Cisco Secure Wireless Plant: Security and Quality of Service for Industrial Environments

Today's process industries, from oil and gas producers and mining companies to manufacturers of chemicals, foods, and beverages, are exploring new ways to improve production processes and automate them to raise plant efficiency. By relying on automation, organizations can improve profit margins, enhance monitoring and visibility throughout the facility, achieve compliance with safety standards, and make workers more productive Though each has its own challenges and business drivers, industrialists also have many needs and trends in common. These include:

- Gathering more information from the production process to improve safety, asset utilization, and production yield
- Distributing information in real time to a globally dispersed workforce and field personnel throughout the plant site
- Integrating data from production systems to business applications and partners
- Reducing capital and operating expenses of control systems and IT systems
- Improving safety for workers and security for information
- Meeting increasing regulatory requirements
- Improving connectivity between systems and between personnel
- Improving integration of production systems and IT

However, many companies cannot meet these goals. A significant percentage of organizations still rely on manual methods to oversee production stages, verify the status and condition of facilities, check and maintain equipment, and assemble records for audits. They are falling behind the competition as highly paid personnel spend their time and expertise on basic data collection to keep the plant running.

Many firms have taken a step forward from the manual approach, relying on wired computer networks and control systems to support basic automated monitoring of the physical plant. However, installing wired networks in industrial environments can be prohibitively expensive, limiting the amount of information that is gathered. More data remains to be harvested.

To improve the functionality and efficiency of industrial monitoring and control systems, therefore, process industries are looking toward wireless sensor networks (WSNs) to provide detailed, accurate data collection from previously hard-to-reach, unaffordable areas. In plants still relying on manual oversight, a wireless sensor network may be installed for a fraction of the cost (sometimes up to 90 percent less) of a wired network, which can cost up to US$3000 per foot of cable to install in industrial environments. For plants with a wired control system network already in place, the addition of wireless sensors, commonly called wireless field devices, significantly enhances data collection, expands security perimeters, and brings the organization to a new level of efficiency and productivity.

Cisco and Dust Networks are leading this trend with the Secure Wireless Plant solution, which combines industry-leading networking and field device development to deliver a comprehensive wireless solution for the industrial environment. This powerful technology offers the power to

oversee, remotely maintain, accurately assess, and fully protect every aspect of the facility, its data, and its operation. Based on this solution, operations managers and IT personnel are positioned to enter a new phase of their business, operating with more confidence in their data and able to rely more completely on plant equipment and processes.

What is a Wireless Sensor Network?

Developed during the 1990s, secured WSNs are increasingly being used for a variety of commercial applications, such as monitoring machinery, automatic temperature regulation in buildings and plants, and monitoring of industrial environments such as oil pipelines or storage areas for chemicals. WSNs can also be used to watch for physical attacks on sensitive tanks, buildings, or holding areas, or for equipment malfunctions caused by an Internet-based attack or operator error.

Installed at a critical location, such as on a water pump at a water treatment plant, each field device forms part of a mesh network, acting as both a sensor (or node) and a relay device (or router) to exchange data in brief, coordinated radio transmissions. Each node joins the network to forward data collected by its own sensor or others nearby. The mesh requires little power because each brief transmission travels only a short distance to reach nearby nodes. In practice, this means that batteries can last for five to ten years—sometimes even outlasting the usefulness of the sensor. The mesh, in turn, communicates with a wireless LAN (WLAN) that sends data to the control room for monitoring and analysis.

A mesh network is self-organizing and self-healing, which minimizes maintenance costs and helps to ensure constant availability of information. If one node goes down, the system finds an alternative path for sensor traffic, looking across all the available radio frequencies and enhancing the signal through a spread-spectrum coding technique known as channel hopping. The more devices are attached, the more efficient and resilient the network becomes.

Cisco's powerful networking infrastructure provides the foundation for integrating Dust's sensor networking technology with industrial wired networks, legacy and proprietary systems, and standard Ethernet and non-Ethernet technologies. Based on new specifications for industrial wireless communications, the Secure Wireless Plant solution offers a secured, cost-effective, industrial-grade network capable of supporting the process industry facility's sensor needs.

Sensor Networking Standards

Industrial systems have relied for many years on the Highway Addressable Remote Transducer (HART) Communication Protocol for their control system networks. The HART standard is an early implementation of the wired industrial automation protocol fieldbus, and it is more widely used than any other industrial specification to date. The HART 7 specification, released in September 2007, includes a section for wireless defined as the WirelessHART protocol. Additional support for WirelessHART is planned for the ISA SP100.11 standard, which in its current draft form provides for multiple protocols utilized by a single wireless infrastructure.

The WirelessHART protocol has opened the door to a broad implementation of wireless within industrial environments. It allows organizations to take advantage of full backward compatibility with existing instrumentation and host systems, benefiting from the easy deployment and cost savings of wireless networking while protecting existing investments in HART-enabled devices, tools, training, applications, and procedures.

Highly Available Sensor Networking

The Secure Wireless Plant solution supports WirelessHART-enabled devices based on the time-synchronized mesh networking technologies and protocols pioneered by Dust Networks. WirelessHART devices remain synchronized with each other and communicate in dynamic timeslots, offering redundancy and failover to ensure high reliability even in challenging radio environments. With radios only turned on for scheduled periods, WirelessHART devices use frequency hopping to avoid interference: Data packets traveling between devices are sent on different radio channels depending on the time of transmission or the level of interference seen on a particular channel.

Time-Synchronized Communication

In a WirelessHART system, all devices share a common sense of time so that they transmit, listen, or sleep during communication windows called timeslots. Timeslots are measured in milliseconds, and in typical applications this leads to a duty cycle of less than 1 percent for all nodes in the network, including those relaying messages for neighboring nodes. Thus WirelessHART systems are ultra-low-power networking solutions, greatly extending battery lifespan. A common sense of time enables many network advantages:

- Bandwidth can be preallocated to ensure extremely reliable transmission and zero self-interference.
- Transmitting nodes can effectively change frequencies on each transmission and the receiving node can keep in lockstep.
- Bandwidth can be predictably and methodically added or removed at will to accommodate traffic spikes.

Frequency Hopping

In addition to enabling wireless media by “slicing” time, WirelessHART also slices across frequency. This provides robust fault tolerance in the face of common RF interference and a great increase in effective bandwidth. Commonly referred to as frequency hopping spread spectrum (FHSS), hopping across multiple frequencies is a proven method for sidestepping interference and overcoming RF challenges with agility rather than sheer power.

Another technique used in WirelessHART, direct sequence spread spectrum (DSSS), provides a few decibels of coding gain and improvement in multipath fading. By combining FHSS and DSSS, WirelessHART provides both interference rejection (FHSS) and a coding gain (DSSS).

When a new WirelessHART device joins the network, it receives synchronization information and a frequency hopping sequence from each of its parent nodes. In this way, each pairwise connection is ensured to be on a different channel during each timeslot, enabling broad use of the available band in any one location.

Automatic Node Joining and Network Formation

A key attribute of WirelessHART is its ability to self-organize a mesh network. Every WirelessHART device has the intelligence to discover its neighbors, measure the RF signal strength of these connections, acquire synchronization and frequency hopping information, and establish communications.

The network ID, which is included in all communications, allows multiple WirelessHART-based networks to operate in the same radio space without the risk of sharing data or misrouting information. If a device attempts to join a network and detects devices with a network ID not

matching its own, it continues unsynchronized listening until it hears a device with the right ID. Network integrity is also protected by a “join key” that encrypts a request to join the network. If a device has the wrong join key, its join request is ignored and it reverts to unsynchronized listening.

Fully Redundant Mesh Routing

Every WirelessHART device also has the ability to route traffic from neighbors as dictated by requirements of RF connectivity and network performance. A network is simply a set of devices that share the same network ID and password and are synchronized with each other. A gateway node serves as the timing master and relays configuration information to the other network nodes. It also serves as the point through which the wireless data from the WSN interfaces with the Cisco Wi-Fi mesh backbone (see Figure 1).

Fully redundant mesh routing is essential for WSNs in industrial settings where RF conditions change dramatically over time due to weather, new or unknown RF systems, and moving equipment and plant workers. The router nodes themselves do not use significantly more battery power than nodes that are only sensing. Routing algorithms are also used to dynamically balance the load across the network, further improving battery life. In some cases, field devices can use power scavenging technology, such as solar or vibration scavenging.

Security and Quality of Service

Because there is no need for a physical connection, wireless networking can sometimes be perceived as being less safe than wired networks. In particular, some plant managers and administrators are concerned about the possibility of jamming, malicious eavesdropping, and performance problems.

Security

Wireless sensor networks deployed in a mesh configuration can be among the most secure networks available—equivalent to a wired system. The frequency-hopping protocol of WSNs has proven an efficient means of coordinating node communications: It has been demonstrated that more than 1000 WirelessHART devices can operate in the same radio space without affecting end-to-end reliability. All measurement and control traffic in the network is protected by end-to-end encryption, message integrity checking, and authentication as well as procedures for devices joining the WSN, key establishment, and key exchange.

It is true that traditional point-to-point wireless networks can be vulnerable to industrial issues of RF interference, changes in the position of the device, reconfiguration of the environment, or simple node failure due to damage or a power surge. However, in a mesh architecture, the network isolates any individual points of failure and eliminates or mitigates their impact, allowing the network as a whole to maintain reliability in spite of local failures. The security features provide:

- **Confidentiality:** End-to-end data encryption using 128-bit AES encryption algorithm is employed in the packets to prevent sensitive data from being intercepted.
- **Data integrity:** Data transmitted within the packets is protected by message integrity codes to ensure that it has not been tampered with and that it originated from a known source.
- **Replay protection:** Replay attacks are prevented on both the link layer and the network layer by using nonrepeating replay counters.
- **Denial-of-service (DoS) protection:** DoS attacks are mitigated with a combination of all of the above. In addition, the slotted channel hopping protocol diminishes the risks of a DoS attack by using the entire radio space.

- **Access control:** The source address of a WSN packet is verified with a secure key to prevent device spoofing.
- **Compartmental security:** Loss of any one piece of data does not compromise the entire network.

In industrial environments, the physical strength of the equipment is also important. High-quality mesh network equipment is based on ruggedized enclosures that protect against harsh industrial conditions as well as rain, lightning, wind, and vibration from storms or road traffic.

A well-designed wireless mesh architecture transparently adapts to changing environments, allowing long-term operation with little or no maintenance. Wireless sensor networking technology is able to provide extremely high reliability and predictability for up to years at a time, without constant tuning by technicians. In fact, many of the older control network technologies that plants still rely on, such as distributed control systems (DCSs), are far more vulnerable to attack and poor service performance.

Quality of Service

Plant administrators are also looking for a high quality of service (QoS), the ability of a network to provide outstanding performance on selected real-time or critical network traffic. QoS is the measure of transmission quality and service availability of a network. The transmission quality of the network is determined by transmission latency, jitter, and loss.

QoS is based on the concept of differentiated services, where data packets are marked with different priority levels corresponding to the type of service. The ISA 100 committee has defined six different classes of wireless automation:

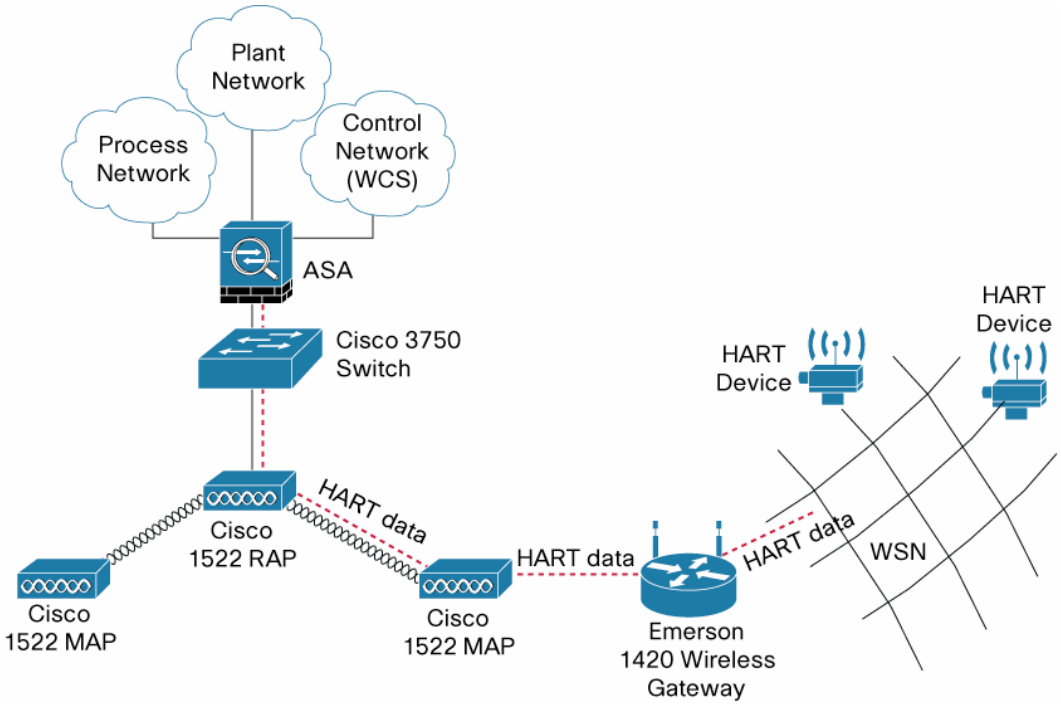
- **Class 0:** Includes safety-related actions that are critical to personnel and plant, such as safety-interlock, emergency shutdown, and fire control.
- **Class 1:** Motor and axis control as well as primary flow and pressure control.
- **Class 2:** Longer time constants, with timeliness of communications measured in seconds to minutes.
- **Class 3:** Includes actions where an operator, rather than a machine, “closes the loop” between input and output. Such actions may include taking a unit offline when conditions so indicate.
- **Class 4:** Monitoring with short-term operational consequences, including high-limit and low-limit alarms and other information that might instigate further checking or dispatch of a maintenance technician.
- **Class 5:** Monitoring without immediate operational consequences. Some, such as sequence-of-events logs, require high reliability; others, like reports of slowly changing information of low economic value, need not be so reliable, as loss of a few consecutive samples may be unimportant.

With QoS, plant administrators manage bandwidth more efficiently across the network based on these class definitions, providing enhanced and predictable network service by supporting dedicated bandwidth for critical users and applications, controlling jitter and latency, and minimizing congestion.

The Cisco Approach to WSNs

The Cisco® Secure Wireless Plant solution is built upon the sensor networking technologies of Dust Networks and the family of products that make up the Cisco Unified Wireless Network Architecture. This powerful infrastructure delivers scalable, manageable, and secure WLANs to support meshed sensor networks. It includes RF capabilities with transparent connection through Cisco's 802.11 wireless networks to the control room and corporate IT systems. The Secure Wireless Plant solution provides industrial organizations with the same level of security, scalability, reliability, ease of deployment, and management for WLANs that they already expect from their wired networks. (See Figure 1.)

Figure 1. Cisco Secure Wireless Plant Solution



This capability is built upon the Cisco Aironet® 1500 Series of lightweight outdoor mesh access points, which connects field devices into a single network and provide automated capabilities to help reduce deployment and maintenance costs. These include intelligent routing, which allows the access point to sense the best possible path for each packet of data, and optimizing the network and choosing new routes or resetting if exposed to radio interference or outages. Cisco Radio Resource Management (RRM) software enables access points to monitor each environment and adjust channels and frequencies in real time to avoid interference from other devices.

The access points in turn are managed and monitored by the Cisco Wireless Control System (WCS), a centralized platform for WLAN planning, configuration, and management. Cisco WCS allows IT managers to design, control, and monitor enterprise wireless networks from a single location, simplifying operations. It oversees a series of WLAN controllers, which are responsible for networkwide wireless functions such as security policies, intrusion prevention, RF management, QoS, and mobility. Cisco WCS itself facilitates load balancing and traffic management, policy provisioning, network optimization, troubleshooting, user tracking, and monitoring for end-to-end security.

With this flexible infrastructure, the embedded intelligence in each device ensures that networks can be built very easily, without even the need for a site survey. This marked departure from the static infrastructure of the traditional point-to-point wireless network has enabled significant advances in ease of use and network flexibility. The Cisco network gateway is simply connected through a wired Ethernet connection directly to the Cisco network switch.

Zero-Touch Configuration and Deployment

The Dust sensor network can be easily deployed based on the Lightweight Access Point Protocol (LWAPP), which enables each access point to automatically discover its controller and download the correct configuration and software for its role in the wireless mesh. The intelligent sensors in turn discover the access points as they are deployed.

Once the system is up and running, having better visibility and control of the RF environment reduces operational costs for operations and IT administrators. Up to tens of thousands of indoor and outdoor lightweight access points are automatically managed by the WLAN controllers, which are in turn centrally managed by Cisco WCS. The intuitive user interface of Cisco WCS allows personnel to easily configure, monitor, and troubleshoot the network with minimal training.

The Self-Configuring and Self-Healing Network

The Cisco Aironet 1500 Series access points can be installed anywhere power is available, without the need for a network connection. Intelligent wireless routing based on LWAPP allows a remote access point to dynamically optimize the best route to the connected network within the mesh, providing resiliency against interference and helping ensure high network capacity. LWAPP also performs a smoothing function to signal condition information, ensuring that the ephemeral nature of RF environments does not affect network stability.

Deployment and management costs for the access points are reduced through support of zero-touch configuration deployments and through the ability of the access points to bring themselves back to operational status (self-heal) in response to interference or outages.

Robust Embedded Security

Security of data transmitted over the sensor network is enforced by requiring that all messages be encrypted, authenticated, and checked for integrity. This is enabled by Dust's end-to-end encryption, message integrity checking, and authentication, as well as procedures for devices accessing the network, key establishment, and key exchange.

Within the wireless network, Cisco provides multiple additional layers of protection, including:

- **RF security:** Detects and avoids 802.11i radio frequency interference and controls unwanted signal propagation.
- **WLAN intrusion prevention and location:** Detects and locates rogue access points or field devices, as well as potential wireless threats such as an attempt to eavesdrop, which helps IT administrators to quickly assess the threat level and take immediate action. Replay attacks are prevented on both the link layer and the network layer by using non-repeating replay counters. The slotted channel hopping protocol diminishes the risks of a DoS attack by using the entire radio space.
- **Network Access Control (NAC):** Enforces policies pertaining to access point configuration and behavior to help ensure that only recognized sensors can gain access to the network.
- **Secure mobility:** Maintains the highest level of security in mobile environments with Cisco Proactive Key Caching, an extension to the 802.11i standard and precursor to the 802.11r

standard.

- **Certificates:** Use of X.509 certificates and AES encryption for LWAPP transactions. This X.509 and AES encryption is embedded into the wireless mesh solution with each LWAPP transaction and all encrypted traffic.
- **Encryption:** CCM mode is used in conjunction with the AES-128 cipher to provide authentication and encryption on backhaul links.
- **Data integrity:** Data transmitted within the packets is protected by message integrity codes to ensure that it has not been tampered with and that it originated from a known source.
- **Segmentation:** Supports creation of virtual LANs (VLANs) that protect sensor networks by separating them and their traffic from other company networks (also known as flow isolation).

In addition, identity-based networking enables individualized security policies for sensors with different access rights, device formats, and application requirements. Security policies include:

- **Layer 2 security:** 802.1X (PEAP, LEAP, TTLS), WPA, 802.11i (WPA2), 802.11w
- **Layer 3 (and above) security:** Integration with wired intrusion prevention systems (IPSs)
- **Access control lists:** IP restrictions, protocol types, ports, and differentiated services code point values
- **Authentication, authorization, and accounting/RADIUS:** User session policies and rights management

802.11 Quality of Service

In the Cisco Secure Wireless Plant solution, the QoS standard for the sensor networks is based on 802.11e-2005, an approved amendment to the IEE 802.11 standard. This specification defines a set of QoS enhancement for WLAN applications through modifications of the MAC layer, allowing QoS to be configured with great precision. QoS-enabled access points have the ability to request specific transmission parameters (such as data rate or jitter) that allow more complex applications to work more effectively on the Wi-Fi network.

Based on this standard, the capabilities of the wireless network for providing a high-quality data stream are enhanced through a new coordination function, the Hybrid Coordination Function (HCF). This provides two methods of channel access, both of which define traffic classes to help differentiate high-priority and low-priority traffic.

Robust Software

The Cisco mesh solution software provides robust, optimal parent selection and fast convergence to help nodes organize themselves quickly and support better mesh network management. It includes mechanisms to guard against stranded access points, as well as a software-based recovery mechanism so that engineers or administrators do not have to dispatch a technician to the access points any time one goes down. The network automatically recovers from misconfigurations, such as a wrong IP address, DHCP server errors, bridge group name typos, or misprovisioning of the network. In addition, Cisco's "exclusion list" algorithm allows a child node to intelligently exclude a parent node in case of a routing problem, and only return to the relationship based on the parent node's subsequent behavior.

Scalability

The Cisco mesh architecture makes it easy to scale coverage as capacity needs dictate, including increasing access point density; adding wired connections, controllers, and radios; and using dual

high-powered, high-sensitive radios and a selection of high-gain antennas. The Cisco Aironet 1500 Series mesh access points can scale to 24 controllers, each with up to 16 Multiple Beacon Service Set Identifiers (MBSSIDs) that support segmentation of the wireless sensor network, and 256 virtual local area networks (VLANs), while each controller can support more than 100 access points. Capacity in a mesh network can be easily increased by adding mesh access points at the edge of the network or configuring more rooftop access points in the network.

Power Management

The Dust sensors in the Cisco Secure Wireless Plant solution are tailored for use in battery-powered and energy-scavenging wireless devices for applications that demand proven performance and scalability. Based on an IEEE 802.15.4-compliant design and power amplifier, each enables up to a decade of battery life on a pair of AAA batteries. All sensors function as both battery-powered routers and nodes, enabling a full mesh topology that provides more redundant routes and higher performance. Integrated radio circuitry components eliminate the burden of complex RF design, requiring only a simple antenna connector for wireless connectivity.

Coexistence with Other Wireless Networks

Wireless networks need to be designed to coexist with other wireless networks in the vicinity. Since the 2.4 GHz band is a shared spectrum, coexistence helps to ensure a high standard of performance. As defined by the IEEE, coexistence is the ability of one system to perform a task in a given shared environment, where other systems have an ability to perform their tasks and may or may not be using the same set of rules. Collisions and coexistence issues can happen when two or more packets overlap in both time and frequency with sufficient energy to interfere with one another.

The Cisco Secure Wireless Plant solution addresses this issue with support for:

- The density enabled by the Cisco mesh network architecture, which allows more than 1000 WirelessHART devices to operate within the same radio space.
- Time-division multiplexing (TDM), a synchronized system that reserves time slots for a specific communication link. This technique is supported by the ISA 100.11 and WirelessHART protocols.
- Code-division multiplexing, which utilizes single code systems such as DSSS to operate in the same frequency region with minimal or no interference.
- Frequency diversity, in which wireless devices dynamically choose different channels of operation, including Bluetooth, DSSS, or non-periodical systems such as ZigBee.
- The ability to control the power transmissions of sensors in areas where they might cause interference with neighboring devices.

Benefits of the Cisco Secure Wireless Plant Solution

The Cisco Secure Wireless Plant solution provides a compelling set of benefits to industrial managers, administrators, and operations personnel. Wireless sensor networks overcome the challenges of traditional point-to-point wireless networks with a rugged design and adaptability that makes them an appropriate control network technology for industrial environments.

This open-standards solution helps industrial facilities function more efficiently and effectively. Operations engineers and plant managers gain:

- Additional plant and process information, adding operational insight to improve production

and maintenance management

- Improved workforce productivity
- Better business and plant management
- Advanced services to help tailor solutions to specific plant needs

The self-organizing mesh network fulfills the requirements of industrial environments for highly secure, reliable data collection and plant monitoring that is resistant to interference, damage, and hacking and that coexists effectively with other wireless networks. Its powerful management system allows IT managers to design, control, and monitor wireless sensor networks from a centralized location, thus simplifying operations, reducing the total cost of ownership and achieving a better return on investment. Finally, this sensor network solution saves money by eliminating the need for trenching and cabling in remote locations.

By deploying the Cisco Unified Wireless Network as the Wi-Fi platform for the wireless sensor network foundation, process industry managers also can take advantage of other capabilities that can be cost-effectively added to the same network, allowing them to improve workforce productivity through remote and mobile operations and maintenance, automated workflow management, and mobile worker communications by phone or handheld device. They also gain the option of adding business and plant management applications including security, video surveillance, and people and asset tracking.

To improve the functionality and efficiency of industrial monitoring and control systems, Cisco and Dust Networks give today's process industries the power to remotely maintain, accurately assess, and fully protect their facility, data, and operation with cost-effective wireless sensor networks. By providing the networking infrastructure for multiple wireless capabilities, these two technology leaders not only help industrial organizations address today's needs, but lay the foundation for tomorrow's growth.

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.**

Printed in USA c11-473894-00 05/08