Airport Security: IP-Based Solutions for Increased Situational Awareness and Operational Effectiveness

Solution Overview

What You Will Learn

This solution overview is intended for airport security teams, airport IT departments, and security consultants. The overview briefly describes an IP-based network foundation and airport security solutions from Cisco and its partners.

- Network Foundation
- Video Surveillance
- Physical Access Controls
- Control Rooms
- Communications
- Passenger Information
- Partner Solutions
Network Foundation

A common IP network foundation potentially supports all airport services, including asset tracking, CCTV, communications, access control, and passenger information (Figure 1). The Cisco® mission-critical network architecture consists of a media-ready network for airport video traffic, Cisco Multiprotocol Label Switching (MPLS), and Cisco SecureX Architecture. The Cisco Unified Wireless Network extends the network throughout the airport property.

Figure 1. The Network as the Foundation for Airport Applications
Mission-Critical Network Architecture

The mission-critical network is built from standard Cisco network components such as Cisco Catalyst® switches, Cisco Integrated Services Routers, and Cisco Adaptive Security Appliances. Use of standard components makes the network resilient and cost-effective. A single network platform supports mission-critical operational traffic as well as everyday administrative traffic.

Cisco developed the architecture to minimize failure recovery times and deliver 99.99975 percent or better reliability. The core network is split into two planes, for critical data and standard operational data (Figure 2). The plane for standard operational data can be used as backup for critical data. Provider-edge nodes (PE nodes in Figure 2) classify incoming traffic as critical or non-critical and route it to the appropriate plane. To meet service-level agreements (SLAs) for critical traffic, the nodes use the weighted random early detection (WRED) algorithm, drop thresholds, and high-priority queue allocation. All provider-edge nodes are configured as redundant pairs, for high availability. Quality of service (QoS) is present on both planes so that critical traffic routed to the standard operational plane can receive priority treatment.

Airport servers and devices have either a single or redundant connection to the mission-critical network. Servers and devices that attach to the critical plane always have two independent connections. Those that attach to the standard plane can have either one or two connections, depending on the airport’s financial considerations. The IT department can define appropriate SLAs for each individual service, including bandwidth, jitter, latency, drop threshold, and criticality measure.

To protect sensitive data traveling over the airport network, the infrastructure supports wired network encryption as well as Session Border Control mechanisms at the customer edge, provider edge, or peering points. For more about network security, see the section Cisco SecureX Architecture.
Multiprotocol Label Switching

MPLS enables the airport to securely isolate different types of services that share the same network foundation. These services can include security services such as IP CCTV, IP telephony, Internet access, IPTV, and digital signage, as well as information access for tenants. The ability to quickly set up a separate information flow for each service enables the airport to adapt to organizational changes and comply with stringent SLAs for availability.
Cisco SecureX Architecture

Cisco SecureX architecture enforces security policies across the Airport’s entire distributed network, not just at a single point in the data stream. This way, it responds to the evolving security needs of the airport’s network environment.

Cisco SecureX uses context-aware security to identify critical information needed to make dynamic and intelligent network access, control, and threat protection decisions that traditional security solutions simply can’t provide. It identifies:

- Who is attempting to access the network
- What role that person plays in the organization
- What resources that person is trying to access
- Where that person is located at the time of the access attempt
- What device is being used to gain access
- How that person is accessing the network

Cisco SecureX is designed to align closely with the airport’s business policies. This simplifies policy administration, provides broader visibility into events, strengthens security controls, and optimizes business efficiency and flexibility. More specifically, Cisco SecureX:

- Establishes and enforces context-aware policy across the airport’s entire distributed network
- Creates a converged security strategy across wired, wireless, and VPN networks
- Gives the airport the ability to create policies that correlate directly with IT enforcement needs and business rules
- Uses the Cisco Security Intelligence Operation (SIO) for real-time insight into the global threat environment
A Proactive Approach to Threats
Cisco’s security products stay ahead of the latest threats using real-time threat intelligence from Cisco SIO. Cisco SIO is the world’s largest cloud-based security ecosystem, using almost a million live data feeds from deployed Cisco email, web, firewall, and intrusion prevention system (IPS) solutions. Cisco SIO weighs and processes the data, automatically categorizing threats and creating rules using more than 200 parameters. Security researchers also collect and supply information about security events that have the potential for widespread impact on networks, applications, and devices. Rules are dynamically delivered to deploy Cisco security devices every three to five minutes. The Cisco SIO team also publishes security best practice recommendations and tactical guidance for thwarting threats.

Cisco Unified Wireless Network
The Cisco Unified Wireless Network delivers information to security personnel using 802.11 wireless devices anywhere in the wireless coverage area.

Personnel can perform their jobs more efficiently when they can use smartphones and in-vehicle laptops to receive alarms, CCTV images, man-down information, and maps and diagrams. The wireless network also provides the foundation for a variety of location-based services, including asset tracking and context-aware information delivery (Figure 4).
The Cisco Unified Wireless Network provides critical services, including:

- Enterprise-class security with a built-in intrusion prevention system (IPS) and intrusion detection system (IDS)
- Real-time radio frequency (RF) monitoring and management that is self-configuring, self-optimizing, and self-healing
- Integrated mobility services for security, voice services, guest access, and location services
- The same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that airports expect from their wired LANs

**Figure 4. Cisco Unified Wireless Network Architecture at the Airport**
Location-Based Services for Assets and Personnel
Location-based services enable airports to pinpoint the location of 802.11 devices (such as laptops, smartphones, and PDAs), other assets, and people. The airport simply attaches 802.11-based active RFID tags to equipment or incorporates them in security badges. Location-based services enable the security department to monitor and manage moveable assets and help to create a safer working environment for staff.

Read More
• Cisco 3300 Series Mobility Services Engine
• AeroScout Unified Asset Mobility

Cisco 3300 Series Mobility Services Engine
The Cisco 3300 Series Mobility Services Engine transforms the airport’s existing wireless LAN into a mobility network that can collect contextual information about people, things, and assets. Cisco partners can use the open API to add new capabilities.

Partner Solution for Asset Tracking and Management: AeroScout Unified Asset Visibility
The AeroScout Unified Asset Visibility solution allows airports to track the location, condition, and status of mobile assets and people over the Cisco Unified Wireless Network. Active RFID tags are affixed to moveable assets or embedded in employee or visitor badges.
Video Surveillance

An IP video surveillance solution enables authorized personnel to view real-time and archived video from any analog or digital camera in the airport, from any monitor, including on PCs and mobile devices. IP-based video surveillance uses the airport’s wired and wireless IP network as the foundation, eliminating the costs associated with building and managing a separate network. Solution components include:

- Software to manage, replicate, distribute, and archive video streams
- Software to authenticate and manage access to video feeds
- Software to allow operators to select any video feed from the airport to view, provided they have authorization
- Video storage system, which automatically enforces retention policies
- Cameras

Read More
- Cisco Media-Ready Network Architecture
- Cisco IP Video Surveillance Solution
- Partner solution for CCTV control rooms: Tyco Mosaic

Cisco Media-Ready Network Architecture

Simply adding bandwidth is not enough to support IP video surveillance or other airport video applications, such as digital signage and video collaboration. The network also needs quality of service (QoS), high availability, and low latency. The Cisco Media-Ready Architecture provides a comprehensive set of video services that are shared by all airport video applications. Using the network as the platform for all video services costs far less than deploying them separately for each video application. Services in the Cisco Media-Ready Network Architecture include:

- **Access services**: Access control and identity of video clients, as well as mobility and location services
- **Video transport services**: Packet delivery, using QoS and delivery optimization techniques to help ensure high service levels
- **Bridging services**: Transcoding, conferencing, and recording
- **Storage services**: Content capture, storage, retrieval, distribution, and management
- **Session control services**: Signaling and control to set up and tear down sessions
Integration
Airports can augment the capabilities of the Cisco IP Video Surveillance solution by using its open standards-based interface to integrate with:

- External alarms and access control systems
- Advanced video analytics from multiple vendors
- Control room console systems, such as Tyco Mosaic

Cisco IP Video Surveillance Solution
Using Cisco Video Surveillance solutions, airports can migrate smoothly from their existing analog systems to an IP-based system. The security department can continue to use existing analog equipment while gradually adding new IP cameras, which extends the life of existing investments. Components of an IP CCTV solution include the video-ready network as well as the following components, also shown in Figure 5:

- **Cisco Video Surveillance IP Gateways**: High-performance IP gateway encoders work with analog cameras from various vendors to facilitate video transport and access over an IP network. IP gateway decoders allow operators to continue using familiar analog keyboards and displays while gaining new capabilities, such as simplified search and playback.

- **Cisco Video Surveillance Integrated Services Platform**: This fault-tolerant, scalable video recording and storage solution works with existing analog matrix switches. The platform can accept video either through built-in digitization and compression technologies or Ethernet and USB connections.

- **Cisco Video Surveillance Manager Software**: Operators use an intuitive interface to view live and recorded event-tagged video, and to configure, manage, and operate the video surveillance system.

- **Cisco Video Surveillance Media Server**: Media Server is a highly scalable and reliable video management platform that manages, replicates, distributes, and archives video streams.

- **Cisco Video Surveillance Manager**: A web-based user interface authenticates and manages access to video feeds. It is a centralized administration tool for the management of Media Server hosts, Virtual Matrix hosts, cameras, encoders, and viewers. Deployed today in airports throughout the world, Cisco Video Surveillance Manager (VSM) delivers relevant live and archived video to decision-makers in airport security and command centers, mobile security personnel, and law enforcement agencies. Using industry communication standards, Cisco VSM integrates with the airport’s access control and video analytics to present security personnel with video associated with intelligent alarms and aberrant behavior. Personnel can access live or recorded airport video anywhere, at any time. Video can be shared within the airport security department and other departments. The main benefits are faster event investigation, response, and resolution.
• **Cisco Video Surveillance Virtual Matrix**: Virtual Matrix monitors video feeds in command center and other 24-hour monitoring environments. It allows operators to control the video being displayed on multiple local and remote digital monitors.

• **Cisco IP Video Surveillance Cameras**: These high-resolution cameras have an enhanced, progressive scan imager for excellent video and color, even in the most demanding lighting conditions. They use MPEG-4 compression to produce DVD-quality video. Features include automatic day/night mode, dual streams, bidirectional audio, motion detection, alarm inputs and outputs, and an analog BNC connector for ease of installation.

Figure 5. Cisco IP CCTV Network Architecture for Airports
Partner Solution for CCTV Control Room Console: Tyco Mosaic

Tyco Mosaic is an IP control system for the airport’s security and surveillance applications, including CCTV. It provides a single management console that airport security personnel can use to control live video from a mix of analog or IP cameras, and search and retrieve recorded video. Operators can view video feeds from any camera on any monitor by dragging the camera onto a map.
Physical Access Controls

Airports need landside physical access control throughout the airport—in terminals, the bonded warehouse in the cargo center, Air Traffic Control tower, Hangars and airport administration buildings. Controlled access is also required in remote buildings such as generator huts, Meteorology equipment and NAVAID sites.

By connecting physical access hardware to the IP network, airports can take advantage of the inherent advantages of IP for reliability, scalability, and integration. Existing card readers and gate locks can co-exist with new IP-based hardware and control systems and biometric readers. The airport security department can centrally control new and existing hardware in multiple sites, and centrally record access attempts to create an audit trail.

Read More
- Cisco Physical Access Control
- Partner Solution for Access Control: CEM Systems AC2000 Airport Edition

Cisco Physical Access Control

The Cisco Physical Access Control solution enables airport security personnel to manage up to several thousand doors from the same interface, in any location with a web browser. The physical access solution is highly scalable. It easily integrates with Cisco Video Surveillance Solutions and can use IP network services (Figure 6). Solution components include:

- **Cisco Physical Access Gateway**: This intelligent, distributed processing networking edge device connects door hardware, such as locks and readers, to the network. Accessory modules are available to handle additional doors and input/outputs.

- **Cisco Physical Access Manager**: This management software is used to configure hardware, monitor activity, enroll users, and integrate with IT applications and data stores.

CEM Systems is a brand of Tyco International, a leading provider of physical security products and services. Designed specifically for airports, CEM AC2000 Airport Edition (AE) provides advanced access control and a highly reliable security management solution. It supports advanced CEM card readers with on-board databases and airport-specific door modes. The system supports thousands of readers and tens of thousands of cardholders. Airports can start with the number of readers they need today, and expand as required.
Control Room

Using IP-based control room systems, airports can consolidate separate control rooms and consoles. Rather than having to walk to a different console to monitor each system, operators can access the appropriate resources from anywhere in the control room or other location in the airport. They log in at any terminal, and then the console system applies role-based access control to provide appropriate access to information, images, and resources. Within the control room, console systems provide the tools that operators need to perform their roles, from simple alarm or CCTV monitoring to management of critical emergency situations. IP-based console systems simplify the implementation of distributed control rooms or contingency/fall-back centers.
Communications

Reliable communications are vital to ensure efficient operations and optimal coordination of resources around the airport, inside buildings, and in the air. Airports can achieve these goals using IP solutions for communications interoperability and for collaboration.

Communications interoperability refers to the ability to communicate directly with personnel using any device, including fixed resources such as telephones and intercoms as well as mobile devices such as:

- Private mobile radio (PMR)
- Global system mobile (GSM) terminals and handsets
- Advanced digital radio systems, such as terrestrial trunked radio (TETRA) and Project 25 (P25)
- Cisco Unified IP Phones
- Mobile phones

Cisco IP Interoperability and Collaboration System (IPICS) connects all of these communications systems over the IP network. Any operator in the airport can communicate with personnel using any device, increasing situational awareness and making it simpler to provide instructions and information.

With Cisco IPICS, ground staff can also use wired or wireless Cisco Unified IP Phones to monitor airline frequencies, and to transmit and receive on their own company channels. In airports with Cisco Unified Wireless Networks, control room personnel can see the location of wireless IP phones as their owners move about the airport.

The ability to collaborate with voice, video, and web sharing is another valuable communications capability for airport operations, useful for training, disruption planning, and routine operational meetings. Cisco WebEx® enables personnel to collaborate or participate in training from anywhere in the airport, increasing productivity by eliminating time spent walking or even driving to remote meeting rooms.

Airports can also use Cisco Unified IP Phones for simple applications, such as displaying flight departure and arrival times.

Read More
- Cisco IP Interoperability and Collaboration System (IPICS)
- Cisco WebEx
- Partner Solution for Control Rooms: Tyco Mosaic
Cisco IP Interoperability and Collaboration System
Cisco IPICS provides a platform to interconnect the airport’s different communications resources and notify staff of events. Sending radio traffic over an IP network is a cost-effective solution for airport security personnel and first responders to join talk groups when they are using incompatible radios, as well as standard telephones, IP phones, mobile phones, and PCs or laptops with the appropriate software.

Cisco WebEx
Cisco WebEx enables voice, video, and voice collaboration for staff training and emergency planning, eliminating the time and inconvenience spent gathering staff in one location. It combines real-time desktop sharing with phone conferencing so that all participants see the same screen. Cisco WebEx is hosted in the Cisco Collaboration Cloud.

Partner Solution for Control Rooms: Tyco Mosaic
Tyco Mosaic is an IP control system for the airport’s security and surveillance applications, including CCTV, access control, fire and intruder alarms, and communications. It provides a single management console that airport security personnel can use to control live video from a mix of analog or IP cameras, search and retrieve recorded video, manage alarms and events from multiple sources, and manage other connected systems such as access control, fire and intruder alarms, public address, and intercoms. Operators can view video feeds from any camera on any monitor by dragging the camera onto a map.

Partner Solution: Telent MICA
Telent Management Integration and Control of Assets (MICA) is a network-centric building management control system. Control room personnel use standard interfaces to manage new assets, existing systems, and other building applications. These can include CCTV, public address systems, visitor information displays, and help points. The solution can also perform supervisory control and data acquisition (SCADA) for airport systems such as elevators and escalators. Telent has deployed MICA to control the 74 London Underground stations that are being upgraded for Tube Lines.

Partner Solution: Zetron Acom
Zetron Acom Advanced Communications System is a fully digital switching and multiplexing communications system designed for mission-critical communications. It integrates voice (radio and telephone), data, paging, and video.
Passenger Communications and Information

For more noticeable passenger communications, airports are supplementing their public address systems with digital signage. Network-connected digital signs in strategic areas provide passengers with information about a situation or provide evacuation or other instructions. If the airport owns and manages the digital media infrastructure used for advertising, or has made arrangements with the airport’s advertising contractor, the security department can override pre-programmed advertising or passenger information. The security-related information can either take over the screen entirely or, if less urgent, can scroll across the screen while advertising content continues to play.

Read More
• Cisco Digital Media System
• Partner Solution for Public Address: Singlewire InformaCast

Cisco Digital Media System
The Cisco Digital Media System provides a common platform that all airport departments can share, reducing costs. Network-connected signs are centrally controlled and can display:

• Flight information display system (FIDS)
• Passenger Information
• Business TV
• Advertising
• Security warnings or advice, which can pre-empt other content or scroll across the bottom of the screen while other content continues to play

The Cisco Digital Media Suite provides everything the airport security department needs to create and schedule content:

• Create content, such as security training videos, with Cisco Digital Media Encoders (DMEs): The encoders capture and digitize media from a variety of inputs into a variety of digital formats for live and on-demand delivery across the IP network.
Manage content with the Cisco Digital Media Manager (DMM): This web-based application allows security personnel to manage video assets, create playlists, and schedule instant and future content playback.

Publish content to Cisco Digital Media Players (DMPs): These are highly reliable IP-based hardware endpoints connected to Cisco Digital Signs.

Partner Solution for Public Address: Singlewire InformaCast
Singlewire (formerly Berbee) InformaCast IP Broadcasting Solution sends an audio stream and text messages to any combination of IP phones, supported IP speakers, and PCs. Airport security personnel just click a button to send a live, recorded, or scheduled broadcast to one or more paging groups.

For More Information
For more information, visit [http://www.cisco.com/web/strategy/transportation/index.html](http://www.cisco.com/web/strategy/transportation/index.html)
Partner Solutions

**Category:** Control Rooms

**Partner:** Tyco

**Product:** Mosaic

**Description:** Tyco Mosaic is an IP control system for the airport’s security and surveillance applications, including CCTV, access control, fire and intruder alarms, and communications (Figures 7 and 8). It provides a single management console that airport security personnel can use to control live video from a mix of analog or IP cameras, search and retrieve recorded video, manage alarms and events from multiple sources, and manage other connected systems such as access control, fire and intruder alarms, public address, and intercoms.

Operators can view video feeds from any camera on any monitor by dragging the camera onto a map. Tyco Mosaic automatically presents video associated with alarm events. Sophisticated real-time video analysis and post processing can include motion detection, automatic license-plate identification, and incident detection for airport CCTV applications.

The deployment can include multiple levels of redundancy plus consolidated management and storage of video, audio and data. Mosaic can scale to handle thousands of cameras and thousands of operators across multiple sites.

**Figure 7. Tyco Mosaic Connectivity**
Figure 8. Tyco Mosaic Operator View
The Zetron Acom Advanced Communications System is a digital switching and multiplexing communications system designed for mission-critical communications (Figures 9 and 10). It provides connectivity for voice (radio and telephone), data, paging, and video. Acom supports the wide variety of radio technologies and communications used in airports, including:

- Project 25 (P25)
- OpenSky
- iDEN
- Terrestrial Trunked Radio (TETRA)
- EDACS
- Cisco SMARTnet® Service
- SmartZone
- MPT 1327

Operators can use the Acom system to control radios, permitting channel change, talk group selection, and advanced radio features such as “Stun” and “Silent Listen.” Operators can choose a console view, including airport map, blueprint, and more.

Acom also includes a feature-rich telephony communications package that can integrate with standard analog subscriber and exchange ports, as well as Cisco Unified Communications Manager through ETSI ISDN and E1 QSig.
Figure 9. Zetron Acom Network Connectivity

Figure 10. Sample Acom Operator Views
Category: Control Rooms
Partner: Telent
Product: MICA

Telent’s MICA solution offers comprehensive control and monitoring of various security assets through a touch-screen operator interface (Figures 11 and 12). MICA is capable of integrating:

- CCTV
- Public Address
- Visual information displays
- Help Points
- Clocks
- SCADA
- SNMP monitoring of station LAN equipment
- Interface to remote control centres
- Interface to remote maintenance centre
- Specialist systems, including baggage handling, walkways, access control systems, building management systems
- Others

Figure 11. Telent MICA Network Connectivity
Telent MICA provides advanced control and monitoring features needed in airport operations centers. For example, a single log-on gives operators a secure management interface for all equipment, both new and existing. And redundancy and load sharing meet high availability requirements.
Category: Access Control
Partner: CEM Systems
Product: AC2000 Airport Edition

CEM Systems is a brand of Tyco International, a leading provider of physical security products and services. Designed specifically for airports, CEM AC2000 Airport Edition (AE) provides advanced access control and a highly reliable security management solution (Figure 13). It supports advanced CEM card readers with on-board databases and airport-specific door modes. The system supports thousands of readers and tens of thousands of cardholders. Airports can start with the number of readers they need today, and expand as required.

CEM AC2000 also produces the different types of badges used in airports, including temporary and contractor barcode passes, vehicle passes, and ACTA construction passports. CEM has integrated third-party biometric systems into AC2000, including iris scan.

In addition to supporting airport security efforts, AC2000 contributes to streamlined airport operations by helping to:

- Manage access throughout the airport environment and prevent unauthorized access to secure areas
- Manage the flow of passengers, visitors, and baggage through checkpoints
- Collect more accurate clock on/clock off times for billing
- Manage the ID pass production system with an interface for invoicing
- Provide command and control for airport security, law enforcement, and airport management personnel
- Provide one graphical user interface for all electronic systems within the airport
- Enable shared check-in desk usage
- More efficiently use and control the air bridges
- Manage vehicle flow and control vehicle access
Case Study: London Heathrow Airport

London Heathrow Airport uses a CEM solution to control 2000 card readers that control airside/landside boundaries, gate rooms, and offices. The solution is also integrated with alarms processing and pass production systems. The central server processes more than 1.5 million card swipes monthly for over 240,000 cardholders. If the card reader ever loses its connection to the controller, it uses a local database.

It is part of the largest networked system in the U.K., where Heathrow, Gatwick, and Stansted airports share the same data over a network, providing 135,000 people with access to some 3500 doors.
**Category:** Asset Tracking  
**Partner:** AeroScout  
**Product:** Unified Asset Visibility

Airports can use AeroScout Unified Asset Visibility solution to track the location, condition, and status of mobile assets and people over the Cisco Unified Wireless Network. Affix active RFID tags to moveable assets, or embed them in badges for people whose location you want to track. Smart tags from AeroScout can also accurately monitor the temperature and other environmental conditions.

Airport security departments can also use AeroScout solutions to quickly identify the nearest person with the right skills to react to incidents. Airports can also link location information with other information to create context-aware services. For example, if the location data is tied into a task management system, the system becomes aware of each security officer’s name, profile, round, and real-time location. It can then deliver relevant information such as CCTV images and alarms status in the officer’s vicinity (see Figures 14 and 15).

**Figure 14. AeroScout Unified Access Visibility Connectivity**

![Diagram of AeroScout Unified Access Visibility Connectivity](image-url)
Figure 15. AeroScout Unified Asset Visibility Operator View
Category: Passenger Information – Public Address
Partner: Singlewire (formerly Berbee)
Product: InformaCast

Singlewire InformaCast IP Broadcasting Solution simplifies airport-wide communication. The security department can simultaneously send an audio stream and text messages to any combination of Cisco Unified IP phones, IP speakers, and PCs. To send a live or recorded broadcast to one or more paging groups, security personnel simply push a button on the IP phone or click on the PC interface.

Airports that implement InformaCast can:
• Create live, ad-hoc, or pre-recorded audio broadcasts and/or text broadcasts
• Create paging groups using a variety of means
• Filter access to message types and recipient groups by user
• Schedule messages to be sent at a preset time or on a recurring basis
• Configure the frequency of message playback
• Administer broadcasts from a secure web interface or IP phone
• Broadcast multiple messages simultaneously to different paging groups
• Mix audio broadcasts with a conversation if a phone is in use, or indicate that the broadcast should not be played through phones that are in use
• Integrate flexible IP speakers (available from Atlas Sound) to provide an indoor or outdoor loudspeaker option
• Using zone controller hardware (available from Atlas Sound) to connect the network to an amplifier from which you can daisy chain analog speaker
• Allow all recipients of a broadcast to take turns talking within the group by pressing a talk soft key