

Bridging Systems Interface: A Voice over Internet Protocol Specification for Public Safety

By Anna Paulson



Advances in telecommunications technology and the ever-increasing need for system interoperability have pushed the capabilities of traditional public safety communications networks. Traditionally, emergency-responder communications systems were comprised mainly of analog, two-way radios – known as land mobile radios (LMR) – that operated in the VHF or UHF regions of the radio spectrum. Today's public safety networks may need to integrate cellular phones and Internet Protocol (IP)-based voice and data systems with traditional LMR and dispatch systems from an increasing number of manufacturers. Safety agencies often rely on bridging solutions to communicate with other agencies and to link disparate communications technologies with conventional equipment.

Bridging solutions translate outgoing traffic from an endpoint device on one type of system (e.g., a handheld VHF radio) then pass the translated traffic to its intended recipient (e.g., a manager's IP telephone or to a radio connected to another system). The endpoints are either directly connected to the bridging solution or to a remote bridging device via another network. The connection between two bridging systems is more commonly known as a Bridging System Interface (BSI). Conventional bridging devices typically use an analog voice signal as the basis for interchange between LMR systems. The BSI addresses the connection between bridging devices and extends the range and capabilities of networks. Agencies are increasingly using Voice over Internet Protocol (VoIP) -based connections to transmit voice communications between bridging devices.

Although VoIP itself is standards based, there are many ways to implement VoIP between bridging devices; as a result, each implementation is essentially proprietary. Bridges and gateways that are based on digital VoIP technology must either connect to bridging systems from the same manufacturer or drop to a "lowest common denominator" connection. These types of connections negatively affect communications because they introduce latency problems and drop support of common features such as caller ID and encryption. Currently, there is no way to guarantee that one manufacturer's VoIP-based equipment will successfully

interface with another's. To address this problem, the Office for Interoperability and Compatibility (OIC) within the U.S. Department of Homeland Security (DHS) and the Office of Law Enforcement Standards (OLES) within the National Institute for Standards and Technology (NIST) led the creation of the Public Safety VoIP Working Group in 2006.

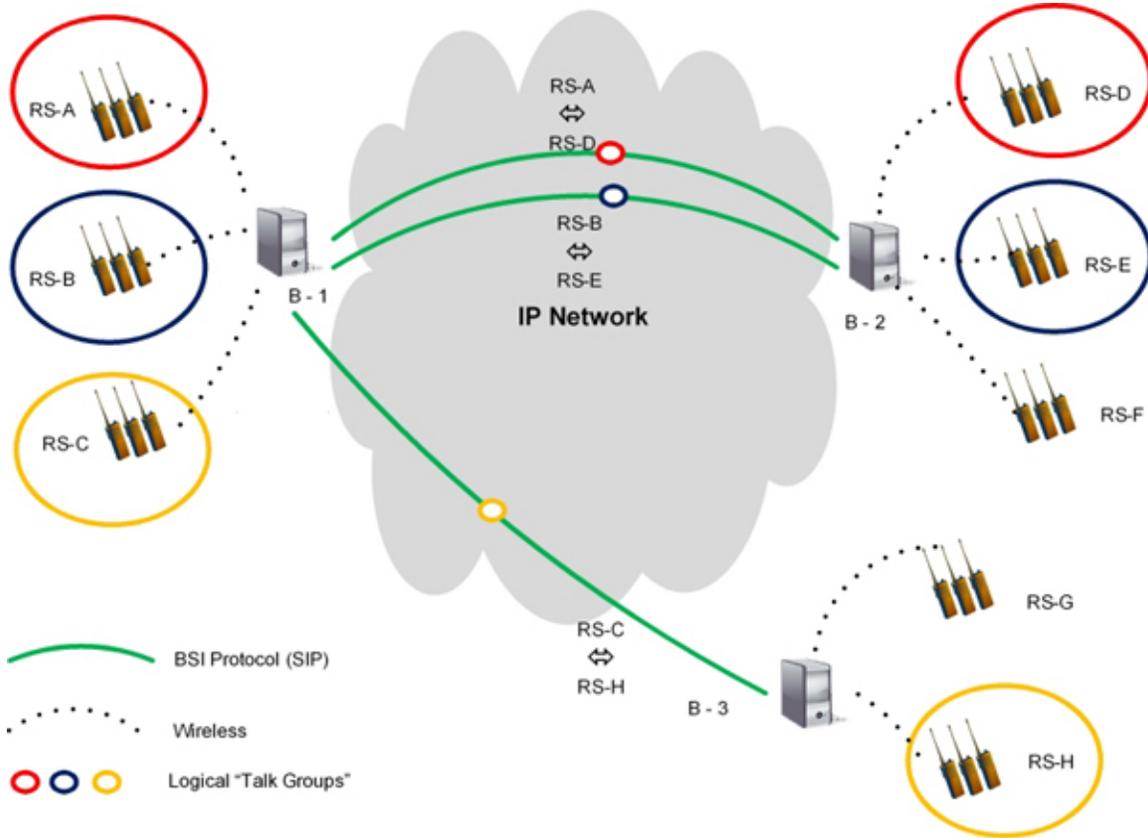
The Public Safety VoIP Working Group is a coalition of public safety officials and VoIP vendors brought together to create VoIP specifications, or implementation profiles, that will solve the interoperability problem using today's VoIP technologies. The group developed a BSI Core Profile, which would support group voice communications across multiple bridging solutions, support static or dynamic configuration and activation, meet temporal (access-time or latency) quality standards, and mitigate audio quality degradation issues due to improper codec selection or tandeming. Since its finalization in September 2008, over a dozen manufacturers have implemented the BSI Core Profile into their bridging devices. The Working Group is currently developing a BSI Enhanced Profile, which would extend the capabilities of bridging systems by allowing for transmission of priority information, permitting resource arbitration, implementing a control plane, and improving user-awareness of connected channels.

Development of the Public Safety VoIP Working Group BSI Core and Enhanced Profiles has increased the safety of the public and

emergency response community by extending the effectiveness and capabilities of their communications networks. Experience gained during the BSI Profiles development process will promote the rapid adoption of a compliance assessment program, test procedures for which are already under development. Compliance assessment is the guarantee to agencies that bridging devices operate as expected and advertised. BSI Profile-compliant products reduce the cost of system design and installation. Reduced upfront costs will increase an agency's buying power when deciding how to most effectively use the limited budgeted and grant dollars available for equipment purchases.

DHS, OIC, and NIST/OLES will partner with manufacturers to demonstrate the use of BSI as an interoperability specification between bridges at IWCE 2009. The demonstrations will be held in room N206 at the Las Vegas Convention Center and are currently scheduled for 1:00 p.m., 2:30 p.m., and 4:00 p.m. on Wednesday March 18; and at 11:30 a.m. and 1:00 p.m. on Thursday March 19. Currently, there are eight bridge manufacturers scheduled to participate in this demonstration.

Anna Paulson is an engineer with the Institute for Telecommunication Sciences in Boulder, Colorado. She is currently working developing test tools for the BSI that will help determine if an implementation is compliant to the specification.



A Sample Bridge Interconnection Scenario Using the BSI

NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.