

SECURELY EXTENDING MOBILE BACKHAUL

An IP/MPLS Backhaul Network Provides Resilience & Enhanced Security Against Cyber Attacks

BY DAVID CHRISTOPHE



Cybersecurity threats and attacks on government systems are increasing in frequency. In these and other emergency situations, it's critical to ensure the availability of mission-critical land mobile radio (LMR) voice communications with minimal interruptions between first responders and dispatch. As public safety, utility and transportation agencies extend LMR backhaul networks to eliminate coverage gaps, and while they build capacity and an extended footprint for mobile broadband with LTE, they also possess an excellent opportunity to further enhance security. Of course, with today's tight budgets, any solutions must have a minimal impact on the overall cost.

Globally, agencies are deploying backhaul solutions based on IP/MPLS technology as their LMR network footprint expands, as well as to replace older backhaul equipment that lacks capacity or is no longer supported. This allows them to efficiently support new LMR systems and powerful IP-based applications, such as video surveillance on a single secure network.

with IP/MPLS riding on top. An IP/MPLS backhaul network also provides the required foundation for mobile broadband with LTE.

INCREASED SECURITY

Backhaul communications originate, transit and terminate in remote areas, as well as in close proximity to citizens, homes and businesses. This potentially offers cyber criminals entry points for hacking into an agency's communications network. As a result, an increasing focus on security is warranted for these increasingly more sophisticated threats. Figure 1 (below) identifies several facets to securing the flow of communications in backhaul. The capabilities inherent in IP/MPLS protocols and routers secure this critical information and provide a flexible, powerful platform for further enhancements.

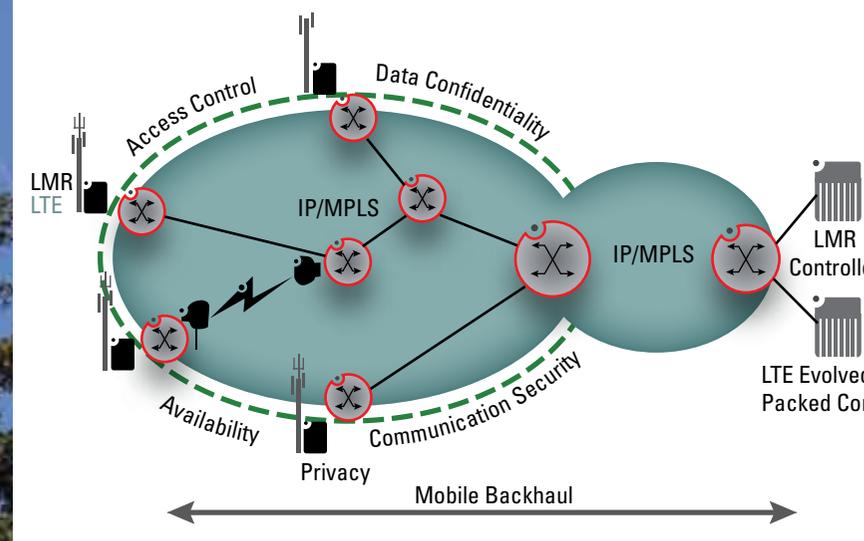
ACCESS CONTROL

Limiting physical equipment access to authorized personnel is a key element in securing backhaul communications. This may include placing equipment in locked enclosures and securing base station site perimeters with fencing. In remote areas, a motion-activated camera is deployed at a base station so that when physical security is compromised, the camera alerts an operations center and provides images of whatever activity is taking place at the site. Agencies can then initiate the appropriate, immediate response.

Limiting access to the IP/MPLS router and supported services is critical, and typically is handled with user IDs and passwords with defined spans of control. For example, a field technician may use an ID and password to access a base station router to initiate troubleshooting, but that person may only have the ability to view, not change, router system parameters. Strong technician/administrator system access security is provided with industry-standard Simple Network Management Protocol (SNMP) v3 confidentiality and integrity features and Secure Shell (SSH) encryption.

Within the IP/MPLS network, access control lists (ACLs) and filters are used to control access to specific users and host IP addresses. These prevent spoofing, denial-of-service (DOS)

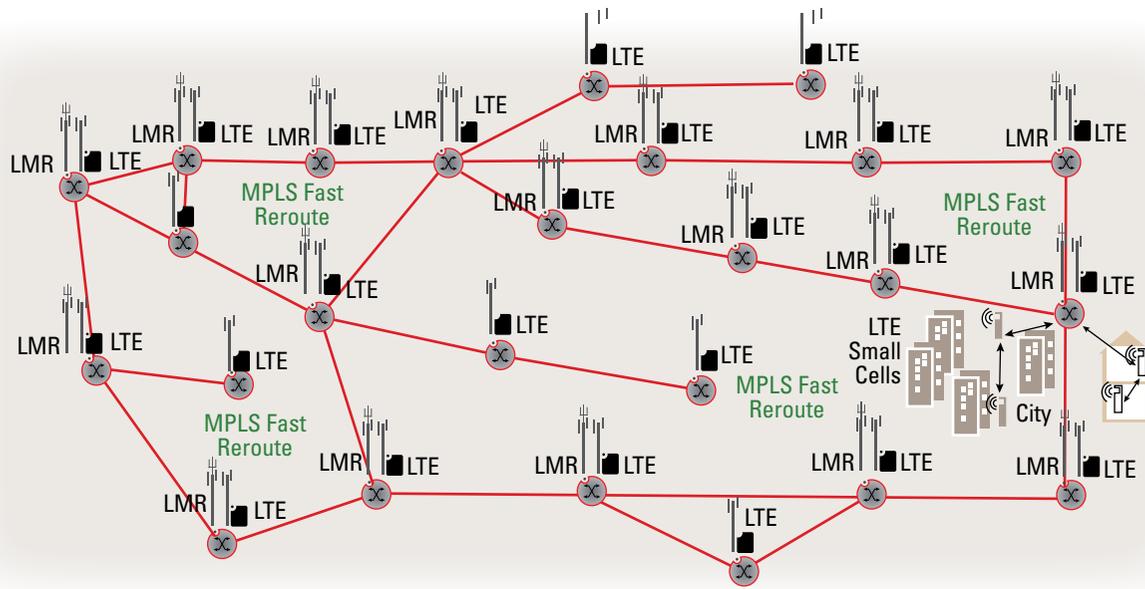
FIGURE 1 Securing the Communications Flow in Mobile Backhaul



Converging all of this new and existing traffic onto a single backhaul network increases flexibility, simplifies network management, enhances security and reduces costs without jeopardizing reliability. For base stations that lack fiber or copper access, agencies are deploying packet microwave radio for transport,

PHOTO: KEVIN LINK

FIGURE 2 Network Architecture & Use of MPLS Control & Failure Recovery Mechanisms for High Availability



attacks and other malicious acts.

Network access security can be further enhanced with the inclusion of a firewall that helps stop unexpected and unwanted traffic from entering the network through the router. This includes a set of rules to determine which traffic passes or is dropped or rejected in each direction, based on criteria such as source and destination address or port. To tightly control access, a specific rule set is assigned to a specific port, host group or protocol. *Example:* Traffic entering and exiting the port associated with the LMR base station can only go to, and originate from, the unique address associated with the controller. Other traffic is dropped or rejected.

DATA CONFIDENTIALITY

Encryption and authentication can further enhance traffic privacy and confidentiality in the backhaul network, inhibiting eavesdropping and tampering with user voice, video and data traffic in transit. Even a cyber criminal who gained network access would not have visibility of the user traffic.

Widely deployed Internet Protocol Security (IPsec) can be used for Layer 3 (IPv4 and IPv6) traffic in a point-to-point encryption solution. With this protocol, each packet in a communications session is authenticated and encrypted. When a session is initiated, the cryptographic

keys that will be used during the session are negotiated.

To inhibit the destabilization of synchronous services, 1588v2 packet authentication is deployed. For example, this might be used when 1588v2 is providing timing distribution for the backhaul network to minimize the chance of a cyber criminal destabilizing the synchronization and causing base stations to shutdown to avoid radio frequency interference.

Encryption also can be extended to additional types of traffic such as TDM (not just IP with IPsec), and router control plane communications. The latter inhibits a cyber criminal from gathering intelligence on the network topology and then, for example, changing routing adjacencies to disrupt or redirect backhaul traffic flows.

COMMUNICATION SECURITY

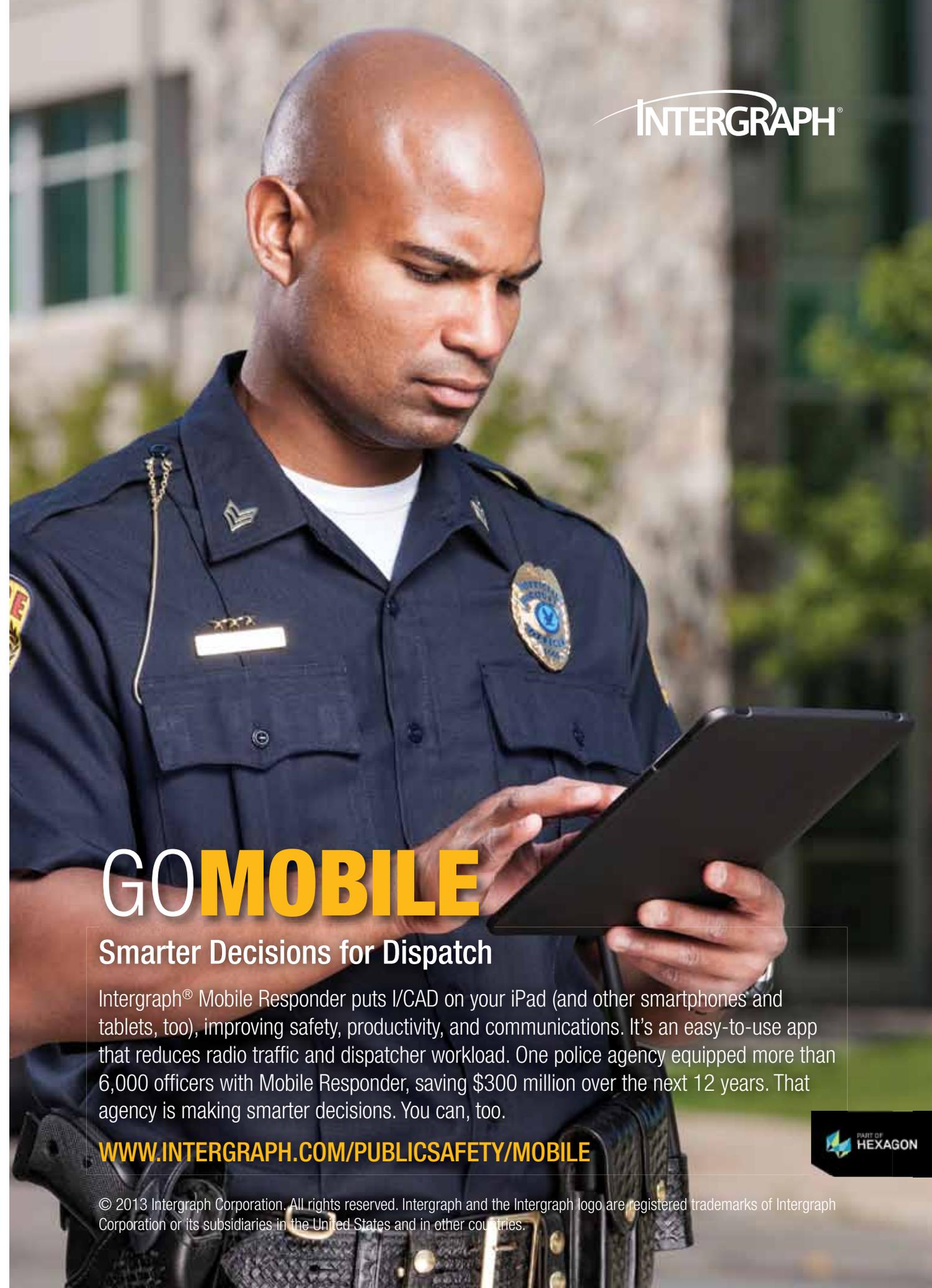
Virtual private networks (VPNs) isolate traffic, keeping it private and unaffected by other data streams. For example, one VPN is established for LMR user data traffic from a base station, and another for signaling traffic. Agencies can maintain communications security through the use of VPNs along with MPLS label swapping and its associated tables on routers, which ensure traffic only enters/exits the network at pre-identified points.

PRIVACY

To help ensure that the identification and use of devices on the network remains private, a network address translation (NAT) capability is added to an IP/MPLS network. This enables the device address on the network to remain hidden to outsiders while permitting access by authorized

FIGURE 3: Inherent IP/MPLS & Incremental Capabilities to Secure Communications

Access Control	Password, Span of Control, Secure Shell (SSH), Access Control Lists, Firewall
Data Confidentiality	Encryption
Communication Security	VPN, MPLS
Privacy	Network Address Translation, Encryption
Availability	Network Redundancy and Architecture, Intrusion Detection System, Intrusion Protection System



GO MOBILE

Smarter Decisions for Dispatch

Intergraph® Mobile Responder puts I/CAD on your iPad (and other smartphones and tablets, too), improving safety, productivity, and communications. It's an easy-to-use app that reduces radio traffic and dispatcher workload. One police agency equipped more than 6,000 officers with Mobile Responder, saving \$300 million over the next 12 years. That agency is making smarter decisions. You can, too.

WWW.INTERGRAPH.COM/PUBLICSAFETY/MOBILE

© 2013 Intergraph Corporation. All rights reserved. Intergraph and the Intergraph logo are registered trademarks of Intergraph Corporation or its subsidiaries in the United States and in other countries.



users. Encryption can be deployed in backhaul to further enhance privacy and data confidentiality.

AVAILABILITY

When economically feasible, backhaul can be architected for high resiliency through a network design that includes multiple paths to base stations and controllers. High network availability

is achieved using control and failure recovery mechanisms such as MPLS Fast Reroute, which switches traffic in less than 50 ms to an alternative path upon detection of a failure (Figure 2, page 42). Mission-critical backhaul traffic can be made resilient to a link failure during congested periods when IP/MPLS is combined with packet microwave radio equipped with

intelligent discard, utilizing multiple radio links.

An intrusion detection system (IDS) detects and reports anomalous activities and behaviors recognized as attack patterns. It's combined with intrusion protection system (IPS) capabilities that automatically contain attacks, further ensuring high availability throughout backhaul.

IDS detects activities that may make the network unavailable for its intended use—for example, denial-of-service (DOS)/distributed denial-of-service (DDOS), transmission control protocol reset (TCP RST) and TCP SYN (synchronize) attacks. It also detects the TCP/UDP port scan activities of cyber-criminals seeking an open port for network access, and provides valuable attacker identification.

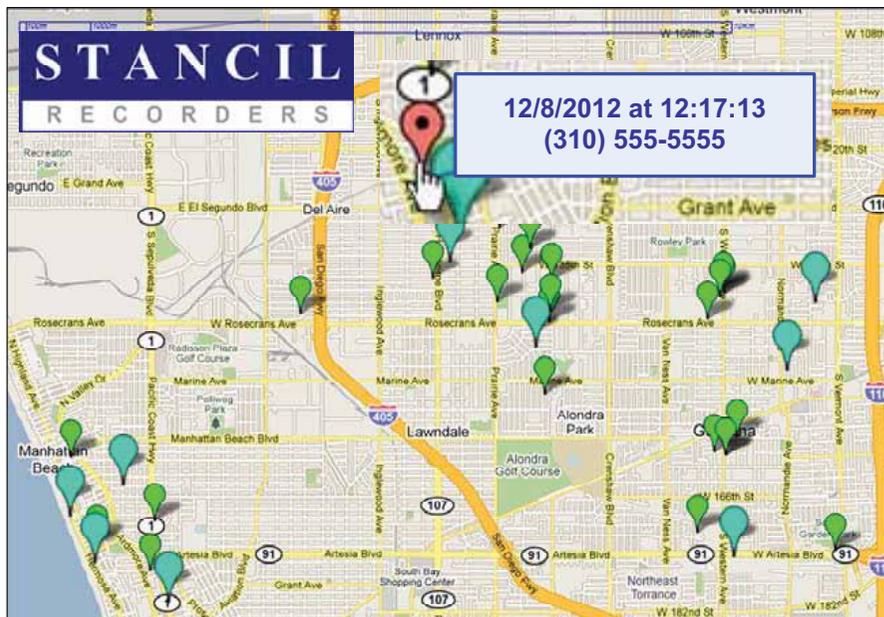
IPS provides automatic mitigation actions in response to a detected intrusion. This can include separately defined actions for a service, port or groups. For example, for the port associated with a base station, mission-critical backhaul traffic is placed on a white list to ensure that it gets through. Attacking traffic is blacklisted and excluded. Of course, during the attack mitigation mechanisms will need to maintain the high throughput of the mission-critical traffic with low latency through the firewall.

GOAL: RESILIENCE

The capabilities inherent in IP/MPLS routers are securing backhaul network communications. An opportune time to further enhance security capabilities is when extending a network's reach and adding capacity in preparation for mobile broadband with LTE. IP/MPLS router solutions that provide capabilities such as encryption, firewall, intrusion detection/protection and NAT, along with a resilient network architecture, will make backhaul more resilient to the growing frequency and sophistication of cyber security attacks.

||PSC||

DAVID CHRISTOPHE is a marketing director at Alcatel-Lucent. Send questions or comments to him at david.christophe@alcatel-lucent.com.



With Stancil You Also Know Where

**The SLR - Stancil Logging Recorder
Next Generation - NOW**

- ▶ P25 Validated
- ▶ NG9-1-1 Ready
- ▶ Web Access – Tablets
- ▶ Web Access – Smartphones
- ▶ Quality Scoring
- ▶ Multi Storage Capabilities
- ▶ Redaction
- ▶ GeoCentric Capture & Display
- ▶ VoIP
- ▶ RoIP
- ▶ SIPREC
- ▶ Video
- ▶ Text & Pictures
- ▶ Screen Capture
- ▶ 24x7 Support
- ▶ System Monitoring

Santa Ana, CA
www.stancilcorp.com
Bill Houser
Cell: (760) 519-0671
bill.houser@stancilcorp.com



Melbourne, FL
www.stancil.net
Mike Hanner
Direct: (888) 431-7950 Option 1
mhanner@stancil.net

Don't Settle.

Expect more. A lot more.

- Call Handling • VIPER® Call Handling Solutions • Power 911® Emergency Call Control • Power MIS® Advanced Call Reporting and Analysis • A9-1-1® Connect™ Purpose-Built Call Handling Appliance • Emergency Call Tracking System (ECaTS) • Call Control Interface • **NextGen GIS** • MapFlex™ 9-1-1 Geospatial Call Management • MapSAG® GIS Data Management System • Enterprise Geospatial Database Management System (EGDMS) • **Supplemental Data** • TXT29-1-1® • Beware™ Incident Intelligence • Smart911™ Personal Safety Profile • **Operational Continuity** • THOR Shield® Comprehensive Mobile Emergency Communications Program • HFConnect™ Emergency Communications of Last Resort

Visit booth #1217 at APCO to discover all we have to offer.

