

CASE STUDY

Federal Government



Department of the Interior Taps Fortress for Glacier National Park Renovation Program Secure Wireless Solution to Provide Road Condition Information

When the U.S. Department of the Interior needed to provide secure wireless communications for Glacier National Park's Going-to-the-Sun Road Rehabilitation and Mitigation program, they chose Fortress. The program required enabling immediate voice, video and data capabilities in a completely secure wireless environment from mobile construction trailers.

The Going-to-the-Sun Road is one of the most intricate roadways in the United States and this renovation project is essential to ensuring the safety and reliability of the entire 50 mile span. The Department of the Interior required a wireless solution that could provide reliable communications between disperse access points - up to 20 miles apart - as well as a low-profile, non-intrusive, aesthetically pleasing product to blend into the natural environment.

Fortress ES520s are Perfect Fit

Opened in 1932, the Glacier National Park's Going-to-the-Sun Road provides public access through the park's wild interior. The National Park Service (NPS) and Federal Highway Administration (FHWA) initiated the rehabilitation and mitigation project in June 2006 to provide significant design, development and construction improvements. As part of the project, the Fortress ES520 secure wireless access bridges will be fixed to mobile construction trailers, providing the ability to communicate road construction updates, as well as traffic and condition information internally and to visitors. The mobility of the solution enables NPS and FHWA personnel to travel the road and provide updates in real-time.

Fortress ES520 Secure Wireless Access Bridges are able to provide secure wireless networking in areas that have no available infrastructure. This is the exact scenario Glacier National Park faced.

Fortress secure wireless access bridges are all-in-one network access devices with built-in security. The ES520 is ideally suited to work as a self-contained network combining the functions of an access point, Ethernet switch and security gateway in a form factor engineered specifically for harsh outdoor environments. The solution integrates commercial cryptographic algorithms - including Advanced Encryption Standard (AES) for encryption, Elliptic Curve Cryptography (ECC) for digital signatures and key exchange, as well as hashing - into its Defense Information Systems Agency's (DISA) Joint Interoperability Test Command (JITC) and National Institute of Standards and Technology's (NIST) FIPS 140-2 certified security solutions.



Challenges

- Application is to network mobile construction trailers on "Road-to-the-Sun" and to provide traffic updates and conditions for visitors
- Aesthetics matter in this implementation - the devices used cannot be permanent
- Landscape architects at the site require low-profile, non-intrusive solution
- 20 mile reach supporting 6Mbps throughput

Solution

- Fortress ES520 Secure Wireless Access Bridges were chosen because of the long reach of their powerful radios
- Small, rugged and easily mounted, the ES520s are well suited for this environment

Results

- Fortress ES520s act as relays so that only one device is needed where the competition would have had to place two devices
- Throughput and reach back requirements were easily met
- Solution complies with aesthetics requirements as Fortress ES520s are small and easily pole-mounted
- Visitors and employees to national park get real-time road condition information



For more information about the Fortress product suite for Federal Government:

phone: 813.288.7388

visit: www.fortresstech.com

email: info@fortresstech.com

Fortress Technologies Inc.
4023 Tampa Rd., Ste. 2000
Oldsmar, FL 34677