



**Homeland
Security**

**Office of Grants and Training
Directorate of Preparedness**



Technical Information Working Group Technical Note 2006-5

Voice over IP in LMR Environments

This document is a redacted version of an ICTAP technical note on the technology and use of “Voice over IP” (VoIP) in Public Safety Land Mobile Radio (LMR). It is important that public safety agencies throughout the United States be made aware of VoIP capabilities, technologies, and issues, as they are rapidly being adopted in LMR environments. This version may be disseminated outside ICTAP channels. No comment or remark in this paper should be construed as an endorsement of any vendor’s product.

Redacted Version

November, 2006



**ICTAP TECHNICAL INTEGRATION WORK GROUP
TECHNICAL NOTES
TECHNICAL NOTE 2006-5, VoIP, November 2006**

SUMMARY OF TECHNICAL ISSUES:

What are the technical issues?

- This technical note discusses Voice over IP (VoIP) technologies and their application in public safety, with focus on land mobile radio environments.

How do these issues relate to ICTAP services and Sites?

- These issues are of concern to UASI-supported Sites considering new equipment and capabilities.

What is the status of VoIP?

- Many LMR manufacturers are offering VoIP-based solutions for public safety LMR.
- VoIP usage is growing rapidly in the commercial sector.
- Several VoIP signaling standards exist: H.323, SIP, and Megaco are the most highly adopted but very few are used in public safety communications systems. The Inter-RF Subsystem Interface (ISSI) protocol being developed within the Project 25 standards suite is the first VoIP standard based on public safety requirements. These protocols all use the Real-Time Transport Protocol (RTP) and Session Initiated Protocol (SIP).
- When VoIP is extended into the radio realm, carrying signaling information for basestations, repeaters, and mobile units, it is sometimes referred to as Radio over IP or "RoIP".

What are the benefits/disadvantages of VoIP?

- VoIP enables voice and signaling (call set-up, call tear-down, etc.) to travel over an IP network instead of over traditional circuit switched networks. The advantages are:
 1. Cost - VoIP costs considerably less than circuit switched networks, and COTS equipment can be leveraged,
 2. Availability - IP networks are inherently fault tolerant,
 3. Interoperability - conversations can be routed between networks, such as between public safety personnel operating in different bands or in different localities, and
 4. Flexibility / Scalability - IP networks are easy to expand.
- Disadvantages can include:
 1. Packet Loss - silent pauses
 2. Jitter - variability in packet delivery time
 3. Latency - voice transfer time, usually measured in milliseconds
 4. Echo - as the name implies, for either transmitting or receiving user
 5. Distortion - as the name implies, for either transmitting or receiving user

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



These disadvantages are largely overcome by advances in protocols and networking hardware and technologies.

What resources are available to ICTAP in support of UASI sites?

- ICTAP personnel may study this document to learn about or refresh their understanding of VoIP technologies in relation to Public Safety.
- ICTAP engineers can answer technical questions from supported sites and other ICTAP personnel.

KEY TALKING POINTS FOR ICTAP PERSONNEL

This ICTAP technical note provides an overview of VoIP in public safety LMR. The primary points are as follows:

- IP, or Internet Protocol, is the addressing protocol used by the Internet, and there are at present two versions: IPv4, which allows for billions of unique addresses, and has been almost ubiquitously adopted; and the newer IPv6, which has a nearly unlimited number of addresses, and has been only marginally adopted (The US government is migrating its IP backbone to IPv6 in 2008).
- VoIP is the concept of encoding voice into data packets for distribution over an IP network using a variety of open and/or proprietary protocols.
- Divided into packets, voice may be transmitted to its destination over numerous redundant paths, versus a single path as is the case in circuit switched communications.
- Being IP-based, encoded VoIP can leverage the use of Commercial Off The Shelf (COTS) hardware and software components for both voice and signaling traffic which can translate into significant cost savings and improvements in flexibility and scalability.
- In VoIP, a speaker's voice signal is encoded into an efficient binary form using a voice codec or vocoder, of which popular examples include ITU standard G.711 (Pulse Code Modulation) and the DVSI's proprietary IMBE and AMBE codecs.
- The primary protocols used for transfer of voice over IP are RTP and UDP (in tandem).
- VoIP signaling protocols include H.323, SIP, and MGCP.
- Almost all new LMR systems leverage VoIP in some capacity, including trunked systems, consoles and gateways.
- The Project 25 Inter Subsystem Interface (ISSI) will leverage VoIP technologies based on RTP/UDP and SIP.

These topics are important because:

- Users should be aware of the existing and emerging technologies so that they can consider them in their long term communications procurement plans.

Please see the Glossary for definition of terms.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.

DESCRIPTION OF OVERALL TECHNOLOGY OR TECHNICAL ISSUES

This technical note explores Voice over IP (VoIP) technologies and protocols. VoIP is a growing technology that for Land Mobile Radio (LMR) promises a number of advantages over traditional circuit-switched architectures. These advantages include cost savings, reduced complexity, improved availability, flexibility, security, and interoperability. Disadvantages may include reduced voice quality (e.g. Packet Loss, Jitter, Latency, Echo, and Distortion), although recent advances are minimizing such effects in traditional IP networks. This technical note discusses VoIP technologies and standards, trade-offs and advantages of VoIP, and Public Safety VoIP solutions and vendors. The contents include:

1. VoIP vs. Circuit Switched Communications	4
2. IP Networking Basics	5
3. VoIP Basics	10
4. Advantages and capabilities afforded by VoIP	10
5. VoIP Disadvantages & Challenges	11
6. VoIP Protocols	13
7. VoIP Equipment	18
8. VoIP and LMR	18
9. Public Safety VoIP Solutions	22
GLOSSARY	26

1. VoIP vs. Circuit Switched Communications

In traditional communications, dedicated channels are used to transfer voice information between parties. For example, radio users may use a single dedicated radio channel to communicate, or a phone call may be set up over a route or “circuit” that is then fixed for the duration of the call. In telecommunications, circuits generally involve two fixed links in full duplex mode (one send / one receive) usually coordinated via a separate network. When a call ends, the circuit is torn down and the network path or “trunk” is made available for other calls. This architecture is depicted in a simplified manner in Figure 1, where the nodes (circles) represent switches within an exchange.

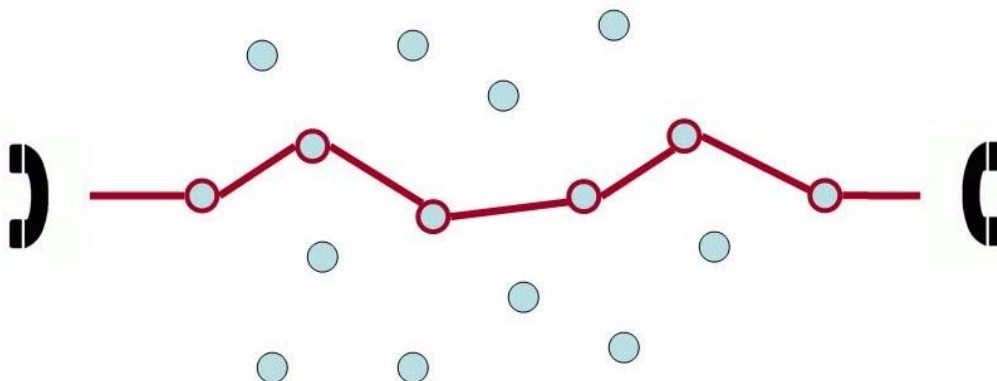


Figure 1 – Circuit-Switched Architecture

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.

VoIP, on the other hand, does not require fixed and dedicated routes between communicating parties. Instead, digitally encoded voice signals are broken into multiple data packets that are routed individually over a packet-based network such as the Internet. Packets may take many different routes and may share the network with other traffic such as for email and the web. This architecture is depicted in Figure 2, where the circles represent IP network nodes such as routers and gateways.

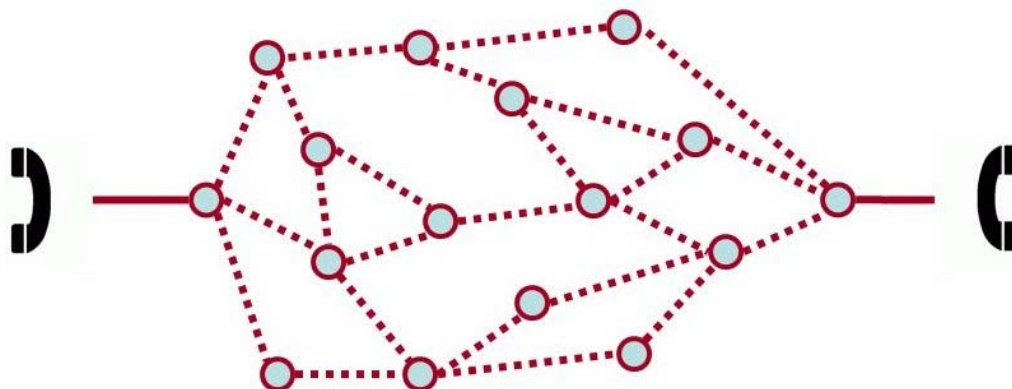


Figure 2 – Packet-Switched Architecture

A number of packet network technologies exist, including IP and ATM. IP is the most prevalent, although it was not originally designed for critical real-time data communications such as for voice. Advances in VoIP protocols and network equipment, however, have made VoIP not only possible but also extremely popular. Further advances in networking equipment, protocols, and IP itself (IPv6), will only serve to improve VoIP quality, reliability, capabilities, and cost.

2. IP Networking Basics

IP stands for “Internet protocol,” a data networking technology invented by Robert Kahn and Vinton Cerf at DARPA¹ in the early 1970s. The purpose of IP is to provide unique global node (computer) addressing to ensure that two nodes over an IP network, such as the Internet, can uniquely identify and communicate with one another. IP was adopted as a standard networking technology by the US military in the early 1980s, later by consumers beginning in the late 1980s, and it exploded in popularity in the late 1990s through the emergence of the Mosaic and Netscape browsers and the World-Wide Web.

2.1 Layers

The Internet Protocol Suite takes a layered approach to networking, where each layer is responsible for specific aspects of communication. There are two network layering representations commonly used to characterize IP-based networking protocols that users should be aware of. They are the International Standard Organization's Open System Interconnect (ISO/OSI) 7-layer network model

¹ Defense Advanced Research Projects Agency (<http://www.darpa.mil>)

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



(diagrammed in Figure 3, top left), and the simplified 4-layer DoD or TCP/IP model (Figure 3, top right). For example, RTP (Real Time Protocol) is characterized as operating in level 5 (Session layer) in the OSI model, and level 4 (application layer) in the DoD model. In either representation, once data is created for transfer, each layer in the protocol “stack” adds bits to the beginning of a packet, called a packet header, which it passes to the next layer (See Figure 3, bottom, for example with UDP traffic). With RTP operating over UDP, for example, RTP will add a header to a data packet and pass it to UDP (adding to overhead), and then UDP will add its own header, and so on down the layers. Because of this layered approach, the higher layers do not need to concern themselves with how the data is transferred, and the lower layers do not need to be concerned about the content.

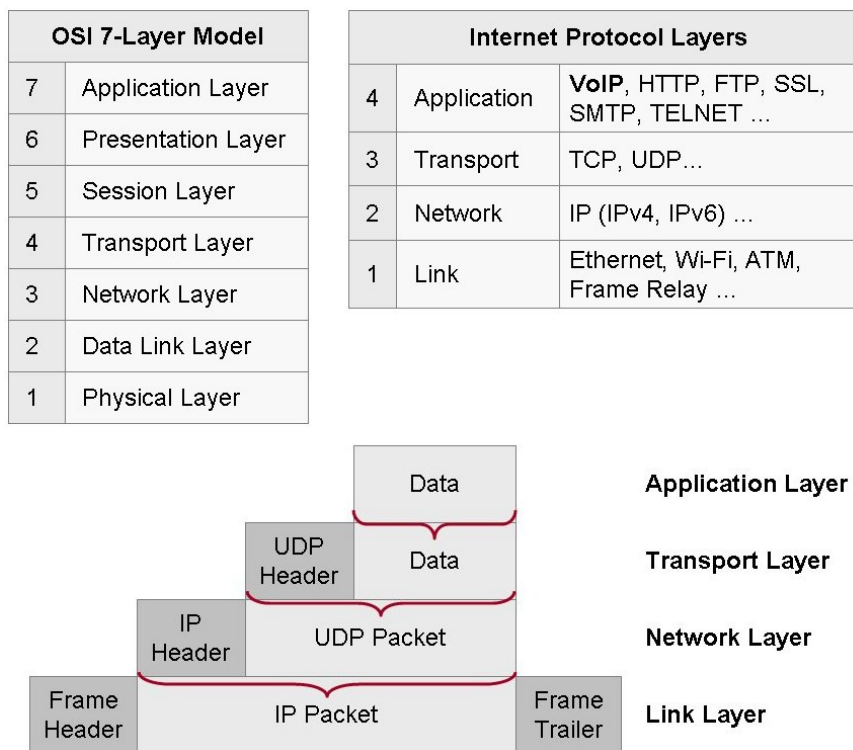


Figure 3 – Network Protocol Layers

2.2 Link Layer

The link layer coordinates and handles delivery of IP packets between directly connected (adjacent) nodes, which may be connected by any of a number of technologies such as Ethernet, Wi-Fi, and/or ATM. In general, the IP packet is encapsulated in a link layer envelope (header bits and trailing bits), transferred over some medium (such as a wire), which are reconstructed at each node through which it hops. The IP packet remains intact throughout all the hops to the packet's final destination, so long as the packet it is not dropped for some reason or its data corrupted.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



2.3 Network Layer

The IP protocol itself operates in the Network Layer (OSI 7-Layer Model), and it provides addressing between nodes in an IP network. It is important to note:

- IP is a “best effort” protocol that does not guarantee delivery of packets to the destination
- IP does not specify the routing of packets – packets are sent independently and can take different routes depending upon the algorithms used by the routers along the path
- IP does not guarantee that packets will arrive uncorrupted (only that the header is uncorrupted)
- IP does not guarantee that packets will arrive in order
- IP does not guarantee that packets are not dropped along the way to their destination

All of these shortcomings of IP may be addressed in the higher layers. For example, TCP (Transport Control Protocol), which operates in Layer 4, provides coordination between communicating nodes to guarantee error-free delivery to the application layer.

IP Versions

The most popular version of IP at present is version 4, called “IPv4”, which was defined by the Internet Engineering Task Force (IETF) RFC 791 and DoD MIL-STD-1777/1778 in 1981. In IPv4, a header is added to the data packets that provides addressing information. This is often referred to as encapsulation. IPv4 uses 32-bit addresses which supports up to approximately four billion unique addresses. IPv4 does not guarantee delivery, and it does not support packet prioritization very well. Packet prioritization, known as Quality of Service (QoS), allows packets to be assigned a priority in the packet header. With QoS, packets marked as real-time data, such as voice, are routed preferentially over data marked as non-critical, such as email, to reduce latency and jitter in the transfer of real-time data.

An improved version of IP called IPv6 was adopted by the Internet Engineering Task Force (IETF) in 1994 to overcome many of the limitations of IPv4. Although still not highly adopted yet, IPv6 has a number of benefits:

- IPv6 supports 128-bit addresses, which translates to 3.4×10^{28} or more than 50 billion x billion x billion addresses per person alive today. Not only does this large number remove the looming problem of IPv4 address depletion (as there are only 4 billion addresses available for the entire “public” IPv4-based Internet²), but the large number improves security – scanning certain IP blocks for vulnerabilities is infeasible as there is little likelihood of hitting an active address by randomly searching the large IPv6 address space.
- IPv6 has an improved header format (see Figure 4), which makes the protocol more efficient than IPv4. However, IPv6 headers are not compatible with IPv4 – routers must be able to detect both types for both systems to work together.

² This is alleviated by the use of Network Address Translation, or NAT, which enables multiple computers to connect the public IPv4-based Internet sharing a single public IP address.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.

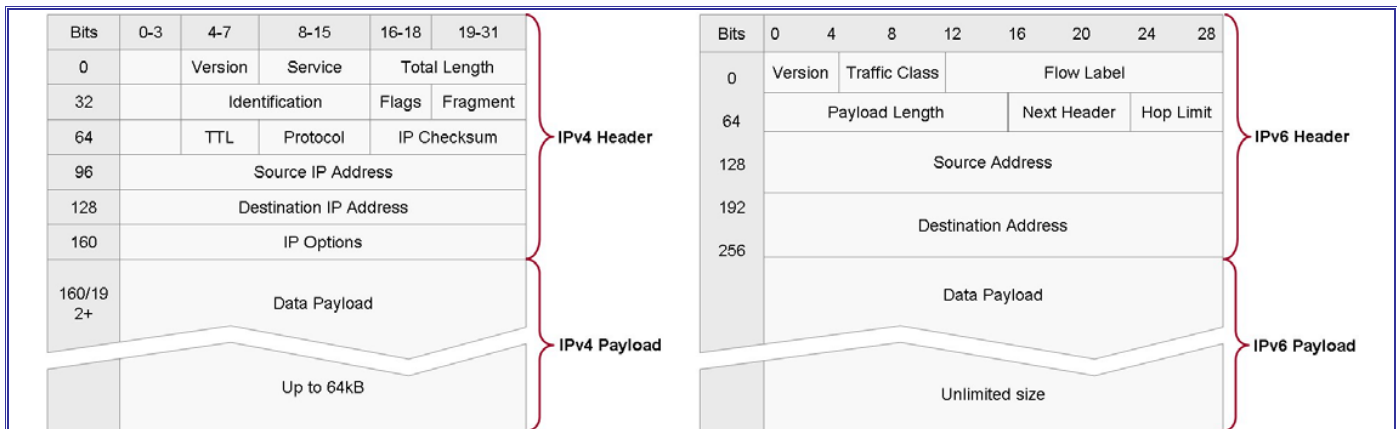


Figure 4 – IP Packet Headers, IPv4 vs. IPv6

- IPv6 supports standardized Quality of Service, which will improve real-time data communication such as VoIP.
- IPv6 namespace leads to efficient routing, allowing simpler end-to-end communications with fewer hops.
- IPv6 allows for automatic address configuration.
- IPv6 addresses security with integrated IPsec encryption and authentication capabilities.

It is important to note, the Federal Government and DoD mandated a transition to IPv6 for their network backbones in 2008.

The TIA TR8 working group, which is the body responsible for developing standards for public safety communications is aware of the IPV4 to IPV6 transition issue. Traditionally, public safety communications systems have not used the internet to any significant degree in their Standards. This is beginning to change with the recent completion of the ISSI for interconnecting LMR systems. There is also a large investment in legacy applications and the increasing use of networked data in public safety applications. Due to time pressures, the present position of this body is to complete the suite of work based on the ISSI in IPV4, and explore the transition to IPV6 in 2007 or later.

Public Safety users may wish to inquire with vendors about IPv6 compliance and the possibility of an upgrade should IPv6 become more widely adopted and deployed.

2.4 Transport Layer

The Transport layer coordinates the creation of data links between end-nodes (hosts) on an IP network and controls the integrity of the data that is exchanged between the hosts. The two primary protocols used in the Transport layer are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Each protocol uses the concept of *ports* on IP hosts, a port being a 16-bit number (0 to 65,535) to distinguish connections, of which ranges are reserved for special purposes.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



For example, TCP port 80 is used generally for web traffic and port 25 is generally used for sending email.

The TCP protocol guarantees reliable and in-order delivery of data between sender and receiver. In TCP every packet is assigned a sequence number that ensures the IP packets can be properly reconstructed at the receiving end should packets be received out of order. Sequence numbers also enable the receiver to identify packets that have been lost or not received within a preset time limit, in which case a request is made for that specific packet to be resent. The TCP module at the receiving end also sends acknowledgements for packets that are successfully received by the sender. TCP also ensures that no data is corrupted during transfer by employing a checksum in each packet (like a signature for the data). With its sophisticated algorithms and overhead, TCP slows data transfer somewhat. Given its reliability, however, TCP is the most widely used transport protocol on the Internet.

Unlike the TCP protocol, the UDP Protocol is designed for speed. UDP does not provide the reliability and ordering guarantees that TCP does. Without such overhead UDP is often better suited for real-time applications that do not necessarily require 100% integrity, such as VoIP. UDP is also required for broadcast (send to all on local network) and multicast (send to all subscribers). UDP accounts for approximately 20 percent of all Internet traffic.

A comparison of TCP and UDP packet headers that illustrates the difference in complexity is displayed in Figure 5.

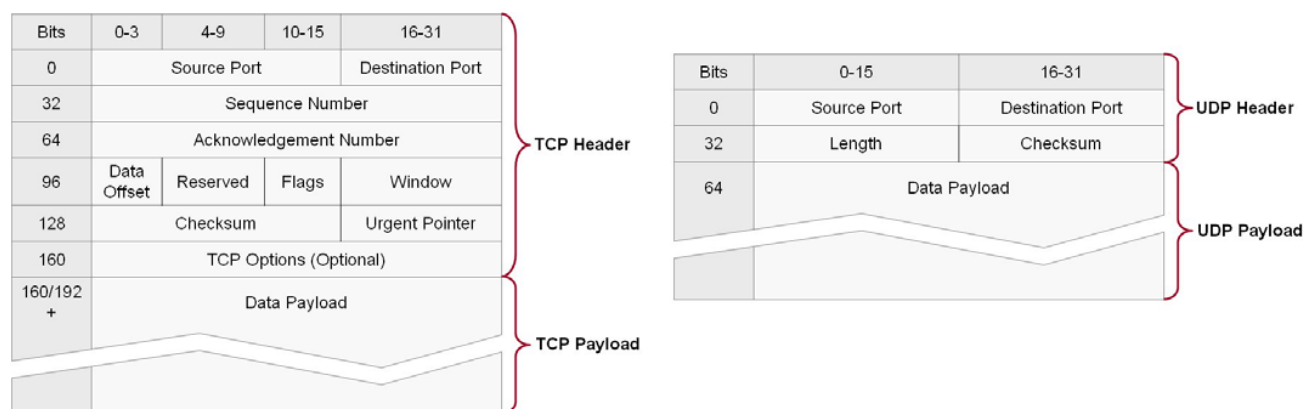


Figure 5 – TCP vs. UDP Packet Headers

2.5 Application Layer

The Application layer includes the higher-level protocols that process data once it arrives at its destination, and before being sent from the source. Examples include the Hypertext Transmission Protocol (HTTP), that publishes and receives HTML web pages, and Session Initiated Protocol (SIP), that processes interactive user sessions involving, for example, real-time voice communications.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



3. VoIP Basics

The basic mechanics behind VoIP are as follows.

1. A user initiates a call to another user through an exchange of VoIP protocol signaling information over an IP network. A call can be between nodes directly connected to the IP network, such as between two personal computers, or between traditional analog handsets that interface with the IP network transparently via a VoIP gateway device.
2. Once a call is initiated, each party's voice is digitally sampled from a microphone and encoded using one of various codecs. The objective of encoding is to compress the voice signal and reduce the amount of data that is transferred over the IP network, thereby minimizing the data bandwidth required. Codecs must, however, be efficient enough that they do not themselves increase the time it takes to transfer the voice between parties, which is referred to as latency.
3. The packetized voice is then channeled from one user to the other over an IP network using the Internet Protocol Suite described earlier.
4. As VoIP packets arrive at their destination, they are collected in a memory buffer and reassembled.
5. Once all the header information has been removed, leaving only the encoded voice, the data is decoded back to analog form and played over a speaker at the receiver's end.

4. Advantages and capabilities afforded by VoIP

4.1 Cost

The cost of VoIP systems can be significantly less than circuit switched systems. In circuit switched systems, proprietary technologies are often used and equipment may be produced in relatively low volume, equating to higher prices. Also in circuit switched communication, signaling information is also carried over an additional and separate signaling network from the voice information, which adds additionally to the cost.

VoIP, on the other hand, operates over IP which is based largely on highly commoditized standards-based hardware thus leading to lower prices. In IP, signaling is also carried over IP, so only one network is required. Furthermore, there is a convergence of communications technologies into the IP realm, meaning that different technologies can share the same IP network, commonly referred to as a "converged network." For example, VoIP voice and signaling can share an IP network with email and Internet traffic as well as streaming video and instant messaging. This all translates into potential cost savings because only one network needs to be procured and maintained rather than several.

It should be noted that some VoIP systems use private networks for a combination of security (e.g. to prevent viruses) and performance (e.g. to ensure voice quality) benefits. This may increase costs somewhat. In public safety, isolated IP networks are often created specifically for mission critical VoIP communication. When converged networks are employed, it is imperative that QoS be enabled

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



(described in Section V) to prioritize the real-time voice traffic. Procurement officials should also be aware that vendor specifications like “enhanced IP” can translate to proprietary (non-COTS) network equipment requirements, which may increase the cost of a VoIP-based LMR solution considerably.

4.2 Availability

IP networks are inherently fault-tolerant. Data may traverse the network along a large number of possible paths, so when a data link goes down data is simply re-routed over an alternative path by the link layer protocols.

4.3 Interoperability

With VoIP, conversations can be routed between networks. For example, conversations can be held between public safety personnel operating in different bands or in different localities by using VoIP as a gateway, so long as the VoIP networks are configured for this capability.

4.4 Flexibility / Scalability

In VoIP, voice communication is channeled over an IP network, rather than through circuit-switched channels. Adding capacity or redundancy can be as simple as adding additional networking equipment.

5. VoIP Disadvantages & Challenges

5.1 Packet Loss

In an IP network, packets can be lost due to congestion, dropped connections, or other network problems. When packets are lost, the protocol may request that the sender re-send. In real-time communication like VoIP it is not feasible to request lost packets be resent because of the additional delay created. Infrequent lost packets are typically handled by the voice codec and go unnoticed to the human ear. However several lost packets in a row may translate into silent pauses. More robust and reliable networks can alleviate problems due to packet loss. Typically VoIP systems require that no more than 1% of packets are lost in transmission.

5.2 Jitter

A number of different types of jitter exist, but in VoIP jitter generally refers to the variability in packet delivery time. For example, if a network is congested, some packets may transfer quickly and other slowly, reducing the quality of a call. Typically, a high quality network will have less than 1 ms of jitter throughout the entire system. Jitter can be mitigated by using jitter buffers, which store packets in memory for a certain amount of time before aggregating the voice signal and releasing it to the user. The tradeoff to larger jitter buffers is an increase in packet latency.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



5.3 Latency

Each step in the transfer of voice takes time – such as encoding, transfer over the network, and decoding. The overall time from when a user speaks and the other user hears the voice is called latency. If the latency is too long, conversations can become difficult to follow – callers may sense a pause in conversation and begin speaking simultaneously, halting when they hear the other speaker beginning. Traditional analog voice systems have latency on the order of 50 milliseconds or less. VoIP systems should approach this latency to be fully accepted. The International Telecommunication Union (ITU) recommends a latency of 150 milliseconds or less for one-way communication³. The average human ear will detect latencies over 250 milliseconds⁴. In contrast, P25 standards requires no more than 500 ms delay through a single RF subsystem, and no more than 1 sec through multiple RF subsystems⁵. Latency is generally overcome by fast networks, and fast and efficient encoding / decoding of VoIP data streams. QoS, or “Quality of Service”, which in IP refers to prioritizing certain packets over others based on types, can also reduce latency when voice traffic is favored over general non-real-time network traffic such as email.

5.4 Echo

In certain circumstances, VoIP conversation can be susceptible to echo, where a speaker will hear their voice repeated back to themselves like an echo in a large room or cavern, or a listener will hear the speaker’s voice echo. In VoIP, this can be caused by acoustic feedback from a speaker to a microphone in a handset, or mismatched analog-to-digital VoIP gateways. Well tuned equipment can overcome echo in a VoIP network. Digital signal processing (DSP) chips or software are available today that include echo canceling capabilities. Some examples include SoftEcho and OCT 9600 by Octasic Semiconductor⁶ and Echo Cancellation technology by IBM⁷.

5.5 Distortion

The conversion of analog voice to digital and back again can potentially cause distortion. Distortion can be alleviated by using improved encoding/decoding (codec) techniques.

5.6 Quality of Service (QoS)

Quality of Service (QoS) is important in VoIP based land mobile radio systems. QoS refers to the optimization of voice and/or data packet traffic in order to create a reliable connection between transmitter and receiver. Since a VoIP service does not use a dedicated circuit for each

³ See the ITU-T G.114 Recommendation for details.

⁴ See “10 important questions to ask your VoIP provider” posting by Russel Shaw in *Experts on Demand*, May 2006 (http://expertanswercenter.techtarget.com/eac/blog/0,295203,sid63_tax303505,00.html).

⁵ For more information, see the ICTAP Technical Note 2005-1 “P25 Standards”

⁶ http://www.octasic.com/en/tech/echo_cancel.php

⁷ http://www.haifa.il.ibm.com/projects/multimedia/audio_video/spkr.html

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor’s product.



communication path, packet congestion can occur on shared network lines. This congestion can lead to a lower level QoS in VoIP based radio systems.

QoS for VoIP systems can be characterized by the three major factors described earlier: latency, jitter and packet loss. These QoS factors can be reduced, but not eliminated, by deploying public safety radio systems on private and dedicated IP networks. This can increase the available bandwidth for system, but alone will not increase the systems level of QoS. Packet prioritization techniques must still be deployed to minimize latency, jitter and packet loss in VoIP networks. Some techniques include bandwidth reservation, packet service classification, priority queuing and Multi-Protocol Label Switching (MPLS). Network bandwidth can also be reserved for packets labeled with higher priority, and priority queuing systems will process those packets faster. In LMR systems, voice and call signaling packets should be given higher priority than text messaging and other data packets using such techniques.

6. VoIP Protocols

A number of VoIP technologies exist for call setup and the transfer of voice between parties. This section looks at the most commonly adopted VoIP technologies, including 1) voice transfer protocols, that transfer real-time voice data once a VoIP call is established, 2) signaling protocols, that define how calls are set up, maintained, and closed, and 3) voice codecs, that digitally encode and decode analog voice.

6.1 VoIP Voice Transfer Protocols

RTP / RTCP – For the transfer of voice information in real-time once a call is established, VoIP uses UDP in the Transport layer in combination with the Real-time Transport Protocol (RTP) and the Real-Time Control Protocol (RTCP). This pair of protocols was originally developed by the IETF in the late 1990s and updated in RFC 3550 in July 2003. RTP includes a sequence number and timestamp for voice packets to enable the VoIP application to efficiently buffer and reconstruct the digitized voice. RTCP provides information on the quality of the network which enables the application to manage bandwidth efficiently. UDP in combination with RTP/RTCP provides many of the benefits of TCP but is tailored for real-time data with less overhead.

6.2 VoIP Signaling Protocols

A large number of proprietary and non-proprietary protocols exist to set up RTP-based voice connections. This section covers the most widely adopted protocols – H.323, SIP, Megaco, and MGCP. Some of these protocols are *centralized* (like H.323, Megaco, and MGCP), where a centralized system is used to coordinate the connections between users. Other protocols are *decentralized* (like SIP), where users can coordinate with each other directly without the use of a centralized management system.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.

H.323 – H.323 is a suite of standards recommended by the ITU-T (ITU Telecommunication Standardization Sector) in 1996 that collectively provide for audio-visual communication sessions on any packet network, although primarily for IP. H.323 is well adopted because it is an early standard, it defined a basic call model as well as additional business services, and it was the first complete standard to adopt RTP to transport audio and video over IP networks. H.323 is a centralized binary protocol and it is well suited for interfacing with legacy communications systems.

The current version of H.323 is version 6, approved in June, 2006. H.323 defines protocols for signaling (H.225.0); messages and procedures used for opening and closing audio, video and data channels (H.245); protocols for supplementary services (H.450); and protocols for security (H.235).

SIP – Session Initiation Protocol (SIP) is an IETF standard for the establishment of multimedia sessions. Although it was initiated at the same time as H.323, the first usable standard was not published until 1999 as RFC 361, with later improvements in 2002. Because of its late publishing SIP was not initially well adopted, but its simplicity has led to rapid adoption since then. Unlike H.323, SIP is an ASCII-based signaling protocol that is not designed to interface with legacy equipment. SIP is modular in design and is considered easier to setup and troubleshoot.

SIP has two primary elements – the user agent and network server. The user agent initiates requests, and the server responds to requests. Requests include information about the session and media types being transferred, described in the Session Description Protocol (SDP). Requests are generally channeled via SIP proxy agents that serve to locate the end-user. SIP addresses are referred to as SIP-URLs of the form sip:user@host.domain. The steps involved in a SIP signaling session are highlighted in Figure 6.

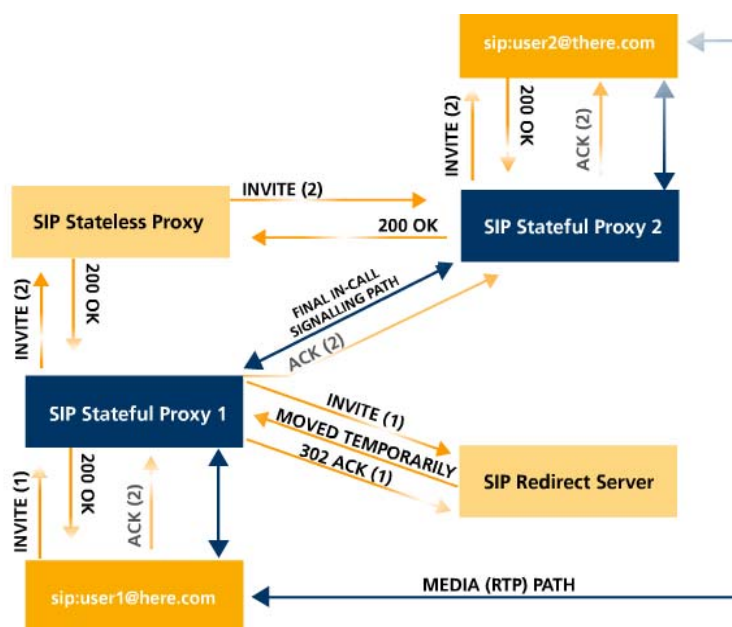


Figure 6 – SIP Signaling Overview⁸

⁸ Source – Sipcenter.com – Non-Copyright, Released to Public Domain

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



Megaco (H.248) – Megaco is a signaling protocol used to coordinate real-time communication between a Media Gateway and a Media Gateway Controller in a VoIP network. Megaco is defined by IETF RFC 3525 and it was developed jointly by the IETF and ITU, which call it Megaco and H.248 respectively. Megaco is used primarily to control gateways in order to support voice/fax calls between PSTN-IP or IP-IP networks.

MGCP – Media Gateway Control Protocol (MGCP) is a gateway-internal VoIP signaling protocol defined by IETF RFC 3435. It is a predecessor to Megaco. MGCP is used by telephony providers to keep track of subscriber calls, and it supports large distributed systems that appear to operate like a single VoIP gateway. MGCP implements a Call Agent that acts as a software switch for a VoIP network, but it is not involved in encoding or other such basic VoIP functions.

6.3 Centralized vs. Decentralized Signaling

Centralized and decentralized signaling protocols each have advantages and disadvantages, outlined in Figure 7.

Centralized Call Control	Distributed Call Control
H.323, Megaco, MGCP	SIP
Centralized administration	Distributed administration
Supplementary Services	Supplementary Services harder to implement
Difficult to Scale – all new features and applications must be implemented on central controller	Scalable – if more applications, functions or performance are needed, servers can be added anywhere
Difficult to provide network redundancy	Easier to provide network redundancy
WAN inefficient	WAN efficient
Static endpoint capabilities	Flexible endpoint capabilities negotiated per session
Typically Lower Operations and Maintenance Costs	Typically Higher Operations and Maintenance Costs

Figure 7 – Centralized vs. Distributed for VoIP Setup and Call Control⁹

Configuration: The centralized call control model provides superior control of configuration and maintenance whereas the distributed model is more difficult to administer and maintain.

Security: Centralized control requires endpoints be known to a central authority making access easier to control. The distributed model makes it more difficult to control access thus increasing the security risk.

⁹ Source – Cisco CVOICE 4.2 VoIP Fundamentals Class Material

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.

Reliability: The centralized model is vulnerable because of its single point-of-failure and contention whereas the distributed model can lessen the dependency on any single component of the network.

It is possible for multiple signaling systems to operate together. An example is illustrated in Figure 8.

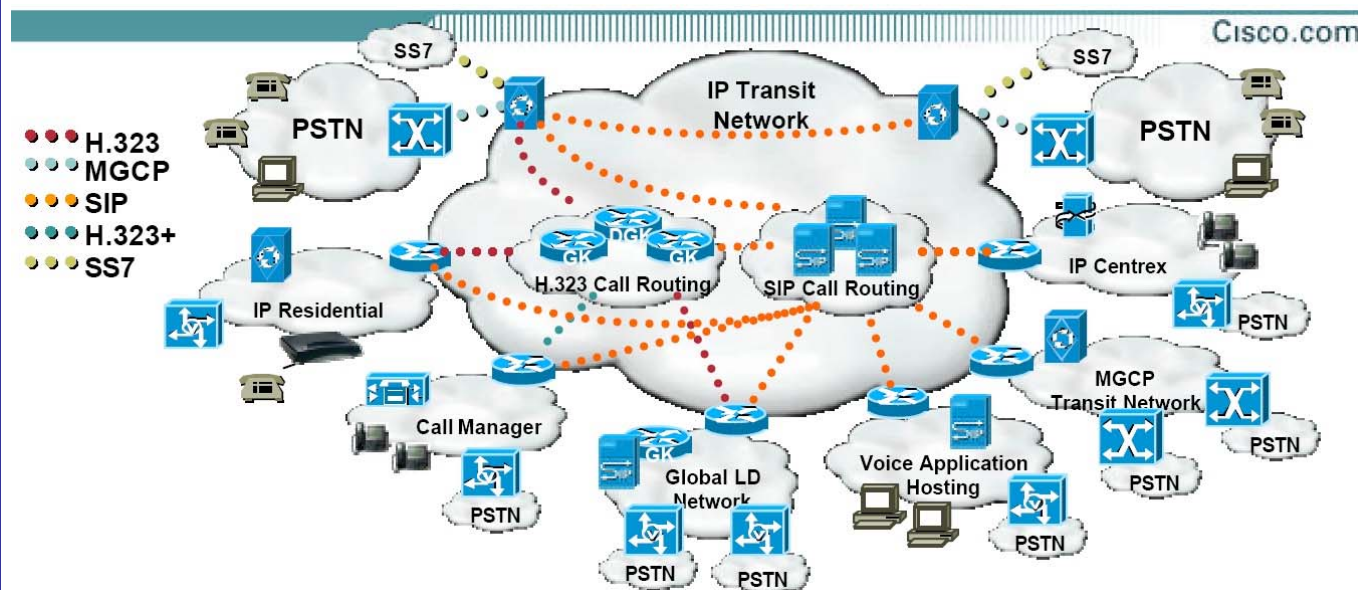


Figure 8 – Multiple VoIP Protocols and the PSTN¹⁰

6.4 Voice Codecs

In VoIP, when voice is converted from analog to digital and vice versa, conversion is done using a voice codec (also known as a vocoder). A voice codec's job is to represent the analog waveform accurately and efficiently so that voice quality is maintained and bandwidth usage is minimized. A number of algorithms may be employed in this process, each with varying levels of compression (how small they can compress the voice information in bits per second) and quality (how intelligible the voice is to the listener once reconstructed). A high degree of compression and voice quality are required for LMR. This section highlights a few common codecs.

AMBE – Advanced Multi-Band Excitation, a proprietary vocoder developed by Digital Voice Systems, Inc (DVS), used, for example, in satellite telephony, XM radio, and M/A-COM Opensky trunked radio systems. AMBE operates at a variable encoding rate, but can compress successfully down to 2.4 kbps.

G.729 (CS-ACELP) – Conjugate Structure Algebraic Code-Excited Linear Prediction, defined by G.729a, which is part of the ITU-T suite of voice coding standards under the G.7xx heading. G.729 encodes a voice signal down to 8 kbps.

¹⁰ Source - http://www.cisco.com/application/pdf/en/us/guest/tech/tk701/c1482/ccmigration_09186a00800b3f21.pdf

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



GSM 06.10 – a standard developed by ETSI based on a Regular Pulse Excitation Long Term Predictor (RPE-LTP) algorithm. This vocoder is used in all GSM cellular voice communications, a technology used heavily throughout the World, including the US. GSM encodes a voice signal down to 13 kbps.

IMBE™ – a proprietary vocoder developed by Digital Voice Systems, Inc (DVS), used, for example, in P25 Phase I. AMBE® improves upon the technologies used with the IMBE™ vocoder. IMBE operates at a variable sampling and encoding rate and can compress down to 2.4 kbps. P25 phase I standards employ IMBE encoding at 7.2 kbps. P25 phase II standards will use a half-rate IMBE vocoder, also developed by DVS, which is optimized to support phase II's 6.25 kHz narrowband slots.

G.711 (PCM) – Pulse Code Modulation, defined by ITU recommendation G.711. G.711 samples voice at 8 kHz (8000 samples per second) and encodes the voice signal at 64 kbps. Lower bitrates in schemes based on this standard were developed, such as through Adaptive PCM (APCM) which varies the size of the quantization step.

Characteristics of these codecs are summarized in Figure 9, including the voice bit rate, a number that is important to VoIP in LMR applications as radio links cannot typically support higher rates.

Codec	Bitrate	Mean Opinion Score (MOS) ¹¹
AMBE	Variable, down to 2.4 kbps	3.4 (@ 3.2 kbps)
G.711	64 kbps	4.1 (@ 64 kbps)
G.729	8 kbps	3.92 (@ 8 kbps)
GSM	13 kbps	4 (@ 13 kbps)
IMBE	Variable, down to 2.4 kbps	3.4 (@4.4 kbps)

Figure 9 – Voice Codec Characteristics

One of the key issues with VoIP packets is payload size – the amount of data transmitted within each packet. The header information is fixed and doesn't change as lower rate codecs are used. Consequently, the overhead increases significantly as a greater proportion of information transmitted in the headers. If the payload is increased to try to counter the increased overhead rate, that can increase overall delay. This is a trade-off that must be balanced by the VoIP protocols.

6.5 Transcoding

Transcoding is the direct digital-to-digital conversion from one codec to another codec, or between the same codec sampled at different rates. Transcoding is used when calls are bridged between different VoIP systems and codecs. It is a process that takes place in a gateway. Transcoding involves decoding/decompressing the original data to a raw intermediate format in a way that mimics

¹¹ A MOS score of 4 is equivalent to the voice quality of a standard telephone line.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



standard playback of the content (including any losses), then re-encoding it into a new format. Transcoding causes a progressive loss of quality and increased latency with each successive generation, and it should be discouraged unless unavoidable. The effects of transcoding can be minimized by minimizing the number of gateways in the system, or by using identical codecs between gateways. These are design issues that must be considered when procuring VoIP technologies.

7. VoIP Equipment

This section discusses the equipment that is used in a VoIP system.

Gateway – If a communication device, such as an LMR handset or traditional landline phone is not connected directly to an IP network, the connection is achieved using a gateway, sometimes referred to as a media gateway or softswitch. A gateway can be as simple as a program running on a personal computer. At the highest level, a media gateway is a carrier-class server (99.999% availability) that sits on an edge of a network and performs switching and coordinates connections to a Public Standard Telephone Network (PSTN) switch on one side, and “speaks” all major VoIP protocols over an IP network on the other side. The most powerful gateways, which may coordinate thousands of “digital VoIP circuits”, are regulated by a media gateway controller which is a part of centralized signaling systems, described earlier. In VoIP-based LMR systems, gateways would be used to bridge different systems together, as highlighted in the previous section on transcoding.

PBX – A Private Branch eXchange (PBX) is essentially a telephone exchange that is owned by a business or individual rather than an operator. In VoIP, a PBX (or router) will link a VoIP network with a POTS (Plain Old Telephone System) line, enabling the setup and transfer of calls within an organization, as well as the connection of calls from and to outside POTS lines. For example, a PBX can allow a VoIP device to receive calls on a traditional telephone number¹², or to make calls from a traditional telephone number. A PBX may also be employed to link an LMR voice channel with a POTS line.

8. VoIP and LMR

Land Mobile Radio systems are used to provide communications between a large number of users over large geographic regions. Communications between mobile users and dispatch centers are established using base stations and centralized network infrastructure which are linked using external interfaces such as leased lines or microwave connections. In the current market, two basic types of LMR networks are available: circuit-switched and packet-switched (VoIP).

A traditional circuit-switched LMR system is displayed in Figure 10. In circuit switched networks, devices known as channel banks are used to link sites through their particular external interface. Circuit-switched systems provide communication between sites by setting up dedicated channels (circuits) which allocate a fixed amount of bandwidth for transmissions. The available bandwidth per channel is fixed and thus so is the number of simultaneous channels that can be supported. Although dedicating bandwidth to fixed communication paths can be advantageous in many situations, single

¹² Traditional numbering schemes are defined by ITI recommendation E.164.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.

points of failure within the network may be significant enough to leave portions of the system inoperable.

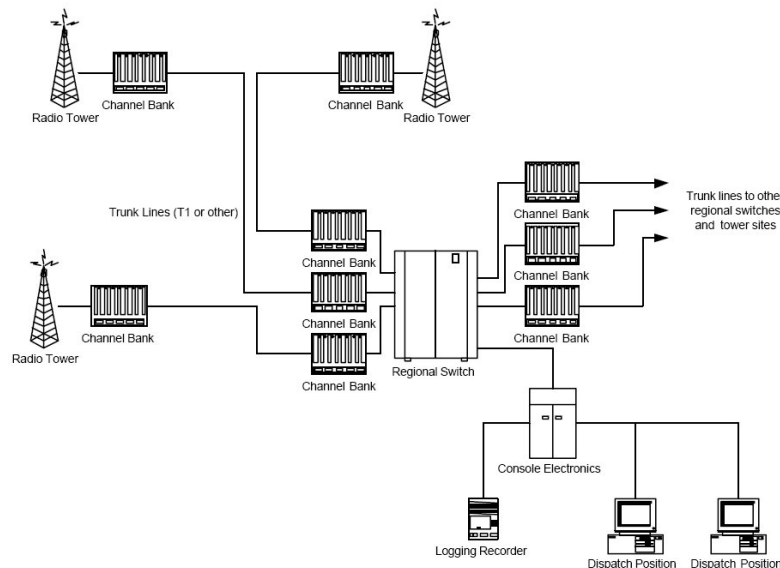


Figure 10 – Circuit-Based LMR System¹³

A simplified packet-switched LMR system is displayed in Figure 11. In packet-switched networks, the information (whether voice or data) is converted to digital format and divided into packets for distribution over the network. The individual packets that comprise the original message are sent separately and do not require the dedicated channels as in a circuit-switched network. Packets that comprise a message may arrive at the final destination having traversed several different communication paths, and thus several messages may be sent over a single channel.

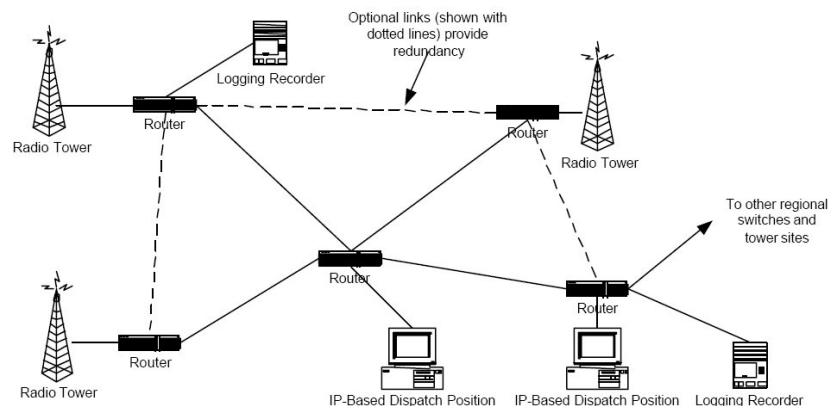


Figure 11 – An Equivalent VoIP-based LMR System¹⁴

¹³ This figure is extracted from Software-Enabled Wireless Interoperability Assessment Report – Voice-Over-Internet Protocol Technology”, PSWN Program Report, December, 2001

¹⁴ This figure is extracted from Software-Enabled Wireless Interoperability Assessment Report – Voice-Over-Internet Protocol Technology”, PSWN Program Report, December, 2001

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



In VoIP-based systems, the functionality provided by the channel banks of the circuit-switched network is provided instead by COTS routers and/or switches¹⁵. This networking infrastructure is designed in accordance with standard (IP-based) protocols, thus providing a baseline level of interoperability between two or more separate systems. Additionally, the COTS routers/switches are less expensive when compared to the channel bank infrastructure used in traditional circuit-switched LMR systems. Figure 12, below, provides a comparison between circuit switched and packet switched LMR network architectures, including advantages and disadvantages for each.

Circuit-Switched Networks		Packet-Switched Networks	
Advantages	Disadvantages	Advantages	Disadvantages
Legacy system (Similar to Plain old Telephone Service (POTS) or Public Service PSTN.) • Implements deterministic multiplexing. • Uses Frequency Division Multiplexing (FDM) or Time Division Multiplexing (TDM) to encode and transmit data. However, TDM is the predominant technology in place now. • Purely connection oriented. • Mature technology. • Guaranteed capacity. • Systems are currently in place and organizations are trained/have experience with the technology. • Has inherent security.	Costly to implement. • Single points of failure – if a link between two nodes such as between a base station and a dispatch station were to be disengaged then communication between possibly many users and a vital point of the circuit would be removed and made useless reducing the overall effectiveness of the network. • Due to the way circuit-switched networks are implemented (circuits are set up between two nodes and resources allocated) it has some inherent disadvantages such as: ○ Inefficient utilization of network resources ○ Limited number of users ○ Difficult to integrate with packet networks. • Fixed location for control functions. • Scales poorly and topology is difficult to change.	May be less costly by utilizing common off the shelf IP based technology (i.e. routers, gateways, and network applications). • Implements statistical multiplexing to maximize efficiency of network resources. • Provides for possible data and voice integration on a single network. • Can have significantly more concurrent network users – limited by acceptable network packet delay and loss. • Scales easily and seamlessly to accommodate more users or to allow further extension of coverage area. • Flexibility is inherent to the system. • Redundant topology. • Easy to integrate with other packet-switched networks. • May provide data services for other systems, including shared capacity with generic IT systems.	Transition costs associated with moving to new technology. • While relatively mature, not as mature as circuit-multiplexing. • Organizational retraining required. • Rely on service providers to provide contracted QoS (i.e. service level agreements). • Less secure than circuit-switched systems (without additional measures).

Figure 12 – Circuit Switched vs. Packet Switched Networks¹⁶

¹⁵ Certain providers may require “Enhanced-IP” support which may imply non-COTS equipment.

¹⁶ This figure is adapted from Center for Wireless Telecommunications, “USCS Tactical Communications: Objective Architecture Report,” Virginia Polytechnic Institute and State University, March 2003

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor’s product.



8.1 Project 25 (P25)

Project 25 is a suite of standards for digital radio communications used by federal, state and local public safety agencies to enable them to interoperate with other agencies regardless of the manufacturer of the P25 compliant equipment. The P25 standards define a number of interfaces and features, some of which are still under development. Phase 1 P25 systems adopt 12.5 kHz radio channels that support both digital and analog communication between mobile units, basestations, and repeaters, with a data rate of up to 9.6 kbps. Phase 2 standards, which are still under development, will support two voice conversations in 12.5 kHz bands using a TDMA frame structure, giving an equivalent per-user bandwidth of 6.25 kHz. This requires the use of the half rate IMBE vocoder, which was recently agreed to.

The use of IMBE vocoders has necessitated the development of a specialized VOIP protocol to carry the LMR voice within and across systems. This is because transcoding to and from one of the more conventional voice standards results in significant loss of voice quality while adding delay (see section 6, Transcoding). These protocols also ensure that the voice and data packets from the air interface are carried with minimal overhead. Furthermore, the standards developers felt that the special needs of LMR voice and its use were not adequately covered in the protocols available to date. The P25 standard also has delay requirements which must be satisfied, and additional signaling that must be carried, while taking into account user mobility.

For these and other reasons, the P25 VoIP protocol uses RTP for voice and signaling transport, and SIP for call set up and management. RTCP is not used; but additional in-band signaling is incorporated. This hybrid approach was selected after careful debate, and is expected to provide superior performance.

The P25 VOIP protocol is used in the following interfaces which are currently in various stages of development

- Trunked Inter-RF Sub-Systems Interface (ISSI)
- Conventional Fixed Station Sub-systems Interface (CFSI)
- Conventional ISSI
- Console Subsystems Interface (CSI), for conventional and trunked systems consoles

The first version of the Trunked ISSI (designated as ISSI Scope 1) has been completed and sent for publication. The CFSSI document (TIA 102.BAHA) was published in June, 2006, and describes both analog and IP based digital interfaces. The trunked FSI and CSI will be based on the next version of the trunked ISSI, (called ISSI Scope 2) which is an extended version of ISSI Scope 1. Scope 1 supports the transport of clear and encrypted voice and also user mobility from system to system. It does not support data, Over the Air Re-keying (OTAR), encryption management and other advanced functionality, which are expected in Scope 2.

The ISSI and CSI for conventional systems will be based on the CFSI, with extensions. This is because the CFSI is a much simpler interface, designed to operate over telephone lines, etc. The size, complexity and cost of the trunked ISSI are not seen as justified in the much simpler and

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



cheaper conventional systems. However, the trunked ISSI will be expanded with the ability to connect to a conventional system, when necessary.

Finally, a powerful potential use of the P25 VOIP protocol and the ISSI is the ability to build P25 gateways for legacy systems. Hence manufacturers can build gateways to interconnect their proprietary systems to proprietary systems of other vendors via the ISSI in a much more effective manner, not only passing voice, for example as is done today with the JPS/Raytheon ACU-1000, but also connecting the signaling as well. This will extend the useful life of legacy systems while enabling them to be connected seamlessly to newer systems during emergencies.

9. Public Safety VoIP Solutions

The following vendors offer IP-based P25 trunked systems. The details presented are based upon vendor claims:

EADS – EADS offers a P25 trunked solution using VoIP to connect all components of the system which includes Universal System Controllers, Trunking Site Controllers and Network Web Management. EADS also demonstrated their P25 ISSI at the Orlando APCO conference in August 2006. <http://www.eads-ps.com/>

EF Johnson – In July, 2005 EF Johnson announced their IP25 Trunked Infrastructure System which is an encrypted end-to-end digital Project 25-compliant system. It uses VoIP technology to integrate repeaters, a digital dispatch console, system management, a secure key management facility for over-the-air re-keying of radios in the field and a portable PDA-based key loader. <http://www.efjohnson.com/products/IP25Trunked.asp>

M/A-COM – M/A-COM's P25^{IP} solution provides end-to-end IP. M/A-Com provides system and network components including network and key managers, gateways to legacy equipment, over-the-air programming (OTAP) and system administration. M/A-COM also demonstrated its P25 ISSI at the Orlando APCO conference in August 2006. <http://www.macom-wireless.com/products/p25/>

Motorola – Motorola's ASTRO 25 v7.x is a trunked solution offering end-to-end IP connectivity to all components of the network. The system can also be integrated with a Motorola data network using the same infrastructure. http://www.motorola.com/governmentandenterprise/northamerica/en-us/public/functions/browseproduct/productdetailpage.aspx?navigationpath=id_807i/id_1174i

The following vendors offer VoIP capable gateways/consoles:

Avtec DSPatchNET – A mission critical dispatch system built to support over 512 consoles over local or wide area networks. <http://www.avtecinc.com/Products/dspatchnet/index.html>

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



Catalyst Communications - Catalyst's solution gives dispatchers radio control over the network in addition to voice capabilities. This radio control or Radio over IP (RoIP) allows users to change channels, scan and pass DTMF (Dual-tone multi-frequency) tones over the IP connection. Because most radio interfaces are not standardized, Catalyst works with different radio manufacturers to develop their respective interfaces for selected radios.

<http://www.catcomtec.com/index.php>

Cisco IPICS – The IP Interoperability and Collaboration System (IPICS) uses Cisco routers that support standard VoIP protocols and voice interface cards to convert radio traffic to IP for distribution over the network. The system also includes an IPICS server providing a suite of applications to setup and manage the network.

<http://www.cisco.com/en/US/products/ps6712/index.html>

Codespear SmartMsg – The SmartMsg application along with Codespear the Radio Interoperability module provides text and voice broadcast to all end users over a VoIP architecture. (See attached e-mail)

<http://www.codespear.com/interoper.asp>

JPS/Raytheon WAIS – The Wide Area Interoperability System (WAIS) is software that enables patching via VoIP for multiple products from the ACU family.

<http://www.jps.com/index.asp?node=178>

M/A-COM NetworkFirst – NetworkFirst uses M/A-COM's VIDA Network architecture providing voice interoperability over an IP backbone. The same hardware and software products used in NetworkFirst are also used in M/A-COM's P25 and OpenSky solutions.

<http://www.networkfirst.com/>

Motorola MOTOBRIDGE™ – Offered in four configurations, the MOTOBRIDGE™ solution is comprised of radio and workstation gateway units, a management center and a SIP server.

http://www.motorola.com/governmentandenterprise/northamerica/en-us/public/functions/browseproduct/productdetailpage.aspx?navigationpath=id_807i/id_2553i

SmartLink I-Network™ – Designed for mission critical networks to provide interoperability using SmartLink's I-Network products. These include a software defined I-Switch™, various I-Site™ channel modules at each radio site and an I-Console™ for dispatch.

<http://www.smmlink.com/products/index.asp>

Telex Vega – Telex Vega offers a variety of VoIP consoles and patching equipment. Telex Vega also partnered with EF Johnson to provide the console equipment for EF Johnson's P25 IP-based trunked infrastructure.

<http://www.telex.com/radiodispatch/products.nsf/pages/ProductType=VOIP>

Twisted Pair WAVE – WAVE for LMR™ is Windows-based software that enables interoperability over standard IP networks for dispatchers and radio users. WAVE is able to integrate with H.323 networks, Cisco router voice interface cards as well as direct connections to various audio gateways.

<http://www.twistpair.com/page.php?page=wave>

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



Zetron – Zetron offers a variety of consoles including a SIP based console that connects to SIP Radio Gateways (SRGs) over local or wide area networks. The SIP based console is also built to comply with the new P25 standard for the Conventional Fixed Station Interface, TIA-102.BAHA.

http://www.zetron.com/data/site/templates/zetrontemplate.asp?resolutionfile=templatespath|ZetronTemplate.asp&area_0=pages/menus/radiodispatchprod&area_1=pages/products/dispatch/sipbasedconsole

IX. VoIP Security Considerations

The security of a VoIP network can be described by four major requirements.

Authentication - The means to validate that the VoIP packets both originate from and are received by the intended users.

Integrity - The need for the IP packet content to remain unchanged during its transmission through the network. A slight change in the packet content may render the voice unintelligible when it is reconstructed at the receiving end.

Privacy - Any conversation transmitted over a public network is subject to interception by third party users. Having network privacy and/or encryption ensures that any intercepted packets cannot be understood by anyone other than the intended recipient. Methods and programs for decoding VoIP communications on a number of poorly configured systems are publicly available, but they tend to decode only unencrypted pulse code modulation (G.711) encoded voice¹⁷.

Availability - Users should be able to use their VoIP networks whenever necessary with little to no outages. Network outages can occur through natural means (flooding, lightning, etc) or man-made (denial of service [DoS] attacks or congested networks).

The first three requirements can be addressed by either shared-key or public-key encryption techniques. In shared-key encryption, a secret code (key) is known by both the sender and recipient. Knowledge of this unique key allows the sender to encrypt the message and the recipient to decrypt the message. Public-key encryption uses a pair of asymmetric keys (public key and private key) and digital signatures to increase the security of the VoIP messages. The asymmetric keys are used to encrypt/decrypt messages while digital signatures provide a way to authenticate users. For public-key cryptography, several defined protocols exist: Transport Layer Security (TLS), IPsec, and Secure Real-time Transport Protocol (SRTP). Public-key encryption methods are CPU-intensive and can introduce latency into a VoIP system. To reduce latency, if large data transmissions are expected, full public-key encryption can be first used to establish a shared secret. The shared secret has the properties of being less CPU-intensive to use than the full public key but at the expense of less security. The shared secret is only used for a small amount of time, usually one session.

¹⁷ See <http://www.enderunix.org/voipong/> or <http://vomit.xtdnet.nl/> for examples.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



To address the fourth requirement, the availability requirements of a VoIP service, the network administrator needs to protect both the VoIP audio device and the underlying IP network. Typical techniques include: disabling unused ports or services, using Host-based Intrusion Protection Systems (HIPS), segmenting the network into varying levels of priority or traffic type, and finally, policing the network traffic to ensure one VoIP device does not consume all the bandwidth.

ISSUES RELATING TO IMPLEMENTATION OR EXECUTION:

Contact ICTAP Chief Engineer Neil Hoff (619) 553-9402, nwhoff@spawar.navy.mil

STATE OF PRACTICE IN THE FIRST RESPONDER COMMUNITY:

See attachment.

INDUSTRY OR NATIONAL GUIDANCE/STANDARDS:

A number of open VoIP standards exist including H.323 and SIP. Proprietary standards also exist, such as Megaco.

CONTRIBUTORS

CONTRIBUTORS (in alphabetical order):

- Daniel Devasirvatham
- Jason Heger
- Brian Hobson
- Patrick Kempker
- Dan Law
- Ben Sharon
- Dick Tenney

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



GLOSSARY

BICC	Bearer Independent Call Control - a signaling protocol based on N-ISUP that is used to support narrowband ISDN service over a broadband backbone network without interfering with interfaces to the existing network and end-to-end services.
Checksum	A value used to ensure data are stored or transmitted without error. It is created by calculating the binary values in a block of data using some algorithm and storing the results with the data. When the data are retrieved from memory or received at the other end of a network, a new checksum is computed and matched against the existing checksum. A non-match indicates an error
Egress	In the telecommunications industry "egress" is often used as a term to identify traffic (typically IP) exiting a carrier backbone network across a communications link (such as DSL or Ethernet) and into the customer's network.
DiffServ	Differentiated Services - a method of trying to guarantee quality of service on large networks such as the Internet
Duplex	where a signal can flow in both directions between connected parties
Gateway	a computer or a network that allows or controls access to another computer or network
h.323	an umbrella recommendation from the ITU-T, that defines the protocols to provide audio-visual communication sessions on any packet network
Ingress	Data originating outside the local network that is transmitted to a station within the network
IP	Internet Protocol
IPv4	Internet Protocol version 4 – the most common version of IP at present that dates back to 1981, defined by the Internet Engineering Task Force (IETF) RFC 791, and in DoD MIL-STD-1777/1778. IPv4 uses 32-bit addresses (approximately 4 billion unique addresses), it does not guarantee delivery, and it does not support packet prioritization very well, known as Quality of Service (QoS)
IPv6	Internet Protocol version 6 – the next version of IP. Although not highly adopted at present, IPv6 support 128-bit addresses, which translates to 3.4×10^{28} or more than 50 billion x billion x billion addresses per person alive today. IPv6 also supports improved Quality of Service and simplified address allocation. The Federal Government and DoD mandated a transition to IPv6 for their network backbones in 2008.
Megaco	Media Gateway Controller - a signaling protocol, used between a <i>Media Gateway</i> and a <i>Media Gateway Controller</i> (also known as a Call Agent or a Soft Switch) in a VoIP network. It defines the necessary signaling mechanism to allow a Media Gateway Controller (Call agent) to control gateways in order to support voice/fax calls between PSTN-IP or IP-IP networks
MGCP	Media Gateway Control Protocol
MPLS	MultiProtocol Label Switching - a standard from the IETF for including routing information in the packets of an IP network. MPLS is used to ensure that all packets in a particular flow take the same route over a backbone. Deployed by many telcos and service providers, MPLS can deliver the quality of service (QoS) required to support realtime voice and video as well as service level agreements (SLAs) that guarantee bandwidth. Large enterprises may also use MPLS in their national networks
P25	APCO Project 25 - a suite of standards for digital radio communications for use by federal, state/province and local public safety agencies in North America to enable them to communicate with other agencies and mutual aid response teams in emergencies.
PBX	Private Branch eXchange - an inhouse telephone switching system that interconnects telephone extensions to each other as well as to the outside telephone network
POTS	Plain Old Telephone System or Service see PSTN

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



PSTN	Public Switched Telephone Network - the worldwide voice telephone network
QoS	Quality of Service – in networking, this refers to the ability to assign priorities to data packets, ensuring that critical real-time packets, such as VoIP voice packets, are prioritized over non-critical packets, such as email packets. IPv4 does not support QoS, but IPv6 does.
RTP	Realtime Transport Protocol - an IP protocol that supports realtime transmission of voice and video
RTCP	Realtime Control Protocol - a companion protocol to RTP that is used to maintain QoS
SIP	Session Initiation Protocol - An IP telephony signaling protocol developed by the IETF
SS7	Signaling System 7 - The protocol used in the public switched telephone system (the "intelligent network" or "advanced intelligent network") for setting up calls and providing services
TCP	Transmission Control Protocol - The reliable transport protocol within the TCP/IP protocol suite. TCP ensures that all data arrive accurately and 100% intact at the other end
UDP	User Datagram Protocol - A protocol within the TCP/IP protocol suite that is widely used for streaming audio and video, voice over IP (VoIP) and videoconferencing, because there is no time to retransmit erroneous or dropped packets
VoIP	Voice over Internet Protocol

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



REFERENCES

- http://www.safecomprogram.gov/NR/rdonlyres/65398E2E-C4EE-4779-BB91-600847499056/0/voip_technology_assessment.pdf - "Software-Enabled Wireless Interoperability Assessment Report – Voice-Over-Internet Protocol Technology", PSWN Program Report, December, 2001
- <http://www.fcc.gov/voip/> - FCC Website on VoIP
- http://www.officescreen.com/assets/resource_lib/voice_over_IP/Voice_Over_IP_101_Understanding_VoIP_Networks.pdf - White Paper - Voice over IP 101, Juniper Networks, August 2004
- http://en.wikipedia.org/wiki/Internet_Protocol - Wikipedia article on IP
- <http://en.wikipedia.org/wiki/VoIP> - Wikipedia article on VoIP
- http://en.wikipedia.org/wiki/Quality_of_service - Wikipedia article on QoS
- <http://insight.zdnet.co.uk/business/management/0,39020490,2133533,00.htm> – B. Posey, "IPv4 versus IPv6", TechRepublic, April 16, 2003
- <http://www.radvision.com/NR/rdonlyres/858A96AE-D027-40DD-AE7A-E7FBDD3E17DA/0/RADVISIONH323Revolution.pdf> - Radvision White Paper, "The H.323 Revolution", 2002
- http://mrtmag.com/mag/radio_making_sense_ip/ - J. Facella, "Making sense of IP for public safety", MRT Magazine, November, 2004
- http://mrtmag.com/mag/radio_efjohnson_debuts_voip/index.html - G. Bischoff, "EFJohnson debuts VoIP P25 trunking system—finally", MRT Magazine, June, 2005
- <http://electronics.howstuffworks.com/ip-telephony.htm/printable> - very basic guide to VoIP from howstuffworks.com
- http://mrtmag.com/mag/radio_managing_ip_migration/ - M. Polulak, "Managing the IP Migration", MRT Magazine, November, 2005
- <http://tools.ietf.org/html/3550> - IETF RFC 3550 defining RTP and RTCP.
- <http://www.packetizer.com/voip/h323> - Informational site on H.323 and VoIP
- http://www.packetizer.com/voip/papers/understanding_voip/ - Excellent VoIP Overview
- <http://searchvoip.techtarget.com> – "How does VoIP work? A technical guide to functional VoIP", May 28, 2006, registration required.
- http://mrtmag.com/mag/radio_efjohnson_debuts_voip/index.html - Article on EF Johnson, P25 VoIP System, July, 2005
- <http://www.cisco.com/warp/public/788/voip/delay-details.html> - Cisco web page on "Understanding Delay in Packet Voice Networks" with additional information on voice compression, sources of delay, and other useful topics.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



- <http://www.packetizer.com/voip/h248/history.html> - History of H.248 showing the relationship with MGCP
- http://www.cisco.com/application/pdf/en/us/guest/tech/tk701/c1482/ccmigration_09186a00800b3f21.pdf - diagram displaying how multiple VoIP protocols can be integrated and used together with PSTN networks
- <http://www.dvsinc.com/products/software.htm> - DVSII link on vocoders.
- http://www.cisco.com/warp/public/788/signalling/waveform_coding.html - informational Cisco web page on Waveform Coding Techniques.
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/qos.htm - Cisco QoS reference.
- http://www.zetron.com/data/site/templates/zetrontemplate.asp?area_0=pages/menus/radiodispatchprod&area_1=pages/products/dispatch/sipbasedconsole - Zetron's new VoIP console supporting SIP.
- <http://www.voip-info.org/wiki/> - useful website with information on VoIP.
- <http://www.voipplanet.com/> - useful website with information on VoIP.
- http://www.empower.com/pages/telecom_VoIP.htm - article on FCC mandate for commercial VoIP companies to channel E-911 calls to local emergency operators.
- http://mrtmag.com/mag/radio_roip_success_details/ - "RoIP success is in the details", by John Facella, MRT Magazine, December, 2004

ATTACHMENTS

Redacted ICTAP-specific examples

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



ICTAP VoIP EXAMPLES

Name of Site	VoIP System
Site 1	Motorola ASTRO 7.x Technology Site 1 has chosen a Motorola an ASTRO 25 700/800 MHz v7.1 multi-zone system that is currently being installed. The system's 10 sites provide coverage for four counties. Three sites are used for a 30-channel simulcast cell while two other sites are used for a 15-channel simulcast cell. The remaining 5 sites are IntelliRepeater sites which make up a multi-site network. The system also includes 22 console stations. One county is in the process of upgrading their Motorola SmartZone v4.1 system to a 700/800 MHz v7.1 multi-zone system. The county system was selected as Motorola's test site for their 7.x technology. Another county is also in the early procurement stage with the plans to move to an ASTRO 25 7.x system. Current initiatives include upgrading their microwave backbone to new digital technology in preparation for their new trunked system.
Site 2	M/A-COM NetworkFirst System After a field trial held in 2004, the Site 2 Police Department selected M/A-COM's NetworkFirst solution to address interoperability. The system currently includes 30 talk-paths and supports 29 agencies throughout the Urban Area including police, fire and EMS agencies. The system is also being expanded using an EDACS IP Gateway for improved functionality with Site 2's M/A-COM EDACS trunked system.
Site 3	Catalyst System Site 3 Metro 9-1-1 have implemented a Catalyst Communications interoperability solution that provides dispatch capabilities to over 50 remote sites in the region. The system is integrated with a M/A-COM EDACS system and includes 31 gateways for police and 18 gateways for fire. The Radio-over-IP (RoIP) system allows Site 3 Metro 9-11 to provide backup dispatch for the entire city and county should something happen to its primary dispatch center.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.



ICTAP VoIP EXAMPLES

Site 4

PSAP Integration

The Site 4 Regional Council is the metropolitan planning organization and association of local governments serving 114 cities and 8 counties.

In 2005, the Site 4 Regional Council solicited proposals for a Dynamic Multiple Agency Public Safety Interconnect Communication System. The system will support the interconnection of voice transmissions originating from different public safety radio systems. The System will connect all of the forty-nine (49) Public Safety Answering Points (215 dispatch positions total) via a closed T1 network that was recently installed.

Responses to the proposal were received from Motorola, M/A-COM, JPS Raytheon, RACOM (w/ Catalyst), SmartLink and ARINC (w/ Twisted Pair). All proposals included VoIP technology in their solutions from each of the respective vendors. Funding issues have led to some delays in the procurement process however the Site 4 Regional Council is intent on identifying the funding required to implement one of the proposed solutions.

Note: This is a redacted ICTAP technical note. No comment or remark in this paper should be construed as an endorsement of any vendor's product.