
Communications Interoperability Incident Area Network Gateway:

An Effective Approach to Fill Gaps in Statewide Plans and
Advance Public Safety Along the Interoperability Continuum

National Association of State Fire Marshals



Summary: The lack of effective, reliable and interoperable emergency communications is a risk to emergency responders whenever two or more public safety agencies or different jurisdictions respond to incidents across all hazards. Statewide networks are steps in the right direction; they are long-term solutions that will take years to implement. However, they still won't resolve the challenge of communications operability and interoperability at the scene of incidents, or in the event that communications infrastructure is damaged.

The purpose of this document is to outline the functional characteristics of a new and readily available technology solution that achieves reliable incident-level communications urgently needed by emergency responders today. The language in this document can easily be incorporated to fill gaps in Statewide Communications Interoperability Plans. This approach can also be cost effectively leveraged for Investment Justifications under the Public Safety Interoperable Communications (PSIC) grant program and other funding opportunities. NASFM is currently working with several states to maximize the effectiveness of this approach at regional and statewide levels. NASFM is available to provide similar support to other states on a limited basis.

1 General Needs Statement

The Department of Homeland Security (DHS) Office has required each state to create a Statewide Communication Interoperability Plan (SCIP). The SCIP is intended to document both the operational aspects of the states' existing interoperability communication resources as well as their strategic vision moving forward. As each state develops their strategic vision for the future, they are identifying technology that is currently available as well as working with industry to identify technology that will be available within the next year or two.

2 Technology Assessment

SAFECOM defines communication interoperability as the ability of public safety agencies to talk across disciplines and jurisdictions via radio communication systems, exchanging voice and/or data with one another on demand, in real time, when needed, and as authorized. SAFECOM has designated four basic types of equipment that can be utilized to achieve communication interoperability. These are:

- Swap / cache radios
- Shared Channels
- Gateways
- Shared Systems

U.S. Department of Homeland Security¹ defines gateways as:

“Gateway systems provide connections between two or more radio networks, allowing users on one network to communicate with users on other networks. For example, a group of users on an ultra-high frequency (UHF) channel used by Agency A can be connected to a group of users on a very-high frequency (VHF) channel used by Agency B. An interconnection is created by connecting two or more radio channels or voice paths with a gateway device or console patch. Gateway systems can be configured to support any number of channels. Using gateway systems, usually graphical user interface, a dispatch operator can select the appropriate channels to interconnect. With many gateways, multiple interconnect sessions involving distinct groups can be established at any given time by the gateway operator. The maximum number of simultaneous interconnect sessions in progress depends on the gateway system.”

Gateways can be fixed, mobile and incident area network based. Mobile and incident area network gateways address coverage gaps and are used to provide redundant coverage even during natural and man-made disasters. Mobile gateways are currently staged in selected locations so that they can be called for and deployed within a reasonable time. Incident area network gateways are the next generation gateways that utilize the temporary incident area network that is automatically established at the incident scene as the transport medium for voice interoperability. In addition to supporting voice interoperability, the incident area network will also be able to provide the responders with video, geolocation information, telephony, video conferencing, instant messaging, database translations,

¹ U.S. Department of Homeland Security Office of State and Local Government Coordination and Preparedness [“Tactical Interoperable Communications Planning Guidance and Template defines Gateways”](http://www.ojp.usdoj.gov/odp/docs/TICPGuidanceandTemplate.pdf) (<http://www.ojp.usdoj.gov/odp/docs/TICPGuidanceandTemplate.pdf>)

paging, file transfers, and web browsing. Incident-Area Mesh Networks combine the benefits of a traditional gateway with the innovative architecture of a shared system, allowing seamless integration with large multi-state shared voice and data systems. The table below identifies several key features of each type of gateway and each type of gateway should be included in a state's interoperability plan.

Type	Fixed Gateway	Mobile Gateway	Incident Area Network Gateway
Deployment	Fixed infrastructure between agencies	Mobile unit that is transported to the incident area	Mobile unit that is distributed in the responding vehicles
Planning	Interoperability negotiated between responding agencies' dispatch center	Interoperability negotiated in advance between responding agencies represented on scene	Interoperability available at scene immediately and changes negotiated between responding agencies on scene
Availability	Minutes to hours depending on approval process	Hours to days depending on resource availability	Immediately after two or more responding units arrive at the incident scene
Training/ Operation	Specialized trained operator required to setup and manage the gateway	Specialized trained operator required to setup and manage the gateway	Standard operating procedures at the incident scene. Minimal training to establish talk groups.
Mobility	Fixed location and coverage area.	Mobile system that is deployed in task or communication vehicles	Mobile units are deployed in responder's vehicles and automatically configured
Service	<ul style="list-style-type: none"> • Mission-critical real-time, high-interaction voice • Non-mission critical IP telephony and video conferencing. • Signaling for voice 	<ul style="list-style-type: none"> • Mission-critical real-time, high-interaction voice • Non-mission critical IP telephony 	<ul style="list-style-type: none"> • Mission-critical real-time, high-interaction voice • Non-mission critical IP telephony and video conferencing. • Signaling for voice or video conferencing. • Instant messaging and database transactions. • Voice paging, file transfers, geolocation information, and near-real time streaming video. • World Wide Web browser-based Applications

Incident Area Network Gateway: The Incident Area Network Gateway system is a dispersed mobile ad-hoc incident area network gateway (IANG) where each responding agency deploys at least one IANG to the incident scene that is compatible with their existing radio system user devices. When the IANGs arrive at the incident scene they automatically recognize each other, pass pertinent information, and automatically establish an incident area network (IAN) to support communication interoperability. Each IANG dynamically and automatically enters the IAN allowing access to and from all other IANGs in the IAN. Users from each agency with their IANG at the scene can communicate across the IAN to any other Agency via their IANG without concern for the specific radio or frequency each Agency is using.

Incident Area Network Gateway Supports NIMS: The IAN established by the IANGs at the incident scene supports the creation, monitoring and maintenance of talk groups. The Incident Commander, or designated Communications Officer, utilizes talk group capabilities to establish and maintain a single chain of command. This structure greatly enhances Incident Commander and response operations, improving emergency responder life safety.

Incident Area Network Gateway operates during Disasters: The IANG operating on vehicle power provides an interoperability solution even during natural and man-made disasters. IANGs are not dependant on infrastructure (towers and base stations); instead the IANGs connect wirelessly to each other and create an IAN at the incident scene. This IAN is available even though other infrastructure may be damaged, destroyed or inoperable due to a loss of power. This demonstrates the added resiliency and value of the new generation of incident area network technology.

Incident Area Network Gateways bridge legacy and the future technologies: IANGs exist for legacy radios, digital radios, P25 radios and 700MHz radios providing interoperability between all of these device types. It is not necessary to know in advance the user devices that will be deployed for any incident. Each IANG is compatible with the user devices each Agency deploys and all IANGs are compatible with each other. The IAN is automatically created at the incident scene and consists of any IANG that arrives.

As new user devices emerge through technology, compatible IANGs will be available to provide interoperability across all user devices without altering or replacing currently deployed IANGs.

Incident Area Network Gateways Cost Benefit: IANGs are installed in responder vehicles and operate independent of infrastructure. They do not require additional cables or additional radios. Once installed, there are no costs for special purpose vehicles, no cost for additional cables and no cost for additional radios. IANGs are simple to use and do not require special training since they establish the mesh network automatically without interaction. Responders using the IANG follow standard operating procedures to access the interoperability solution. Meanwhile the Incident Commander or Communications Officer establishes and manages talk groups with an easy to use Graphical User Interface.

Incident Area Network Gateways Sustainability: In addition to being cost effective, IANGs provide an interoperability solution for every day use in small incidents requiring few agencies to respond maximizing the utility of the equipment. As an incident grows, requiring additional agencies to respond, the IANG automatically grows with the additional IANGs, scaling to the size of the response required. These factors ensure the approach's financial and operational sustainability.

3 Incident Area Network Gateway Operating Procedure (SOP)

This section provides guidance about the rules of use, how to activate and how to deactivate the mobile IANG system during planned events, training exercises, or emergency responses.

Rules of Use: The following rules of use should govern the use of the incident area gateways:

- Use of an Incident Command System compliant with the NIMS is required for use of any interoperability resource.
 - All radio traffic should be in plain language. The use of 10-codes and specific agency acronyms is discouraged.
-

-
- Agencies will identify themselves by county or agency name and designated call sign/radio designator.
 - All encrypted radio uses will be required to work in the “clear” mode.
 - Agencies are encouraged to work in the simplex mode.

NOTE: Interconnecting encrypted and non-encrypted channels on any gateway can compromise operations or allow sensitive information to be intercepted because it is difficult to ensure all encrypted channel users are aware when they are connected to non-encrypted channels. An encrypted channel user can mistakenly believe that their communication is secure, when in fact the communication is being broadcast in the “clear” over a non-encrypted channel through a gateway connection. For this reason, the default policy will be that encrypted channels will not be used where non-encrypted channels are being interconnected with a gateway.

Interoperable Communications Request: The Incident Commander or designated Communications Officer will determine when a situation exists that requires use of an interoperability resource and notify his/her dispatch center. The following information will be provided by the requesting agency:

- On-scene agencies requiring interoperability
- Reason for request/type of incident
- Expected duration of the request
- Location required
- User / requestor contact phone number
- Availability of Incident Area Gateway

Incident Area Network Gateway Activation: Once confirmation has been made, the responding agency will switch their portable radio to their designated incident area gateway channel and contact the Incident Commander.

The Incident Commander or Communications Officer should follow these procedures in accordance with NIMS:

- Required participating agencies should check in with the command post.
- Assign radio call sign/designator information to the connecting agencies
- Confer with the incident area gateway operator regarding command level or other specific talk groups required.

The Incident Commander or Communications Officer operating the Incident Area Network should follow these procedures:

- Assign the requested unit/agency to that talkgroup as designated by the Incident Commander.
 - If required, adjust vehicle positions with incident area gateway units for optimal incident area network coverage. (i.e. provide operability and interoperability between users on all sides of a building)
-

Network Deactivation: The Incident Commander will determine when interoperable communication is no longer required. Agencies should follow these deactivation procedures:

- The Incident Commander or Communications Officer at the incident shall make an announcement on the incident area network channel indicating that the incident area gateway is no longer needed and that all responders should return their devices to appropriate home system channels.
- All personnel shall return to their appropriate home system channel.

Problem ID and Resolution: Agencies using the incident area networks should report any problems experienced. The Communications Officer will be responsible for ensuring effective resolution of problems that exist with interoperability resources.
