



Cisco Open Platform for Safety and Security: Understand the Mobile Force Architecture Building Block

What You Will Learn

The Cisco Open Platform for Safety and Security is an architecture framework for building solutions to prevent, prepare for, respond to, and recover from incidents. The framework comprises six building blocks: Command and Control, Mission-Critical Network, Incident Collaboration, Sensing and Actuation, Mobile Force, and Citizen-Authority Interaction.

This white paper, intended for organizations planning investments in safety and security technologies and for solutions providers, focuses on the Mobile Force architecture building block. It enables public safety organizations to:

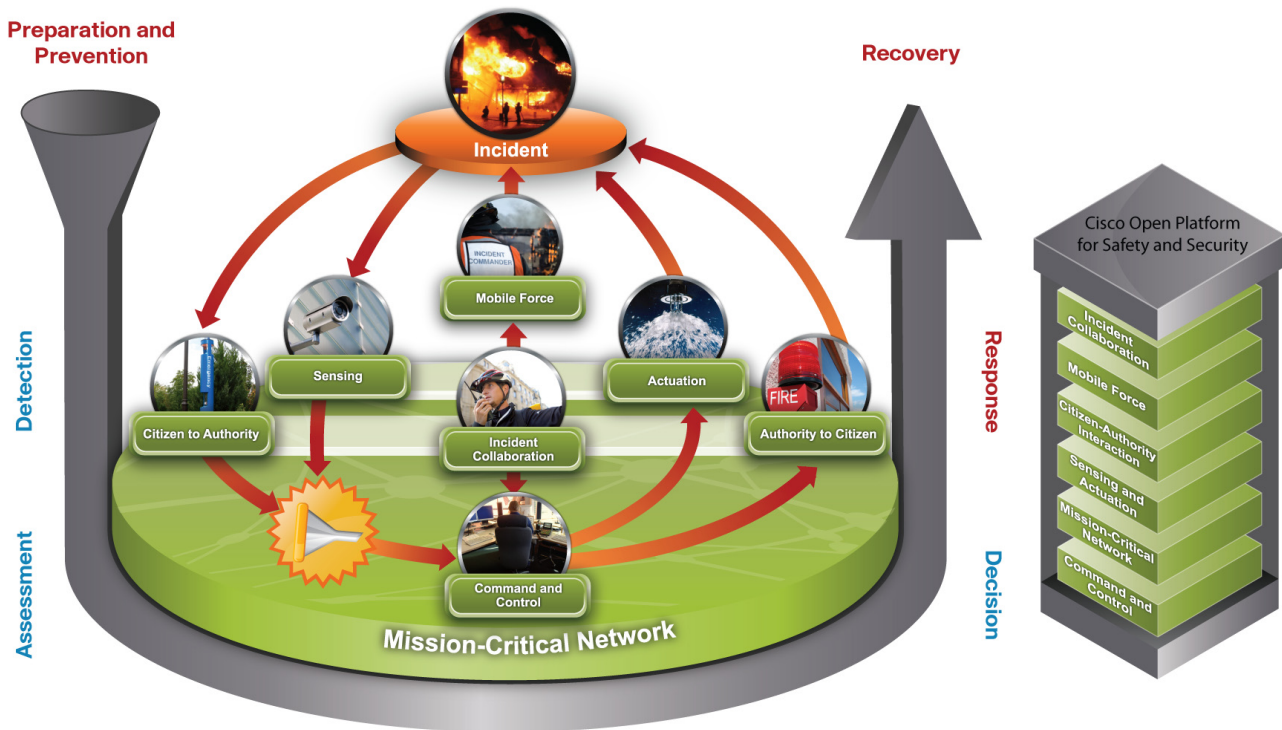
- Connect emergency responders to the information, applications, and human resources they need to achieve the mission
- Provide efficient dispatch, problem resolution, and emergency communications
- Optimize operational processes, for example by automating the creation of incident reports
- Quickly establish a mobile command center even in places without any network infrastructure

The Role of the Mobile Force in Safety and Security

To protect lives and property, emergency responders in the field need access to critical information and services from any place, any time, and in the right format. During hurricane Katrina, for example, organizations involved in rescue and recovery efforts needed to establish remote worksites at the edge of the heavily flooded Gulf Coast.

The Mobile Force architecture building block ensures that safety and security professionals can access critical information wherever they are, during routine as well as emergency response (Figure 1).

Figure 1 The Mobile Force Architecture Building Block Supports Incident Management



The main goal of the Mobile Force architecture building block is to empower deployed forces to be as effective in the field as they would be in the office. Examples include:

- Enabling security guards to control video surveillance cameras and view feeds from a smartphone or other handheld device.
- Enabling first responders to access databases from in-vehicle laptops so they can answer questions such as: Is the person pulled over for a traffic violation armed and dangerous? Does this building contain hazardous materials? Which way is a chemical plume moving?
- Enabling police officers and firefighters to transmit video from vehicle-mounted cameras to the command center, increasing situational awareness for commanders.
- Collecting environmental data from biosensors integrated into firefighter's suits.
- Improving medical care by transmitting a patient's vital signs from the ambulance on the way to the hospital and retrieving charts and physician analysis.
- Enabling first responders at an emergency scene to immediately establish a wireless network to collaborate with each other and also to share voice, video, and data with headquarters.

The Mobile Force architecture building block provides the devices, networks, and services needed to gain these capabilities (Table 1).

Table 1 Solutions in the Mobile Force Architecture Building Block

	Personal Passive Devices	Personal Computing Devices	Vehicle Computing Devices	PAN	IAN	Location Services	Mobile Command and Control	Zero-Touch Configuration and Management
Rapidly Deployable Communications (RDC)					✓	✓	✓	✓
Cisco 5900 Embedded Services Routers			✓		✓		✓	✓
Cisco Outdoor Wireless Mesh Network					✓			✓
Aeroscout	✓							
AnyWeb			✓				✓	
Intermec		✓						
Panasonic		✓						
pTerex			✓				✓	

Devices

This building block includes personal passive devices used to monitor health and environmental conditions, mobile devices used for communications, and in-vehicle devices that provide connectivity while the vehicle is in motion:

- **Personal passive devices:** These include sensors and actuators. Biological sensors monitor the health information of first responders and injured persons, including heart rate, body temperature, electrocardiogram signal, and more. Environmental sensors attached to first responders' protective suits can monitor for the presence of harmful gasses. Actuators respond automatically to sensor information—for example, by cooling down firefighters when their body temperature is too high.
- **Personal computing devices:** Examples include mobile phones, smartphones, two-way pagers, radios, and mobile laptop computers. Some mobile devices can be used to access real-time video surveillance feeds, update and retrieve database information, and exchange instant messages. Mobile devices used in emergency scenes must be designed to withstand vibration, drops, spills, extreme temperature and dust, and other rough handling.
- **Vehicle computing devices:** First responders on the move need constant connectivity to the operations center as they roam across different wireless coverage areas. Vehicle computing devices must be able to smoothly hand off the connection to different wireless networks, including local WiFi hotspots (802.11), General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS), or Terrestrial Trunked Radio (TETRA). Examples of on-board vehicle devices include embedded rugged PCs, onboard video surveillance cameras, smartphones, and scanners.

Case Study: City of Zurich Police

Zurich City Police officers who needed information about a driver or vehicle previously had to request the information by radio. The dispatcher would relay the information, resulting in delays and sometimes leading to misunderstandings. Now officers in the field can use in-vehicle laptops to consult federal and local databases, access the Internet, and transmit information. The connection is established over the highest-bandwidth available wireless network, including the wireless LAN at headquarters, the 500Kbps UMTS network, or the slightly slower GSM network. A Cisco Mobile Access Router 3200 in the vehicle enables officers to retain their connection without interruption even as the vehicle roams in and out of different coverage areas. Officers in motion can also use IP video cameras, scanners, printers, and IP phones.

Technology Highlight: Mobile Routing

Mobile routing technology enables a vehicle to maintain unbroken connectivity as it roams throughout the city or county. Laptops, IP video surveillance cameras, and other mobile devices retain the same IP address during the session, even if the connection is successively handed off to multiple networks. With uninterrupted connectivity, the mobile force can access information to plan an effective response, such as structural diagrams, mug shot data for identity verification, and streaming video of a crime in-progress. Similarly, the mobile force can contribute to others' situational awareness by transmitting information such as digital photos and digital video. With the proper equipment they can capture mug shots and scanned fingerprints at the point of arrest, transmitting the information to headquarters, where it can be automatically propagated to regional, state, and federal databases.



Mobile Networks

Mobile networks can combine satellite and terrestrial technologies, for redundancy. The Mobile Force architecture building block includes two types of mobile networks:

- **Personal Area Network (PAN):** A PAN connects all devices that a particular first responder carries, often using IrDA or Bluetooth network technologies. Devices might include an audio microphone and earpiece, a helmet-mounted camera, environmental sensors, compass, accelerometer, and thermometer, for example.
- **Incident Area Network (IAN):** An IAN, established for the duration of a particular incident, connects all personnel at the incident scene. Figure 2 shows the three types of IANs: nomadic, seamless, and ad hoc, and Table 2 provides examples of when to use each type.

Figure 2 Different Types of Incident Area Networks Suit Different Requirements

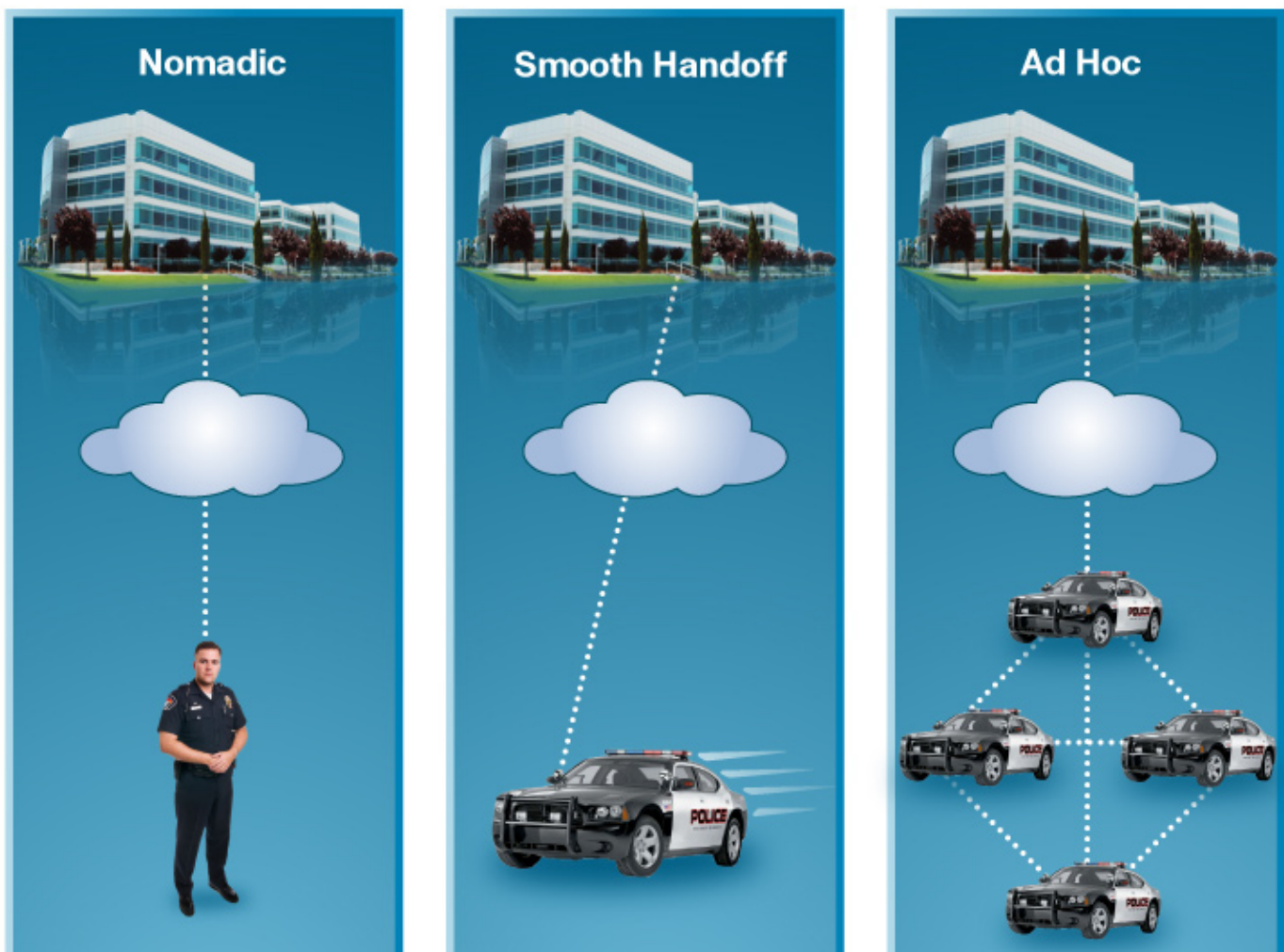


Table 2 When to Use Nomadic, Seamless, or Ad Hoc Incident Area Networks

Type of Incident Area Network	User Experience	Usage Examples
<p>Nomadic</p>	<p>Devices need to disconnect before moving, and then reconnect when stationary.</p>	<p>A security inspector visits multiple facilities but only needs network access during the inspection.</p> <p>A microprocessor continuously collects data from a truck or ship but only needs to upload the data when the vehicle reaches a base.</p>
<p>Smooth Handoff</p>	<p>Devices remain connected while in motion.</p> <p>The hand-off from one wireless access point to another is so fast that the application is not affected. A voice connection is not dropped, for example.</p>	<p>Personnel use wireless IP phones throughout the coverage area.</p> <p>Security staff view video surveillance feeds on smartphones as they patrol an area.</p> <p>Moving trains, buses, ships, or airplanes provide wireless connectivity to occupants while in motion.</p>
<p>Ad Hoc</p>	<p>The mobile force can communicate at the emergency scene without any fixed infrastructure. Communications are established between any moving objects: vehicles, aircraft, marine vessel, or person.</p> <p>The ad hoc network is self-forming and self-healing.</p>	<p>When firefighters enter a burning building, they often lose connectivity to the outside world. By carrying ad-hoc personal communications devices, they can establish a dynamic network between themselves, and relay the communications to the emergency commander posted outside the building.</p> <p>The commander's vehicle can use a satellite uplink to provide connectivity to all other vehicles involved in the rescue operation. If a vehicle is too far to connect directly to the commander's vehicle, the occupant can dynamically establish an ad-hoc connection to a neighboring vehicle that will relay the communication.</p>

Case Study: City of Austin

The City of Austin integrated a rapidly deployable communications system into its mobile command vehicle, ensuring that first responders have network access even in the event of a power outage or a massive disruption to the public communications infrastructure. The equipment in the vehicle automatically connects using whatever method is available: wired, wireless mesh, or satellite. Once connected, the system provides wired and wireless connectivity in and around the vehicle so that public safety personnel can use laptops, handhelds, and other devices to access maps, database information, streaming video, and more. The system also enables the city to support the more than a dozen different radio systems used by its various agencies, including push-to-talk radios and regular phones, as well as to communicate with the emergency medical service dispatch team within the city's Combined Transportation Emergency and Communications Center. Having all the different types of radio and other voice technologies available in one system enables incident commanders to make informed decisions and relay those decisions to the field as quickly as possible.

Mobile Services

The Mobile Force architecture building block defines the following types of services required in emergency situations: mobile command, control, and communications (C3) services; location-based services; and management services.

Mobile Command, Control, and Communications

In emergency situations, public communication systems are often overloaded, damaged, or destroyed. Therefore, organizations need a rapidly deployable, mobile C3 system to enable emergency responders' to sense, respond, coordinate, and effectively manage the emergency event.

The Mobile C3 system in the Mobile Force architecture building block provides a subset of the functions in the architecture building blocks for Command and Control and Incident Collaboration. Its main functions are:

- An emergency plan, including:
 - Implementation and management of the safety and security policy
 - Technology and processes to address the risk
 - Continuous monitoring of the unfolding emergency
- Situational awareness and control, including creation of a Common Operational Picture
- A role-based view of the situation for emergency responders. The view should include the event location and might also include information such as the event type, number and type of vehicles involved, and so on.

Technology Note: Mobile Ad Hoc Network

A Mobile Ad Hoc Network (MANET) has the following characteristics:

- Mobility: Mobile nodes can travel in a random or predictable direction, at any velocity. The nodes can move as individual entities or as a group.
- Topology: The topology is variable, defined by the positions of the mobile nodes at a particular time.
- Wireless network: The wireless Media Access Control (MAC) address is not specified. Cisco can provide Layer 2, Layer 3, and hybrid MANET solutions. Most current research on MANET routing protocols uses 802.11 MAC addresses.

Technology Note: Rapidly Deployable Communications

Cisco Rapidly Deployable Communications enables first responders to quickly establish voice, video, and data communications in any location, over wired, wireless, mobile radio, and satellite networks. Rugged, easy to set up, and based on open standards, Cisco Rapidly Deployable Communications solutions enable flexible disaster recovery, incident management, and command and control.

Two options are available:

- Cisco iComm (formerly IMICS) is capable of scaling for a whole agency. It is easy to use, weighs less than 200 pounds, requires no more than 600 watts of power, and can be operational in less than 10 minutes. Once it is set up, first responders can collaborate using IP telephony, analog phones, fax, voicemail, and radio. Cisco iComm is especially useful for disaster recovery, as a replacement for destroyed communications infrastructure to maintain essential government services, or to augment existing capabilities. You can also use it to provide a mobile infrastructure for onsite communications.
- Cisco Tactical Communications Kit is simple enough for one person with minimal training to set up and operate it within 10 minutes. It provides tactical IP communications over wired, wireless, or satellite networks in harsh conditions. It offers up to 36 IP phone connections and fax capability in a single kit, and provides an 802.11 point-to-point wireless connection of up to 20 miles. The suitcase-sized network in a box can operate off a car battery and fits easily in an emergency vehicle.

Location-Based Services

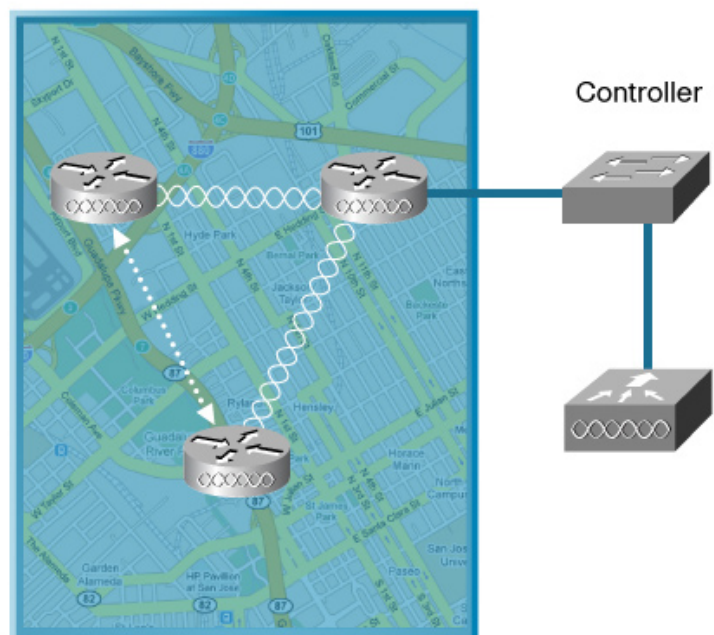
The most popular types of location-based service are the Global Positioning System (GPS) and triangulation methods based on the signal strength received by WiFi access points or GSM antennas. Geographic Information Systems (GIS) provide the tools to provision and administer basic map data such as streets, buildings, mountains, and rivers. You can also use GIS to map points of interest such as water points for firefighters or factories that produce hazardous byproducts.

Zero-Touch Configuration and Management

Zero-touch configuration and management enables the mobile force to quickly set up a temporary network for the duration of a specific incident. It saves emergency responders valuable time they would otherwise spend configuring protocols, ensuring equipment compatibility, and assigning device addresses.

The Mobile Force architecture building block includes indoor/outdoor wireless mesh solutions that are self-configuring and self-healing. The wireless access points automatically establish a connection with the controller and then download configuration and radio parameters (Figure 3). No IT effort is required.

Figure 3 Automatic, Secure, Zero-Touch Mesh Access Point Configuration



Conclusion

Public safety and security is a complex and rapidly evolving discipline, and a single vendor cannot provide all pieces of an architecture. Therefore, it is vital for the industry to develop and adopt open interfaces that enable best-of-breed solutions to work together. The Cisco Open Platform for Safety and Security provides a framework for solution providers to jointly create and implement solutions. The Mobile Force architecture building block provides:

- The devices used to communicate with other members of the mobile force and with headquarters, with voice, video, and data
- Mobile networks
- Services for command, control, and communication; detecting the location of people and events; and zero-touch management

For More Information

To read more about the Cisco Open Platform for Safety and Security, including partner profiles, visit:
www.cisco.com/go/copss




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARtNet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)