



Communications on the Border

The U.S. Customs and Border Protection (CBP) implements an innovative Project 25 (P25) and mesh network to secure the Southwest.

By William M. Brown

Effective LMR communications are vital to officer safety in the field for border patrol, customs inspection and air/marine operations. One of the largest Project 25 (P25) networks in the world provides reliable, resilient and secure voice and data communications to the thou-

sands of men and women of the Department of Homeland Security (DHS) Customs and Border Protection (CBP) who patrol and secure the U.S. Southwest frontier. Immigration and Customs Enforcement (ICE) officers and other federal officials use the network as well.

The overall project provides communications capabilities for CBP field personnel in 20 geographic focus areas across the United States. The total cost was about \$85 million, with \$3 million for the two-way radio base station and repeater equipment and another \$3 million for the wireless IP backbone equipment including broadband radio links.

The P25 tactical communications modernization project in California, Arizona and New Mexico incorporates a wireless IPv4/IPv6 mesh networking backbone, which integrates into a common, secure infrastructure. Several hundred repeaters, voters and satellite receivers service a 250,000-square-mile area.

System Overview

The Arizona CBP network — conceived in 2006 with phased operations starting in 2007 — is in many respects, the most technically sophisticated regional P25 network deployed to date. The network fuses IP and P25 network equipment into a single, multistate system to maximize operational effectiveness at a reasonable capital deployment cost and operational expense. The completed Yuma and Tucson sector network includes more than 215 repeater and base station networked sites.

The CBP required 15 operational objectives based on lessons learned from past deployments to achieve its mission and operational goals:

1. Provide 24/7 secure, digital P25 service along the entire length — nearly 500 miles — of the Arizona/Mexico border;
2. Provide continuous two-way radio service in the event critical communications facilities such as radio links, telco hubs or equipment are lost;
3. In the event of a site equipment failure, provide the ability to remotely access the problem site and provide a patch-around capability;
4. Provide a minimum latency transport infrastructure to enable operation of key P25 features such as over-the-air rekeying (OTAR)



The CBP sectors show the overall responsibility of the CBP along the international borders with Mexico and Canada.

and programming (OTAP);

5. Full support of non-network-based appliances on the IP network without affecting radio network traffic performance;

6. Support for all P25 base and repeater equipment interfaces including interfacing to the Motorola Quantar and AstroTac via V.24 interfaces;

7. Provide full online remote access to all Motorola equipment via Motorola's Radio Service Software (RSS) port, minimizing the need for on-site support personnel;

8. Provide a true mesh least-cost networking capability for near-instantaneous alternate routing in the event of site or link failure;

9. Allow remote operations for multiagency and disaster operations;

10. Provide the ability to quickly and securely provision the network for special needs and requirements;

11. Support maintenance via a deep ability to remotely diagnose and monitor traffic of all LMR and non-LMR assets;

12. Enable federal, state and other governmental agencies to independ-

ently and securely use the network;

13. Minimize site installation and provisioning visits by pre-staging, provisioning and testing each network site prior to installation;

14. Support T1 to DS-3 telco service connections; and

15. Provide support to future broadband wired and wireless media connectivity.

System Design Strategy

CBP staff at the National Law Enforcement Communications Center (NLECC) in Orlando, Fla., along with CBP personnel in the field and the Office of Information Technology (OIT) contributed to the design. The OIT staff managed the implementation, commissioning and cutover to a government-run system. The NLECC personnel designed and implemented the network operations tasks responsible for system networking and monitoring.

Overall IP Network Design Concept. Ad-hoc networking architecture — wireless nodes that directly communicate with each other — is employed in the Arizona network. Operating in ad-hoc mode, all wireless devices within range and through a wireless controller communicate in peer-to-peer fashion without involving a centralized routing or access system. This decentralized approach is ideal for mission-critical applications where central nodes can't be relied on and fault avoidance is critical. In addition, the ad-hoc methodology makes for a highly scalable network, requiring minimal configuration and allowing for quick deployment suitable for small- to large-sized systems, such as public-safety, industrial and government systems. Adding a dynamic adaptive routing protocol enables ad-hoc networks to form quickly and to react nearly instantaneously to link breaks and faults.

The Arizona CBP P25 backhaul network uses full-duplex wireless links providing a 768 kilobits per second (kbps) payload capacity in each direction — east to west and west to east. An in-depth analysis

CBP Upgrade Equipment Suppliers

Backhaul RF Path Design	CBP OIT
LMR Coverage Design	Motorola
P25 Radios	Motorola, Tait Radio Communications and EF Johnson Technologies
Combiners and Antennas	TX RX Systems Bird Technologies Group
IP Backbone Site Controllers and Networking Equipment	Metric Systems
Integration of Backbone Networking Equipment	Metric Systems
T1 Backhaul Radios	General Electric
IP Backbone Antennas	Kathrein Scala Division, General Dynamics Satcom Technologies (Gabriel)
Solar Panels	Kyocera Solar
Hydrogen Fuel Cells	ReliOn

was undertaken to arrive at a licensed operating band that balanced point-to-point links of 60 plus miles with real tower heights, antenna type and gains, signal reliability, available frequencies and the availability of off-the-shelf data radios. A subsequent spectrum search by the National Telecommunications and Information Administration's (NTIA) Office of Spectrum Management (OSM) granted multiple pairs of transmit/receive (TX/RX) operating frequencies in the lower microwave spectrum. With nearly two years of operational service, the reliability and robustness of the original spectrum choice has been demonstrated.

Network Routing Element. The key to a robust, decentralized ad-hoc mesh network is the use of a flexible routing element at each mesh node. In addition to providing the dynamic mesh routing capability, each Arizona routing element provides key additional capabilities for diagnostics and network control and monitoring:

- Physical interface support for Motorola Quantar V.24 synchronous interfaces;

- Physical and support interfaces for up to four independent ad-hoc wireless link radios;

- Multiple secure virtual local area network (VLAN) tunnels to support non-mobile radio network appliances;

- Diagnostic agents and tools to support simple network management protocol (SNMP)-driven network management system and site monitoring analog and digital input/output (I/O) system requirements;

- Ability to remotely and securely access and provision LMR station parameters and provisioning elements with no on-site intervention and minimum off airtime; and

- Tools to avoid or offset the frequency of physically returning to the remote site.

Motorola, Tait Radio Communications and EF Johnson Technologies supplied LMR infrastructure



An LMR solar site shows the pre-staged P25 station installed at a typical remote site node.

and subscriber handheld units for the network. The CBP, following laboratory and in-field on-the-air evaluations, chose the Safari wireless networking controller from Metric Systems as the core routing element for its Arizona network.

Network Support Devices. CBP decided to standardize an approach to packaging and powering each two-way radio remote and central site. The strategy centered on pre-staging all backbone equipment into a single 14U ruggedized transportable Hardigg case. This approach allowed the systems integrator to pre-wire, provision and live test all components interfaced with the specific two-way radios expected at the site. In addition to the full-duplex fractional T1 radio and Safari controller, five components were added to the pre-staged enclosure to ease site integration and operation. A network-managed AC strip allowed the controlled startup of each remote element, along with the ability to gauge AC current and selectively restart each component if required. The asynchronous serial server enabled maintenance and network management personnel to independently access Quantar RSS ports, along with serial interfaces from non-mobile radio devices.

A purpose-built user shelf pro-

vided a positive connection scheme for interfacing the Motorola Quantars V.24 and RSS ports. The user shelf also provided four high-speed, switched Ethernet ports, which together with the controller provided eight additional Ethernet ports for IP-based P25 repeaters and non-two-way radio devices. This overall modular design has been proven in more than 80 remote installations. Typical site integration and turnaround time is less than an hour given that the backbone radio antennas are up and correctly aligned.

Network Diagnostics and Commissioning Tools. Once a site was installed and commissioned, effort was taken to avoid a maintenance visit unless necessary. About 20 percent of the sites are accessible only through airlift or long drives over dangerous desert and mountain roads. Costing time, dollars and personnel safety, the technical objective was to provide a robust set of diagnostic and commissioning tools that allow all responsible personnel the ability to request and observe the range of communications and site parameters available to correctly ascertain system operation or faults.

The utility and value of delving into a network's traffic flow and interpreting packet types and protocols is paramount. About 10 percent of Arizona sites are remote solar-powered sites, on mountaintops and accessible only by helicopters costing \$5,000 per hour to operate. So it's imperative that as a site buildout is completed, it is unambiguously certified as operating. Networking all available site parameters, such as communications, security and power, facilitates check out.

This requires that all network devices receive a unique IP address and device identifier. Hundreds of IP addresses are required in the Arizona network. Duplicate IP addresses cause serious problems. In the final days of a large-scale system commissioning exercise demonstrating interoperability among multiple P25 repeater vendors, a rogue device on the network responding as

CBP Upgrade Cost Breakdown

The total cost was about \$85 million with \$3 million for the two-way radio base station and repeater equipment and another \$3 million for the wireless IP backbone equipment including broadband radio links.

The balance was allocated for the following equipment items:

- Backbone support antennas
- LMR support equipment — antennas, combiners
- Dispatch center equipment
- Remote solar sites
- Site upgrades
- Site leases
- Environmental assessments
- Electrical upgrades
- New tower and equipment shelters
- Labor
- Remote site and antenna installs
- Base station and dispatch installs
- Airlift and mobilization
- Commissioning

an LMR device was quieting other two-way radio repeaters. All diagnostics led to a specific vendor. If true, that vendor's equipment would have been removed from the network with negative consequences for further deployment.

The controller's capability to simultaneously monitor traffic at multiple sites and at multiple network device interfaces involved testing the duplicate IP address hypothesis by monitoring traffic at the suspected offending devices. While this didn't exonerate the suspected devices, it pointed to an unexpected problem source — an Ethernet network interface card on a non-mobile radio power device at

another remote site. With the rogue card removed, the commissioning processes continued to an acceptable conclusion. Total time to track and verify the problem was an hour.

Because of the network's size and complexity, the overall commissioning strategy was to leverage the network's space ad-hoc architecture into a tool that would allow standing up networked sites as they became operational. Executing this strategy required five key events:

1. Verify that the intersite wireless link antennas were installed correctly and path statistics were verified and acceptable;
2. Install pre-staged network package and verify physical layer wireless link operations as required;
3. Conduct stress-traffic tests between local and remote nodes;
4. Verify network connectivity with non-LMR site elements; and
5. Verify connectivity among all P25 equipment.

A set of wireless controller-based embedded HTML administration, monitoring and provisioning tools allowed a radio technician to declare a node operational and externally networked. When network segments were physically completed, they were easily integrated into the total network and readied for mobile communications operational validation.

While the networking hardware often attracts the center of interest in designing networks, software validation tools are playing an increasingly key role in managing limited labor and time resources. Working with the CBP, the monitoring tool was tailored to meet three key needs not served by SNMP management tools:

1. A summary and in-depth look at the viability and overall traffic status of all P25 assets connected at

each backbone and telco T1 POP. This view provided an end-to-end view of a "nailed down" V.24 wireless circuit;

2. A summary and detailed look at the backhaul wireless radio status; and

3. The ability to remotely reconfigure and re-provision the network and network support assets such as V.24 power systems and sensor devices without risking the integrity of the system.

From the beginning, the Arizona CBP digital network upgrade featured several new concepts in logistics, mobile radio IP networking, and techniques of the administration and operations and maintenance (OAM) of large networks, including the following:

- Pre-staging and provisioning of each site;
- Mix-mode IP transport and packet switching of circuit- and packet-based P25 traffic;
- Using both new and existing legacy infrastructure media such as UHF and microwave;
- Analog and digital telco facilities; and
- Advancing techniques of remote diagnostics, remediation of faults and system provisioning.

As the CBP builds its digital secure network, lessons learned in the intense two-year effort have been transformed into a series of best practices to collectively benefit the two-way radio community and subsequent CBP deployments. ■

William M. Brown is president and founder of Metric Systems. He previously held positions with Motorola and Raytheon. This article was written with the assistance of U.S. Customs and Border Protection (CBP) technical staff. E-mail comments to editor@RRMediaGroup.com.