Bridging Systems Interface Best Practices

Public Safety Voice over Internet Protocol Working Group
April 2010

Table of Contents

Executive Summary

As manufacturers increasingly implement Voice over Internet Protocol (VoIP) technology in their products, confusion continues to grow around the use of the technology in public safety communications. To address this problem, the U.S. Department of Homeland Security (DHS) and the U.S. Department of Commerce (DOC) formed a working group that includes key stakeholders from the public safety and industry communities. The Office for Interoperability and Compatibility (OIC) within DHS and the Public Safety Communications Research Program within DOC established the Public Safety VoIP Working Group to define and clarify the expectations for VoIP in the public safety environment. The group created VoIP specifications, also known as an implementation profile, which is a collection of existing standards, parameters, and values necessary for VoIP-based devices to connect with one another.

This document expands the VoIP implementation profile into a best-practices approach. Specifically, it provides practical operational and technical information for public safety responders who need to achieve voice interoperability between radio systems using bridge and gateway devices. As public safety entities invest in new communications technology around the country, there is an increasing need to "bridge" disparate legacy systems to achieve cost-effective interoperable communications during incidents that require multi-jurisdictional and multi-disciplinary response. This document provides best practices that focus on the bridge and gateway devices that connect to radio systems on one side, and have a VoIP interface to connect through Internet Protocol (IP) to bridge and gateway devices on the other side. This connection is based on Bridging Systems Interface (BSI) specifications, which allow VoIP-based devices to connect to one another.

Bridging systems with interfaces built with the guidance and specifications included in this document will allow emergency response agencies to seamlessly connect radio systems over an IP network, regardless of the device's manufacturer. The governance section includes operational best practices on governance planning, standard operating procedures (SOPs), service level agreements (SLAs), memoranda of understanding (MOUs), and a description of the system-of-systems approach. The technical section provides architectural and network specifications for simple and complex topologies; network engineering, management, and provisioning; naming and address conventions; bridging system robustness and redundancy; transcoding; interpreting Session Initiated Protocol (SIP) error codes; and essential configuration information. The endorsement and use of the material contained in this document by local,

regional, and state public safety responders will help promote best practices for the interconnection of local gateway resources. The inclusion of training, exercises, and testing involving the BSI will ensure that public safety responders are prepared to use a BSI when necessary.

Background

Problem Statement

As public safety entities invest in new communications technology around the country, there is an increasing need to cost effectively "bridge" disparate legacy systems to achieve interoperable communications during incidents that require multi-disciplinary and multi-jurisdictional response. For example, during the large-scale responses to Hurricanes Gustav, Ike, Katrina, and Rita, there were many problems with the gateway devices used to make these connections, resulting in limited communications among responders. Since then, there has been a proliferation of new gateway device technologies from a variety of vendors. Although manufacturers market these devices under different names, all provide the basic ability to connect two or more communication systems. With the development of this new technology comes the ability to connect Land Mobile Radio (LMR) systems to networks using Voice over Internet Protocol (VoIP). However, unless operators use these devices properly, the possibility exists that they could harm the networks' normal operations. As a result, it is necessary to develop a set of Bridging Systems Interface (BSI) Specifications that would allow VoIP-based devices to connect to one another. Bridging systems built to common specifications will facilitate the seamless connectivity of these radio systems over an Internet Protocol (IP) network, regardless of the device's manufacturer.

Scope and Purpose

This document intends to provide practical information about the network configurations where the BSI is applicable and to offer guidance for public safety responders who need to achieve voice interoperability between radio systems by using bridge and gateway devices. In particular, this document applies to bridge and gateway devices that connect to radio systems on one side and have a VoIP interface to connect via IP to other bridge and gateway devices on the other side.

In general, the radio systems being connected are legacy or proprietary systems. However, if a legacy or proprietary system requires voice interoperability with a Project 25 (P25) system, then the Inter-RF Subsystem Interface (ISSI) should connect the P25 systems together.[1] Additional information on P25 development and the ISSI is available through the P25 Interest Group: http://www.ptig.org.

[1] This document does not cover P25 systems.

The Public Safety VoIP Working Group

Confusion is growing around the use of the technology in public safety communications as manufacturers implement VoIP in their products. To address this problem, the U.S. Department of Homeland Security (DHS) and the U.S. Department of Commerce (DOC) formed a working group that includes key stakeholders from the public safety community and industry. The Office for Interoperability and Compatibility (OIC) within DHS and the Public Safety Communications Research Program within DOC established the Public Safety VoIP Working Group to define and clarify the expectations for VoIP in the public safety environment.

Rather than going through the lengthy process of creating new standards, this coalition of public safety practitioners, industry representatives, and Federal partners is creating VoIP specifications, also known as implementation profiles. A VoIP implementation profile is a collection of existing standards, parameters, and values necessary for VoIP-based devices to connect with one another. Bridging systems with interfaces built to these specifications will allow emergency response agencies to seamlessly connect radio systems over an IP network, regardless of the device's manufacturer.

An Overview of the BSI Core 1.1

The Working Group convened a planning meeting to determine which VoIP interface to address first. During this meeting, practitioners identified their requirements when connecting bridging systems. The Working Group asked practitioners, "If the Working Group disseminates a specification quickly, which of these requirements would be high priority, and which requirements would you be willing to wait for?" The public safety practitioners prioritized their list of options and, in cooperation with manufacturers, established a set of requirements for the BSI Core profile. The Working Group deferred the requirements on which public safety was willing to wait for potential inclusion in a future product referred to as the BSI Enhanced profile. The core requirements are necessary to get a basic interoperable voice connection up between two bridging devices. The enhanced requirements are additional features that public safety would find helpful to conduct their activities. Requirements for both the BSI Core and BSI Enhanced profiles are as follows:

BSI Core Requirements

- Basic voice connectivity between bridges from different manufacturers
    - Basic connection set-up and tear-down

    - Ability to accept or reject calls
    - Ability to gracefully exit in-progress connections
    - Common vocoder and means to negotiate optional vocoders
    - Common packaging of voice data (including dual-tone multi-frequency [DTMF] payloads)
    - Least possible negative impact on voice quality and delay/latency
- Naming and address capability and convention
- "Heartbeat" mechanism to verify the link is still alive in the absence of voice

BSI Enhanced Requirements

- Data and control information exchange capabilities[2]
    - Push-to-talk (PTT) collision indication
    - Call priority information
    - Confirmed and unconfirmed call information
    - Resource arbitration
    - Channel connection information
    - Network management and provisioning
- High-latency, low-bandwidth (e.g., satellite) connections capabilities
- Performance Requirements
- Security

[2] While the BSI Enhanced may support the exchange of data and control information, the bridging device and the communications systems to which it is connected will define any action taken on this information. For example, a bridge may be able to use call priority information to preempt an existing call, it may queue high-priority messages for delivery when the current message has completed transmission, or it may not have the capability to act on the information at all. Regardless of the approach, once this information is available for transmission, users will have to specify how they expect to use the information in the bridging devices they purchase.

Note that this document gives some of the BSI Enhanced requirements cursory attention. For the items highlighted in this document (e.g., Security and Performance Requirements), the assurance of these items is up to the user. For the requirements left unaddressed, the user should note that different manufacturers claiming compliance to the BSI Core and providing these features may have implemented the enhanced features in a manner that will not interoperate with other manufacturers' implementations of the same features.

More detailed information on the functionality required to meet the BSI Core requirements appears in Appendix D.

Governance

Overview

The Interoperability Continuum, shown in Figure 1, assists emergency response agencies and policy makers in planning and implementing interoperability solutions for data and voice communications. This tool identifies the five success elements that are critical to achieving an interoperability solution. These elements are as follows:

1. Governance
2. Standard Operating Procedures (SOPs)
3. Technology
4. Training and Exercises
5. Usage of Interoperable Communications

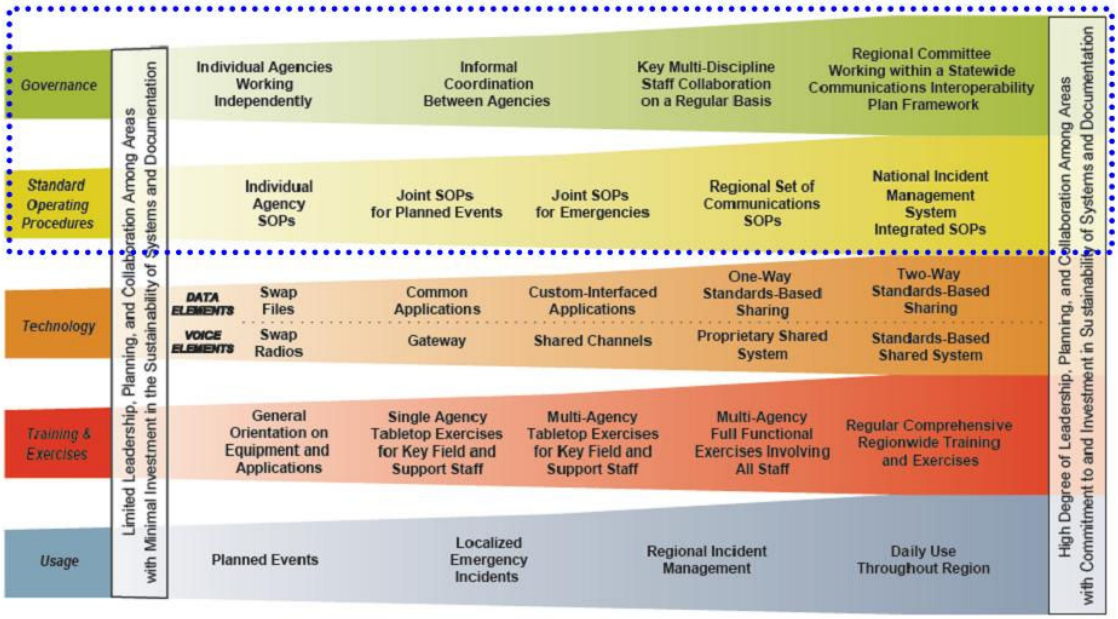

Figure 1 – Interoperability Continuum

While most of the work associated with the BSI Core 1.1 profile relates to the Technology lane of the Continuum, the Governance and SOP lanes are also very important. Emergency response agencies must establish governance structures and SOPs in advance to ensure channel publication and control. This section explains governance and SOPs as well as provides resources and tools to assist organizations with establishing governance and SOPs.

It is essential that all relevant governmental stakeholders participate in voice interoperability projects involving the BSI. The importance of the role this foundational element plays in achieving interoperability cannot be overstated because various levels of governments own and operate the disparate radio systems. Public safety practitioners recognize that interoperability is contingent upon coordinating diverse stakeholders from different disciplines and jurisdictions. When governmental stakeholders align, a support system of informed decision makers that understand the operational and technical requirements of the BSI exists, resulting in a comprehensive operating picture that embraces a greater range of technology.

In addition, public safety agencies must consider the differences in decision making among governments in rural and urban environments. The points of progression along the Governance lane of the Interoperability Continuum apply equally to rural and urban governmental entities. However, these agencies make decisions in a different manner and those differences come into play when discussing the BSI. For example, it may be easier to gain consensus within a rural governmental entity versus an urban one because rural governments may be less hierarchical which, in turn, can mean fewer approval steps in the decision making process. Conversely, urban areas may experience less economic impact, with regard to per capita costs, because their larger populations help diffuse the costs.

Governance Planning

Governance refers to establishing a shared vision and an effective organizational structure to support any project or initiative that seeks to solve interoperability issues. Establishing a common governance structure for solving interoperability issues will improve the policies, processes, and procedures of any major project by enhancing communication, coordination, and cooperation; establish guidelines and principles; and reduce any internal jurisdictional conflicts.

Governance structures provide the framework in which stakeholders can collaborate and make decisions that represent a common objective. The emergency response community realizes that a single entity cannot solve communications interoperability; rather, achieving interoperability requires a partnership among emergency response organizations across all levels of government. As such, a governing body should consist of local, tribal, state, regional, and Federal entities, as well as representatives from all pertinent emergency response disciplines within an identified region. Memoranda of Understanding (MOUs) are an important part of governance structures because they define the responsibilities of each party, highlight the scope and authority of the agreement, clarify terms, and outline compliance issues.

Figure 2 describes the points of progression along the Governance lane of the Continuum. Communities can use these as reference points for evaluating their current state of interoperability and gauging improvement over time.

- **Individual Agencies Working Independently**—A lack of coordination among responding organizations.
- **Informal Coordination Between Agencies**—Loose line level or agency level agreements that provide minimal incident interoperability.
- **Key Multi-Discipline Staff Collaboration on a Regular Basis**—A number of agencies and disciplines working together in a local area to promote interoperability.
- **Regional Committee Working within a Statewide Communications Interoperability Plan Framework**—Multi-disciplinary jurisdictions working together across a region pursuant of formal written agreements as defined within the larger scope of a state plan, thus promoting optimal interoperability.

Figure 2 – Points of Progression of the Governance lane of the Continuum

In the context of this document, governance planning identifies the people, planning, and process components that communities need to improve interoperability. Key stakeholders support strategic planning initiatives, which in turn generate operational processes. However, governance planning is a relatively static undertaking; it requires standard operating procedures, as described in the next section, to implement these core components.

For more information on governance and tools for creating governance structures and MOUs, please review the following documents:

1. *Establishing Governance to Achieve Statewide Communications Interoperability: A Guide for Statewide Communication Interoperability Plan (SCIP) Implementation,* U.S. Department of Homeland Security, http://www.safecomprogram.gov/NR/rdonlyres/24F10648-2642-42F3-8305-B29315F833BF/0/EstablishingGovernanceGuide.pdf

- This document presents information about the role, system, and operations of statewide governing bodies that are responsible for improving communications interoperability across a state.

2. *Writing Guide for a Memorandum of Understanding (MOU),* U.S. Department of Homeland Security, http://www.safecomprogram.gov/NR/rdonlyres/70169F1E-F2E9-4835-BCC4-31F9B4685C8C/0/MOU.pdf

- This tool provides guidance for developing an MOU. The document follows the recommended MOU structure with suggested headings for each section. Each section poses questions to consider when writing content for an MOU. Sample paragraphs are included for reference.

3. *Operational Guide for the Interoperability Continuum: Lessons Learned from RapidCom*, U.S. Department of Homeland Security, http://www.safecomprogram.gov/NR/rdonlyres/5189828C-8D5E-4F66-9B3E-CFF847660023/0/LessonLearnedFinal101305.pdf

- This report shares valuable information learned from the representatives of the emergency response community that participated in RapidCom. It also provides a framework for communities and regions to use in their interoperable communications planning efforts.

Standard Operating Procedures

SOPs are formal written guidelines or instructions for incident response. SOPs typically have operational and technical components, and in the event of an incident, they enable emergency responders to act in a coordinated fashion across disciplines. Clear and effective SOPs are essential in the development and deployment of any solution.

Creating SOPs that foster interoperable communications across an area or region is one of the more difficult elements to implement, as it relies heavily on the deployed technology and the current operational environment. However, this is one of the first areas that can benefit from immediate improvements without a large financial investment.

Figure 3 describes the points of progression along the SOP lane of the Continuum. Communities can use these as reference points for evaluating their current state of interoperability and gauging improvement over time.

- **Individual Agency SOPs**—SOPs exist only within individual agencies and are not shared, resulting in uncoordinated procedures and/or incompatible data systems among agencies that can hinder effective multi-agency and multi-discipline response.
- **Joint SOPs for Planned Events**—The development of SOPs for planned events—this typically represents the first phase as agencies begin to work together to develop interoperability.
- **Joint SOPs for Emergencies**—SOPs for emergency level response that are developed as agencies continue to promote interoperability.
- **Regional Set of Communications SOPs**—Region-wide communications SOPs for multi-agency/multi-discipline/multi-hazard responses serve as an integral step towards optimal interoperability.
- **National Incident Management System Integrated SOPs**—Regional SOPs are molded to conform to the elements of the National Incident Management System.

Figure 3 – Points of Progression for the SOP lane of the Continuum

For more information on SOPs and tools to create SOPs, please review the documents cited in the previous section and:

1. *Writing Guide for Standard Operating Procedures*, U.S. Department of Homeland Security, http://www.safecomprogram.gov/NR/rdonlyres/2D396F0E-CE19-4DCB-A30A-35982721F5AA/0/SOP.pdf

- The purpose of this document is to assist communities that want to establish formal written guidelines or instructions for incident response. Each section poses questions to consider when writing content for SOPs. Sample paragraphs are included for reference.

SOURCES

- *National Summary of Statewide Interoperability Communications Plans (SCIPs),* U.S. Department of Homeland Security, http://www.safecomprogram.gov/NR/rdonlyres/C6C0CD6A-0A15-4110-8BD4-B1D8545F0425/0/NationalSummaryofSCIPs_February2009.pdf

- *Interoperability Continuum Brochure*, U.S. Department of Homeland Security, http://www.safecomprogram.gov/SAFECOM/tools/continuum/default.htm

- *Operational Guide for the Interoperability Continuum*, U.S. Department of Homeland Security, http://www.safecomprogram.gov/NR/rdonlyres/5189828C-8D5E-4F66-9B3E-CFF847660023/0/LessonLearnedFinal101305.pdf

- *Writing Guide for a Memorandum of Understanding (MOU),* U.S. Department of Homeland Security, http://www.safecomprogram.gov/NR/rdonlyres/70169F1E-F2E9-4835-BCC4-31F9B4685C8C/0/MOU.pdf

- *Writing Guide for Standard Operating Procedures*, U.S. Department of Homeland Security, http://www.safecomprogram.gov/NR/rdonlyres/2D396F0E-CE19-4DCB-A30A-35982721F5AA/0/SOP.pdf

Service Level Agreements

Service Level Agreements (SLAs) are negotiated agreements between a customer (e.g., an agency or other public safety entity) and the company or other organization from which they are buying equipment and services. An SLA records a common understanding about the relationship and expectations of both parties in the agreement. Customers are encouraged to negotiate an SLA with their service providers when procuring services that provide an essential component of a critical communication system. In the case of an IP-based network that is part of a mission critical communication system, an SLA might contain agreements on the following areas:

- Definition of service(s)
- Performance objectives
    - Requirements may include throughput/committed information rate, transfer delay/latency, error ratio, delay variation/jitter, availability/uptime, packet loss ratio, mean time to repair, etc.
    - Sets of performance objectives are often bundled together to form a class of service. Sometimes arbitrary terms (e.g., Gold, Silver, and Bronze) define those classes; other terms are better defined, like the Quality of Service (QoS) classes in figures 3 and 4.
- Performance measurement methods
- Problem management/resolution process
- Responsibilities of each party
- Warranties/guaranties

- Recovery plans
- Termination of agreement

In some cases, e.g., when a local agency procures service or leases equipment from a state agency, one document may combine features of SLAs with MOUs to fully define the relationship and expectations between those entities.

Memoranda of Understanding

While similar to SLAs, MOUs are typically agreements between agencies or other public safety entities that describe methods of sharing or exchanging resources. While these documents can cover any type of resource or asset used by an agency, this particular topic focuses on communications equipment and procedures related to successfully implementing a BSI-based connection between communication systems. Examples of topics in a BSI-related MOU include:

- Definitions of the agencies and organizations involved
- Lists of any assets and resources to be exchanged or shared
- Duration of any asset exchange or sharing
- Means by which an organization may initiate an asset exchange or sharing
- Authority/escalation chain for incident management
- Responsibilities of each party
- Spectrum sharing agreements[3]
- Warranties/guaranties
- Recovery plans
- Termination of agreement

[3] Depending on the spectrum sharing needs, these agreements may be a requirement of the Federal Communications Commission (FCC). Note that an MOU cannot extend the terms or area of coverage of an FCC license, so any spectrum sharing must abide by the terms of the license.

In some cases, such as when a local agency procures service or leases equipment from a state agency, one document may combine the features of MOUs with SLAs to fully define the relationship and expectations between those entities. SOP documentation may also incorporate some features of MOUs (e.g., authority/escalation chain for incident management).

System-of-Systems Approach

For many years, the public safety community has used a system-of-systems approach to achieve interoperable communications. A system of systems exists when a group of independently operating systems—comprised of people, technology, and organizations—are connected, enabling emergency responders to effectively support day-to-day operations, planned events, or major incidents.

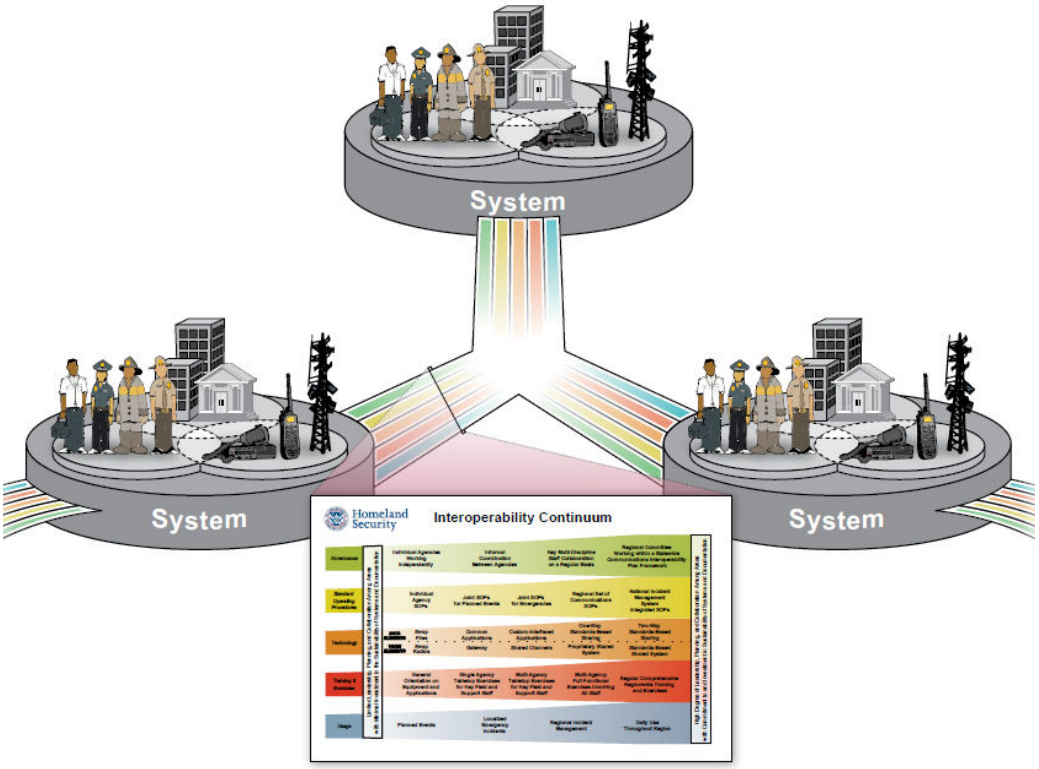

Figure 4 – System-of-Systems Approach

In Figure 4, independent systems are *inter*dependently related within and across all lanes of the Interoperability Continuum—including governance, SOPs, technology, training and exercises, and usage. Compatible technology between jurisdictions alone will not make an agency interoperable; the jurisdictions must connect technology, people, and organizations to achieve

interoperability. Strong relationships among the lanes are the foundation for the successful implementation of a system of systems.

A successful system of systems relies on the following fundamental concepts:

- Systems are composed of human, technological, and organizational components.
- Relationships among governance, technology, SOPs, training and exercises, and usage are addressed during a system-of-systems implementation.
- Systems are independently operated and managed and can connect with other systems without losing this independence.
- A system of systems expands beyond local geographical boundaries.

In the context of the BSI, implementing this standard fosters an approach to interoperability that will help ensure the effective and complimentary linkage among agencies moving to newer, more advanced technologies, and those agencies that maintain legacy technologies. The standard takes advantage of existing infrastructure, potentially saving substantial time and money. It allows users to continue to use systems that adequately meet their operational needs. Lastly, it brings with that implementation the opportunity to effectively achieve interoperability across disparate systems, and to reach out to multiple disciplines and levels of government while embracing system technology advancements for participant systems.

Other benefits of this approach allow for interoperability that reflects real differences in local geography, structural density, and other crucial variables. It minimizes the risk of a single point of failure that a single system might have; and allows for easier migration to newer technologies for agencies with unique needs or circumstances and the resources to do so. On the other hand, it allows for a slower, more manageable transition for agencies that do not need or lack the resources for a more rapid technology transition.

However, with all other lanes of the Continuum in place, there remains a technology requirement for the system-of-systems solution to be applicable in a mission-critical voice environment. To meet this technology requirement, one of the following must exist:

1) All infrastructure and subscriber units (mobiles/portables) must operate in the same radio frequency (RF) band, or

2) Subscriber units must be able to operate in one of the bands supported by the overlaying infrastructures and those infrastructures must all provide coverage throughout the area where interoperability is required, or

3) If overlaying infrastructures do not provide coverage throughout the area where interoperability is required, all subscriber units must be able to operate in at least one of the bands and using the communications mode (e.g., conventional or trunked and same protocols) of infrastructure that does provide such coverage throughout the area where interoperability is required, potentially requiring multi-mode, multi-band subscriber radios.

These three requirements assume there is capacity on the available networks to handle required interoperable voice traffic.

For more information on the system-of-systems approach, including case studies, please visit the DHS SAFECOM program Web site: www.safecomprogram.gov.

SOURCE

- *The Systems of Systems Approach for Interoperable Communication,* U.S. Department of Homeland Security, http://www.safecomprogram.gov/NR/rdonlyres/FD22B528-18B7-4CB1-AF49-F9626C608290/0/SOSApproachforInteroperableCommunications_02.pdf

Technical

Example Topologies

A BSI is a hardware and/or software platform that enables radio system or radio gateway interoperability. To see where BSIs fit into the overall system architecture, refer to the following architecture:

Radio System<-> BSI<-> BSI Protocol<-> BSI<-> Radio System

Note that this architecture is not indicative of every scenario for a BSI. Also, it is possible that the BSI and radio gateway are the same physical device. A device that enables interoperability with or between radios or other devices (e.g., phones and computers) is a BSI. Such a BSI is stand-alone in nature and functions on its own. When disparate radio gateways that enable Radio over IP connections need to be interoperable with each other, they must communicate with each other using a BSI.

The following section highlights some practical bridging system topologies and discusses practical considerations assuming that the governance and operating procedures issues discussed in the Publication and Control section of this document are resolved.

Using a variety of IP technologies, such as private IP networks, virtual private network (VPN) over public/private IP networks, or IP satellite links, may achieve the necessary interconnection links. The Network Engineering, Management and Provisioning section provides information on how to engineer the networks that support the BSI interconnections to help ensure the necessary voice quality.

Basic Pair-Wise Interconnection Scenario

Figure 5 shows the simplest topology where pair-wise interconnection is defined for several radio systems. In this example, the use of donor radios Radio System (RS) RS-A through RS-H achieves the connection. The green lines show the bridging interconnections that allow, for example, users on RS-A to communicate with users on RS-D despite possible incompatibilities of radio technology and differing radio bands. All BSI Core devices will support this basic pair-wise interconnection subject to the number of bridging ports.

Bridging Systems require separate BSI links to establish radio interoperability across multiple radio systems. Figure 5 shows two separate BSI links between B-1 and B-2 to enable

interoperability between RS-A and RS-D (in red) and separately between RS-B and RS-E (in blue). These BSI links are independent and do not imply that all four radio systems can communicate with each other.

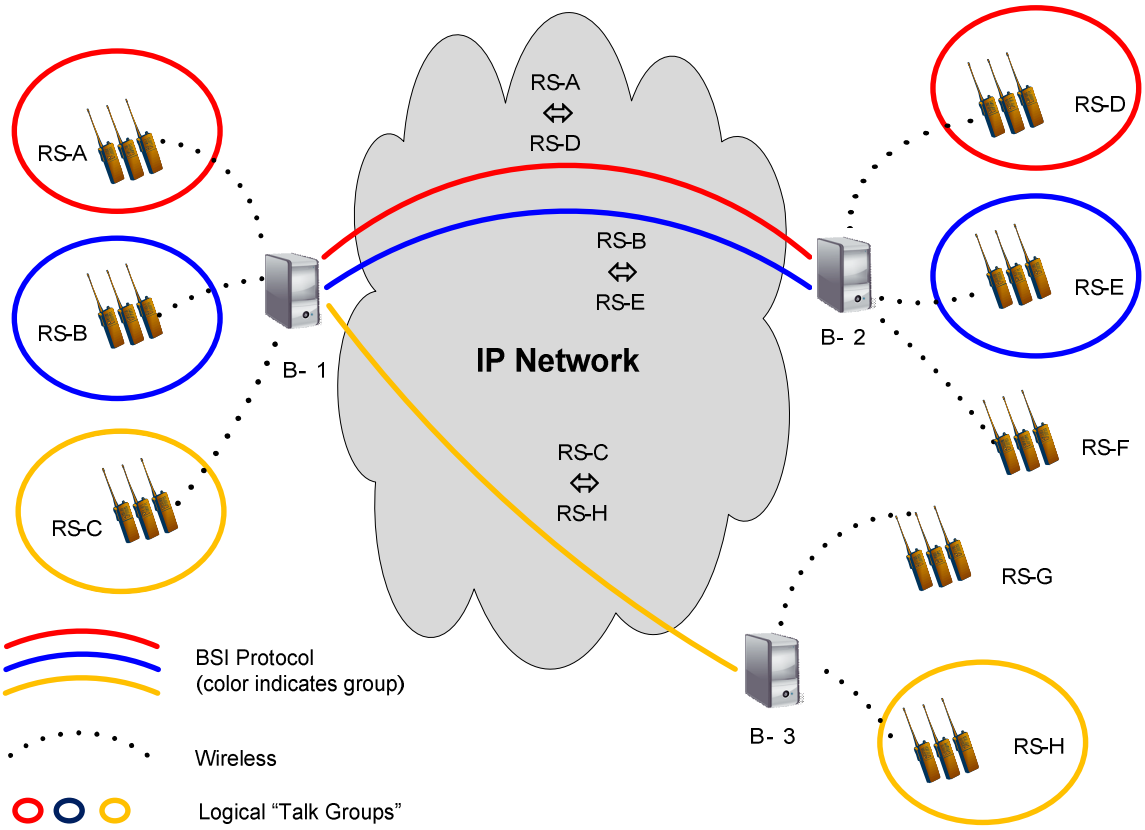

Figure 5 – Basic Pair-Wise Interconnect Topology for BSI

If the agencies require security, the interconnected agencies need to agree on mutually acceptable security means (e.g., VPNs) to protect the traffic over the BSI links as discussed in the Network Security section. Each agency is also responsible for issues relating to traversal of its firewalls as discussed in the Network Engineering, Management, and Provisioning section.

Complex Five-Bridge Scenario

Figure 6 shows a more complex topology where multiple radio systems are interconnected. This topology of five bridges and donor radios could satisfy the "Tanker Truck Rollover Scenario" presented in Appendix C.

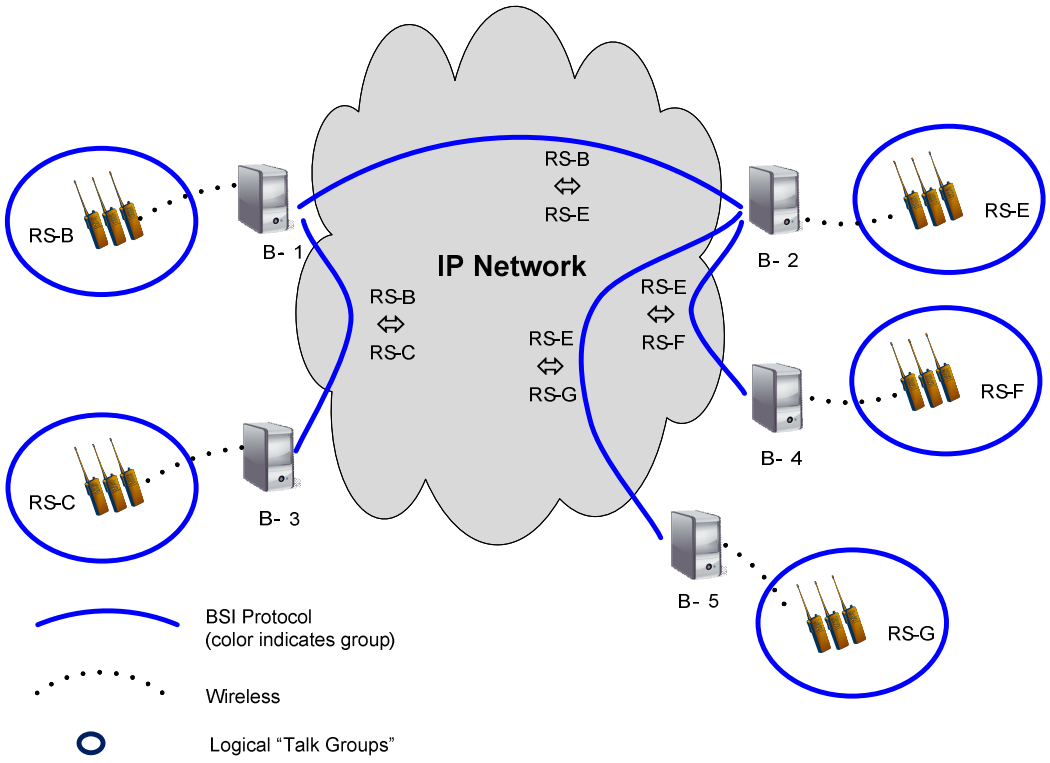

Figure 6 – Five-Bridge Interconnect Topology for BSI

Again, the green lines show the bridging interconnections that allow, for example, users on RS-B to communicate with users on RS-C, RS-E, RS-F and RS-G despite possible incompatibilities of radio technology and differing radio bands. This diagram also shows the need for bridges to repeat interconnections to other bridges in order to eliminate the need for a fully interconnected mesh of nodes (e.g., interconnecting all Bridging Systems with all other Bridging Systems directly). For example, the bridges on the left side of Figure 6 could belong to the agencies of one state and the bridges on the right side could belong to the agencies of an adjacent state.

The addition of multiple bridges also brings up the issue of the interconnection configuration varying over time. For example, in Figure 6 it is possible to establish the interconnection of RS-B and RS-C independently from the interconnection of RS-E, RS-F, and RS-G. After this initial deployment, the established RS-B to RS-E link will effectively interconnect the five radio systems.

Because forwarding traffic between multiple bridges is an optional feature of BSI Core, not all BSI Core bridges can function as bridges B-1 and B-2. If the purchasing agency requires traffic forwarding, the agency should verify the capability with the manufacturers before purchasing a bridge/gateway device. Appendix D shows a full list of required, recommended, and optional features.

Network Engineering, Management, and Provisioning

Traffic Levels/Bandwidth

The amount of bandwidth required for each VoIP connection into or out of a bridge/gateway device is dependent on the bit rate of the vocoder used for the voice and the number of packets per second that carry that voice across the network.

The Internet Engineering Task Force (IETF) publishes standards they call Requests for Comments (RFCs), IETF RFC 3714 notes that there are 40 bytes (i.e., 320 bits) of overhead for each Real-time Transport Protocol (RTP)/User Datagram Protocol (UDP)/IP packet of voice data. The vocoders mentioned in the BSI Core specification all use a 20 ms packet time, or 50 packets per second. This results in an overhead data rate of 320 bits x 50 packets = 16,000 bits per second (16 kbps). Below is information on required total bandwidth for specific vocoders:

- G.711 (64 kbps) requires 64 + 16 = 80 kbps
- GSM Full-Rate 6.10 (13 kbps) requires 13 + 16 = 29 kbps
- Improved Multiband Excitation (IMBE) (7.2 kbps) requires 7.2 + 16 = 23.2 kbps

In order to avoid packet loss and speech signal degradation, it is necessary to predict traffic levels in the network links so they can have enough capacity to avoid packet loss due to congestion. In most terrestrial networks, this typically involves over provisioning the network so that there is never congestion. In some networks, there may be other mechanisms available to help with congestion and traffic priority. These include Differentiated Services (DiffServ), Multi-Protocol Label Switching (MPLS), and Resource Reservation Protocol (RSVP). While the BSI core does not require the availability of any of these, DiffServ is recommended if it is available. A brief description of each of these mechanisms appears below.

DiffServ

DiffServ uses the concept of traffic classification to group traffic into a limited number of different Types of Service (ToS). The specific ToS helps routers make decisions regarding which packets should be forwarded as soon as possible and which can be dropped in the case of congestion. VoIP traffic is classified with the lowest latency and lowest drop rate service available. There are many standards which fully define DiffServ, but the basic definition is in IETF RFC 2474.

MPLS

MPLS supplies a connection-oriented service for transporting data across computer networks. It does this by using a label attached to each packet that quickly discerns where the packet should route. MPLS connections are typically provisioned from end-to-end at the beginning of a connection, and are often used to provision a VPN from end to end. Large "IP-Only" networks typically use MPLS, which may not be available to the end user for VoIP-specific connections, but may be usable for VPN-based connections. There are several standards that fully define MPLS, but the core standard is IETF RFC 3031.

RSVP

RSVP attempts to ensure there is sufficient bandwidth for a data flow by reserving those bandwidth resources through the network. Resources are reserved for each simplex flow of data from a source to a destination. This is most effective for continuous broadcast traffic. In the case of BSI connections where bidirectional communications is required, RSVP results in an over-reservation of resources because all connections must be fully reserved, even when there is no audio. Thus, use RSVP if it is the only mechanism available, but other mechanisms may be more efficient and more effective. There are many standards which fully define RSVP, but the basic definition is in IETF RFC 2205.

Technical Recommendations on Access Time and Latency

As public safety voice services increasingly leverage IP-based networks as a means to transmit information, carefully consider not only to the protocols used between those two (or more) points, but also the underlying network that will transport the information.

The International Telecommunication Union (ITU) and the IETF, among others, have been studying the performance of an underlying network for a number of years. During that time, they have drafted multiple standards that will be valuable to both the manufacturers deploying VoIP services and the emergency responders that will be using those services. The recommendations in this section provide guidance on judging the suitability of a network to transport BSI-based traffic. This section will not inform the reader on the proper design of networks; instead, it will serve as a guide when evaluating a network for its suitability to transport BSI-based traffic.

In particular, ITU's Telecommunication Standardization Sector (ITU-T) has two recommendations for deploying VoIP bridging systems in the public safety community: Y.1540 and Y.1541. The

IETF has developed more than a dozen RFCs around metrics that apply to the quality, performance, and reliability of Internet-based services.

Where the IETF seeks to design metrics that can provide an unbiased quantitative measure of performance for a network service, the ITU discusses where to measure these metrics and provides recommendations for the QoS given a particular type of service. For instance, the IETF has designed metrics that measure connectivity, one-way delay and loss, round-trip delay, loss patterns, packet reordering, bulk transport capacity, link bandwidth capacity, and packet duplication. These metrics and more are on the IP Performance Metrics Working Group page at http://www.ietf.org/html.charters/ippm-charter.html. Given the nature of PTT voice, the metrics that are of the highest value within the context of bridging systems are connectivity, one-way delay and loss, and delay variation.

ITU-T Y.1540 also defines parameters that can be used to specify and assess the performance of speed, accuracy, dependability, and availability of end-to-end IP services of a network (e.g., the when and where of measuring for QoS purposes). ITU-T Y.1541 takes the next step and provides recommendations for IP transfer delay, delay variation, loss ratio, and error ratio, given QoS class. Figure 7 is an image of Table 2 from Y.1541, which defines the six classes of services used in the standard. The figure also introduces a new acronym: Video Teleconference (VTC).

<table>
<tr><th>QoS class</th><th>Applications (examples)</th><th>Node mechanisms</th><th>Network techniques</th></tr>
<tr><td>0</td><td>Real-time, jitter sensitive, high interaction (VoIP, VTC)</td><td rowspan="2">Separate queue with preferential servicing, traffic grooming</td><td>Constrained routing and distance</td></tr>
<tr><td>1</td><td>Real-time, jitter sensitive, interactive (VoIP, VTC).</td><td>Less constrained routing and distances</td></tr>
<tr><td>2</td><td>Transaction data, highly interactive (Signalling)</td><td rowspan="2">Separate queue, drop priority</td><td>Constrained routing and distance</td></tr>
<tr><td>3</td><td>Transaction data, interactive</td><td>Less constrained routing and distances</td></tr>
<tr><td>4</td><td>Low loss only (short transactions, bulk data, video streaming)</td><td>Long queue, drop priority</td><td>Any route/path</td></tr>
<tr><td>5</td><td>Traditional applications of default IP networks</td><td>Separate queue (lowest priority)</td><td>Any route/path</td></tr>
<tr><td colspan="4">NOTE – Any example application listed in Table 2 could also be used in Class 5 with unspecified performance objectives, as long as the users are willing to accept the level of performance prevalent during their session.</td></tr>
</table>

Figure 7 – Table 2 from Recommendation Y.1541

There are six QoS classes defined in Y.1541 (0-5). For the context of bridging PTT voice systems, our recommendation is to use class 1 for applications that are real-time, jitter-sensitive, and interactive. Figure 8 is an image of Table 1 from Y.1541 that shows the network performance parameter value recommendations that are dependent on the QoS class selected. The figure also introduces the following new acronyms: IP Transfer Delay (IPTD), IP Delay Variation (IPDV), IP Loss Ratio (IPLR), and IP Error Ratio (IPER). It is important to note that in wired networks such as those used for deploying BSI-based bridging services, error and loss in many cases become negligible. This does not mean these aspects for QoS can be ignored, however, as the types of networks used by public safety are many and varied.

Based on the recommendation of QoS Class 1, the IPTD should be 400ms, the IPDV 50ms, the IPLR $1x10^{-3}$, and the IPER $1x10^{-4}$.

Visit http://www.itu.int/rec/T-REC-Y/e for more information on both standards.

Network performance parameter	Nature of network performance objective	QoS Classes					
		Class 0	**Class 1**	**Class 2**	**Class 3**	**Class 4**	**Class 5 Unspecified**
IPTD	Upper bound on the mean IPTD (Note 1)	100 ms	400 ms	100 ms	400 ms	1 s	U
IPDV	Upper bound on the $1 - 10^{-3}$ quantile of IPTD minus the minimum IPTD (Note 2)	50 ms (Note 3)	50 ms (Note 3)	U	U	U	U
IPLR	Upper bound on the packet loss probability	1×10^{-3} (Note 4)	1×10^{-3} (Note 4)	1×10^{-3}	1×10^{-3}	1×10^{-3}	U
IPER	Upper bound	1×10^{-4} (Note 5)					U

General Notes:

The objectives apply to public IP Networks. The objectives are believed to be achievable on common IP network implementations. The network providers' commitment to the user is to attempt to deliver packets in a way that achieves each of the applicable objectives. The vast majority of IP paths advertising conformance with ITU-T Rec. Y.1541 should meet those objectives. For some parameters, performance on shorter and/or less complex paths may be significantly better.

An evaluation interval of 1 minute is suggested for IPTD, IPDV, and IPLR and, in all cases, the interval must be recorded with the observed value. Any minute observed should meet these objectives.

Individual network providers may choose to offer performance commitments better than these objectives.

"U" means "unspecified" or "unbounded". When the performance relative to a particular parameter is identified as being "U" the ITU-T establishes no objective for this parameter and any default Y.1541 objective can be ignored. When the objective for a parameter is set to "U", performance with respect to that parameter may, at times, be arbitrarily poor.

NOTE 1 – Very long propagation times will prevent low end-to-end delay objectives from being met. In these and some other circumstances, the IPTD objectives in Classes 0 and 2 will not always be achievable. Every network provider will encounter these circumstances and the range of IPTD objectives in Table 1 provides achievable QoS classes as alternatives. The delay objectives of a class do not preclude a network provider from offering services with shorter delay commitments. According to the definition of IPTD in ITU-T Rec. Y.1540, packet insertion time is included in the IPTD objective. This Recommendation suggests a maximum packet information field of 1500 bytes for evaluating these objectives.

NOTE 2 – The definition of the IPDV objective (specified in ITU-T Rec. Y.1540) is the 2-point IP Packet Delay Variation. See ITU-T Rec. Y.1540 and Appendix II for more details on the nature of this objective. For planning purposes, the bound on the mean IPTD may be taken as an upper bound on the minimum IPTD and, therefore, the bound on the $1 - 10^{-3}$ quantile may be obtained by adding the mean IPTD and the IPDV value (e.g., 150 ms in Class 0).

NOTE 3 –This value is dependent on the capacity of inter-network links. Smaller variations are possible when all capacities are higher than primary rate (T1 or E1), or when competing packet information fields are smaller than 1500 bytes (see Appendix IV).

NOTE 4 – The Class 0 and 1 objectives for IPLR are partly based on studies showing that high quality voice applications and voice codecs will be essentially unaffected by a 10^{-3} IPLR.

NOTE 5 – This value ensures that packet loss is the dominant source of defects presented to upper layers, and is feasible with IP transport on ATM.

Figure 8 – Table 1 from Recommendation Y.1541

Security for BSI Connections

Communications security for public safety is becoming increasingly important. Ideally, communications undergo encryption from end-to-end. However, this is generally not possible when a bridging device is in use, because the donor radio decrypts the signal and provides it to the bridging device as an analog audio signal. It is important to understand the security implications of using a bridging device and also to understand what mitigation strategies might be useful in addressing those implications.

The BSI specification itself does not include or address any security issues. As indicated above, this does not imply that security is not important. In any bridged connection using a BSI, there are several facets of security that are links in a chain that add up to the whole security picture of the connection. *Overall communications security will be no better than the lowest level of security provided by any link in the interconnected system.*

Links in the chain of security include:

- Security of the traffic on each radio link connected to a BSI
- Physical security of the network and radio equipment
- Security of the IP traffic between BSIs and access controls to the bridging device

Figure 9 shows five different network configurations to demonstrate where these security links fit into the network configuration. Parts A, B, and C show consecutive additions of elements of IP network security, while parts D and E add in radio link security elements. These parts of the figure address the different aspects of security in the subsections below.

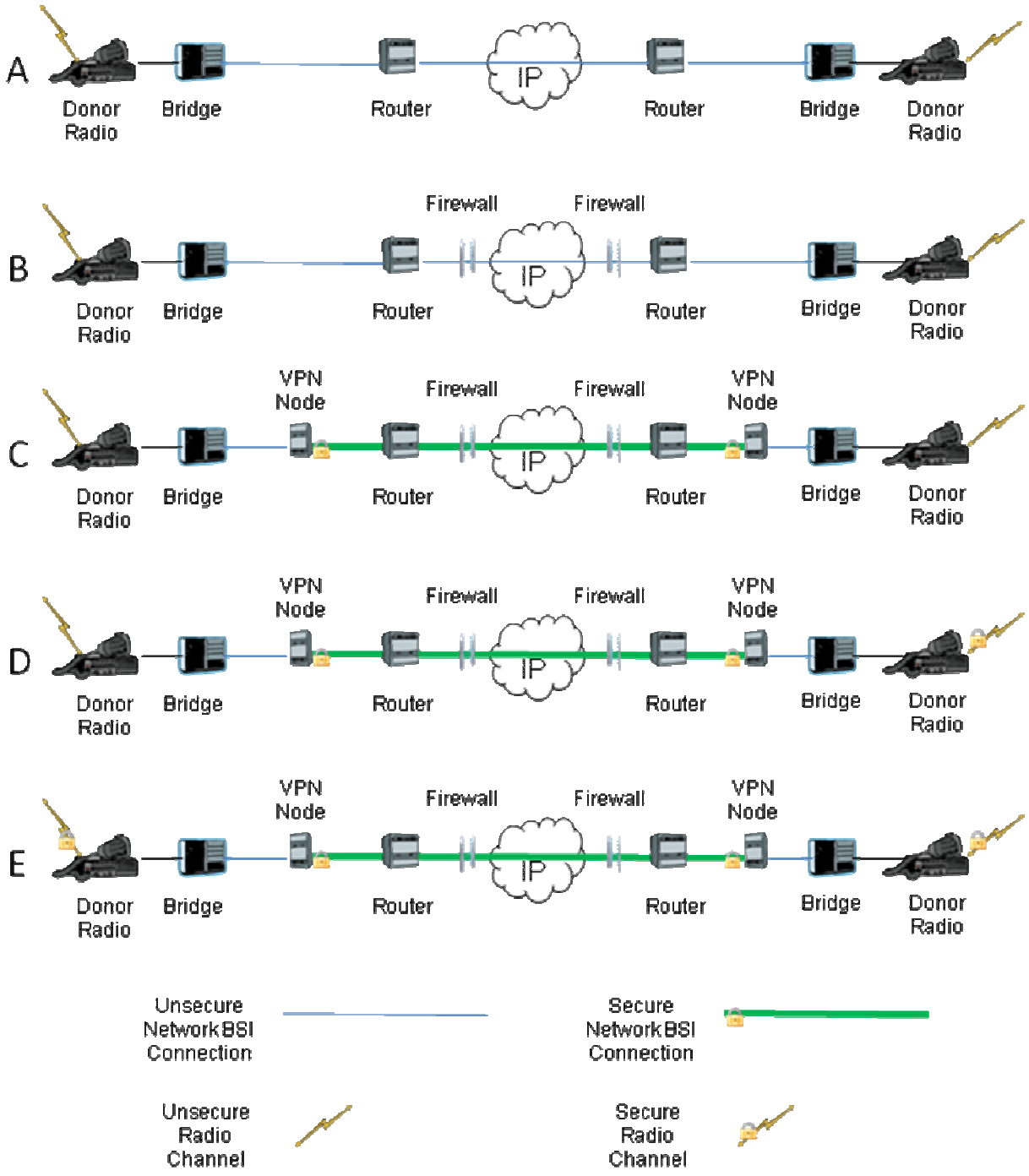

Figure 9 - Security elements for consideration when using the BSI

IP Traffic/Network Security

IP traffic security has many facets to consider. PR traffic security is employed at several places in the IP network. The two biggest categories of network device employed to help IP network are

security firewalls (Figure 9 Row B) and VPN nodes (Figure 9 Row C). Firewalls control access to and from devices on a network, and VPNs encrypt traffic traveling between two nodes connected to the network. Each of these devices are discussed below.

Firewalls

Firewalls restrict communications between devices on an IP-based network. They enable system and network administrators to ensure that only authorized traffic can pass from one side of the firewall to the other. Figure 9 Row B shows a firewall placed between the Internet and a local agency network to allow authorized and disallow unauthorized traffic. It is essential to configure firewalls to allow desired BSI traffic to pass through while blocking undesired traffic. Therefore, firewall configuration is a very important part of a BSI deployment.

Firewalls may be either standalone devices as indicated in Figure 9 Row B, or they may be incorporated into any other device in the network, such as the router or the BSI gateways themselves. In fact, it may be possible for there to be more than one firewall between a BSI gateway and the Internet. Properly configure each of these firewalls to allow BSI traffic through while blocking unwanted traffic.

Firewalls allow or block traffic based on a set of rules. These rules can be based on IP address, IP port, IP protocol, or combinations of address/port or address/protocol. Filtering based on IP address provides a means of defining what devices can access a network. Filtering based on IP port or IP protocol provides a means of defining what services or devices the remote device can access on a network. If possible, this best practices document recommends configuring firewalls on an address/port- or address/protocol-basis rather than IP address, IP protocol, or IP port alone. In the case where an IP address may change or is not be known, it is recommended that ports and protocols be used to restrict the types of traffic allowed to reach the BSI gateway.

Generally, firewalls are configured to, by default, deny both ingress and egress traffic. Beyond the default configuration, additional configurations may be necessary, based on the traffic the firewalls must allow through. In Figure 9 Row B, the configuration must pass regular BSI traffic, which includes SIP and RTP/RTCP. In Figure 9 Row C, the configuration must pass VPN-based traffic and as a result, will be dependent on the VPN implementation. Below is configuration information for allowing BSI traffic through a firewall and for allowing one common VPN through a firewall.

In order to allow plain BSI traffic through a firewall (Figure 9 Row B), consider the following:

- ***SIP***. Although port 5060 is the most commonly used SIP port, the actual ports(s) in use by each BSI gateway may be different. The firewall must allow TCP traffic, and allowing UDP for the same port is recommended. Also remember to include the SIP ports required for any SIP proxies or registrars in use.

- ***RTP/RTCP***. RTP ports have no standard range and are typically assigned dynamically during the SIP invitation and acceptance process. Each of the firewalls in the network path must allow the UDP port ranges in use by all of the BSI gateways through. In addition, make sure that the port range specified by each gateway includes the RTCP ports as well; a somewhat common problem in VoIP is to omit the last RTCP port (since this is just beyond the last RTP port), which causes all RTP connections to successfully operate except for those using the highest allowed RTP port.

In order to allow a firewall using IP-Secure (IPsec) and Internet Security Association and Key Management Protocol (ISAKMP) (Figure 9C), the firewall must allow the following ports and protocols through:

- ***GRE***. Allow General Routing Encapsulation (GRE) protocol (protocol 47) between the two VPN nodes.

- ***ESP***. Allow Encapsulating Security Payload (ESP) protocol (protocol 50) between the two VPN nodes.

- ***ISAKMP***. Allow ISAKMP (port 500) between the two VPN nodes.

- ***IPSEC***. Allow IPSEC (port 4500) between the two VPN nodes.

Specific firewall configurations may need to incorporate other scenarios such as Dynamic Host Configuration Protocol (DHCP) or Domain Name System (DNS); however, these are outside of the scope of this best practices document.

Having a firewall properly configured will generally require communication and negotiation with an agency's IT department.

VPN Nodes

Because the BSI does not require SIP and RTP layer security controls, the operator is strongly encouraged to only interconnect BSIs via secure IP networks. In some situations, one might be able to employ a physically secure Local Area Network (LAN)—such as a single cross-over

cable—to connect BSIs with restricted physical access. In most other situations, and particularly when connecting BSIs via a wireless network or the public Internet, it is advisable to protect the IP layer with a VPN.

Take care to implement a VPN that is appropriate to the environment. Two or more entities with plans to interconnect BSIs must agree to the selection and configuration of the particular VPN technology, and the features of the VPN must meet or exceed the security requirements of each entity. Although specific guidance regarding the VPN configuration is beyond the scope of this document, an example of two entities connecting BSIs over the Internet using IPsec Encapsulating Security Payload appears in the previous section.

VPN nodes come in a variety of shapes and forms ranging from software versions that run on a computer, to standalone devices, to nodes integrated in routers or other network devices. Figure 9 Row C shows the VPN node as a standalone device. VPN nodes also have several possible security protocol options and mechanisms that may require different network configurations when implemented. An example of a firewall configuration for one type of VPN appears above. Confirm with the VPN node provider on the specific protocols and ports that a VPN node requires to be open before opening ports on a firewall.

Most VPN nodes encrypt the IP traffic between nodes to allow privacy, and a password or key is required to be able to establish a secure connection between the devices. Using a VPN, therefore, requires exchanging some information between agencies before they can succeed at connecting to each other. It may be appropriate, therefore, to include in MOUs established with other agencies.

Although the BSI Core does not require BSI devices to support Network Address Translation (NAT) traversal, it may seem an easy choice to configure a tunnel mode VPN that traverses one or more NAT devices. The full understanding and cooperation of the VPN partner entity is necessary to accomplish this, and as a result, is generally inadvisable. A very common problem with such a configuration is the use of duplicate private (RFC 1918) IP address ranges by both entities. The typical solution to this problem is to employ NAT within the VPN tunnel, but this solution is not possible when connecting BSIs that do not support NAT traversal. The BSI Core requires only that BSIs be able to connect to other BSIs that have publicly routable IP addresses. A more-detailed discussion of NAT is included in Section Network Address Translation Traversal.

Physical Security

By nature of the bridging device, it is not possible to have encrypted communications from end-to-end. The signal must be unencrypted at some point to pass from the donor radio to the bridging device and from the bridging device to the VPN hub. It is integral to control the physical access to all network elements as much as possible, as it is during these unencrypted segments of the communication path that the communication is especially vulnerable to eavesdropping or spoofing. Therefore, take great care to ensure that physical access to the BSI gateway, the donor radio, and the VPN node is as restricted as possible. This may mean locking those components in a secure server room, in a locked rack in a communications van, or something similar. Regardless of the method used to ensure physical security, the inter-agency MOUs should record these requirements so that all parties can have some assurance that their communications are as secure and effective as possible.

Radio Link Security

As shown in Figure 9, it is possible to connect bridges to donor radios that are in-turn connected to secure or unsecure radio channels, talkgroups, etc. Each category of connection appears in the discussion below.

Connecting Unsecure Systems

In many (perhaps most) cases, a gateway will be used to connect unsecure/unencrypted radio channels, such as interoperability channels. Figures 9A, 9B, and 9C illustrate this situation. In these cases, encrypting the audio over the BSI link is a minor concern because the audio openly transmits. However, using firewalls and VPNs can reduce potential complicating factors such as message spoofing, so using these features is still recommended.

Connecting Secure Systems

People and agencies that communicate via secure and encrypted radio channels have high expectations that their communications will remain private to their group. Using a bridging device to connect two such channels (Figure 9E) should minimize the impact on the privacy of the communications. Part of the problem is that bridging devices make it impossible to allow complete end-to-end encryption of a voice signal. Typically, the signal must be unencrypted from the donor radio through the BSI gateway to the VPN node. In order to mitigate the security risks associated with this, those components transferring unencrypted voice should be physically secure to avoid unauthorized access. Further, even if the connections between the two groups

are fully secure, it is important to make users aware that tying the systems together has expanded their listening group. The ability to tie secure channels together and the procedures for announcing such a tie to the users of those secure channels should be included in an inter-agency MOU.

Connecting Secure Systems to Unsecure Systems

This particular configuration, demonstrated in Figure 9D, presents some of the most significant challenges related to security. On one hand, there is a group with a high expectation of privacy for their communications; on the other hand, there is a group with no expectation of privacy for their communications. It is very important that both groups be sensitive to the other group's needs. To support the group on the secure and encrypted side, employ every possible option to ensure privacy across the BSI communication path to the donor radio of the unsecured system. Make announcements on both sides to indicate the type of established connection. An inter-agency MOU should cover the parameters that allow connections like this to be established and procedures for announcing the connection.

High-Latency Low-Bandwidth Satellite Connections

Very Small Aperture Terminals (VSATs) enable satellite communications in a mobile environment like that of the public safety environment. VSATs are small satellite antennas with the reflector dish varying in size from 0.75 m to 3 m. The small size of the reflectors enables them to be successfully mounted on mobile command centers and Emergency Operation Centers. Depending on an agency's needs, the antennas are available in both an auto-deploying and a fixed format.

The terminal communicates with a satellite through a modem. There are many different modem technologies used with VSAT antennas to route data traffic across satellite networks. These modems may provide anywhere from 32kbs to 100mbs throughput depending on configuration and bandwidth allocation.

Working Group members have tested BSI links successfully across several VSAT satellite networks. Consider the key factors of latency configuration and capacity of the VSAT network when using the BSI or any VoIP standard across satellite links.

1. Latency: Most communications satellites are located in the Geostationary Orbit (GSO) at an altitude of approximately 35,786 km above the equator. At this height, the satellites go around

the Earth in a west-to-east direction at the same angular speed of the Earth's rotation; therefore, to an observer on the ground they appear fixed in the sky. The path distance from the location of the satellite terminal on Earth to the satellite in GSO introduces high latency. This latency can range from 240ms to over 300ms. When combined with satellite routing delays, typical satellite round trip latency will average around 640ms. It is important to consider that the radio interface should utilize techniques to buffer audio, where appropriate, to assist in minimizing broken or lost words across high latency connections. Adjusting voice buffers to maximize performance when using high latency connections can help minimize this. There may also be a human factor in allowing extra "key time" to ensure no communications are missed or lost.

2. Configuration: Within the Internet, most radio networks (e.g., WiFi splotches) are at the fringe of the network providing connectivity to end systems. Within the emergency services community, wireless communications provide connections between routers (e.g., between a command vehicle and an agency network) in what is known as a Wireless Wide Area Network (WWAN). Because this connection is such an integral part of the communications system, give care to the types of configuration selected for use. Two common configurations appear in the VSAT networks: hub and spoke, and mesh.

- **Hub and Spoke:** Typical VSAT networks operate in a Hub and Spoke type of configuration. This type of configuration means that all traffic transmits between the hub and remote. Additional round trip latency may result if two separate satellite remotes operate a BSI link. This is called a "double hop" as the packet must route through the hub before routing back across the satellite to the second terminal. For these types of connections, roundtrip latency will typically last longer than one second. It is even more important to allow for additional buffering or "key time" when forced to operate in this mode. Configure VPNs to deal with the added latency without timing out.

- **Mesh:** There are some satellite networks that allow for mesh or direct remote-to-remote communications. This mesh network allows for typical latency of less than 640ms as the packet can route at the satellite level directly to the other remote instead of routing to the hub first. This would only be one hop. There are important considerations in this type of configuration to keep traffic from overwhelming the network, such as multicast traffic and precursory discussions with the network operator.

3. Capacity: Radio networks have significantly less capacity than wired networks. For example, terrestrial Internet backbones routinely provision at OC192 (10.6Gbps) today and in-platform

LANs routinely provision at 1 or 10 gigabits. But typically, WWANs, particularly those utilizing satellite connections, can reach a maximum of 100 Mbps. Due to the high cost of satellite communications, speeds are more typically 1 Mbit/sec or less. BSI does allow the use of low bandwidth coder-decoders (CODECs) where supported by the manufacturer. Using low bandwidth CODECs is recommended when utilizing low capacity connections. When supported, they allow for more effective use of bandwidth and the operation of additional simultaneous connections. However, the lower-bandwidth CODECs do not transfer information losslessly. In a situation that uses BSI with digital radio systems, the additional decrease in quality from the lower-bandwidth BSI CODEC may adversely affect the end-to-end voice quality.

This impacts the available bandwidth because satellite communications utilize a shared media. Terrestrial Internet uses largely point-to-point physical technologies (e.g., fiber optic cable). Radio networks, both Wireless Local Area Networks (WLANs) and WWANs, use shared media — the ether. This is most obvious in the case of broad-beam geosynchronous satellites which shine on a third of the Earth's surface. Users should consider establishing SLAs with their providers and confirming that their minimum configurations of QoS and Committed Information Rate support real-time applications such as SIP. This will ensure that the BSI will function correctly over this type of network.

Finally, the limited bandwidth of some VSAT connections may not allow for transmission of more than one voice channel at a time. The provider should address this issue in the SLA.

Network Address Translation Traversal

A NAT deploys, either by itself or in conjunction with a firewall, where an enterprise or private network attaches to the Internet. A NAT performs an Open System Interconnection layer-3 translation of IP addresses so that few public Internet addresses can be mapped to multiple private IP addresses (see RFC 1918 for more information about private IPv4 addresses). This mapping mechanism works well for typical Web applications but can break VoIP applications.

The IETF is currently leading several initiatives to define standard NAT traversal mechanisms; however, these efforts have not yet yielded an accepted standard. Thus, the BSI Core profile does not mandate bridges implement any specific NAT traversal mechanism.

Users of BSI Core bridges are responsible for either deploying their bridges where there is no NAT traversal (such as directly on the Internet or in a Data Management Zone [DMZ] using a public IP address or on a shared VPN) or for buying bridges supporting the specific traversal

mechanisms used by their NATs. Users should be aware of the security implications of attaching bridges directly to the Internet or in a DMZ.

NAT Technical Background

With the growth of the Internet in the 1990s and 2000s, the number of available public IPv4 addresses has rapidly been shrinking. To combat this, Internet Service Providers and Network Administrators have been deploying network devices called NATs. NATs perform a layer-3 translation of IP addresses, so that public Internet addresses map to private IP addresses (RFC 1918). This mapping allows customers to map a large number of private addresses to a limited number of public addresses, thus limiting the number of public addresses required by both Internet Service Providers and Enterprise customers.

What Problems Do NATs Cause On The Internet?

While NAT devices do provide some relief from the ever-growing shortage of public IPv4 addresses, they also introduce certain types of problems on the Internet. These problems can be lumped into several categories, as documented in RFC 2993:

- Works well for Client Server applications with several client and few servers (i.e., WWW), but not for Peer-to-Peer applications
- Breaks the end-to-end connectivity model that the Internet is based on since NATs act as both a network element and an end-point element
- Breaks the end-to-end security model the Internet is based on since NATs intercept and re-write portions of every packet
- Breaks the redundancy model that the Internet is based on since NATs are stateful and single-points-of-failure
- Requires application developers to be aware of NATs in the network and modify their applications accordingly; this slows the deployment and complexity of new applications

While NATs have helped popularize the Internet by giving more users connectivity, it does not come without a price and some challenges.

What Problems Do NATs Cause With VoIP?

As mentioned, NATs work well for Client Server applications, but they break for Peer-to-Peer applications. By definition, VoIP is a Peer-to-Peer application because each end-point can act as either a sender (Client) or receiver (Server) of any call depending on who is originating or terminating the call.

VoIP also has several other characteristics that make it difficult to work in the presence of NAT devices:

- VoIP signaling protocols have IP addresses embedded in the payload (e.g., the Session Description Protocol [SDP]).
- VoIP separates the signaling plane from the bearer plane (RTP, Real Time Transport Control Protocol [RTCP]). This means that two types of traffic will need to be routable.
- VoIP uses dynamic addressing ports for both signaling and media. This makes "well-known" translations on NAT devices almost impossible.

The results of these challenges are that many network topologies and deployment models face the risk that VoIP cannot be a deployable service.

Recommendations for Implementers

Avoid using NAT if possible:

- If deploying only on or across one or more private networks, obtain sufficient IP addresses for all those nodes expected to be on the network(s). Securing these IP addresses is an essential part of the pre-deployment planning that should take place between the jurisdiction(s) involved and should be included in the SLAs between those jurisdictions.

- If a public network must be included, use VPNs to traverse the public network if possible.

If NAT is unavoidable:

- For planned situations, engage the IT departments of all the entities involved to resolve NAT-related issues prior to deployment.

- For ad-hoc situations, NAT translation may cause BSI implementations to fail. Agencies should maintain visibility into this issue through their IT departments.

Ongoing Technical Activities Related to NAT

Within the IETF, the keywords STUN (Simple Traversal of UDP through NATs) RFC 5389, TURN (Traversal Using Relay NAT), and ICE (Interactive Connectivity Establishment) refer to the major NAT traversal activities. Universal Plug and Play (UPnP) also provides a popular way to allow an application to control a NAT by means of the Internet Gateway Device protocol.

View a short overview of the VoIP and NAT issues at:
http://www.youtube.com/watch?v=9MWYw0fltr0

Loop Prevention

While the BSI Core does not specifically discuss functions of management over a BSI link, it does include mechanisms to detect and warn of protocol looping topologies. However, it cannot detect all possible audio feedback loops and the operator must review their bridging configuration carefully. In particular, the BSI cannot detect audio feedback loops introduced when multiple bridges exist between the same radio channels or talk groups.

Plan loop prevention on several layers, including the network, the application, and the radio resources connected on each bridging system. It is important to prevent loops on all levels before connecting bridging systems using the BSI Core profile. While this section provides ideas on how to prevent loops, it is important to remember that loops may still occur. Be prepared to unplug or disconnect equipment should a loop occur.

Network

While the BSI Core profile does not specify the exact network conditions that must exist for the BSI to operate correctly, it is important to consider loop prevention when determining the appropriate network transport between two or more bridging systems.

By default, most networks including the public Internet or a simple hub or switch between bridging systems should prevent loops. Even so, it is important to properly configure the applications running on either side of this network connection for loop prevention.

First and foremost, the network between the bridging systems must be loop free. This document will not detail how to prevent network loops as that lies outside the scope of the BSI Core profile.

The VoIP Working Group suggests working with network administrators to ensure a loop-free network connection exists to the other bridging systems.

Application

This section refers to the software and/or hardware that collectively make up the bridging system that will use the BSI profile to connect to another bridging system. By using the BSI profile to connect with other bridging systems, the application may inadvertently create loops within the bridging system or, possibly, on the remote bridging system. This can happen if more than one SIP call (BSI link) links to the same SIP Uniform Resource Identifier (URI) within the bridging system. Figure 10 shows a set of bridges that have a BSI protocol loop that could create an audio feedback loop. Implementations of the BSI 1.1 protocol will detect this protocol loop and alert the operator. To break the loop, disconnect the link between Bridging System 2 (B-2) and Bridging System 3 (B-3).

While the BSI profile allows for multiple SIP calls to remain active through the same resource within a bridging system, take caution when determining which resources to use to connect into specific resources on the bridging system. Allowing multiple inbound SIP calls to the same resource could potentially create a loop if the bridge or another bridge is unable to keep track of inbound audio and ultimately sends it out to all connected bridges.

If the bridging system application is capable of creating bridges between radios without connecting to other bridge systems, take care not to create loops through these patches. If a separate bridging system wants to connect to the bridging system using the BSI profile, establish unique SIP calls (BSI links) between resources on these separate bridging systems to prevent any possible loops.

Using unique BSI links and patching radio resources locally within the bridging system may still create loops. There is no foolproof way to prevent these loops, so if a loop is created during operation of the bridging system, simply undo (back out) the last change that was made to cause the loop. If this does not prove successful, disconnect the bridging system from the network to break the BSI link. Typically, these loops will appear in ad-hoc environments where changes occur on the fly. In pre-determined environments where communications are well coordinated and planned out, loops should not occur.

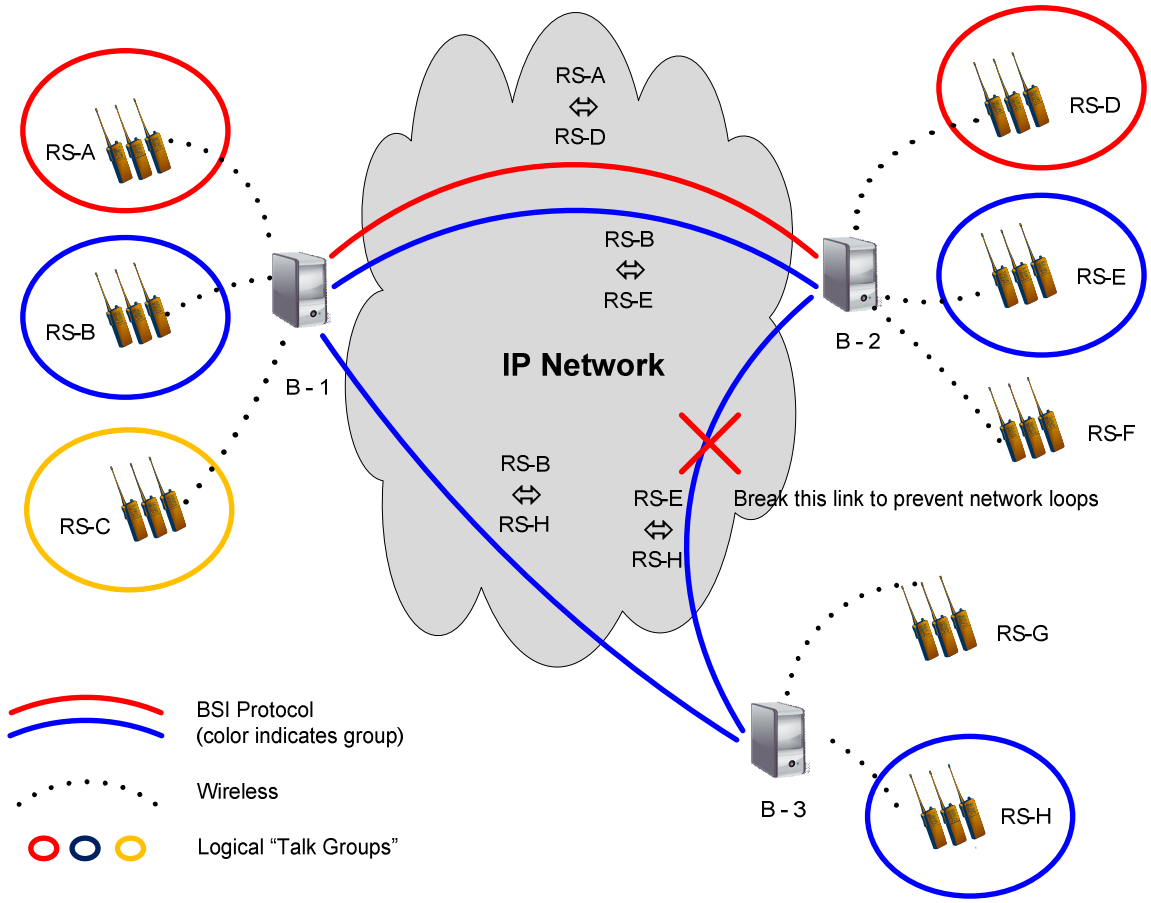

Figure 10 – Improper BSI Protocol Loop Topology

Radio

While radios themselves should not create loops for the BSI profile, the connections between bridging systems will tie together resources that cannot be seen by the bridging system operator. Multiple donor radios connecting to the same system, channel, talk group, or incorrectly configured donor radios could create such a situation. Bridging to mutual aid channels is especially vulnerable to this type of looping. Introducing the loop outside the BSI protocol configuration will result in a lack of detection. Figure 11 shows an example of such a misconfiguration. To break the loop, disconnect link between Bridging System 3 (B-3) and Radio System G (RS-G).

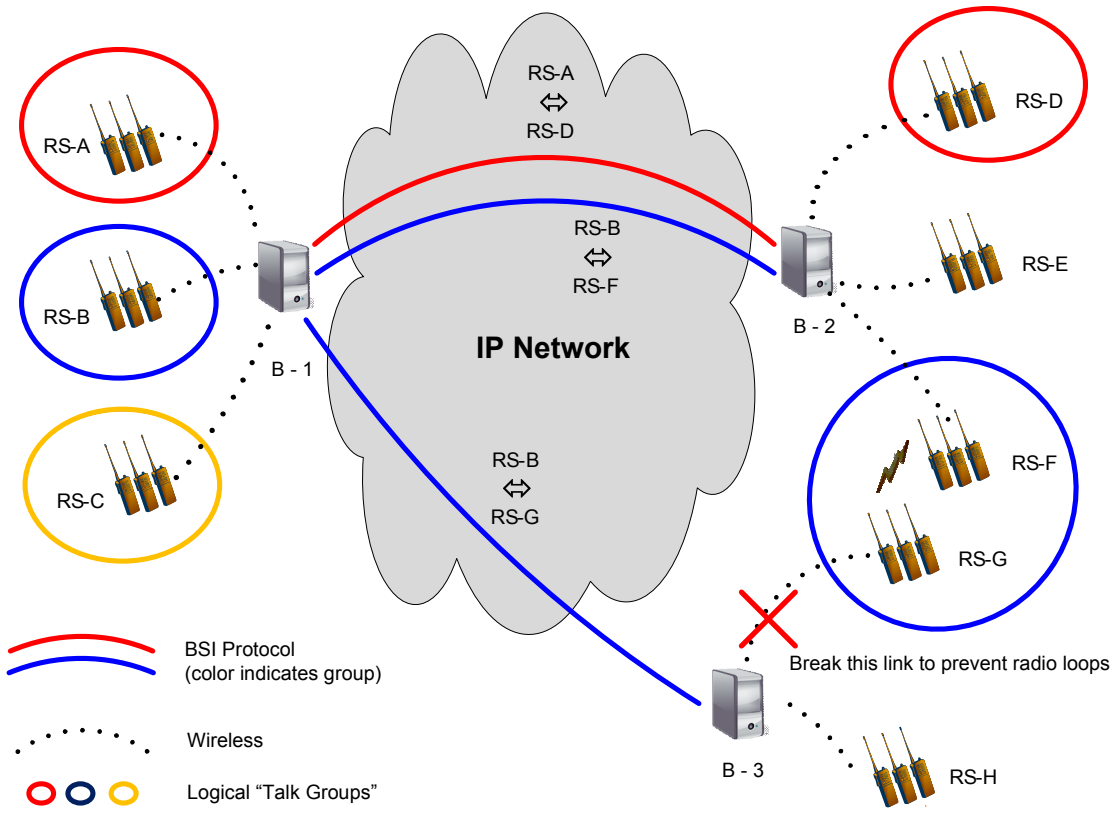

Figure 11 – Illegal Radio Loop Topology

In an emergency situation, establishing a mutual aid channel among fire, police, and ambulance services will often ease the communication problems among these agencies. In addition, the fire, police, and ambulance services may use their own bridging system during the emergency to allow for radio patching as well as telephone connectivity.

If two of these agencies attempt to use the BSI link to patch these radio resources together between the bridging systems, an infinite loop will ensue. Radio traffic destined from bridge A to bridge B will travel out through the connected radio system of bridge B and return through bridge A. Since bridge A will see this as new audio, it will immediately transfer it to bridge B, and so the loop continues.

While this mutual aid scenario is plausible, it also demonstrates how radio loops bridged through the BSI and of any common frequency may cause endless loops.

To sum up the loop prevention best practices section—while many loops can be prevented ahead of time using the these guidelines, it is possible that loops will present themselves during normal

operation when using the BSI profile. Be alert and prepared to disconnect BSI links while sorting out the loops.

Naming and Address Conventions

Addressing

An IP address is a numerical identification assigned to specific pieces of equipment utilizing the Transmission Control Protocol (TCP)/ IP network. The IP address assigned to the bridging system should be consistent with agency network policies and provide a means for interconnection with other bridging systems. In other words, even if a bridging system is installed on a private network using non-routable IP addresses, a mechanism should be configured (e.g., possess VPN access or port forwarding capabilities) to enable remote bridging systems to connect through the TCP/IP network. See the Network Security and Network Address Translation sections and consult with the network engineer for configuration information.

The BSI bridges should be on an IPv4-compatible network. The BSI profile does not require IPv6 nor does it define operations of an IPv6 SIP/SDP stack. Use of IPv6 is beyond the BSI Core profile.

RFC 4294 specifies the general requirements for implementing IPv6 on a network host; **RFC 4213** specifies the transition mechanisms for IPv6 Hosts and Routers. IPv6-based BSI systems should be backward compatible to IPv4 during and after the IPv6 transition and establishment of a common interoperability strategy for the co-existence of two versions of IP (also called dual stack).[4]

Naming Conventions

BSI bridges identify bridged resources using SIP URIs (see **RFC 2396** for complete technical information). Since bridges are not required to support the complete RFC 2396 syntax, the SIP URIs should be limited to the following format:

sip:<Resource_Name>@<Jurisdiction_Domain_Name>:Port

<Resource_Name> = The unique resource name within a jurisdiction that a device bridges to.

[4] For more information about IPv6 adoption within the U.S. Government, please visit http://www.cio.gov/index.cfm?function=showdocs&structure=Enterprise%20Architecture&category=IPv6. To learn more about the IPv6 profile itself, please visit http://www.antd.nist.gov/usgv6/usgv6-v1.pdf.

While resources can be more than just radio channels (e.g., telephones, talk groups), the Public Safety National Coordination Committee and National Public Safety Telecommunications Council (NPSTC) Standard Channel Nomenclature (available at http://tsiec.region49.org/ATT2126321.pdf) for the public safety interoperability channels can be used as a model for creating concise, yet descriptive resource names. For purposes of URIs and SDP-Origin-Usernames, spaces in NPSTC channel names should not be included (e.g., "LE 1" becomes "LE1"). If desired, the space can be used in the display field.

<Jurisdiction_Domain_Name> = Jurisdiction Domain Name or IP address in which the bridging system is operating. Optionally, <Port> = The port number where the request is to be sent.

Examples:

sip: FIRE1@212.123.1.213

sip:FIRE1@212.123.1.213:5060

sip:IR1@AgencyDomain.gov (IR = Incident Response)

sip:IR1@AgencyDomain.gov:5061

While the BSI Core profile does not place any requirements on the format of the <Resource Name>, the use of descriptive, alpha-numeric resource names is recommended. The total length of the URI should be less than 128 characters, unless longer URIs are supported.

While the BSI does not forbid the use of spaces and other special characters in a URI, including them requires additional effort to process. In these cases, SIP follows the requirements and guidelines of RFC 2396 (http://www.ietf.org/rfc/rfc2396.txt) when defining the set of characters that must be escaped in a SIP URI. One of the most common cases would be to implement %20 escaping for the "space" character in a resource name.

Example:

FIRE 1@212.123.1.213 = FIRE%201@212.123.1.213

If supported by the bridges, the BSI profile also allows the use of an optional SIPS URI to request a secure transport between bridges. The format for a SIPS URI is the same as describes above, except that the scheme is "sips" instead of "sip." Security is discussed in more detail in the Network Security section.

Bridging System Robustness/Redundancy

There are three principles of high availability engineering:

1. Elimination of single points of failure (e.g., redundancy, backup power, alternate routes)

2. Reliable crossover

3. Prompt notification of failures as they occur

These three principles all need to be addressed, but they must be addressed in different ways. Elimination of single points of failure is a provisioning issue. An implementation simply needs to have backups. In emergency services, the key point is to recognize other Internet infrastructures associated with schools or other parts of the government and incorporate those infrastructures into the larger system. Some redundancy must be faced as a requirement and purchased.

The stateless, connectionless design of IP solves the issue of reliable crossover throughout the Internet. Routers in the Internet support reliable crossover. As long as the Internet interconnects its segments by routers, there is a solution in hand. Routing is good; bridging is not (Here, bridging means layer 2 bridging). Bridges use the spanning tree protocol [IEEE 802.1] to control ringing in the LAN, and spanning tree protocol deals with alternate routing by disconnecting it—thereby defeating the high availability principles.

The Simple Network Management Protocol (SNMP) provides prompt notification of failures. SNMP agents and a published management information base should procure the BSI Core equipment wherever possible so that an SNMP console can monitor its functionality and potentially manage the device over the network. However, it is not required to have an SNMP agent available on a bridge/gateway device. Establish an SNMP console at a 24-hour watch standing location with trained operators on hand.

Guidance on Transcoding

Transcoding refers to an audio signal being encoded and decoded as it passes through a communication system. In Figure 12, the audio signal is transcoded a minimum of three times: 1) as it goes into radio A and out of radio B; 2) as it goes into gateway C and out of gateway D; and 3) as it goes into radio E and out of radio F. There is potential for the quality and intelligibility of the signal to reduce each time the audio signal is transcoded. In addition, there may be additional factors inside the devices or the transmission systems that further reduce the quality

and intelligibility. Therefore, it is important to consider the following guidance when patching systems together with the BSI:

- Look at the overall system design of all the connected systems and connect things in a way that minimizes the number of times that an audio signal will be transcoded when passing from end to end.

- Use the highest quality coding mechanism for each leg of the connection – the end-to-end quality will never be better than the lowest quality leg.
    - Assess audio intelligibility in the incident environment before a BSI is deployed operationally.
    - Note that using G.711, also known as 64 Kbit/s pulse-code modulation (PCM) as the only required vocoder in the BSI helps ensure that the BSI link will provide the smallest impact possible on the audio performance. Expect performance degradation when lower bit-rate vocoders are used in cases of network restrictions.

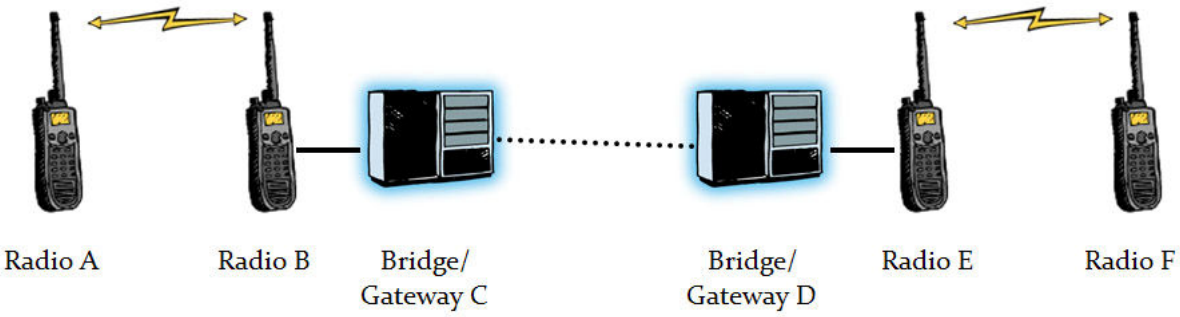

Figure 12 – Example of a Communication Path Requiring Three Audio Transcodings

Predicting Quality When Planning

The ITU recommends a tool that can help a system planner predict end-to-end quality during the design phase of a communications system. Known as the e-Model, the tool is described in Recommendation G.107, and is available online at http://www.itu.int/ITU-T/studygroups/com12/emodelv1/. Guidance for using the e-Model is available in Recommendation G.108 and Recommendation G.113 contains impairment values (*Ie*) for several types of audio coders. Unfortunately, a value of Ie has not been computed for the

Improved Multi-Band Excitation vocoder that is used in P25 radios. However, some information on quality impacts of mixing other low-bit-rate vocoders with the IMBE vocoder is given in Figure 13. The figure depicts the estimated mean opinion score (MOS) of several CODECs alone and in tandem. MOS is presented as a number between 1 and 5, where 5 is the best score possible. A more complete report describing these interactions is available at http://www.its.bldrdoc.gov/pub/ntia-rpt/01-386/.

Assuming that G.711 vocoder (labeled PCM in the figure) is used in the BSI implementation, Figure 8 can also be used to provide an estimate of quality when two radio systems are bridged together by finding the combination of vocoders encountered from end-to-end (using G.711/PCM as a rough equivalent to analog radio channels). Extending this rough equivalence to a connection of two 25 kHz analog radio channels via a BSI using G.711/PCM, one would expect a small degradation (less than 0.5 MOS) in quality from the single PCM case shown in the figure. Using a low-bit-rate vocoder for the BSI will lower performance, depending on the vocoder chosen for the BSI.

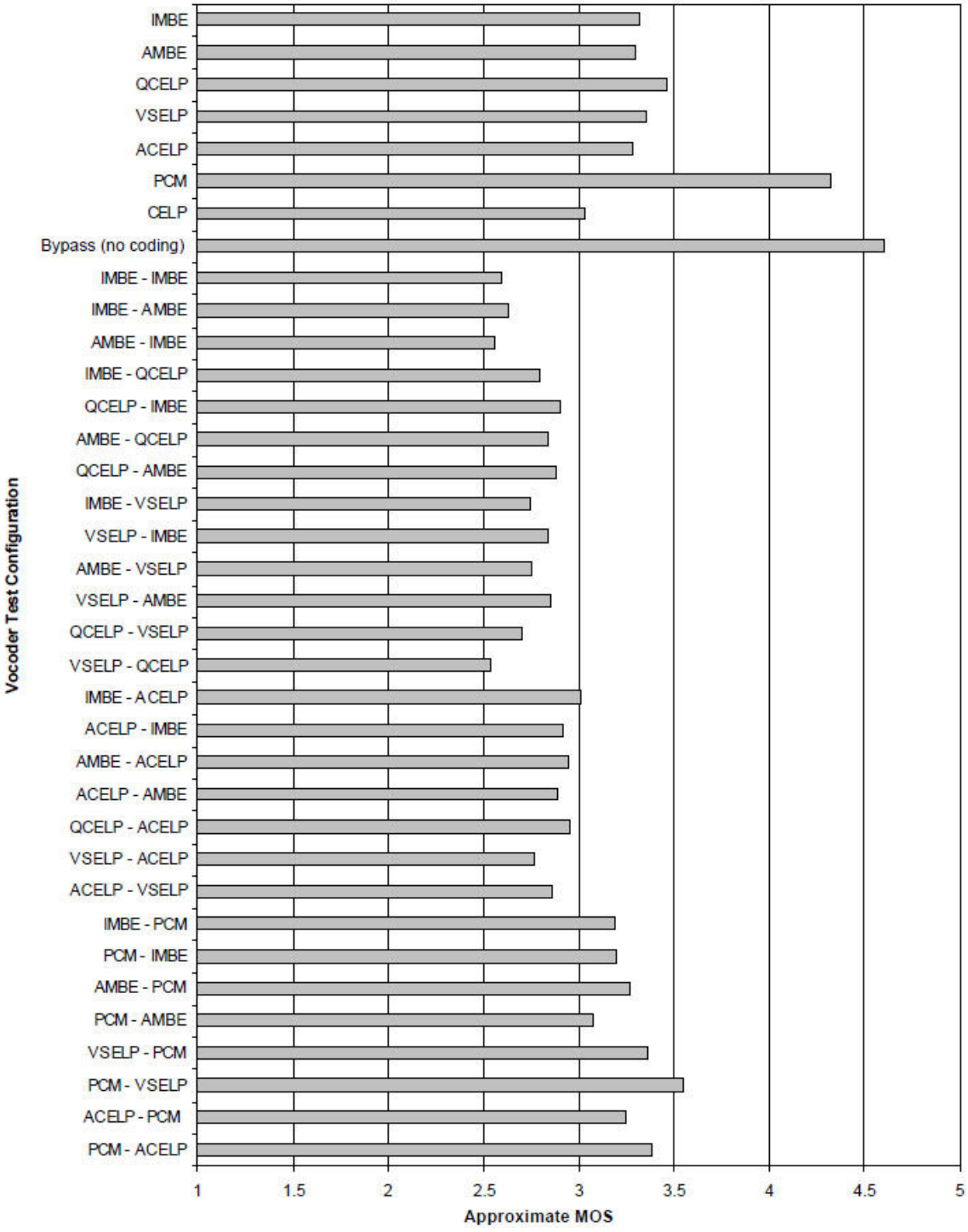

Figure 13 – Estimated MOS for Selected Vocoders Alone and in Tandem

Interpreting SIP Error Codes

RFC3261 contains definitions for standardized error codes and a short descriptive message. Below is a select list of these error codes and their interpretations, which will help users understand what type of action to take based on the error codes and responses. This is not an exhaustive list, but it should account for the majority of errors.

- **400 Bad Request:** The SIP URI was not in an acceptable format. Check to make sure that the URI requested conforms to the section on Naming Conventions. If necessary, check with the remote BSI manager to get a correct URI.

- **401 Unauthorized:** The remote BSI device requires an authentication mechanism. This is not a supported feature of the BSI Core. Contact the remote BSI manager to see if the authentication feature can be disabled for interoperability purposes.

- **403 Forbidden:** A connection to the requested resource is not currently allowed. Contact the remote BSI manager to either provide a connection-approved resource name, or to change the settings on the device to allow for connection.

- **404 Not Found:** The requested resource was not found on the remote BSI. Check for typographical errors, and if that does not provide a solution, contact the remote BSI manger to get the correct resource name.

- **480 Temporarily Unavailable:** Due to some condition of the remote BSI or the systems that it is connected to, the requested resource is temporarily unavailable. The message may contain a time interval to wait for the next attempt to access that resource. If the message continues over several retries, contact the remote BSI manager to find the estimated availability time.

- **482 Loop Detected:** A connection to the resource being called would cause a loop. In this case, a connection already exists through the other existing BSI connections.

- **486 Busy Here:** The resource that is being called currently has the maximum allowable number of connections active. Depending on the situation, connect to a different BSI that is part of the resource group, or contact the remote BSI manager to have them dump existing connections and allow the connection.

- **500 Server Internal Error:** Contact the remote BSI manager and tell them what caused the error so that they can attempt to fix the problem.

- **503 Service Unavailable:** For some reason, the remote BSI is unable to provide VoIP service. If the condition persists, contact the remote administrator to obtain an estimate of the repair time.

Essential Configuration Information

This section provides a basic list of the information that needs to be exchanged to configure bridging devices to communicate with each other. As each bridge has a unique user setup and operational defaults, the goal of this section is to provide the end user a starting point with which to setup connections between BSI Core compliant bridges.

Table 1 describes the parameters to be configured and exchanged, a description of those settings, and recommendations for configuration, as appropriate. Users should request a reference guide from their equipment provider that includes instructions on how to identify current settings and make new settings for these parameters. Keep a reference guide such as this one near the bridging device.

Table 1 – Configuration Information Necessary to Successfully Make a BSI Connection

Parameter to be Pre-exchanged	Description	Comment
POC	Point of contact information for the bridging system.	This information is critical to the swift resolution of connection issues.
SIP Signaling IP Address	IP address that SIP signaling messages should be sent to.	REQUIRED for pre-configuration by BSI implementation profile. Should be set in conjunction with network/IT administrators.
SIP Signaling Host Name	A symbolic string (e.g. Client.BS1.example.com) representing a host name that SIP signaling messages should be sent to.	RECOMENDED for pre-configuration by BSI implementation profile. Should be set in conjunction with network/IT administrators
SIP Signaling TCP Port	The TCP port number used for BSI SIP signaling	TCP:5060 is generally the default. Network administrators will need to know this information for firewall configuration. They may require an alternate port number.
Media IP Addresses	The IP address(es) used by the bridging system to send and receive RTP/RTCP audio packets during a BSI media session	RECOMMENDED for pre-configuration by BSI implementation profile for firewall configuration. Should be set in conjunction with network/IT administrators.

Parameter to be Pre-exchanged	Description	Comment
RTP/RTCP Media Ports Range	The UDP ports range used by the bridging system to send and receive RTP/RTCP audio packets during a BSI media session	RECOMMENDED for pre-configuration by BSI implementation profile for firewall configuration. Should be set in conjunction with network/IT administrators.
Resource Identifier(s) (SIP URI[s])	A SIP Uniform Resource Identifier according to the RFC3261 representing a radio resource at a bridging system	REQUIRED for preconfiguration by BSI implementation profile. RECOMMENDED format is sip:<Resource Name>@<Jurisdiction Domain Name>

Appendix A: Acknowledgements

The Bridging Systems Interface Best Practices document is the result of contributions from members and supporters of the VoIP Working Group including the following individuals listed in alphabetical order:

- D.J. Atkinson, Public Safety Communications Research Program
- Marlin Blizinsky, King County, Washington
- Joe Boucher, Mutualink
- Tom Bretthauer, Ohio MARCS
- Rex Buddenberg, U.S. Naval Postgraduate School
- John Crabill, U.S. Department of Transportation, National 9-1-1 Office
- David Craig, TracStar
- Stephen Devine, Missouri Department of Public Safety
- Laurie Garfinkel, Telex Radio Dispatch, Bosch Security System, Inc
- Craig Georgeson, Telex Radio Dispatch, Bosch Security System, Inc
- Craig Jorgensen, Project 25
- Alan Komenski, Washington State Patrol
- John Lenihan, Los Angeles County Fire Department
- Josie Leyman Elias, Communications-Applied Technology
- Kenneth Link, City of Jersey City, New Jersey
- Timothy Loewenstein, Buffalo County, Nebraska – District 3
- Jennifer Lord, Wisconsin Office of Justice Assistance
- Dave Maples, The MITRE Corporation
- Jim Mathis, Motorola
- Larry Metzger, Cisco
- Rob Mitchell, Twisted Pair Solutions
- Michael Murphy, Gulf States Regional Center for Public Safety Innovations
- Anna Paulson, Public Safety Communications Research Program
- John Powell, National Public Safety Telecommunications Council
- Paul Roberts, Boise Fire Department
- Mike Schools, Catalyst Communications Technologies
- JJ Sheppard, TracStar
- McRae Smith, Raytheon Company
- Dorothy Spears-Dean, Virginia Information Technologies Agency
- Ashley Strickland, Pittsboro Fire Department
- Andy Thiessen, Public Safety Communications Research Program
- Cliff Veale, Twisted Pair Solutions
- Stephen Wisely, APCO
- Stuart Zerbe, C4i

Appendix B: Acronyms

BSI Bridging Systems Interface
CODEC Coder-Decoder
DHCP Dynamic Host Configuration Protocol
DHS U.S. Department of Homeland Security
DiffServ Differentiated Services
DMZ Data Management Zone
DNS Domain Name System
DOC U.S. Department of Commerce
DTMF Dual-Tone Multi-Frequency
ESP Encapsulating Security Payload
FCC Federal Communications Commission
GRE General Routing Encapsulation
GSO Geostationary Orbit
ICE Interactive Connectivity Establishment
IETF Internet Engineering Task Force
IMBE Improved Multiband Excitation
IP Internet Protocol
IPDV IP Delay Variation
IPER IP Error Ratio
IPLR IP Loss Ratio
IPSec IP Secure
IPTD IP Transfer Delay
IR Incident Response
ISAKMP Internet Security Association and Key Management Protocol
ISSI Inter-RF Subsystem Interface
ITU International Telecommunications Union
ITU-T International Telecommunications Union - Telecommunication Standardization Sector
LAN Large Area Network
LMR Land Mobile Radio
MOS Mean Opinion Score
MOU Memorandum of Understanding
MPLS MultiProtocol Label Switching
NAT Network Address Translation
NPSTC National Public Safety Telecommunications Council

OIC Office for Interoperability and Compatibility
P25 Project 25
PCM Pulse-Code Modulation
PTT Push-to-talk
QoS Quality of Service
RF Radio Frequency
RFC Request for Comment
RS Radio System
RSVP Router ReSerVation Protocol
RTCP Real-time Transport Control Protocol
RTP Real-time Transport Protocol
SCIP Statewide Communication Interoperability Plan
SDP Session Description Protocol
SIP Session Initiation Protocol
SLA Service Level Agreement
SNMP Simple Network Management Protocol
SOP Standard Operating Procedure
STUN Simple Traversal of UDP through NATs
TCP Transmission Control Protocol
ToS Types of Service
TURN Traversal Using Relay NAT
UDP User Datagram Protocol
UPnP Universal Plug and Play
URI Uniform Resource Identifier
VoIP Voice over Internet Protocol
VPN Virtual Private Network
VSAT Very Small Aperture Terminal
VTC Video Teleconference
WLAN Wireless Local Area Networks
WWAN Wireless Wide Area Network

Appendix C: Tanker Truck Rollover Scenario

1) A full fuel tanker leaves the refinery in Cheyenne, Wyoming, and heads south on I-25 into Colorado. Just south of the Colorado border, in Weld County, the truck encounters a patch of black ice, slides off the edge of the road, and overturns.

2) While one passing motorist attempts to help the injured driver, a second motorist continues down the road about five miles (into Larimer County) to get into cell phone coverage and call 9-1-1 to report the accident.

3) The NG 9-1-1 system correctly identifies the caller's location and routes the call to the Larimer Country Public Safety Answering Point (PSAP).

4) As the call taker learns the details of the accident, a telephone conference patch is set up to include the Colorado State Patrol (CSP) dispatch center and the Weld County PSAP.

5) Adhering to prior policy, the three dispatch centers recognize that because of the location of the accident, all three agencies need to send a response unit to the scene. Additionally, a shared communications bridge needs to be configured for the accident response teams to communicate on scene.

    a) The State of Colorado has a bridging device (Manufacturer A) to allow for the coordination of those on the statewide 800 MHz trunked system with Weld County's and Larimer County's Rural Fire District's UHF conventional systems. The CSP dispatcher quickly sets up a shared communications bridge to enable communications.

    b) As each agency is added to the common channel, the CSP dispatcher indicates the new agency added and advises all agencies using the channel to use clear speech instead of codes.

6) Upon learning about potential injuries to the driver and understanding that the overturned truck contains hazardous material, the CSP dispatcher determines that they could achieve a faster response by having the Cheyenne Fire Department and Emergency Medical Services (CFR) respond to the accident. These responders are located five miles away as opposed to the Larimer County responders who are 40 miles away in Fort Collins, or the Weld County responders who are even farther away.

7) Based on cooperative agreements between the CSP and the Wyoming Highway Patrol (WHP), the CSP dispatcher contacts the appropriate WHP dispatcher in Cheyenne. The WHP dispatcher immediately dispatches the WHP officer from the Port of Entry, three miles from the Colorado border.

8) As the WHP officer is dispatched, the WHP and CSP dispatchers exchange information to enable a connection between radio bridges and allow the WHP officer to speak directly with responders from the three Colorado agencies en route to the scene.

    a) The State of Wyoming has a bridging device (Manufacturer B) to allow the coordination of the WHP and Wyoming Department of Transportation on the 800 MHz trunked system with the CFR on their 150 MHz conventional system.

    b) The bridges are able to communicate using an Internet Protocol (IP) link between the Colorado bridge and the Wyoming bridge.

    c) The dispatchers from WHP and CSP enable the bridges to communicate with each other over the IP link. Although there are several agencies patched together with the individual bridges (both in Wyoming and Colorado), all three agencies in Colorado can now speak to the aforementioned agencies in Wyoming, and vice versa, all using a single connection between to the two bridges.

9) Upon hearing that there are injuries, the WHP dispatcher also dispatches CFR to the scene.

    a) The dispatcher also follows policy on incorporating CFR into the incident management channel.

    b) As CFR is added, the addition is announced with the caution to utilize clear speech instead of codes.

10) The WHP officer is the first responder on scene and becomes the Incident Commander.

11) The WHP officer confirms the injuries to the driver and notes that the overturned tank trailer is disgorging unleaded fuel onto the shoulder of the road, requiring a HazMat team and recommending a closure of the southbound (SB) lanes of I-25.

12) The WHP dispatcher contacts the Wyoming Highway Department (WHD) and orders the SB I-25 closed and traffic redirected to US-85.

    a) The CSP dispatcher, via the patch, hears the officer recommend closing SB I-25 and alerts the Colorado Department of Transportation that SB I-25 will be closed for a time and that US-85 traffic will be significantly increased.

13) The CFR arrive on scene and report to the Incident Commander via the shared communications bridge and receive their assignments.

    a) The Emergency Medical Technicians starts attending to the injured driver.

    b) The Fire Department begins ensuring that the spilled fuel does not ignite.

14) The Cheyenne HazMat crew arrives, reports to the Incident Commander via the shared communications bridge, and begins work to contain and mitigate the fuel spill.

15) The CSP officer arrives on scene. After receiving a situation brief from the WHP officer, the CSP officer takes over as Incident Commander. With the impending arrival of additional Colorado-based resources, the WHP officer stays on as the resource manager for the Wyoming-based resources.

    a) The change in roles is announced on the shared communications bridge.

16) The CSP officer requests two tow trucks from Fort Collins to right and tow the tractor and trailer of the overturned rig.

17) The Cheyenne Emergency Medical Services (EMS) departs to the Cheyenne hospital with the injured driver.

    a) They check out of the incident scene and the WHP dispatcher disconnects the bridge to their channel—announcing their removal to the rest of the participants.

18) The Weld County and Larimer County Sheriff's Deputies, Fire, and EMS arrive on scene.

    a) The Incident Commander assigns the deputies to perimeter security and initial investigation of the accident.

b) The Colorado-based fire departments are assigned to relieve the Cheyenne Fire Department.

c) The Colorado-based EMS teams are held in reserve.

19) The Cheyenne Fire Department packs up and checks out of the incident scene.

a) The WHP dispatcher disconnects the bridge to their channel—announcing their removal to the rest of the participants.

20) The WHP officer stays on to assist in the investigation documentation.

21) The tow trucks arrive and rights the tractor and tank trailer.

22) The HazMat crew finishes clean up.

23) The Incident Commander dismisses the Colorado-based fire and EMS teams and the Cheyenne HazMat team.

a) The CSP dispatcher disconnects the county agencies from the bridge connection and announces it to the remaining participants.

b) The WHP dispatcher disconnects the Cheyenne HazMat crew from the bridge—announcing their removal to the rest of the participants.

24) The tow trucks depart with the respective pieces of the damaged rig.

25) The Incident Commander declares the road safe to open and the WHP dispatcher informs the WHD to reopen the road.

26) The CSP officer, WHP officer, and the deputies conclude their investigation.

27) The Incident Commander declares the scene clear and the remaining officers depart.

28) The CSP dispatcher disconnects the IP link that enabled inter-state communication.

Appendix D: BSI Core 1.1 Features

The table below shows a list of features that are required, recommended, and optional supported elements for BSI implementations.

Table D-1. BSI Features Matrix

Feature	Section	Required	Recommended	Optional
SIP via TCP	7.1	X		
SIP via UDP	7.1			X
Proxy Server Support	5.6			X
Registrar Support	5.7			X
NAT Support	7.5			X
G.711 vocoder support	6.3	X		
GSM 6.10 vocoder support	6.3.1		X	
G.729 vocoder support	6.3.1		X	
GSM AMR vocoder support	6.3.1			X
IMBE vocoder support	6.3.1		X	
Other vocoder support	6.3.1			X
SIP/TCP Persistent Connections	7.1.1		X	
SIP Requests	5.1.1	X		
SIP Response	5.1.2	X		
SIP Invite[5]	5.2	X	X	X
SIP Invite Response[6]	5.2	X	X	X
SIP Re-Invite	5.3			X
SIP Call Patching	5.3.2			X
SIP Bye	5.4	X		
Media Setup via SDP	6	X		
Media Transport via RTP	6.2	X		
Media Forwarding	6.3			X
DTMF Encoding via RFC 4733	6.5	X		
SSRC for loop prevention	6.2	X		
Voice packet detection	10	X		

[5] Depending on specific SIP features as indicated in 5.2
[6] Depending on situation at the responding bridge.

Media Loss Detection via RTCP	10.1	X		
Reconnect after Media Loss Detection	10.1			X
IP Service Marking	7.2.1		X	
IP V4 Addressing	7.3	X		
Operate on unencrypted networks	8	X		
Operate with encryption mechanisms	8			X