Case Study

Seattle Fire Department: Improving Firefighter and EMS Responses

A Sierra Wireless® Mobile Workforce Solution

CUSTOMER CRITICAL CHALLENGE

- Leverage new mobile technology that could support increased bandwidth and meet new voice, video and data initiatives for critical services while sharing the network with other agencies.
- System security and the ability to cater to multiple networks as carrier coverage varied.

SOLUTION

- Seattle Fire implemented the AirLink mobile router as their emergency vehicle communications platform.

BENEFITS

- Critical emergency communications are now dedicated to the broadband network shared with Seattle Power, Wi-Fi is used for high-speed file transfers and software maintenance.
- Dispatching and emergency communications can use photos and transmit larger data sets.
- Software and file updates to MDTs and mobile devices can now be done on a regular basis.

BACKGROUND

The City of Seattle Fire Department provides fire suppression and emergency medical services to the culturally diverse and vibrant population of Seattle. Since being organized in 1894, Seattle Fire has evolved from an organization focused only on fire fighting, to include other critical services such as building inspections, fire code enforcement, tactical rescues and public education, and has specialized units for hazardous materials response, dives, confined space rescue, heavy rescue, and marine emergency response.

"We have deployed the mobile communications system to improve patient care and response times as part of our commitment to provide the citizens of Seattle the best emergency and medical services possible."

Leonard Roberts, IT Director,
City of Seattle Fire Department

Seattle Fire responds to nearly 80,000 fire and medical incidents in the City of Seattle each year. The Fire Department's Medic One Program provides the City of Seattle with Advanced Life Support activities and responds to approximately 46,000 Basic Life (BLS) alarms and 19,000 Advanced Life Support (ALS) alarms per year.

Business Challenge

As part of larger Seattle's city-wide public safety network, Seattle Fire Department needed the ability to leverage new mobile technology that could support increased bandwidth and handle other key department objectives while still sharing the network with other agencies. Key concerns with implementing any new mobile technology was the system's security and the ability to cater to multiple networks as carrier coverage varied. Seattle Fire shares the governance of the wireless network with the city's central IT department so any new implementation would require tight coordination and organization.

Before Seattle Fire could consider any solution for mobile technology implementation four key areas had to be addressed:

1. ADDRESS THE BANDWIDTH LIMITATIONS OF WIRELESS NETWORKS

- Ensure bandwidth is available for critical emergency communications.
- Ensure that file transfers and software maintenance such as pre-incident plans, security and package software updates do not interfere with emergency communications.

2. MEET BUSINESS OBJECTIVES AND ADDRESS SECURITY

- Support dispatching and emergency communications' high demand on broadband infrastructure to transmit photos and larger data files.
- Support fleet-wide software and file updates to mobile data terminals (MDT) and attached mobile devices such as medical vaults.
- During mass casualty situations, enable smartphone technology to be used to transmit bar codes and medical triage codes to emergency rooms before patients get transferred.

BENEFITS CONTINUED

- Smartphones can connect to the mobile hotspot provided by the gateway to transmit bar codes and medical triage codes to the emergency room before patients are transferred.
- Paramedics can transmit EKG files to emergency rooms.
- Central management of configuration changes, certificate re-provisioning, pre-shared keys (PSKs), password recycling, security updates etc
- Increased security using PSKs across network devices coupled with a second level of authentication to provide two levels of security, instead of certificates on each device.

AWDS ACCESS WIRELESS DATA SOLUTIONS

SIERRA WIRELESS

- Enable paramedics to transmit audio and EKG files from Physio Control defibrillators to emergency rooms.
- Given that patient medical information is involved, ensure all communications meet HIPAA requirements and are safe from cyber-attack and unauthorized intrusions.

3. DEFINE ONGOING MANAGEMENT STRATEGY (GOVERNANCE)

- Centralize management of configuration changes, certificate re-provisioning, pre-shared keys or certificates (if viable) and password recycling, security updates, etc.
- Engineer for fast network switching and roaming.
- Implement connection management and security technology between Wi-Fi and broadband without loss of credentials, authentication or re-logging.
- Implement a security strategy that can be managed with existing IT resources and, at the same time, with minimal risk.

4. BUILD AN ARCHITECTURE TO MEET OPERATIONAL, BUSINESS, SECURITY AND USE-CASE OBJECTIVES

- Enforce two levels of device authentication.
- Ensure end-to-end VPN connections with data encryption.
- Centralize Wi-Fi management, including centrally managed security.

Sierra Wireless Solution

After carefully reviewing numerous technologies, Seattle Fire decided that the wireless technology to support their initiatives would be best provided by a mobile router. This preferred strategy would allow Wi-Fi/broadband coordination, integration and switching to ensure lower latency without losing important data. After a successful trial of the AirLink mobile routers in three vehicles, Seattle Fire implemented the full solution as their emergency vehicle communications platform.

The solution allows Seattle Fire to leverage new voice, video and data mobile wireless initiatives by providing secure, seamless, fast switching in real-time between multiple networks without the need for each end-user device to have multiple embedded radios. It also allows Seattle Fire to lower the total cost of owning mobile wireless technology because fork-lift upgrades to change radios are not required – the routers are upgradeable. The solution provides Seattle Fire with a secure, manageable end-to-end communications system to extend the enterprise network to the vehicle fleet. Seattle Fire now has a solution for mobile technology implementation in which their four key challenges have been addressed:

1. OVERCOME LIMITED WIRELESS BANDWIDTH

- With the router's capability for operating on multi-networks, critical emergency communications can now be dedicated to the broadband network that is shared with Seattle Power while Wi-Fi can be used for high-speed file transfers and software maintenance such as pre-incident plans, security and package software updates.

2. ACHIEVED BUSINESS OBJECTIVES

- Dispatching and emergency communications can use photos and transmit larger data sets and have the flexibility of switching between Wi-Fi and broadband infrastructure within the router. A dispatch message goes to the fire apparatus most of the time over the Wi-Fi network to the mobile data terminal (MDT) because vehicles are usually in the station at the time of dispatch. When the vehicle responds and leaves the fire station, data transmissions switch automatically to the broadband network within the router.
- Fleet wide software and file updates to MDTs and attached mobile devices such as medical vaults can now be done on a regular basis, starting in the station and automatically switching between Wi-Fi depots through the router. These updates are handled by the AirLink Mobility Manager (AMM) for configuration and security while the AirLink Connection Manager (ACM) handles the persistent connection and switching requirements.
- During mass casualty situations such as earthquakes and natural disasters, smartphones or other handheld devices can connect to the Wireless Access Point (mobile hotspot) provided by the router to transmit bar codes and medical triage codes (red, yellow, green, white and black) to the emergency room before patients are transferred. The information is encrypted and sent through a VPN tunnel outside of the city network for HIPAA compliance/security.
- Paramedics can now transmit EKG files from Physio Control defibrillators to hospital emergency rooms using the router through the ACM on a VPN tunnel outside of the city network for HIPAA compliance/security over the Physio Control network.

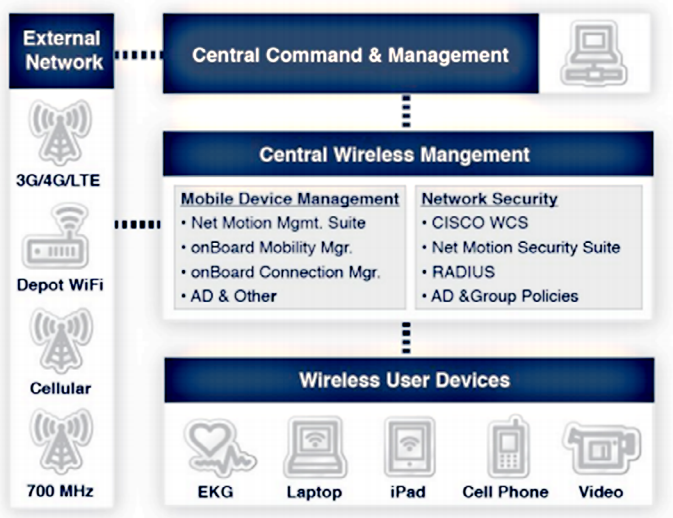
3. PROVIDED AN ONGOING MANAGEMENT STRATEGY (GOVERNANCE)

- The solution delivers effective mobility management technology that provides secure, fast network switching and roaming to maintain a persistent connection between Wi-Fi and broadband networks without loss of credentials, authentication or re-login. The router allows Seattle Fire to use diverse networks from 4.9 GHz to 2.4 GHz, Wi-Fi, mesh, and fixed wire to their primary carriers, Sprint and Verizon Wireless, that provide the network back-haul.

"With 33 fire stations and over 60 vehicles including fire engines, ladder trucks, and medic units, we needed IT to have the ability to remotely monitor vehicle's health, location, and network connections, and to accurately monitor our mobile devices – which is only possible with the AirLink solution."

Leonard Roberts, IT Director,
City of Seattle Fire Department

- The AMM allows for central management of configuration changes, certificate re provisioning, pre-shared keys (PSKs), password recycling, security updates etc. Certificates work best for device authentication, but are very difficult to manage on a 24x7 mobile platform that does not support auto-enrolment. This can now be handled more efficiently with the use of PSKs and a second level of authentication with RADIUS. Seattle Fire initially provisions all devices in the laboratory with keys and IP addresses before deployment, so they can all be managed remotely and centrally.
  - By implementing the AirLink solution, Seattle Fire has a security strategy that can be managed with existing IT resources, and can support security for other devices through the router's firewall, NAC and WPA2-PSK features. The solution allows the streamlining of current processes and policies for better IT management.



4. MET OPERATIONAL, BUSINESS, SECURITY AND USE-CASE OBJECTIVES

- Seattle Fire has determined that employing the device is the preferred operational strategy for Wi-Fi/ broadband integration instead of using end-user devices with multiple embedded radios.
- The solution offers unique broadband capabilities by allowing multiple network cards and switching automatically between networks. When Seattle Fire wishes to upgrade, they only need to replace the network card in the router, not each mobile device. This decreases the total cost of owning mobile wireless technology because fork-lift upgrades to change radios are not required.
- Through the device, Seattle Fire can increase security by using PSKs across network devices coupled with a second level of authentication to provide two levels of security, instead of certificates on each device. Seattle Fire MDTs are always logged on, and only shut down for maintenance, with a reboot once every shift. Passwords and codes are hard-coded and encrypted on the MDT and used to log on.
- Seattle Fire now has the ability to leverage the centralized management of all wired and wireless devices by using the router, providing data encryption through an end-to-end VPN connection for increased security.

AWDS ACCESS WIRELESS DATA SOLUTIONS
SIERRA WIRELESS

- The centralization of Wi-Fi/broadband management into the router allows fast switching between Wi-Fi and/or broadband without losing valuable information. The device can switch networks in under 8 seconds, rather than the longer switching times of 60-90 seconds provided by other technologies. Seattle Fire can't afford to lose key information while responding to any emergency.

Results

Seattle Firefighters and Paramedics are now better equipped to handle incident responses en route and on scene, pre-hospital emergency patient care, and day-to-day operations.

- Firefighters can now, in real-time, look at pre-fire plans including building diagrams, bird's eye views, hazardous materials, access and egress routes and fire control systems.
- Dispatch and emergency communications can now be allocated based on multi-network capability.
- Manage fleet-wide software and file updates to mobile data terminals (MDTs) and attached mobile devices such as medical vaults. Previously, fire and software updates over a broadband connection took one week, and pre-incident plans took 10-14 days. Now, the entire fleet can be updated over Wi-Fi within one day.
- Paramedics can transmit EKG files from Physio Control defibrillators to hospital emergency rooms to enable the ERs to be better prepared for patient arrivals.

"With 33 fire stations and over 60 vehicles including fire engines, ladder trucks, and medic units, we needed IT to have the ability to remotely monitor vehicle's health, location, and network solutions, and to accurately monitor our mobile devices - which is only possible with the solution," said Leonard Roberts.

AWDS
ACCESS WIRELESS DATA SOLUTIONS

About Access Wireless Data Solutions

Access Wireless Data Solutions (AWDS) provides advanced cellular connectivity solutions for M2M and IoT fixed and mobile applications. We understand wireless and as an industry leading distributor and value-added reseller of cellular gateways and modems we work closely with our customers to implement technology to keep them connected.

Access Wireless Data Solutions is your premier value add reseller for the best in brand cellular routers and modems. Access is the first word in connecting your networks. These devices from industry distinguished OEM manufacturers are designed to fit your cellular application, both fixed and mobile, in our modern IoT and M2M world. Our professional consultative sales team is ready to assist with device recommendations for your project. Let us do the heavy lifting so you don't have to.

For more information contact AWDS at (813) 751-2039 or visit www.accesswds.com.

About Sierra Wireless

Sierra Wireless is building the Internet of Things with intelligent wireless solutions that empower organizations to innovate in the connected world. We offer the industry's most comprehensive portfolio of 2G, 3G, and 4G embedded modules and gateways, seamlessly integrated with our secure cloud and connectivity services. OEMs and enterprises worldwide trust our innovative solutions to get their connected products and services to market faster. Sierra Wireless has more than 950 employees globally and operates R&D centers in North America, Europe, and Asia.

For more information, visit www.sierrawireless.com.

SIERRA WIRELESS