

Seaport of the Future— Optimizing and Securing Cargo Movement Using Network Technology



Executive Summary

Seaport commissioners and directors are facing an increasingly complex range of operational challenges in their management of highly complex, multi-tenant port environments. Significant competitive challenges, ongoing labor issues, and new security requirements mandated by the U.S. government and the International Maritime Organization (IMO) are straining already scarce resources.

The need to safely manage an ever-expanding cargo and passenger load is driving many port officials to evaluate new technologies that drive increased efficiency, improved security, and revenue for port authorities, as well as tenants. In addition to the growing need for more advanced applications and systems, the introduction of U.S. government programs such as the U.S. Customs Service’s Container Security Initiative (CSI), pilot programs such as Operation Safe Commerce, and requirements in Part A of the new IMO-sanctioned International Ship and Port Facility Security (ISPS) Code are placing

unprecedented pressure on port managers to innovate and adapt quickly to the new realities of port security. All these new technologies must be integrated into an existing port information infrastructure that, today, is often highly fragmented across both port authority and tenant operations. Port managers must use investments in security upgrades to enhance overall productivity. This is the future for port operations.

The notion of the “seaport of the future” is rapidly taking hold as authorities increasingly use network-centric innovations to improve:

- Security of cargo, including containers, bulk and break-bulk shipments, as well as passengers
- Decision-making and responsiveness
- Compliance and communication with government organizations and other ports
- Flexibility and resource utilization
- Satisfaction of terminal operators and other tenants

A converged communications infrastructure is an important enabler of integrated security and operational efficiency.

Using a Common Communications Infrastructure

Cisco Systems’ solution for seaports is a secure, unified standards-based communications infrastructure allowing seaports to capitalize



on emerging security, operational, and cost-cutting opportunities. With an underlying operational communication infrastructure, core processes can be consolidated across seaport operations, whether on the dock or in the office.

A multiservice network also can replace multiple proprietary networks with a single architecture for all information—data, voice, or video—and enable seaports to use and scale their network investment when deploying or integrating new applications. Additionally, significant cost savings can be realized because IP networks require fewer and less specialized staff for management and maintenance.

Improved Security and Safety

Networked Video Surveillance

Surveillance initiatives, including the use of digital video to monitor perimeters, access points, and public spaces are among seaports' most pressing priorities. By introducing a common communications infrastructure, seaports can utilize multi-use, network-enabled video in place of aging, single-use analog closed circuit television (CCTV) systems.

Networked video surveillance provides many advantages over traditional CCTV systems including:

- Ease of retrieval, storage, and archiving
- Simultaneous recording and monitoring of multiple video streams
- Event reconstruction and correlation
- Multiple monitoring and control stations for a single camera or video stream
- Secure remote and mobile monitoring
- Improved system scalability
- One camera, multiple purposes
- Transport over a common infrastructure
- Support for video distribution to multiple devices (for example, handheld computers)

Container Security

Ports in the United States handle about six million incoming containers each year, or approximately 17,000 containers each day. However, inspectors open only about two percent of these containers. An important priority for seaports is therefore to ensure the security of containers and to prevent unauthorized parties from tampering with cargo.

Shippers are using novel methods such as seals with embedded radio-frequency identification (RFID) tags to detect container tampering. In the future, RFID may be combined with global positioning systems (GPS) on ships, land transport vehicles, and gantry cranes to ensure container integrity while tracking and documenting container movement and storage.

In addition to ensuring that containers remain intact, shippers, seaports, and customs authorities must inspect containers to ensure they do not hold proscribed goods such as stolen automobiles or weapons. Mobile, noninvasive inspection systems are being employed to allow for the inspection of containers with minimum effect on the flow of commerce. These systems create low-resolution pictures of cargo inside containers, using x-ray and gamma ray technologies. These images can be viewed directly, transmitted to appropriate authorities using wireless networks, or archived for later reference.



Access Control

Although seaports have historically used more conventional forms of access control such as ID badges, the increased focus on seaport security is driving organizations like the U.S. Department of Transportation, the Department of Homeland Security, the U.S. Coast Guard, and port commissioners to promote the use of a national credentialing system for seaport workers, as well as technology-intensive access control systems. The emergence of the Transportation Worker Identification Credential (TWIC) will transform access control throughout U.S. seaports, making comprehensive data capture, cost-effective storage and archiving, and efficient integration and sharing of data crucial operational priorities for ports.

Accordingly, seaports are turning to multiple types of access control devices to enhance authorization of seaport personnel for entry into dock and cargo areas. The development of biometric controls, including facial, retina, iris, fingerprint, and hand geometry scans has opened up opportunities for more far more robust analysis and tracking across the supply chain and in intermodal operations. Utilizing storage networking technology that maintains ready access to data also expedites the verification process at access points, reducing traffic congestion and long lines at port access points.

Seaports are also deploying numerous other sophisticated sensors to secure the complete spectrum of seaport operations and physical assets. New technologies such as intelligent fence systems, chemical and biological detectors, underwater cameras, and infrared perimeter motion detectors are other examples.

Emerging biometric and remote sensing applications can be greatly enhanced by a robust and flexible network infrastructure. The Cisco® common communications infrastructure for seaports helps enable the integration of standards-based security systems through improved communications and information correlation.

Operational Efficiency

Seaports have a driving mission to move cargo quickly and safely through the port. To accomplish this mission, a reliable, flexible, and secure flow of information is vital.

Wireless Mobility

In the quest to improve vessel turnaround times, seaports are relying more and more on wireless technologies to enhance the flexibility of operations and improve efficiency. In a world where most workers still record container numbers on clipboards, wireless solutions can drive significant cost savings. For example:

- Use of wireless handheld computers for dock workers drives cargo processing efficiency
- GPS and wireless-enabled heavy equipment such as cranes, forklifts, and trucks
- Use of a wireless LAN (WLAN) for data transmission throughout the seaport
- Voice communications over non licensed (free) spectrum eliminates costly and non-secure radio networks

All the data these systems consume and generate can be transmitted using a Cisco WLAN, based on ruggedized hot spots (points of access to the Internet and port networks) located throughout the seaport. Hundreds of seaports worldwide are already using wireless technology to optimize efficiency.

Increasing Tenant Satisfaction

Port authorities are eager to meet the needs of their tenants, particularly operators of critical terminals, to drive revenue and protect already compressed margins. If seaport tenants cannot safely and efficiently operate their businesses, including moving cargo on and off ships, repairing vessels, and ensuring that ships are adequately supplied, it is the seaport that will ultimately suffer through lost business as shippers move to other ports and volume declines.

Value-Added Services to Tenants

Cisco can help seaports provide ways to generate new revenue and to provide added customer service to seaport tenants. The same network the seaport uses for its operations and security can be used to provision network services such as Internet access or IP telephony for the seaport's tenants. This provides a cost savings and convenience for tenants, allowing them to improve their own operational efficiency.

The Cisco common communications infrastructure enables port authorities to use the same network resources to transmit data, voice, and video for operations and security. This network may also provide value-added services such as Internet access, IP telephony (the ability to transmit voice calls using the Internet) and yard management system information to seaport tenants. Providing fast

and secure network connectivity and IP telephony offers port authorities an opportunity to increase top-line revenue while driving down communication costs for tenants.

Getting There

Together with Cisco partners, including leading application providers and system integrators serving the seaport industry, the Cisco Seaport solution links functional areas through a common communications infrastructure that seaports can cost-effectively deploy today, while establishing a sound, efficient foundation for continuous improvements.

Cisco solutions help seaport operations and communications processes gain from increased speed, greater efficiency, reduced cost, minimized space requirements and simplified network management, helping enable the seaport of the future, now.



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

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, and the Cisco Systems logo 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.
(0303R) KJ/LW4322 0303