Unit 4: Interoperable Communications

STUDENT GUIDE

Objectives

By the end of this unit, students will be able to:

- Identify methods for the application, coordination, and use of interoperable communications
- Define the concept of interoperability
- Identify and describe the five lanes of the SAFECOM Interoperability Continuum

Methodology

This unit uses lecture and discussion based activities.

Knowledge of unit content will be evaluated through administration of the final exam (to be administered upon completion of the course.

The purpose of this unit is to provide students with a high-level orientation to interoperable communications.

The purpose of Exercise 4-1 is to provide the participants with an opportunity to develop deployment strategies for portable repeaters in all-hazards environments, explain the challenges their strategy overcomes, and identify any challenges created by their strategy.

The purpose of Exercise 4-2 is to provide the participants with an opportunity to identify the challenges specific to communications in certain all-hazards environments and explain how to use existing communications technology to overcome these challenges.

Knowledge of unit content will be evaluated through administration of the final exam (to be administered upon completion of the course). Instructors will evaluate students' initial understanding through facilitation of Exercises 4-1 and 4-2.

Time Plan

A suggested time plan for this unit is shown below. More or less time may be required, based on the experience level of the group.

Topic	Time
Lesson	2 hours
Exercise 4-1	30 minutes
Exercise 4-2	30 minutes
Total Time	**3 hours**

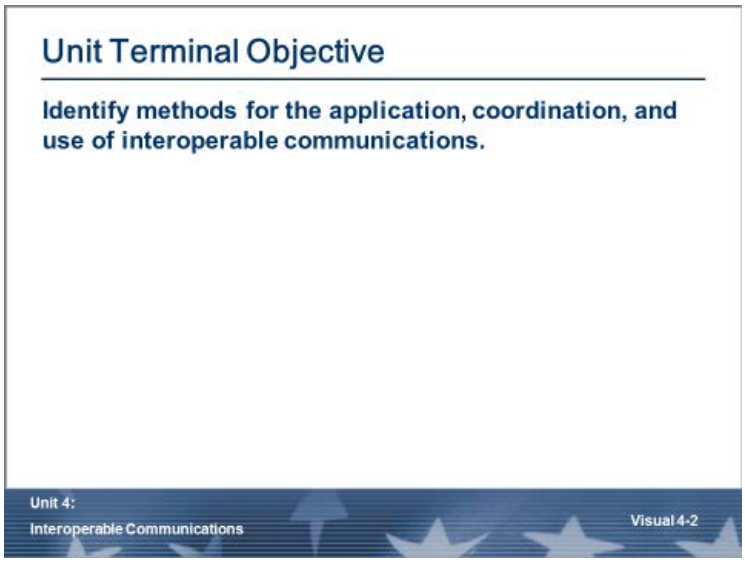
This page is intentionally left blank.

Topic Unit Title Slide

Key Points

This unit is designed to give the student a broad overview of various considerations that the Communications Unit Leader must keep in mind in relation to the SAFECOM Interoperability Continuum as it provides an understanding of the processes utilized in the urban environment to achieve interoperable communications.

Topic Unit Terminal Objective



Key Points

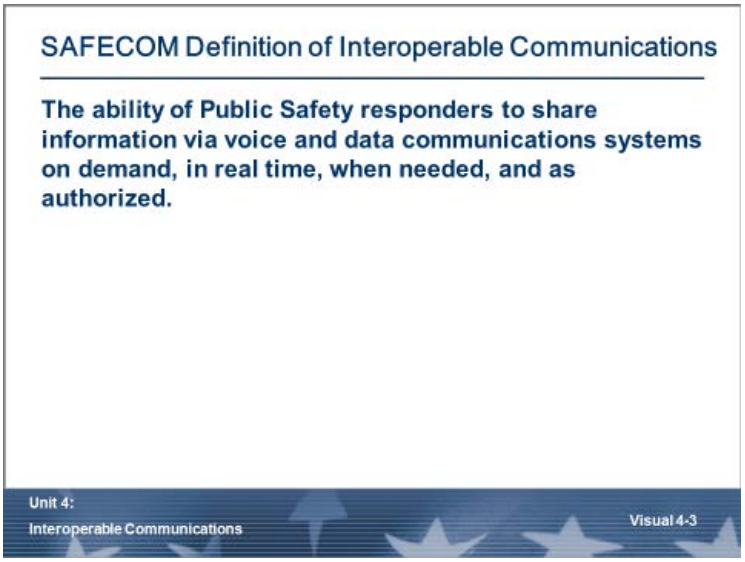
Unit Terminal Objective

Identify methods for the application, coordination, and use of interoperable communications.

Unit Enabling Objectives

- Define the concept of interoperability
- Identify and describe the five lanes of the SAFECOM Interoperability Continuum

Topic SAFECOM Definition of Interoperable Communication



Key Points

The purpose of this slide is to clarify the concept of interoperability in communications.

The Interoperability Continuum, and the interoperability concept, can be misunderstood quite easily. Interoperability must be carefully managed to avoid mass confusion. The Communications Unit Leader's job is specifically to prevent confusion in communication.

Interoperability does not require allowing all radio users to speak to all other radio users, which would create mass confusion. Rather, it refers to systems and processes that allow parties to communicate even if their equipment differs.

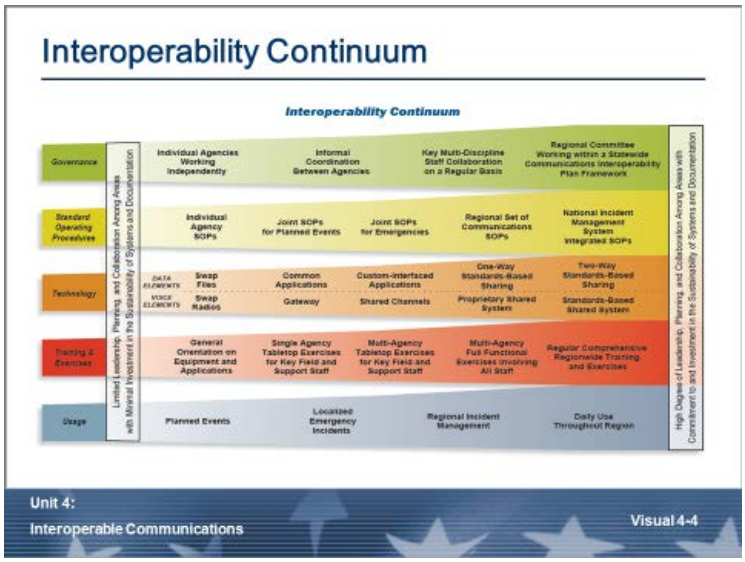
Interoperability is not the creation of a "party line."

Interoperable systems can grow quickly in complexity and are therefore easy to overload.

National Emergency Communications Plan (NECP)

The NECP established three goals for response level emergency communications. As defined by the 2008 National Emergency Communications Plan, response-level communications is the capacity of individuals with primary operational leadership responsibility to manage resources and make timely decisions during an incident. Primary operational leadership is at the top level of the Operations Section. The 2014 NECP is available at http://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf

Topic Interoperability Continuum



Key Points

A full copy of the Continuum is on the last page of this unit.

What is the SAFECOM Continuum?

The Interoperability Continuum is a tool designed to aid the emergency response community and local, tribal, state, and Federal policy makers to ensure they address critical elements for success as they plan and implement interoperability solutions.

What are the lanes in the SAFECOM Interoperability Continuum?

- Governance, which is the actions and programs undertaken by leadership for the purposes of managing the organization
- Standard Operating Procedures, which are the policies and procedures determined by organizations to ensure consistency and accuracy of response; the continuum measures the geographic level of coordination
- Technology, which displays the level of sophistication and ease of interoperability as radio systems go from less to more sophistication
- Training and exercises, which measures the sophistication of training and the integration with other agencies during exercises
- Usage, which describes the frequency of use of interoperable systems and practices

Interoperability is a lot more than technology. All of the items listed in these lanes are tools for interoperability. All are acceptable and even essential for effective interoperability.

Topic Governance Lane

Key Points

Governance allows for the codification of interagency relationships. It is the "frame of the car," or the organizational infrastructure that everything else is built upon. Governance can build sustainability in relationships between agencies. It is not always about control. It is also about having a problem solution before the problem occurs.

Governance refers to actions and programs undertaken by leadership for the purposes of managing the organization. Good governance in advance of an incident helps secure funding for communications operations, avoid confusion, and establish rights and responsibilities.

The Governance lane encourages individual agencies working independently to achieve regional cooperation by establishing authority through elected officials or executive councils. Organizations oftentimes establish a regional urban area working group with operational and technical subcommittees. This group then develops a regional strategic plan for interoperable communications and identifies a funding source (or sources).

The Governance section also establishes agency rights and responsibilities to avoid confusion once an incident occurs.

It is the ability to codify relationships and make relationships sustainable. It is also about having a problem solution before the problem occurs.

Topic Standard Operating Procedures Lane

Key Points

The SOPs lane promotes a set of SOPs at the local agency level to a regional set of communication SOPs that adopt ICS and integrate communications into National Incident Management Systems (NIMS) SOPs.

A proper SOP establishes:

- Rules of use
- Procedures for activation, response, and deactivation of communication resources
- A process for problem resolution

SOPs, as well as planning and operations, are created and run using common terminology rather than agency-specific codes or jargon. This avoids confusion on an incident, where personnel may be coming from different backgrounds.

Technology is not an unconditional solution to interoperability. SOPs are essential to effective interoperable communications.

The SOP Lane promotes a set of SOPs at the local agency level to a regional set of communications SOPs that adopt ICS and integrates communications into NIMS SOPs. They establish rules of use, procedures for activation, response, and deactivation of communications resources. They provide a process for problem resolution.

- The SOPs lane promotes a set of SOPs at the local agency level to a regional set of communication SOPs that adopt ICS and integrate communications into NIMS SOPs
- Using common terminology provides everyone on the incident a common dialect for describing the “who, when, why, where, what, and how” of operations, which is necessary when planning and running operations or forming SOPs

- Technology is not an unconditional solution to interoperability; SOPs are essential to effective interoperable communications

Topic Technology Lane

Key Points

Radio caches are extremely useful tools for interoperability. These are radios set aside as a regional communications resource that are fully charged, have extra batteries and battery chargers, and are labeled with the owning agency information, frequencies, band, and system. Many times the deployment of cache radios can keep interoperability simple.

Emergency Management Assistance Compact (EMAC) allows for states to assist each other directly without federal declarations. EMAC may be very useful in making agreements with adjacent states.

The technology lane is a toolbox with a number of solutions. The Communications Unit Leader/COMT should be able to choose from any number of these solutions as appropriate to meet communications requirements of the specific incident being supported.

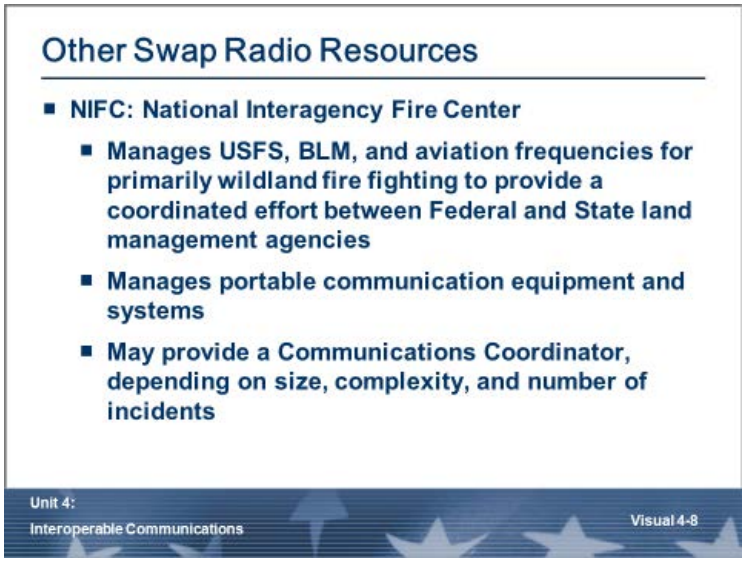
It is important to know:

- Where are your caches?
- What are the ordering procedures for a cache?
- Are there costs involved?
- Can you account for the cache you use?

E M A C

Agreements are in place for the use of resources between states www.emacweb.org

Topic Other Swap Radio Resources



Key Points

The National Interagency Fire Center (NIFC) provides a Communications Coordinator at times, depending on the complexity and number of incidents occurring, to assign frequencies and equipment to incidents and prevent interference.

You must have a pre-arranged contract with NIFC to utilize their resources. Make contact through your State Land Management Agency to find out the process. This should also go in your MOB Guide.

NIFC facilitates a coordinated effort between Federal and State land management agencies for wildfire management by managing portable communication equipment and systems.

To utilize the National Incident Radio Support Cache there must be a prearranged reimbursable agreement in place to request this resource. The NIICD Cache System is designed to support land management incidents, namely wildfires. When NIICD radios are deployed to a non-wild land incident, they are typically requested by going through a State Forestry Agency, Department of Natural Resources, EMAC or other emergency management procurement process. It is required the cache be accompanied by a NWCG-qualified COMT.

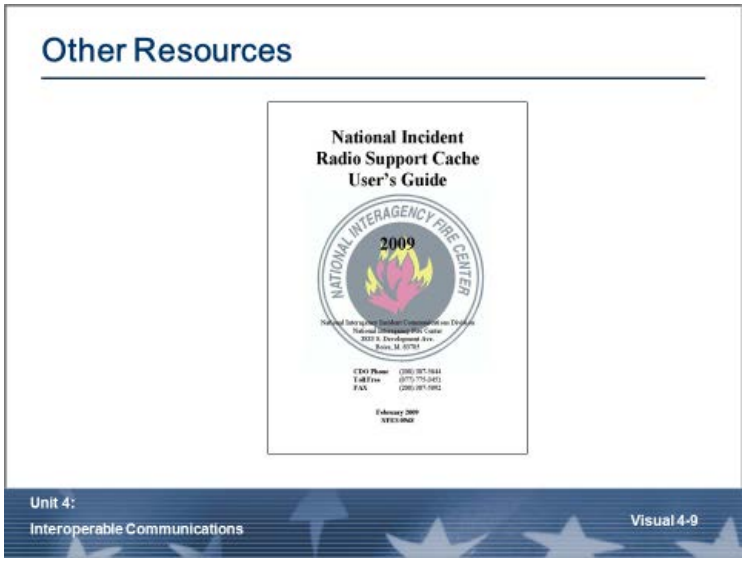
It is important to go through the proper channels when requesting these resources; however, even then, they are limited in availability. Availability may vary according to the state of the fire season and other factors at any given time.

- The NIFC manages USFS, BLM, and aviation frequencies, primarily for wildland firefighting

- NIFC manages portable communication equipment and systems and may provide a communications coordinator, depending on size, complexity, and number of incidents involved
- The National Incident Radio Support Cache also has equipment available for federally recognized incidents

Access the National Interagency Incident Communications Division at http://www.fs.fed.us/fire/niicd/index.html. To download the Radio Inventory Database, go to http://www.fs.fed.us/fire/niicd/documents, and select Radio Inventory Database under NIICD Documents.

Topic Other Resources

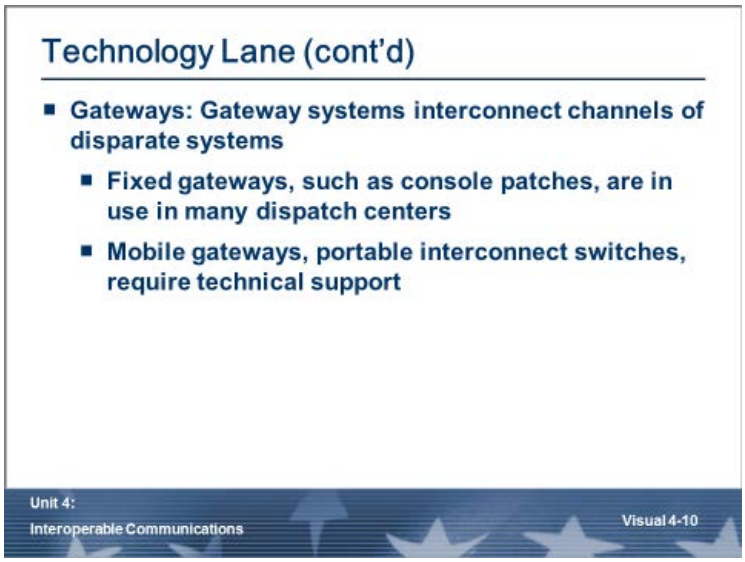


Key Points

You must have a prearranged reimbursable agreement in place to request this resource. As alternative, request through a State Forestry Agency, Department of Natural Resources, or through the emergency management procurement process.

This cache was designed primarily to support wildfire and land management agencies. Resources may be scarce during fire season.

Topic Technology Lane (cont'd)



Key Points

Gateways provide a connection between unlike radio bands or radio systems. They can make interoperability a reality, with quality audio and clean signals. Gateways are a tool, but can create issues as well. Proper gateway management is essential for safe and effective utilization.

Mobile gateways are not "Plug and Play." Competent personnel must be available for most mobile gateway deployments.

Fixed gateways can be engineered, tested, and exercised with minimal expenditure of resources, and are therefore easy to train on.

Gateways are one of several tools available to bridge interoperability issues.

What is the basic function of a gateway, also referred to as an audio bridge or audio gateway?

What are the two basic types of gateways?

Fixed and Mobile

What is a mobile gateway?

Gateways may be portable or transportable, which means they can be taken to the incident, event or exercise.

What is a fixed gateway?

A fixed gateway is a centrally located in a fixed location to operate with the local area communication assets.

What is a console patch?

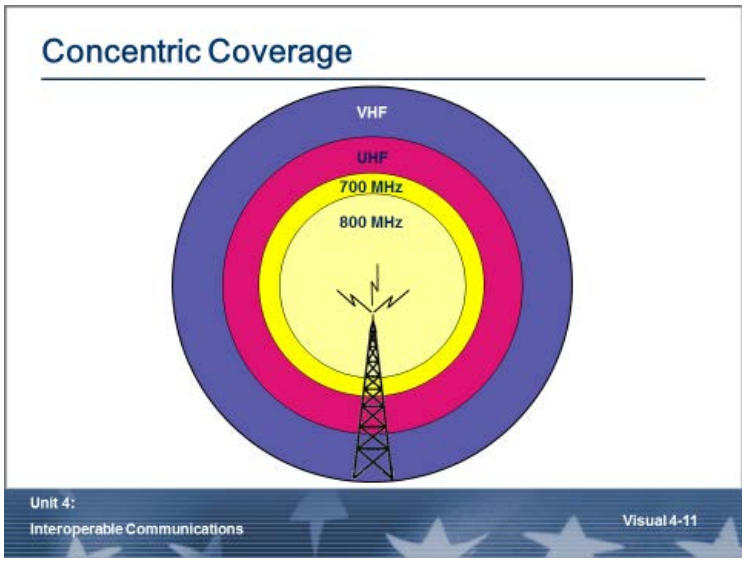
Console patches are preconfigured/hardwired into the console.

How does an audio gateway differ from a console patch?

This allows flexible patching between any/all systems interfaced with the audio gateways.

Are you using a gateway when a simpler method is available?

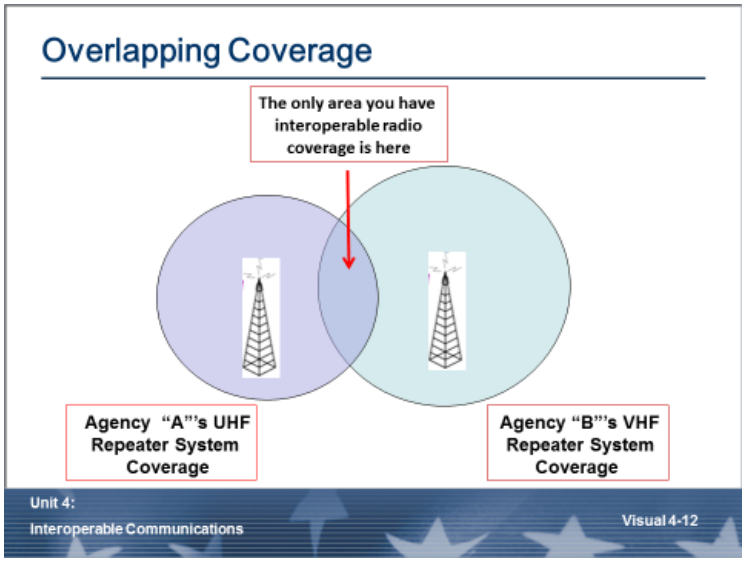
Topic Concentric Coverage



Key Points

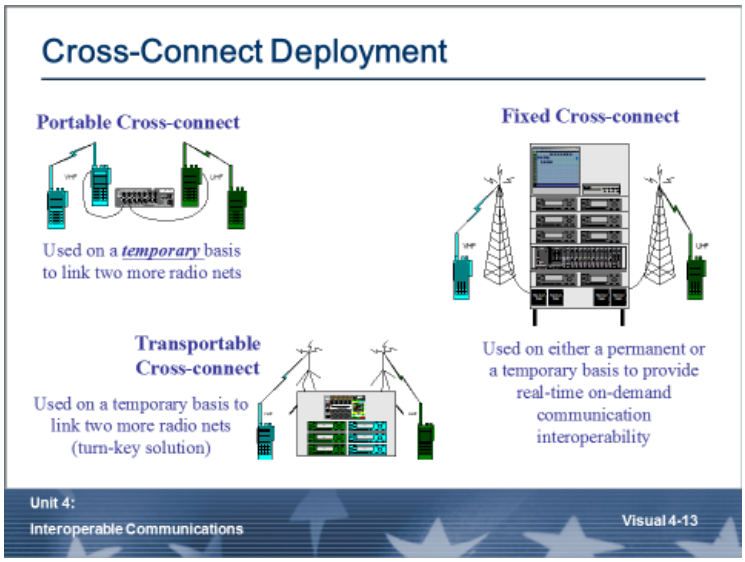
Topic

Overlapping Coverage



Key Points

Topic Cross-Connect Deployment



Key Points

- Fixed gateways are simple to deploy and can be tested and trained with regularly
  - Overlap coverage of disparate systems should be mapped
- Mobile gateways may have range limitations (simplex) and can have interference issues
- Portable gateways can have power supply limitations, reduced performance of portable receivers, and antenna limitations

Topic Technical and Operational Resources

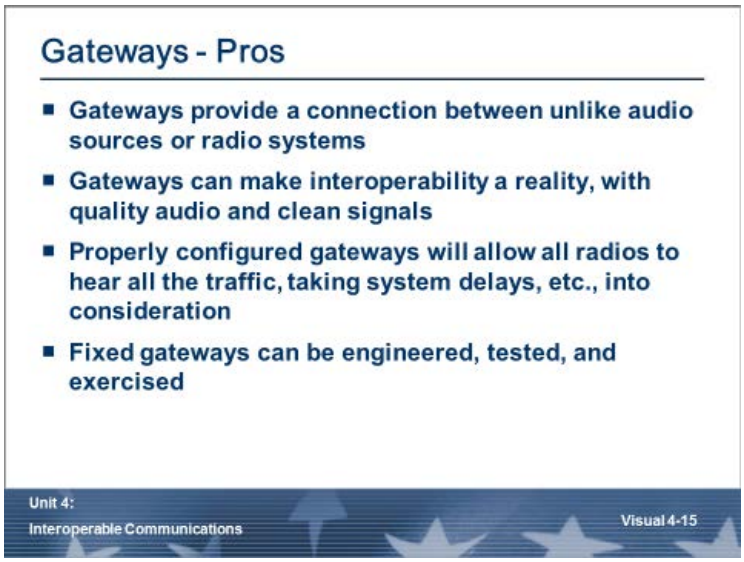
- 

Key Points

What are some things to consider when choosing a gateway?

- What will the gateway be used for? (i.e., deployment environment, mobile, fixed, in building, tunnel…)
- How many interfaces are required?
- Where will the interface devices be connected? (i.e., directly to the gateway, remotely via the Internet…)
- What types of patches are needed? (Many, one to many, many to one, one way monitor only…)
- What is your budget?
- How are you going to troubleshoot interference?
- How are you going to troubleshoot major system failure?

Topic Gateways—Pros

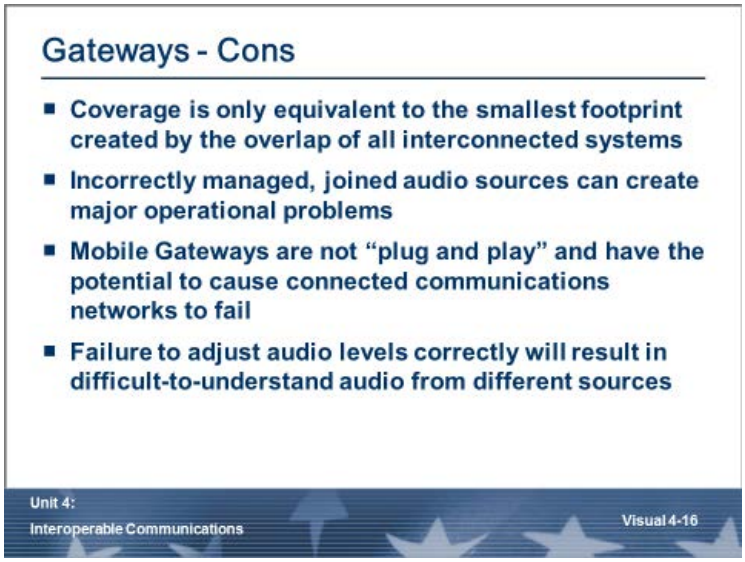


Key Points

What is the biggest advantage of a gateway?

Gateways provide interoperability between public safety service and support providers (i.e., law enforcement, firefighters, EMS, emergency management, the public utilities, transportation, and others). Gateways allow public safety agencies to communicate with staff from other responding agencies, and exchange voice and/or data communications on demand and in real-time.

Topic Gateways—Cons



Key Points

Why don't you use a gateway to patch everyone at an incident to everyone else?

Only patch those systems that really need to talk to each other for the time they need to talk, to prevent excess chatter. It will cut down on the confusion of hearing different organizations on your net and there will be less people vying for air time. Remember, just because you can patch someone doesn't mean you should.

How can you ensure gateways are properly configured prior to deployment?

Many mobile radios require special programming; some require hardware modification to properly interface with a gateway. Interface radios should be tested and adjusted with the audio gateway when it is first received and prior to deployment.

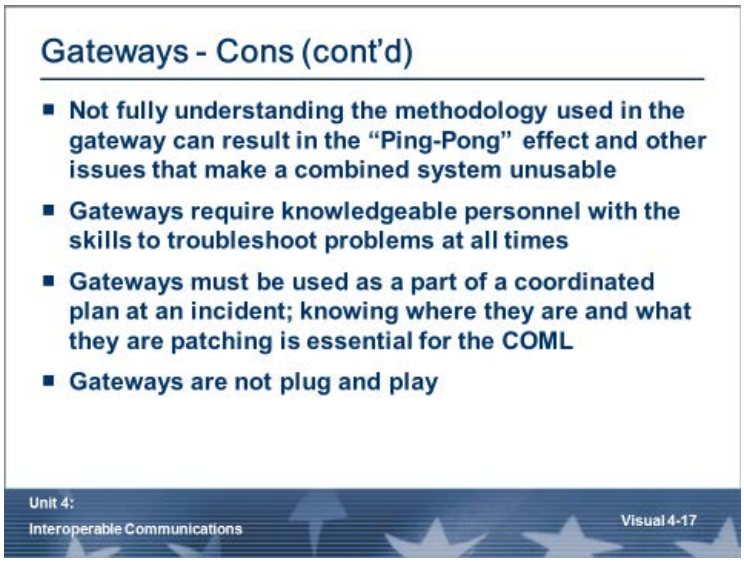
Why are audio levels of the gateway important?

- Correct levels are required for proper operation
- Too high levels will cause flat-topping and distortion
- Too low levels will not provide adequate audio volume to drive the interface devices

Patched channels may not have identical coverage:

- Different location of transmitter
- Different frequency band characteristics

Topic Gateways—Cons (cont'd)



Key Points

Ping ponging is the effect when the radios in the patch begin bouncing between TX and RX with no signal present.

Why do you need a Gateway Specialist?

Gateways are not plug and play. A knowledgeable person can recognize and fix a problem before it affects the people in the field.

When at an incident where multiple gateways are used, what is the key to interoperability?

Coordination is the key; always go through the Communications Unit Leader prior to creating a patch and know what is being patched.

Portable and mobile gateways should have a specialist with them at all times.

Use caution to address itinerate gateways.

Gateway management is essential. Communications Unit Leaders should have the authority over any inventory on the scene.

Topic Technology Lane (cont'd)

Key Points

Interoperability is promoted when agencies share a common frequency band, air interface (analog or digital), and are able to agree upon common channels.

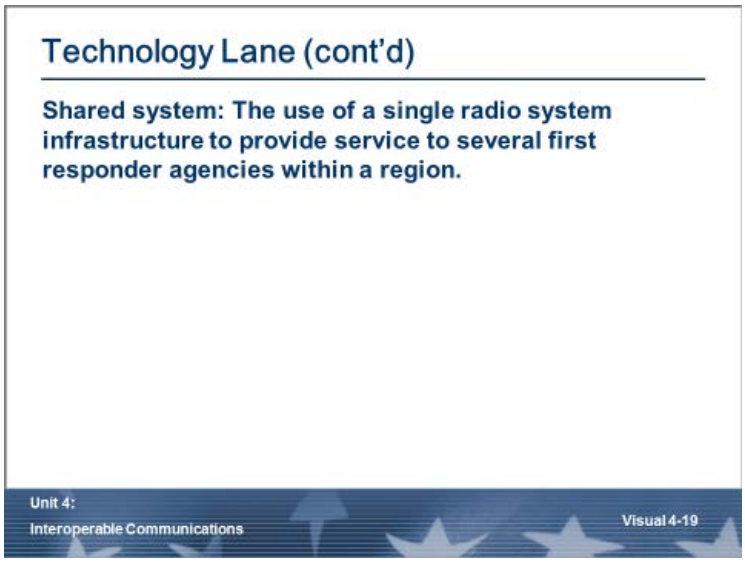
Why don't public safety agencies all use the same shared channels?

The general frequency congestion that exists across the United States can place severe restrictions on the number of independent interoperability talk paths available in some bands. Also, different bands have different characteristics.

Shared channels are often ignored for more complex solutions. Shared channels are the most direct form of interoperability.

The selection of shared channels is often heavily dependent on the governance lane, as long-term decisions must be made about which organizations will use which frequencies.

Topic Technology Lane (cont'd)



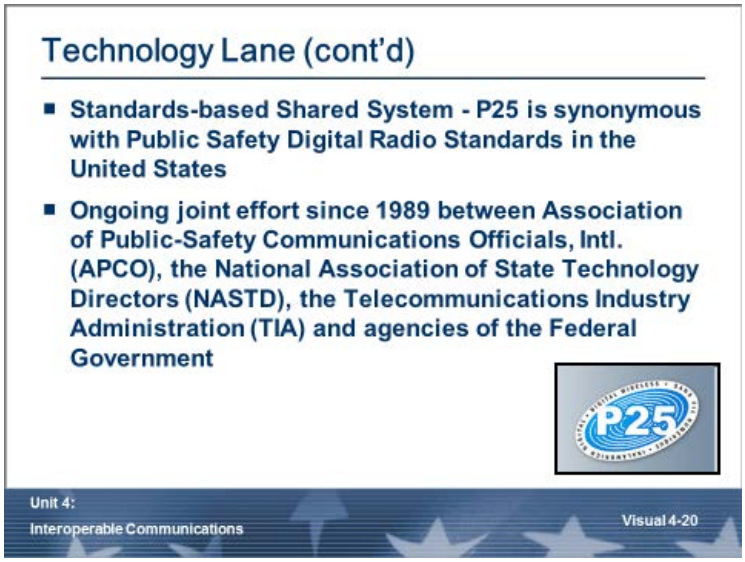
Key Points

A shared system involves use of a single proprietary radio system infrastructure (usually with all components from a single manufacturer) to provide service to several Public Safety agencies within a region.

Why are regional shared systems a solution to interoperability?

With proper planning of the talk group or channel structure, interoperability is provided as a byproduct of system design. Usually these are established at the request of the members of the governance lane, and require considerable coordination so that the shared system that is selected fits all of the local organization's needs.

Topic Technology Lane (cont'd)



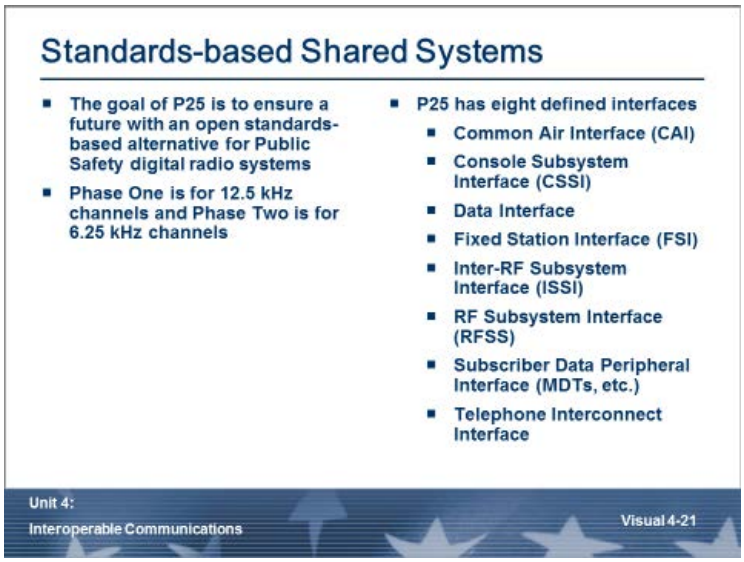
Key Points

Standards-based systems to ensure a future with an open, standards-based alternative for Public Safety digital radio systems have been a joint effort since October 1989 when APCO Project 25 came to being in a meeting jointly sponsored by APCO, NASTD, National Telecommunications and Information Administration (NTIA), the National Communications System (NCS) and the U.S. Department of Defense (DoD).

There are eight common elements of a standards system. These elements are:

- Common Air Interface (CAI): Point of connection between radio transmitters and receivers; defines the technical form and function of the digital signal that goes over the airwaves
- Console Subsystem Interface (CSSI): Defines how radio frequency components of a standards-based system and dispatcher consoles connect with one another
- Data Interface
- Fixed Station Interface (FSI): Defines how components of a shared standards radio system that are fixed in place connect with other components of the system
- Inter-RF Subsystem Interface (ISSI): Defines how different standards-based radio networks can connect with one another
- RF Subsystem Interface (RFSS)
- Subscriber Data Peripheral Interface (MDTs, etc.)
- Telephone Interconnect Interface

Topic Standards-based Shared System



Key Points

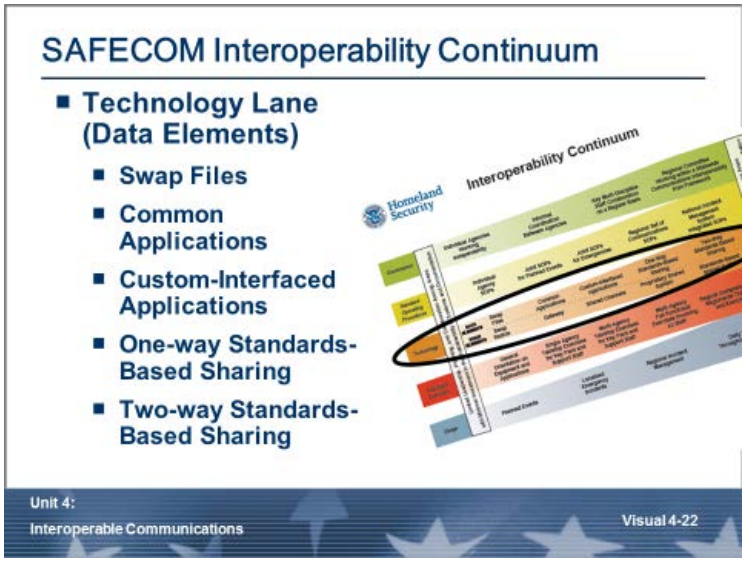
Project 25, or P25 is a phased approach to fielding new Public Safety communications technology as quickly as it is available, the development of standards and the testing of the technology in the field.

P25 is an ongoing, phased effort to introduce technology promoting interoperability, providing a backward/forward migration path to related technologies. P25 also ensures lifecycle competitive procurement, spectrum efficiency, and is operationally user friendly.

The goal of P25 is to ensure a future with an open standards-based alternative for Public Safety digital radio systems in the United States and across the globe (P25 is also used in many other countries).

P25 is not a completed standard at this time. Several P25 interfaces are still in the standards approval process. P25 standards are recognized ANSI standards.

Topic SAFECOM Interoperability Continuum



Key Points

Swap Files - Swapping files involves the exchange of stand-alone data/application files or documents through physical or electronic media (e.g., universal serial bus devices, network drives, emails, faxes). This process effectively creates a static “snapshot” of information in a given time period. Though swapping files requires minimal planning and training, it can become difficult to manage beyond one-to-one sharing. With data frequently changing, there may be issues concerning the age and synchronization of information, timing of exchanges, and version control of documents. Each of these issues can hinder real-time collaborative efforts. In addition, the method of sharing files across unprotected networks raises security concerns.

Common Applications - The use of common proprietary applications requires agencies to purchase and use the same or compatible applications and a common vocabulary (e.g., time stamps) to share data. Common proprietary applications can increase access to information, improve user functionality, and permit real-time information sharing between agencies. However, the use of common proprietary applications requires strong governance to coordinate operations and maintenance among multiple independent agencies and users; these coordinated efforts are further compounded as the region expands and additional agencies use applications. Common proprietary applications also limit functionality choices as all participating agencies must use compatible applications.

Custom-Interfaced Applications - Custom-interfaced applications allow multiple agencies to link disparate proprietary applications using single, custom “one-off” links or a proprietary middleware application. As with common applications, this system can increase access to information, improve user functionality, and permit real-time information sharing among agencies. Improving upon common applications, this system allows agencies to choose their own application and control the functionality choices.

However, if using one-to-one interfaces, the use of multiple applications requires custom-interfaces for each linked system. As the region grows and additional agencies participate, the required number of one-to-one links will grow significantly. Proprietary middleware applications allow for a more simplified regional expansion; however, all participants must invest in a single “one-off” link to the middleware, including any state or Federal partners. Additionally, custom-interfaced applications typically require more expensive maintenance and upgrade costs. Changes to the functionality of linked systems often require changes to the interfaces as well.

One-Way Standards Based Sharing - One-way standards-based sharing enables applications to “broadcast/push” or “receive/pull” information from disparate applications and data sources. This system enhances the real-time common operating picture and is established without direct access to the source data; this system can also support one-to-many relationships through standard-based middleware. However, because one-way standards-based sharing is not interactive, it does not support real-time collaboration between agencies.

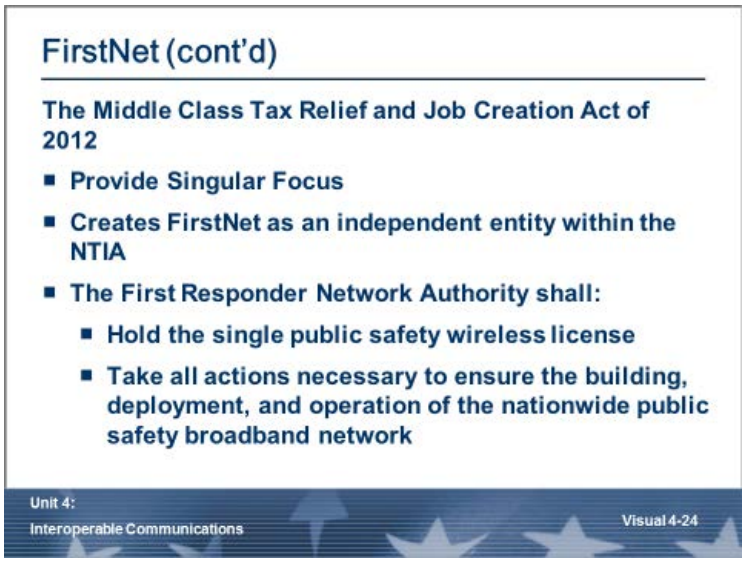
Two-Way Standards-Based Sharing - Two-way standards-based sharing is the ideal solution for data interoperability. Using standards, this approach permits applications to share information from disparate applications and data sources and to process the information seamlessly. As with other solutions, a two-way approach can increase access to information, improve user functionality, and permit real-time collaborative information sharing between agencies. This form of sharing allows participating agencies to choose their own applications. Two-way standards-based sharing does note face the same problems as other solutions because in can support many-to-many relationships through standards-based middleware. Building on the attributes of other solutions, this system is most effective in establishing interoperability.

Topic FirstNet

Key Points

Secretary of Commerce must appoint at least 3 individuals to represent the collective interests of States, localities, tribes, and territories; seek to ensure geographic and regional representation of the United States; seek to ensure rural and urban representation; and appoint at least 3 individuals who have served as public safety professionals and at least 3 appointed individuals are to represent the collective interests of States, localities, tribes, and territories.

Topic FirstNet (cont'd)



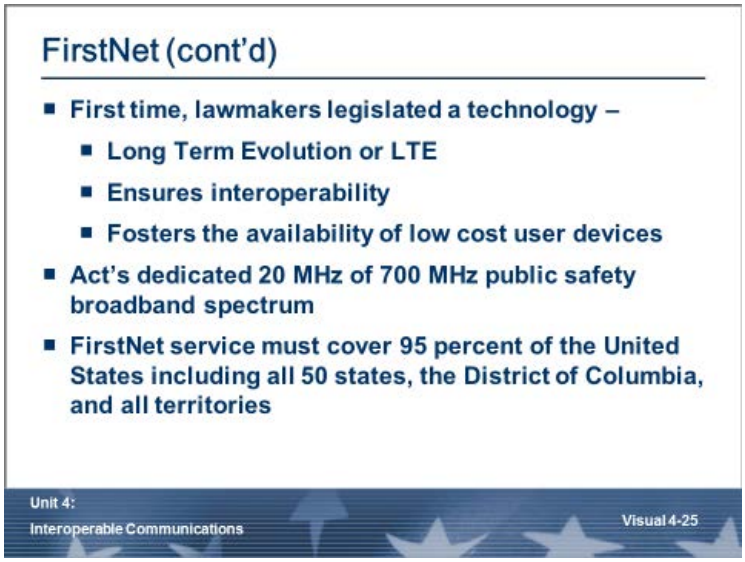
Key Points

The Middle Class Tax Relief and Job Creation Act of 2012 creates FirstNet as an independent entity within the NTIA and empowers it to oversee the establishment of an interoperable broadband network for public safety. The act requires that state and local agencies have a consulting role in the development, deployment, and operation of the nationwide network. The act further provides an opportunity for states to build their own radio access networks within the framework of the nationwide broadband network.

Key elements of the legislation:

- Reallocates the 10 MHz D Block to Public Safety, and along with the Public Safety Spectrum Trust (PSST) 10 MHz, provides a total of 20 MHz broadband public safety spectrum.
- Establishes a Network Construction Trust fund of $7 billion.
- Establishes a temporary FCC Interoperability Board.
- Establishes a standing FirstNet Board.
- Establishes a standing Public Safety Advisory Board to the FirstNet board.
- Establishes NTIA state planning grants ($135M).
- Requires public safety licensees to vacate T-Band channels within 9-11 years.
- Provides a $300 million fund to NIST for research.
- Does not affect the 700 MHz public safety narrowband (i.e. P25 voice) spectrum.

Topic FirstNet (cont'd)



Key Points

Topic FirstNet (cont'd)

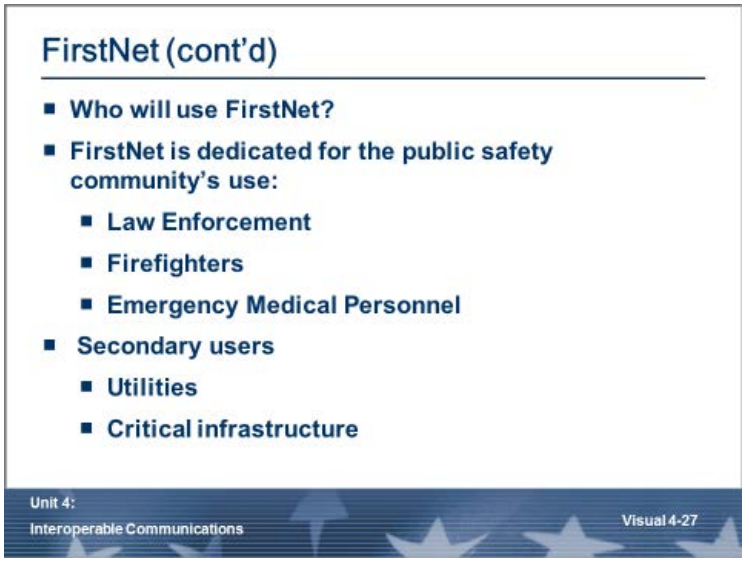
Key Points

Despite billions spent on homeland security, the public safety community has been frustrated by the lack of progress in realizing the recommendations of the 9/11 Commission to establish a dedicated, reliable, interoperable network for first responder and public safety communications.

Ten years after 9/11, public safety users still are hindered by fragmented systems, using differing frequencies and disparate equipment, resulting in costly inefficiencies. At the urging of public safety stakeholders, Congress passed legislation in 2012 to fund and govern a nationwide public safety broadband network.

FirstNet represents a most significant development for public safety – the promise of a dedicated, fully interoperable broadband system across the United States. A network that provides vast new capabilities, enhances safety and performance, and improves the cost effectiveness of public safety communications.

Topic FirstNet (cont'd)

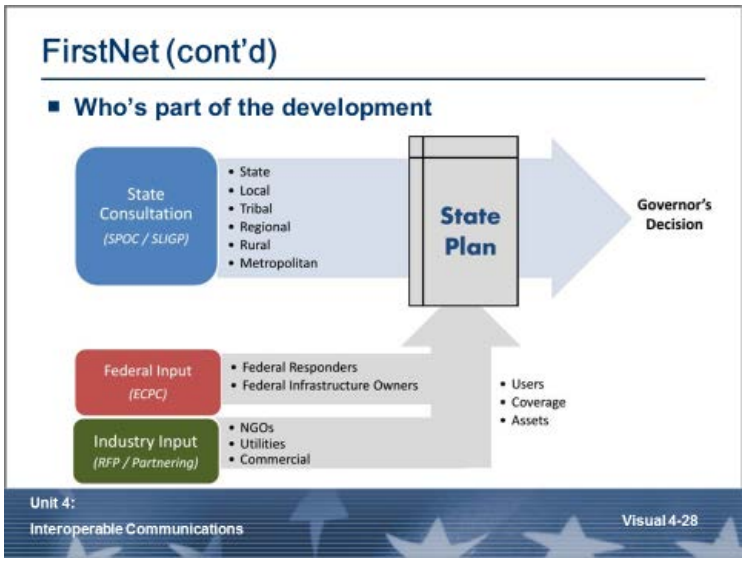


Key Points

The FirstNet Network will provide high speed data network coverage wherever public safety needs it, including the most rural and remote areas of a law enforcement agency's jurisdiction. The expansive data throughput of LTE broadband, which is theoretically more than 15 times faster than 3G cellular data today, is truly a transition "from garden hose to fire hose," enabling a broad range of new public safety mission support capabilities that, until now, were simply not possible.

Using this high speed data network, public safety personnel will see real-time information from their hardened smart phones, such as viewing detailed building diagrams and dynamic geographic information system (GIS) map data. First responders can act quickly and in coordination as the network supplies video feeds from traffic cameras, immediately indicating the severity and extent of an accident. Emergency medical personnel will transmit patient information and health telemetry to emergency rooms and trauma centers while en route to the medical center, with vital lifesaving data arriving in advance of the injured.

Topic FirstNet (cont'd)



Key Points

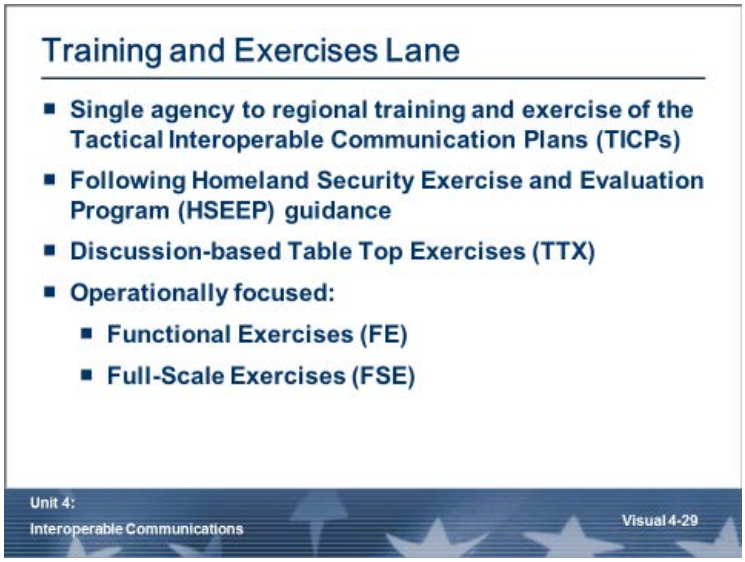
- State POC (SPOC)
- State and Local Implementation Grant Program (SLIGP)
- Emergency Communications Preparedness Center (ECPC)
- Request for Proposal (RFP)

Each governor has the option to decide whether his or her state wants to conduct its own deployment of a broadband Radio Access Network (RAN).

If a state decides to opt-out, it has 6 months to develop and complete its own RFP process for a broadband RAN within the state, subject to FCC approval.

States that are approved to opt-out are eligible to apply to the NTIA for a grant for construction of their broadband RAN, and for a spectrum lease, however, they will be required to connect to the federal core.

Topic Training and Exercises Lane



Key Points

Regional exercises are an excellent opportunity to establish a Communications Unit Leader for the area, in addition to the benefits of working cooperatively, and aid the goal of interoperability accordingly.

A result of these exercises is the opportunity for creation and exercise of Tactical Interoperable Communication Plans (TICPs), which provide a context and/or reference for a Communications Unit Leader, should an actual incident occur.

The Training and Exercise Lane provides for single-agency training and exercising as well as regional training and exercising of the TICP. Regional exercises are an excellent opportunity to establish a Communications Unit Leader.

Following Homeland Security Exercise and Evaluation Program (HSEEP) guidance, and making ample use of the NIMS discussion-based Table Top Exercises (TTX) ensures maximum readiness and understanding of interoperability scenarios.

Topic Usage Lane

Key Points

The Usage Lane encourages the use of a Communication Plan for planned events, local emergencies, and regional incidents, used on a daily basis.

Gaining familiarity with the format and requirements of the plan allows the Communications Unit Leader to function more efficiently when called to a major incident. Regular usage of interoperable systems builds confidence in responders who develop better familiarization.

This lane encourages the use of the TICP for planned events, local emergencies, regional incidents, and on a daily basis.

Usage is the keystone of all interoperable communications. If it is not used on a daily basis, it will not be used in incident response.

Routine usage of interoperable elements promotes familiarity and consistency.

The Usage lane of the Interoperability Continuum encourages daily use of a communication plan whenever staffing:

- Planned events
- Local emergencies
- Regional incidents

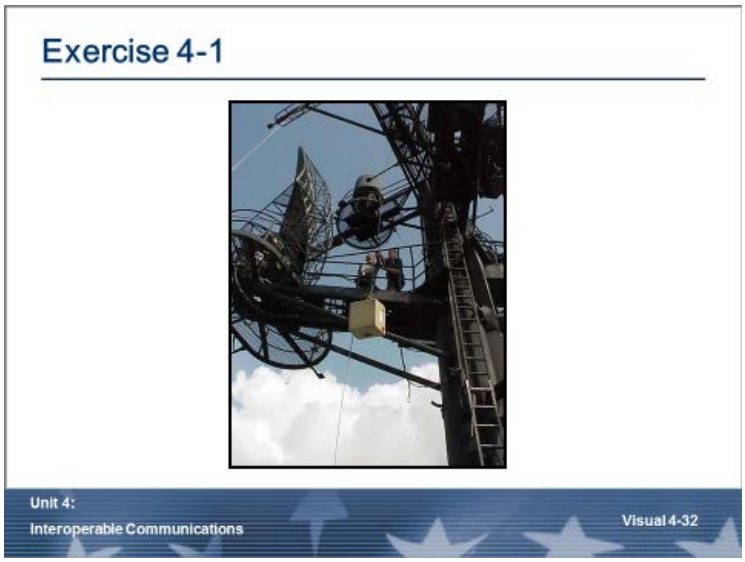
Topic Exercise 4-1 - Communication Asset Deployment Strategies

- 

Key Points

The purpose of the exercise is to provide the participants with an opportunity to develop deployment strategies for portable repeaters in all-hazards environments, explain the challenges their strategy overcomes and identify any challenges created by their strategy.

Topic Exercise 4-1, Image 1



Key Points

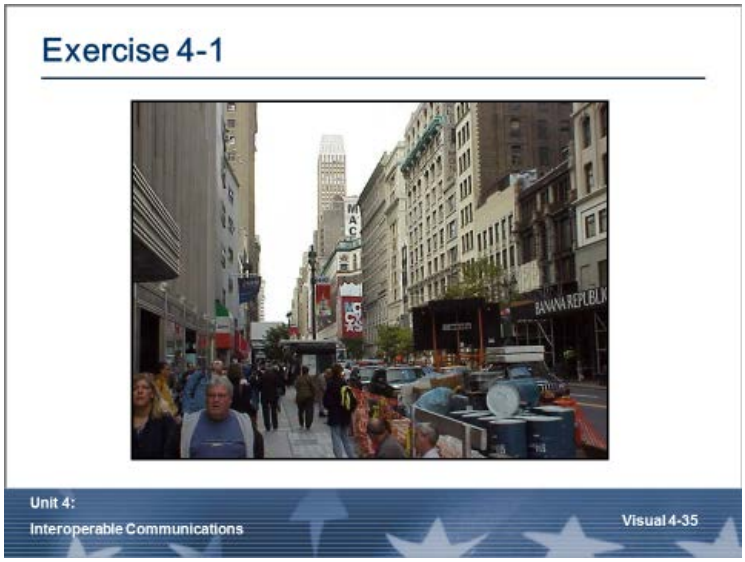
Topic Exercise 4-1, Image 2

Key Points

Topic Exercise 4-1, Image 3

Key Points

Topic Exercise 4-1, Image 4



Key Points

Topic Exercise 4-1, Image 5

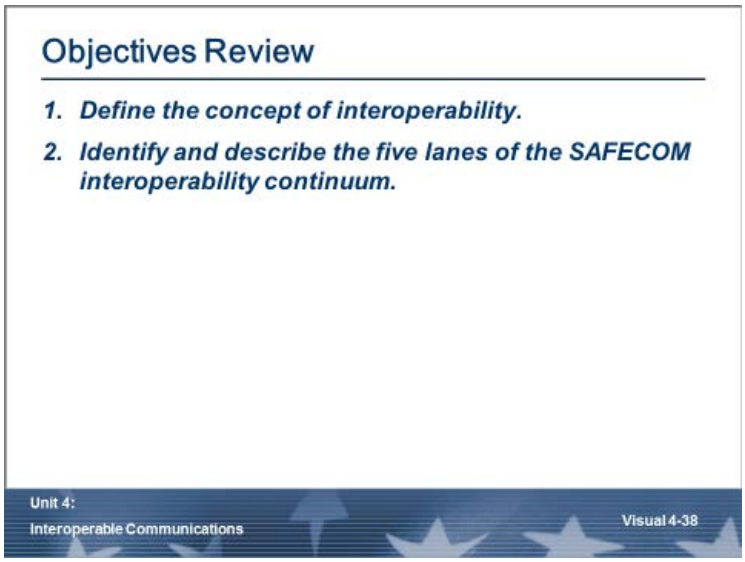
Key Points

Topic Exercise 4-2

Key Points

The purpose of this exercise is to provide the participants with an opportunity to identify the challenges specific to communications in certain all-hazards environments and how to use existing communications technology to overcome these challenges. The exercise is scheduled to last approximately 30 minutes, including small group discussions and presentation of group findings. Students will break into small groups and compile a list of potential challenges and solutions to operating within the urban environment in the train derailment scenario. Students will then present their findings to the class.

Topic Objectives Review



Key Points

Unit Terminal Objective

Identify methods for the application, coordination, and use of interoperable communications.

Unit Enabling Objectives

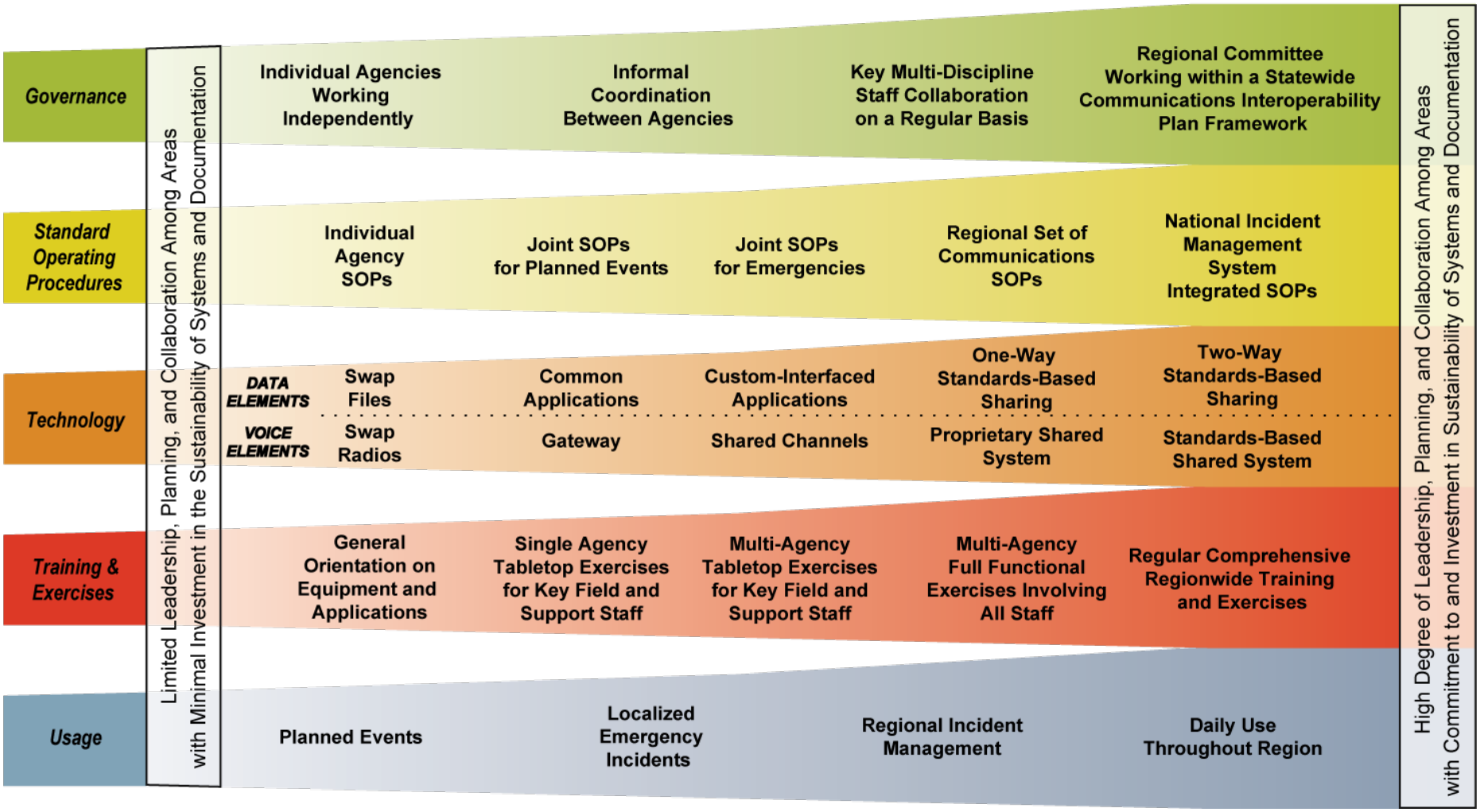
- Define the concept of interoperability.
- Identify and describe the five lanes of the SAFECOM Interoperability Continuum.

Topic Questions?

- 

Key Points

Interoperability Continuum



This page intentionally left blank.