



Architecting for Security and Efficiency in the Airport

“We must continue to set the highest standard for safe, efficient air travel through the industry’s inevitable recovery and change.”

FAA Administrator Marion C. Blakey

Background

One of Cisco’s largest North American airport customers must support 28 million passengers, 50 passenger airlines, 67 freight carriers, and more than 100 freight forwarders and customs brokers at its international facility. Safety, efficiency, and profitability are the prime objectives, and safe and efficient administration requires more than 17,000 onsite employees that deliver a wide variety of services to passengers, airlines, aviation support, and the federal government.

Challenge

The customer operated 82 networks in the airport. These included airport back-office systems, security/video surveillance, and networks to support the airlines, retailers, and other tenants. These networks supported data, voice, and video, and were both wired and wireless. The variety of networks and systems resulted in an environment where integration, maintenance, and upgrades were very expensive and difficult to maintain.

Solution

Airport executives wanted to reduce the cost to maintain and expand the networks while supporting all the various information-technology (IT) requirements of multiple customers. They envisioned one network that consolidated voice, video, and data services, and supported both wired and wireless environments. They chose to implement a Cisco® IP/MPLS network that offers state-of-the-art, integrated, intelligent services and uncompromised performance. The Cisco network enabled them to safely and efficiently offer necessary services to all of their airport tenants, and to increase their revenue and profit.

Results

The Cisco network is resilient and secure. It gives the airport the manageability, flexibility, scalability, and feature richness it needs, and it has turned the network into a profit center and a source of customer satisfaction from tenants. The airport takes advantage of a common cabling infrastructure, common service-creation infrastructure, and shares services among all its tenants. With the Multiprotocol Label Switching (MPLS) core network, the airport now offers VPN services to all its tenants and provides a secure network for accessing data, voice, video, or wireless applications.



Introduction

Even the most frequent fliers have a limited perception of what it takes to run an international airport. The amount of data required to support daily operations is staggering, and when airport executives are planning for growth, they have to be able to see far into the future.

Airport management teams have to focus on implementing new security measures, improving operational flexibility, and generating new revenue. Administrators must have access to information that allows them to react strategically to changes that happen constantly around them. Some challenges they face in their difficult operating environment include:

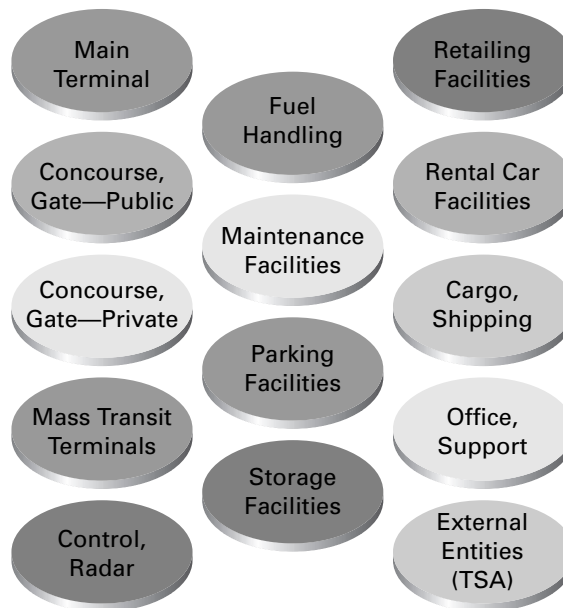
- *Physical*—A multitenant environment with congested passenger, baggage, and cargo flow
- *Regulatory*—Difficulty in integrating new safety and security measures
- *Economic*—Airline financial difficulties, a limited ability to grow capacity, and inflexible resource-allocation capabilities

Complicated Issues in a Complex Environment

Most airports have numerous networks running throughout the facility, and many of these networks are built on traditional technologies that cannot deliver real-time information or support real-time communications. The airport highlighted in this case study was supporting 82 networks, including its own back-office systems as well as networks for its tenants: airlines, aviation support, cargo shippers, concessions, food services, fuel, immigration services, customs, retailers, cargo lines, and security (Figure 1).

Figure 1

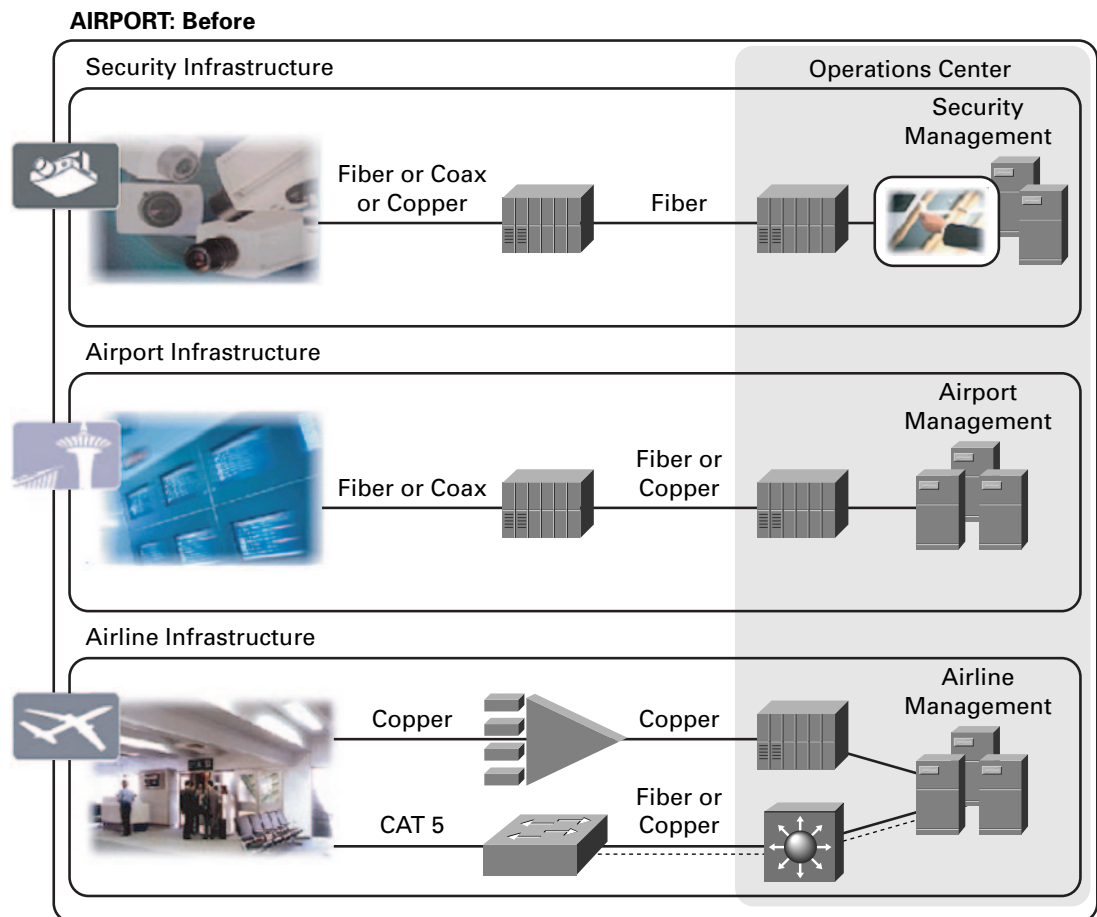
A Variety of Tenants and Systems





The airport had to manage an environment where integrating, maintaining, and upgrading networks and applications was very difficult and expensive, a situation which was made more challenging by a lack of control of its tenants' application environments and increasing technology expenses. Figure 2 shows the airport's dispersed network. The disparate systems made it almost impossible to add services and scale for airport management.

Figure 2
Separate Networks for Security, Airport Administration, and Airlines



Solution: A Converged Network That Scales for the Future

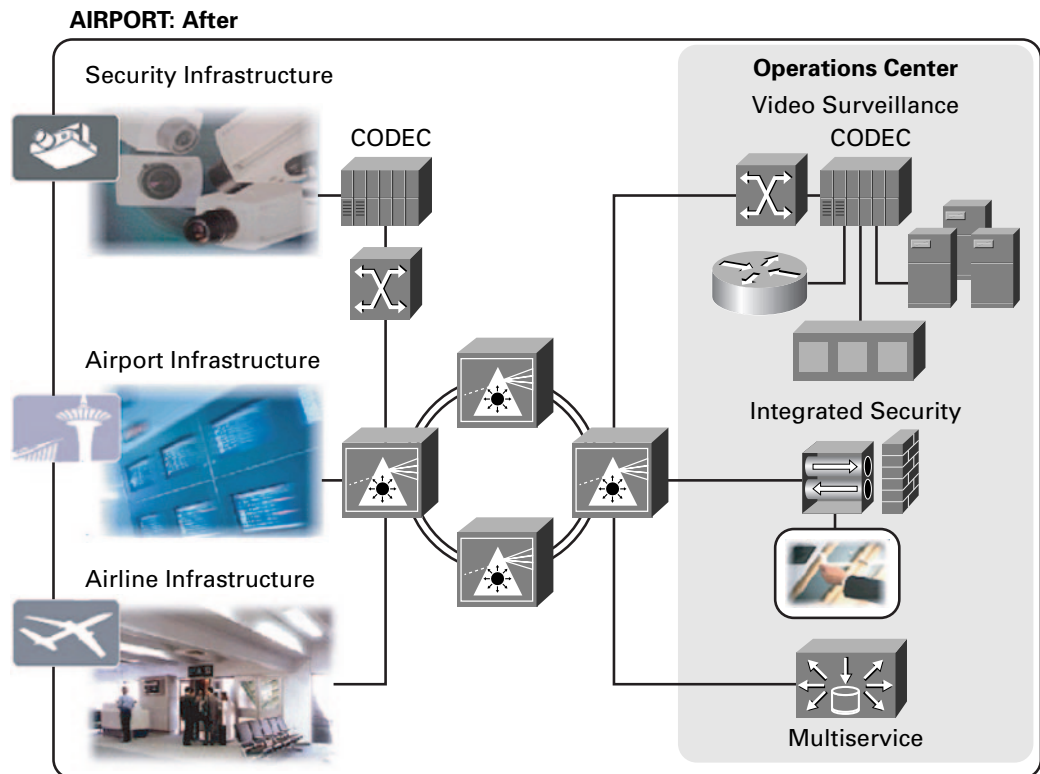
Airport executives needed a network that not only consolidated voice, video, and data services into one network, but also provided high security and intelligent services to all tenants. In researching their alternatives, they found they could replace their existing internal ATM infrastructure with a Cisco IP/MPLS network that could support their ATM services and also meet their requirements for security, intelligence, scalability, performance, ease of management, and cost savings. The management calculated that in two years this new network would pay for itself.

The airport converged its 82 separate networks onto a single, highly resilient, high-performance network that carries data, voice, and video. Built on a dense wavelength-division multiplexing (DWDM) optical core, the network's Multiprotocol Label Switching (MPLS) and Synchronous Optical Network (SONET) services have vastly improved



network redundancy, and the airport has sold more revenue-generating services to airport tenants. The airport has made a strategic investment in an intelligent network with features that make it easy to bring all the tenants and their applications together, while giving them the flexibility to incorporate future applications for voice, wireless, and enhanced security technologies (Figure 3).

Figure 3
The Converged Airport Infrastructure



The Choice of an Optical Solution—Scalability and Density at a Low Cost per Wavelength

The airport's campus-area network is built on eight Cisco ONS 15454 Metro DWDM systems, with four Cisco ONS 15454 systems comprising each DWDM optical ring. This optical backbone provides scalable, high-density services at a low cost per wavelength. Network administrators can scale in single wavelength increments and aggregate wavelengths over the campus-area network's regional-metro ring network architecture.

Dependability, Rich Features, and Scale—Cisco 7000 Routers

Anchored by Cisco 7600 Series routers, the airport's new network provides high reliability and scalability plus rich MPLS-based services. Two Cisco 7600 Series MPLS core routers are housed in separate, physically isolated sites. These routers attach to the Cisco ONS 15454 systems, creating a full-mesh infrastructure. The airport has four main locations, and two Cisco 7609 distribution routers are installed in each location. These routers form the distribution layer to deliver MPLS services, with each connection consuming only a single wavelength on the optical core. Because

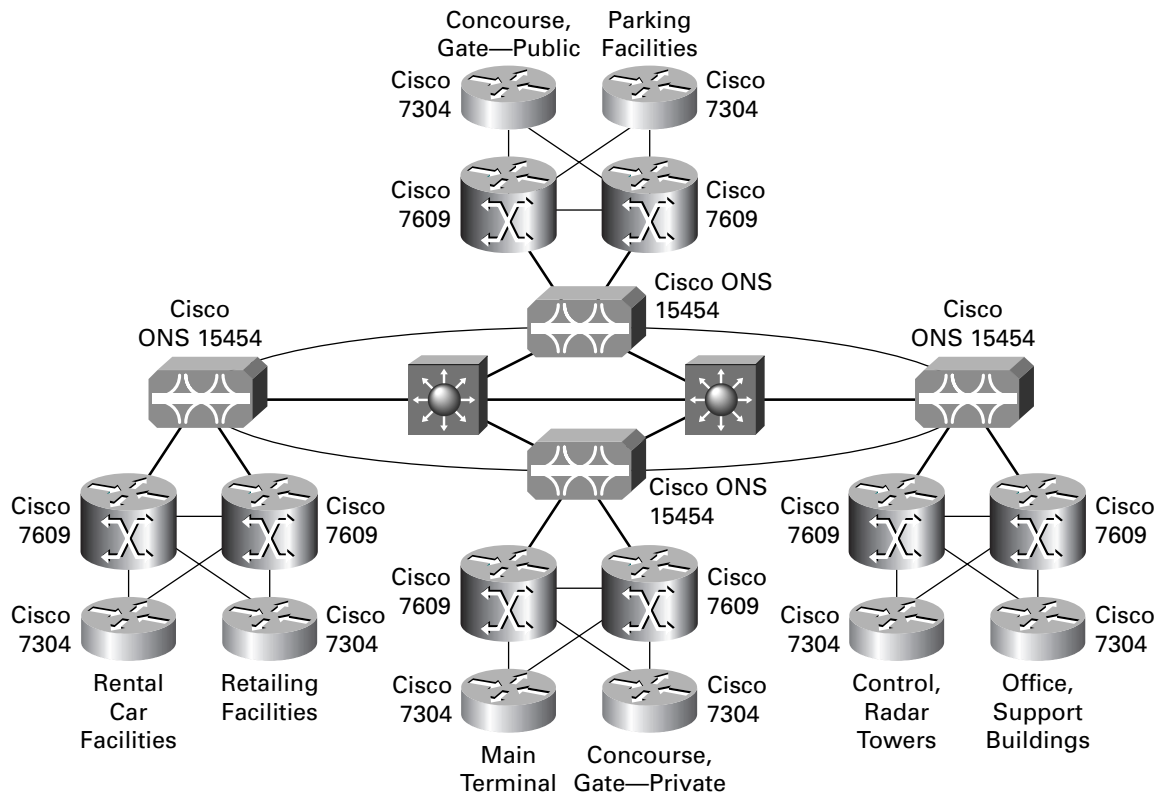


each core router is fully redundant in supervisor modules, fabric modules, and power supplies, their use helps to ensure high availability. The airport's core routers also contain 4-port optical services modules (OSMs) and three open slots for future expansion.

To help ensure absolute reliability, redundant paths and cables connect the core routers to each other and to the eight Cisco 7609 distribution routers. Each Cisco 7609 distribution router is dual-homed to the core routers and to Cisco 7304 routers at the network edge (Figure 4). The Cisco 7304 edge routers are also built for high availability, with fully redundant router processors and power supplies. The Cisco 7304 scales from DS0 to OC-48 interfaces, and by using the Cisco 7304 router, not only was the customer able to use some of its existing interfaces but it could also scale the edge with higher-performance interfaces on the Cisco 7304 router.

Figure 4

Cisco 7000 Routers Anchor the Airport's Network



The network managers were already familiar and comfortable with the quality and reliability of the Cisco Catalyst® 6500 Series Switch—the product on which the Cisco 7600 Series router is based—so they preferred the Cisco 7000 routers. They chose Cisco 7600 and 7300 series routers for the products' high-redundancy features—from power supply to supervisor engine, which allows the airport to minimize network downtime and achieve the resiliency required for nonstop operations and tenant services. In addition, the Cisco 7600 and 7300 series provide performance and scalability, and a broad range of network services to meet the management vision of an MPLS-based network.



Cisco was able to offer an Ethernet-based solution, to specify a familiar chassis, and to add optical services modules for Layer 3 MPLS. The Cisco 7600 and 7300 series routers were selected as the key components of the network because the routers deliver the scalability, flexibility, and redundancy that met the airport's current and long-term network requirements.

Service Flexibility and Manageability

The redundant MPLS infrastructure provides the airport with aggregation for Ethernet over MPLS traffic and MPLS VPNs for high-bandwidth, data, voice, and video services. Today the airport is managing its optical network using the Cisco Transport Manager. It is possible to more rapidly roll out and maintain revenue-generating services using Cisco Transport Manager's network provisioning, surveillance, and performance-monitoring features.

To manage MPLS services, the airport uses the Cisco VPN Solution Center, which simplifies management by automating service and network provisioning. The software product includes features that improve ease of use, frees network administrators for other tasks, and enables the airport's IP VPN services to scale easily and reduce costs.

CiscoWorks LAN Management Solution (LMS) is used for managing the network edge devices. Built upon popular Internet-based standards, CiscoWorks LMS enables the airport's network operator to more efficiently and effectively manage the network through a simplified browser-based interface that can be accessed anytime from anywhere within the network.

Why Cisco?

The airport IT team chose Cisco Systems® for innovative technology solutions, high-quality products, dependable service, low total cost of ownership, and helpful programs that other network infrastructure companies cannot offer. Cisco was able to assist them in designing an integrated, converged network that lowered their costs for existing services yet provided greater overall bandwidth capacity and flexibility for new and evolving applications and services.

With only five IT staff to support the entire airport "city," the airport chose the Cisco solution because it is easy to manage and requires low maintenance. The new Cisco network lets staff implement any policies or services they want to add—and extend services such as e-mail, voice, videoconferencing, and wireless access to the traveling public. Airport tenants benefit, too. By sharing an adaptable and reliable intelligent network, every tenant at the airport can cost-effectively improve productivity.

A complete solution required more than just the network hardware, however. As a service provider to a variety of tenants, the airport wanted to enhance its credibility and offer safe, reliable, and secure services to its customers. Airport leaders chose to associate their services with the worldwide leader in networking for the Internet, and became a member of the Cisco Powered Network program to take advantage of expanded marketing resources that only Cisco offers. The Cisco team worked closely with airport executives to define a service model, define service-level agreements (SLAs), establish pricing, and identify the network's utility capabilities. They also helped the airport sell its solutions to prospective internal and external customers.

Relationships between airport executives and the IT team have never been stronger, and the new network is already doing its part to enhance the airport's profitability. As new technologies are developed, the airport can rely on the Cisco team to help ensure their investment is protected while scaling and optimizing their network to take advantage of new applications and services.



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. Catalyst, 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.
(0304R) BU/LW5024 08/03