



Cisco Open Platform for Safety and Security: Understand the Mission-Critical Network 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 Mission-Critical Network building block. It provides the following services:

- Resiliency
- Network virtualization
- Traffic optimization
- Mobility and location
- Management and monitoring
- Storage
- Identity
- Unified Communications
- Compute
- Application networking
- Security

“In the aftermath of Hurricane Katrina, a unitary reliance on Land Mobile Radio (LMR) systems failed public safety agencies, leaving them without any source of communications once they lost transmission capability. Unfortunately, in the wake of this tragedy, many have dusted off traditional prescriptions for improving public safety communications.”

Source: Toward a Next Generation Strategy: Learning From Katrina And Taking Advantage Of New Technologies white Paper – Mobile Satellite Ventures

The Role of the Mission-Critical Network in Safety and Security

First responders and rescue teams on the front line depend on network connectivity to share information needed for an effective response. The Mission-Critical Network building block meets the full set of requirements:

- **Technology evolution:** Public safety agencies want to extend new applications to first responders on their handheld devices. Modern applications include real-time video, maps with satellite imagery, Global Positioning System (GPS) tracking, and global database searches.
- **Shared services:** Increasingly, state and local governments are implementing shared networks and storage for multiple agencies and departments. Each agency can keep its own resources isolated, sharing them selectively when needed for a collaborative response. This approach reduces capital and operational costs and also simplifies collaboration.
- **Ubiquitous access:** First responders need to be able use land-mobile radio (LMR) systems from any location, including inside buildings.
- **Reliability:** Mission-critical networks must continue to operate during any type of disaster, including hurricanes, earthquakes, fires, or high-powered blasts caused by a bomb.
- **Cyber Security:** Public safety agencies need to protect sensitive information and guard against attacks that could take down the network.
- **Communications interoperability:** Public safety personnel need to collaborate within their own agencies as well as with interagency task forces. They need the flexibility to adopt new communications standards as they are introduced, while protecting their existing investments in networks and devices.

The Mission-Critical Network does much more than transport data packets. Rather, it provides the platform for all of the other architecture building blocks (Figure 1). As the platform, the Mission-Critical Network provides a collection of integrated network services and proven designs for different places in the network (Table 2). The remainder of this white paper describes these components.

Figure 1 The Mission-Critical Network Building Block Forms the Foundation for the Other Building Blocks

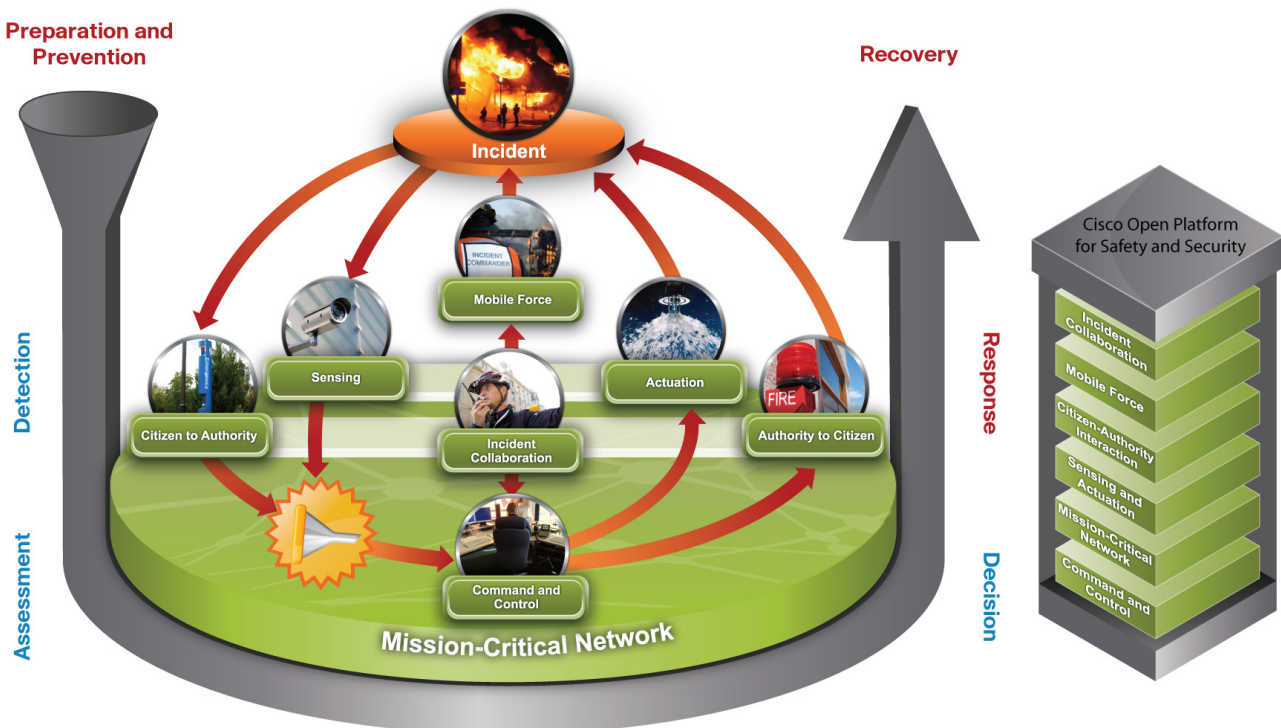


Table 2 Solutions in the Mission-Critical Network Building Block

	Resiliency	Network Virtualization	Traffic Optimization	Mobility and Location	Network Management and Monitoring	Storage	Identity	Unified Communications	Compute	Application Networking	Security
Cisco IOS Software	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Cisco Wireless and Mobility Solutions				✓	✓						✓
CiscoWorks Network Management Solutions					✓		✓	✓			✓
Multilayer Data Center Solution	✓	✓			✓	✓			✓	✓	✓
Cisco Trust and Identity Management					✓		✓				✓
Cisco ISR Multiservice Routers, Catalyst Switches	✓		✓	✓	✓			✓		✓	✓
Cisco Unified Computing		✓			✓	✓			✓	✓	
Cisco Wide Area Application Services, Cisco ACE Application Control Engine, Cisco AVS Application Velocity System, Cisco Application Content Networking Solution	✓		✓		✓	✓				✓	
Cisco Self-Defending Network Solution					✓		✓				✓

Integrated Network Services

The network services integrated into the Mission-Critical Network building block include resiliency, network virtualization, compute, storage, traffic optimization, mobility and location, management and monitoring, identity, unified communications, application networking, and security.

Resiliency

During emergencies, first responders and commanders rely on the network to access information and people that will help them protect lives and property. To build a resilient network you need technologies that provide reliability, redundancy, and survivability:

- **Reliability:** Reliability refers to the quality of voice, video, and data. Grainy video or garbled voice, for example, are unacceptable. Resiliency services include Quality of Service (QoS) to assign priority to latency-sensitive traffic. They also require adequate bandwidth.
- **Redundancy:** First responders need to be able to communicate with headquarters under any circumstances. If one network is destroyed or otherwise unavailable, personnel at the incident scene need another means of access. Many organizations use wireless or satellite networks as a fall back.
- **Survivability:** Survivability refers to the ability to maintain command-and-control operations at the incident scene even if all redundant networks become unavailable. You can accomplish this by establishing an ad hoc meshed network between all remaining nodes, including first responder vehicles.

Some resiliency services are integrated into devices and others are implemented at the network level. Examples of device-level resiliency features include nonstop forwarding with stateful switchover and unidirectional link detection. Examples of network-level resiliency services include routing protocol enhancements and EtherChannel.

Network Virtualization Services

Network virtualization refers to consolidating multiple WANs or SANs into one, and then provisioning multiple virtual networks. For example, a state or local government can build a single SAN and provision multiple virtual SANs, one for each agency or department. Network virtualization enables organizations to more quickly provision new network resources when needed. It improves device utilization to reduce capital costs. And it reduces operational costs because the IT department can manage many assets as a single resource.

Compute Services

Just as network virtualization services consolidate and virtualize network resources, compute services consolidate and virtualize server resources. Rather than tying each operating system to a particular server, you enable the operating system to operate on any available server, when needed. Advantages of virtualizing compute services include:

- You can consolidate the workloads from underutilized servers onto a smaller number of fully utilized servers. This reduces hardware costs, management overhead, and energy consumption.
- Multiple versions of applications can run on a single operating system without conflict.
- The same version of an application can run on multiple operating systems without modification.
- Application upgrades and patches take less time.

Storage Services

Storage services enable public safety agencies to securely store information collected before, during, and after a crisis. The information can come from video surveillance cameras, sensors, or communications systems. The storage services in the Mission-Critical Network building block provide the following functions:

- **Consolidation:** Instead of maintaining a separate network and storage for each department or application, you can consolidate them into a single, scalable SAN that is less expensive and easier to manage.
- **Virtualization:** IT managers can quickly provision new virtual SANs (VSANs) on the consolidated SAN. Each VSAN is logically separate from the others, ensuring privacy, and not affected by outages on the others.
- **Security:** Data is protected at rest and in transit.
- **Availability:** Access to data from remote disaster recovery data centers.
- **Data replication:** The agency can copy data from a host server to another server in any location, not necessarily in the same data center

Traffic Optimization Services

Traffic optimization services help to ensure that voice, video, and data traffic arrive at their destination in timely fashion. One aspect is assigning priority to packets based on the application type or sender. For example, video transmitted from an incident scene to fire fighters should take priority over training video. Techniques used for traffic optimization include:

- IPv6
- Quality of Service (QoS) and multicast support
- Load balancing
- Traffic engineering
- Layer 2 and 3 VPNs

Mobility and Location Services

Mobility and location services take advantage of wireless networks (WiFi, cellular, radio, and others) to extend all resources available to headquarters personnel to the field. First responders can use in-vehicle laptops and handheld devices to access to information such as real-time video captured at the incident scene, hazmat databases, floor plans, information about road closings and aid resources, the location and case histories of people at the scene.

Location services are a distinct type of mobility services. They enable first responders and security personnel to identify the location of assets within a few feet, using radio frequency (RF) technology. This enables them to locate wireless devices as well as any other asset affixed with an RFID tag. Location services are useful to locate mobile assets such as crates of emergency supplies, and also to find out quickly if high-value assets have been moved. The Mobility and Location services in the Mission-Critical Network building block include the technology to display the location of thousands of devices, superimposed on a site floor plan.

Unified Network Management and Monitoring Services

Network managers use the Unified Network Management and Monitoring service to centrally monitor and configure all wired and wireless network elements and services. They can manage elements 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 showing a visual representation of traffic bottlenecks
- Reporting on the network and equipment
- Automatically discovering new devices added to the network
- Enforcing access rules

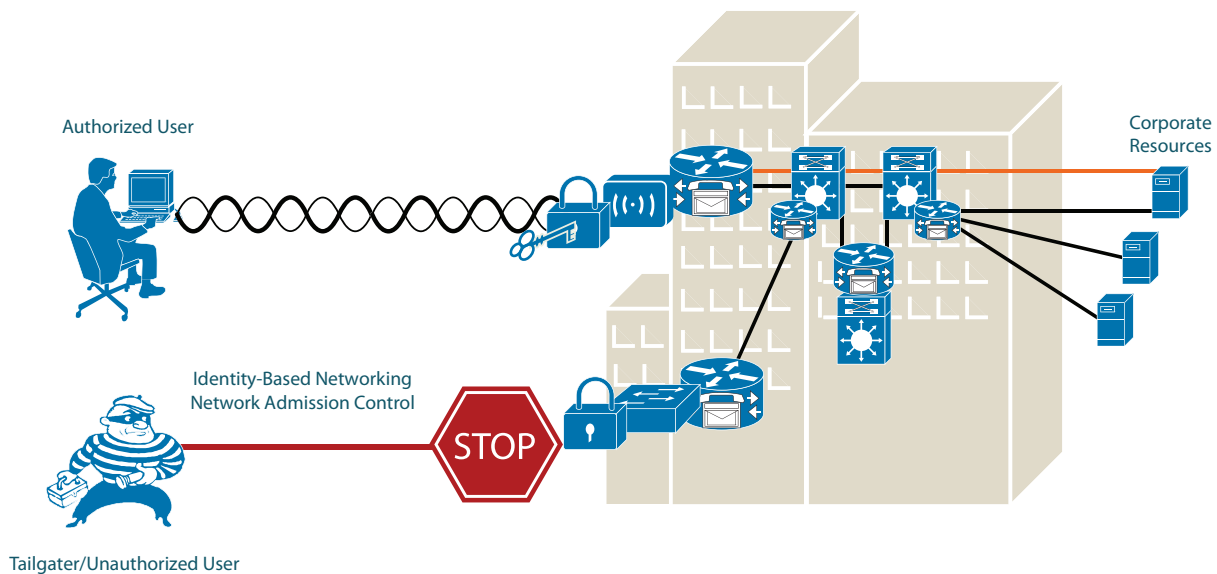
Identity Services

Many countries are currently developing national credentialing systems to identify police, fire, and emergency medical professionals. The Identity services in the Mission-Critical building block enable public safety organizations to create, manage, and authenticate credentials so that they can:

- Verify the identity of service personnel and people visiting sensitive areas of a building or incident scene
- Deny access to and report individuals who represent themselves as service or delivery personnel but do not have the appropriate credentials
- Maintain detailed and accurate records of service and delivery personnel

The Mission-Critical Network building block provides two kinds of identity services (Figure 2). *Identity-based Networking* identifies the user or device on the network and grants access to appropriate network resources. *Network Admission Control (NAC)* 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.

Figure 2 Identity Services



Unified Communications Services

Unified Communications services enable people in the same or different organizations to collaborate using voice, video, and web sharing. The Mission-Critical Network building block provides four main types of Unified Communications services:

- Call routing services direct calls to the appropriate person. Some organizations adopt centralized call processing, distributing services to remote offices over the network. Organizations without adequate connectivity can deploy local call processing in all or some remote offices.
- Distributed voice control services include mechanisms for failover and alleviation of call congestion.
- Network-Integrated Voice Components include gateways and media resources. Gateways enable voice traffic to cross between the public switched telephone network (PSTN) and IP networks. Media resources include conferencing systems and transcoding capabilities.
- IP video services include training applications and video telephony.

Application Networking Services

Application Networking services improve the performance of mission-critical applications by using two technologies:

- *Application delivery controllers* perform real-time data manipulation. They improve the performance of web-based and client-server applications using techniques such as real-time protocol manipulation, protocol offload, load-balancing services, and others.
- *WAN optimization controllers* reduce the volume of traffic that travels over the WAN by caching and repositioning popular data at posts. This reduces bandwidth costs and also reduces latency to create a LAN-like experience.

Security Services

Public safety and security organizations increasingly use web-based applications to reduce client software costs and enable personnel to use any browser in any location. It is essential to protect web-based applications from unauthorized access by individuals who would use the data to cause harm. Table 1 summarizes the security services in the Mission-Critical Network building block.

Table 1 Security Services Combine Threat Defense, Secure Connectivity, and Trust Management

Security Factors	Technologies
Threat Defense	Intrusion detection systems and intrusion prevention systems monitor and respond to security events as they occur. Central management tools define and distribute configurations, monitor and audit device usage, and enforce policies.
Secure Connectivity	VPNs ensure data privacy and integrity during transmission to and from remote locations. Wireless LANs provide security over mobile infrastructures. Firewalls protect the network edge, controlling access to critical network applications, data, and services
Trust Management	Using Authentication, Authorization and Accounting (AAA), the network: <ul style="list-style-type: none"> ▪ Identifies users and the network resources to which they wish to connect ▪ Grants or denies access ▪ Creates audit trails of network access built on standards based protocols like 802.1x

Places in the Mission-Critical Network

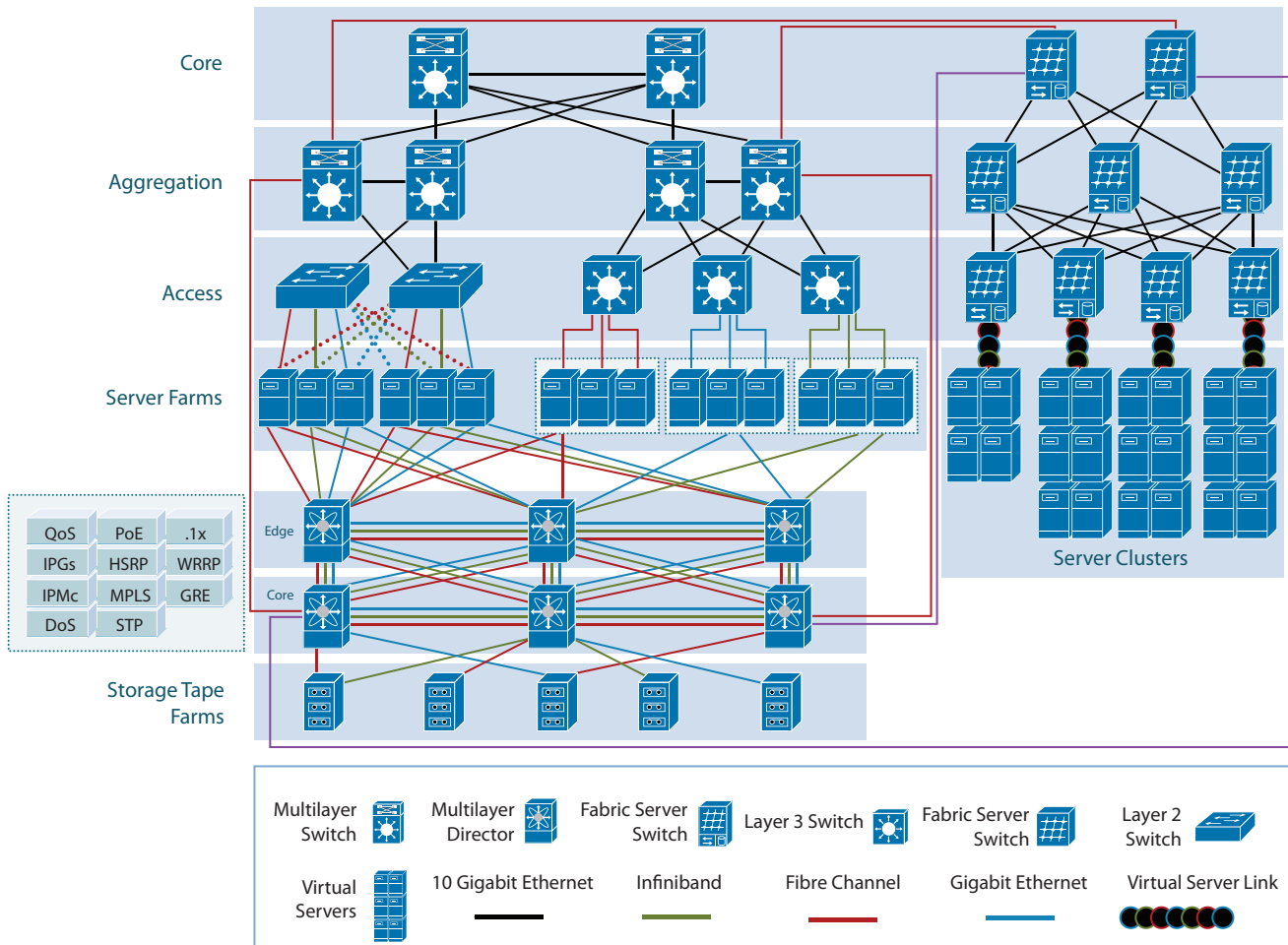
In addition to providing network services, Mission-Critical Network architecture building block also specifies the design for places that require network connectivity. These are the data center, nationwide network, headquarters, remote posts, and the mobile workforce.

Data Center

Home to critical servers, storage, and applications, the data center must be designed for scale, performance, security, and reliability. The data center design in the Mission-Critical Network building block uses a layered approach, shown in Figure 3.

- Core
- Aggregation
- Access
- Server farms
- Edge
- Storage
- Server cluster

Figure 3 Layered Design for the Data Center



Nationwide Network

Individual public safety agencies generally select their own network technologies, making interoperability a major challenge. Most public safety agencies use private WAN connections such as Frame Relay, ATM, or leased-line services. Modern WAN and MAN architectures provide many advantages, but many still lack the capabilities to support VoIP and video, such as high availability, IP multicast, and QoS needed for high-quality voice and video.

The Mission-Critical Network building block provides the technology to build a modern, nationwide public safety network providing wired and wireless networks. Public safety employees can access it using any commercially available technology.

The wired network is based on IP MPLS. Important characteristics include:

- Scalability and reliability, through redundancy and fast reroute (FRR) capabilities
- Support for a wide range of QoS and service level agreement (SLA) requirements
- Optimized bandwidth usage through traffic engineering

Wireless network technologies supported by the Mission-Critical Network building block include private mobile radio (such as Terrestrial Trunked Radio [TETRA] and P25), 3G, WiFi mesh, WiMAX, and satellite. Public safety personnel can connect to the networks using any wireless device, including Push-to-Talk (PTT) radios, laptops, and smartphones. Some of the network technologies have the bandwidth to support large files, such as photographs, fingerprints, structural diagrams, telemetry information, voice calls, and video feeds.

Headquarters

The headquarters environment includes the Dispatch Center, the Emergency Operations Center, and the back-office organization. These entities deliver the services that emergency workers rely on during incident response, such as wired and wireless IP telephony, video, and database access. Therefore, the headquarters infrastructure must be resilient, flexible, and high performing. A weak foundation can be broken by high traffic volume or security threats, causing all building blocks atop it to also fail. A strong foundation, in contrast, scales easily to accommodate higher traffic volumes, larger files, and new services. In the Mission-Critical Network architecture building block, the headquarters design follows Cisco's proven design blueprints for campus networks.

Remote Posts

Remote posts include border control posts, oil platforms, and critical infrastructure such as nuclear plants. Remote posts require redundant network connectivity to help ensure that personnel can always access services housed at headquarters. Like WAN and MAN environments, remote posts are likely to experience degraded network performance because of traffic congestion. The Mission-Critical Network building block addresses this challenge using QoS classification and policing.

Mobile Force

The Mobile Force has its own building block within the Cisco Open Platform for Safety and Security framework. Deployed forces need access to the same information from the field that they would have at headquarters. They need an intuitive interface that is easy to use in chaotic conditions. Examples of ways that emergency organizations can use the Mobile Force building block include:

- Enabling security guards to control video surveillance cameras and view feeds from a smartphone or other handheld device
- Equipping police vehicles with a mobile router so that officers can access law enforcement databases from in-vehicle laptops and transmit video from vehicle-mounted cameras to the command center
- Collecting environmental data from biosensors integrated into firefighter's suits.

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 Mission-Critical Network building block provides:

- The network services required for secure, reliable, network access
- Virtualization services for the network, storage, and compute resources, reducing equipment and management costs and enabling rapid provisioning.
- Unified management and monitoring services
- Proven designs for different places in the network

For More Information

To read more about the Cisco Open Platform for Safety and Security, including partner profiles, visit:

www.cisco.com/web/strategy/government/national-open-platform.html




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)