Public Safety VoIP + Bridging

Anna Paulson

Electronics Engineer

Public Safety Communications Research Program

apaulson@its.bldrdoc.gov

PSCR Partnership

PSCR Sponsors

Department of Homeland Security

Office for Interoperability and Compatibility

Department of Justice

Office of Community Oriented Policing Services

Background

Why Voice Over Internet Protocol (VoIP)?

- System interoperability needs have pushed the capabilities of traditional public safety communications networks.
- Today's public safety networks may need to integrate cellular phones and Internet Protocol (IP)-based voice and data systems with traditional Land Mobile Radio (LMR) and dispatch systems from various manufacturers.
- Safety agencies often rely on VoIP bridging solutions to communicate with other agencies and to link disparate communications technologies with conventional equipment.

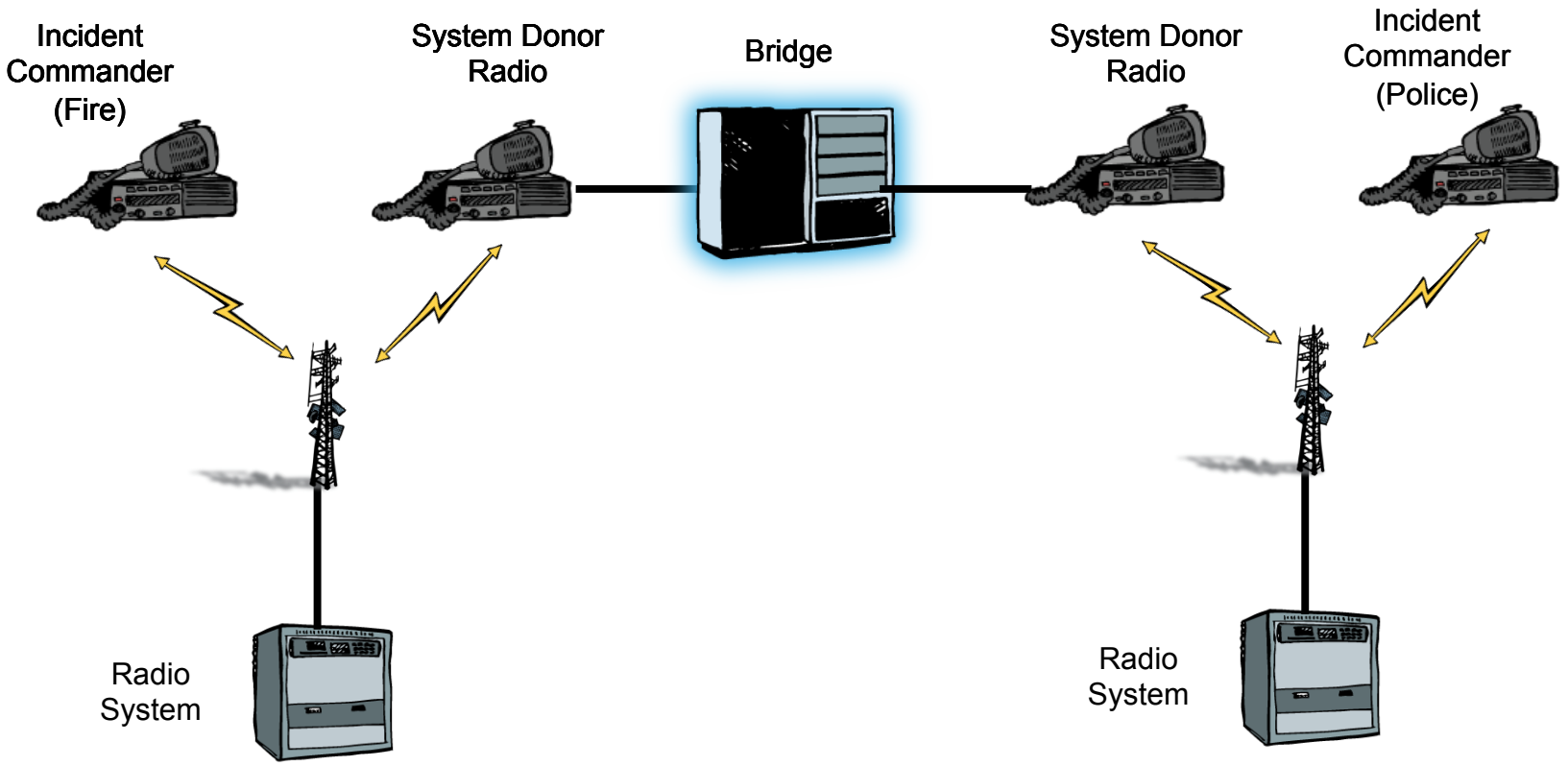
Background

What is a Bridging System?

- A communications endpoint aggregator
- Translates outgoing traffic from one type of endpoint device to another e.g., a handheld VHF radio to an Incident Commander's IP telephone.
- Bridging devices typically use an analog voice signal as the basis for interchange between LMR systems.
- Endpoints are either directly connected to the bridging solution or connected to a remote bridging device via another network.

Background

A typical bridging system scenario



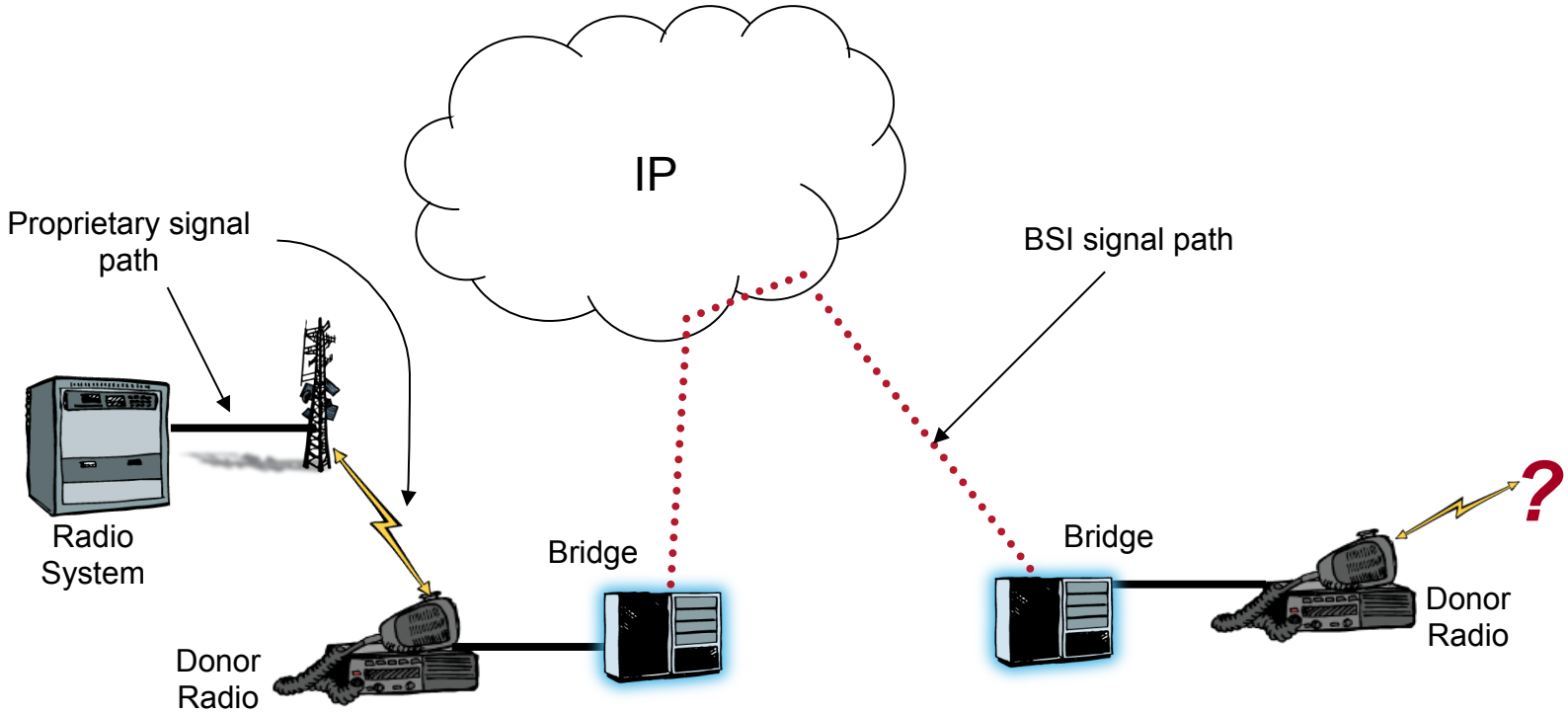
Background

What is a Bridging System Interface (BSI)?

- Large-scale incidents require the cooperation of multiple public safety disciplines and agencies.
- Bridging systems can be internetworked between agencies to extend the range and capabilities of existing networks.
- The connection between two bridging systems is more commonly known as a Bridging System Interface (BSI).
- BSI uses Session Initiation Protocol (SIP, an Internet standard) as the basis for call setup and teardown.
- SIP is a text-based, request/response, call setup protocol which uses Internet standard Real-time Transport Protocol (RTP) and Session Description Protocol (SDP) to pass voice and session parameter data.

Background

A typical BSI network scenario



VoIP Efforts

The U.S. Department of Homeland Security's (DHS) Office for Interoperability and Compatibility (OIC) and the U.S. Department of Commerce's PSCR program are working with public safety and industry representatives to improve emergency response interoperability through the use of VoIP.

VoIP Efforts

Public Safety VoIP Working Group (PSVWG) Project goals:

- Generate a clearer idea of VoIP's potential use in public safety
- Define benefits and limitations of VoIP for public safety
- Develop an understanding of the security and reliability issues surrounding VoIP for public safety
- Gather user community feedback as to how industry can best meet their needs

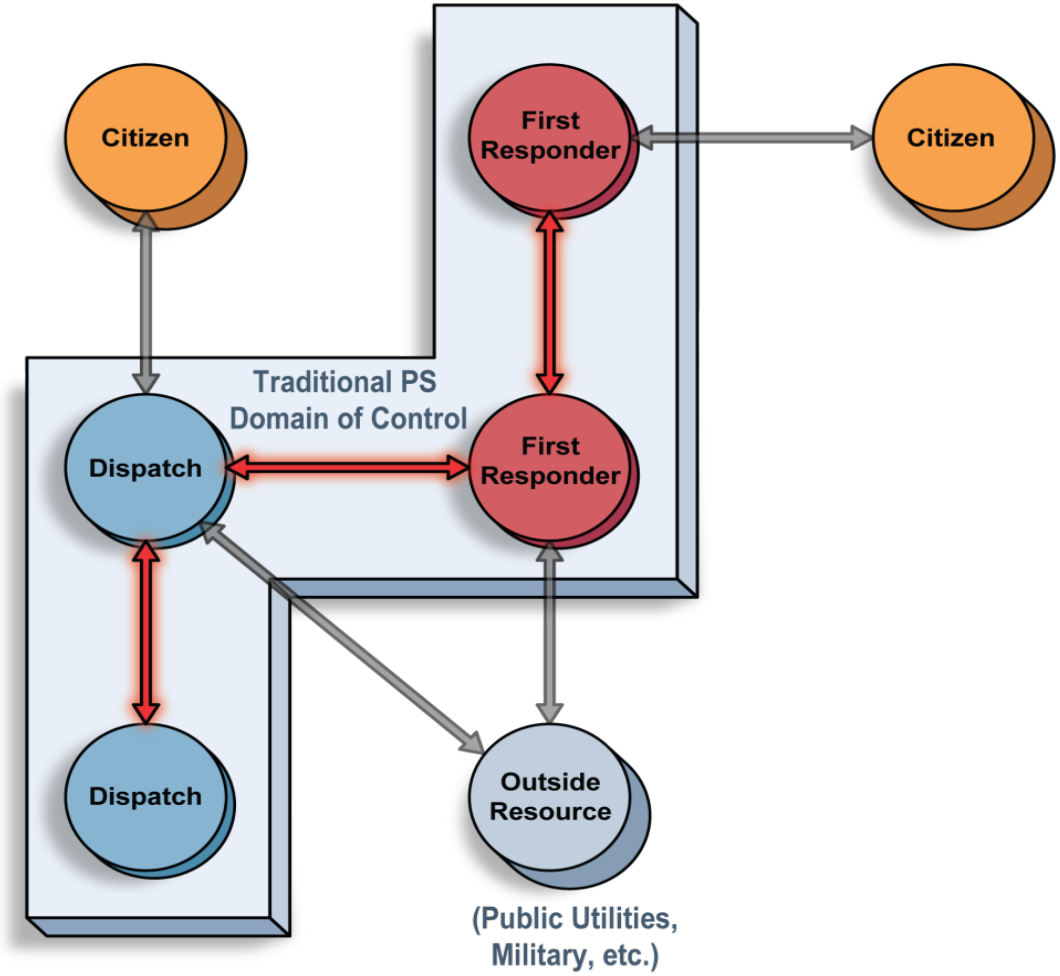
VoIP Efforts

PSVWG Project goals:

- Facilitate open, unscripted dialogue between the public safety practitioner and industry communities
- Gather practitioners, manufacturers, and agencies together to participate in roundtables, conference calls, “plugfests”, and network testing.
- Create a BSI Core and Enhanced Profile.
- Develop automated compliance testing measures.
- Extend BSI work to other VoIP interfaces.

VoIP Efforts

Scope of VoIP Interfaces



VoIP Efforts

In Scope VoIP Interfaces:

- Bridging Systems Interface, Subscriber Unit to Subscriber Unit Interface, Radio System to Radio System Interface, Radio Site Interface, Wired End Unit to System Interface, System to Subscriber Unit Interface, Dispatch Console Interface

Out of Scope VoIP Interfaces:

- 9-1-1 call taking
- Interactions with Public Switched Telephone Network (PSTN)

VoIP Efforts

PSVWG Roundtable I – August 2006

- Set project vision and goals.
- Defined project scope and what interfaces would be addressed.

VoIP Efforts

Public Safety VoIP Working Group Roundtable II – February 2007

- Defined the goal of producing an "Implementation Profile" and its parameters.

  "the minimum set of standards, parameters, and values required to ensure interoperability between distinct implementations"

- Identified public safety's requirements for the BSI

- Defined a work plan and Protocol Reference Model

VoIP Efforts

Public Safety VoIP Working Group Roundtable III – May 2007

Defined features for the BSI Core and BSI Enhanced

CORE

-Supports group voice communications across multiple bridging solutions
-Supports static or dynamic configuration, and static or dynamic activation
-Meets access-time, latency, and temporal clipping thresholds
-Ensures there is no "statistically significant" quality degradation as a result of improper codec selection or tandeming

---

ENHANCED

-Provides the ability to transmit priority information
-Allows for the arbitration of resources:
    E.g., transmit Push to Talk management information
-Provides control plane solution for this interface extensible for features other than voice:
    E.g., ability to transmit confirmed and unconfirmed call information
-Allows for awareness of channels to which the user is connecting
    Operators need to know

VoIP Efforts

Public Safety VoIP Working Group Roundtable IV – September 2007

Solidified draft implementation profile into a "release candidate" which illustrates how bridging systems from different vendors connect to each other using Internet Protocol (IP) through:

- Establishing simple **one-to-one audio pathways** between bridging systems
- Using **Session Initiation Protocol** (SIP) (RFC 3261), and related RFCs as the basis for an interoperable interconnect mechanism/model/profile
- Using **Real-time Transfer Protocol** (RTP) (RFC 3550) for the audio transport

Planned "plugfest" to evaluate implementations and work kinks out of specification

VoIP Efforts

VoIP Roundtable V– September 2008

- Finalized the BSI Core 1.0 Profile, the stable draft document
- Began Work on the BSI Enhanced Profile

IWCE – March 2009

- Decided to table the BSI Enhanced to focus on the BSI Core 1.1 and Best Practices

VoIP Roundtable VI – September 2009

- Validated the Draft BSI Core 1.1, which clarified BSI Core 1.0
- Got practitioner feedback on the Best Practices Document
- Reprioritized work efforts based on practitioner priorities

VoIP Efforts

Current priorities:

- **Complete Best Practices Document - e**diting groups have finished
- **Provide core capabilities for other key interfaces then enhance**

CORE

Radio system infrastructure interface
Dispatch console interface
End unit (soft device) interface
Radio site interface

ENHANCEMENTS

Floor control
Priority mechanism/Collision management
Directory service/resource availability
Information (Channel ID, PTT ID, Geodata)
Network Management
Network Security
Paging

VoIP Efforts

Best Practices document (two sections)

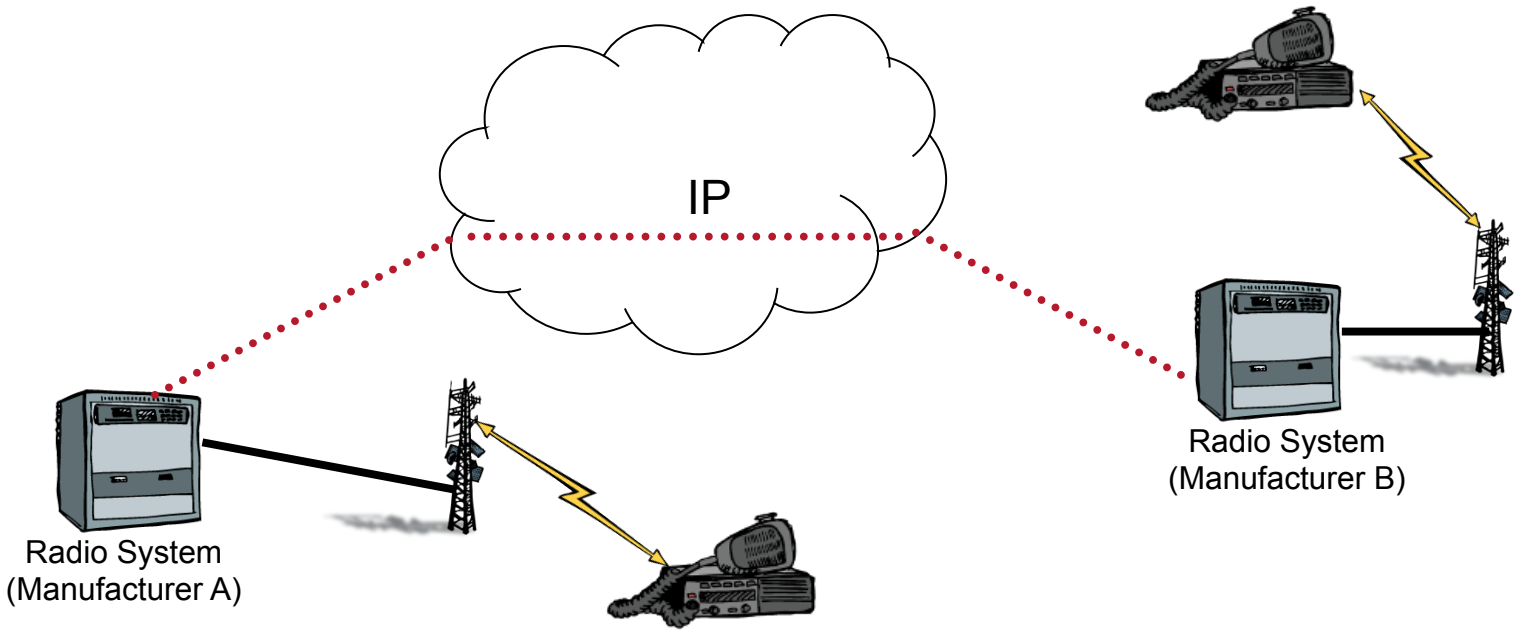
- **Administrative**
  - Used for contracting and by managers (CTO, Chiefs, etc.)
  - Sections include:
    - Governance/Planning
    - Service Level Agreements
    - Interagency Agreements
    - Standard Operating Procedures
    - Network Diagrams

Technical

- Used by practitioners/technicians (those that set up/run the devices)
- Sections include:
  - Network Provisioning and Capacity
  - Security
  - Voice Quality and Performance
  - Required Set-Up Information

VoIP Efforts

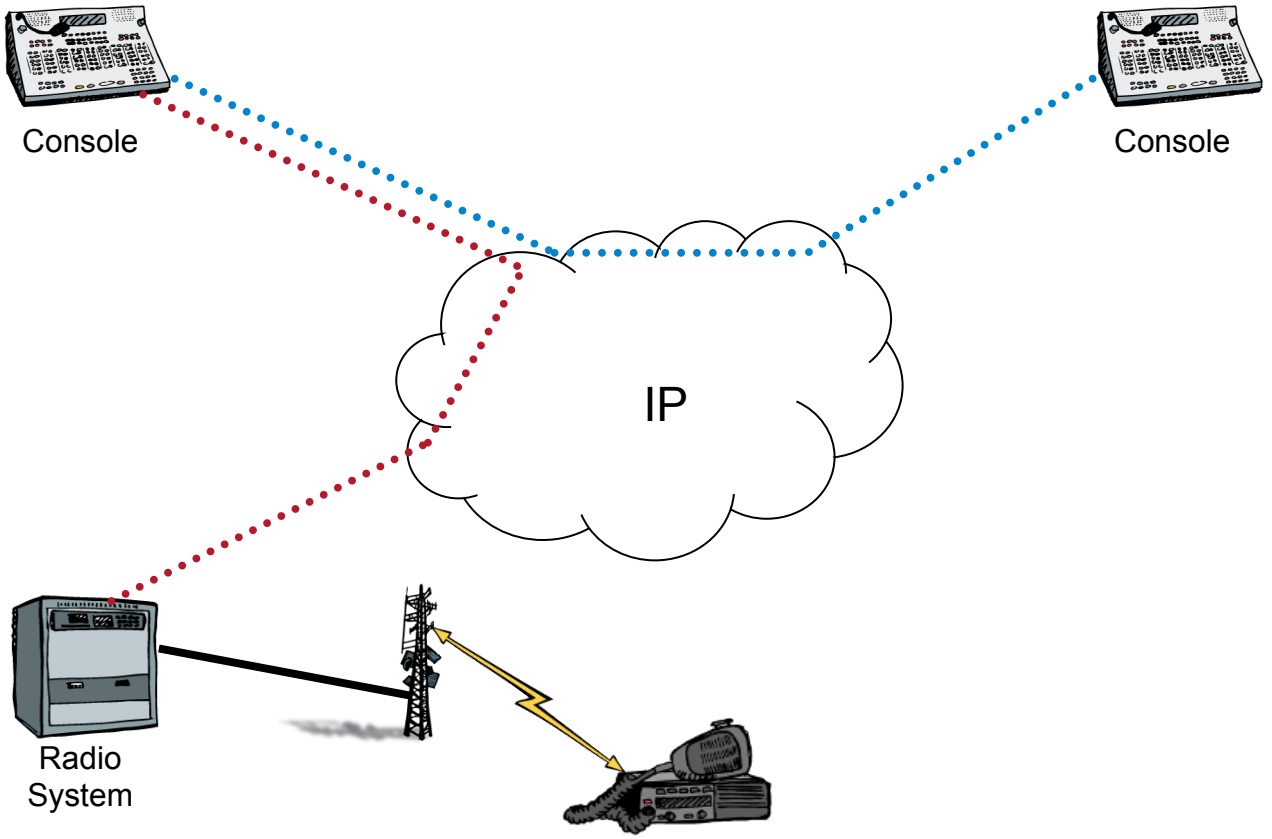
A typical Radio System Infrastructure Interface scenario.



21

VoIP Efforts

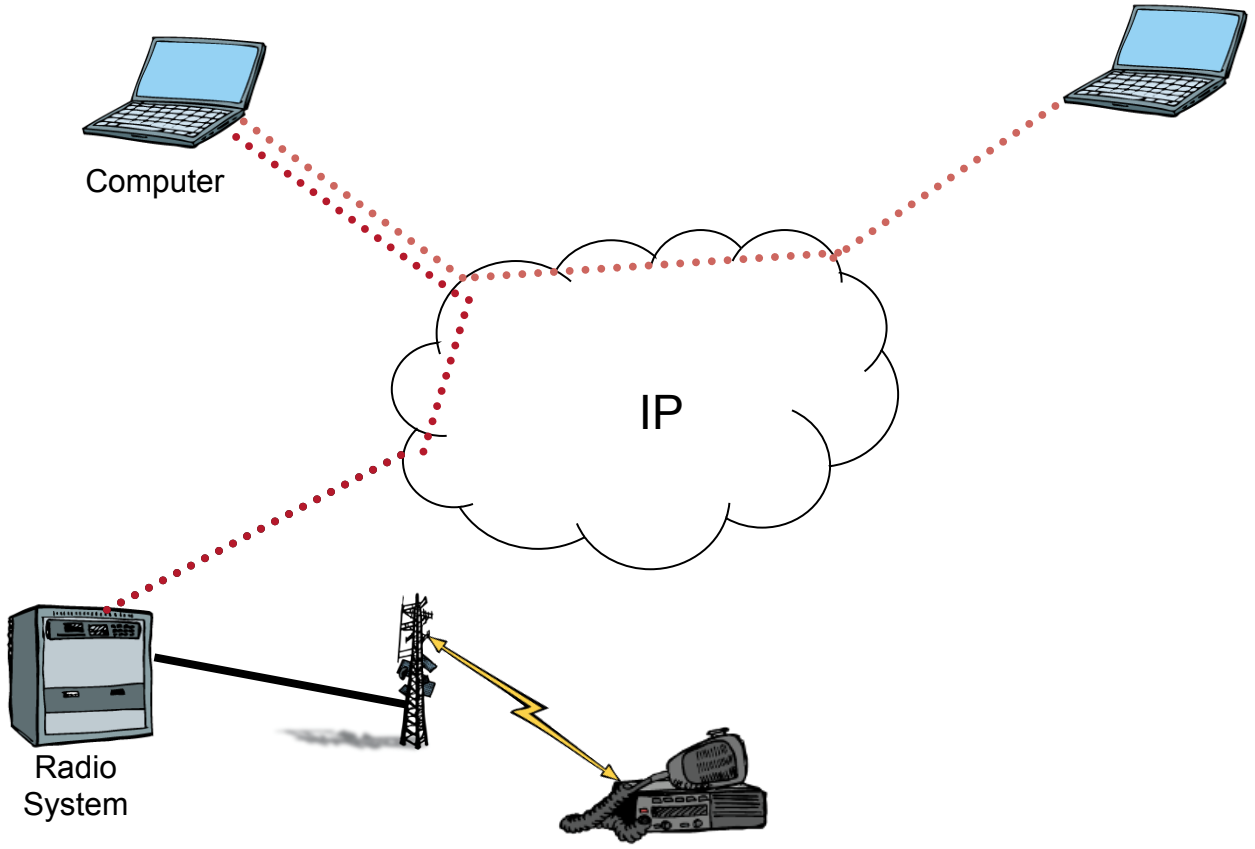
A typical Dispatch Console Interface scenario.



22

VoIP Efforts

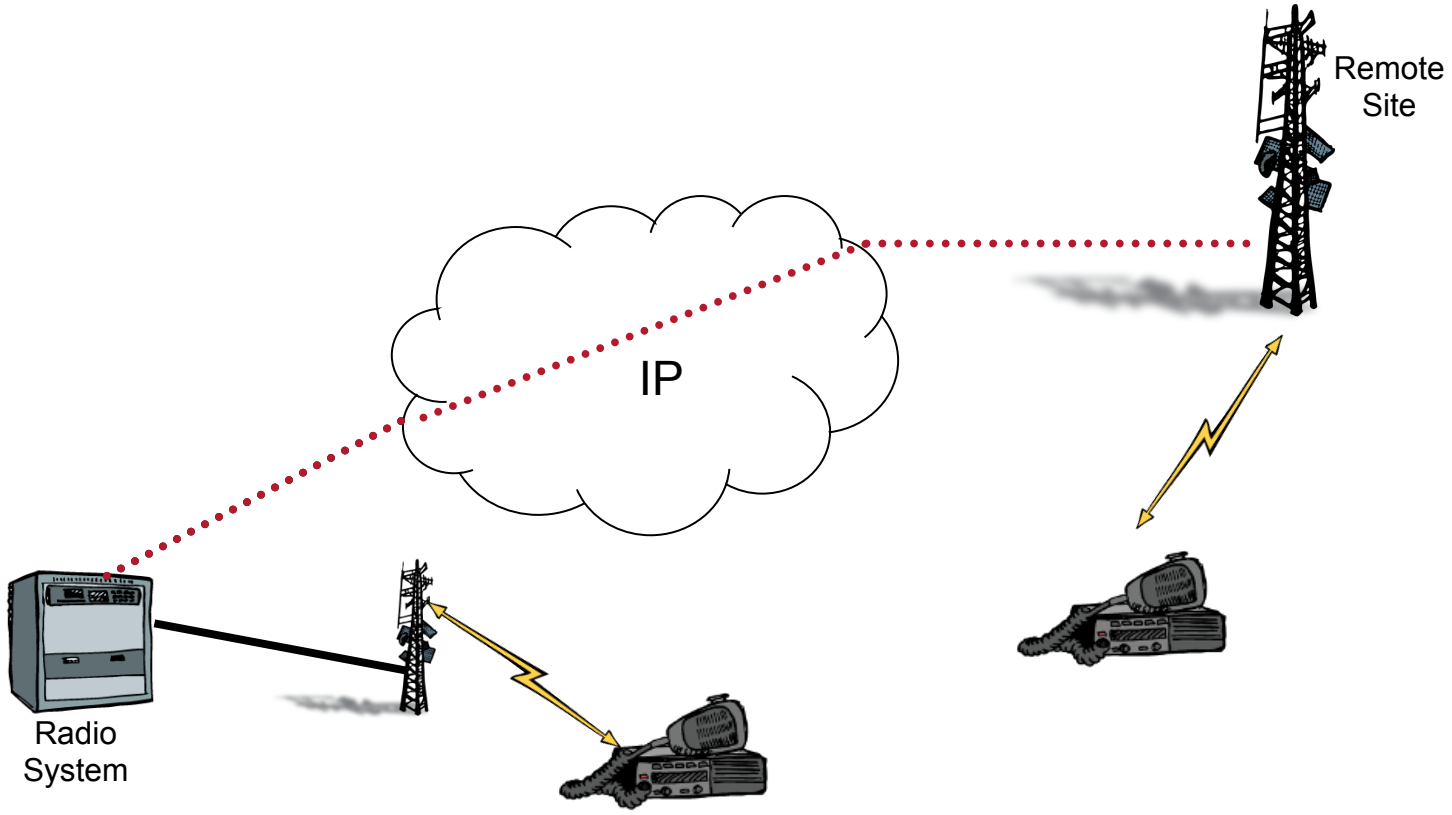
A typical End Unit (Soft Device) to System Interface scenario.



23

VoIP Efforts

A typical Radio Site Interface scenario.



24

VoIP Efforts

Known BSI Implementers

- C4i
- Catalyst
- Mutualink
- Raytheon JPS
- TracStar
- Twisted Pair Solutions
- Cisco
- Motorola
- National Interop
- SyTech
- VoiceInterop
- Zetron

BSI Automated Testing

Problem

- Manufacturers need timely access to standardized testing procedures and feedback from public safety (PS) customers.
- Getting together for plugfests is time-consuming and expensive
- PS needs assurance that products purchased will interoperate with products purchased by agencies they have to communicate with.

BSI Automated Testing

Solution

- Develop a two-pronged testing methodology and platform that manufacturers and practitioners can use to ensure their products meet the BSI profile.
  - Available at any time
  - Available remotely
  - As automated as possible
- The test suite consists of an automated conformance test tool (reference system) and Virtual Private Network (VPN) interoperability testing platform (testing system).
- VPN solution hosted at PSCR in Boulder, CO

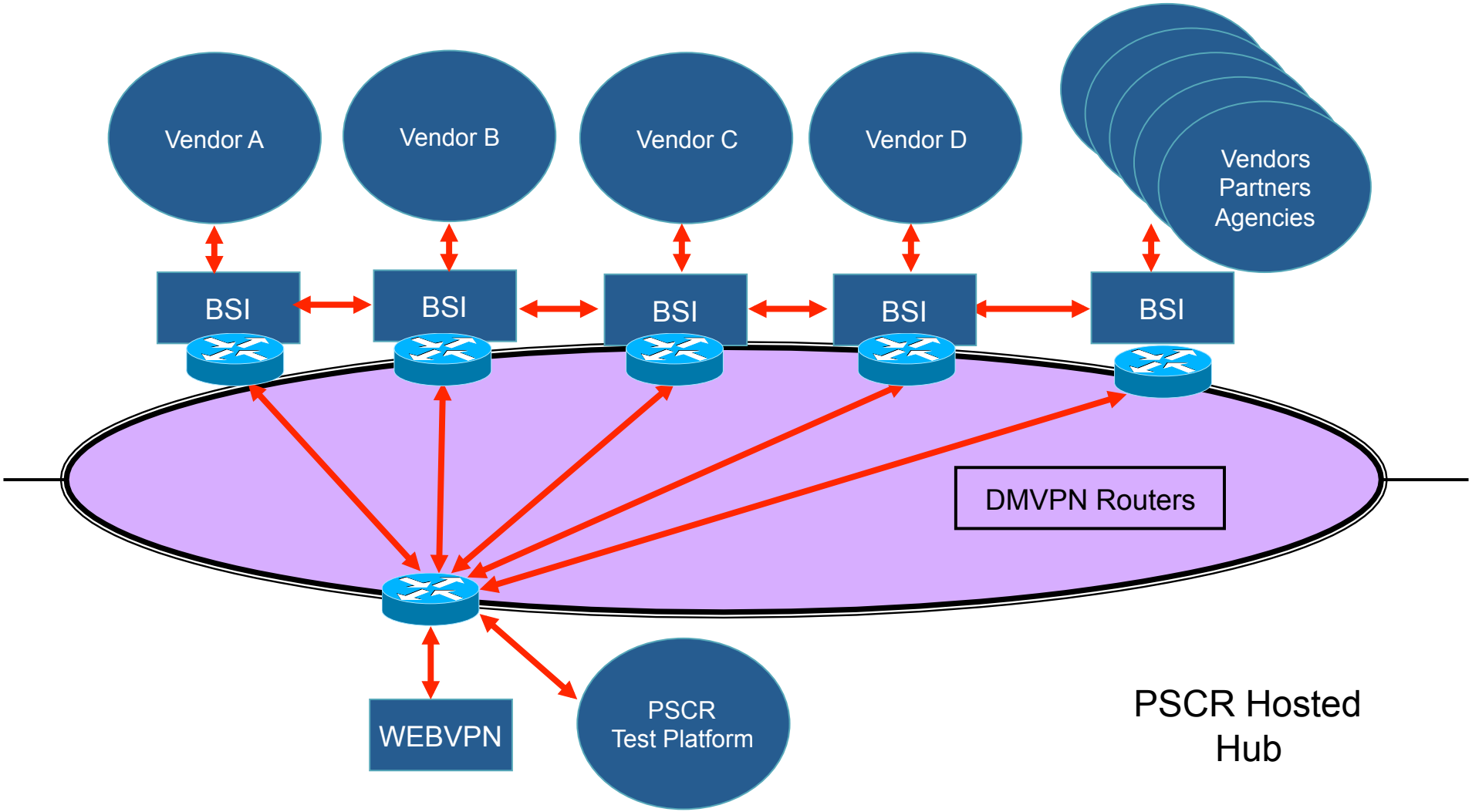
BSI Automated Testing-Development

- SIPp, an open-source test tool developed by Hewlett-Packard, is the heart of the test platform.
- SIPp makes use of SIPStone user agent scenarios and Call Processing Language commands embedded within XML scripts.
- SIPp is a good fit for this project because…
  - it's open source
  - has a vibrant user/developer community
  - has a robust command set (conditional branching, media/RTP support, regular expressions, etc.)
  - rapid scenario creation.

BSI Automated Testing-Development

- Test platform runs on a Red Hat Enterprise Linux 5 blade server with Asterisk PBX, OpenLDAP, etc.
- Users will connect to the test platform remotely via a PSCR VPN connection.
- The tool will verify that a bridging system passes all required BSI Core Profile tests. BSI Enhanced Profile test cases will be added to the tool as needed.
- A pass/fail report will be generated and returned to the user and may serve as proof of interoperability compliance.

BSI Automated Testing-Development

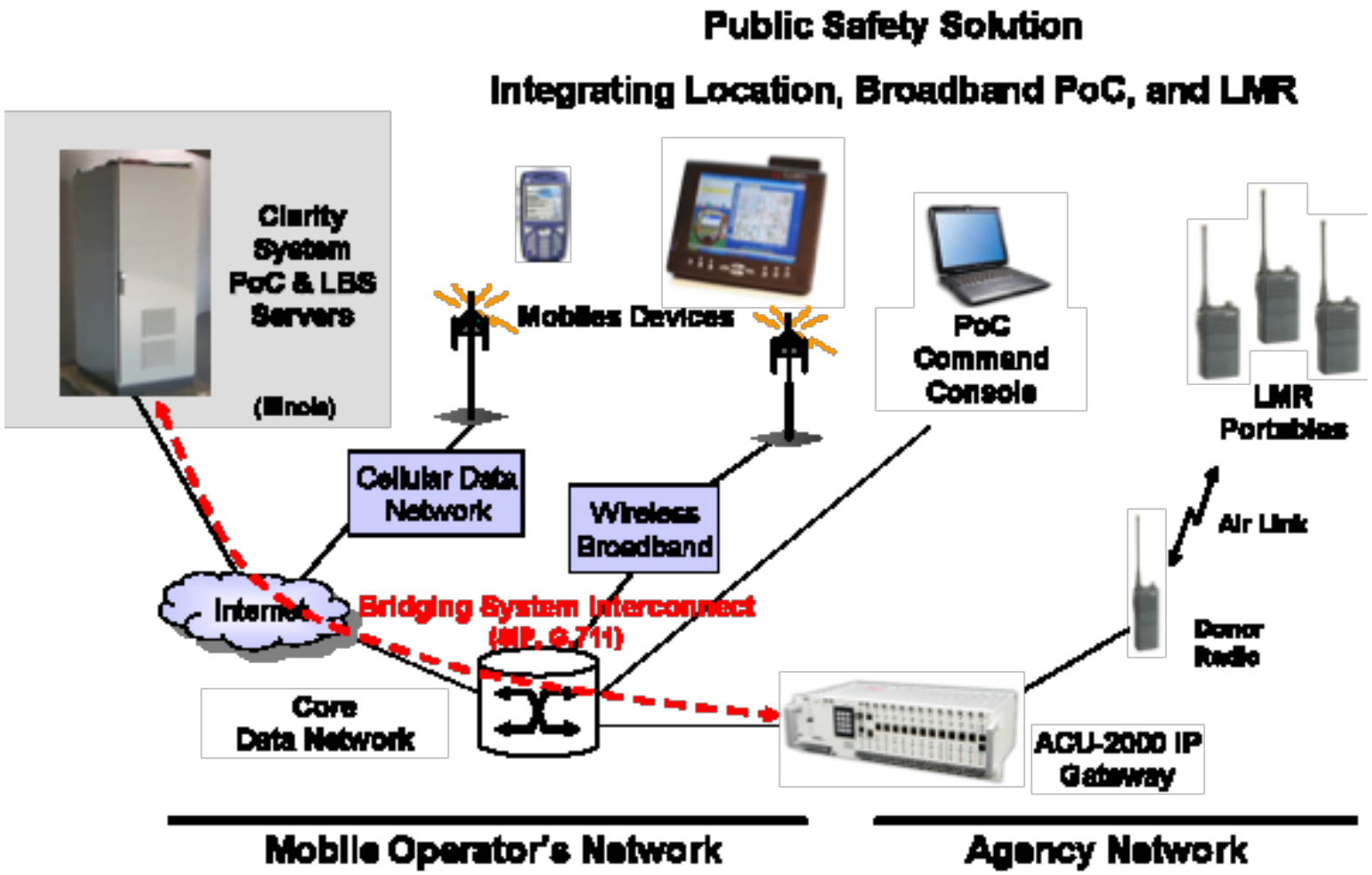


BSI Automated Testing-Next

- Tool development continues using bridging systems we have on hand.
- Will be made available to manufacturers as capabilities are completed and documented.
- Full test suite expected before IWCE 2010.
- Test suite can be used to show compliance with BSI profile.
- Manufacturers can provide test reports to prospective clients.

BSI Automated Testing-ROW-B

DHS Demonstration Architecture



Follow-up

Additional information is available at:

DHS SAFECOM program homepage
http://www.safecomprogram.gov/SAFECOM/

PSCR program homepage
http://www.pscr.gov/

Anna Paulson-PSCR Engineer
apaulson@its.bldrdoc.gov

DJ Atkinson-PSCR Engineer, Project Lead
dj@its.bldrdoc.gov

Thank you!