NPSTC Broadband Task Force
Operations Working Group

Required and Desired Applications

17 Aug 2009 – V2

This document describes required and desired applications identified by the Operations Working Group of the NPSTC Broadband Task Force.

Make comments for update of this document to Dan Hawkins, Operations Working Group chair, dan.hawkins@search.org.

Change log:

- Version 1 (V1) - First working draft.
- Version 2 (V2) – Second working draft with changes discussed during August 11 and August 12 conference calls of the working group.

Table of Contents

Short Title
Internet Access

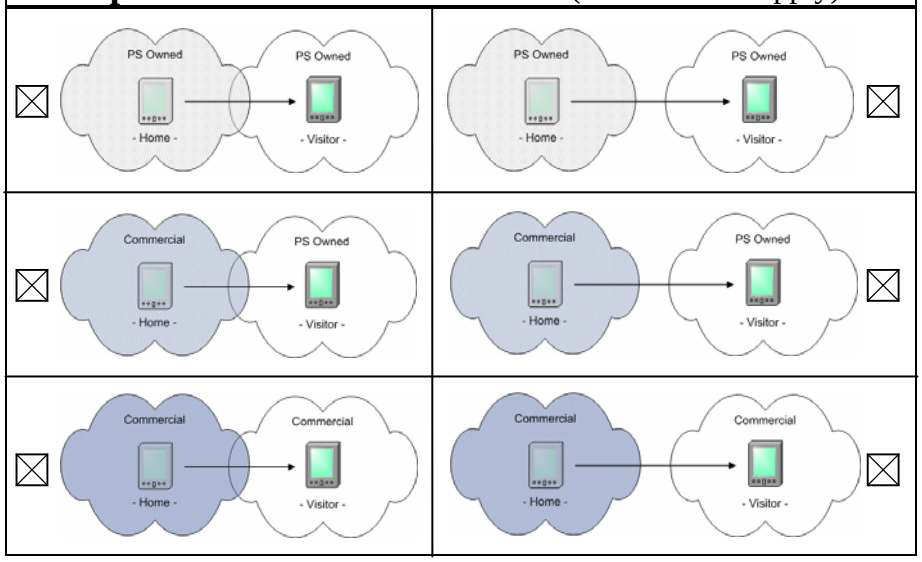
Submission Date: 8/7/2009

Submitter(s): Gabe Elias, Joe Ross

Source
Title: 2007 Broadband SoR
Section/Citation: Section 2.6, Item # 12

Basic Operational Scenario
Select: Any Use

Operational Service Scenarios (check all that apply)



Contents

Public Safety subscribers shall have access to the global Internet. Users will use the Internet both as a way to access home network systems and to access other systems and services available over the public Internet, including but not limited to messaging systems and web servers.

Applicability/Analysis

A Public Safety user arrives for mutual aid during a disaster recovery and uses the visited 700 MHz broadband network to access the visited state's web-based EOC management site, a publicly available traffic camera web site, home-network e-mail system to correspond, and sets up an IP voice and video conference with a distant incident command post to coordinate activities. Various types and volumes of IP traffic are transported to and from the public Internet by the 700 MHz subscriber device.

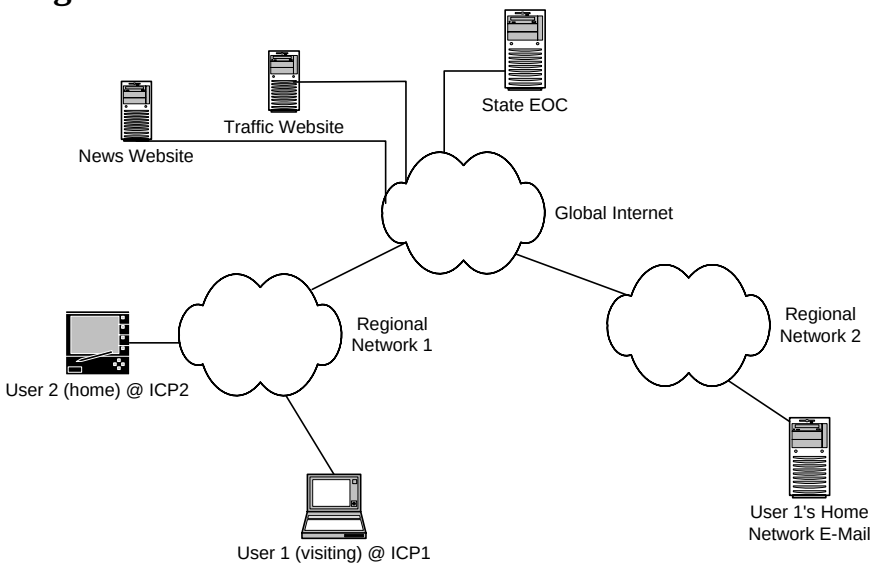
Suggested Language for Concept of Operations Document

While network operators (Public Safety, commercial or Public/Private Partnership) may engage in some traffic shaping and traffic or content filtering for network protection purposes, the subscriber should expect broadly open access to the global Internet on home or visited 700 MHz broadband networks. Network operators shall make every effort not to filter traffic unless necessary for security of systems. For example, Public Safety or Public/Private Partnership network operators should not restrict VoIP traffic. Network operators shall publish in a secure manner their particular network restrictions to the PSST so that public safety users understand network or application limitations and appropriate configurations. (These notifications apply to public Internet traffic and do not require agencies to publish internal firewalling information.)

Other Notes

Working Group Resolution

Diagrams


State EOC
Traffic Website
News Website
Global Internet
Regional
Network 1
Regional
Network 2
User 2 (home) @ ICP2
User 1's Home
Network E-Mail
User 1 (visiting) @ ICP1

Short Title
VPN Access To Home Networks v2

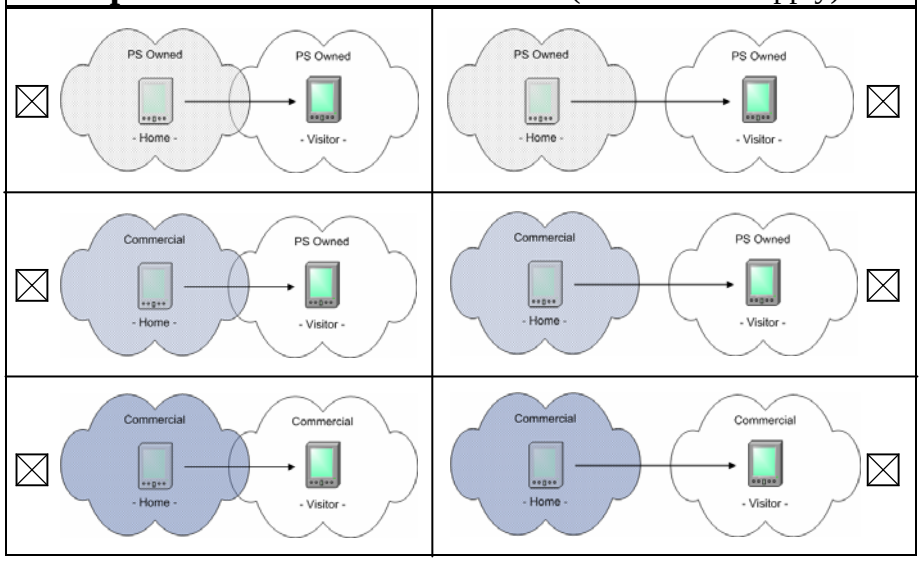
Submission Date: 8/9/2009

Submitter(s): Dan Hawkins

Source
Title: ~BBTF Ops WG
Section/Citation: N/A

Basic Operational Scenario
Select: Routine or Incidental Use

Operational Service Scenarios (check all that apply)



Contents

This is a statement of requirement for wireless broadband network operators to allow roaming users to set up and use virtual private networks (VPNs) between their devices and their home networks.

Applicability/Analysis

Public safety and other public sector users of wireless broadband networks require access to home networks and applications while roaming on other public and commercial networks. Virtual private networks are commonly used to logically extend home networks and provide security for information traversing untrusted networks. U.S. criminal justice agencies accessing Federal Bureau of Investigation (FBI) Criminal Justice Information System (CJIS) Division systems, such as the National Crime Information Center (NCIC) and criminal records systems, are subject to the particular security requirements that commonly lead to the use of VPNs.

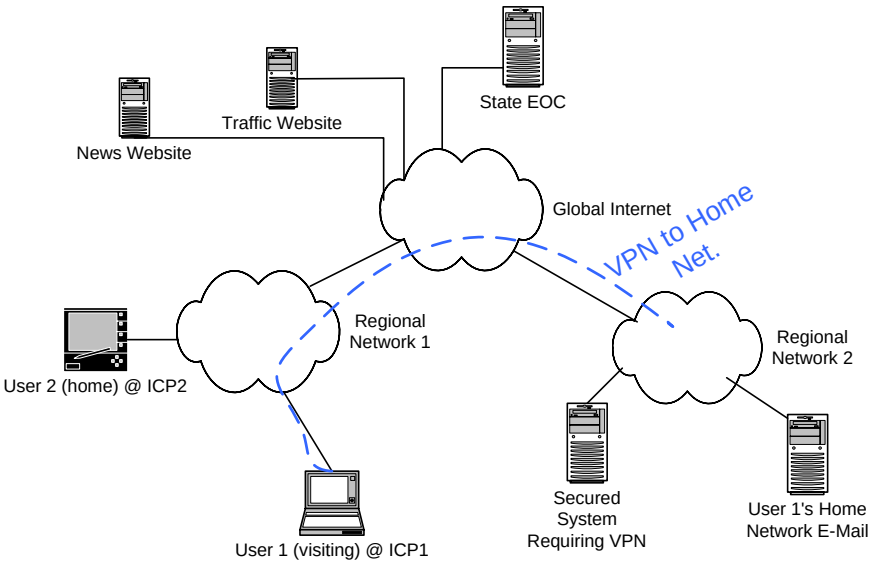
Suggested Language for Concept of Operations Document

Regional sublicensee and commercial networks operating in conjunction with the Public Safety Broadband Licensee (PSBL) shall be required to allow establishment and use of virtual private network (VPN) connections by roaming users on their networks to other networks.

Other Notes

Working Group Resolution

Diagrams


State EOC
Traffic Website
News Website
Global Internet
VPN to Home Net.
Regional Network 1
Regional Network 2
User 2 (home) @ ICP2
User 1 (visiting) @ ICP1
Secured System Requiring VPN
User 1's Home Network E-Mail

Short Title
Status/Information "Homepage"

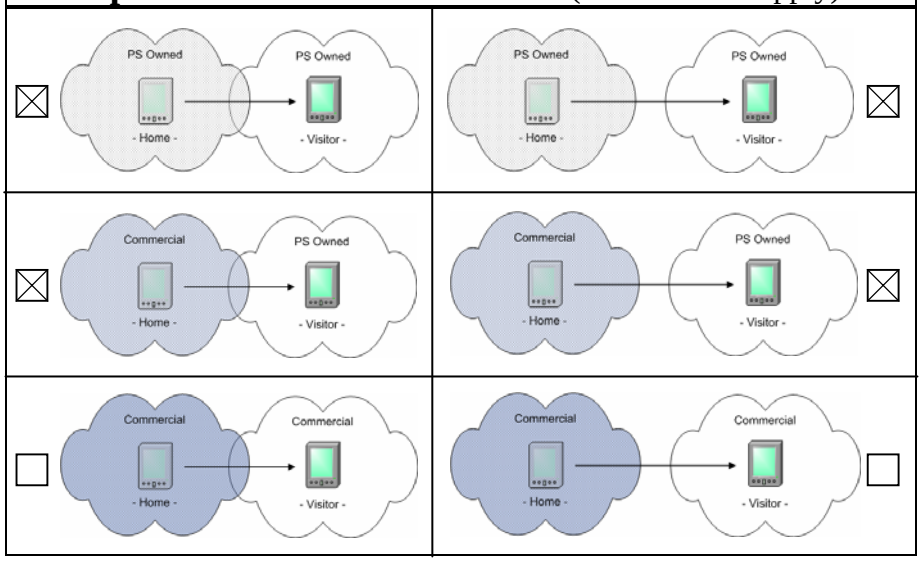
Submission Date: 8/7/2009

Submitter(s): ~BBTF Ops WG
(Gabe Elias, Joe Ross)

Source
Title: ~ BBTF Ops WG
Section/Citation:

Basic Operational Scenario
Select: Any Use

Operational Service Scenarios (check all that apply)



Contents

Public Safety or Public/Private Partnership network operators shall provide a universal method to obtain a "home page" for visitors to the system. This "home page" will facilitate acces to and distribution of available applications, alerts, incident-specific information, system status information, and information that the operator deems important to share with visitors to the system. Federated authentication could be used to allow for online resource registration (Example: user arrives and registers as urban rescue tech,) including announcing to Incident Command who the user is and what equipment/resources he or she has on hand.

Applicability/Analysis

A Public Safety user arrives on a visited network while responding for mutual aid operations. She opens her browser and automatically accesses an informational welcome page which provides general information and the ability to input credentials for authentication. The page may also warn of specific safety hazards on main roads in the area. Information provided after authentication may include such items as interoperable radio frequency, ICS facility locations, command assignment and may also allow input of NIMS-compliant resource typing. A web page provides operational information and allows further access or input based on credentials.

Suggested Language for Concept of Operations Document

Users visiting a network will need a simple and universal way to obtain basic information. The method for reaching this home page should be straightforward and the same across networks. In addition to displaying basic information about the network itself, this page can and should be used to list available applications, incident information and updates, AMBER alerts and so on. Some information may be on a need-to-know basis and should be protected by credentials issued to the visitor by the visited agency. As new incidents develop, network operators may re-capture users for updates.

Other Notes

Working Group Resolution

Diagrams

Short Title
Status/Information "SMS-MMS Messaging"

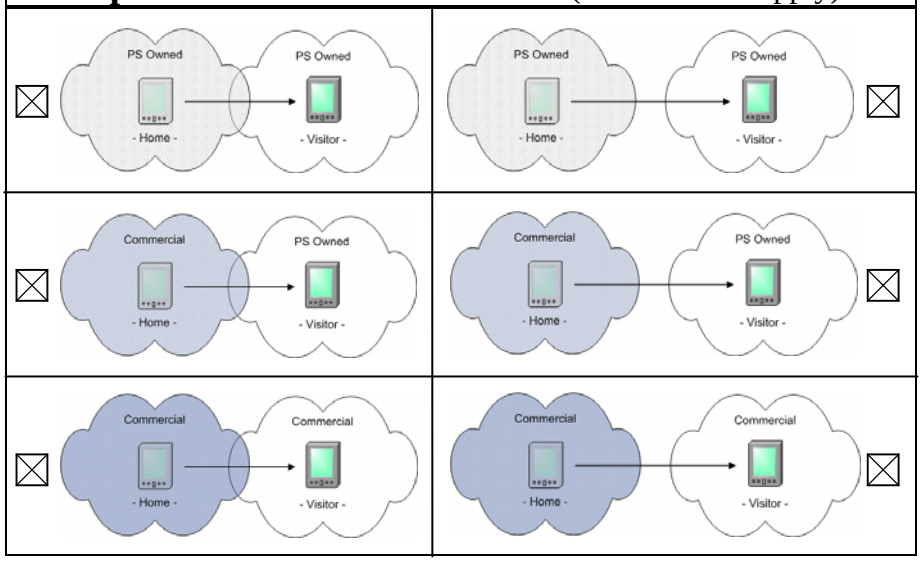
Submission Date: 8/7/2009

Submitter(s): ~BBTF Ops WG

Source
Title: ~ BBTF Ops WG
Section/Citation:

Basic Operational Scenario
Select: Any Use

Operational Service Scenarios (check all that apply)



Contents
Public Safety, Public/Private Partnership, and Commercial network operators shall provide the ability for users to send and receive SMS and MMS messages.

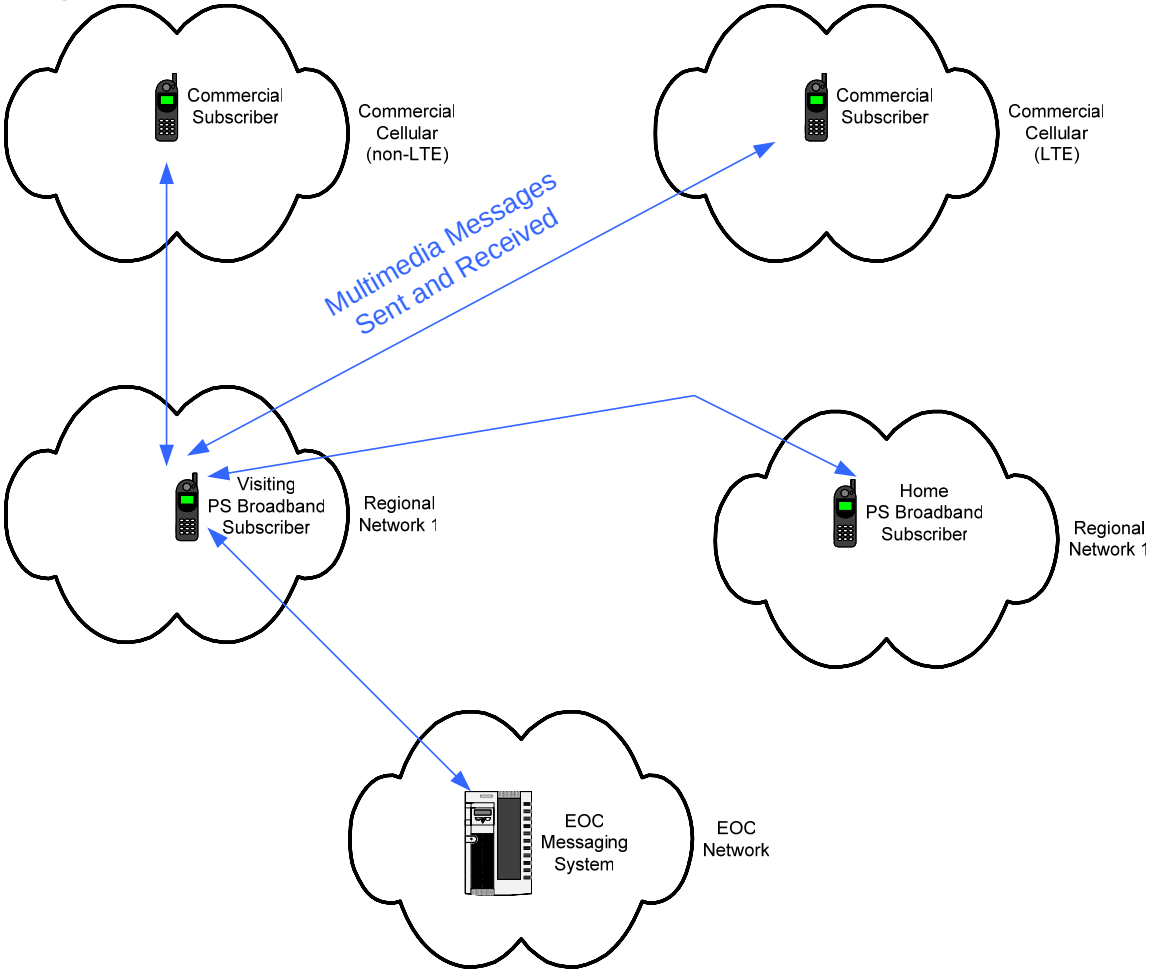
Applicability/Analysis
A Public Safety user arrives on a visited network while responding for mutual aid for disaster recovery. She is able to receive text messages providing status updates on staging locations and voice radio assignments. Once on the scene, she is able to take photographs of damaged infrastructure and send them to the local EOC. She also exchanges multimedia messages with support staff who utilize commercial cellular phones on commercial networks run by various carriers.

Suggested Language for Concept of Operations Document
The ability to send and receive SMS and MMS messages on commercial networks is presently accepted as standard service of commercial data networks. This capabilty should also be provided on the nationwide network by all network providers.

Other Notes

Working Group Resolution

Diagrams


Commercial Subscriber
Commercial Cellular (non-LTE)
Commercial Subscriber
Commercial Cellular (LTE)
Multimedia Messages Sent and Received
Visiting PS Broadband Subscriber
Regional Network 1
Home PS Broadband Subscriber
Regional Network 1
EOC Messaging System
EOC Network

Short Title
Location Based Data Capability

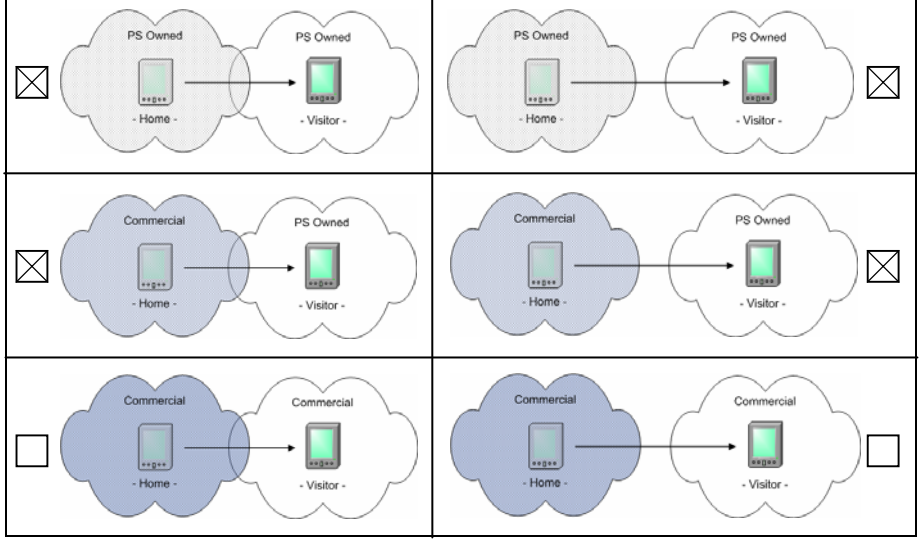
Submission Date: 8/11/2009

Submitter(s): Ron Haraseth

Source
Title: ~ BBTF Ops WG
Section/Citation: N/A

Basic Operational Scenario
Select: Any Use

Operational Service Scenarios (check all that apply)



Contents

Location based data information is the fundamental geo-spatial data information indicating the physical location of a subscriber unit in real time. The network administrator may use any technical means to provide location based data as may be appropriate for their specific network as long as the method meets the appropriate functionality of this capability.

Applicability/Analysis

Location identification technology is proving to be an invaluable tool for managing mobile fleets. In the public safety LMR role, it is referred to as AVL used to track and manage a mobile work force. In commercial services, it is referred to as Location Based Services to generate Wireless Enhanced 9-1-1 location status and additionally has many other commercial applications. Location is typically developed by subscriber device initiated GPS reception and/or infrastructure based location support. Location identification capability will have a large base of application possibilities ranging from subscriber unit navigation to personnel/equipment tracking and management. Location services have a significant safety-of-user component as well as utilitarian management applications. Location data access needs to be managed by either the subscriber unit or agency application in order to address security concerns.

Suggested Language for Concept of Operations Document

National and/or regional networks should include the capability to collect and convey subscriber unit location data in real time. The technical ability to covey location information should be inherent on any PS network and associated commercial networks. Location data should be accessible to appropriate applications, as may be authorized by management level policy. Location data applications may be located on both subscriber units and associated agency level command/control applications. Subscriber units of future public safety networks should meet the same minimum location data information requirements (format and accuracy) as is currently applicable on current commercial services networks in order to retain a broad level of compatibility with incumbent systems.

Other Notes

Working Group Resolution

Diagrams

Short Title
LMR Gateway Devices

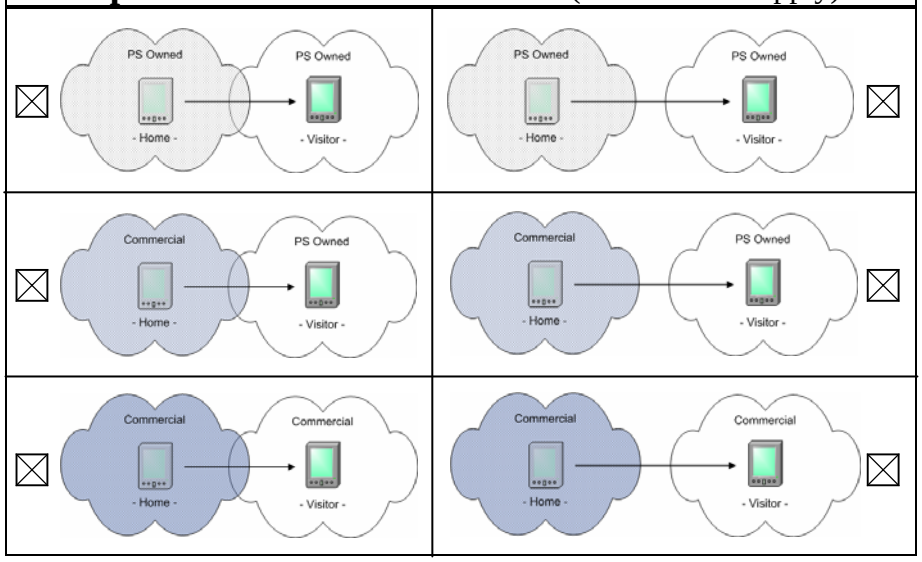
Submission Date: 8/7/2009

Submitter(s): Gabe Elias, Joe Ross

Source
Title: ~ BBTF Ops WG
Section/Citation:

Basic Operational Scenario
Select: Any Use

Operational Service Scenarios (check all that apply)



Contents
Networks shall allow for connection and operation of IP-based voice interoperability gatways.

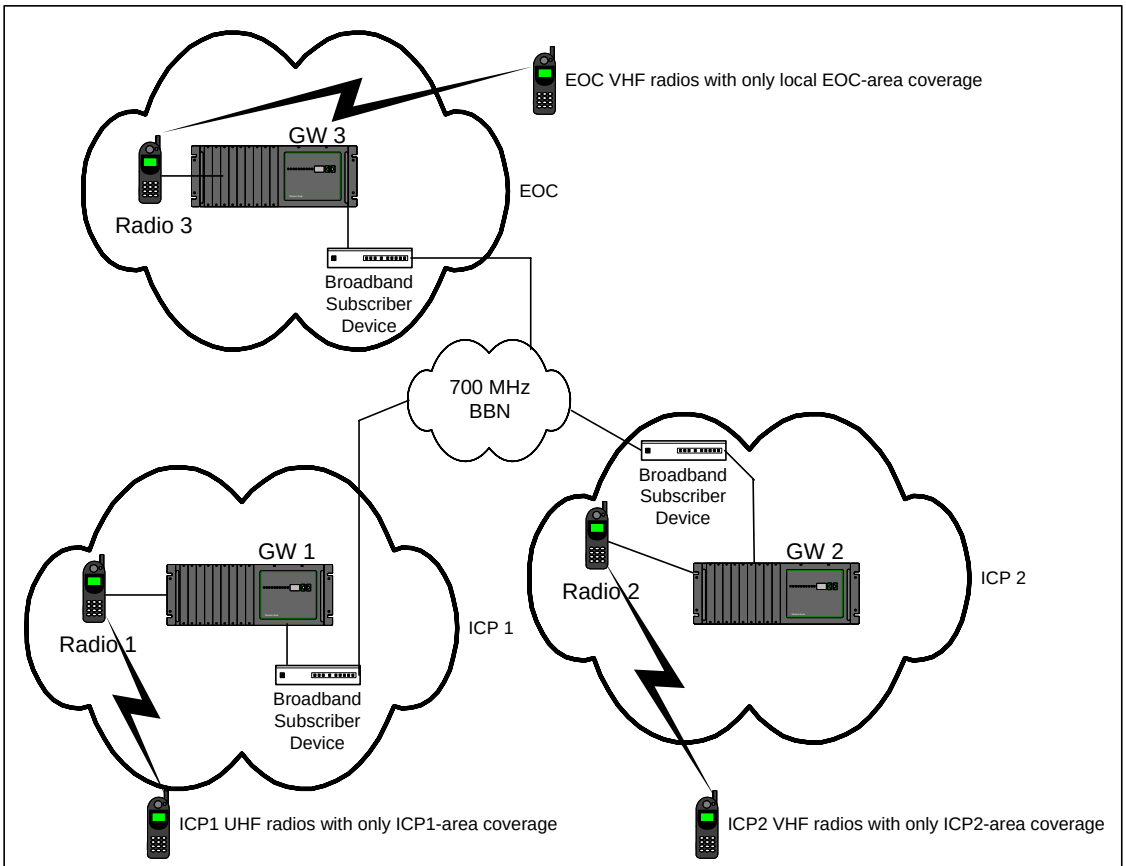
Applicability/Analysis
A large portion of a region's voice radio system is knocked out by a hurricane, though the 700 MHz broadband network is still operational. Multiple incident commands and an EOC are brought up around the area and are staffed by local responders and large numbers of out-of-area mutual aid responders. Each Incident Command Post (ICP) has established local communications but the ICPs and EOC cannot talk to each other. IP-based LMR gateways are brought to each ICP and the EOC and are connected to each other over the 700 MHz broadband network to provide overall command and control communications. (The LMR gateway is brought to a command post and connected by Ethernet to a 700 MHz subscriber. VoIP traffic carries audio from the disparate radio systems back and forth over the IP network.)

Suggested Language for Concept of Operations Document
A mutual aid responder should be able to field-deploy an IP-based voice gateway (Example: Raytheon ACU-2000, Sytech RIOS) to bridge disparate voice systems (Example: LMR systems on different frequency bands or trunking architectures) using the 700 MHz broadband network as some portion of the IP connectivity between gateways. The gateway should be capable of being contacted in any visiting location, i.e. use a static IP. The gateway will require a 700 MHz subscriber device to provide an Ethernet port. The setup shall be simple and the authentication and flow of information shall be transparent to the user.

Other Notes

Working Group Resolution

Diagrams



Disparate local-only radio systems bridged using 700 MHz broadband network as backhaul connectivity

Short Title
Access by Responders Under ICS

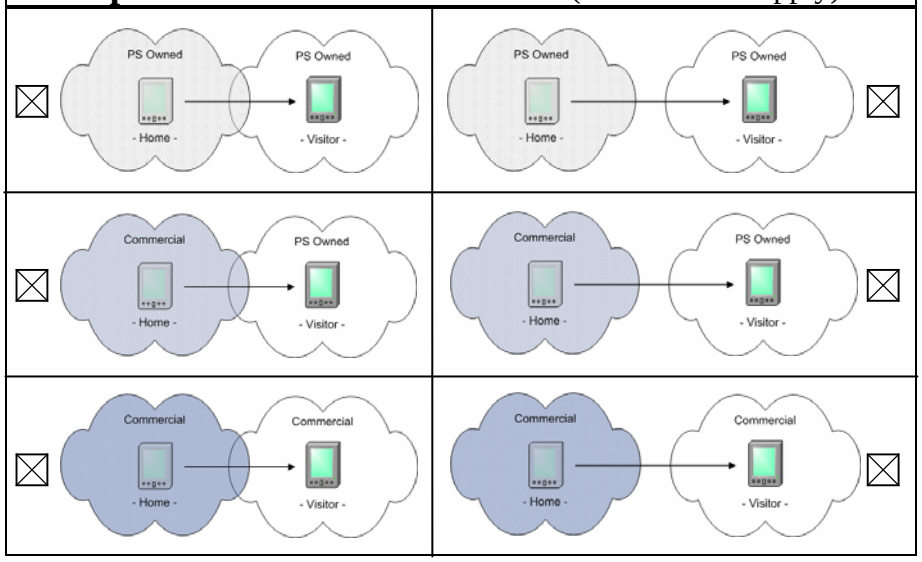
Submission Date: 8/17/2009

Submitter(s): Dan Hawkins

Source
Title: ~BBTF Ops WG
Section/Citation: N/A

Basic Operational Scenario
Select: Mutual Aid Use

Operational Service Scenarios (check all that apply)



Contents
This is a statement of requirement for wireless broadband network operators to allow access to all users responding in mutual aid to the visited region who operating under a defined NIMS ICS structure.

Applicability/Analysis
Responders in mutual aid to agencies served by public safety broadband networks need access to the network to carry out their responsibilities and communicate with the agencies served. The National Incident Management System (NIMS) Incident Command System (ICS) provides a logical framework for command, control, and communications that can be used to determine information nodes and flows. All responders falling within the ICS structure defined for the mutual aid incident may need access.

Suggested Language for Concept of Operations Document
All mutual aid responders managed under the ICS structure of a requesting agency served by a public safety broadband networks shall be provided access to that network to carry out incident objectives and communicate with their home networks.

Other Notes

Working Group Resolution

Diagrams

Short Title
Ambulance Roaming

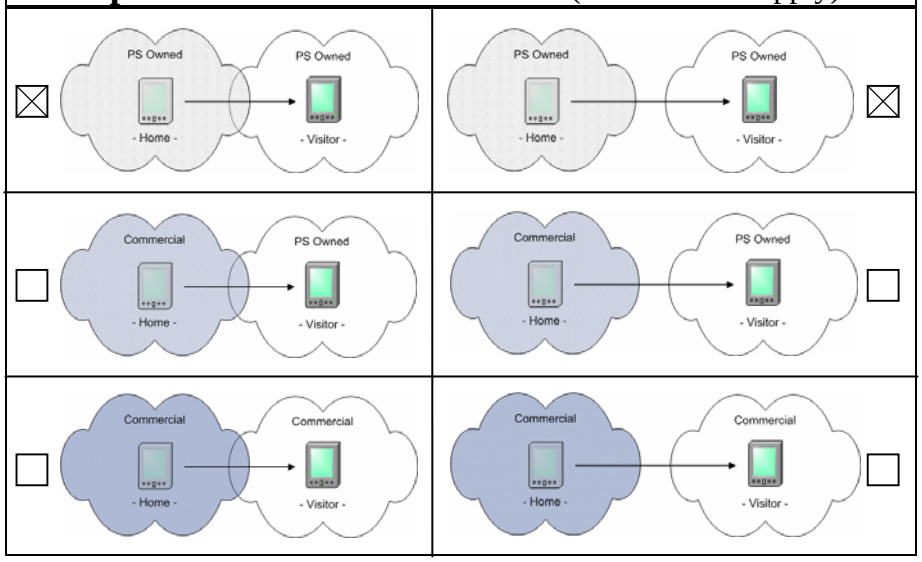
Submission Date: 8/12/2009

Submitter(s): Kevin McGinnis

Source
Title: SafeCom SoR Vol. 1 Ver. 1.2
Section/Citation: Section 3.2.3 steps 8-10

Basic Operational Scenario
Select: Routine or Incidental Use

Operational Service Scenarios (check all that apply)



Contents
Ground and air ambulances routinely transport patients through multiple jurisdictions and past multiple hospitals. Patient telemetry and other apps requiring BB capacity should be able to be sent to the destination hospital as well as other hospitals en route that may need to be communicated with if a patient emergency arises.

Applicability/Analysis
Standardized access methodology should exist for ambulance roamers to connect to regional hospitals in "roam through" transports and in "roam in" mutual aid circumstances.

Suggested Language for Concept of Operations Document
Ambulances from outside a region should be able to have BB access in a nationally standardized fashion to hospitals in that region for emergency consultations when going from a point outside the region to another point also outside the region and "roaming through", or when "roaming into" the region from outside for the purpose of bringing a patient to a hospital in the region or operating per a mutual aid request from inside the region.

Other Notes

Working Group Resolution

Diagrams

Short Title
One-To-Many Communications Across All Media

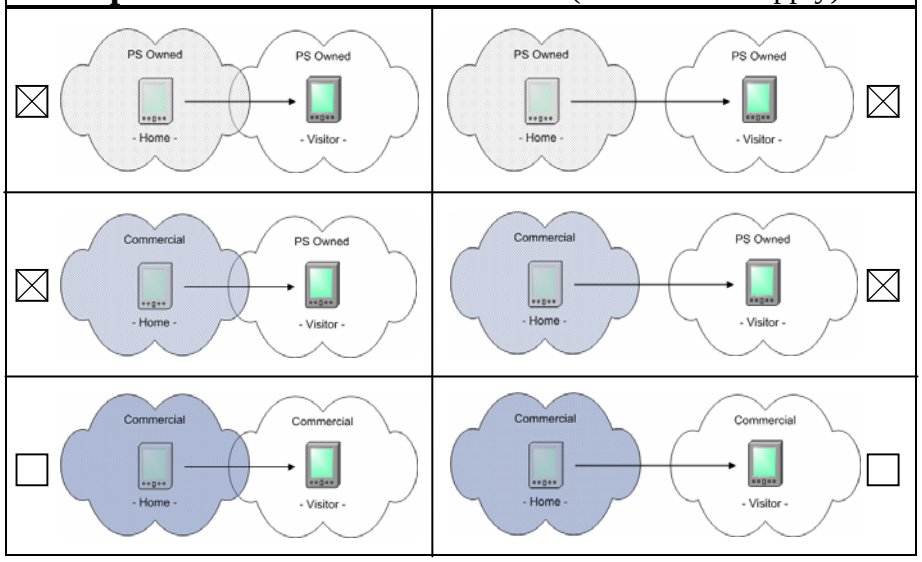
Submission Date: 8/9/2009

Submitter(s): Dan Hawkins

Source
Title: ~BBTF Ops WG
Section/Citation: N/A

Basic Operational Scenario
Select: Mutual Aid Use

Operational Service Scenarios (check all that apply)



Contents
This is a statement of requirement for wireless broadband network operators to provide one-to-many communications capabilities to across all media to users of the network providing mutual aid.

Applicability/Analysis
First responders and other emergency response support personnel rely on the one-to-many communications provided by traditional land mobile radios. As responders increasingly rely on other media of communications, the need for one-to-many exchanges continues. Jurisdictions have an obligation to provide communications services to responders providing them mutual aid. For purposes of scope, a video broadcast to up to 10 simultaneous receiving users at the scene of an incident is estimated as the practical maximum one-to-many usage expectation. Simultaneous receipt of video means that all recipients are able to see the same image at the same time.

Suggested Language for Concept of Operations Document
Regional sublicensees should provide one-to-many communications capabilities to outside network users responding in mutual aid to the sublicensee. These communications capabilities should extend from voice, as commonly used in traditional land mobile radio systems, to text messaging, to video, and other forms of data communications.

Other Notes

Working Group Resolution

Diagrams

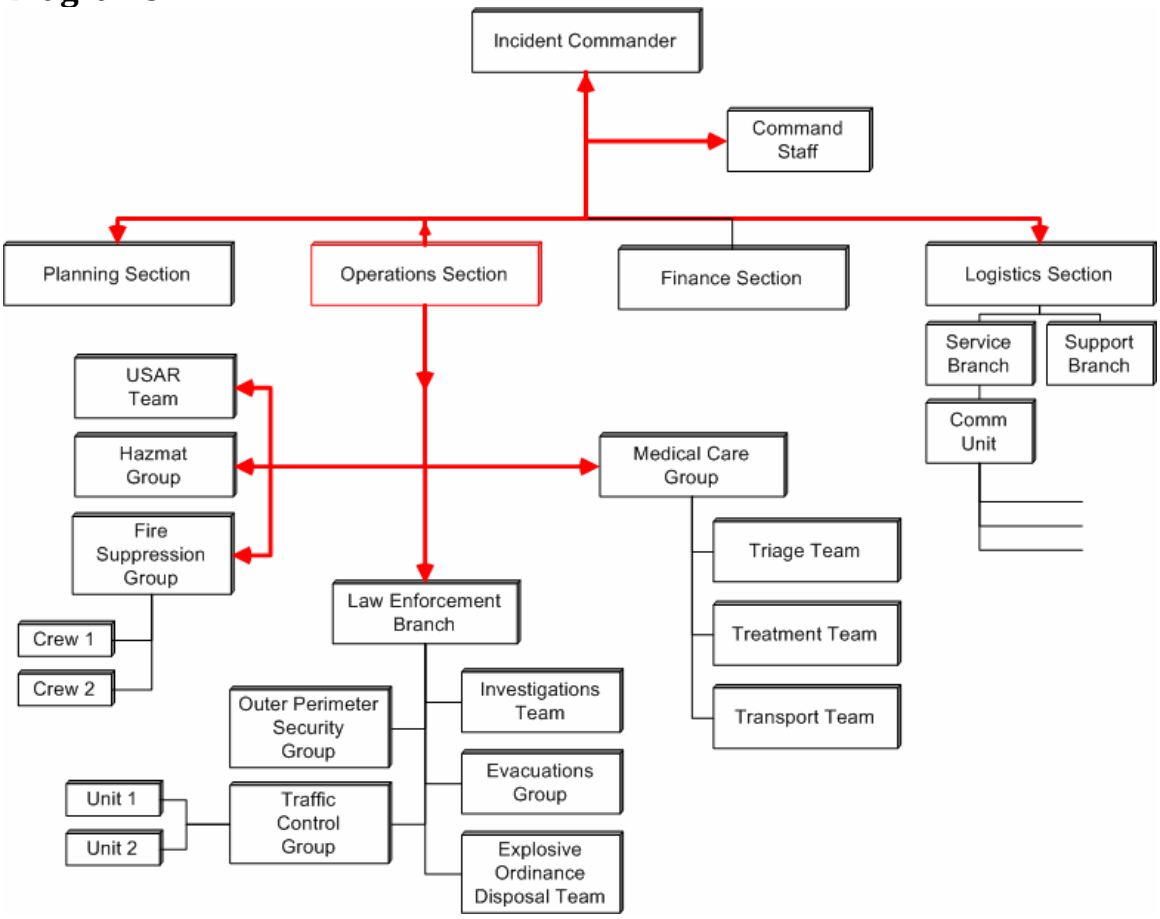


Figure 1 - Logical Information Flow During a Hypothetical Incident (one use case)
Flow is from the Operations Section Chief to the indicated general staff, command staff, team leader, group supervisors, and branch directors. No depiction of physical transmission flow is intended.

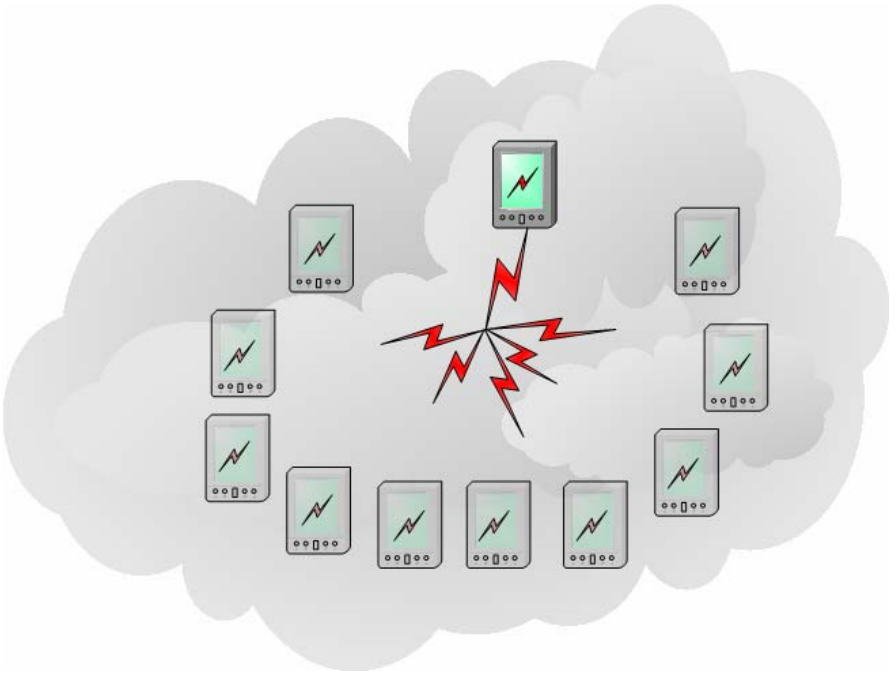


Figure 2 - Notional Information Flow Depicting Video Transmission from One Source and Simultaneous Receipt at Ten Others

Short Title
LMR Voice

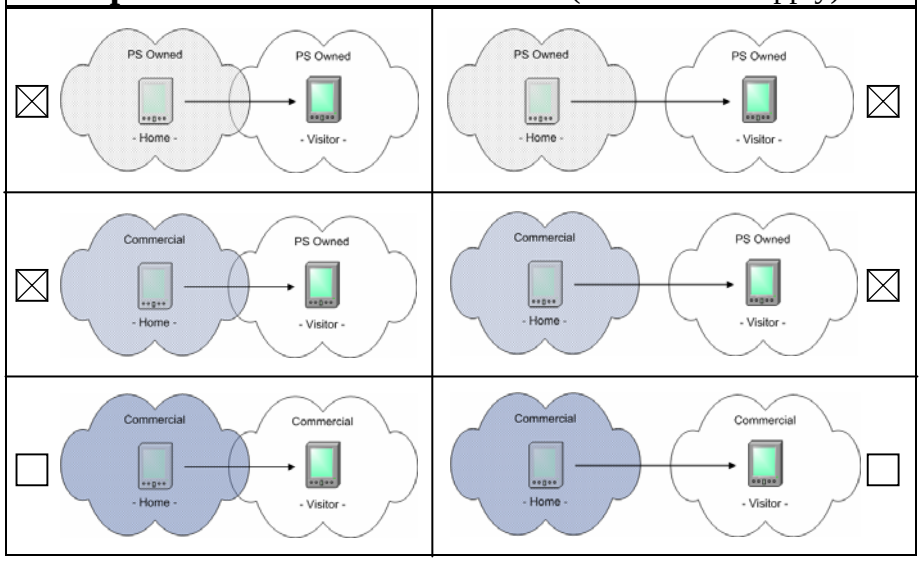
Submission Date: 8/9/2009

Submitter(s): Gabe Elias, Joe Ross

Source
Title: 700 MHz SoR
Section/Citation: 2.6 - Items 1& 2

Basic Operational Scenario
Select: Any Use

Operational Service Scenarios (check all that apply)



Contents

Public Safety or Public/Private Partnership networks which provide voice service as an application should (but are not obligated to) provide voice interoperability interfaces to existing agency LMR systems in the area served by the 700 MHz Broadband Network. Public Safety users on such home or visited networks should be able to call or hail an authoritative dispatch agency or control point using the 700 MHz subscriber device with microphone and speaker for two-way audio and talk or be connected to other serving agency voice communications resources.

Applicability/Analysis

A responder arrives in a 700 MHz broadband area for mutual aid and connects to the Public Safety network with a handset. He calls the universal "hailing" number/channel and requests assignment and asks to be patched to the incident command assignment channel/talkgroup for further instruction. The 700 MHz broadband subscriber with microphone and speaker for two-way audio places a cellular voice call to a universal “hailing” number or destination to reach a dispatch center and is later patched to the agency LMR system for voice interoperability.

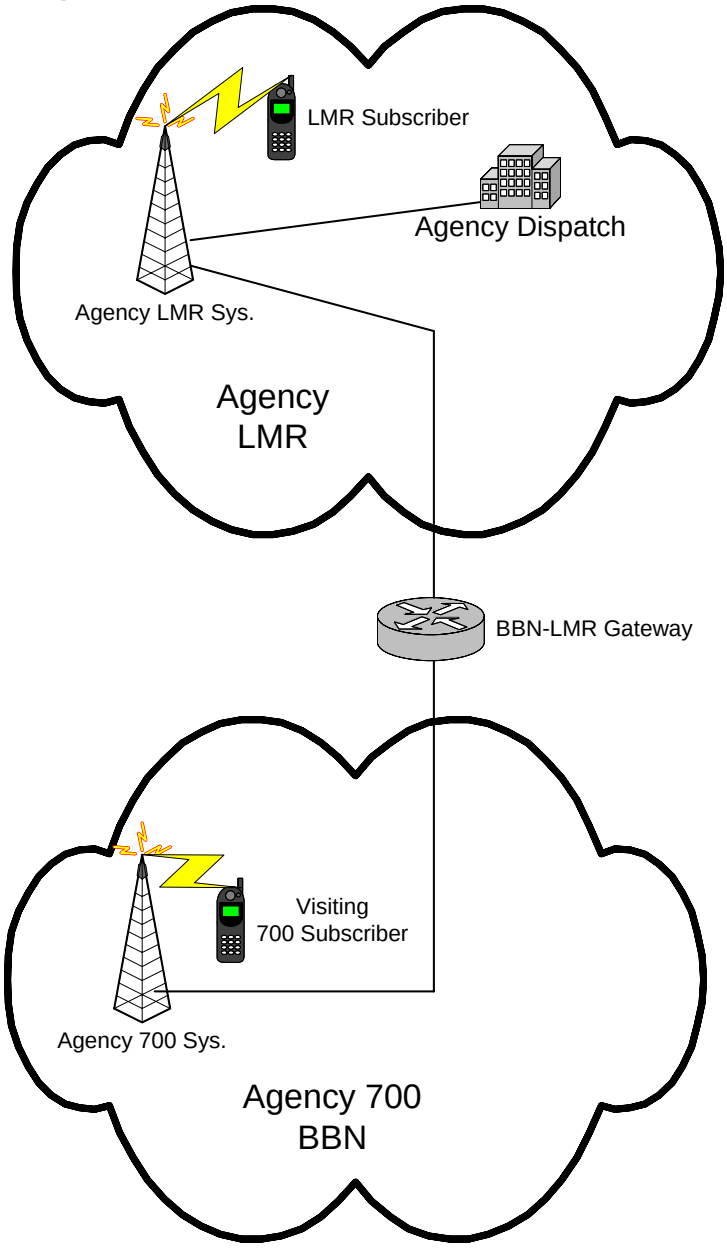
Suggested Language for Concept of Operations Document

Different than the "LMR Gateway" interface, this should provide a fixed interface to agency LMR systems such that 700 MHz subscribers with voice service can be connected or "patched" to existing agency voice radio networks for communications interoperability. As with the existing 800 MHz national calling channel, an authoritative dispatch agency should monitor any calling channel/number provided by the 700 MHz broadband network. Operators may restrict visiting users to only specific hailing/calling channels until further authorization by the control point. Operators may further restrict certain groups or classes of users to a listen-only mode if appropriate. While this interface is not obligatory, it is imperative we come up with a national, interoperable solution such that this functionality works the same in every network.

Other Notes

Working Group Resolution

Diagrams


LMR Subscriber
Agency Dispatch
Agency LMR Sys.
Agency
LMR
BBN-LMR Gateway
Visiting
700 Subscriber
Agency 700 Sys.
Agency 700
BBN

Short Title
PSTN Voice

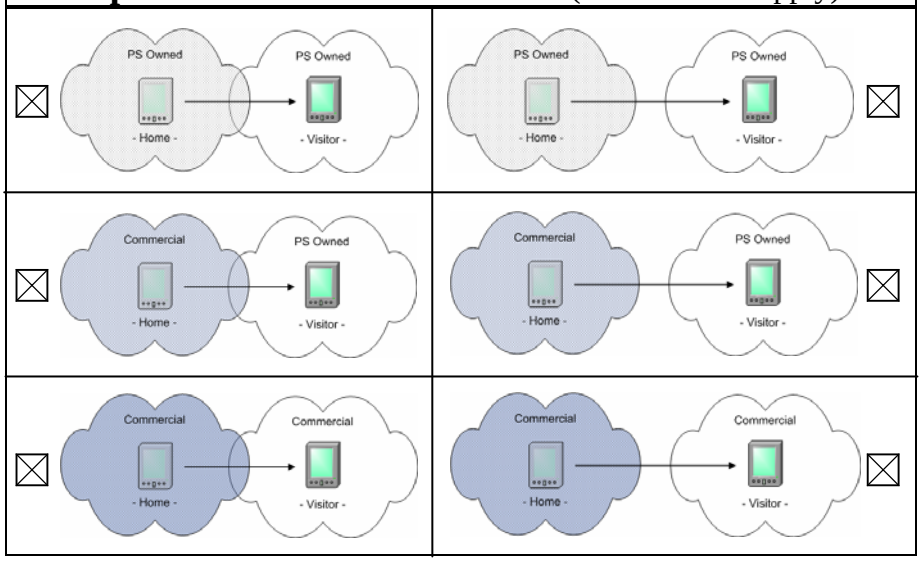
Submission Date: 8/9/2009

Submitter(s): Joe Ross, Gabe Elias

Source
Title: 2007 Broadband SoR
Section/Citation: Section 2.6, Item # 3, 5, 6 and 3.2, Item # 4 and 8

Basic Operational Scenario
Select: Any Use

Operational Service Scenarios (check all that apply)



Contents

Public Safety subscribers shall have access to the global Public Switched Telephone Network and it's full-duplex voice capabilities. When a public safety user roams in to a visited network, the public safety user shall have access to voice telecommunications services using commercially available cell phone like devices. This includes the ability to place and receive phone calls while in the visited network. The network operator shall make reasonable efforts to provide good audio quality on the network and it is recommended to block or queue calls in the event that network resources can not sustain a good call. The visited network is not required to provide these voice services; only provide the conduit for them to be successfully delivered in visited region.

Applicability/Analysis

It is acknowledged that the devices and/or network capabilitiy may not be available on the outset of 700 MHz service due to the business plans of the commercial carriers operating at 700 MHz. In advance of this, it is expected that public safety voice needs will be met using a variety of proprietary or open source non-mobile based VoIP solutions. When the commercial market does mature to allow for such devices using 700 MHz LTE, the public safety devices should accommodate nationwide voice roaming and do so in an interoperable manner. It is acceptable to implement this capability in the same manner that the cellular carriers implement the feature, including, if necessary, using 2G/3G voice networks. In that case, however, the regional network shall be required to redirect the LTE user to a 2G/3G network capable of supporting local voice capabilities.

Suggested Language for Concept of Operations Document

Public safety 700 MHz voice capable devices such as cell phones, PDAs, or their equivalent shall be capable of placing and receiving full-duplex telephone calls to any telephonic device on the Public Switched Telephone Network (PSTN) in the visited network with the same functionality that cellular telephones operate nationally today. This includes location based PSAP call routing, E911 Phase II location transmission, and, if necessary CALEA. In the case where the user transitions in to or out of one regional system, the voice session shall be handed off between the two networks with limited loss of audio during the transition. Because the devices and device capabilities for this feature will develop over time, this feature is a future requirement.

Other Notes

Working Group Resolution

Diagrams

Short Title
Field-Based Server Application

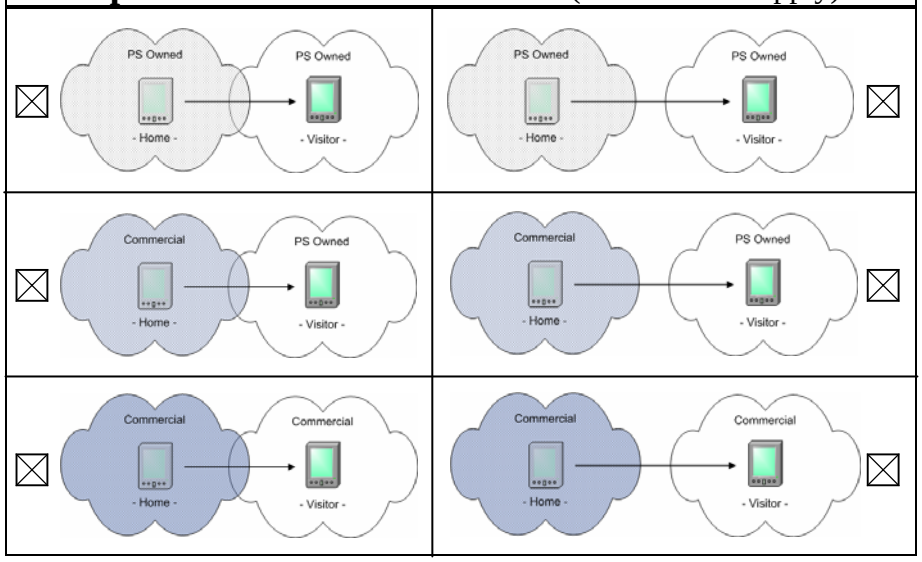
Submission Date: 8/12/2009

Submitter(s): Joe Ross

Source
Title: ~ BBTF Ops WG
Section/Citation:

Basic Operational Scenario
Select: Mutual Aid Use (but routine may be possible)

Operational Service Scenarios (check all that apply)



Contents
The 700 MHz regional broadband systems shall support the use of field-deployed server applications. This requirement includes the need for client devices to consistently and continuously reach these server based systems from any other location on the Internet. The capability is not required for every subscriber device on the 700 MHz broadband network but is limited to a subset of the users that actually require such a feature.

Applicability/Analysis
A public safety user may need to deploy an application for which other client devices will need to find the application server for that service where the server is deployed anywhere on the 700 MHz broadand network and the clients (or other servers) are located anywhere on the Internet. In other words, the visiting network must be capable of the equivalent of a static IP address that is reachable from any public IP address (while this is not the proscribed solution, it is merely included as an example of an acceptable solution). A variety of scenarios exist where this feature could become required. For example, a mutual aid agency could field-deploy its command bus that is equipped with email, VoIP, video, and web servers to faciliate communication at a major incident. These applications would need to be reachable by their respective clients.

Suggested Language for Concept of Operations Document
The 700 MHz broadband public safety systems must support the field-deployment of application servers. The servers will likely be deployed as part of a mutual aid operation whereby applications are delivered as part of the overall emergency operations (e.g., a command vehicle serving email). In order for incident client devices to be able to communicate with these servers, the system must support a method for them to communicate with the server anywhere on the national 700 MHz broadband network and while the devices are anywhere on the Internet. It is anticipated that servers will consist of the majority of cases where this capability is needed, however, it is possible that other scenarios may necessitate consistently reachable client devices. Therefore, the system should provide such capability to any subscriber device requiring such capabilities be it a subscriber that provides connictivity for a server or client. It is not required that all devices shall have this capability.

Other Notes

Working Group Resolution

Diagrams