled phone moves. However, in current VoIP/E9-1-1 enterprise deployments it is a challenge, because every ELIN requires an assigned Direct Inward Dial (DID) number. DIDs are assigned from a 10-digit limited number space and carry an associated cost. The net impact of this issue is that enterprises often cannot enable E9-1-1 service that locates callers to a specific office, cube, or dorm room in a university. A compromise solution requires that caller location is limited to a specific building or floor, and this is not sufficient for the needs or desires of many enterprises.

The NENA has identified this as a problem today, because ALI database updates are processed on a daily, as distinguished from a real-time, basis. The NENA has identified two main classes of solutions:

- Enable real-time updates to the ALI database, complete with civic address information. However, this introduces concerns regarding data integrity and MSAG-validation.

- Enable an independent numbering space (i.e., ELINs) to represent pre-populated physical locations that can be validated prior to emergency calls. Commercial solutions link a geographical address database with Ethernet port locations rather than the phones themselves. The Registered Jack (RJ)-45 data ports, usually mounted in walls, do not move. A cluster of RJ-45 jacks can be associated with an address database that is made accessible to 9-1-1 dispatchers.

Current industry products employ the latter class of solutions, which are designed to work with VoIP-enabled enterprises and require no changes to the public E9-1-1 infrastructure. A difficulty caused by this solution is that ELINs today are the same field as the ANI or Caller Identification field, so that customers must have a sufficient number of DIDs to support phone number assignment to people and phones, as well as an unused block to use as ELINs assigned to physical locations. It is not a scalable solution as customers are required to have a separate ELIN for every phone.

2.3.3 Standardized ALI Records

Large enterprises with many sites must independently work with each regional ALI provider (e.g., RBOCs, CLECs, or directly with PSAPs) to obtain ALI service, and PS/ALI record formats²¹ vary among industry vendors. The current lack of easily obtainable location information is an obstacle to enterprises trying to deploy VoIP/E9-1-1 across North America. NENA is seeking to make it easier for enterprises to determine how to handle Private Switch (PS)/ALI DBMS updates. The Internet DNS has been identified as one means to render a standardized, highly distributed, and scalable solution for the publication of this public data by organizations.

2.3.4 VoIP/E9-1-1 Deployment Considerations

E9-1-1 network architectures can be classified according to their technology migration status ranging from traditional wired 9-1-1, to FCC mandated wireless phases 1 and 2, and then VoIP-enabled PSAPs. While not directly tied to VoIP, wireless phases are included as part of the E9-1-1 network migration path, because these architectures are in the process of being deployed and they provide transition experience from fixed to mobile users, which the IETF expects to become the norm for VoIP-based architectures.

From the perspective of a PSAP today, VoIP user endpoints can be categorized according to three variables:

- The type of administrative domain
- The device mobility profile
- The roaming capability - whether movable devices remain within the local administrative domain or can cross to other administrative domains.

Additionally, NENA has expressed concern that unless local ordinances require E9-1-1 calls to be sent to the local PSAP, enterprise VoIP technologies will be configured so that emergency calls are routed to the company's onsite security staff instead of the PSAP. Another concern, especially for corporations that operate their own voice network over the Internet, is that the loss of the Internet connection renders all of the users at that location without emergency service capabilities.

In planning for PSAP call centers, one proposal is that a VoIP call server should be able to furnish an ESRK in the IP call setup. Such solutions will be helpful during transition, but a more complete and standardized approach built on proven technology, such as DNS, should be the long-term goal.

2.4 VoIP/PSN Gateway E9-1-1 Limitations

VoIP service providers may depend on third parties to translate their customer's IP connections into corresponding PSN calls via a gateway, due to the high entry cost of obtaining nationwide presence points into the existing E9-1-1 network. Also, it may be necessary for some VoIP service providers to send their customers' E9-1-1 calls to a general administrative number at the PSAP, rather than sending the call to the E9-1-1 dispatcher due to technical limitations (e.g., no local tandem switch, CAMA, or ISDN PRI trunk access) associated with this solution. Since these are general PSAP telephone numbers, they may not be answered outside of regular business hours.

2.5 Quiet VoIP

One facet of circuit switched technology is that it provides background sounds even in the absence of an active conversation. During E9-1-1 emergency situations, background sounds, such as conversations, sounds commonly associated with violence, church bells, and trains, could provide vital clues to the nature of the emergency. With VoIP technology, no packets are sent during the absence of a primary speaker. The advantage, of course, is that fewer packets are "wasted" (about 60% of each telephone conversation is made up of silence). The result is that VoIP developers have introduced what is commonly referred to as "comfort noise," which is technology that selectively blends sound frequencies at just the right volume to create the impression that the phone line is still alive. While this works to create the impression that the other caller is still on the line, without the need for wasting packets, it does not provide the vital information that has been invaluable to PSAPs ability to deliver high-quality E9-1-1 services.

2.6 Network Address Translation (NAT) Issues

Internet addressing has changed in many ways from the original ARPANet. Originally, all address ranges within three classes of networks were "routable" over the Internet. This changed in 1994 when RFC 1597 (obsolete) *Address Allocation for Private Internets*²² allocated 1 Internet class A network, 16 contiguous class B networks, and 256 contiguous class C networks (using pre-Classless Inter-Domain Routing [CIDR] terminology). One beneficial aspect of using the private network addressing schemes is that none of the IP addresses can be routed over the public Internet, so that private traffic remains private. The downside is that many millions of computers and network devices are not visible (nor can they be routed to) from the public Internet. To provide networking between a device in a private network address space and the public Internet, a Network Address Translator (NAT) is required. It is problematic in the short-term that VoIP/E9-1-1 emergency communications networks employing firewalls and transparent proxies are not transparent.

RFC 3022 *Traditional IP Network Address Translator (Traditional NAT)*²³ extended the NAT concepts introduced in RFC 1631, by adding Internet Standard 0006 *User*

*Datagram Protocol (UDP)*²⁴ and Internet Standard 0007 *Transmission Control Protocol (TCP)*²⁵ port translation; with the extension being referred to as the Network Address Port Translation (NAPT). When NAT originally appeared, there were significant concerns about the Internet addressing structures capability to handle enormous user growth rates. NAT provided a necessary pressure release valve on the demand for public IP addresses and also aided with certain network security concerns simply by hiding the true contents of thousands of IP networks.

NAT successfully worked to solve the address space issue, but it has caused operational problems for some applications and increased the design complexity for others. NAT functions by replacing the IP addressing portion of the data packet. Some applications, to function properly, have source-IP addressing buried within the actual data portion (payload) of the data packet. The NAT process doesn't typically check this payload field unless an Application Level Gateway (ALG) function is enabled. An ALG is designed to allow the proxy process to determine what kind of packet is being examined and if the packet's payload needs to be adjusted. Numerous application layer gateways (ALG) have been imbedded into NATs in order to provide transparency. ALGs typically rewrite application layer messages to contain translated addresses. ALGs are known to have scalability and reliability issues, which are important user support issues for a real-time application such as VoIP.

RFC 3489 *Simple Traversal of UDP Through NAT (STUN)*²⁶ and RFC 3303 *Middle Box Communications (MIDCOM) Architecture and Framework*²⁷ were developed to provide a NAT solution for VoIP applications. First, STUN allows SIP entities behind a NAT to discover its presence, determine its type, and to learn the address bindings allocated by NAT. STUN requires no changes to NATs and works with multiple numbers of NATs. Second, MIDCOM allows an application entity, such as an H.323 end client or network SIP server, to control a NAT in order to obtain NAT bindings and to open or close security pinholes. This would involve standard pre-configuration of TCP or UDP to well known services port number 5060 to support VoIP. A MIDCOM implementing NAPT would provide a port binding to redirect incoming SIP calls to private SIP phones. Thus, an INVITE from an external caller is made to the external NAPT address and then translated by MIDCOM to the internal IP address.

SIP applications rely on the UDP for audio transmission. STUN identified the common variations in the treatment of UDP by different NAT implementations. The four UDP treatments are described as follows:

- Full Cone: In full cone implementations, all requests from an internal IP address and port are mapped to the same external IP address and port. Any external host can send a packet to the internal host, by sending a packet to its mapped external address.
- Restricted Cone: A restricted cone NAT has the capabilities of a full cone implementation, with the exception that an external host can send a packet to an internal host only if the internal host initiated the association.
- Port Restricted Cone: A port-restricted cone NAT has the features of a restricted cone NAT, but the restrictions are extended to include the exchanged port numbers.
- Symmetric: In a symmetric NAT configuration all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same

external IP address and port. Only an external host that receives a packet can send a UDP packet back to the internal host.

One example of the possible difficulties can be observed by considering that the SIP Via header will always contain a host name and may contain a port number. When the SIP UA is behind a NAT, the IP and port in the Via header may be unreachable from outside the NAT, and so the need arises to send the answer to the IP:port from which the request arrived. Solutions currently exist for perhaps 95% of all cases, but some anomalies linger and may impact E9-1-1 in the short term.

Additional example of the complexities of working SIP through NAT is that STUN does not work for symmetrical NATs because the mapping of external ports and addresses varies based on destination. Thus, the external port that the STUN server reports back to the STUN client can't be used with other hosts. For cases involving symmetrical NATs, *Traversal Using Relay NAT (TURN)*²⁸ was proposed as a work in progress in 2003. TURN is a protocol that is useful for elements behind symmetric NATs or firewalls that need to be on the receiving end of a connection to a single peer. It accomplishes this by relying on a server inserted in the signaling path. Numerous other draft proposals for SIP interworking via NAT have been published. One noteworthy IETF publication applicable for WiFi VoIP IPv4 implementations is RFC 3519 Standards Track *NAT Traversal for Mobile IP*,²⁶ which allows IP-in-IP tunnels (UDP tunneling for SIP) to operate through NAT.

2.7 Database Issues

A large amount of the work in today's E9-1-1 networks is performed long before a user places a 9-1-1 call. In addition to circuit provisioning, configuration, and testing, it is necessary to consult all of the database records in order to provide the required identification and location information to the PSAP. One of the most significant limitations of the existing E9-1-1 system is that the telephone networks only provide a 10-digit phone number. The phone number is then used as a search key for DBMS lookup, formatting, and transmission of the necessary information (e.g., location, etc.), along with the phone number, to the correct PSAP.

Major database systems kept by every telephone service provider involved in E9-1-1 call processing include: the Telephone Number (TN) database, the ALI database, the county MSAG database, and the Selective Routing Database (SRDB) that (for Wireless Telephony) associates a cell site with a particular PSAP. The TN and SRDB are used to support telephone signaling so, for the purpose of this section, it is sufficient to focus on the ALI and MSAG databases. TIA/EIA/IS-J-STD-036²⁷ Enhanced Wireless 9-1-1, Phase II, E2 interface is utilized to provide location information to the ALI database. ALI and MSAG contain the public record data need by the PSAP. But, like the E9-1-1 systems themselves, they are isolated by SS7 protocols and by the databases that provide the information required by PSAPs in order to notify responders. One of the largest hurdles facing VoIP service providers that wish to provide E9-1-1 services to their customers is that the access to these databases is not openly available. One suggestion proposed to the FCC is that access to these DBMS systems be opened to companies that seek to provide VoIP services. Without open access, competition will be restricted to those service providers who own the ALI and MSAG data. Also, current E9-1-1 networks limit the

people responsible for making updates, changes, and deletions to DBMS systems. This may involve ALI DBMS service providers, the phone company TN database personnel, and MSAG maintenance.

The NENA has published standards for the types of data exchange formats employed in exchanging E9-1-1 database information. Four versions have been defined for use in ALI, MSAG, header and trailer records, and for dynamic updates to support wireless. The data exchange formats use extended XML to encode data using standardized tags. But NENA standards do not currently specify any security measures for the XML layer and user information needs to be protected over the Internet. XML Signatures provide integrity, message authentication, and signer authentication services and Internet RFC 3075 (Standards Track) *XML-Signature Syntax and Processing*²⁹ defines mechanisms for XML signing.

2.7.1 MSAG Database

The MSAG is the portion of the E9-1-1 database that contains the address and ESN information. The MSAG associates the appropriate ESN to the ANI or pANI number based on the address on the data record provided by the telephone carrier.

The MSAG contains all street information in the E9-1-1 service area. ESNs are assigned to streets in order to route E9-1-1 calls to the proper PSAP. As ANI and the pseudo ANI (pANI) data records are processed from the wireless carriers, the address information on the data record is validated against the MSAG. Address information on the data records must be an exact match of the MSAG information or the data records will be considered invalid and returned to the wireless carrier for correction. Data records are not posted to the database until they pass validation.

It is the responsibility of the E9-1-1 customer to assign, maintain, and resolve discrepancies in MSAG data for their service area. The E9-1-1 customer is also responsible for providing new address information and changes to address information used to update the MSAG database.

Telephone companies in a participating E9-1-1 service area are responsible for ensuring that all data records sent to the E9-1-1 host database have a valid MSAG address. Each telephone company works with the E9-1-1 customer to resolve any address discrepancies.

2.7.2 TN Database

The TN database contains all the out-dial subscriber lines within the exchanges in the city or county. This information includes the individual telephone number, name, address, location (apartment, lot, etc.), class, and type of service. The TN database is necessary, in the current closed architecture, to support the ALI retrieval to be displayed at the PSAP.

Each telephone company initially creates the TN database from an extract of customer account data. The extract is then processed against the MSAG. All subscriber lines must be exactly matched and are then assigned the appropriate ESN. Any discrepancies between the records of the telephone company and the city or county must be resolved.

The TN database is subsequently updated by processing daily service orders against the MSAG.

2.8 Power for VoIP/E9-1-1 Interoperability

One of the initial concerns about replacement for existing telephone services was that phone systems receive power from the local central office so that during electrical power outages telephone service remains operational. In 2003, the IEEE addressed power concerns for Local Area Network (LAN) devices, including VoIP phones, through the publication of IEEE 802.af. A representative short title for IEEE 802af is: *Carrier Sense Multiple Access/Collision Detection (CSMA/CD) Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI)*.³⁰ The standard incorporates additions to the objects, attributes, and behaviors to support 100 megabits per second (Mb/s), 1,000 Mb/s and 10 gigabits per second (Gb/s), full duplex operation, Media Access Control (MAC), Link Aggregation, and DTE Power via MDI. DTE powering is intended to provide a 10 Mb/s over twisted pair device, with a single interface for both data and the power to process these data. This promises a whole new class of Ethernet devices, including IP telephones, wireless access points, and Personal Digital Assistant (PDA) charging stations, that will not require additional power wiring or external power transformers. With about 13 watts of power available, small data devices can be powered by their Ethernet connections. Sophisticated detection and power monitoring techniques prevent damage to legacy data-only devices, while still supplying power to newer, Ethernet powered devices over the twisted-pair cable.

A device that supplies power is called Power Sourcing Equipment (PSE). A device that draws power from the wire is called a Powered Device (PD). A PSE is typically an Ethernet switch, router, hub, or other network switch. A PSE is required to provide a nominal 48 volts (V) DC between either the signal pairs or the spare pairs. The power is applied as a voltage between two of the pairs, typically by powering the center taps of the isolation transformers used to couple the differential data signals to the wire. Since Ethernet data is transformer coupled at both ends and is sent differentially, a voltage difference between the transmit pairs and the receive pairs does not affect the data. A 10base-T/100base-T Ethernet connection only uses two of the four pairs in the cable. The unused or spare pairs can be powered directly without affecting the data. However, 1,000base-T uses all four pairs and power must be connected to the transformer center taps if compatibility with 1000base-T is required.

2.9 VoIP Congestion Control Concerns

In March 2004, Informational RFC 3715 titled: *IAB Concerns Regarding Congestion Control for Voice Traffic in the Internet*³¹ was published. The document discusses Internet Architecture Board (IAB) concerns about the lack of an effective end-to-end congestion control capability for best-effort voice traffic in the Internet. The dominant issues addressed in the RFC included: fairness, user quality, and the dangers of congestion collapse presented by VoIP. The concerns expressed by the IAB in this RFC are especially relevant to VoIP/E9-1-1, in light of the absence of a widespread Internet QoS, and the likelihood that this situation is not likely to change in the near term. The RFC acknowledges that some ISPs deploy QoS on their backbones, and some corporate

intranets offer end-to-end QoS internally, but end-to-end QoS is not generally available to customers in the current Internet. Due to the importance of QoS support in VoIP/E9-1-1, a detailed examination of Internet QoS research is provided in Appendix D.

RFC 3715 acknowledges that in the near term, VoIP services are likely to be deployed over broadband best-effort connections. Current Internet real time media encoding and transmission practices ignore congestion considerations, resulting in the potential for trouble if VoIP becomes a broadly deployed service in the near to intermediate term. Poor user quality, unfairness to other VoIP and TCP users, and the possibility of sporadic episodes of congestion collapse are some of the potential problems in this scenario.

The RFC suggests that these problems can be mitigated in applications that use fixed-rate CODECs, by requiring the best-effort VoIP application to specify its minimum bit throughput rate. This minimum bit rate can be used to estimate a packet drop rate at which the VoIP call would terminate. The RFC recommends that in IETF standards for protocols regarding best-effort flows with a minimum sending rate, a packet drop rate must be specified, such that the best-effort flow terminates, or suspends sending temporarily, when the steady-state packet drop rate significantly exceeds the specified drop rate.

RFC 3715 additionally states that CODECs that are able to vary their bit rate depending on estimates of congestion will be more effective in providing good quality service while maintaining network efficiency under high load conditions. Adaptive variable-bit-rate CODECs were recommended as the preferable means of supporting VoIP sessions on shared usage Internet environments.

RFC 3715 considers the specific question of whether such traffic should be required to terminate, or be temporarily suspended, when the ISP faces a persistent, high packet drop rate and when reducing the sending rate is not a viable alternative. The RFC suggests that an over-provisioning of the network core is not sufficient to avoid congestion collapse, because it does not address the problem of congestion on the access links and access links routinely suffer from congestion.

RFC 3715 describes four efforts that are currently underway in the IETF to address issues of congestion control for real-time traffic: (1) an upgrade of the RTP specification, (2) RFC 3448 *TCP Friendly Rate Control (TFRC)*,³² (3) *Datagram Congestion Control Protocol (DCCP)*,³³ a work in progress, and (4) work on audio CODECS (coder-decoder). The RFC observes that off-the-shelf ITU-T vocoders (voice encoders), such as ITU-T G.711,³⁴ were generally designed explicitly for circuit-switched networks and are not as well adapted for Internet use, even with the addition of Forward Error Correction.

The recommendation of this RFC is that VoIP flows with minimum sending rates should have corresponding configured packet drop rates, such that the flow terminates or suspends when the persistent packet drop rate of the flow exceeds the configured rate.

Real-time traffic such as VoIP could benefit from the use of RFC 3168 *The Addition of Explicit Congestion Notification (ECN) to IP*.³⁵ RFC 3168 states routers may indicate congestion to end-nodes by marking packets instead of dropping them. Obviously, ECN was developed for use with transport protocols that react appropriately to marked packets as indications of congestion. RFC 3715 concludes that implementations supporting

mechanisms for terminating or suspending activity when the packet dropping and marking rate is too high would be able to satisfy the congestion-control requirements for ECN, while a non-supporting VoIP implementation would not. The RFC notes that additional mechanisms are required before it is safe for applications running over UDP to use ECN. For example, the sending application would have to ensure that the receiving application was capable of receiving ECN-related information from the lower-layer UDP stack, and that it can interpret the ECN information as a congestion indication.

This RFC is of interest from an NS/EP E9-1-1 perspective, because the recommendations that VoIP packets should be dropped in association with network congestion may have serious implications during emergency events.

3 VOIP STANDARDS AND TECHNOLOGIES

The current day general model of VoIP, depicted in **Figure 3**, supports interoperability between the Internet and the PSN by means of a gateway.

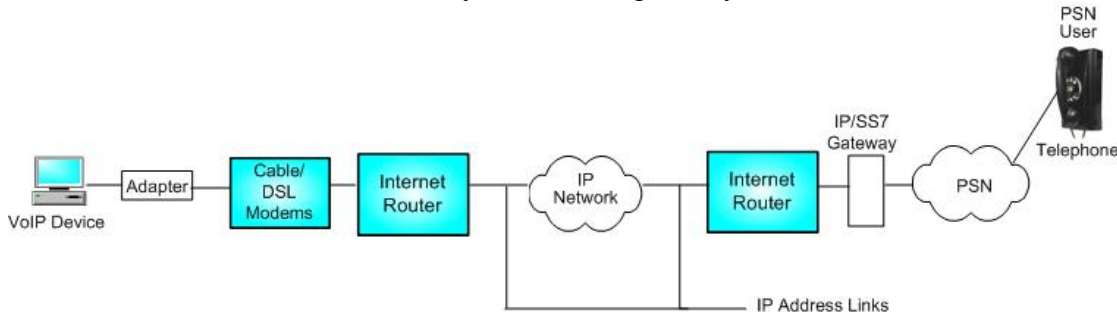


Figure 3 VoIP/PSN Convergence

From left to right, it depicts a PC running a VoIP software application. The PC would need to be equipped with a microphone and speakers. In other common configurations, legacy telephones can be plugged into an adapter that provides the necessary VoIP protocol stack. VoIP ready phone sets can support wireless, gigabit connections, eXtensible Markup Language (XML) programming, and operate over an existing IP Ethernet connection. Although a high-speed (cable/DSL) connection is generally preferred, VoIP can operate over low-speed dial-up modem connections. When the “phone call” reaches an IP router it is routed using conventional Internet addressing and protocols to the terminating router. During convergence, the call must then be fed into an IP/SS7 gateway, which serves as the originating point on the PSN. The call is delivered to the receiving Plain Old Telephone System (POTS) by the PSN.

There are several distinct types of VoIP technologies in use today. The ITU-T H.323 Series H: Audiovisual and Multimedia Systems Infrastructure of Audiovisual Services Systems and Terminal Equipment for Audiovisual Services *Packet-based Multimedia Communications Systems Recommendation*³⁶ defines the most widely implemented and deployed category to date. Another type has been enabled by a series of Internet Engineering Task Force (IETF) IP standards that utilize the SIP, but also include RTP, and others. SIP is considered to be the “carrier” quality solution for VoIP. Due to the popularity of the Internet, SIP-based implementations are currently experiencing rapid growth. Another type of evolving technology that supports VoIP is described by IEEE 802.11x WiFi/WiMAX technologies. Lastly, this TIB briefly describes Internet Peer-to-Peer (P2P) technology.

A fully comprehensive tutorial review of these standards is beyond the scope of this TIB. Therefore, the material presented is largely focused on the specific features and capabilities that are currently available to support VoIP/E9-1-1 NS/EP emergency communications, along with a limited general overview of each standard.

3.1 Packet-based Multimedia Communications Systems

The ITU-T H.323 is an international “umbrella” standard for the convergence of real-time multimedia communications (voice, video, data) over packet-based networks. H.323 was designed specifically to operate over IP networks but it may also operate over other packet-switched networks. H.323 was designed to support multipoint voice and video conferencing capabilities. H.323 is currently the world market leader for transporting VoIP and video; supporting billions of minutes of voice traffic every month.

H.323 was designed to provide support over a wide-range of packet data networks including Local Area Networks, Metropolitan Area Networks, Enterprise Area Networks, Intra-Networks and the global Internet. H.323 also supports dial-up connections or point-to-point connections over the PSN using the Internet Point-to-Point Protocol (PPP). H.323 defines the roles of various “entities” (e.g., software or hardware), which may be used in point-to-point, multipoint, and broadcast configurations. H.323 entities can also be integrated into personal computers or implemented in stand-alone devices, such as videophones.

H.323 leaves the specific packet-based network interface outside of the scope of the ITU-T Recommendation. The standard only requires that the network interface must provide the services as described in ITU-T Recommendation H.225.0 *Call Signalling protocols and media stream packetization for packet-based multimedia communications systems*,³⁷ otherwise known as “Information Streams.” The standard mandates reliable (TCP) end-to-end service for the H.245 Control Channel, the Data Channels, and the Call Signaling Channel. End-to-end unreliable (UDP) service is mandated for audio channels; video channels; and the Registration, Admission, and Status (RAS) channel. The services utilized on an H.323 connection may be simplex or duplex, unicast or multicast depending on the application, the capabilities of the H.323 terminals, and the configuration of the network.

3.2 H.323 Entities

The H.323 standard specifies six components, which together provide point-to-point and multipoint multimedia communication services over the IP:

- Terminals that provide real-time, bi-directional, multimedia communications. An H.323 terminal may be a stand-alone device, such as an IP telephone or a personal computer software program.
- Gateways that enable interworking between H.323 and a non-H.323 networks, such as the PSN.
- Gatekeepers are the “information broker” of H.323 networks. They provide support for authentication of Terminals and Gateways, authorization, addressing, call routing, and zone and bandwidth management.
- Multipoint Control Units (MCU) that consist of an MC and zero or more MPs and enable conferences between three or more endpoints in a multipoint conference.
- Multipoint Controllers (MC) provide H.245 negotiations between all terminals in order to determine audio, video, and data capabilities

- Multipoint Processors (MP) that provide mixing, switching, and the processing of audio, video and/or data streams in a multipoint conference.

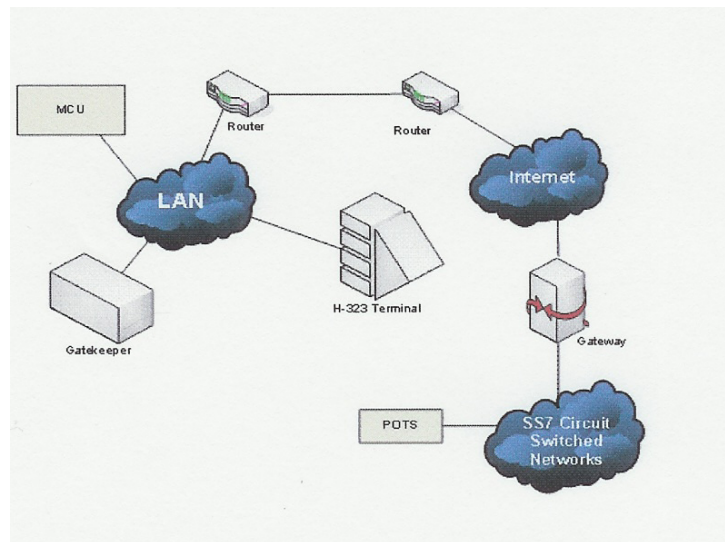


Figure 4 H.323 Terminal Configuration

Figure 4 depicts these elements of an H.323 configuration. Note that the MC can be located within a Gatekeeper, Gateway, Terminal, or MCU and the MP can be located within a Gatekeeper, Gateway, or MCU. Thus, they are not depicted separately. The control messages and procedures within H.323 define how these components communicate. The latest implementers guide H.323 systems³⁸ incorporate the H.323, H.225.0, H.235, H.245, H.246, H.283, H.341, H.450 series, H.460 series, and H.500 series of standards.

To date, there have been five versions of H.323 approved. The most current release, version 5, was approved in July 2003. H.323 data streams are encoded using ITU-T Recommendation X.680 (2002), *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.³⁹ More specifically, the ASN.1 Packed Encoding Rules (PER) for H.323 is specified in ITU-T Recommendation X-691 (2002)/ ISO/IEC 8825-2:2002, *Information Technology - ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER)*.⁴⁰ Unlike previous revisions of the Recommendation, H.323 version 5 defined only modest extensions to the base protocol and thus it is intended to provide stability.

3.2.1 H.323 Call Priority

One area of interest from an NS/EP perspective is that H.323 version 5 provides for the identification and treatment of emergency traffic through incorporation of ITU-T H.460.4 **CallPriorityInfo** to identify the priority of the call. It supports designation of a call priority for four distinct levels. The highest-level priority choice is to signal a request for an **emergencyAuthorized** indication, which is intended for use by local, state, Federal, or other recognized emergency service responders. The next level is an **emergencyPublic** indication to support prioritized treatment of public emergency service access, such as

E9-1-1. There are two additional priority values, **high** and **normal**, and a **priorityExtension** octet that may be used to further subdivide each of the defined levels, in association with Service Level Agreements (SLAs). The call priority capabilities are intended to render a specific probability of call completion.

```

Module CALL-PRIORITY (H.460.4)
CALL-PRIORITY {itu-t(0) recommendation(0) h(8) 460 4 version1(0)}
DEFINITIONS

AUTOMATIC TAGS ::=BEGIN

IMPORTS ClearToken, CryptoToken
FROM H235-SECURITY-MESSAGES;
CallPriorityInfo ::= SEQUENCE -- root for Call Priority related asn.1
{
priorityValue
CHOICE { emergencyAuthorized NULL,
emergencyPublic NULL,
high NULL,
normal NULL,
...},
priorityExtension INTEGER(0..255) OPTIONAL,
tokens SEQUENCE OF ClearToken OPTIONAL,
cryptoTokens SEQUENCE OF CryptoToken OPTIONAL,
rejectReason
CHOICE { priorityUnavailable NULL,
priorityUnauthorized NULL,
priorityValueUnknown NULL,
...} OPTIONAL, -- Only used in CallPriorityConfirm }

```

Figure 5 ASN.1 Call-Priority

As depicted in **Figure 4**,⁴¹ the CALL-PRIORITY module imports both clear and crypto tokens, which can be used to perform the authentication necessary to determine if the user has the authority required to request the **emergency Authorized** level of service. Internet RFC 3487 *Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP)*⁴² pointed out that the definition of a label such as **emergencyPublic** would open a security vulnerability whereby non-emergency calls could be marked for priority treatment and used in a Denial of Service (DoS) attack. Additionally, RFC 3689 *General Requirements for Emergency Telecommunication Service (ETS)*⁴³ identified digital signatures as potential network vulnerability for DoS attacks. The transmission of ASN.1 encoded data instead of a more simple form, such as ASCII text, presents a very low hurdle of security protection that would only be expected to deter the most amateur level of intruders.

3.2.2 H.323 URI Addressing and Resolution

Annex O of H.323 contains information regarding the registration and resolution of Uniform Resource Indicators (URI). The main focus is on the use of Internet Domain Name Service (DNS) to perform address resolution. The basic H.323 URI address is in the form “**h323: name@agency.gov.**” H.323 also supports RFC 2916 *E.164 Number and DNS*⁴⁴ the use of ENUM [0-9] addressing.

For DNS server configuration, H.323 has defined a number of symbolic names that may be used in the Service and Proto field of DNS SRV records, as per RFC 2782 *A DNS RR for specifying the location of services (DNS SRV)*.⁴⁵ H.323 defines the following symbolic names to be used in the *Service* field of the SRV record:

Service	Name	Meaning
H323ls	Location Service	H.323 entity supporting H.225.0 LRQ
H323rs	Registration Service	H.323 entity supporting H.225.0 RRQ
H323cs	Call Signalling	H.323 entity that performs H.225.0 call signalling
H323be	Border Element	H.323 supporting communication defined in Annex G/H.225.0

Table 1 ITU-T H.323 Registration for the Service field of the RFC 2782 SRV Record

H.323 Annex O also defines the following symbolic names to be used in the *Proto* field of the SRV record:

Symbolic name	Meaning
Udp	UDP as defined by RFC 768 <i>User Datagram Protocol</i> ⁴⁶
Tcp	TPKT over TCP according to Appendix 4/H.225.0
Sctp	SCTP as per RFC 2960 ⁴⁷
H323mux	As defined in Annex E

Table 2 ITU-T H.323 Registration for the Proto field of the RFC 2782 SRV Record

3.2.2.1 H.323 DNS Zone Records

This section illustrates an H.323 fragment of a DNS zone file for “agency.gov.” It depicts H.323 service that is provided through both a Border Element and Gatekeeper servers. No priority is defined or assumed between the Border Element and a primary and secondary Gatekeeper. Selection is based upon an application request. For example, voice-only high quality service is provided through the Border Element, while H.323 videoconferencing is provided through the Gatekeepers. An H.323 voice phone residing in the domain could have the following URI: **h323:jane.doe@agency.gov;service=be.** Here `_h323be._udp` becomes the default lookup. An E9-1-1 emergency videoconferencing service could be provided by an H.323 MCU located in the zone of either a

main-gatekeeper or secondary-gatekeeper. Its URI might be h323:emergency_conference@agency.gov;service=cs.

\$ORIGIN agency.gov.	
_h323be._udp	SRV 0 1 2099 border-element.agency.gov.
_h323cs._tcp	SRV 0 1 1720 secondary-gatekeeper.agency.gov.
_h323cs._tcp	SRV 0 3 1720 primary-gatekeeper.agency.gov.
border-element	A 66.98.244.1
main-gatekeeper	A 66.98.244.5
secondary-gatekeeper	A 66.98.244.10
*._h323mux	SRV 0 0 0 .
*._tcp	SRV 0 0 0 .
*._udp	SRV 0 0 0 .

Figure 6 H.323 DNS Zone Record

ITU-T H.323 based VoIP services can be supported within the Internet by means of these types of DNS entries.

3.2.2.2 H.323 Caller ID Services Calling Party Address Restriction

The calling party address restriction is a feature of H.323 that allows the client or the calling party's Gatekeeper to restrict presentation of the calling party alias address to the called party. This feature may reside in the endpoint or in the Gatekeeper for Gatekeeper routed calls. It may be desirable for NS/EP to enable override of this feature, so that PSAPs may receive this important information.

3.2.3 H.323 Internet Service Registration

In April 2004, RFC 3762 a Standards Track RFC titled *Telephone Number Mapping (ENUM) Service Registration for H.323*⁴⁸ was published. This document registers a Telephone Number Mapping (ENUM) service for H.323 according to specifications and guidelines in RFC 3761. The RFC registers H.323 to provide a means for it to take advantage of Internet services, such as DNS and ENUM to help facilitate the completion of multimedia calls.

3.3 H.245 Non Standard Identifier

ITU-T H.245 *Control Protocol for Multimedia Communication*⁴⁹ is a control channel protocol that operates during H.323 communication sessions. H.245 includes information about flow control, preference requests, and other commands that need to be sent back and forth during a call. It also defines separate receive and send capabilities.

The H.245 standard also reserved bits for national use. It defines a **NonStandardParameter** that consists of an identifier and parameters, which are octet string encoded. The H.245 standard defined **NonStandardIdentifier**, to identify the type of non-standard parameter. It can be encoded as an object identifier or with an H.221 identifier that consists of a four octets encoded as the country code (first octet) and a manufacturer's code (second octet). The first octet is reserved for the country code and

the second octet is reserved for assignment nationally. If, however, the first octet is escape encoded (i.e., 11111111) then the second octet contains the country code according to ITU-T T.35 Annex B. The last two octets are reserved for a manufacturer's code. The authority to assign manufacturer codes within North America resides with the Alliance for Telecommunications Industry Solutions (ATIS).

```
NonStandardParameter ::= SEQUENCE {
  nonStandardIdentifier NonStandardIdentifier,
  data OCTET STRING }

NonStandardIdentifier ::= CHOICE {
  object OBJECT IDENTIFIER,
  h221NonStandard
  SEQUENCE {t35CountryCode INTEGER(0..255), -- country, per T.35--
    t35Extension INTEGER(0..255), -- assigned nationally—
      -- unless T.35 country code is binary 1111
      -- 1111.
    manufacturerCode INTEGER(0..65535) -- assigned nationally
```

Figure 7 H.245 Non Standard Parameter

The common view is that **NonStandardParameter** is for use by manufacturers who wish to add additional facilities, capabilities, commands that are unique to their equipment.

Within the Internet community, another use was proposed in an Internet-Draft (I-D) *Simple RTP Multiplexing Transfer Methods for VoIP*⁵⁰ work in progress. This I-D proposed the use of the “Non Standard Message” as a mechanism to exchange multiplexing mode negotiation and Synchronisation SouRCe (SSRC) values for the stream identifier. There are no current proposals to define a USA national encoding of the second octet string for NS/EP or any other purposes. It is the second byte of the country code that is subject to assignment by the “national body.” At present, this byte is assigned a default value of hex 00.

3.4 Internet VoIP

The list of IETF proposals related to VoIP and emergency communications is long and growing rapidly. This section provides a basic level introduction to the Session Initiation Protocol (SIP) and a number of work in progress documents that are being defined to support emergency services, such as VoIP/E9-1-1.

3.4.1 SIP

RFC 3261 *SIP: Session Initiation Protocol* (SIP)⁵¹ was published in June 2002. SIP is a text based application-layer signaling protocol for initiating, managing, and terminating sessions that involve one or more participants across networks and may be considered a lightweight protocol for provisioning next generation network telephony. SIP uses the character set defined in RFC 2279 *UTF-8, a transformation format of the International Organization for Standardization (ISO) 10646*.⁵² SIP was created to provide a

mechanism for inviting people to large-scale multipoint conferences on the Internet Multicast Backbone (Mbone). VoIP applications were still experimental when SIP was published in 1999. However, it was soon realized that SIP could be used to set up point-to-point conference phone calls. SIP now supports Internet telephone calls, multimedia distribution, and multimedia conferences. SIP relies on highly extensible text-encoded dialog, which is similar to other successful Internet protocols, such as RFC 2616 *Hypertext Transfer Protocol (HTTP)*⁵³ and RFC 2821 *Simple Mail Transfer Protocol (SMTP)*.⁵⁴

SIP supports five functions that are necessary to establish and terminate multimedia communications. These are:

- Determine the location of the end points to be used for communication.
- Determine the availability of the called entity to engage in communications.
- Determine the media and parameters to be used.
- Initiate session by establishing session parameters (e.g., ringing) for the called and calling party.
- Manage session, including transfer and termination of sessions and modifying session parameters. SIP provides primitives that can be used to implement different services.

The first function is of great importance in PSAP operations where determining the location of an emergency is the first step toward dispatching an appropriate response. However, from a broader NS/EP applications development perspective the SIP functions as a whole provide a rich base that has great potential to support the development of an entirely new set of network centric automated and non-automated emergency services.

As a signaling protocol, SIP is designed only to make communications sessions possible; other protocols are required to actually render the communications. RFC 2327 *SDP: Session Description Protocol*,⁵⁵ RTP, RFC 2326 *Real Time Streaming Protocol (RTSP)*,⁵⁶ and other protocols are used in addition to SIP for this purpose. SDP is used to communicate the capabilities of session participants.

Architecturally, SIP is very different from the PSN where state and logic are maintained within the network and the end user devices (e.g., telephones) contain very limited functionality. SIP places the emphasis on distributed intelligence, which will enable new services to be easily implemented and quickly deployed.

3.4.1.1 SIP URI

SIP entities are identified using either a SIP URI or the ITU-T E.164 *The International Public Telecommunication Numbering Plan*.⁵⁷ A SIP URI is generally in the form of **sip:username@domain**. Since the format used for a SIP URI is based on the same type of semantics as an SMTP address, it provides a great deal of flexibility. For example:

<p>sip:stockbroker@example.com?subject=callme sip:bob@hotel.xyz; geo.position:125.31_-128.53_100.</p>

Figure 8 SIP Addressing

Capabilities such as the 3-dimensional “geo-position” illustrated in the second line of **Figure 7** can be of direct benefit to PSAP E9-1-1 operations.

In February 2004, an Internet Draft titled *Emergency Services URI for the Session Initiation Protocol*⁵⁷ was published as a work in progress. It recommends that SIP end systems and proxy servers support a uniform emergency identifier - “sos” - within any domain. Thus SIP URIs, **sip:sos@domain** and **sips:sos@domain**, were proposed as a means to allow SIP user agents to contact the local PSAP. Additionally, the work in progress reserved “sos” type addresses for specific emergency services, such as:

- sos.fire fire emergency
- sos.rescue ambulance services
- sos.marine maritime services
- sos.police law enforcement
- sos.mountain mountain rescue.

SIP also supports an E.164 style address in the form: **tel: 1-800-555-1212**. The URI provides an unlimited addressing space and does not require the user to enter lengthy strings of numbers.

3.4.1.2 SIP Entities

A SIP network is composed of four types of logical entities. These are:

- User Agent
- Proxy Server
- Redirect Server
- Registrar.

Each entity has specific functions and participates in SIP communication as a client (one who initiates a request), as a server (one who responds to a request), or as both. A “physical device” can have the functionality of more than one logical SIP entity. For example, a network server working as a Proxy Server can also function as a Registrar at the same time.

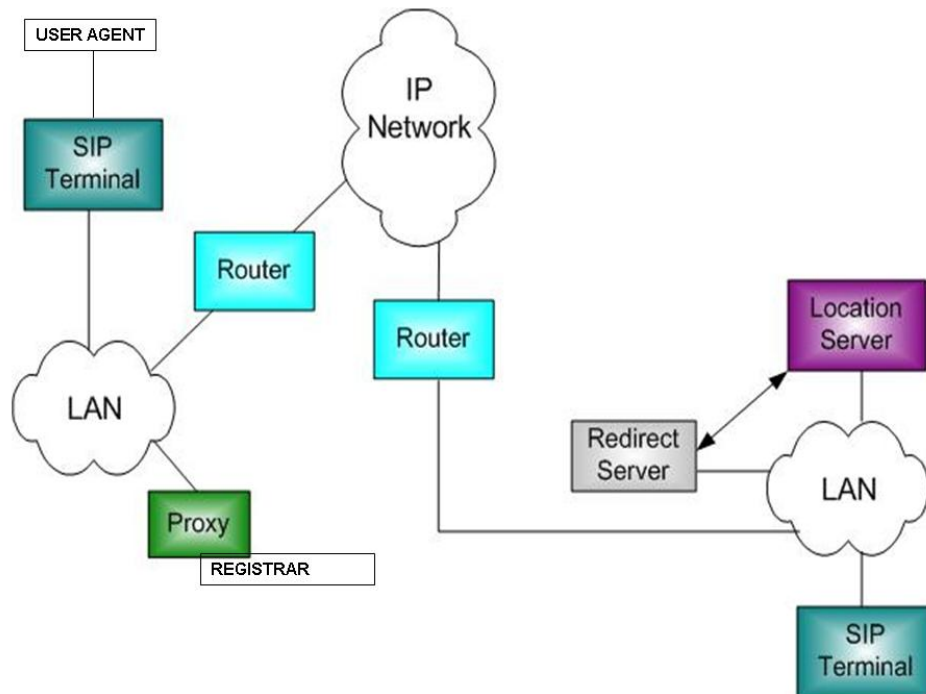


Figure 9 SIP Entities

Figure 9 depicts a typical SIP configuration. The User Agent functionality has been incorporated into the SIP Terminal. The registration process is part of the Proxy Server.

3.4.1.2.1 User Agent

The User Agent in SIP is an end system entity. User Agents initiate and terminate sessions by exchanging requests and responses. RFC 3261 defines the User Agent as an application, which contains both a User Agent Client (UAC) and User Agent Server (UAS), as follows:

- UAC - an end system entity that generates SIP requests.
- UAS - a server application that contacts the user when a SIP request is received and that returns a response on behalf of the user. Some of the devices that can have a UA function are workstations, IP-phones, telephony gateways, call agents, and automated answering services.

3.4.1.2.2 Proxy Server

A Proxy Server is an intermediary entity that acts as both a server and a client for the purpose of routing requests on behalf of clients to the user's current location, authenticates and authorizes end user services, supports provider call-routing policies, and provides features to users. A proxy server operates in a transactional manner. A call proxy is "stateful" only for the duration of the SIP transaction. Otherwise, a proxy operates as a stateless server. Requests are serviced either internally or by passing them

on, possibly after translation, to other servers. A Proxy interprets, and, if necessary, rewrites a request message before forwarding.

3.4.1.2.3 Redirect Server

A Redirect Server is a server that accepts a SIP request, maps the SIP address of the called party into zero (if there is no known address) or more new addresses, and returns them to the client. Unlike Proxy servers, Redirect Servers do not pass the request on to other servers. SIP Redirection is depicted in **Figure 10**.

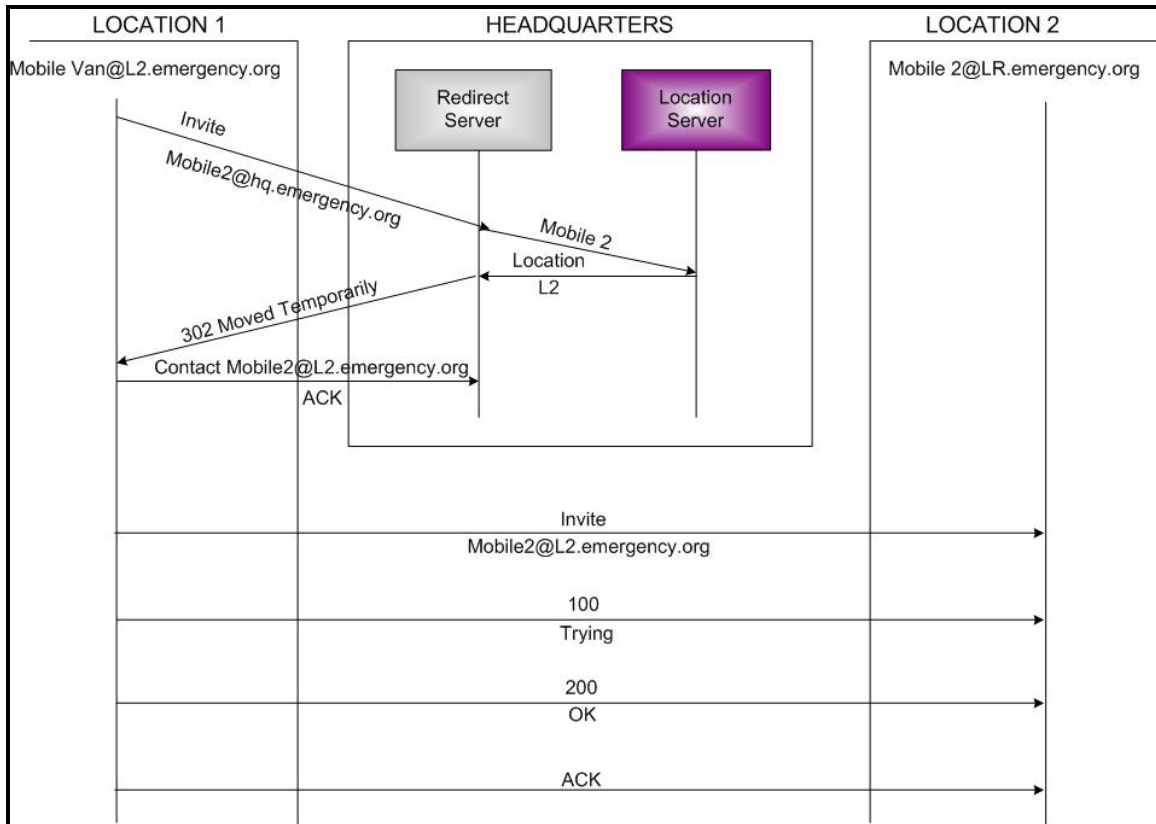


Figure 10 SIP Redirection

3.4.1.2.4 Registrar

A Registrar is a server that accepts REGISTER requests for the purpose of updating a location database with the contact information of the user as specified in the request. However, a Registrar server is not limited to storing information from a single source but could, for example, receive updates from an office phone, a home phone, and a mobile phone simultaneously. A proxy could subsequently be used to search and determine the user's location. During registration, a SIP URI is bound to the user's address (e.g., IP address, geospatial position, etc.).

3.4.2 SIP Messages

A SIP message is either a request from a client to a server or a response from a server to a client. SIP messages are composed of three parts: (1) Start Line, (2) Header, and (3) Body. The Start Line contains an identification of the message type and SIP protocol version. SIP Header fields are used to identify message attributes and to modify the message meaning. RFC 3261 permits new header field parameters and parameter values to be defined and I-D *SIP Parameter Registry* June 2004,⁵⁸ a work in progress, defines the supporting Internet Addressing and Naming Authority (IANA) registration process. A SIP Message Body describes the session that is being initialized. Some of the possible message Body types include: Session Description Protocol (SDP), Multipurpose Internet Mail Extensions (MIME), and others defined by the IETF and product implementers.

3.4.3 SIP Resource Priority Mechanisms

3.4.3.1 RFC 3487

In February 2003, an Informational RFC 3487 *Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP)*⁵⁹ was published. It was a product of the Internet Emergency Preparedness Working Group (IEPWG).

RFC 3487 identified four types of combinations of IP and circuit-switched network topologies:

- **IP End-to-End** which has both the request originator and destination on an IP network without an intervening CSN-IP gateway. Any SIP request could be subject to prioritization in this configuration.
- **IP-to-Circuit Switched Network (CSN)** where the request originator is in the IP network in IP-to-CSN configurations, while the called party is in the CSN. This model only applies to SIP-originated phone calls not other SIP requests, such as those supporting instant messaging services.
- **CSN-IP** where calls originate in the CSN and terminate via an Internet telephony gateway in the IP network in CSN-to-IP configurations.
- **CSN-IP-CSN**, also known as IP bridging, is a concatenation of the two previous configurations. It is worth noting that the two CSN sides may use different signaling protocols. Also, the originating CSN endpoint and the gateway to the IP network may not know the nature of the terminating CSN. Thus, encapsulation of the originating CSN information is insufficient. The bridging model can be viewed as the concatenation of the CSN-to-IP and IP-to-CSN cases.

Network congestion in SIP networks also is an important issue and was recognized by the RFC. Network congestion can effect emergency communications, including telephone circuits, IP bandwidth, and gateways between circuit-switched and IP networks. From a SIP vantage point, there are five different resources that may become congested during an emergency:

- Gateway resources
- Circuit-switched network resources
- IP network resources

- Receiving end-system resources
- SIP proxy resources.

RFC 3487 identifies four IP network models that influence the requirements for resource priority. Sequentially, each model inherits the restrictions of those before it. The models are:

- Pre-configured for Emergency Telecommunications Service (e.g., MLPP)
- Transparent (e.g., GETS)
- SIP/RTP transparent
- Restricted SIP.

In a pre-configured emergency telecommunications service IP network, an agency is the owner and is free to add traffic shaping, scheduling, or support for RSVP to the routers. A transparent network may be a commercial ISP that offers to forward valid IP packets but, by default, does not require customized setup or allow an application to request modified behavior from network elements. GETS does provide relief from network management restrictions, but does not require the user to have any specialized telephone equipment. In SIP/RTP transparent networks, users are allowed to receive and place SIP phone calls and RTP media streams. However, the network may block RSVP, and more critically, may reset the value of the RFC 2474 *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*⁶⁰ commonly known as the Differentiated Services Code Point (DSCP) to the Internet default bit pattern 00000000. Lastly, Restricted SIP networks may bar users from adding protocol elements beyond a prescribed set. As a separate and distinct problem, RFC 3487 stated SIP networks may administratively prohibit or otherwise fail to support existing, special NS/EP access numbers, such as the GETS 710 area code.

RFC 3487 identified 17 requirements necessary for SIP to achieve resource prioritization for emergency services. The requirements are:

- Prioritization is not specific to one scheme or country
- Network architecture independence
- Invisible to the IP layer
- Mapping from SIP to existing schemes
- No information loss
- Naming scheme extensibility
- Policy and mechanism separation
- SIP method neutral
- Default behavior
- Address scheme neutral
- Priority marking is user identity independent
- Network location independence
- Support for multiple simultaneous prioritization schemes
- Namespace discovery

- Test capability
- Support sip 3rd party call control
- Proxy visible.

The security requirements associated with SIP resource priority mechanisms are:

- Rigorous authentication and authorization mechanisms
- Network attack protections
- Resource priority and authentication mechanism independence
- Non-trusted end systems
- Authentication mechanisms resistant to replay attacks
- Cut and paste attacks
- Bid down attacks
- Confidentiality
- Anonymity
- DoS attacks
- Minimize resource use by unauthorized users
- Attack amplification avoidance.

These requirements form the foundation of requirements upon which VoIP/E9-1-1 services may be established.

3.4.3.2 Resource Priority for SIP

In March 2004, an Internet Draft (I-D) *Communications Resource Priority for the Session Initiation Protocol (SIP)*⁶¹ was published as a work in progress. It defines two new SIP header fields for communications resource priority, namely “Resource-Priority” and “Accept-Resource-Priority.” The I-D recognizes at least five different resources that may become scarce and congested during emergencies. The resources include:

- Gateway resources
- Circuit switched network resources
- IP network resources
- Receiving end systems resources
- SIP proxy resources.

The “Resource-Priority” header field depicted (it is in green to distinguish that it is not ASN.1 encoded) in **Figure 11** can influence the behavior of SIP UAs, such as PSN gateways, and SIP proxies but it is not intended to directly influence the forwarding behavior of IP routers.

```
INVITE sips:sos@psap.city.state.us SIP/2.0
Via: SIP/2.0/TLS client.city.state.us:5061;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Responder <sips:responder@city.state.us>;tag=1234567
To: 9-1-1 <sips:sos@psap.city.state.us>
Call-ID: 12345F01@city.state.us
Resource-Priority: 9-1-1.authorized_emergency
CSeq: 149541 INVITE
Contact: <sips:responder@city.state.us>
Content-Type: application/sdp
Content-Length: 105
```

Figure 11 SIP Resource Priority Header

The I-D includes a section that identifies initial IANA namespace registrations for the U.S. Defense Switched Network (DSN), ITU-T Q735.3,⁶² which provides Multi-level Precedence and Preemption in SS7 networks and the U.S. Defense Red Switched Network. The following priority values were registered for both the DSN and the Defense Red Switched Network: (1) routine, (2) priority, (3) immediate, (4) flash, and (5) flash-override. ITU-T Q735.3 registered the least (routine) to greatest priority (Flash-override) values as: 4 to 0.

3.4.4 E.164 to URI DDDS ENUM

In April 2004, IETF RFC 3761 Standards Track *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*⁶³ was published. It provides for the transformation of E.164 numbers into DNS names and vice versa. The top level domain “e.164.arpa” has been defined within the IETF to enable delegated (e.g., subdomain) zones.

The SIP application provides a good example of the way DNS operates to support E.164 addressing. An address of the form “tel: +1-710-555-1212” could be entered (manually or voice activated) into the client system. The first process is to yield an application unique string. This is done by removing all non-digit characters except for the “+” sign thus yielding +17105551212. This is the result of the application of the first step, as defined by RFC 1123 *Requirements for Internet Hosts -- Application and Support*.⁶⁴ The second step consists of inserting dots between each digit, which yields 1.7.1.0.5.5.5.1.2.1.2. The order of the digits is then reversed (because DNS is processed from right to left) producing 2.1.2.1.5.5.5.0.1.7.1. Next, this is appended to the e164.arpa domain name to form 2.1.2.1.5.5.5.0.1.7.1.e164.arpa. This is the domain name that ENUM uses to request a DNS query. Once the authoritative name server is found, ENUM retrieves the relevant Network Address Pointer (NAPTR) records or it renders new domain name keys.

This same approach can be used to support private enterprise networks. A corporation, for example, could employ an internal four-digit numbering plan. Using 7324 as an example would result in 7.3.2.4, which reversed and added to the domain space results in 4.2.3.7.e164.company.com.

The potential applications of ENUM and private addressing plans are far reaching, but the principle focus to date has been on VoIP and on Voice Protocol for Internet Mail (VPIM).

3.4.5 ENUM Service Registration for SIP

An Internet Proposed Standard RFC 3764 *ENUM Service Registration for Session Initiation Protocol (SIP) Address-of-Record*⁶⁵ was published in April of 2004. This RFC registers an Electronic Number (ENUM) service for the Session Initiation Protocol (SIP), pursuant to the guidelines in RFC 3761. Specifically, this document focuses on identifying the available services associated with one E.164 address. An organization, for example, may wish to designate an ENUM domain as preferring to connect first by means of SIP, second by means of H.323, and third by SMTP.

3.4.6 IETF Emergency Services for Internet Telephony Systems

An Internet Draft titled *Emergency Services for Internet Telephony Systems*⁶⁶ was published as a work in progress in February 2004. It focuses on describing how Emergency Call Centers (ECC), known as PSAPs in the USA, can handle Internet Telephony calls. More specifically it describes how SIP can be used to provide advanced emergency (e.g., real-time voice, video, instant messaging) services via VoIP. It requires no new protocol mechanisms and recommends the use of DNS to map civil and geospatial locations to the appropriate PSAP.

The draft identifies four sources for location information: (1) civil information that describes the location of a person by floor and street address, (2) postal (e.g., P.O. Box 123), which is unsuitable for emergency call routing in current implementations but may be the only address record available that an ISP can provide, (3) geospatial addresses containing longitude, latitude, and altitude information, and (4) Cell tower.

The draft RFC indicates that location information may not be available at call setup time, using the example of a GPS-enabled cell phone that when initially powered on may require 20-25 seconds to acquire a GPS fix. The draft recommends that initial call setup proceeds, with the location information furnished, as it becomes available.

The draft also recommends requirements for SIP proxy servers, which includes SIP with UDP, TCP, and RFC 2246 *Transport Layer Security (TLS)*.⁶⁷ Additionally, it recommends that an Emergency Services Routing Proxy (ESRP) should not use RFC 1918 *Address Allocation for private Internets*⁶⁸ and should not be behind NAT, because of the interoperability uncertainties these introduce.

3.4.7 VoIP over WiFi

IEEE 802.11 is a standard for Wireless Local Area Networks (WLANs) operating in the unlicensed 2.4 GHz and 5 GHz Industrial, Scientific, and Medical (ISM) bands. IEEE 802.11b⁶⁹ PHY, commonly known as Wi-Fi, is a standard for WLANs operating in the 2.4 GHz spectrum with a bandwidth of 11 Mbps. IEEE 802.11a⁷⁰ is a standard for WLANs operating in the 5 GHz frequency range with a maximum data rate of 54 Mbps using Orthogonal Frequency-Division Multiplexing (OFDM) modulation techniques. IEEE 802.11g⁷¹ is for WLANs operating in the 2.4 GHz frequency, but with a maximum

data rate of 54 Mbps. Additional IEEE groups are working on enhanced security (802.11i),⁷² spectrum and power control management (802.11h),⁷³ and QoS 802.11e.⁷⁴ The IEEE 802.11e QoS standard will likely be ratified by mid-2005. However, manufacturers have already released products based on the draft specification. For further information, the reader is directed to NCS Technical Information Bulletin 03-1, “Wireless Networking Technologies.”

IEEE 802.11e Draft 8 is a proposed amendment to the Standard for Information Technology, Telecommunications and Information Exchange Between Systems, Local Area Network (LAN)/Metropolitan Area Network (MAN) Specific Requirements, Part 11 Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Quality of Service (QoS) Enhancements. Until IEEE 802.11e has received final approval by the IEEE, the technology and/or specifications are subject to further modification and change. QoS is one of the major issues surrounding VoIP over WiFi. Discussions have been held within the IEEE to examine the need for a voice-centric standard. To date, the IEEE has not announced plans for the development of a VoIP over 802.11 standard, even though the marketplace currently offers VoIP over “WiFi” products.

Wireless, especially in the unlicensed LAN spectrum, is characteristically unpredictable. The IEEE 802.11 Task Group E is defining enhancements to distinguish QoS capable stations from non-QoS stations and QoS capable access point (QAP) from non-QoS access point (AP) in order to provide support for QoS. These capabilities are collectively called the QoS facility. The two main modules defined in 802.11e are the Channel Access Functions and Traffic Specification management, which provide integration between the Channel Access Functions and higher layer QoS protocols, such as those provided by RFC 2998 *A Framework for Integrated Services Operation over Diffserv Networks* Integrated Services⁷⁵ or RFC 2475 *An Architecture for Differentiated Services (Diff-SERV)*.⁷⁶

The QoS facility defines a coordination function called the Hybrid Coordination Function (HCF). HCF has two modes of operation: (1) Enhanced Distributed Channel Access/Wireless Media Extensions (EDCA/WME), which is a contention-based channel access function that operates concurrently with HCF, and (2) HCF Controlled Channel Access (HCCA)/WiFi Scheduled Media (WSM), which is based on a polling mechanism that is controlled by the Hybrid Coordinator (HC). The HC is co-located with the QoS enhanced Access Point (QAP). Both access functions extend the capability of the original access methods. Distributed Coordination Function (DCF) and Point Coordination Function (PCF). EDCA is designed to support prioritized traffic like Diff-SERV and HCCA supports parameterized traffic like IntServ.

EDCA enhances the original DCF to provide prioritized QoS by introducing the concept of traffic categories. Each station has eight traffic categories or priority levels. Prioritized QoS is realized through the introduction of four Access Categories (AC) that provide delivery of frames associated with user priorities. Each AC has its own transmit queue and its own set of AC parameters. The differentiation in priority between AC is realized by setting different values for the AC parameters. Using EDCA, stations try to send data after detecting the medium is idle and after waiting a period of time defined by the

corresponding traffic category. These parameters include: (1) the Arbitration Inter-frame Space Number (AIFSN). AIFSN is the minimum time interval between the wireless medium becoming idle and the start of frame transmission. A higher-priority traffic category will have a shorter AIFSN than a lower-priority traffic category. (2) Contention Window (CW), which is a random number used as a window, for the back off mechanism. If another station transmits before the countdown has ended, the station waits for the next idle period, after which it continues the countdown where it left off. No guarantees of service are provided, but EDCA establishes a probabilistic priority mechanism to allocate bandwidth based on traffic categories.

HCCA is a component of HCF and provides support for parameterized QoS. It inherits some of the rules of legacy PCF, and it introduces many extensions. Similar to PCF, HCCA provides polled access to the wireless medium. Unlike PCF, QoS polling can take place during CP and scheduling of packets is based on admitted Traffic Specification (TSPEC). The central concept of HCCA is Controlled Access Phase (CAP), which is a bounded time interval and formed by concatenating a series of HCCA (polled) Transmission Opportunities (TXOPs.).

The TSPEC is the traffic stream management capability specified by the 802.11e. It provides the management link between higher layer QoS protocols, such as IntServ or Diff-SERV, with the 802.11e channel access functions. TSPEC describes characteristics of traffic streams, such as service interval, data rate, delay, and packet size. TSPEC negotiation between peer MAC layers controls admission, establishment, adjustment, and removal of traffic streams which is important in the limited bandwidth available in the wireless medium. Bandwidth access must be controlled to avoid traffic congestion, which can lead to breaking established QoS and a drastic degradation of overall throughput. The 802.11e standard specifies the use of TSPEC for both EDCA and HCCA. QoS Management frames, primitives, and procedures are also defined for TSPEC negotiation.

The new 802.11e standard will assist home users to establish wireless multimedia networks and will allow corporate users to deploy wireless handsets using VoIP technology. It is expected to be available as a software download for many wireless networking devices. Upgrading to 802.11e may make wireless VoIP networks a realistic choice for network managers. It is also expected that handset makers will begin producing dual-mode phones that support wireless LAN technology, such as 802.11 and Global System for Mobile (GSM) communications.

3.4.8 P2P

Peer-to-Peer (P2P), a popular form of Internet Telephony, can interoperate with the existing PSN infrastructure, but does not provide any capability to interoperate with the closed E9-1-1 emergency communications systems. P2P does not currently support multimedia and it is not the major focus of IETF VoIP efforts. P2P does not employ a numbering plan but E.164 calling is supported through interconnections with the PSN and typically involves per minute charges. P2P uses friendly naming conventions in which end users choose a name for identity purposes. There is no type of authentication performed and indeed nothing to govern the operations of P2P. Basic P2P services enable users to download freely available software and make worldwide calls to any other user of the system.

4 VOIP RESEARCH AND REGULATORY EFFORTS

4.1 IETF Research and Development Efforts

The IETF is an organized activity of the Internet Society. This section is intended to provide an introduction to work within the Internet community that is specifically targeted to support emergency communications requirements, including those of the NCS. The initial foundation for Internet support of multimedia applications had already been accomplished through the addition of Quality of Service (QoS) and other enhancements designed to support application requirements. The Internet community has been voluntarily responding beyond QoS to the needs of emergency services since 9/11. Technical capabilities within the Internet community are very dynamic. Visit <http://www.ietf.org> for the latest information regarding the activities of the IETF. IETF documents have been referenced throughout this TIB where appropriate.

In recognition of the emerging role of the Internet to facilitate emergency communications, the Internet Engineering Steering Group (IESG) approved a charter to form an emergency preparedness-working group (WG) in early 2002. The IEPREP falls within the Transport Area of the IETF. The WG was chartered to develop a “Requirements for Internet Emergency Preparedness in the Internet” RFC, to detail the specific functions and technologies needed to provide support for Emergency Preparedness systems that utilize Internet Protocols. The WG was also authorized to develop an RFC for a framework for Supporting Internet Emergency Preparedness in IP Telephony, if it can be determined that IP telephony requires special treatment above what would be in the requirements document. The charter also stated that the international community needs advice as to what standards to rely on, in the form of a Best Current Practice (BCP) document. The charter of the IEPREP WG restricted the group from protocol or protocol feature development work. A number of objectives have been defined within the Internet community and these are worth examination. For example, the WG was instructed from the beginning not to focus on national regulations. The “only international requirements” position within the IETF is unique from other standards organizations, such as the ISO and the ITU-T, which routinely reserve protocol bits for national level definition so that national governments and Recognized Private Operating Agencies may satisfy their own national security and other cultural requirements in a cost effective, standardized way. Additional information regarding the work of the IEPREP is examined in the sections that follow.

The most current information regarding the work of the IEPREP can be found at <http://www.ietf.org/html.charters/ieprep-charter.html>.

4.2 General Requirements for ETS

RFC 3689, “General Requirements for ETS,” identified five existing standards that apply to International Emergency Preparedness operations by means of the PSN. They are: ANSI T1.631, ITU-T E.106, ITU-T F.706, ITU-T H.460.4, and ITU-T I.255.3.

RFC 3689 identifies seven general areas of requirements for Internet ETS. These are:

- Signaling

- Labels
- Policy
- Network Functionality
- Authorization
- Integrity and Authentication
- Confidentiality.

An additional area discussed by this informational RFC is that the set of requirements for ETS should not be constricted to just IP telephony applications, but should include applications such as the I-Am-Alive (IAA)⁷⁷ database system used in Japan. Thus, this RFC lays out general requirements that go beyond network signaling. The RFC identifies within the Internet community, application “labels” that have commonly been identified, are protocol independent, and may be used either within an application layer or within an IP header packet. This approach provides for a flexible environment that supports both emergency telecommunications applications and network protocol functions where required.

There are three ETS requirements issues identified by this RFC:

- Accountability
- Admission Control
- Digital Signatures.

The RFC recommended that solutions used to provide Emergency Telecommunications Service should not preclude the use of accounting mechanisms. The RFC states: “In cases where emergency related flows occur outside of controlled environments, the development of technologies based on admission control is not recommended as the foundation of emergency services.” Additionally, the RFC identified the potential for a DoS attack upon any type of emergency label supported and therefore recommended a further definition of operational and protocol measures to reduce the potential for DoS on the system performing authentication.

This informational RFC is beneficial for NS/EP because it defines a baseline level of support that may be expected from the public Internet and it identifies the use of one or more ETS label(s) as a solution for supporting emergency traffic via the Internet protocols and SLAs. But it is also important to recognize that this RFC acknowledges that mandating acceptance and support of Emergency Telecommunications Requirements is out of scope. The RFC states that “there is an expectation that business contracts, e.g., SLAs, will be used for those requirements.” In the absence of SLAs, “best effort” service is the default for the Internet.

4.3 IP Telephony Requirements For ETS

An Informational RFC 3690 *IP Telephony Requirements for Emergency Telecommunication Service (ETS)*⁷⁸ was published in February 2004. The RFC first seeks to inform the user community that the IETF is not empowered to mandate the requirements or capabilities supported by the independent networks that comprise the Internet. Since ISP service providers cannot be required to operate any telephony-related

gateways or services, users should expect that SLAs would be required to support certain requirements. Where no SLAs are in place, the Internet is expected to provide best effort service.

The RFC identifies five requirements that are added to those already identified in RFC 3689. The RFC states that the requirements must be taken in their entirety so they are highlighted here for brevity:

- The RFC requires that telephony signaling applications used with Internet telephony must be able to carry labels.
- It requires that the labels supported must be extensible to support a variety of types and number of labels.
- The RFC requires that signaling labels should have a mapping with the various emergency markings used in other telephony networks, such as the ANSI T1.601 markings used in the PSN. Where no mappings are possible the signaling can revert to a non-emergency enhanced level.
- Application layer IP telephony capabilities **MUST NOT** preclude the ability to do application layer accounting. The RFC further clarifies that “Accounting is a useful feature in support of billing and tracking down abuse of service.” Undoubtedly, the NCS will, in many cases, want to take advantage of the ability to monitor systems for potential abuse and for cost accounting services. However, the NCS has a requirement for non-traceability and it will require an exemption capability to disable all accounting and traceability.
- The RFC requires that the gateways and proxies that recognize ETS labels must be able to support a best available service. It suggests that the best available service should focus on the probability of forwarding packets and that the probability may reach 100% depending on the local policy associated with the label.

This RFC is helpful for NS/EP planning purposes because it clarifies that, in the absence of SLAs with vendors whose network provides transit for NS/EP traffic, there can be no reliability or other guaranteed service expected.

4.4 Technology Leveling

Global technology “leveling,” such as the Internet, is economically beneficial to the U.S. in terms of commerce, trade, and other globalization efforts, but the fundamental role of communications within the context of NS/EP has not changed. The QoS available to support Internet NS/EP VoIP technologies, in some respects, will test the nation to make choices where business interests and NS/EP interests may be in conflict. Nevertheless, the next generation ETS will benefit greatly from having an international scope like what the Internet provides.

4.5 International vs. National Standards Groups

The ISO, and ITU in particular due to its affiliation within the United Nations, historically have, through national representation, recognized the need to allocate mechanisms (e.g., designated or reserved bits) for use by national governments. The standards produced by these International standards organizations reflect the coordinated

intersection of government and private industry interests. The ANSI has served a similar role in the U.S. Today, the IETF operates under the auspices of the Internet Society, which is a self-governed entity. IETF standards have not designated or reserved bits to serve national interests.

4.6 FCC Activities

As a result of the events on September 11, 2001, the FCC formed the Homeland Security Policy Council in November 2001. The council is committed to working with industry to ensure the reliability and security of the nation's communications infrastructure. In December 2003, the FCC organized an Internet Policy Working Group (IPWG) to identify, evaluate, and address policy issues that will arise as telecommunications services move to Internet-based platforms. The FCC ruled on February 12, 2004, that an entirely Internet-based VoIP service is an unregulated "information service." Subsequently, the FCC initiated a process to determine what role it should play in the new environment, with regards to meeting the role of safeguarding the public interest.

In March 2004, the IPWG sponsored a solutions summit on "9-1-1/E9-1-1 Issues Associated with Internet-based Communications Services." In May 2004, the FCC held a solutions summit on "Disability Access Issues Associated with Internet-Protocol Based Communications Services."

On April 21, 2004, the FCC announced and released an Order on a petition by AT&T for a declaratory ruling that access charges do not apply to its service in which calls originate and terminate on circuit switched PSN facilities, but are routed on the Internet backbone. The FCC rejected AT&T's request, and ruled that the service at issue is "telecommunications service upon which interstate access charges may be assessed." The FCC noted that IP technology should be deployed based on its potential to create new services and network efficiencies, not solely as a means to avoid paying access charges.

The FCC has developed an informative section on its web site <http://www.fcc.gov/voip/welcome.html> that is devoted to providing the public with an introduction to the advantages and current disadvantages of VoIP technologies and other news of interest to the VoIP communities.

4.7 CALEA

In response to the FCC's December 2003 VoIP Forum, the Department of Justice, the U.S. Drug Enforcement Administration, and the Federal Bureau of Investigation submitted comments to the FCC regarding the Communications Assistance for Law Enforcement Act (CALEA). The comments stated that CALEA regulation of VoIP is needed to avoid industry confusion. The concluding remarks stated, "As the Commission drafts its VoIP notice of proposed rulemaking, Law Enforcement strongly urges the Commission to require VoIP providers to comply with CALEA to ensure that no new loophole is created that allows criminals, terrorists, and spies to use VoIP services to avoid lawfully authorized surveillance." The comments recommended that the Commission should adopt clear and specific CALEA regulations and not leave public safety to chance. It was further stated that prudent regulatory oversight would enable the

Commission to satisfy CALEA and still permit VoIP to succeed in the competitive marketplace.

4.8 Legislative Action

On December 23, 2004, President Bush signed into law H.R. 5419,⁷⁹ a bundled telecommunications legislative package known as the ENHANCE 911 Act of 2004. The title may also be cited as the “Ensuring Needed Help Arrives Near Callers Employing 911 Act of 2004.” The legislation establishes a Federal Coordination Office within the Department of Transportation, to perform oversight and ensure that the nation’s 9-1-1 PSAPs are funded and equipped to meet E9-1-1 needs. The program will spend \$250,000,000 for grants to states during each of the fiscal years from 2005 through 2009. The language in H.R. 5419 does not specifically include VoIP/E9-1-1 so it remains to be seen how the bill will be interpreted in subsequent regulations that implement the law.

5 OBSERVATIONS AND CONCLUSIONS

The events of September 11, 2001 have resulted in an increased level of cooperation among the government, industry, and the public. Approximately 10,000 GETS calls were processed during 9/11 over the PSN and 95% were completed. Many of the 5% that could not be completed were due to “destination unreachable” network responses. Thus, it has been successfully demonstrated that the NCS can provide the leadership necessary to influence the rebuilding and revitalizing of the telecommunications infrastructure paving the way for newer and better applications.

For over 100 years, the telecommunications infrastructure of the U.S. was based on a deterministic circuit switching architecture. Voice communications is not just another technology, but a cornerstone of our national security and emergency preparedness capabilities. In contrast, only one decade has passed since the first VoIP applications over the Internet appeared. VoIP is a promising star on the Internet horizon. The Internet community has been supporting the identification of emergency services requirements through the IETF standards development process. The IETF has been actively coordinating E9-1-1 requirements with organizations, such as the NENA, to ensure that sufficient IP capability is available to enable PSAPs operations. The interests of both the consumer and the government will be best served by constraining any regulation of VoIP to the lowest common denominator required to maintain national security and law and order. To date, there have been no national laws requiring the provisioning of Internet VoIP/EP E9-1-1 service.

Present day technology alternatives to dialing 9-1-1 exist. Modern telephone sets can respond to voice commands making it easy to program in different phone numbers for fire, police, etc., and to have those numbers dialed directly. At a minimum, the PSAP systems of the future can be automated to support caller activated voice interaction requiring only a minimum of operator intervention to handle exceptional emergency services requests.

The VoIP/E9-1-1 environment today presents the NCS with an array of very difficult technical, cost, and regulatory/legislative challenges. Technically, the QoS guarantees that are inherent in the PSN circuit-switched environment are difficult to duplicate within the Internet architecture. Additionally, PSN networks today provide the NCS with enhanced priority treatment of NS/EP voice communications by means of the ANSI T1.631 *High Probability Of Completion (HPC) Network Capability*⁸⁰ standard, which provides relief from network management controls. There is no Internet equivalent to provide a HPC with a deterministically guaranteed QoS that is standardized or widely deployed. The PSN operates down to the end user device level during commercial power failures, but the Internet does not. In terms of the development of new applications for NS/EP E9-1-1 services, the Internet offers tremendous opportunities that are highly unlikely to be cost effective in SS7 networks.

Through programs such as GETS, preferential emergency communications entities (Federal, state, local) have grown increasingly dependant on commercial service networks provided by the private sector. The NSTAC Recommendations addressed the GETS convergence issue as follows: “*The potential implications of Convergence and the*

[Next Generation Networks] NGN for GETS services include new blocking sources, lack of ubiquity and interoperability, lack of access to GETS features, disparate congestion handling, and a lack of commensurate network reliability and security.” The findings presented in this TIB affirm the NSTAC report and provide the basis for concluding that the convergence issues are extensible to VoIP/E9-1-1 services.

In looking beyond VoIP/E9-1-1, the requirements bar is raised to a much higher level when consideration is given to rapid adoption of VoIP by NS/EP agencies. Many NS/EP planning scenarios, including nuclear war, carry responsibilities that must include considerations that extend far beyond achieving lower communications costs. Fortunately, a number of NS/EP members are actively working with Internet technologies that incorporate QoS, MLPP, and other advanced capabilities that may experience very slow adoption and deployment in the commercial sector. The significantly higher level of technical skills necessary to successfully implement and maintain such operational capabilities is more commonly found within the NCS network support community.

The deployment rate for broadband, best-effort VoIP is expected to continue to experience rapid growth. The most commonly accepted approach today for supporting VoIP is over provisioning of network capacity. However, an informational RFC has been issued warning about possible congestion collapse induced by real-time applications in IP networks. One possible solution is that such applications as VoIP should detect network congestion and yield to other traffic. The RFC warns that “current real time media encoding and transmission practice ignores congestion considerations, resulting in the potential for trouble should VoIP become a broadly deployed service in the near to intermediate term. Poor user quality, unfairness to other VoIP and TCP users, and the possibility of sporadic episodes of congestion collapse are some of the potential problems in this scenario.”

The Internet presents unique challenges from an NS/EP perspective, because IETF Internet standards are intentionally designed for global use and have not been responsible for providing protocol mechanisms to identify or support national requirements. As a globally distributed network of networks, the Internet does not currently operate under any single point of control. The interests of a free market driven Internet and those of any nation are often divergent.

Historically, the Federal Government was able to view all domestically owned telecommunications network assets (including their international extensions) as potential support for NS/EP emergency purposes. Absent any regulations to the contrary, Internet assets are being defined in a manner that is independent of national borders, which by implication has exempted the Internet from U.S. national responsibilities. Nevertheless, it clearly is the responsibility of each national government to define and require support for national security requirements. The Internet has not changed the fact that wars are fought between nations. The role of telecommunications and information systems technologies (intercept, processing, encryption, etc.) has played a major role in the past history of national conflicts.

6 RECOMMENDATIONS

In light of the recommendations by the NSTAC, the NCS should consider the merits of a public service announcement campaign, sponsored by the appropriate organization or agency, to educate citizens about the changing nature of the nation's telecommunications infrastructure. This is especially important considering the number of children that have been instructed to dial 9-1-1 during an emergency.

Since it is expected that over time the PSN will converge with the Internet, the NCS needs to effectively plan for a future operational environment in which portions of the U.S. public telecommunications infrastructure could be experiencing sporadic congestion collapse, DoS attacks, or other failures that preclude public access to VoIP/E9-1-1 emergency services. Today, there is research into the ability to operate IP over Connection Oriented Network Service, which provides a deterministic alternative to CLNP. The Hybrid Optical and Packet Infrastructure project (HOPI)⁸¹ is examining the ability to provide time-multiplexed channels over a single 10-Gb/s λ . The NCS should encourage the development of technologies that can provide a deterministic VoIP/E9-1-1 NS/EP infrastructure.

It is recommended that the NCS advocate support for GETS by VoIP providers, ISPs, and/or carriers. Concurrently, the NCS should encourage an update of RFC 3487 to identify the requirement for support of GETS at the earliest possible date. However, it is important to acknowledge that accidental or unintentional misconfigurations by personnel could result in some GETS traffic failure during an emergency. The NCS should ensure that Internet DNS supports GETS E.164 addresses through coordination with the IANA registration process.

The NCS would benefit from having the means to regularly test whether or not a service provider is actually provisioned to satisfy NS/EP survivability traffic requirements under conditions that include, but are not limited to, concurrent, distributed, and sustained DoS attacks. Additional standardization, beyond the ANSI T1.500 series of standards, should be supported, especially as it relates to IP traffic congestion. It is additionally recommended that NCS work with its suppliers to establish appropriate SLA agreements that restrict the maximum level (e.g., 2%) of prioritized traffic load over NS/EP IP links to the appropriate level.

It is recommended that the NCS not seek to establish a requirement for public network support of an NS/EP code point(s) (e.g., Diff-SERV) due to the risks this creates for DoS attacks to further cripple communications during an NS/EP event. Instead, private SLAs are recommended. It is recommended that the NCS should support further study in this area and encourage wide participation in the process.

To protect the Internet from DoS attacks, especially at domain interconnect points during NS/EP emergencies, it is recommended that public VoIP providers, ISP, and IP transmission carriers should be encouraged to continue the Internet practice of resetting to zero the DSCP values of any packet received from an originating IP source not covered by an SLA.

It is recommended that NCS participate in the development of emergency communications standards, especially the ANSI Homeland Security Standards Panel. ANSI continues to play a key role in the coordination of United States national interests in global technology development. Additionally, it is recommended that the NCS assure a process by which the assignment and recommended use of “national” parameters defined by International standards organizations are regularly identified and processed by a national body.

In addition to the NS/EP assets already registered with IANA in association with the “*Communications Resource Priority for the Session Initiation Protocol (SIP)*,” the NCS should determine what additional registrations are needed to support the full range of NS/EP (e.g., FEMA, etc) requirements and then assist with the process.

It is recommended that the NCS determine requirements for IANA namespace registration for SIP Priority identification of NS/EP GETS traffic.

It is recommended that the NCS should encourage the development of automated E9-1-1 testing mechanisms that allow consumers to verify that the desired information (callback number, location, etc.) can be received at the PSAP without the need to interrupt PSAP employees.

Disaster situations are often regional and can involve disaster recovery efforts from multiple nations working in close cooperation. ETS traffic, therefore, needs to receive favorable treatment at international gateways and within national networks that provide an ETS. Adequate security/protection must be included in the authentication process to allow the service provider handling incoming international ETS traffic to validate its authenticity and employ countermeasures against DoS attacks.

Appendix A: Acronyms

1000BASE-T	1000 megabits per second base-band twisted-pair
100BASE-T	100 megabits per second base-band twisted pair
10BASE-T	10 megabits per second base-band twisted pair
AC	Access Categories
AC	Alternating Current
AF	Assured Forwarding
AGPS	Assisted Global Positioning System
AIFSN	Arbitration Inter-Frame Space Number
ALG	Application Layer Gateway
ALI	Automatic Location Identification
ANI	Automatic Number Identification
ANSI	American National Standards Institute
AP	Access Point
APCO	Association of Public-Safety Communications Officials
ARPA	Advanced Research Planning Agency
ARPAnet	Advanced Research Planning Agency network
AS	Autonomous System
ASIC	Application Specific Integrated Circuits
ASN.1	Abstract Syntax Notation One
AT&T	American Telephone & Telegraph
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transmission Mode
AUTOVON	Automatic Voice Network
BCP	Best Current Practices
BE	Best Effort
BGP	Border Gateway Protocol
C4I	Command & Control, Communications, Computers and Intelligence
CAC	Call Admission Controls
CAD	Computer Aided Dispatch
CALEA	Communications Assistance for Law Enforcement Act
CAMA	Centralized Automatic Message Accounting
CAP	Controlled Access Phase
CBR	Constant Bit Rate
CDMA	Code Division Multiple Access
CIDR	Classless Inter-Domain Routing
CIP	Critical Infrastructure Protection
CLEE	Competitive Local Exchange Carrier
CLNS	Connection Less Network Service

CODEC	Coder Decoder
CONS	Connection Oriented Network Service
CRDB	Coordinated Routing Data Base
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSN	Circuit Switched Network
CW	Contention Window
DANTE	Delivery of Advanced Network Technology to Europe
DBMS	Data Base Management System
DCCP	Datagram Congestion Control Protocol
DCF	Distributed Coordination Function
DDDS	Dynamic Delegation Discovery System
DHS	Department of Homeland Security
DID	Direct Inward Dial
Diff-Serv	Differentiated Services
DISA	Defense Information Systems Agency
DMS	Defense Messaging System
DNS	Domain Naming Service
DoD	Department of Defense
DoS	Denial of Service
DRSN	Defense Red Switched Network
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Loop
DSN	Defense Switched Network
DTE	Data Terminal Equipment
E.O.	Executive Order
E-9-1-1	Enhanced 9-1-1
ECC	Emergency Call Center
EDCA/WME	Enhanced Distributed Channel Access/Wireless Media Extension
EF	Expedited Forwarding
ELIN	Emergency Location Identification Number
eMLPP	enhanced Multi-Level Precedence and Preemption
EMSS	Enhanced Mobile Satellite Service
ENUM	Electronic Number
EOTD	Enhanced Observed Time Difference
ERL	Emergency Response Location
ESN	Emergency Service Number
ESRD	Emergency Services Routing Digits
ESRK	Emergency Services Routing Key
ESRP	Emergency Services Routing Protocol
ETS	Emergency Telecommunications Services
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency

Gb/s	Giga-bits per second
GCCS	Global Command and Control System
GETS	Government Emergency Telecommunications System
Ghz	Gigahertz
GNP	Global Network Positioning
GSM	Global System for Mobile Communications
HC	Hybrid Coordination
HCCA	Hybrid coordination function Controlled Channel Access
HCF	Hybrid Coordination Function
HF	High Frequency
HOPI	Hybrid Optical and Packet Infrastructure
HPC	High Probability of Completion
HTTP	Hypertext Transfer Protocol
Hz	Hertz
IAA	I Am Alive
IAB	Internet Architecture Board
IAIP	Information Analysis and Information Protection
IAM	Initial Address Message
IANA	Internet Address and Naming Authority
ID	Idaho
I-D	Internet Draft
IEEE	Institute of Electrical and Electronic Engineers
IEPREP	Internet Emergency Preparedness Working Group
IEPWG	Internet Emergency Preparedness Working Group
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
Int-Serv	Integrated Services
IP	Internet Protocol
IPDV	Instantaneous Packet Delay Variation
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPWG	Internet Policy Working Group
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISUP	ISDN Users Part
ITPITFR	Information Technology Progress Impact Task Force
ITU-T	International Telecommunications Union – Telecommunications sector
IWG	Interoperability Working Group
IXC	Inter-eXchange Carrier
JANAP	Joint Army Navy Air Force Publication

K/bps	Kilo bits per second
LAN	Local Area Network
LBE	Less than Best Effort
LEC	Local Exchange Carrier
MAC	Media Access Control
MAN	Metropolitan Area Network
MATTS	Mobile Air Transportable Telecommunications Systems
Mb/s	Mega-bits per second
Mbone	Multicast backbone
MC	Multipoint Controller
MCU	Multipoint Control Unit
MDI	Media Dependent Interface
MERS	Mobile Emergency Response Support
MIDCOM	Middle Box Communications
MIME	Multipurpose Internet Mail Extensions
MLPP	Multi-level Precedence and Preemption
MPLS	Multi-Protocol Label Switching
MRV	Multi-Radio Van
MSAG	Master Street Address Guide
MSO	Multiple System Operator
MTP	Message Transfer Part
N6	Technology and Standards Division
NAPT	Network Address Port Translation
NAPTR	Network Address Pointer Record
NAT	Network Address Translation
NCS	National Communications System
NENA	National Emergency Number Association
NGI	Next Generation Internet
NIPRnet	uNclassified IP Router network
NREN	National Research and Education Networks
NS/EP	National Security/Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NTCN-HF	National Telecommunications Coordinating Network – High Frequency
OFDM	Orthogonal Frequency Division Multiplexing
P2P	Peer 2 Peer
pANI	pseudo Automatic Number Identification
PBX	Private Branch eXchange
PD	Powered Device
PDA	Personal Digital Assistant
PER	Packet Encoding Rules
PHB	Per Hop Behavior

PHY	Physical Layer
POTS	Plain Old Telephone Service
PQ	Priority Queue
PRI	Primary Rate Interface
PS/ALI	Private Switch/Address Location Indicator
PSAP	Public Services Answering Point
PSE	Power Sourcing Equipment
PSN	Public Switched Telephone Network
QAP	Quality of Service enhanced Access Point
QoS	Quality of Service
QPS	Qbone Premium Service
RAS	Registration, Admission, Status
RCAP	Reserve Capacity Assurance for the Public
RFC	Request For Comments
RJ	Registered Jack
RPOA	Recognized Private Operating Agency
RR	DNS Resource Record
RSVP	Resource Reservation Protocol
RTP	Real Time Protocol
SDP	Session Description Protocol
SEQUIN	Service QUality Across Independently managed Networks
SHARES	SHARED RESources
SIP	Session Initiation Protocol
SIPRnet	Secret IP Router network
SLA	Service Level Agreement
SRDB	Selective Routing Data Base
SRV	DNS Services Record
SS7	Signaling System No. 7
SSRC	Synchronization SouRCe
STU	Secure Telephone Unit
STUN	Simple Traversal of UDP through NAT
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDOA	Time Differential of Arrival
TFRC	TCP Friendly Rate Control
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TN	Telephone Number
ToS	Type of Service
TSPEC	Traffic Specification
TURN	Transversal Using Relay NAT
TXOP	Transmission Opportunity

UA	User Agent
UAC	User Agent Client
UDP	Unreliable Datagram Protocol
UDP	Universal Datagram Protocol
UHF	Ultra High Frequency
URI	Uniform Resources Indicator
USA	United States of America
U-TDOA	Uplink Time Difference of Arrival
V	Volts
VHF	Very High Frequency
VLAN	Virtual LAN
VLf	Very Low Frequency
VoIP	Voice over Internet Protocol
VPIM	Voice Protocol for Internet Mail
VPN	Virtual Private Network
VPNs	Virtual Private Networks
W	Watts
WAN	Wide Area Network
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPS	Wireless Priority System
WPS	Wireless Priority System
WRR	Weighted Round Robin
WSM	WiFi Scheduled Media
XML	eXtensible Markup Language

Appendix B: Bibliography

1. "Preferential Emergency Communications, From Telecommunications to the Internet." Carlberg, Desourdis, Polk, Brown. Kluwer Academic Publishers. 2003.
2. "Practical VoIP using VOCAL." Dang, Jennings & Kelly. O'Reily. 2002.
3. "An Engineering Approach to Computer Networking." S. Keshav. Pearson Education. Sixth reprint 2003.
4. "Volume Two: Homeland Security, A Governor's Guide To Emergency Management." NGA Center for Best Practices. 2002 by the National Governors Association.
5. "A New Charging Scheme for Multi-Domain DiffServ Networks." Liang Ji, Theodoros N. Arvanitits and Sandra I wooley. Electronic, Electrical and Computer Engineering, School of Engineering, The University of Birmingham, United Kingdom.
6. "Analog Centralized Automatic Message Accounting E911 Trunk." Release 12/2(11)T. Cisco System Incorporated.
7. "Cisco Emergency Responder Administration Guide." Cisco Systems Incorporated. 2003.
8. "Qwest Detailed SR/ALI to MPC/GMLC Interface Specification for TCP/IP Implementation of TIA/EIA/J-Std-036 E₂ with Phase I Location Description Addition." Intrado Incorporated. April 2004.
9. "An Architecture for E9-1-1 in VoIP Networks." An engineering white paper. Nortel Networks. 25 March 2004.
10. "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Priority Telecommunications Services (EPTS); Part 1: Requirements Analysis." ETSI TR 102 302-1 V4.11.1 2004.
11. "Telecommunications and Internet Protocol Harmonization Over Network (TIPHON) Release 4; Test Scenarios; Security testing – H.323 environment." ETSI TS 101 888 V4.2.1. 2003.
12. Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Service Independent Requirements Definition; Service and Network Management Framework; Overview and Introduction." ETSI TS 101 303 V4.1.1. 2003.
13. "Managing Call Flows Using H.323." DigiNet Corporation. Mark A. Miller. May 2002.

14. "IEEE 802.11e Wireless LAN for Quality of Service." Stefan Mangold, Sunghyun Choi, Peter May Ole Klein, Guido Hiertz, Lothar Stibor. Proceedings European Wireless 2002, Florence, Italy, February 2002.
15. "9-1-1 Calls for Voice-over-IP Ex-Parte Filing for Docket 94-102." Columbia University Department of Computer Science. Henning Schulzrinne. Feb 2003.
16. "Using IEEE 802.11e MAC for QoS over Wireless." Priyank Garg, Rushah Doshi, Russell Greene, Mary Baker, Majid Mallek, Xiaoyan Cheng. Computer Science Department, Stanford University.
17. "MIT Implementation." Internet2 Member Meeting SIP.edu Initiative. Dennis Baron. October 14, 2003.
18. "Internet2 VoIP Initiatives." Walt Magnussen, Ph.D., Director for Telecommunications Texas A&M University. January 2004.
19. "Internet Emergency Communications." Shin-Gak Kang. ETRI Protocol Engineering Center. June 25, 2003.
20. "Intrado PS/ALI for CLEC's, Reference Guide, Version 2.2." Intrado Incorporated. 2001.
21. "Multi Service Provider Interfaces for IP QOS, IP VPNs and IP Telephony." ITU-T Focus Group on Next Generation Networks. Cisco Systems Incorporated. 23 June 2004.
22. "ETS Support in H.323." Delta Information Systems Incorporated. Gary Thom. February 2003.
23. "New Perspectives on Voice Quality." Callisma. Matt Stoen. October 2002.
24. "VoIP and Amateur Radio." QST ARRL. Steve Ford. February 2003.

Appendix C: NS/EP Requirements and Operational Assets

C.1 NS/EP Requirements and Operational Assets

Voice over any protocol plays such a critical role, not only for E9-1-1 crisis events, but also for national security needs, that some discussion of NS/EP requirements for VoIP that go beyond E9-1-1 is warranted.

Part two of this appendix identifies and discusses NS/EP requirements and services that have been defined by various Federal affinity groups responsible for providing emergency services operations. The umbrella of emergencies within the context of the NCS range from systems that support single, personal injury incidents, to a natural disaster that can cover a large region of the nation, acts of terrorism, and even the use of weapons of mass destruction, including nuclear weapons. For presentation purposes, this section first examines the range of requirements that have been defined by the NCS to support the broadest range of emergencies that can face the United States.

Part three of this appendix provides a brief overview of select existing NS/EP networks and services that comprise portions of the NCS core assets.

C.2 NCS NS/EP Functional Requirements

In a white paper *The Emergency Telecommunications Service in Evolving Networks*,⁸² Hal Folts of the NCS enumerated 14 functional requirements (see **Figure C-1**), which were identified by a government working group (WG).

C.2.1 NCS Requirements Descriptions

The set of NS/EP requirements defined in **Figure C-1** covers the needs of a wide spectrum of users that range from the public's ability to make emergency 9-1-1 emergency phone calls up to and including continuity of government operations involving the President of the United States. Thus a broad range of integrated technologies, networks, and systems are required to satisfy the full spectrum of NS/EP requirements.

For example, with respect to emergency communications generated by the public in the form of E9-1-1 calls, telecommunications carriers do not currently provide priority treatment. However, this may be changing, as described in section 3 of this TIB.

Historically, priority treatment has been best exemplified by the capabilities found within the Department of Defense (DoD) where five distinct levels of priority treatment (i.e., flash override, flash, immediate, priority, and routine) can be applied by the user to both voice and data traffic.

Enhanced Priority Treatment	Services supporting NS/EP missions must be provided priority treatment over other traffic.
Secure Networks	Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
Non-Traceability	Selected users must be able to use NS/EP services without risk of usage being traced, i.e., without risk of user or location being identified.
Restorability	Should a disruption occur, services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.
International Connectivity	Services must provide access to and egress from international carriers.
Interoperability	Services must interconnect and interoperate with other selected government or private facilities, systems, and networks.
Mobility	The communications infrastructure must support transportable, re-deployable, or fully mobile communications (e.g., personal communications service, cellular, satellite, high frequency radio).
Ubiquitous Coverage	Services must be readily accessible to support the national security leadership and inter- and intra-agency emergency operations, wherever they are located.
Survivability/Endurability	Services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or man-made disaster up to and including nuclear war.
Voice Band Service	The service must provide voice band service in support of presidential and other communications.
Broadband Service	The service must provide broadband service in support of NS/EP missions (e.g., video, imaging, web access, multimedia).
Scaleable Bandwidth	NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.
Affordability	Services must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf technologies, services).
Reliability/Availability	Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

Figure C-1 NS/EP Requirements

(Figure courtesy of the NCS)

C.3 National Security/Emergency Preparedness Networks

Each of the 23 members of the NCS operates one or more private networks for voice, data, video, and other purposes. Each agency brings a customized set of computer processing systems and interoperable networking equipment assets that may be used jointly for NS/EP. While space does not permit a full examination of each network, it is clear that several key networks have the capability to present a properly authorized NS/EP user with a great diversity of communications capabilities. This section presents an overview of the following networks: (1) DoD networks, (2) Government Emergency

Telecommunications System (GETS), (3) Wireless Priority System (WPS), (4) SHARED RESOURCES (SHARES), and (5) Federal Emergency Management Agency (FEMA) deployed capabilities. The sum total of these limited NS/EP assets, when added to state and local government emergency response (e.g., E9-1-1) capabilities provide the nation with a formidable total NS/EP system that renders a wide-range of response options. The reader is reminded that this set of networks by no means constitutes the full set of NS/EP assets. For example, should emergency requirements for extraordinary hospital support arise, adding one additional NCS member to the mix, the Department of Veterans Affairs, adds networked capabilities to link in 171 medical centers; more than 350 outpatient, community, and outreach clinics; 126 nursing home care units; and 35 domiciliaries. Clearly, the combined assets of all 23 NCS member agencies are considerable.

C.3.1 DoD Networks

The Defense Information Systems Agency (DISA) manages network services within the DoD. It would require a series of TIBs to provide a comprehensive treatment of DoD network assets, but fortunately that level of detail is not required. DoD networks may currently be described along the lines of voice, data, and video capabilities, with the understanding that convergence is underway.

One of the most distinct features that has been available for decades in both voice and data communications networks is the capability for priority precedence and preemption on a call-by-call and message-by-message basis. This will be examined in more detail in subsequent subsections. The military use of mobility communications, more commonly known as “tactical communications,” is extensive and ranges from battlefield tanks to submarines. Therefore, satellite and radio systems (High Frequency [HF], Very High Frequency [VHF], Very Low Frequency [VLF]) may also be employed.

C.3.1.1 DoD Voice Networks

There are at least three distinct networks that provide voice services within the DoD. These are: the Defense Switched Network (DSN), the Defense Red Switch Network (DRSN), and the Enhanced Mobile Satellite Service (EMSS).

C.3.1.2 Defense Switched Network (DSN)

The DSN is a global private-line telephone network that in the 1990’s became the digital successor of the analog Automatic Voice Network (AUTOVON), which was activated in December 1963. The DSN Multilevel precedence and preemption (MLPP) capabilities ensure that the highest-priority calls achieve connection quickly to support crisis situations. The precedence levels supported in order from highest to lowest are: (1) flash override, (2) flash, (3) immediate, (4) priority, and (5) routine.

In addition to voice, the DSN also provides global data and video services using dial-up switched 56 kbps or 64 kbps ISDN services. Secure voice services are provided by the Secure Telephone Unit, Third-Generation/Secure Terminal Equipment (STU-III/STE) family of equipment that provides end-to-end encryption over non-secure DSN circuits. Interfaces are provided between strategic and tactical forces, allied military networks, and EMSS.

The military services and agencies in the DoD are authorized users, but other Federal Government departments and agencies, allies, and DoD contractors can use the DSN with approval. The DSN also can be used to provide access to the GETS.

C.3.2 DoD Data Networks

From the mid 1960's through the late 1990's, the DoD operated the Automatic Digital Network (AUTODIN) data network. It was a store and forward network that supported the same precedence and preemption services as the Automatic Voice Network (AUTOVON). AUTODIN supported the secure transmission of unclassified through Top Secret data. The data transmitted through the AUTODIN network were formatted in accordance with the Joint Army Navy Air Force Publication (JANAP) 128 specification. Essentially, this format was an early form of electronic mail, with the exception that high precedence data could preempt lower precedence data. For example, a routine six-page message could be preempted while printing by a flash precedence message, requiring the printing of the routine message to start over at the beginning once the flash message had completed printing. Eventually, the capabilities of AUTODIN evolved into multiple networks, including the Defense Data Network (DDN), the Defense Messaging System (DMS), the uNclassified but sensitive IP Router Network (NIPRNet), the Secret IP Router Network (SIPRNet), and other special purpose networks. The DMS is implemented using ITU-T X.400 Messaging and ITU-T X.500 directory services. DMS supports organizational messages (official documents) and individual messages (informal email). The uNclassified but Sensitive IP Router Network (NIPRNet) supports unclassified applications and controlled Internet access. Direct connection data rates range from 56 Kilo bits per second (K/bps) to 155 M/bps. Remote dial-up services are available up to 56 K/bps.

SIPRNet supports the DMS for online message preparation, coordination, and release of organizational messages. Additionally, SIPRNET supports the Global Command and Control System (GCCS), which is the DoD's largest interoperable command and control data network. It also support collaborative planning and classified war fighter applications. Direct connection data rates range from 56 Kbps to 155 Mbps for the NIPRNet, and up to 45 Mbps for the SIPRNet. Remote dial-up services are also available, ranging from 19.2 kbps on SIPRNet to 56 kbps on NIPRNet.

C.3.3 GETS

Today, the Department of Homeland Security, Office of the Manager, National Communications System manages the Government Emergency Telecommunications Service (GETS). The GETS capability was fielded in October 1994, and unlike E9-1-1 GETS is not available to the public; it is reserved for use by designated official authorities, such as emergency responders. As of October 2003, there were approximately 60,000 authorized users of GETS. On September 11, 2001, approximately 1 out of every 1,000 calls in New York City was a GETS call. In 2001, the NCS mission was expanded to include protection of critical information assets, as directed by the Office of Homeland Security.

GETS provides an emergency access procedure and special processing for local and long distance telephone calls through the PSN. It is available for use during natural and man-made disasters or emergencies. The process for establishing a GETS call is:

1. Dial a designated non-geographical area code number in the form: 710-NCS-GETS.
2. Enter a Personal Identification Number.
3. Dial the destination number.

In addition, Carrier Access Codes for AT&T, MCI, or Sprint plus 710-NCS-GETS, as well as special 800 numbers, are provided to users on the back of the GETS card as alternatives.



Figure C-2 GETS Phone Card

(Figure courtesy of the OMNCS)

GETS supports five classes of users: (1) National Security Leadership, (2) National Security Posture and U.S. Population Attack Warning, (3) Public Health, Safety, and Maintenance of Law and Order, (4) Public Welfare and Maintenance of National Economic Posture, and (5) Disaster Recovery. GETS can be accessed from a number of Federal networks, including the Federal Telecommunications Service, the Diplomatic Telecommunications Service, and the Defense Information Systems Network.

The technical foundation for GETS was defined by publication of HPC. The standard allocates an 8-bit NS/EP call identifier (11100010) that is carried in the calling party's category field of the Initial Address Message (IAM) to render a higher probability of call completion during periods of SS7 network congestion. The NS/EP code identifier marked calls are assigned Signaling Priority Level 1 to enable Priority Treatment by the SS7 network. Additionally, Signaling System No. 7 (SS7) - Message Transfer Part (MTP), ANSI T1.111-1996,⁸³ approved March 14, 1996, provided for IAM Signaling Priority levels (0, 1, 2, 3), with POTS = 0, NS/EP calls = 1, and priority 2 and 3 reserved for traffic and network control/management. Annexes A and B in ANSI T1.111.5 specify priority assignments for Integrated Services Digital Network User Part (ISUP) messages transferred between U.S. SS7 networks and establish engineering principles for priority assignment. The standard requires that all IAMs be assigned priority level 0 with the provision that "Message priority level 1 shall be limited to those network services or

capabilities that have been approved in ANSI T1 standards to have an IAM message priority of 1 (e.g., High Probability of Completion, Multi-level Precedence and Preemption, Emergency Calling Service).”

In addition to HPC, GETS calls receive advantaged treatment over normal calls through a variety of methods. Two GETS features that are triggered by the HPC class mark are Trunk Queuing and Exemption from Restrictive Network Management Controls. In the presence of the GETS code point, when a GETS call encounters a restrictive network management control that has been activated to reduce traffic overload to a congested route, the Local Exchange Carriers (LEC) provide the GETS call priority by exempting the call from this restriction. If the GETS call finds all circuits busy in the route after receiving the exemption, the LEC will provide further treatment by applying Alternate Carrier Routing, which is an Advanced Intelligent Network capability that automatically tries all three GETS inter-exchange carriers (IXCs).

During convergence, the NS/EP HPC SS7 supporting GETS will need to be interoperable with the form(s) of advanced priority treatment that are possible to provide within the context of the Internet, as described within RFC 3487. Instead of a HPC, the Internet is capable of providing a lowered probability of dropped packets.

C.3.4 Wireless Priority Service

In the 1990’s, the NCS began efforts to develop and implement a nationwide cellular priority access capability to serve as a cellular equivalent to GETS. Subsequently, it was necessary for the FCC to determine that WPS is in the public interest and optionally allowed carriers to implement support.

Key requirements for the WPS include:

- Up to 200,000 simultaneous users
- WPS calls may not exceed 25% of engineered capacity
- Average call holding times of 150 seconds
- No special allocation of spectrum
- Existing cell calls may not be preempted.

WPS can be initiated on a call-by-call basis by dialing the WPS prefix *272 followed by the number on a WPS subscribed phone. Five priority levels were defined for NS/EP wireless calls. WPS services are assigned a priority on a scale of 1 to 5 (with 1 being the highest) based on the appropriate class of service.

WPS is based on an algorithm known as the Reserve Capacity Assurance for the Public (RCAP). RCAP capability is supported in both GSM and Code Division Multiple Access (CDMA) software. The algorithm operates like a governor by restricting NS/EP users to approximately 25% of the capacity of any cellular site under all levels of congestion. This is intended to preclude situations in which the general public could be preempted from cellular access by WPS priority calls. The systems are engineered to ensure that the public encounters no more blocking during a WPS emergency than it would without any priority capability in place. The GSM technology is based on a feature called enhanced Multi-Level Precedence and Preemption (eMLPP). During congestion, eMLPP allows

each emergency call to queue for the next available radio channel, without preempting any calls in progress. This means that all calls using WPS phones receive priority service under conditions of radio channel congestion. WPS GSM priority queuing implementations do vary slightly from one vendor to the next. The WPS wait in each queue has been engineered to last approximately 30 seconds under the heaviest congestion situations.

C.3.5 SHARES

One of the important emergency response capabilities developed through the combined efforts of the 23 NCS member organizations is the SHARed RESources (SHARES) High Frequency (HF) Radio network. SHARES is designed to provide a single emergency message handling system by bringing together the existing HF radio resources of Federal, state, and industry organizations to share communications resources when normal communications are either destroyed or otherwise unavailable.

There are approximately 1,100 HF radio stations, representing 91 Federal, state, and industry contributors comprising the network. SHARES stations are located in every state and at 20 overseas locations. The SHARES network has over 150 HF frequencies reserved for use during emergencies.

The Federal community also uses SHARES as a forum for addressing HF radio interoperability issues. The SHARES Interoperability Working Group (IWG) is established as a permanent standing committee under the NCS. The SHARES IWG currently consists of 146 members, representing 106 separate participating organizations.

The NCS has expanded the number of National Telecommunications Coordinating Network - High Frequency (NTCN-HF) radio stations participating in SHARES to include all of the major regulated telephone service providers.

C.3.6 FEMA

To support the needs of government managers and first responders, the Federal Emergency Management Agency (FEMA) Mobile Operations Division operates five geographically dispersed Mobile Emergency Response Support (MERS) detachments and one Mobile Air Transportable Telecommunications System (MATTS). The MERS Detachments are located at Bothell, Washington; Denver, Colorado; Denton, Texas; Thomasville, Georgia; and Maynard, Massachusetts. The MATTS is located at Berryville, VA. The purpose of MERS and MATTS is to support the Federal, state, and local responders. They were not designed to provide direct support to disaster victims.



Figure C-3 Multi-Radio Van (MRV)

(Figure Courtesy of FEMA)

To illustrate one of many FEMA deployable systems **Figure C-3** depicts the MRV, which is a 30-foot long communications van. The roof contains a rear section that opens to deploy a 2.4m satellite antenna. The remainder of the roof contains additional antennas for use with the MRV suite of radios. The interior of the van includes a small office and work area in the front. The MRV's screen room, which contains communications gear, is in the rear. The MRV truck carries two self-contained 20 kilo (k)W power generators. A second antenna system mounted on another truck can be connected to provide an additional satellite link.

The MRV is capable of supporting communications diversity through numerous technologies. It contains HF radios, encrypted VHF, and Ultra High Frequency (UHF) radios, with telephone interface capabilities. It also contains a Ku band satellite system, which can provide connectivity for telephones, LAN, WAN, compressed video 2-way teleconferencing, and full broadcast television. There are computers with scanning, printing, copying, and facsimile capabilities. The MRV also has a small telephone switch that can support 48 telephone lines and landline connections.

C.4 Conclusions

The NCS systems described in this appendix support voice communications and data communications. As VoIP evolves each NCS agency can be expected to incorporate its new applications and services. Evolution of existing SS7 and other legacy voice based networks will result in new opportunities for cooperative use of VoIP technologies among all NCS members during emergencies of all scale levels.

Appendix D: VoIP QoS Issues

D.1 Introduction

When circuit switched networks become congested (e.g., Mother's Day) they block new call attempts by returning an "all trunks busy" signal known as a reorder signal. Existing circuit-switched calls are not affected by the congestion, because once a call is connected the network provides a guaranteed QoS until the call is completed. There is no guaranteed QoS in the Internet today. Instead, each packet is an autonomous entity such that upon entering the network it contains the source and destination addressing information necessary for worldwide routing. The network holds no state information so all traffic operates in "connectionless" mode. Instead of denying access, the Internet today continues to accept new data on a "first come first served" basis until such time as the incoming traffic exceeds the processing capacity at a network node. When a node reaches maximum processing capacity, newly arriving packets are simply discarded. TCP adjusts transmission parameters for computer-to-computer communications and although throughput may be reduced the transmission continues.

Voice and other real-time applications require networks to provide a guaranteed QoS. Deploying QoS on a single network requires various mechanisms, including scheduling, admission control, shaping, control on routing latency/performance, and resource planning. The provisioning of end-to-end QoS over multiple networks involves the concatenation of a variety of independently managed networks, each of which may be based on different networking technologies. The following discussion of different means to provide IP QoS includes:

- Bandwidth over provisioning
- Virtual Circuits
- IETF QoS
- IEEE 802.1p.

D.1.1 Bandwidth Over-Provisioning

Instead of deploying a QoS mechanism throughout all Internet networks, an alternative idea has been to simply over provision network bandwidth in the core. Network bandwidth over-provisioning requires that the amount of bandwidth in the various links is far greater than the peak utilization value. This is usually quantified either by the absence of congestion in any part of the network for a finite amount of time, or so that the average network load is always less than a finite percentage in each link. So long as the network is constructed with over-provisioned core links and with hardware capable of delivering packets at wire speed, over-provisioning offers QoS "like" guarantees for capacity. It is however, still necessary to enable QoS support (e.g., DSCP marking, traffic shaping, etc.) on access links. Additionally, it is necessary to engineer stringent guarantees for delay variation, which are a function of the network load.

D.1.2 Virtual Circuits

An architecture that can provide QoS guarantees is Asynchronous Transmission Mode (ATM). The ATM Constant Bit Rate (CBR) capability can be used to provide the equivalent of a leased line virtual circuit. However, a QoS based on ATM means that it must be deployed at every hop in the network, including all attached LANs. Moreover, ATM has failed to gain wide use as a LAN technology, and its great complexity and inefficiencies have held back its full deployment as the single integrating network technology. Further, ATM introduces addressing overhead that is not really needed in IP networks, reducing the efficiency of the protocol. Many of the best capabilities of ATM were incorporated into the RFC 3270 *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services*⁸⁴ and related specifications. MPLS is a generic layer 2 packet switching protocol. MPLS works by encapsulating packets with a simple header containing one or more labels. MPLS labeled packets are forwarded along a virtual circuit based on the contents of the labels.

D.1.3 IETF QoS

IETF working groups have defined two approaches to provide QoS mechanisms in the Internet:

- IP Integrated Services (Int-Serv)
- Differentiated Services (Diff-SERV).

D.1.3.1 Integrated Services

RFC 1633 *Integrated Services (Int-Serv) in the Internet Architecture – an Overview*⁸⁵ describes a service model to provide fine-grained assurances to individual flows. Presently, there are two services defined in the model:

- RFC 2212, *Specification of Guaranteed Quality of Service*,⁸⁶ which offers quantifiable bounds on latency to flows that conform to a traffic specification.
- RFC 2211, *Specification of the Controlled-Load Network Element Service*,⁸⁷ which offers delay and packet loss “equivalent to that of a lightly loaded network.”

Int-Serv requires state information in each participating router and, if this state information is not present in every router along the path, QoS guarantees cannot be ensured. Usually, but not necessarily, Integrated Services are associated with RSVP signaling. Signaling processing times and the need for storing per flow information in each participating node is believed to lead to scalability problems, particularly in the core of the Internet.

D.1.3.2 Differentiated Services

RFC 2475 (Diff-SERV) provides a layer 3 framework to control aggregate flows. State awareness is required only in the edge of a Diff-SERV domain. The edge of a domain is where packets are classified into flows and the flows are conditioned (marked, policed, or shaped) to the traffic conditioning specification. Then, the flows are aggregated. A DSCP identifies a per-hop behavior (PHB) and it is set in each packet header. The DSCP is carried in the Differentiated Services (DS) field, which is formed from six bits of the

former Type of Service (ToS) IP header octet. The PHB is the forwarding behavior, which is to be applied to the packet in each node in the Diff-SERV domain. Although there is a recommended DSCP associated with each PHB, the mappings from DSCPs to PHBs are defined by the DS-domain. Several DSCPs can be associated with the same PHB. Three major PHBs are:

1. RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IP *version 4 (IPv4) and IPv6 Headers*.⁸⁸ The class selector PHB subsumes the IP precedence semantics of the former ToS byte and offers relative forwarding priorities.
2. RFC 3248 *A Delay Bound alternative revision of RFC 2598*.⁸⁹ The Expedited Forwarding (EF) PHB guarantees that packets will have a well-defined minimum departure rate, which, if not exceeded, ensures that the associated queues are short or empty. EF is intended to support services that offer tightly bounded loss, delay, and delay variation.
3. RFC 2597 *Assured Forwarding (AF) PHB group*⁹⁰ offers different levels of forwarding assurances for packets belonging to an aggregated flow. Each AF group is independently allocated forwarding resources. Packets are marked with one of three drop precedence, such that those with the highest drop precedence are dropped with lower probability than those marked with the lowest drop precedence. DSCPs are recommended for four independent AF groups, although a DS domain can support more or fewer AF groups.

D.1.4 IEEE 802.1p

Most LANs are based on the IEEE 802 standards. IEEE 802.1p *Traffic Class Expediting and Dynamic Multicast Filtering*⁹¹ defines a field in the layer 2 header of the 802 packets to carry one of eight priority values. LAN devices, like switches, are expected to handle the traffic according to the 802.1p priority, by means of appropriate queuing mechanisms. The scope of 802.1p is limited to a LAN so that once the packet crosses a layer 3 device the 802.1p tag is removed. It can, however, be mapped to a layer 3 equivalent, such as the DSCP byte of the IP header.

The IEEE 802.1p signaling technique is a specification that also offers provisions to filter multicast traffic, to ensure it does not proliferate over layer 2 switched networks. The 802.1p header allows packets to be grouped into eight possible traffic classes. The IEEE has made broad recommendations concerning how network managers can implement these traffic classes, but it stops short of mandating the use of its recommended traffic class definitions. It can also be defined as best-effort QoS at layer 2 and is implemented in network adapters and switches without involving any reservation setup. 802.1p traffic is simply classified and sent to the destination; no bandwidth reservations are established. 802.1p is a spin-off of the 802.1q *Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks*⁹² (Virtual LANs [VLAN] tagging) standard and they work in tandem. The 802.1q standard specifies a tag that appends to a MAC frame. The VLAN tag has two parts: the VLAN ID (12-bit) and Prioritization (3-bit). The prioritization field was not defined in the VLAN standard. The 802.1p implementation defines this prioritization field. This effort defines a 32-bit tag header that is inserted after a frame's normal destination and source address header info. Switches, routers, servers, even desktop systems, can set these priority bits. This extension to the 802 framing is where the prioritization information resides.

While there is general agreement today that 802.1p is the mechanism to tag frames for prioritization, there is no single uniform approach to implementing the underlying queuing mechanisms that are needed to actually implement the priority flows. The eight levels of priority in 802.1p are similar to the outdated IP ToS bits. Network adapters and switches route traffic based on the priority level. Using layer 3 switches allows mapping 802.1p prioritization to DSCP or ToS before forwarding to routers. Even though the IEEE standard supports up to eight priority level definitions, numerous vendors support only two or three priority queues in their switches. For example, a switch might assign 802.1p values of 0 through 3 to a low-priority queue and priority levels 4 through 7 to a high-priority queue. In essence, this reduces the priority levels to just two, so any data defined as high priority and classified as a level 7 priority rides alongside priority level 4 traffic. Switches implementing prioritization with more than two traffic queues are capable of offering a broader range of priority levels. It is important to understand how the vendor has mapped the different priority levels recommended for use with 802.1p to the devices traffic queues. Today, it is possible that two switches with the same number of traffic queues could forward traffic marked with the same priority level (e.g., layer 3), but with differing internal priorities.

D.2 Internet QoS Research Efforts

If VoIP/E9-1-1 Internet service is to receive any better treatment than “best effort,” then some mechanism to provide QoS is needed. The short supply of QoS commercial offerings by ISPs and carriers gives incentives to look toward the research community for possible solutions. Worldwide, a number of advanced Internet computer research networks are operational for the purpose of developing and testing new applications. The names of a few of these efforts are Internet2, the Abilene Backbone Network, the HOPI project, and GÉANT. This section examines the results in the area of QoS provisioning that has been reported on by two of these projects, Internet2 and GÉANT.

D.2.1 Internet2 Research Efforts

Internet2 is a consortium led by 206 universities working in partnership with industry and government to develop and deploy advanced network applications and technologies, with the goal of accelerating the creation of a Next Generation Internet (NGI). Internet2 worked to specify and deploy a Quality of Service Backbone (Qbone) Premium Service (QPS), to provide an inter-domain virtual leased-line IP service built on Diff-SERV (i.e., DSCP) QoS forwarding primitives between May 1998 and October 2001. QPS was specified by the Draft QBone Architecture, which was demonstrated, but never successfully deployed operationally.

It is recognized that other Internet2 VoIP efforts (i.e., *Implementation of QoS-Provisioning System for Voice over IP*⁹³) reported on congestion control mechanisms, such as call admission control (CAC). Although a variety of CAC mechanisms (including the familiar fast busy) have been proposed and offered in commercial products, no one method has gained dominance. Indeed, CAC has not been widely adopted within the Internet. Thus, the Inter-domain perspective of the Premium IP service project appears to be more appropriate for examination from an NS/EP perspective.

The Internet2 QPS design team identified the reasons that QPS failed to deploy in an informational document titled, *Why Premium IP Service Has Not Deployed (and Probably Never Will)*.⁹⁴ The chief obstacles described in this report included: (a) poor incremental deployment properties, (b) intimidating new complexity for network operators, (c) missing functionality on routers, and (d) serious economic challenges. More specifically, the team determined that the costs of providing Premium IP services were too high relative to the perceived benefits. More important for NS/EP considerations is the team observation that even if it can be successfully deployed, Premium IP service fundamentally changes the Internet architecture, running contrary to the end-to-end design principles, and thus threatening the future scalability and flexibility of the Internet. The design team asserted that the conclusions reached apply not just to Premium, but to any IP-based QoS architecture. The Internet congestion collapse described in RFC 3715 is not comparable to the QPS report details, because one attempted to implement QoS congestion control mechanisms and the other did not. However, the findings published by Internet2 are important considerations as the NCS moves forward to incorporate Internet VoIP/E9-1-1 for NS/EP. A careful detailed review of the findings contained in the Internet2 QPS report is provided in the following subsections to assist the NCS efforts.

D.2.1.1 Qbone IP QoS Premium Service and Denial of Service

The Qbone team initially noted that Premium service on a well-provisioned network would do little to change packet forwarding under normal conditions. Internet2 networks operate using the latest advanced technologies and high-speed links. Thus, the network environment is well provisioned and generally lightly loaded. The packet loss and jitter experienced by “best-effort” traffic on Internet2 paths is almost always zero or is due to non-congestive causes.

The Qbone Premium Service project was intended to provide a guaranteed QoS, by eliminating the probability that network congestion could result in a network transaction failure. The ability of any network to offer guaranteed service levels is an important consideration from the vantage point of NS/EP events, which naturally cause network congestion. Although well-provisioned networks typically deliver very good performance, under periods of congestion they can deliver unpredictable service or in the worst case (e.g., DoS attack) no service.

Traffic forecasting and statistical provisioning have traditionally worked well for circuit-switched networks. IP data networks are, however, more difficult to predict. This is due in part to the fact that there is a no-usage based pricing policy. Unless pricing disincentives are employed, individual users can very significantly and very suddenly affect network utilization. Protection, at least of priority traffic, from sudden changes in network utilization is the test of guaranteed service.

D.2.1.2 Overview of Deployment Problems

The Qbone Premium Service team report expressed confidence that every deployment problem they encountered could have been overcome. The question raised by the team, however, is “at what financial cost?” Many of the problems could have been overcome by incurring additional up-front costs. Overcoming other problems would have required

recurring costs. Still other problems required both up-front and recurring costs to overcome. The following subsections describe in detail the difficulties that could be encountered in the deployment of DSCP for NS/EP.

D.2.1.2.1 Poor QoS Incremental Deployment Properties

To support a Premium IP QoS, the Qbone team determined that a network must provide expedited forwarding (EF), in accordance with RFC 3246 *An Expedited Forwarding PHB (Per-Hop Behavior)*⁹⁵ treatment for Premium traffic on all of its interfaces. Since EF must be implemented by a priority queue, the network must be configured to police on all ingress interfaces, in order to avoid a catastrophic EF DoS attack. Thus the Qbone team determined that it would be impossible to deploy Premium incrementally only when and where there is congestion; instead it must be deployed at the granularity of the entire network. This requirement would extend to all concatenated Internetworks within the NCS. Thus, DSCP priority treatment for NS/EP traffic needs to be carefully analyzed.

The Premium IP team described that in addition to presenting an ideal target for DoS attacks, the DSCP as currently deployed on some router interfaces can only police, if at all, with a non-trivial degradation of performance. Performance degradation and security were identified as two reasons why public network operators (e.g., ISPs) will be inclined to zero the DSCP of all traffic ingressing on an interface.

D.2.1.2.2 Missing Diff-SERV Functionality

The Qbone design team found that although today's high-speed routers usually have some QoS functionality, it was insufficient for implementing Premium service. DSCP-based traffic classification, leaky-bucket policing, and priority queuing alone were determined to be insufficient. The additional Diff-SERV router functionality that is required to implement Premium is discussed below.

D.2.1.2.3 Route-Based Classification

Premium-enabled network service providers will need to classify and police ingressing EF traffic based on routing aggregates. Fire hose policing (a single EF leaky bucket per ingress interface) results in inefficient network use, since the provider must assume that the EF traffic from all interfaces could, in the worst case, converge on a single interior or egress interface. Micro-flow policing (one EF leaky bucket per micro-flow reservation traversing an ingress interface), unravels most of Diff-SERV's aggregation properties at interdomain boundaries and would not scale in the core. Thus the Qbone team concluded that Premium-enabled network service providers would want to sell "virtual trunks" between a pair of ingress and egress interfaces. The virtual trunks could be policed at ingress on the basis of an egress-dependent profile using a mechanism, such as DSCP based rate limits between autonomous systems (AS). The operation and maintenance of Premium is difficult to achieve without such mechanisms. The Qbone team noted that no high-speed router today provides such mechanisms, because the forwarding performed by line cards does not require full routing information. To reduce the price of line cards, forwarding tables provide a highly localized view of routing that usually only contain next-interface data. Caching the AS path in the forwarding tables could make routers

significantly more expensive, while going to the route-processor for the AS path would make routers significantly slower.

D.2.1.2.4 Shallow Token Buckets

Premium IP aggregates must be smoothed to be nearly jitter-free as they traverse interdomain boundaries. Policing such an aggregate effectively requires a classical token bucket policer that is only one or two packets deep. The Qbone team found that few routers today support token bucket policers this shallow at high line rates due to the fine-grained timing required.

D.2.1.2.5 Shaping Multiple Aggregates in a Priority Queue Class

Since the downstream interface across an interdomain boundary may be policing multiple EF aggregates, an egress interface must be able to accurately shape several aggregates within a priority queue (PQ) class. That is to say, on the egress line card, shape several aggregates and then give them EF treatment across the link. Too often shapers are matched one-to-one with forwarding classes (e.g., there is only one PQ class and it can be shaped or not).

D.2.1.2.6 DSCP Translation to Switched Ethernet QoS

The team found that implementation of IEEE 802.1p is needed on LAN edge devices that must translate between DSCP markings and 802.1p markings. Also, work is still underway to complete the IEEE 802.11e QoS specification.

D.2.1.2.7 The Cost of Complex Forwarding

The Qbone team found that some router vendors elected to include complex QoS functionality in microcode running on their interface cards, rather than in custom Application Specific Integrated Circuits (ASIC) that add to the power consumption and cost of a card. The Qbone Premium IP service determined that this approach can result in a drop of maximum packet-per-second forwarding rates by 50% or more. Such a CPU cycle shortage hurts all traffic, including Premium.

D.2.1.2.8 Operational and Economic Paradigm Shifts

If the deployment of Premium is an all-or-nothing proposition, it requires fairly sudden and significant changes to network operations and peering agreements. On the operations side, operators must configure a lot of router features they usually ignore, they must respond to admissions requests, and they must provision carefully to honor the service assurances of admitted requests. Transitions to new routers or circuits must be performed with the utmost care. Finally, very rapid Internet Gateway Protocol (IGP) convergence becomes essential and admissions decisions must be made with careful attention to routing or be made so conservatively as to allow routing to be ignored.

Peering arrangements between network providers also would experience a dramatic paradigm shift. Today, a typical ISP's technical interface to the outside world is unicast IPv4, Border Gateway Protocol (BGP), and possibly a simple service-level assurance (SLA), while its economic interface is some combination of per-line and per-bit charges.

Premium service would complicate this with a series of additional external interfaces, including shaping, policing, reservation signaling, and per-reservation billing and settlement. Not only does Premium change the interface between an ISP and its neighbors, but it also adds new complexities for customer support personnel, creates the need for accurate third-party service auditing, and in the commercial world increases the risk of litigation costs.

D.2.1.2.9 Premium and Best-Effort Co-existence

In a DSCP Premium IP service environment the relationship among peering networks is different. Today, all Internet traffic is engineered for “best effort” service. If QoS mechanisms are enabled in the routers to allow ISPs to classify traffic on the basis of AS path to enable a “trickle down” payment system, it is unclear what disincentive the provider has for rendering lower quality to all “best effort” transit traffic. Erosion of best-effort service could result in a completely different Internet where all serious work gets done over Premium service and users are generally expected to make virtual circuit reservations for most of what they do.

D.2.1.2.10 Service Level Agreement Standards

Although it is possible to specify Premium IP service with expected service parameters for loss and delay, there is very little agreement thus far about how statistics can be brought to bear on either the engineered service assurance or the provisioning techniques. In practice, the service that is advertised and sold to the customer (e.g., Premium service with zero loss and jitter) cannot be the actual service that is engineered by the provider.

To maximize profit, Premium must ultimately be explained to the customer in simple terms, but engineered carefully by the provider with a strong understanding of the statistical nature of traffic and of the network's performance. The statistical nature of traffic is always changing as new applications emerge and older ones fade away, so this effort would have to be ongoing. Today, there is insufficient theoretical understanding of how to do this kind of traffic modeling well for IP networks.

D.2.1.2.11 Service Verification

Premium service is not really about the network performance that is experienced by a reservation holder, but is rather about the performance that would be experienced by the reservation holder in the event of a network DoS attack or congestion on the scale of NS/EP events. Service is about assurance. Consequently, an observation of zero loss and jitter on a Premium reservation over an extended period of time does not confirm that the Premium assurance is functioning correctly.

This is not merely a theoretic concern. It is natural for customers to want to verify their service assurance and it is natural for providers to verify that they are providing the assurance they think they are. How does a provider confirm that the policers are functioning correctly after the configurations have been changed? Likewise, how does a customer confirm their service assurance? In either case, service verification is analogous to launching a distributed, interdomain DoS attack against the provider. Credible service verification would seem to require an industry of third-party service auditors with access

to peerings (including private peerings). It is especially difficult for the user to determine whether the network operator is indeed providing guarantees or merely has a well-provisioned, high-performance network that could at any time be brought down by a DoS attack.

D.2.1.2.12 Inadequate Standardization and Architectural Gaps

A factor contributing to the reluctance of ISPs to deploy Premium has been the debate in the IETF Differentiated Services Working Group over several key areas of standardization. Chief among these is the EF per-hop behavior itself. The original EF PHB draft RFC 2598⁹⁶ published in June 1999 could not be implemented. It required more than a year of debate within the working group to decide on a course of action that could fix it. The result was the formation of a design team to author a new EF specification RFC 3248.⁹⁷ However, this specification was ultimately rejected in favor of a competing alternative, RFC 3246, which was published as a standards track RFC in March 2002.

The Qbone design team alluded that a second factor was the decision that DSCP values would have local significance only. The QPS team regarded this as a colossal mistake, burdening all edge routers with the need to re-mark traffic and creating a frivolous (but nevertheless confusing) choice for engineers. Although the choice not to have DSCPs with global significance hurts Premium deployment, it hurts services with nice incremental deployment properties even more. Indeed, from a NS/EP perspective the optimum choice would have been to have global DSCP significance.

Some of the architectural gaps identified by the QPS team included the provisioning and matching of policers and shapers across interdomain boundaries to support micro-flow aggregation; the calculation of worst-case jitter bounds; and the need for scalable, automated signaling.

D.3 GÉANT

The GÉANT project is a collaboration between 26 National Research and Education Networks (NREN) representing 30 countries across Europe, the European Commission, and Delivery of Advanced Network Technology to Europe (DANTE). The GÉANT network is a multi-gigabit pan-European data communications network. GÉANT offers a Premium IP service that provides network priority based on the use of DSCP and other QoS⁹⁸ related mechanisms. Premium IP traffic takes priority over other services, such as Best Effort (BE) and Less Than Best Efforts (LBE). Premium IP traffic receives a better, and guaranteed, level of network performance during times of congestion. This can be particularly useful for real-time applications, such as Voice Over IP (VoIP) and video conferencing. Premium IP provides a service similar to that of a virtual leased line. Data packets that are sent using the Premium IP service will experience no congestion in the network regardless of the load of other traffic classes. As a result, delay and packet loss are kept to a minimum. The Premium IP service on GÉANT provides the following performance metrics:

- Upper-bounded one-way delay
- Upper-bounded Instantaneous Packet Delay Variation (IPDV)

- Zero congestion packet loss
- Guaranteed capacity.

Premium IP packets are tagged with DSCP 46 (101110). Any packets tagged as Premium IP (with DSCP 46) that are sent to GÉANT without prior reservation are considered unauthorized and are re-tagged as Best Effort (DSCP 0 or DSCP 6). They are then treated as LBE on the first GÉANT router and as BE on subsequent GÉANT routers. Packets that are tagged with DSCP 40 (101000) are always forwarded as BE traffic, but without the packets being re-marked. This means that packets can be tagged so that they receive Premium IP in the peer networks (i.e., NRENs) and BE in the GÉANT network. However, the network offers no SLAs because the monitoring infrastructure allowing SLA metric verification is still under study.

The Service Quality across Independently managed Networks (SEQUIN) Premium IP specification states that, for a Diff-SERV based implementation, the amount of Premium IP that can be supported on a circuit is 10% of the circuit capacity (or 20% in case the traffic of a failed circuit is re-routed to a circuit of equivalent capacity). Combined with GÉANT's Premium IP queuing mechanisms, this limitation has allowed the performance metrics to be guaranteed. **Figure D-1** depicts Premium and Best Effort traffic patterns.

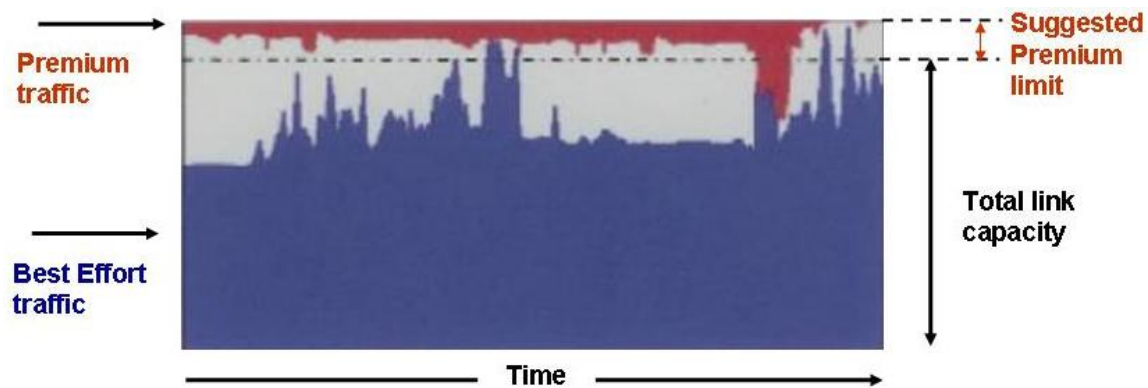


Figure D-1 Premium vs Best Effort Capacity

(Figure courtesy of SEQUIN⁹⁹)

GÉANT specified very specific operating characteristics in advance of deployment. For example, it was specified that the source node in the first domain should perform shaping of outgoing traffic and must be responsible for sharing fairness of the premium capacity. The source node was allowed to tag the premium packets with the correct Premium IP tag value for the domain it is in. The first domain was required to perform as near as possible to the source:

- Admission control based on IP source and destination prefixes
- Marking of valid premium packets with agreed DSCP or IP precedence values
- Remarking of invalid packets to best effort
- Policing according to a token bucket depth of 2 MTUs to the agreed sending rate

- Enable queuing using PQ or Weighted Round Robin (WRR) or similar queuing mechanism with premium packets being assigned the highest priority queue on all border and internal routes/switches
- Propagate packets inside the domain according to the EF PHB along all hops of its path
- Propagate packets on links to a different domain according to the EF PHB.

GÉANT specified similar operational details for elements within a single network core, between AS points, and for egress points. Thus, the result was a published set of operational guidelines that each network operator throughout Europe could implement.

D.4 VoIP QoS Research Conclusions

In the U.S. today, the price of high speed network capacity is low and falling but the apparent one-time and recurring costs of deploying and maintaining DSCP QoS and related mechanisms are high due to the skill levels required for network engineers with appropriate training and experience. Today, it is far cheaper to buy more capacity and to provide everyone with excellent service than it is to implement and support a QoS environment. The drawback, from an NCS perspective, is that without public (e.g., Internet) infrastructure supports for QoS the costs to support NS/EP VoIP prioritized traffic by means of private networks or by SLAs is likely to be high. The ability to purchase (e.g., SLAs) NCS prioritized traffic support that will function seamlessly over multiple commercial Autonomous Systems is today a unique requirement that will be priced accordingly.

In a world of guaranteed services, applications will either rely on the guarantees provided by the network or they will begin to incorporate the functionality necessary to employ adaptive techniques. If this solution is adopted, then adaptive applications will once again have the competitive advantage over QoS mechanisms. An Internet where both QoS and best-effort services co-exist appears to be, at least thus far, commercially unstable. The deployment, operational, and business complexities of changing the Internet architecture to support QoS could inhibit the scalability and growth of the Internet in the future.

References

-
- 1 “Assignment of National Security and Emergency Preparedness (NS/EP) Telecommunications Functions.” Executive Order of the President of the United States 12472.
 - 2 “Critical Infrastructure Protection (CIP).” Executive Order of the President of the United States 13010.
 - 3 “Critical Infrastructure Protection: Who’s In Charge?” Testimony of Kenneth C. Watson, President, Partnership for Critical Infrastructure Security to US Senate Committee on Government Affairs. October 4, 2001.
 - 4 “Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security.” Executive Order 13286. February 28, 2003.
 - 5 “Information Technology - Abstract Syntax Notation One (ASN.1) & ASN.1 encoding rules.” ITU-T X.680-X.693. July 2002.
 - 6 “Information Technology Progress Impact Task Force Report (ITPITFR) on Convergence.” The President’s National Security Telecommunications Advisory Committee (NSTAC) report dated May 2000.
 - 7 “The Convergence of Signaling System 7 and Voice-over-IP.” NCS TIB 00-8 dated September 2000.
 - 8 “Glossary of Telecommunications Terms.” Federal Standard (Fed-Std) 1037C, the Federal Telecommunications Standards Committee (FTSC). August 1996.
 - 9 International Telecommunications Union – Telecommunications (ITU-T) sector G.114 One-way transmission time.
 - 10 ITU-T H.323 Packet-based Multimedia Communications Systems Recommendation.
 - 11 RFC 3261 SIP: Session Initiation Protocol. Rosenberg et al. June 2002.
 - 12 Internet Standard 0064 RTP: A Transport Protocol for Real Time Applications. H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson . June 2003.
 - 13 RFC 2205 Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification. Standards Track. R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin. September 1997.
 - 14 RFC 3006 Integrated Services in the Presence of Compressible Flows. B. Davie, C. Iurralde, D. Oran, S. Casner, J. Wroclawski. November 2000.
 - 15 RFC 2475 An Architecture for Differentiated Services. S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss. December 1998.
 - 16 <http://www.deloitte.com>.

-
- 17 Federal Communications Commission (FCC) mandated phase II of wireless cellular deployment.
 - 18 American National Standards Institute (ANSI)-41. Cellular Radiotelecommunications Intersystem Operations.
 - 19 National Emergency Number Association (NENA). <http://www.nena.org>.
 - 20 National Emergency Number Association Solution Requirements Document Version 0.2. IP UNITES Working Group. IP User-Network Interface to Emergency Services.
 - 21 NENA-02-010: NENA Recommended Formats and Protocols for ALI Data Exchange, ALI Response & GIS Mapping. January 2002.
 - 22 RFC 1597 (obsoleted by RFC 1918 in 1996) Address Allocation for Private Internets.
 - 23 RFC 3022 Traditional IP Network Address Translator (Traditional NAT). P. Srisuresh, K. Egevang. January 2001.
 - 24 Internet Standard 0006 User Datagram Protocol (UDP). J. Postel. August 1980.
 - 25 Internet Standard 0007 Transmission Control Protocol (TCP). J. Postel. September 1981.
 - 26 RFC 3489 Simple Traversal of UDP Through NAT (STUN). J. Rosenberg, J. Weinberger, C. Huitema, R. Mahy. March 2003.
 - 27 RFC 3303 Middle Box Communications (MIDCOM) Architecture and Framework. P. Srisuresh, J. Kuthan, J. Rosenberg, A. Molitor, A. Rayhan. August 2002.
 - 28 Traversal Using Relay NAT (TURN). J. Rosenberg, draft-rosenberg-midcom-turn-05 (work in progress), July 2004.
 - 29 RFC 3075 (Standards Track) XML-Signature Syntax and Processing. D. Eastlake 3rd, J. Reagle, D. Solo. March 2001.
 - 30 IEEE 802af Carrier Sense Multiple Access/Collision Detection (CSMA/CD) Data Terminal Equipment (DTE) Power via Media Dependent Interface (MDI).
 - 31 RFC 3715 IAB Concerns Regarding Congestion Control for Voice Traffic in the Internet. March 2004, Informational.
 - 32 RFC 3448 TCP Friendly Rate Control (TFRC). M. Handley, S. Floyd, J. Padhye, J. Widmer. January 2003.
 - 33 Datagram Congestion Control Protocol (DCCP). Eddie Kohler, Mark Handley, Sally Floyd. Internet-Draft dated November 2004. Expires May 2005.
 - 34 ITU-T G.711, Pulse Code Modulation (PCM) of Voice Frequencies.
 - 35 RFC 3168 The Addition of Explicit Congestion Notification (ECN) to IP. K. Ramakrishnan, S. Floyd, D. Black. Standards Track. September 2001.

-
- 36 ITU-T H.323 Series H: Audiovisual and Multimedia Systems Infrastructure of Audiovisual Services Systems and Terminal Equipment for Audiovisual Services Packet-based Multimedia Communications Systems Recommendation.
- 37 ITU-T Recommendation H.225.0 Call Signalling protocols and media stream packetization for packet-based multimedia communications systems.
- 38 ITU-T Implementors Guide for Recommendations of the H.323 System Version 4: H.323, H.225.0, H.245, H.246, H.283, H.235, H.341, H.450 Series, H.460 Series, and H.500 Series. July 2003.
- 39 ITU-T Recommendation X.680 (2002), Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.
- 40 ASN.1 Packed Encoding Rules (PER) for H.323 is specified in ITU-T Recommendation X-691 (2002)/ ISO/IEC 8825-2:2002, Information Technology - ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER).
- 41 ASN.1 Code Generated by ASNP, France Telecom R&D.
- 42 RFC 3487 Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP). H. Schulzrinne. February 2003.
- 43 RFC 3689 General Requirements for Emergency Telecommunication Service (ETS). K. Carlberg, R. Atkinson. February 2004.
- 44 RFC 2916 E.164 Number and DNS. P. Faltstrom. September 2000.
- 45 RFC 2782 A DNS RR for specifying the location of services (DNS SRV). A. Gulbrandsen, P. Vixie, L. Esibov. Standards Track. February 2003.
- 46 RFC 768 User Datagram Protocol. J. Postel. August 1980.
- 47 RFC 2960 Stream Control Transmission Protocol. R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang, V. Paxson. Standards Track. October 2000.
- 48 RFC 3762 Telephone Number Mapping (ENUM) Service Registration for H.323. Standards Track. O. Levin. April 2004.
- 49 ITU-T H.245 Control Protocol for Multimedia Communication.
- 50 Internet-Draft (I-D) titled Simple RTP Multiplexing Transfer Methods for VoIP. Tohru Hoshi, Koji Tsukada, Keiko Tanigawa. Internet Draft, November 1998.
- 51 RFC 3261 SIP: Session Initiation Protocol (SIP). J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. June 2002.
- 52 RFC 2279 UTF-8, a transformation format of the International Organization for Standardization (ISO) 10646. Standards Track. F. Yergeau. January 1998.
- 53 RFC 2616 Hypertext Transfer Protocol (HTTP). – HTTP 1.1. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter. P. Leach, T. Berners-Lee. June 1999.
- 54 RFC 2821 Simple Mail Transfer Protocol (SMTP). J. Klensin, Editor. April 2001.

-
- 55 RFC 2327 SDP: Session Description Protocol. M. Handley, V. Jacobson. Standards Track. April 1998.
- 56 RFC 2326 Real Time Streaming Protocol (RTSP). H. Schulzrinne, A. Rao, R. Lanphier. Standards Track. April 1998.
- 57 February 2004, an I-D titled Emergency Services URI for the Session Initiation Protocol. Henning Schulzrinne. Internet-Draft. August 2004.
- 58 Internet Draft, a work in progress, The Internet Assigned Number Authority (IANA) Header Field Parameter Registry for the Session Initiation Protocol (SIP). G. Camarillo. June 2004.
- 59 RFC 3487 Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP). H. Schulzrinne. February 2003.
- 60 RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. K. Nichols, S. Blake, F. Baker, D. Black. December 1998.
- 61 In March 2004, an I-D Communications Resource Priority for the Session Initiation Protocol (SIP). H. Schulzrinne, J. Polk. Internet-Draft expires April 2005. October 2004.
- 62 ITU-T Q735.3 Stage 3 description for community of interest supplementary services using Signalling System No. 7: Multi-level precedence and preemption. March 1993.
- 63 IETF RFC 3761 Standards Track The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM). P. Faltstrom, M. Mealling. Standards Track. April 2004.
- 64 RFC 1123 Requirements for Internet Hosts -- Application and Support. R. Braden, Editor. October 1989.
- 65 RFC 3764 ENUM Service Registration for Session Initiation Protocol (SIP) Address-of-Record. Standards Track. J. Peterson April of 2004.
- 66 February of 2004, an I-D titled Emergency Services for Internet Telephony Systems. H. Schulzrinne. Internet-Draft. October 2004.
- 67 RFC 2246 Transport Layer Security (TLS). Standards Track. T. Dierks, C. Allen. Standards Track. January 1999.
- 68 RFC 1918 Address Allocation for private Internets. Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear. Best Current Practice. February 1996.
- 69 IEEE 802.11b Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band.
- 70 IEEE 802.11a Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 1: High-speed Physical Layer in the 5 GHz band.

71 IEEE 802.11g Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band.

72 IEEE 802.11i Standard for Information technology--Telecommunications and information exchange between system--Local and metropolitan area networks - Specific requirements--Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications--Amendment 6: Medium Access Control (MAC) Security Enhancements. 2004.

73 802.11h IEEE 802.11h Standard for Information technology—Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Spectrum and Transmit Power Management Extensions in the 5GHz band in Europe.

74 802.11e Wireless medium access control (MAC) and physical layer (PHY) specifications:Medium access control (MAC) enhancements for quality of service (QoS), Draft 5.0. July 2003.

75 RFC 2998 A Framework for Integrated Services Operation over Diffserv Networks. Y. Bernet, P. Ford, R. Yavatkar, F. Baker, L. Zhang, M. Speer, R. Braden, B. Davie, J. Wroclawski, E. Felstaine. November 2000.

76 RFC 2475, An Architecture for Differentiated Services.S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss. December 1998.

77 I-Am-Alive Alliance (IAA). <http://www.iaa-alliance.net>.

78 RFC 3690 IP Telephony Requirements for Emergency Telecommunication Service (ETS). K. Carlberg, R. Atkinson. February 2004.

79 H.R. 5419 ENHANCE 911 Act of 2004.

80 ANSI T1.631 Telecommunications – Signaling System No. 7 (SS7) High Probability of Completion (HPC) Network Capability. 1993.

81 Internet2 Hybrid Optical and Packet Infrastructure project (HOPI). <http://networks.internet2.edu/hopi>.

82 Internet-Draft “Emergency Telecommunications Service in Evolving Networks work in progress.” Hal Folts. February 2002.

83 ANSI T1.111-1996 Signaling System No. 7 (SS7) - Message Transfer Part (MTP), March 14, 1996.

84 RFC 3270 Multi-Protocol Label Switching (MPLS) Support of Differentiated Services. Standards Track. F. Le Faucheur, L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, J. Heinanen. May 2002.

85 RFC 1633 Integrated Services in the Internet Architecture – an Overview. R. Braden, D. Clark, S. Shenker. June 1994.

86 RFC 2212, Specification of Guaranteed Quality of Service. S. Shenker, C. Partridge, R. Guerin. September 1997.

87 RFC 2211, Specification of the Controlled-Load Network Element Service. Standards Track. J. Wroclawski. September 1997.

88 RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IP version 4 (IPv4) and IPv6 Headers. Standards Track. K. Nichols, S. Blake, F. Baker, D. Black. December 1998.

89 RFC 3248 A Delay Bound alternative revision of RFC 2598. G. Armitage, B. Carpenter, A. Casati, J. Crowcroft, J. Halpern, B. Kumar, J. Schnizlein. March 2002.

90 RFC 2597 Assured Forwarding (AF) PHB group. Standards Track. J. Heinanen, F. Baker, W. Weiss, J. Wroclawski. June 1999.

91 IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering was revised to IEEE 802.1D MAC Bridges. November 2003.

92 IEEE 802.1Q Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks. 2003.

93 “Implementation of QoS-Provisioning System for Voice over IP” by Shengquan Wang, Zhibin Mai, Walt Magnussen, Dong Xuan, and Wei Zhao.

94 “Why Premium IP Service Has Not Deployed (and Probably Never Will).” Informational Paper by Benjamin Teitelbaum and Stanislav Shalunov, Internet2 QPS design team, 2003.

95 RFC 3246 An Expedited Forwarding PHB (Per-Hop Behavior). Standards Track. B. Davie, A. Charny, J.C.R. Bennett, K. Benson, J.Y. Le Boudec, W. Courtney, S. Davari, V. Firoiu, D. Stiliadis, March 2002.

96 RFC 2598 An Expedited Forwarding PHB. Standards Track. V. Jacobson, K. Nichols, K. Poduri. June 1999.

97 RFC 3248 A Delay Bound alternative revision of RFC 2598. G. Armitage, B. Carpenter, A. Casati, J. Crowcroft, J. Halpern, B. Kumar, J. Schnizlein, March 2002.

98 “Quality of Service Definition.” Sequin Deliverable D2.1 – Addendum 1, Mauro Campanella. 2001.

99 “Implementation Architecture Specification for the Premium IP Service.” Deliverable D2.1 – Addendum 1, SEQUIN. 1999.