IN SHORT

TOWARD CRIMINAL JUSTICE SOLUTIONS

NIJ

www.ojp.usdoj.gov/nij | **MAY 07**

NCJ 217864

Voice over Internet Protocol

Key Points

- Voice over Internet Protocol (VoIP) is the digital transmission of voice communications through a data network based on Internet Protocol (IP).

- IP technology allows voice and data communications to share networks and thus increase efficiency, reliability, and cost savings.

- Standards have not been adopted for the use of VoIP by public safety agencies. As a result, data encoded by one vendor's device will likely not be decoded by another vendor's device.

- An emerging standard for public safety communications is called Project 25 (P25) InterSubSystem Interface (ISSI).

OVERVIEW

Internet Protocol is an open, standards-based set of rules that can route data around network failures and persistently transport data with minimal delay and loss of content.[1] IP also has mechanisms that can automatically discover the best route through a network with multiple paths.

Voice over Internet Protocol is a technology for encoding and routing digitized voice and data traffic over the Internet. Two VoIP categories are particularly relevant to public safety: VoIP telephony and VoIP within public safety communications systems.[2]

Through IP technology, voice communications are digitized and then segmented into standard digital data payloads (i.e., batches or collections of data) that are, in turn, encapsulated within IP packets so they can be transmitted via the IP transport network. This process allows voice and other information—such as video data—to coexist in a single

IP data network so it can be transmitted using shared equipment and communications lines. "IP gateway" is a term often used to describe the device that takes voice or video and encodes or decodes it into outgoing or incoming IP data.[3] A variety of VoIP-based products are available, including personal computers and specialized network appliances.

BENEFITS

The potential benefits of IP-based voice technology for public safety include:

- **Reduced communications costs.** Voice and data communications may be combined into a single, well-designed network.

- **Increased reliability.** A well-designed IP transport network can reroute data around congested network paths so communications integrity is maintained.

■ **Enhanced scalability.** IP protocols for routing data are scalable to support a large number of users.

■ **Interconnectivity.** IP-based radio interoperability equipment is often used to interconnect older or different private radio systems if traditional radio techniques cannot be used.

ISSUES TO CONSIDER

Most IP networks, including the Internet and many closed IP networks (such as intranets), will support VoIP traffic. The Internet, however, is relatively non-secure, unpredictable, and uncontrollable, and thus unsuitable for many public safety uses. Agencies need to evaluate their options before deploying VoIP as a solution for communications operations.

An IP network can transmit voice and image data efficiently, but there is also the potential for loss of clarity or delay in transmission. Agencies can implement a quality-of-service protocol to give voice data priority over other data, especially if the overall load of the network is unpredictable.

Although transmitting voice data via IP is common, the methods of encoding and signaling differ from vendor to vendor. Information encoded by one vendor likely will not be decipherable by another vendor's device or encoding software. Agencies should consider IP interoperability from multiple vendors and across multiple jurisdictions before making final decisions.

EMERGING PUBLIC SAFETY STANDARD

The Project 25 (P25) InterSubSystem Interface (ISSI), which is part of the P25 standards suite, is emerging as the most mature public safety IP standard. The ISSI has been partially approved within the Telecommunications Industry Association

and will allow for P25 trunked radio system inter-connectivity over a wide geographic area using IP-based technology.[4]

FOR MORE INFORMATION

■ NIJ's Communications Technologies (CommTech) Web site: www.ojp.usdoj.gov/nij/topics/commtech.

■ Regional National Law Enforcement and Corrections Technology Centers:

Northeast (Rome, NY) 888–338–0584

Southeast (Charleston, SC) 800–292–4385

Rocky Mountain (Denver, CO) 800–416–8086

Western (El Segundo, CA) 888–548–1618

Northwest (Anchorage, AK) 866–569–2969

Rural Law Enforcement Technology Center 866–787–2553

NOTES

1. Although persistent IP transport protocols for preventing loss and delay of data are available, VoIP applications typically do not exclusively employ these IP protocols for various reasons. Persistent mechanisms are used for control signaling and not usually for actual voice data.

2. For more information, see NIJ InShorts, *Telephony Implications of VoIP,* NCJ 212976, February 2006; and *Public Safety Communications and Interoperability,* NCJ 214331, May 2007.

3. An IP gateway in this context is not the same as the gateway described in NIJ InShort, *Interoperability Gateways/Interconnects,* NCJ 217105, March 2007.

4. The Telecommunications Industry Association is accredited by the American National Standards Institute. Learn more at www.tiaonline.org.

NCJ 217864