WIRELESS NETWORK SOLUTIONS

PTP Security and Compliance

Safeguarding Your Wireless Communications

You're in the process of upgrading your communications capabilities to support several new high-bandwidth requirements, and wireless looks like an excellent option. As you review your criteria, security is still a major question to be answered. Will our wireless solutions give you the high level of security you need? We agree that security is absolutely crucial to protect wireless communications. Therefore, our Point-to-Point (PTP) Wireless Ethernet Bridges offer several robust security features* that are sure to put your mind at ease.

Protecting the Management Interface

PTP bridges support standard management protocols – HTTP, SNMPv1 and v2c, and TFTP over standard Transmission Control Protocol (TCP/IP) and User Datagram Protocol (UDP/IP) port interfaces. Certain PTP systems also support secure versions of these protocols, including:

- **HTTPS/TLS:** This secure version of HTTP has been implemented on certain PTP models to protect the systems' management interface. PTP bridges also support installation of user-provided X.509 digital certificates. HTTPS/TLS requires the purchase of an AES license key.
- **SNMPv3:** Simple Network Management Protocol (SNMP), version 3, adds security and remote configuration enhancements to SNMP. Several PTP systems support SNMPv3. In certain cases, a license key is required.
- **Identity and Event Management:** On several system models, identity-based user accounts with configurable password rules can be enabled to control user access to the radios. Up to ten local users may be permitted access to a PTP radio, and each user can be assigned a different level of access: security officer, system administrator and read only. In addition, Remote Authentication Dial In User Service (RADIUS) can be used to remotely authenticate users and their levels of access based on your network policies.
- **Auditing and Event Management:** Security and other events are logged locally and optionally can be sent to a centralized logging server using syslog. Examples of such messages include: successful and failed log-in events and changes to security configuration.

* Certain security features and compliance certifications may not be available on all PTP systems.

Protecting Over-the-Air Transmissions

Over-the-air communications can present potential risks for information confidentiality. We provide strong security measures for protecting data, voice and video as they travel through the air.

- **Proprietary Air Interface:** As PTP radios transmit data, the data is packed into airside packets, and an error correction code is applied. For systems with *intelligent* Orthogonal Frequency Division Multiplexing (*i*-OFDM), the data is also spread over many frequencies. While snooping and unscrambling is possible, an intruder would need a great deal of knowledge and resources to achieve that state.
- **AES Encryption:** As an added security layer, many PTP systems support implementation of FIPS 197 compliant, 128-bit and/or 256-bit Advanced Encryption Standard (AES) approved algorithms. On PTP 100 and 200 links, AES encryption is included as a feature on specified models. For PTP 300, 500, 600 and 800 links, AES encryption is a system option that requires the purchase of a license key.

Disaster Recovery

PTP radios have deployment-assistance features that help installers deploy radios quickly and easily. During emergencies or natural disasters, the following features offer enhanced recovery capabilities:

- **Save and Restore:** Many PTP models provide a "Save and Restore" feature that allows a system administrator to backup a radio's operating configuration file. Then the system administrator can restore the saved file if a unit must be reset or replaced. In the case of a faulty unit, the saved configuration file can be captured and uploaded to the new unit.
- **Link Name Access:** Where radios are deployed at great distances or in difficult to reach locations, Link Name Access is a way to speed up deployment of a new radio when the original device is damaged or lost. This feature allows you to establish a link between radios with identical Link Name attributes. If you need to replace a radio in the future, you can drop in the replacement device without having to alter the link name attributes on the remote radio.

Vulnerability Management

Using commercially available tools, we regularly scan our PTP solutions for vulnerabilities. After scanning, vulnerabilities that pose significant risk to customers are resolved.

Compliance Certifications

Various PTP systems have been or are in the process of being certified as compliant with the following regulatory standards:

- **FIPS 140-2:** Certain PTP systems support a FIPS 140-2 Level 2 mode which meets regulatory requirements for cryptographic algorithms, key security and tamper evidence. AES encryption is required with FIPS 140-2. This mode also requires the purchase of a license key. Certification status may be confirmed online at: http://csrc.nist.gov/groups/STM/cmvp/inprocess.html.
- **FIPS-197:** PTP systems that support AES encryption also support the Federal Information Processing Standard (FIPS) 197 standard. Published by the U.S. National Institute of Standards and Technology (NIST), FIPS-197 specifies the AES cryptographic algorithm that can be used to protect electronic data.

Summary

We have made and continue to make significant investments in security best practices. Through ongoing technological innovation, we strive to provide you with robust, multi-layered security for your PTP communications. Our mission is to proactively defend your wireless network from those who work to attack it.

Wireless Network Solutions

Motorola's portfolio of unrivaled wireless network solutions includes indoor WLAN, outdoor wireless mesh, point-to-multipoint, point-to-point networks and voice over WLAN systems, giving customers the agility and seamless connectivity they need to grow their business or better protect and serve the public. Combined with powerful software for wireless network design, security, management and troubleshooting, Motorola's solutions deliver trusted networking and anywhere access to organizations worldwide.

MOTOROLA

Motorola, Inc., 1303 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. • www.motorola.com/ptp