TESSCO
making wireless work®

BelAir NETWORKS

Case Study

Ports on Atlantic, Pacific and Inland Waters Enhance Security, Operational Efficiency and Interoperability with BelAir Networks

Whether serving as conduits for national and international trade and tourism or home to critical naval initiatives, ports are a vital part of a nation's economic prosperity and defense strategies. Port security, therefore, is a matter of both national security and economic necessity. Because of the key role that major ports play in the supply chain of international trade, there is a constant struggle to manage security risks effectively in a manner that doesn't unduly impede the flow of goods. In any technology decisions, therefore, the often contradictory challenges of enhanced security and operational efficiency must both be considered and addressed.

Stephen E. Flynn, Ph.D., retired Commander, U.S. Coast Guard, author and recognized expert on homeland security notes: "…ports are the on- and off-ramps to global markets, and they belong to a worldwide system operated by many different private and public entities." The involvement of these many different private and public entities compounds the complexity of technology choices, necessitating the prioritization of interoperability in decisions regarding security and operational efficiency.

Whether run by the private or public sector, ports operate within rigid financial constraints. Recognizing the critical role that ports play in its national security, the US Department of Homeland Security (DHS) continues to make substantial amounts of funding available for port security initiatives, most recently through the Port Security Grant Program (PSGP), one of five grant programs within the DHS Infrastructure Protection Program (IPP) designed to strengthen the nation's ability to protect critical infrastructure facilities and systems.

This case study will review the growing role that BelAir Networks patented high-performance wireless mesh technology has and continues to play in increasing security, improving operations and enabling interoperable communications at major commercial and military ports through applications such as video surveillance, chemical detection, voice services and data networking. We will also look at these applications in light of

"…ports are the on- and off-ramps to global markets, and they belong to a worldwide system operated by many different private and public entities."

Stephen E. Flynn, Ph.D., retired Commander, U.S. Coast Guard

relevant funding criteria of the PSGP relative to Maritime Domain Awareness and Improvised Explosive Device (IED) Prevention, Protection, Response, and Recovery Capabilities for Port Facilities, Including Public Cruise Lines and Terminals.

A cross-section of BelAir Networks live port deployments, supporting civilian, military, freight and cruise traffic, will be discussed. Applications enabled by these wireless mesh networks at military and commercial ports, including Tier 1 (i.e. highest risk port regions per PSGP) on the Atlantic, Pacific and Inland Waters will be detailed. *However, BelAir Networks recognizes and respects the important role that the company's technology plays in port security and has agreed not to disclose the specific locations of the ports referenced in this case study.*

The Challenges

Security

Regardless of their location, the challenges faced at major ports are much more similar than different. They are hotbeds of activity, generally representing a mix of public access and secured areas, through which customers, personnel, visitors and travelers, valuable goods and containers, and various sizes of vehicles travel to and from adjacent roads and waterways. Despite their vast size and challenging logistics, maintaining the physical security of the port area is generally the domain of a relatively small number of individuals. Whether it's the Coast Guard, Customs and Border Protection agents, port authority police forces or other public, private or military security personnel (or some combination of these), the key to security is visibility.

The variable and high-bandwidth nature of video transmissions necessitates a predictable and high-performance wireless mesh network.

Comprehensive visibility of much of the port area can be achieved through 'pan, tilt, zoom' (PTZ) video cameras mounted throughout the property. But, for established ports, installing the necessary cabling to link a network of video surveillance cameras to central and remote monitoring areas, while not impossible, may be expensive and impractical. Underground cabling requires extensive time, labor and expense and disrupts port operations. Overhead wiring is problematic due to the necessary mobility of dockside, port and gantry cranes. Thus, wireless solutions start to look appealing provided that they can offer the performance and reliability characteristics required for real-time, high quality video surveillance.

One option is to provide dedicated point-to-point wireless links from each IP camera to the monitoring center. While technically this solution may provide the performance characteristics necessary, a single wireless connection between each camera and the monitoring center or centers inherently lacks the resiliency that these critical surveillance networks require. As a result, many ports have begun to deploy wireless mesh solutions that provide both the reliability and performance requirements. Wireless mesh backhaul solves this resiliency issue but only represents a viable alternative when the unpredictable performance associated with traditional wireless mesh technology is overcome. The variable and high-bandwidth nature of video transmissions necessitates a predictable and high-performance wireless mesh network with very low latency (i.e. delay) and jitter (i.e. timing/sequencing of IP packet delivery).

While visibility is critical, video alone is not enough to identify all of the threats in the port environment. Port personnel must also be vigilant in detecting the presence of hazardous chemicals and other materials that may put the port itself at risk, or for which the port is merely a gateway to a larger public safety threat.

Operational Efficiency

Along with the smooth flow of goods and people, reliable and efficient communications is key to major ports' operational efficiency, and to their ability to respond effectively in an emergency situation. Furthermore, the inherent mobility of most port personnel dictates a requirement for wireless voice and data communications to maximize their productivity. But cellular services are expensive and, like traditional radio solutions, lack the bandwidth required for large data and video transfers. Traditional wireless access point architectures necessitate extensive wiring, and associated labor, time and disruption and wireless mesh options typically introduce too much latency to support the often critical nature of voice communications among port personnel.

Additionally, given the requirement for outdoor mounted wireless communications gear, the relatively exposed nature of port environments dictates the need for extremely robust equipment that will survive weather extremes, depending on the port's specific location, and even lightning strikes. The firearms resistance capabilities of the wireless gear should also be considered to avoid the expense and challenge of having to install it within a bulletproof enclosure. Installation of this wireless networking gear can be also be more challenging and expensive if the wireless nodes lack the necessary interfaces required to connect with the available wireline egress.

Finally, where ship-to-shore communications are required, traditional cable-based systems generate high recurring maintenance costs for the cable infrastructure, while also disrupting communications during the period when the ship is entering but not yet docked at the port.

For operational efficiency to be achieved, all of these requirements must be addressed in a cost-effective fashion.

Interoperability

Though day-to-day security of a port typically falls to a fairly limited number of people, they often represent more than one agency or jurisdiction. In some cases, they also represent a combination of private, public sector, and/or military organizations. In the event of a significant security breach, emergency, accident, or disaster involving the port site even more agencies and departments will likely become involved. This multi-agency, multi-jurisdictional nature of the port security team can create huge communications challenges when the various agencies involved are operating on different wireless networks and frequencies.

A disaster situation will also drive a massive increase in network usage, resulting in the potential for service disruption. The need to share large amounts of video and data – including footage of the disaster scene and detailed geographical information system (GIS) mapping files of the area – among mobile security and public safety personnel also creates huge bandwidth demands on the network. Depending on the location and scope of the emergency, network coverage may also need to be immediately extended to support multi-agency, multi-jurisdiction security personnel.

The Solution for Efficient and Interoperable Security

Secure, standards-based, high performance wireless mesh network deployments based on BelAir Networks patented technology, as depicted in Figure 1, have cost-effectively addressed these security, operational and communications challenges at each of the ports discussed in this case study.

High-Performance Video Surveillance and Chemical Detection Networks

Video surveillance networks have been installed by collocating IP-based video cameras with BelAir Networks wireless mesh nodes. Ports have chosen different video security cameras and associated digital video recording (DVR) or network video recording (NVR) equipment according to their preference or requirements, but all are seamlessly supported on the BelAir mesh. These wireless video surveillance networks also incorporate analytics software and intelligent scene analysis to detect targets as well as management systems to control and manage the large number of cameras.

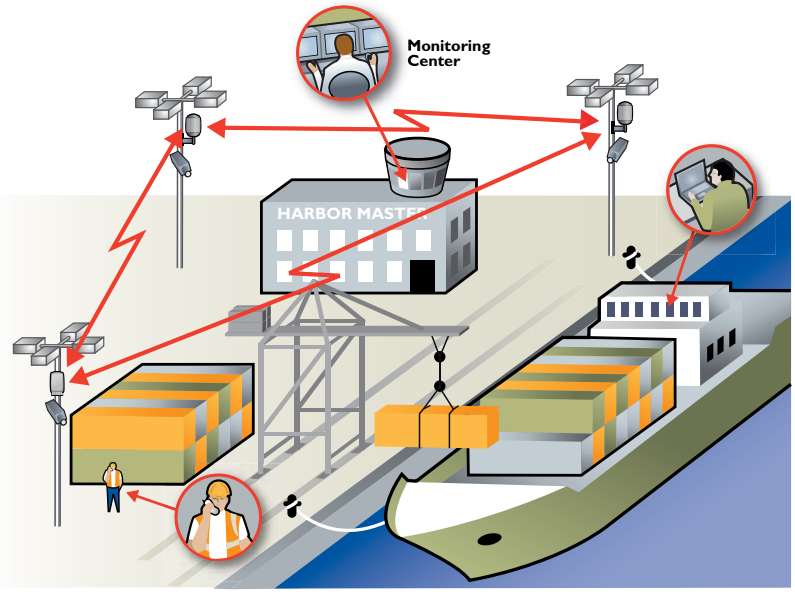

Figure 1. At civilian and military ports, carrier-grade wireless mesh networks support video surveillance cameras and Chemical Detection Sensors (CDS), voice services and data communications.

In some port locations, chemical agent detection units are installed at continuous monitoring points and integrated with BelAir wireless mesh nodes through a standard Ethernet interface. The detection units 'sniff' for the presence of chemical warfare agents (CWA) and toxic industrial chemicals (TIC) and the relevant telemetry data is instantly transmitted to the command and control centers over the high-speed wireless mesh network.

Both the video surveillance and chemical agent monitoring systems must operate around the clock, necessitating a resilient and highly reliable wireless network infrastructure. Additionally, video places high demands on network bandwidth, and requires exceptionally low latency and jitter. BelAir wireless mesh provides predictable, high-performance, high-bandwidth wireless networking with the industry's lowest latency rate and minimal jitter.

Recognizing the critical role that video surveillance and chemical monitoring play in port security, funding criteria of the PSGP includes provisions for the deployment of detection and surveillance equipment in support of maritime domain awareness. Chemical agent detection sensors and video surveillance systems that contribute to IED prevention, protection, response and recovery capabilities are also included in the funding criteria.

Carrier-Grade Wireless Networking Delivers Security and Operational Efficiencies

The same BelAir Networks nodes that are used to create a resilient wireless network to transport video traffic from surveillance cameras to monitoring sites are also used to provide broadband access to a wide range of standards-based wireless-enabled end user devices. These devices include a growing number of cost-effective and readily available wireless voice over Internet Protocol (VoIP) and dual mode (cellular/Wi-Fi) phones, and other mobile/handheld devices like laptops and tablet computers.

While video surveillance deployments tend to focus on the port and dockside areas, BelAir Networks nodes have also been used to extend broadband voice, video and data networking services in ship-to-shore applications and on the ships themselves. In the ship-to-shore applications for underway vessels entering and leaving the harbor, and docked at port, BelAir Networks wireless mesh has been deployed to replace the cable infrastructure previously used. This provides the ships with uninterrupted high bandwidth service, even as they transition from underway communications to pier side, reducing both the recurring maintenance costs and the service disruptions associated with the cable-based connections.

Port personnel are able to access, receive, transmit and share classified information over a secure wireless architecture.

Portwide, dockside, ship-to-shore and ship-wide broadband wireless networking enables all port personnel, including those responsible for port security, to work more productively and improves the security and efficiency of port operations overall. Port personnel are able to access, receive, transmit and share classified information over a secure wireless architecture that is less expensive, less disruptive and more robust than traditional wireless access point architectures. In some ports, additional savings have been realized through a reduction in cellular charges.

Differentiating BelAir from traditional wireless mesh technology is our ability to reliably support Quality of Service (QoS) parameters and classification and prioritization of traffic by application and user. The ability to prioritize traffic by application ensures high-quality low latency and jitter-free voice and video transmissions. Meanwhile, the ability to prioritize traffic by user type ensures secure, uninterrupted, high-bandwidth network availability for port personnel around the clock. For example, even while cruise ship passengers are enjoying high-speed, public internet access, the same wireless mesh is delivering critical voice, data, and video communications to port security and other personnel on a separate and secure network.

From a funding perspective, the PSGP includes provisions for the development/enhancement of information sharing systems, including equipment (and software) required to receive, transmit, handle, and store classified information.

Interoperability for Secure Multi-Agency, Multi-Jurisdiction Cooperation

In the case of an emergency or disaster, the same high priority network availability associated with port personnel can be securely and reliably extended to personnel from multiple agencies, departments and jurisdictions, using a wide range of readily available wireless-enabled IP-based phones, devices, and laptops. In traditional wireless mesh networks, and often in cellular networks, the spike in usage associated with a critical event can result in noticeable service degradation and even disruption. The high capacity associated with BelAir Networks switched mesh architecture and its ability to prioritize critical traffic ensures consistently high performance and reliability.

To qualify for deployment at these ports, BelAir Networks wireless mesh products have undergone rigorous testing both pre- and post-deployment by both private and public sector agencies, including the National Security Agency (NSA).

Thankfully, none of the ports that have deployed BelAir Networks gear have yet faced a manmade or natural disaster. But the same BelAir wireless mesh networking technology was proven in a live disaster scenario when the I-35 bridge collapsed in Minneapolis in what Governor Tim Pawlenty described as a "catastrophe of historic proportions for Minnesota." In that case, personnel from multiple agencies and jurisdictions used the Wireless Minneapolis network (comprised of BelAir wireless mesh nodes and expanded to cover the riverbanks and other affected areas) for a number of critical applications. These included real-time video surveillance of the disaster site with remote monitoring from both the command centers and the Emergency Operations Center (EOC), and sharing and transmitting massive GIS-based mapping files to assist recovery efforts. These same wireless mesh nodes supported public access use by more than 6000 concurrent users, many of whom turned to the Wireless Minneapolis network when the cellular networks failed due to the increased volume of users.

In addition to highlighting the importance of the wireless network's ability to support communications interoperability among a sharply increasing number of users, the Minneapolis bridge disaster highlights three other issues common to port emergency situations. First, bandwidth heavy applications such as transmission and sharing of real-time and recorded emergency or disaster scene video footage and massive GIS files of the affected area, among mobile security and public safety personnel place huge capacity demands on the network. Secondly, depending on the geographical location and scope of the emergency relative to the port's existing wireless mesh network coverage, interoperable and high performance communications may need to be immediately expanded. Finally, while recognizing the human toll of a critical situation, the resumption of 'business as usual' status, including the smooth flow of goods and people, is a priority that drives disaster recovery efforts of all agencies and jurisdictions involved. In Minneapolis, BelAir's high performance wireless mesh technology enabled high-bandwidth communications interoperability among multiple public safety agencies from local, state and federal jurisdictions to help get re-building efforts underway as quickly as possible. In fact, the video surveillance network set up for recovery efforts was retained to provide security at the bridge construction site.

The importance of communications interoperability in port security is underscored by provisions of the PSGP enabling funding for the enhancement of interoperable communications for sharing terrorism threat information (including ensuring that mechanisms are interoperable with Federal, State, and local agencies). Interoperable communications equipment supporting IED prevention, protection, response, and recovery capabilities for port facilities, including public cruise line and terminals can also qualify for funding.

The Design

To qualify for deployment at these ports, BelAir Networks wireless mesh products have undergone rigorous testing both pre- and post-deployment by both private and public sector agencies, including the National Security Agency (NSA). All BelAir wireless mesh outdoor products are environmentally hardened and proven to perform consistently and reliably in the most extreme temperatures, from the cold of Alaska, to the heat of Arizona and in the salty dampness of the maritime environment. The BelAir products also meet the firearms resistance requirements outlined in Telcordia GR-487 Generic Requirements for Electronic Equipment Cabinets, so no additional enclosures (along with their associated expense and deployment challenges) are required. The variety of Ethernet and fiber interfaces available on the BelAir nodes enables integration with a broader range of wireline environments to facilitate network planning and deployment.

Comprehensive Family of Carrier-Grade Products

BelAir's wireless mesh product line is the most comprehensive in the industry and includes the flagship four-radio BelAir200 Wireless Multi-service Switch Router, the three-radio BelAir100T wireless mesh node, the dual-radio BelAir100 Multi-service Node, the single- or dual-radio BelAir100C Multi-service Node featuring point-to-multipoint backhaul, and the strand-mounted BelAir100S all seamlessly using the BelAirOS operating system and managed by BelViewNMS. The modular nature of the BelAir nodes supports multiple frequencies on a single mesh and ensures a seamless upgrade path to accommodate new standards and spectrum bands. Depending on their application and coverage requirement (across or in specific areas of each port, dockside or vessel), the ports discussed in this case study have taken advantage of BelAir's flexible architecture to deploy a mix of 'multiple point-to-point', 'point-to-multipoint', and 'point-to-point' wireless connections.

Given the critical nature of port communications, BelAir's patented switched mesh architecture was a key deciding factor in all cases.

Patented Switched Mesh Architecture = High Performance Networks

Given the critical nature of port communications, BelAir's patented switched mesh architecture was a key deciding factor in all cases. While all wireless mesh solutions provide a redundant path from one node to another, most wireless mesh nodes communicate on the same channel of the same frequency in a hub-like multipoint-to-multipoint fashion. As a result, the bandwidth of that single channel, single frequency is shared among all nodes in the mesh simultaneously, resulting in what could be referred to as a "shared mesh". This shared mesh architecture limits the capacity of the network and results in high and unpredictable latency and jitter as traffic grows. Scalability to address increased users and applications is therefore very limited and the unpredictable performance makes the network unsuitable to latency sensitive applications such as voice and video.

BelAir's patented switched mesh architecture is different. BelAir can provide multiple dedicated and isolated point-to-point connections, supporting diverse paths between each BelAir node in the mesh. Additionally, each BelAir node contains a sophisticated Layer 2/3 Ethernet Switch so traffic traversing the BelAir mesh can be classified, rate limited, prioritized and load balanced as shown in see Figure 2.

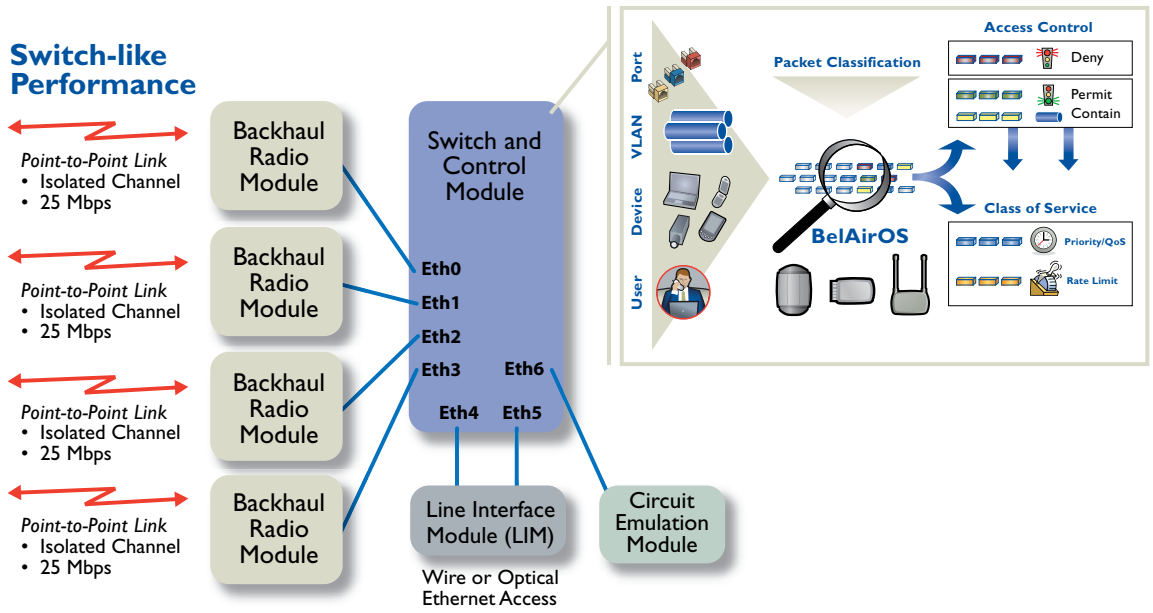

Figure 2. BelAir's patented switched mesh architecture.

As a result, a BelAir mesh operates in the same manner as a wireline Ethernet switch, replicating the performance, high capacity and exceptionally low latency and making it suitable for critical communications including voice and video.

Cost Effective, Instantly Scalable and Secure Coverage

While most of the port deployments discussed in this case study cover a large geographical area, in one case there was a requirement to start with a small network comprised of just a few nodes. Even in small deployments, BelAir offers higher performance and better value than other mesh solutions. And BelAir's unique architecture scales to address more users, applications and coverage area instantly and seamlessly. BelAir's 'capacity on demand' capability enables capacity to be added anywhere the network without adding nodes, just by adding an additional wired egress. The additional capacity can then be directed to wherever it's needed in the network. This capability, combined with the availability of both Ethernet and fiber interfaces on the BelAir nodes, makes network planning and expansion much easier and more cost effective.

Of course, as was proven in Minneapolis, additional coverage areas can be added to the existing mesh network by just adding more nodes. Unlike the shared mesh architecture discussed previously, which degrades in service as nodes are added to the mesh, BelAir's switched mesh architecture maintains its high capacity and high performance as the network is geographically expanded.

BelAir wireless mesh solutions support a multi-layer security strategy to address the user, infrastructure, and management layers of the network. BelAir's wireless mesh architecture leverages standards based methods to prevent unauthorized access to the network, including 802.1x RADIUS and EAP Authentication, WEP, WPA I

(TKIP) and WPA2 (AES) encryption for end user authenticating, authorizing, and accounting. BelView Network Management System leverages SSH, SSL and SNMPv3 standards for encrypted management and network administration log-in ensuring that only authorized personnel gain access to network devices and configuration files. The system also maintains access records for auditing purposes. Network integrity and performance are protected by segregating traffic according to application, authorized user group, and QoS levels through mechanisms such as virtual local area networks (VLAN) and multiple Service Set Identifiers (SSID).

The Result

Ports and port-related industry are responsible for more than 8 million US jobs, according to the American Association of Port Authorities (AAPA), and the ports discussed in this case study, while varying in geographic size and scope, are responsible for the movement of hundreds of thousands of tons of cargo and hundreds of thousands of cruise ship passengers annually. By reliably and consistently supporting critical applications such as video surveillance, chemical detection, voice services and data networking, BelAir Networks patented high-performance wireless mesh technology has increased security, improved operations and business continuity capabilities, and enabled interoperable communications at these major commercial and military ports.

BelAir Networks has increased security, improved operations and business continuity, and enabled interoperable communications at these major commercial and military ports.

It's important to remember that where these applications are deployed to support maritime domain awareness or IED prevention, protection, response and recovery capabilities for port facilities, including public cruise line and terminals, the video surveillance systems, chemical agent detection sensors, and interoperable communications equipment, including the wireless mesh nodes, may address criteria of the PSGP and be eligible for funding.

In addition to the ports discussed in this case study, BelAir Networks has hundreds of deployments worldwide, in leading cities such as New York, Minneapolis, Boston, London and Toronto, and high-profile venues including Dolphin Stadium and Lincoln Center. BelAir Networks offers the industry's most comprehensive product portfolio of environmentally hardened carrier grade equipment supporting 802.11 (Wi-Fi), 802.16 (WiMAX), 4.9 GHz Public Safety standards and spectrum bands.

BelAir NETWORKS

TESSCO making wireless work®

Contact TESSCO Today!
800.472.7373 | TESSCO.com