NIST *Office of Law Enforcement Standards (OLES)*

SAFECOM

Roundtable on Public Safety Interoperability and Voice over Internet Protocol (VoIP)

August 22, 2006

Washington, DC

Table of Contents

Executive Summary

On August 22, 2006, the National Institute of Standards and Technology (NIST)/Office of Law Enforcement Standards (OLES), in conjunction with SAFECOM, brought together members of the public safety and industry communities to discuss the role of Voice over Internet Protocol (VoIP) in public safety communications. The discussions centered on VoIP's current and potential use in that arena.

It was evident throughout the meeting that both public safety and industry lack a common definition of VoIP. A shared understanding is also missing between the two communities on how public safety is currently using VoIP in its communication systems.

However, by holding a roundtable forum with this group of key stakeholders, NIST/OLES and SAFECOM have begun a series of important discussions that will lead to greater clarification and enhanced understanding of the use of VoIP in public safety communications.

Throughout the meeting, participants were able to:

- Better define the strengths and limitations of VoIP usage in public safety communications.
- Gain a shared understanding of the public safety requirements for VoIP.
- Begin discussions for a suite of standards on the use of VoIP in public safety communications.

One of the major outcomes of this meeting was that NIST/OLES and SAFECOM were able to leave the room with a list of agreed upon statements by public safety and industry regarding VoIP. These joint statements will be used as a starting point for future conversations with both parties, so that industry and public safety can educate their respective communities about VoIP's role in their interoperability solutions.

Background

Voice over Internet Protocol (VoIP) as a beneficial technology for public safety communications is a concept that has been gaining popularity in recent years. What is lacking, however, is a common definition of exactly what VoIP is, and how it best fits into public safety communications. Misunderstandings thus far have led to misinformed blanket statements from both public safety officials and industry on VoIP's current and potential role in public safety.

Therefore, the National Institute of Standards and Technology (NIST)/Office of Law Enforcement Standards (OLES), along with their Department of Homeland Security (DHS) partner SAFECOM, brought together key stakeholders from both industry and the public safety community to discuss and clarify the varying perceptions of VoIP's role in public safety communications.

The following sections represent the discussions that were held during the August 22, 2006 meeting.

Purpose and Outcomes

Purpose

- To develop a common understanding between public safety and industry about VoIP's role in public safety communications

Outcomes

- A common understanding of public safety's voice requirements for interoperable systems
- A common understanding of how industry's VoIP solutions currently fit into those requirements
- Possible next steps regarding use of VoIP for public safety

What Is VoIP?

One of the barriers to understanding VoIP usage in public safety communications is the lack of a common definition. The phrase "VoIP" is currently being used in several different ways, such as Internet Protocol (IP) Telephony, Radio VoIP, and Private Wireless VoIP. Pre-meeting interviews confirmed that individuals had very different understandings of VoIP based on their own experience and involvement with the technology. Thus it was necessary to scope the definition of VoIP for the purpose of the day-long discussion.

The following diagram (*Figure 1)* shows the technological scope of the meeting, which consisted of communication systems that the public safety community typically owns and operates itself. VoIP issues relating to citizen to public safety communication are not addressed in this meeting; for example, Enhanced 911 emergency calls.

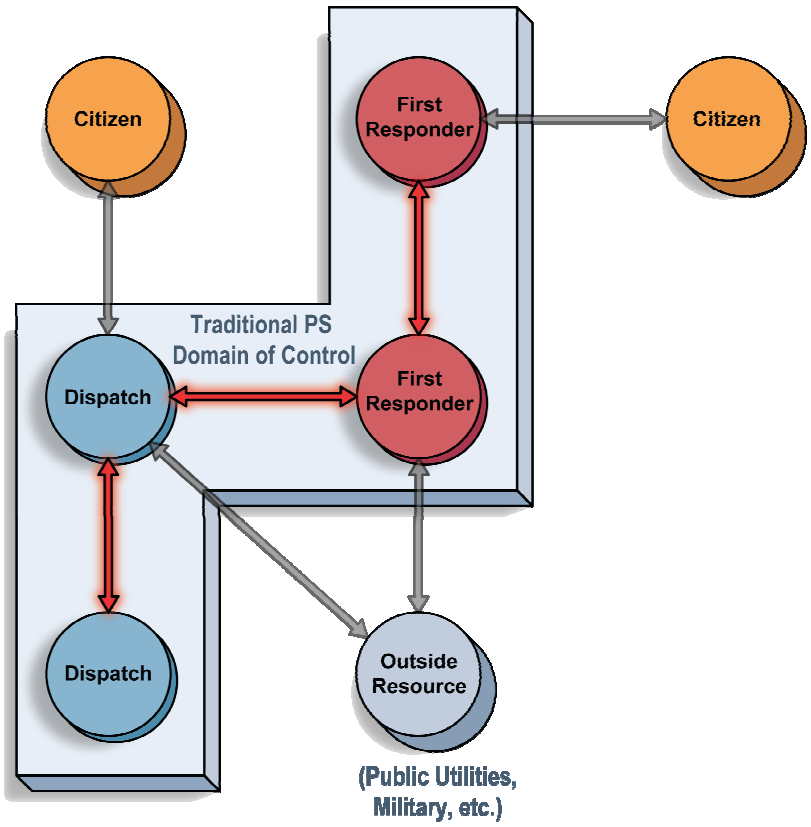


Figure 1 – This diagram shows the communication links that were under discussion for the meeting.
These links are shown by the red arrows.

How Is VoIP Currently Being Used in Public Safety Communications?

Pre-meeting interviews also made clear a gap in understanding between public safety and industry on where VoIP was currently used in public safety communications. Both industry's and public safety initial perspectives of VoIP use in public safety communications are outlined below.

Industry's Perspective

- For radio control (primary and secondary), interoperability, and to monitor radio channels
- Mobile command units sending VoIP over satellite
- Wide area systems-- anything beyond a typical microwave system where you have to distribute repeaters/radios
- To leverage IP networks to bridge new systems
- For microwave installations on radio systems
- To digitize voice for transport between locations
- Using IP as an access (wired and wireless) technology to first responders
- Using IP as a bridging technology between systems
- Mission-critical voice on an incident area network (WiFi/mesh networks)
- Through WiFi/mesh, using IP as practiced to make communications more reliable

Public Safety's Perspective

- To back up mission-critical land mobile systems (has not been widely deployed in mission-critical situations)
- For dispatch to dispatch communications
- To connect remote towers back to the main system

The meeting participants discussed the discrepancies between the two perspectives, and the issues that follow were raised.

Networks

Public safety stated that its limited use of VoIP was partially due to the risk of placing VoIP onto an existing network whose ability to support VoIP is unknown. The network must be properly engineered to ensure that the quality, reliability, and security requirements of public safety are met. Industry stated that although the use of IP may be limited, there are still many cases where it has been successfully deployed. Public safety maintained that while at the *network* level almost all of the traffic is IP, at the *device* level it is not.

Support Staff

There is a gap in understanding and experience between land mobile radio (LMR) support staff and information technology (IT) support staff. LMR support staffs typically have a better understanding of public safety communications requirements.

Product Support

The participants discussed the fact that because IT solutions typically are designed for a shorter lifespan than public safety systems, manufacturer support for IT products tends to end sooner.

Bandwidth

Industry pointed out that although bandwidth on the "last mile"[1] is an issue for VoIP, different methods are being used on wireless and wired networks to deal with it. Further, moving forward, mesh networking and other technologies will have the necessary bandwidth, including the use of unlicensed spectrum, for VoIP. Public safety explained that from its perspective, it is dangerous to rely on unlicensed spectrum, e.g. there are no guaranteed interference protection mechanisms. LMR, on the other hand, is licensed and under public safety control.

Use of Commercial Services

Public safety shared its concerns with commercial services. They feel that commercial services were not designed to support the reliability metrics that public safety needs. Private LMR is a more reliable place for mission-critical communications.

[1] The **last mile** is the final leg of delivering connectivity from a communications provider to a customer. Usually referred to by the telecommunications and cable television industries, it is typically seen as an expensive challenge because "fanning out" wires and cables, an essential part of the executing the last mile, is a considerable physical undertaking.

Standards

Finally, the argument was made that if public safety is to depend on VoIP, basic interface standards are needed.

What Are the Strengths and Limitations of VoIP for Public Safety?

One of the main goals of bringing together industry and public safety was to develop a shared understanding of the strengths and limitations of VoIP usage in public safety communications. It is evident that industry and public safety have differing opinions on VoIP's appropriateness, benefits, and where work still needs to be done before it can be deployed for mission-critical situations.

Public Safety's Perspective

Strengths:

- Enables the blending of technologies and the use of commercial off-the-shelf (COTS) products to minimize public safety costs

Limitations:

- Lack of standards profiles
  - Issues addressed for Inter-RF Subsystem Interface (ISSI) P25 vendors have to be dealt with for VoIP--(e.g. vocoder, control plane, administration)
    - Vendor reliability--multi-vendor solution
- Security
  - Privacy and integrity of messages
  - Authentication and authorization of users
- Reliability
  - Lack of trust in the technology to be deployed in mission-critical situations
  - Distinguishing between VoIP packet from public safety and VoIP from Vonage
    - Priority must be maintained if the packets are on an intranet or an extranet (public network)
  - Spectrum requirements for VoIP in public safety are not well understood
  - Defined as 100% assurance that messages will go through to recipient
  - Impact of data on VoIP--Correctly designing networks to handle VoIP

Industry's Perspective

Strengths:

- Provides communications continuity
- Provides flexible connectivity
- Saves money

Limitations:

- Training and support of the technology:
  - Staffing, maintenance, management of technology
  - Entails a new level of engineering which requires training

The main discussion focused on industry's desire for public safety to be fully aware of the capabilities that VoIP has to offer. Public safety reiterated that, regardless of the current capabilities, reliability is still a concern regarding VoIP use in mission-critical situations.

Consensus View of Public Safety VoIP

The discussion about the strengths and limitations of VoIP prompted a more in-depth discussion about what a standards profile for VoIP usage in public safety should look like. Participants discussed the appropriate environments where standards are necessary. The information below represents environments where it was agreed that standards development is needed.

Last Mile Radio

(Radio to infrastructure, radio to radio, proxy is a mechanism for supporting air interfaces that are non-IP-based--for example: P25 CAI)

- Industry can design an end-user device that is IP-addressable (client) and public safety can operate over a true IP transport, or via a proxy through a non-IP-based gateway.

Radio System Back Haul

- P25 Fixed Station Interface (FSI)
  - FSI Real-Time Transfer Protocol (RTP) profile

Radio System to System Interconnect

- P25 Inter-RF Subsystem Interface (ISSI):
  - ISSI Session Initiation Protocol (SIP) profile--(e.g., group call setup and teardown)
  - ISSI RTP profile--(e.g., bearer, push-to-talk (PTT) management)
  - Home serving base--Provides for mobility of users and talk groups

Dispatch to Dispatch

- P25 Console Subsystem Interface (CSSI):
  - Console to Radio Frequency SubSystem (RFSS)
  - CSSI SIP profile--(e.g., group call setup and teardown)
  - CSSI RTP profile--(e.g., bearer, PTT management)

- Hotline, intercom using other COTS

The additional environments below were identified as having a critical need for standards profiles. However, they were not addressed during this meeting. The understanding was that a follow-on meeting would be held to address them:

- Device-to-device(s) (e.g., computer to talk group)
- Radio to computer
- Bridge devices
- 911 call taking/Public Switched Telephone Network (PSTN) (out of scope for the meeting and this report)

What Are Public Safety's Requirements for VoIP?

SAFECOM, as a user-driven program, emphasizes along with NIST/OLES the importance of a bottom-up approach. Before technology is developed, its developers have to first ensure that it meets the needs of the user. Public safety requires VoIP to be a standardized set of signaling protocols, codecs, security, and services for the conveyance of mission-critical voice communications over an engineered IP network. Public safety agrees that before it will fully begin to deploy VoIP in mission-critical situations, the requirements below must be met.

Interoperability, Compatibility, Interchangeability

Public safety needs to be able to buy equipment from multiple vendors and be assured of interoperability and compatibility between products.

A Minimum Set of Standards and Features

Public safety needs industry to agree on a limited core suite of standards that ensure public safety communication requirements are met.

Common Security Framework

Public safety needs a common denominator of security across all disciplines to allow for security operability/interoperability as needed. To date, public safety has not had a forum to develop this security framework; however, it is recognized as a large problem in the community.

Reliability

Public safety requires reliability: ensuring that the service is available 24/7. One public safety practitioner summed up "reliability" by stating, *"I know nothing is 100% reliable, but in mission-critical situations, it needs to work every time I need it to work*."

Affordability

Public safety needs VoIP products to be priced at amounts that begin to approach the consumer marketplace for VoIP. This issue spurred discussion about total cost of ownership when purchasing a new technology. The cost of equipment is not public safety's sole cost. Transition from existing technology and operations as well as training personnel to use the new technology are just two of many costs that practitioners assume when purchasing a new technology.

Manageability

Public safety needs the ability to compare alternative VoIP offerings against the above characteristics to meet public safety's functional requirements.

Education

A forum is needed for ongoing discussions related to VoIP use in public safety communications. In many cases, vendors expect public safety to know the appropriate questions to ask vendors. Through programs like SAFECOM and NIST/OLES, these ongoing discussions will continue.

Assessments and Conclusions

At the end of the day-long session, members of the public safety community and industry representatives were given the opportunity to validate or change statements that were pulled from the day's discussions. The below statements represent agreed-upon conclusions about the use of VoIP in public safety communications.

Network, Performance, and Support Requirements

- "You can't just dump VoIP into an existing network and expect it to work."
    - The network must be properly and continuously engineered to make it reliable and to achieve the quality of service that public safety requires.

- Most public safety agencies do not often have the staff or funding to continuously upgrade and manage their systems to meet the requirements.

- Procurement is changing. There are more IT factors relating to which pieces of equipment get procured and how. Further, IT is more about data and less about voice.

- Radio vendors that provide IP-based equipment perceive their role as ending at the router or the four wire interface. Users must ensure that there is system-wide support.

Applications

- Many ways exist of sending voice within the IP world.

- Voice is the application, and IP is the technology.

- There are distinctions among full duplex VoIP, PTT (half duplex) VoIP, and streaming (simplex) VoIP.

Need for Standards

- Interoperability to the lowest common denominator must be maintained.

- Standards profiles for public safety VoIP must be defined in the context of an environment.

- There have to be standards for public safety regarding reliability and VOIP and beyond the four wire level.

- P25 ISSI is a VoIP implementation specific to public safety.

Current Understanding and Need for Education

- IP doesn't automatically mean interoperability.

- Government officials need further education on the relationship between the strengths and limits of VoIP:
  - Just because this area involves Internet Protocol does not mean it is using the Internet.
  - VoIP is part of some LMR solutions.

Wireless "Last Mile" Constraints

- The last-mile physics are very much an issue in access technologies for public safety:
  - Cause: Bandwidth is too limited to support VoIP transmissions.

- Public Safety wireless use of VoIP is limited by spectrum.

Current Use

- Use of VoIP technology in public safety is currently very limited:
  - There are early adopters currently; however, the majority of the public safety community does not use it.

- The Roundtable discussion focuses on public safety-to-public safety communications and public safety-to-other emergency services communications.

Public Safety Requirements

- Radio to radio in the absence of infrastructure is critical to public safety:
  - Everything is secondary to voice.

Product Lifecycles, Leveraging COTS, and Economies of Scale

- IT and IP product and applications life cycles tend to be much shorter than public safety funding cycles for communication systems.

Next Steps

This meeting marks the first time that industry and public safety representatives have come together to discuss the use of VoIP in public safety communications. Both NIST/OLES and SAFECOM recognize the need to continue these discussions with both groups, as well as educate others about VoIP use in public safety communications. NIST/OLES and SAFECOM plan to meet again to further discuss the topics that were initially addressed during this roundtable.

Appendices

A. Participant List

B. Meeting Slides

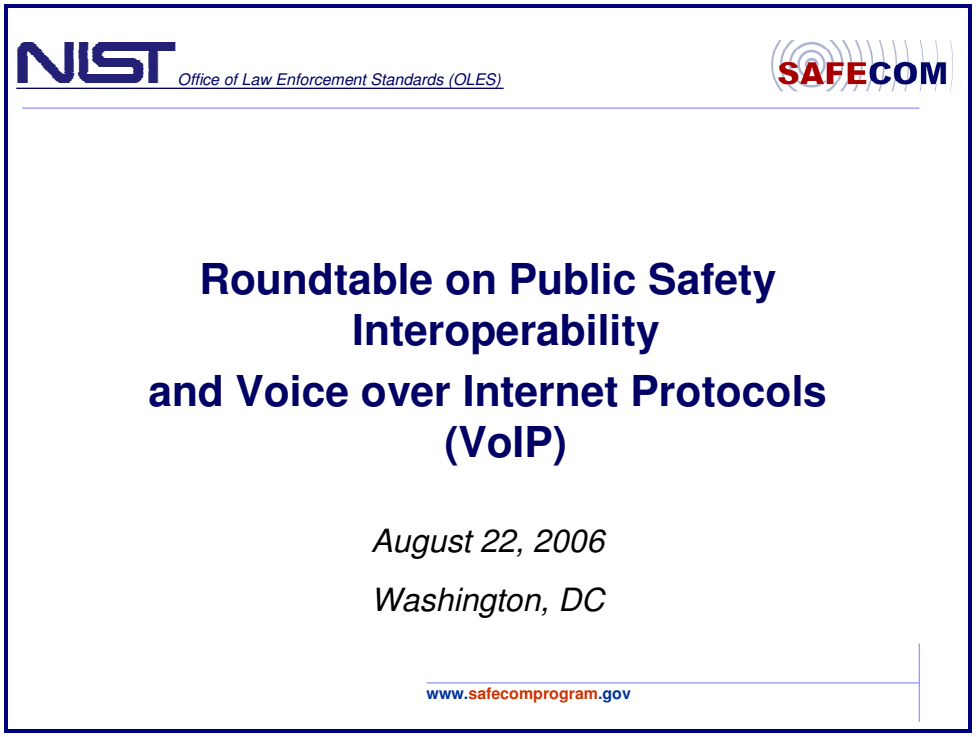
C. List of Acronyms

A. Participant List

Name	Title	Organization
Ake, George	Project Coordinator	National Institute of Justice (NIJ)
Atkinson, DJ	Lead Electronics Engineer	National Telecommunications and Information Administration (NTIA)/Institute for Telecommunications Sciences (ITS)
Botha, Shaun	CTO	Twisted Pair Solutions
Boyd, David	Director	DHS-OIC
Bratcher, Jeff	Lead Engineer	NTIA-ITS
Cannon, Glen	Director, Response Division	DHS/FEMA
Carcillo, Tara	Senior Consultant	SRA-Touchstone Consulting Group
Chapman, Doug	V.P. Product Marketing	Tait Electronics
Chirhart, Thomas	Spectrum Program Manager	DHS-OIC
Chu, Thomas	Distinguished Member of Technical Staff, Bell Laboratories	Lucent
Clinch, Guy	Global Solutions Director, Government and Education	Avaya
DeRango, Mario	Director, Advanced Technology	Motorola
Downes, James	FAC Chair	DHS/Wireless Management Office (WMO)
Fletcher, Mark	CTO Office	Nortel
Grier, Robin	President	Catalyst Communications
Hall, Douglas	Technical Lead	Cisco
Harris, Phil	Communications Engineer	L3COM GSI/NIJ CommTech LS GSI/NLECTC-NE

Name	Title	Agency
Kaluta, Roman	Director, Interoperability Solutions	Raytheon
Klein-Berndt, Luke	Computer Scientist	NIST/OLES
Martinez, Dennis	V.P. Technology	M/A-COM
McClellan, Roy	Standards, P-25	European Aeronautic Defence and Space Company (EADS)
McEwen, Harlin	Chairman, Communications and Technology Committee	International Association of Chiefs of Police (IACP)
McGinnis, Kevin	Program Advisor	National Association of State EMS Officials (NASEMSO)
Nash, Glen	Senior Telecommunications Engineer	State of California
Nelson, Eric	Electronics Engineer	NTIA
Orr, Dereck	Program Manager	NIST/OLES
Prater, Ron	Director, Public Safety Business Unit	SRA-Touchstone Consulting Group
Rivera, Stephanie	Senior Consultant	SRA-Touchstone Consulting Group
Stofer, Kristi	Associate Consultant	SRA-Touchstone Consulting Group
Thiessen, Andy	Lead Engineer	NTIA-ITS
Williams, Ernest	Lead Systems Specialist	DHS/Immigration and Customs Enforcement (ICE)/ Federal Protective Service (FPS)
Wylie, Kristen	Associate Consultant	SRA-Touchstone Consulting Group
Young, Steve	Senior Consultant	SRA-Touchstone Consulting Group

B. Meeting Slides



NIST Office of Law Enforcement Standards (OLES)

SAFECOM

- Interview Data:
  - What do you hope to get of this meeting?
    - A clearer idea of VoIP's potential use in Public Safety
    - Benefits and limitations of VoIP for Public Safety
    - An understanding of the outstanding security and reliability issues surrounding VoIP for Public Safety
    - Feedback from the user community on how Industry can meet their needs
    - A chance to have open, unscripted dialogue between Public Safety and Industry
    - Where do we go from here?

NIST Office of Law Enforcement Standards (OLES)

SAFECOM

Purpose and Outcomes

- Purpose
  - To develop a common understanding between Public Safety and Industry about VoIP's role in public safety communications
- Outcomes
  - A common understanding of Public Safety's voice requirements for interoperable systems
  - A common understanding of how Industry VoIP solutions currently fit into these requirements
  - Possible next steps regarding VoIP use for Public Safety

NIST Office of Law Enforcement Standards (OLES)

SAFECOM

- Agenda
  - Welcome and Introductions
  - Background
  - General Intro
  - Definition and history
  - How is VoIP currently being used in Public Safety communications?
  - How could VoIP be used in Public Safety communications?
  - Assessment and conclusions
  - Next Steps/closing

www.safecomprogram.gov

NIST Office of Law Enforcement Standards (OLES)

SAFECOM

- Introductions:
  - Name
  - Organization
  - Exposure to VoIP to date

www.safecomprogram.gov

What is VoIP?

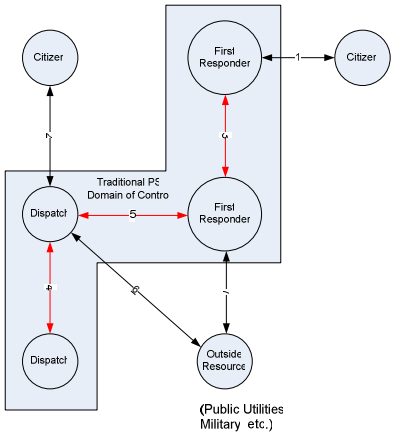
NIST Office of Law Enforcement Standards (OLES)
SAFECOM

- Brief History of VoIP
  - Originated in roughly **1995**
    - Hobbyists with PC-to-PC communications
    - VocalTec released first internet phone software
      - Used H.323
    - Marked by poor sound quality and connectivity
  - **1996**
    - SIP Internet Draft emerges on Dec 2nd 1996
  - **1998**
    - Small companies offering PC-to-PC at first with phone-to-phone to soon follow
    - 3 IP switch manufacturers introduced equipment capable of switching
    - ½ million minutes of VoIP to date
  - **1999**
    - SIP ID published on March 17th as RFC 2543
  - **2003**
    - Skype launches peer-to-peer VoIP services
  - **2004**
    - 100 billion minutes of VoIP to date

www.safecomprogram.gov

NIST Office of Law Enforcement Standards (OLES)

SAFECOM

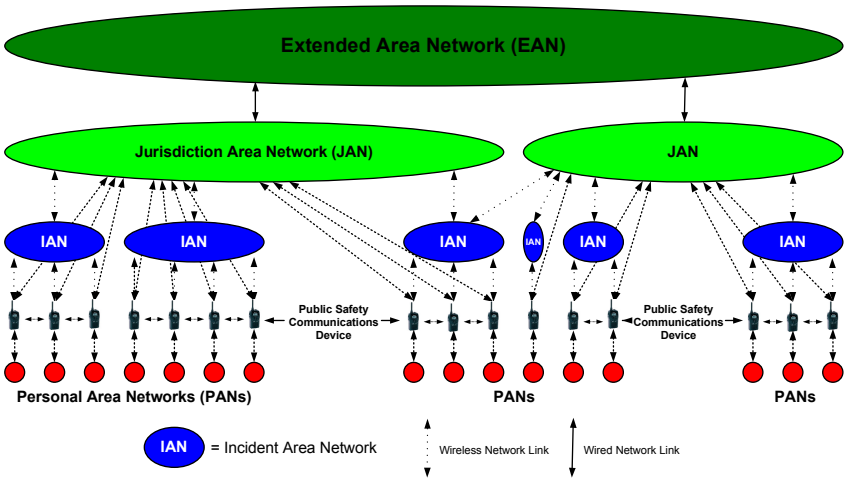


Definition and Scope

- What is VoIP ?
  - No single definition
- Types of VoIP
  - Internet Protocol (IP) Telephony
    - IP network used for telephone communications
    - Commercial world
    - Dispatch to dispatch
  - Radio VoIP
    - Using VoIP as a bridge between radio systems
  - Private Wireless IP
    - Using wireless VoIP as the access technology for first responders in the field

www.safecomprogram.gov

Public Safety Communications Hierarchy



Current VoIP Usage for Public Safety

NIST Office of Law Enforcement Standards (OLES)
SAFECOM

- How is VoIP currently being used for Public Safety?
  - From the Industry perspective:
    - For using radio control VoIP (primary and secondary) interoperability, to monitor radio channels
    - Mobile command units sending VoIP over satellite
    - Wide area systems – anywhere you have to distribute repeaters/radios beyond a typical microwave system
    - To leverage IP networks to bridge new systems
    - For microwave installations on radio systems
    - To digitize voice for transport between locations
    - Using IP as an access (wired and wireless) technology to first responders
    - Using IP as a bridging technology between systems
    - Mission critical voice on an incident area network (wifi/mesh networks)
    - Through Wifi/Mesh IP is being used to make communications more reliable

www.safecomprogram.gov

- How is VoIP currently being used for Public Safety?
  - From the Public Safety perspective:
    - To backup mission critical land mobile systems
      - Has not been widely deployed in mission critical situations
    - For dispatch to dispatch communications
    - To connect remote towers back to the main system

NIST Office of Law Enforcement Standards (OLES)
SAFECOM

What are the strengths and limitations of VoIP for use in Public Safety Communications?

NIST Office of Law Enforcement Standards (OLES)

SAFECOM

- Strengths:
  - Enables the blending of technologies and the use of commercial off the shelf (COTS) products to minimize public safety costs
  - Provides communications continuity
  - Provides flexible connectivity
  - Saves money

- Limitations:
  - Standards
    - Issues addressed for ISSI P25 vendors have to be dealt with for VoIP – (e.g. vocoder, control plane, administration, etc.)
      - vendor reliability – multi-vendor solution
  - Security
    - Privacy and integrity of messages
    - Authentication and authorization of users
  - Reliability
    - Lack of trust in the technology to be deployed in mission critical situations
    - Distinguishing between a VoIP packet from PS vs. VoIP from Vonage
      - Priority must be maintained if the packets are on an intranet or an extranet (public network)
    - Spectrum requirements for VoIP in public safety are not well understood
    - Defined as 100% assurance that messages will go through to recipient
    - Impact of data on VoIP - Correctly designing networks to handle VoIP
  - Training and support of the technology
    - Staffing, maintenance, management of technology
    - VoIP entails a new level of engineering which requires training

Blue = Public Safety

Black = Industry

NIST Office of Law Enforcement Standards (OLES)

SAFECOM

- Where does the P25 ISSI fit in?

www.safecomprogram.gov

How could VoIP be used in Public Safety communications?

NIST Office of Law Enforcement Standards (OLES)
SAFECOM

- What are Public Safety's requirements for VoIP?
  - Interoperability, Compatibility, Interchangeability
  - The minimum set of standards and features
  - Common security framework
  - Reliability
  - Affordable
  - Manageable
  - Ability to compare VoIP offering to other alternatives to meet PS functional requirements (against the above characteristics)
  - Education

www.safecomprogram.gov

- Discussion on Public Safety's Requirements

NIST Office of Law Enforcement Standards (OLES)
SAFECOM

- What does a Public Safety VoIP suite of standards look like?

- What does Public Safety want Public Safety VoIP to be?
  - Standardized set of signaling protocols, codecs, security framework, and services used for the conveyance of mission critical voice communications over an engineered IP network
  - Environments
    - Last mile radio (radio to infrastructure, radio to radio)
    - Radio system back haul
    - Radio system to system interconnect
    - Dispatch to dispatch or like user use (computer to computer)
    - Device to device(s) (e.g. computer to talk group)
    - Radio to computer
    - Bridge devices
    - 911 call taking/PSTN (out of scope for this report)

NIST Office of Law Enforcement Standards (OLES)
SAFECOM

Assessment and conclusions

www.safecomprogram.gov


NIST
Office of Law Enforcement Standards (OLES)
SAFECOM
Next steps/closing
www.safecomprogram.gov

C. List of Acronyms

COTS
Commercial Off The Shelf

CSSI
Console Subsystem Interface *(within P25)*

FSI
Fixed Station Interface (*within P25)*

IP
Internet Protocol

ISSI
Inter-RF Subsystem Interface

IT
Information technology

LMR
Land Mobile Radio

NIST/OLES
National Institute of Standards and Technology/Office of Law Enforcement Standards

P25
Project 25

PS
Public safety

PSTN
Public Switched Telephone Network

PTT
Push-to-Talk

RFSS
Radio Frequency Subsystem

RTP
Real-time Transport Protocol

SIP
Session Initiation Protocol

VoIP
Voice over Internet Protocol