

## Transportation Security— The Benefits of Network-Enabled Security

In a speech to the National Defense Transportation Association on September 16, 2003, Admiral James M. Loy, Administrator of the U.S. Transportation Security Administration, remarked that in the fight against terrorism, nowhere within the transportation security paradigm is a single silver bullet.

“Our ever-evolving challenge and strategy includes a system of systems with integrated, responsive, non-redundant functions, which are designed to work together within an information-sharing environment to close off terrorist opportunities,” Loy says. “These are safeguards beyond passenger and baggage screening such as hardened cockpit doors, training pilots to handle firearms to protect the cockpit, and perimeter security such as cameras, fences, and patrols.”

Security is one of the top priorities of transportation authorities today. Traditional systems—such as video surveillance, access control, and scanning—are being augmented with emerging technologies, such as biometrics, smart cards, and explosive detection systems. However, even with the availability and sophistication of this wide range of security tools, the biggest challenge facing transportation security administrators is the lack of integration

between these systems. This lack of integration limits the ability to quickly and effectively respond to today’s security threats. Security managers must have the tools and technology to quickly combine, analyze, and distribute data from this diversity of security technologies to multiple audiences, using a wide range of media.

Cisco Networked Infrastructure Cisco Systems® is helping airport, roadway, seaport, rail, and bus managers improve the efficiency and cost-effectiveness of point security products. The Cisco® intelligent integrated network infrastructure converges voice, video, and data from traditional and emerging security technologies into a unified resource. Integrating security resources through a common, scalable, secure IP network backbone increases operational efficiency and positions transportation facilities to take advantage of new technologies and services.

The Cisco intelligent network infrastructure provides:

- A *flexible environment* that improves video security coverage by transcending the hard-wired cabling of many traditional security systems to support adds, moves, and changes quickly and cost effectively.



- A *converged voice, data, and video infrastructure* that integrates security information from different systems to improve security responsiveness.
- A *common communications network* that quickly distributes relevant information both to internal security personnel and to external law enforcement agencies using both fixed and mobile computing devices.

### **Flexible Environment Improves Video Security Coverage**

Closed circuit television (CCTV) for video surveillance is a critical element in providing security at commercial airports, bridges, train and bus stations, and other transportation infrastructure. However, the majority of video surveillance systems installed today use outdated technology and with greater demands being placed on existing video surveillance systems, many of these systems are having difficulty meeting expectations. While that technology has served its purpose well for the past two decades, video surveillance systems are rapidly transitioning toward fully digital solutions.

One of the limitations of many traditional systems is that they require a large amount of point-to-point fiber, which can be 50 percent of the total implementation cost. Digital video reduces the demand on the fiber plant by taking advantage of video compression and high-speed networked transport, meaning that the user can deploy more cameras with the same budget.

Storage and retrieval of the stored video is another issue encouraging the migration to digital technology. Traditional recorders for video surveillance are similar in technology to video cassette recorders built for home use. They require human operators to load and unload tapes, as well as a large area for storing tapes. The video recording task is labor intensive, hardware intensive, and difficult to manage.

Video review is equally tedious because there is no instant playback of a recorded event. The tape must be pulled from the recorder and taken to a review station where a security agent analyzes the event. Although in the past that was acceptable, in today's environment where video surveillance is used for preventing terrorist attacks and enabling rapid response, instant playback is a critical requirement.

### **Advantages of Digital Video**

- Digital video enables compression of the video stream, reducing it by as much as 80 percent without losing resolution and up to 99 percent with some degradation.
- Digital video can be transmitted over *standards-based data networks*, speeding data transmission rates from about 90 Mbps to 2.5 Gbps or higher.
- Networks can be made “self-healing” to detect a failure and automatically re-route traffic through an alternate path.
- Networked video allows the camera signal to be multicast to several locations at once, facilitating simultaneous, secure global access.
- The video signal can be stored in the network to provide immediate playback from anywhere on the network and without degradation from multiple viewings.
- Digital video can transparently integrate with applications—such as biometric recognition and automated surveillance—to detect information that is imperceptible to a human observer.
- Digital signal processing makes it possible to analyze the scene for moving objects, motion patterns, license plates, or human faces.



## **Converged Network Improves Responsiveness to Security Events**

Fast threat response is critical to maintaining public confidence that measures are in place to protect their safety. The faster all data related to a security threat is correlated and communicated to security personnel, the faster they can respond in an appropriate and effective manner. In traditional surveillance networks, individual video and alarm data must be sent to security centers for analysis before action can be taken. With network-enabled systems and a common, standards-based communications infrastructure, any node on the network can easily notify any application or security authority anywhere else on the network.

The ability to provide alarm and video surveillance data to multiple monitoring teams simultaneously greatly improves both security-event correlation and responsiveness. Security personnel can correlate security information in real time, activating cameras when an alarm is triggered and using time indexing to quickly correlate events with video images. The video and alarm data can then be transmitted to multiple locations without consuming additional network bandwidth.

Converging all environmental, access, and video events onto a common network with sophisticated applications that integrates access, environmental, motion, and network security alarms enables surveillance teams to respond quicker than before.

## **Common Communications Network Supports Fast Information Distribution**

The use of two-way radios, pagers, cellular phones, and public address systems is critical for communicating information throughout airports, train stations, and other transportation facilities. However, disparate networks and inadequate standards for security make it difficult to ensure that sensitive information will be distributed quickly and sent only to the people who need it, such as first responders, police, and other emergency security staff.

The Cisco converged network infrastructure helps integrate and distribute emergency voice and data communications more quickly, more efficiently, and in a less costly way than ever before. For example, the Cisco wireless LAN solution and in-building surveillance cameras enable streaming surveillance video of a building's interior that can be distributed to multiple operation centers, security agencies, and other first responders. Access to this type of information on a mobile device or over a vehicle network can help emergency personnel evaluate security risks before entering a building.

Cisco offers a common network infrastructure that provides a secure platform for the delivery of consistent, real-time communications. These communications—including such information as situation status updates, instructions, and threat advisements—are delivered using converged data, voice, and video formats to desktop PCs, IP telephones, passenger information systems, roadside display systems, and public address systems.

## **Cisco Networked Security Solution**

The greater cost savings and operational effectiveness that networked video solutions deliver would alone justify the shift to a common network infrastructure. However, these benefits are just the beginning of the possibilities available to transportation operators with the Cisco intelligent networked security solution. Bringing other independent security systems onto a common network infrastructure greatly simplifies the transportation operation's wiring and network management, improves the efficiency of network resources, and provides a scalable, flexible infrastructure.



## Scalability and Flexibility

Today's challenges far exceed those of the past several decades and tomorrow's challenges will continue to evolve. Transportation operators need to know that the network investment they are making today will provide the scalability they need in order to grow and add new applications as they become available, allowing them to meet evolving challenges as they arise.

The Cisco IP Physical Security solution is built on Cisco network features such as:

- *Multicasting*—allows a data source, such as a camera, to stream one copy of content across a network for simultaneous capture and analysis by multiple destinations.
- *Load balancing*—intelligence in the network that distributes data between multiple shared destinations based on system availability or capacity.
- *Route around failure*—enables data to be re-routed in the event of a network node or connection failure. This capability is particularly important during security events and emergency response activities.
- *Quality of Service (QoS)*—assures that data can be prioritized on the network to prevent the interruption of video surveillance feeds.

## Open Standards

As part of its continuing commitment to the transportation industry, Cisco offers advanced network technology and world-class service and support, strengthened by a market-leading approach to partnership. Cisco works with third-party, open standards-based application and technology partners who build on the value of a secure, cost-effective, and flexible network infrastructure.

For example, one of Cisco's partners is integrating a physical security application suite with the Cisco Alarm Interface Controller (AIC) Network Module. This integration delivers an end-to-end physical security solution that allows the application to correlate alarm events from remote sensors located anywhere on the network. Cisco also works with IP camera/IP codec, video management, biometrics, access control, and other physical security solution vendors in developing optimized infrastructure for integrated security and surveillance.

## Cyber-Security

Attaching security cameras, alarms, and applications to the network offers unparalleled flexibility, but it also unleashes the potential for security breaches into that sensitive data. The Cisco IP Physical Security solution incorporates network security features that manage intrusion detection, encryption, VPNs, access control, port identification, and firewalls. Cisco Physical Security solutions build on the security, scalability, and reliability of the Cisco network infrastructure to extract the full potential of an agency's physical security investment.

## Solution Components

The Cisco physical and network security solutions are based on a comprehensive offering that consists of solutions from Cisco and its partners. The major components of the Cisco IP Physical Security solution are:

- **Network Access**
  - Access platforms (Cisco 800, 1700, 2600, and 3700 Series routers)
  - Cisco Aironet® Wireless Solutions
  - Cisco 3220 Mobile Access Router



- **Security**
  - Encryption acceleration cards:
    - Cisco 1700 Series VPN Module (MOD1700-VPN)
    - Cisco 2600 and 3700 Series VPN Modules (AIM-VPN/BP, AIM-VPN/EPII, AIM-VPN/HPII)
  - Cisco PIX<sup>®</sup> Firewall Software
  - Cisco Structured Wireless Aware Network (SWAN)
- **Alarm Termination**
  - Alarm Interface Controller Network Module for the Cisco 2600, 3600, and Cisco ONS 15454 product lines
- **Performance**
  - End-to-End QoS
  - Multiservice VPN
  - Multicast
  - Hardware-based VPN Encryption
- **Management**
  - CiscoWorks/CiscoSecure
  - SWAN
- **Partner Components**
  - Cameras
  - Access Panels
  - Alarm Sensors
  - Video and Alarm Management Software

## Evolution to Cisco IP Physical Security Solution

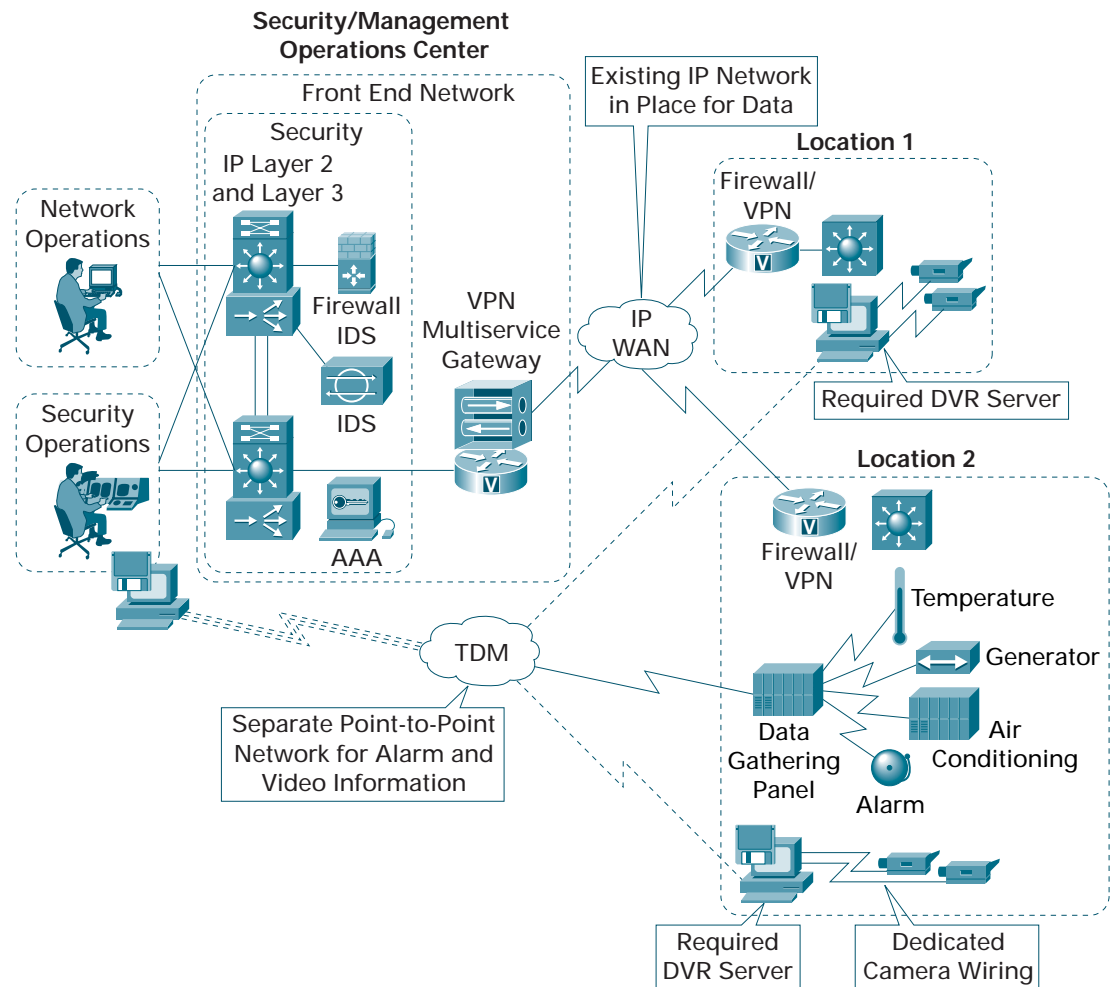
Cisco IP Physical Security solutions offer unprecedented flexibility and cost efficiency by giving transportation agencies the freedom to upgrade any part of their physical security infrastructure without requiring a whole new network buildout. For example, many transit agencies already have security systems that include traditional or digital cameras and digital video recorder (DVR) systems. The Cisco IP Physical Security solution supports simplified migration from dedicated network connections to multipoint IP networks, creating an interoperable environment that integrates existing and new security devices.

## Legacy Devices Often Require Dedicated Networks

In most multisite deployments, each monitored site is connected to the security operations center through a dedicated network. This architecture (depicted in Figure 1 for an operator managing multiple locations) can be costly to operate because of usage-sensitive dial-access lines or the costs of dedicated network connections that run between every remote site and the security center.



Figure 1  
Traditional Physical Security Solution



### Cisco VPN Solution Enables Network Access Through ISP

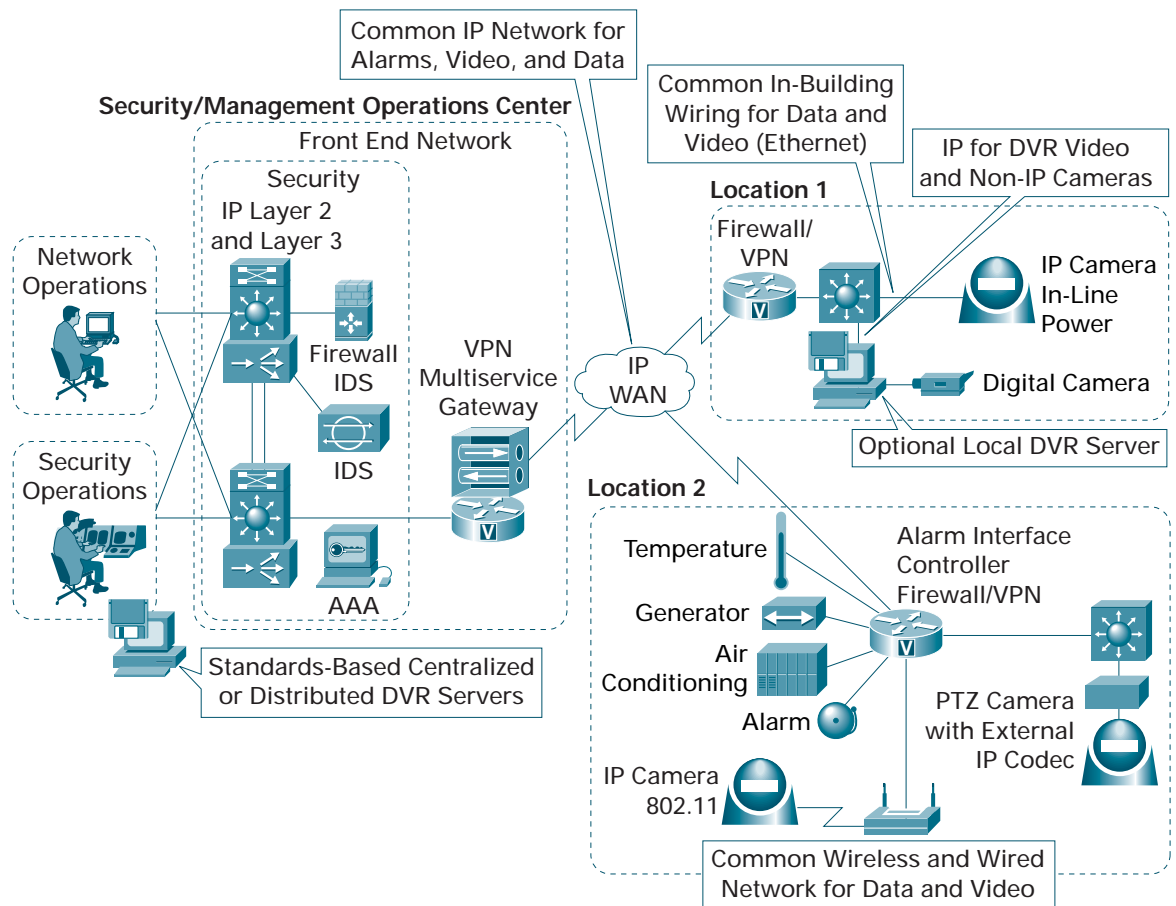
Cisco IP Physical Security solutions eliminate the need for dedicated networks, reducing costs and increasing flexibility. Multiservice VPN network technology from Cisco offers the security and network bandwidth management that video and alarm surveillance requires—without the cost of dedicated network links. Rather than paying for a dedicated network connection between the remote site and a security center location, Cisco IP Physical Security solution customers pay for the network access to their local Internet Service Provider (ISP). This connection is usually very competitive and offers plenty of bandwidth to support voice, video, and data services.

Cisco VPN technology creates a virtual private network that encrypts and protects the security data, even if it traverses public networks on the way from the remote site to the security center. VPN services using Cisco's high-capacity hardware encryption enable high performance and extremely cost-competitive network connectivity alternatives to dedicated ATM, Frame Relay, or usage-sensitive ISDN and Public Switched Telephone Network (PSTN) services.



Even without advanced digital cameras, Cisco VPN technology enables offsite surveillance and analysis of remote locations. Although the industry is migrating toward the advanced video surveillance features of digital cameras, the Cisco IP Physical Security solution works equally well with existing infrastructure products. Transportation operators can reduce recurring network costs of a dedicated video network—usually associated with traditional camera deployments—by connecting existing cameras to DVRs (Figure 2, Location 1). Connecting the DVRs to Cisco VPN technology and an ISP network allows each remote site to offer connections to the on-site DVR from anywhere on the network.

Figure 2  
Cisco IP Physical Security Solution



To gain even more flexibility and efficiency, security managers can add codecs to legacy cameras or install IP video cameras at remote sites (Figure 2, Location 2). This more advanced end-point technology allows cameras to broadcast video to any destination within the organization's wide-area network (WAN). The Cisco IP Physical Security solution supports cameras that send video to local DVRs or remote security operations centers or both at the same time, depending on the network connectivity or security operations policy.



## Cisco IP Physical Security Solution Value

With lives at stake, it's hard to place a finite value on a security system that helps transportation agencies securely transport passengers and cargo, while safeguarding its equipment and premises. However, the table below demonstrates some compelling examples of both the near-term cost reduction and the long-term value that a Cisco IP Physical Security solution can deliver.

Table 1 IP Physical Security Improvements over Conventional DVR

| Category                         | Description  | Improvement <sup>1</sup>                                   |
|----------------------------------|--|--|
| <b>Surveillance Availability</b> | Standard servers enable in-house IT support to facilitate same-day hardware replacement vs. up to 5 days for contractors to repair proprietary servers | 5 percent availability improvement (from 94 to 99 percent) |
| <b>Recording Hardware</b>        | Standard PC Server as opposed to proprietary DVR hardware  | Approx. US\$3K less per server                             |
| <b>Cabling Costs</b>             | Comparison of coax cabling to Cat5 Ethernet  | \$1K less for 16 cameras                                   |
| <b>Large Deployments</b>         | Example 300 camera IP Video Surveillance deployment  | Up to \$3K less than DVR per channel                       |

1. Information from Cisco and Axis Communications data

### Why Cisco?

Cisco offers a highly resilient, responsive, and extensible solution for converging data throughout a comprehensive security environment of traditional and emerging technologies. Based on a sound hardware and software infrastructure that protects the network from outages, service degradation, and security breaches, the Cisco infrastructure is ideal for accommodating critical transportation security devices and applications. On top of this infrastructure, Cisco provides intelligent, application-enabling network services, including IP voice, video, security, Web application acceleration, and connectivity that transportation agencies can use to provide increasingly effective security services. Together, these network components support:

- Secure management of time-sensitive content
- Streamlined communication throughout the network and beyond
- Flexible, cost-effective support for adds, moves, and changes
- Customizable architecture
- Modular network deployment
- Highly optimized applications

Using advanced encryption and tunneling, Cisco network security solutions enable secure, end-to-end, private network connections, intrusion detection systems and wireless protection. Security is built into the hardware which allows embedded protection throughout the entire network to provide greater security than standalone point-product solutions. Effective security solutions provide transportation operators with the safeguards they need to keep unauthorized users out of the network, protect critical data, and keep traffic operation centers running.

With this combination of infrastructure and services, Cisco is the only vendor that can offer market-leading, end-to-end network security solutions that encompass embedded and appliance-based security technology. Implementing the Cisco IP Physical Security solution protects network data and security information while offering cost-effective WAN access alternatives that reduce physical security network costs. For transportation agencies striving to provide a safe environment, increase traveler and carrier satisfaction, and ensure a scalable security infrastructure that is positioned to meet challenging future needs, Cisco is an ideal partner.



**Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**

Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

**Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**

Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Aironet, and PIX are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.  
(0304R) MS/LW5369 11/03