



# Cisco Open Platform for Safety and Security: Understand the Command and Control 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.

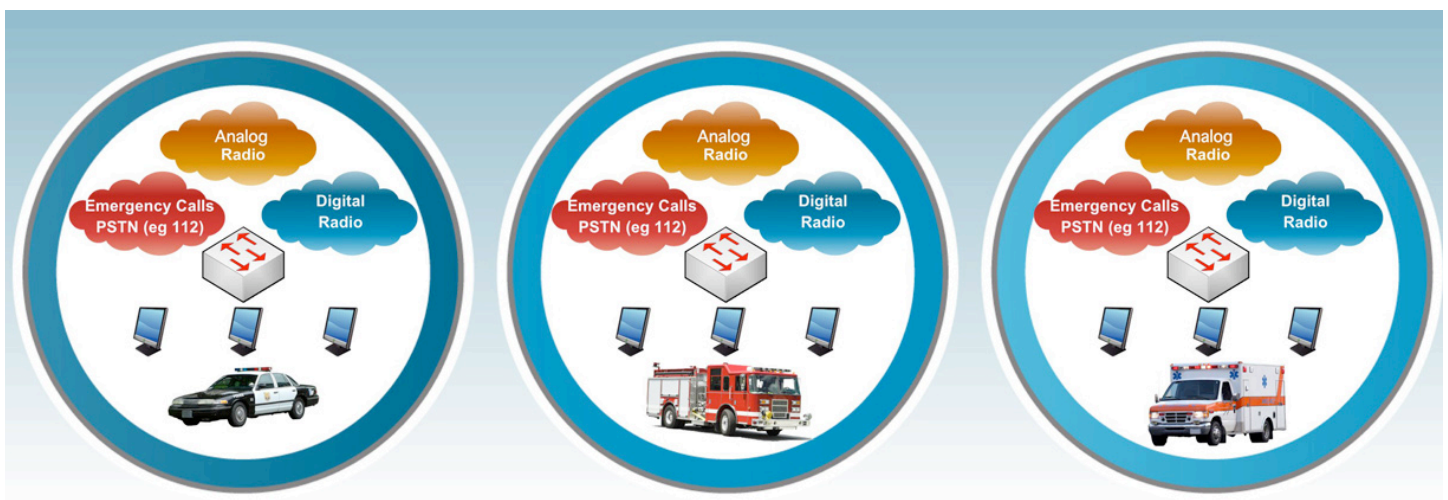
This white paper is intended for organizations planning investments in safety and security technologies and for solutions providers. It focuses on the Command and Control architecture building block and explains the trend towards Fusion Centers. This building block provides the following capabilities:

- Intelligence and process management
- Mission-critical applications
- Infrastructure management and monitoring

## The Role of Command and Control in Safety and Security

Traditionally, public safety agencies each maintained their own control rooms, which were not connected to the others (Figure 1). Agencies exchanged information only by phone.

Figure 1 Standalone Control Centers for Police, Fire, and Emergency Medical Services



The need for interagency collaboration during emergency response has increased. Therefore, traditional Command and Control rooms are undergoing a transformation to become Fusion Centers, so called because they fuse information from multiple sources to create actionable intelligence (Figure 2).

**Figure 2 Fusion Centers Enable Virtualized Command and Control**



A fusion center is a “system of systems.” That is, each participating agency maintains its own systems (knowledge databases, sensors, strategic and operation centers), and takes advantage of open interfaces to connect them into a shared, virtual system. Having each agency maintain its own systems avoids the economic and technology risks of a single “super system,” with its potential for failure. The advantages of virtualizing Command and Control functions:

- Facilitating collaboration during major incidents with the goal of improving decision processes and accelerating response
- Enabling individual agencies to retain ownership of and access to their own resources
- Enabling agencies to manage their own information and user spaces
- Providing a shared infrastructure, reducing the costs for the individual agencies
- Making emergency personnel's location irrelevant by giving them secure mobile access to information and services from any location with a wireless connection

The Command and Control architecture building block provides the functions that the crisis management team needs: up-to-date situational awareness, actionable intelligence, and decision support tools. Figure 3 shows the role of the Command and Control architecture building block in the Cisco Open Platform for Safety and Security.

Figure 3 The Command and Control Architecture Building Block

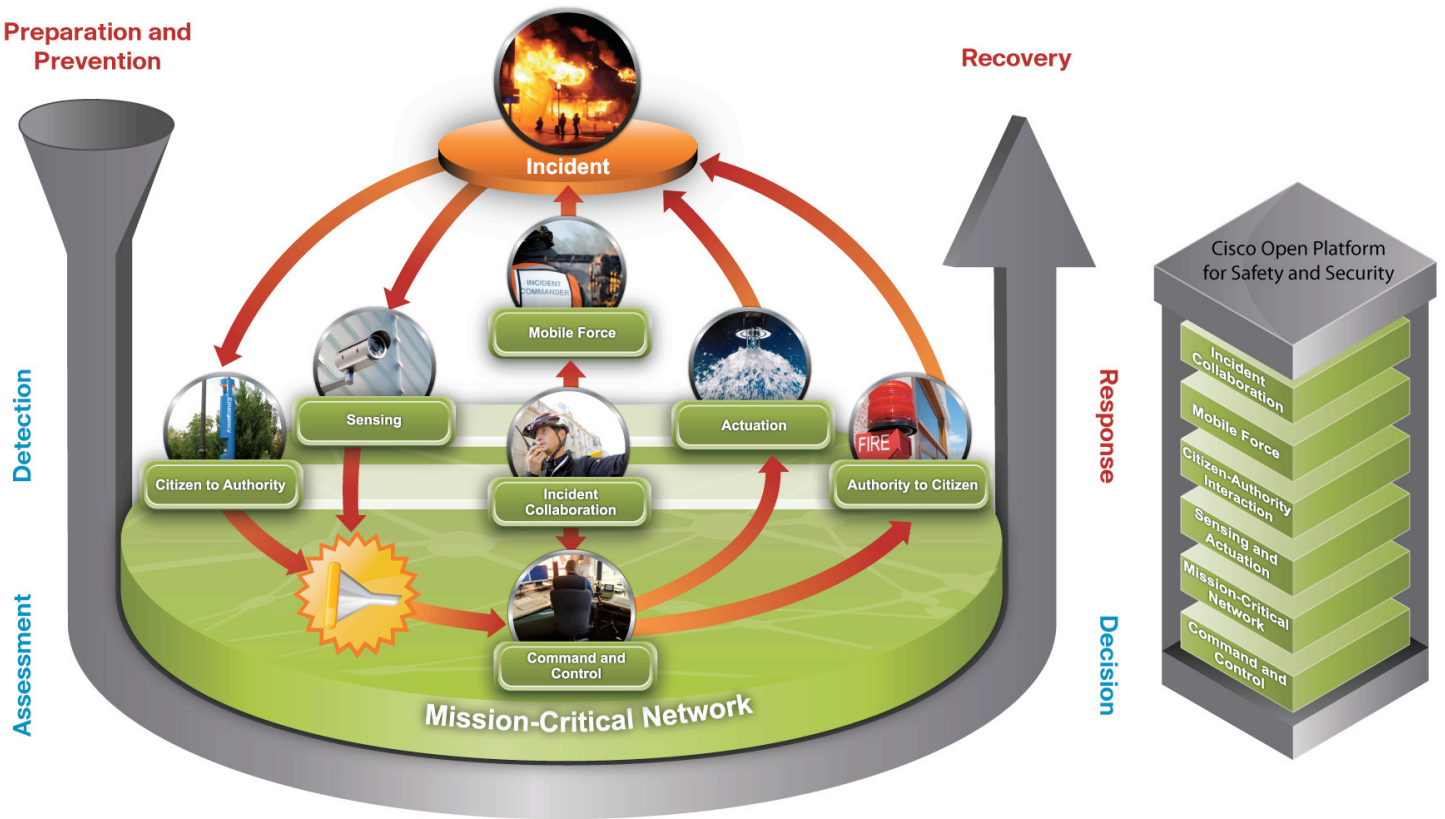
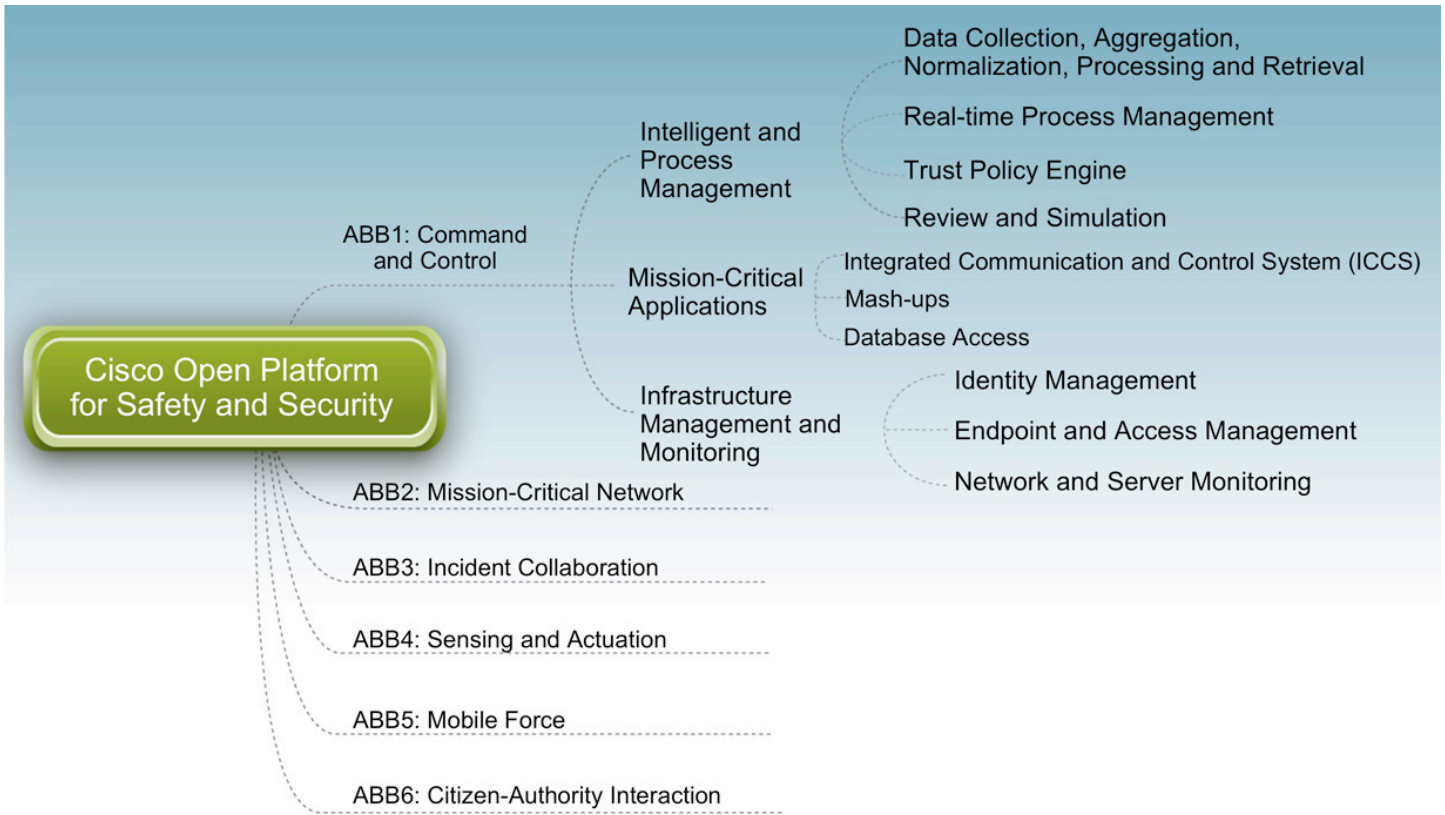


Figure 4 shows the functional elements in the Command and Control architecture building block, and Table 1 lists the enabling solutions from Cisco and its partners.

Figure 4 Command and Control Functional Elements



**Table 1 Products in the Command and Control Architecture Building Block**

	Intelligence and Process Management				Mission-Critical Applications			Infrastructure Management and Monitoring		
	Data Aggregation, Normalization, Processing, and Retrieval	Real-Time Process Management	Review and Simulation	Trust Policy Engine	ICCS	Database Access	Mash-ups	Identity Management	Endpoint and Access Management	Network and Server Management
Cisco Enterprise Policy Manager				✓					✓	
Cisco IPICS				✓						
Cisco Works										✓
Cisco IBNS								✓	✓	
Cisco Security Agent									✓	
Frequentis					✓					
Positron					✓					
SAP		✓	✓	✓		✓				
SwanIsland	✓						✓			
Vialogy	✓	✓								
VidSys			✓		✓					

## Intelligence and Process Management

Intelligence and process management functions include data processing, real-time process management, and review and simulation.

### *Data Collection, Aggregation, Normalization, Processing, and Retrieval*

Today's emergency workers need help to transform continually growing volumes of data into actionable intelligence. The Fusion Center addresses this need by using technology for:

- **Collection:** Open interfaces are used to automatically collect data from other systems, including physical sensors, satellite pictures, videos and photos from surveillance cameras, news services, blogs, Twitter messages, the agency's computer-aided dispatch (CAD) system, other agencies' CAD systems, and so on.
- **Aggregation:** Data from different sources is associated, put into context, and compared.
- **Normalization:** Data is cleaned up by removing duplicates or conflicts and then converted into a standardized format that all agencies can use. An example of a standardized format is Common Alerting Protocol (CAP).
- **Processing:** Different types of data from multiple sources are analyzed, fused together, and transformed into actionable information.
- **Retrieval:** Operators are given an intuitive search interface. The system scores the search results according to the context. In a crisis situation, for example, only the severe events are displayed, while in day-to-day operations, more benign alerts are also displayed.

The goal of the full process is to provide a Common Information Base shared by all participants in the Fusion Center on a need-to-know basis. The Common Information Base also becomes the foundation for the other two capabilities related to intelligence and process management, described next.

### Technology Highlight: ViaLogy



ViaLogy's SPM Sensor Policy Manager combines inputs from multiple networked sensors to provide a complete, real-time operational picture and reduce false positives and negatives. Unlike sensor-management solutions that work only with limited numbers and types of sensors, ViaLogy SPM software fuses and normalizes the inputs from any network-integrated sensor, from any manufacturer, and makes the information available in a distributed manner, from any web browser. Adding a new sensor takes just a few mouse clicks, and ViaLogy can add support for a new type of sensor in 72 hours. ViaLogy SPM triggers real-time actions in response to sensor inputs, thereby improving responsiveness. Fusion center personnel use a simple, secure web browser interface to generate user-defined policies to associate sensor conditions with actions such as notifying emergency personnel.

For more information, visit: <http://www.vialogy.com>

### Real-time Process Management

Fusion Center events that require real-time management include:

- Receiving notifications or requests
- Collecting and analyzing situational information
- Evaluating the status of strategic assets and personnel
- Coordinating and allocating assets and personnel to respond to the incident

As an example, suppose a fire spreads to a nearby building. If firefighters at the scene request more manpower and materials, the real-time process management system contacts other organizations and places requests in their systems. It might also share staff planning information with different units to avoid having all specialists take their holiday at the same time, or to avoid scheduling maintenance at the same time for all fire engines with long ladders.

### Technology Highlight: SAP



The SAP for Security set of solutions increases operational awareness, preparedness, and responsiveness. It combines:

- Risk and intelligence management
- Identity resolution
- Investigative case management
- Command and control with resource deployment
- All solutions are integrated in real time and intended to increase operational awareness, improve operational preparedness, increase responsiveness, and enhance the ability to recover following a threat, incident, or attack.

For more information, see: <http://www.sap.com/industries/publicsector/publicsecurity/index.epx>

### *Review and Simulation*

Improving the effectiveness of emergency operations requires an in-depth analysis of past experiences and simulations of possible future scenarios. As part of the Review function, agencies use data mining techniques to look for patterns that a human might not notice, structured data analysis. These techniques yield valuable information such as:

- The time between the emergency call and the arrival at the emergency scene.
- Estimated, sent out, and needed staff and technical resources at the emergency scene
- Estimated, sent out, and needed technical resources.
- Modus operandi, deduced from operation protocols, recordings of radio traffic, and video material produced during the proceedings.

The companion capability, Simulation, helps to identify measures that might be more effective, based on theory. Sophisticated simulation software can even take the “human factor” into account, using software to record the decisions of people acting out a scripted scenario.

### *Trust Policy Engine*

When different agencies share information, as they do in a Fusion Center environment, they need to enforce trust policies. The Command and Control architecture building block accomplishes this by providing the following capabilities:

- Securing access and usage of information interfaces, applications, and access devices
- Providing appropriate information to individuals based on their role
- Governing who can communicate with whom, including who can initiate a conference and whether certain users can override and disconnect ongoing phone calls if they need the bandwidth for videoconferences or Cisco TelePresence sessions
- Sharing information rapidly as the emergency situation unfolds
- Quickly adding new individuals or agencies to the incident response team

The Trust Policy Engine can flexibly apply different policies depending on real-time conditions. For example, it can determine who is in charge during different types of events, such as a highway fire or major flood. Using one centralized policy engine for all applications ensures consistent application of policy, reduces complexity, and saves time.

### **Technology Highlight: Cisco IP Interoperability and Collaboration System**



Cisco IPICS enables authorized personnel in different agencies to join talk groups using any type of device: radio handsets, telephones, IP phones, mobile phones, and laptops or PCs with special software. This facilitates collaboration because personnel who are outside of radio range can still join talk groups. Dispatchers can also confirm whether all necessary participants have joined a conference. Trust is maintained by using caller authentication and passwords to restrict access to talk groups.

For more information, visit: [www.cisco.com/go/ipics](http://www.cisco.com/go/ipics)

## Mission-Critical Applications

### *Integrated Communication and Control System (ICCS)*

Fusion Center personnel rely on multiple applications, such as CAD, sensors, Early Warning Systems, and real-time video streams from CCTV. Traditionally, they have had to monitor multiple consoles, delaying awareness and response and possibly risking a missed event.

An Integrated Communication and Control System (ICCS) merges information from different sources to provide a Common Operational Picture (COP). The COP increases situational awareness by combining information collected by multiple organizations. For example, it might show the position of units and foreign units, geospatial information, and the location, direction, and velocity of a chemical plume.

A state-of-the-art COP solution integrates information from multiple agencies and multiple systems, provides different information based on the operator's role, can represent events of interest on two- and three-dimensional geospatial maps, provides a rules engine to specify what combination of events triggers an alarm, and includes a dispatch engine.

#### **Technology Highlight: Frequentis**



The Integrated Communication Control System (ICCS) from Cisco and Frequentis enables Fusion Centers to capture information from callers using a variety of devices and media types and forward it to responders on their way to the scene. London's Metropolitan Police Service is using ICCS to enable 23 boroughs to communicate using the national Airwave digital radio system. Boroughs are able to share CCTV images, as well, increasing situational awareness for officers. Frequentis CAD systems provide essential command and control functions. These include receiving emergency calls, mission recording, mission scheduling, alarm, mission control, and management. Incidents and resources can be represented visually with the help of geographic-information-systems (GIS).

For more information, visit: [www.frequentis.com/Internet/PublicSafety/](http://www.frequentis.com/Internet/PublicSafety/)

#### **Technology Highlight: Positron**



Positron's Emergency Communication and Collaboration Platform integrates with Cisco Unified Communications Manager to enable PSAPs to accept citizen communications by VoIP, video, email, or Short Messaging Service (SMS) messaging. It integrates easily with existing equipment and can scale as communications volume increases.

For more information, visit: [www.positron911.com](http://www.positron911.com)

#### **Technology Highlight: VidSys**



VidSys Situation Management and Video Management applications enable fusion centers to integrate all of their physical security assets and to quickly identify and resolve real-time security situations. The web-based software system enhances the surveillance and management of borders, unmanned remote locations, valued assets, and buildings and campuses. Surveillance can be conducted from a central command center, regional command centers, or field operations centers and mobile devices.

For more information, visit: [www.vidsys.com](http://www.vidsys.com)

### *Mash-ups*

A mash-up is a novel presentation of two or more pieces of information that are already available, such as web content, text, images, or video. A familiar example is the association of Google Maps with real estate data, creating a distinct web service. If a citizen presses an emergency button at a train station, the response in the Fusion Center might be to create a mash-up of images from nearby CCTV cameras, the phone location superimposed on a map, and information from nearby water, heat, and smoke sensors.

#### **Technology Highlight: Swan Island Networks**



Swan Island Networks offers TIES, a managed service that gives public safety and enterprise crisis management professionals a platform to fuse open-source and proprietary information from thousands of sources. The service filters data for relevance and presents it as a user-defined operational picture to trusted and authorized decision-makers. TIES creates an online virtual watch center, bringing together such diverse data as local, national, and global incident maps; emergency-number feeds; weather data; flood maps; health advisories and alerts; and traffic information. It disseminates alerts and notifications of potentially disruptive events to web-based and mobile clients.

For more information, visit: [www.swanisland.net](http://www.swanisland.net)

### *Database Access*

Fusion Center personnel do not directly access other agencies' databases. Instead, they access the ICCS application, which performs the queries. An example of a distributed database is the U.K.'s Police National Database. It will provide the 43 police forces in England and Wales with immediate access to up-to-date information from across the service, overcoming geographical and jurisdictional boundaries. Initially, the database will contain information related to criminal investigations, intelligence reports, and child and domestic abuse.

The database access function in the Command and Control architecture building block include:

- Enabling mobile users to perform searches
- Querying multiple databases at once
- Ensuring that data is accurate, up-to-date and consistent
- Restricting data access to authorized users
- Preventing unwanted manipulation of data
- Ensuring data integrity—for example, when multiple users try to write data
- Protecting data in transit through encryption
- Recording access attempts and actions

## Infrastructure Management and Monitoring

Infrastructure management and monitoring functions includes identity management, endpoint and access management, and network and server monitoring.

### *Identity Management*

Identity management systems enable role-based access to Fusion Center services. The system enables an administrator to add users, authorizes the users when they attempt to access systems or information, and records all access attempts. Other types of identity management systems are needed for physical access controls, such as when staff enter and leave secure or restricted incident scenes. First responder authentication credential (FRAC) solutions authenticate and validate the identities and roles of individuals using smart cards with bar codes, magnetic stripes, RFID tags, or biometrics.

#### **Technology Highlight: Cisco Identity-Based Networking Services**



Cisco Identity Based Networking Services (IBNS) combines several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. Cisco IBNS helps emergency organizations enforce policy compliance while simplifying administration.

For more information, visit: [www.cisco.com/go/ibns](http://www.cisco.com/go/ibns)

### *Endpoint and Access Management*

Devices that personnel use to connect to the Fusion Center network must not introduce infections or allow theft of information. In the Cisco Open Platform for Safety and Security, the Endpoint and Access Management is performed by the Mission-Critical Network architecture building block. Capabilities include:

- Personal firewalls for protection against network-borne threats
- Antivirus scanners to detect file-based threats
- Audit or integrity products to detect malicious configuration activity
- Network Admission Control (NAC), which ensures that the user's endpoint complies with the organization's security policies for antivirus software, operating system patches, and so on. If a device is noncompliant, the NAC solution remediates the device without any intervention from the user or the IT department.
- Host Intrusion Prevention System (HIPS) that detects anomalous behavior suggesting an infection. HIPS helps to prevent damage from attacks or from viruses whose signature is not yet known.

#### **Technology Highlight: Cisco Enterprise Policy Manager**



Cisco Enterprise Policy Manager helps Fusion Center personnel enforce entitlement policies for access to applications and information. It replaces application-specific policy managers, which reduces costs and ensures consistent enforcement. Access can be controlled based on user profile, the nature of request, time of day, and environmental attributes.

For more information, visit:

[www.cisco.com/en/US/products/ps9519/Products\\_Sub\\_Category\\_Home.html](http://www.cisco.com/en/US/products/ps9519/Products_Sub_Category_Home.html)



### Technology Highlight: Cisco Security Agent

Deployed on PCs in the Fusion Center, Cisco Security Agent combines defense against zero-day threats, enforcement of policies regarding data loss prevention, and antivirus protection. Fusion Center personnel can establish lists of allowed and unwanted behavior, such as copying data to external media or initiating email blasts. Stopping behaviors rather than simply looking for signatures protects against zero-day threats, before a signature is known.

For more information, visit: [www.cisco.com/csa](http://www.cisco.com/csa)

### Network and Server Monitoring

Fusion Center personnel need to know that critical resources are available and receive timely alerts of potential problems. The Network and Server Monitoring function is shared with the Mission-Critical Network architecture building block. It enables network managers to centrally monitor all wired and wireless network elements and services across a LAN, WAN, or metropolitan area network (MAN). Services include:

- Alerting when network equipment fails
- Performance monitoring for network equipment and troubleshooting of network-related issues, including a visual representation of traffic bottlenecks



### Technology Highlight: CiscoWorks

CiscoWorks enables organizations to manage and monitor all network elements and services across LAN, WAN, and remote network components.

For more information, visit: [www.cisco.com/go/cisoworks](http://www.cisco.com/go/cisoworks)

### 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 Command and Control architecture building block provides:

- Intelligence and process management to fuse information from multiple locations into a Common Information Base
- Mission-critical applications, including ICCS, mash-ups, and database access
- Infrastructure management and monitoring to help ensure that critical information and services are available when needed

### For More Information

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

 CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card 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. (0907R)