SOLUTION BRIEF

Information Assurance for Point-to-Point Wireless Ethernet Bridges

Multi-layered security to protect your wireless communications from malicious attacks

Contents

Executive Summary

Implementing, managing and evolving a multi-layer, enterprise-wide information security system is not an undertaking for the faint-hearted. It requires resolve, persistence and a healthy dose of paranoia. However, our global economy depends on having the right information, at the right time and at the right place; so the value of pursuing the bullet-proof security model cannot be over-stated.

Wireless communication plays a critical role in anytime, anywhere information access. However, wireless technology is often seen as a two-edged sword. On one hand is the ability to deliver information to workers and partners virtually anywhere on the globe. On the other hand, wireless communications present their own unique security challenges. As security technology, policies and procedures have evolved to mitigate risk and guard against malicious attacks on computer networks, that evolution has also given us excellent tools to protect the wireless communications that are being integrated into today's multi-service networks.

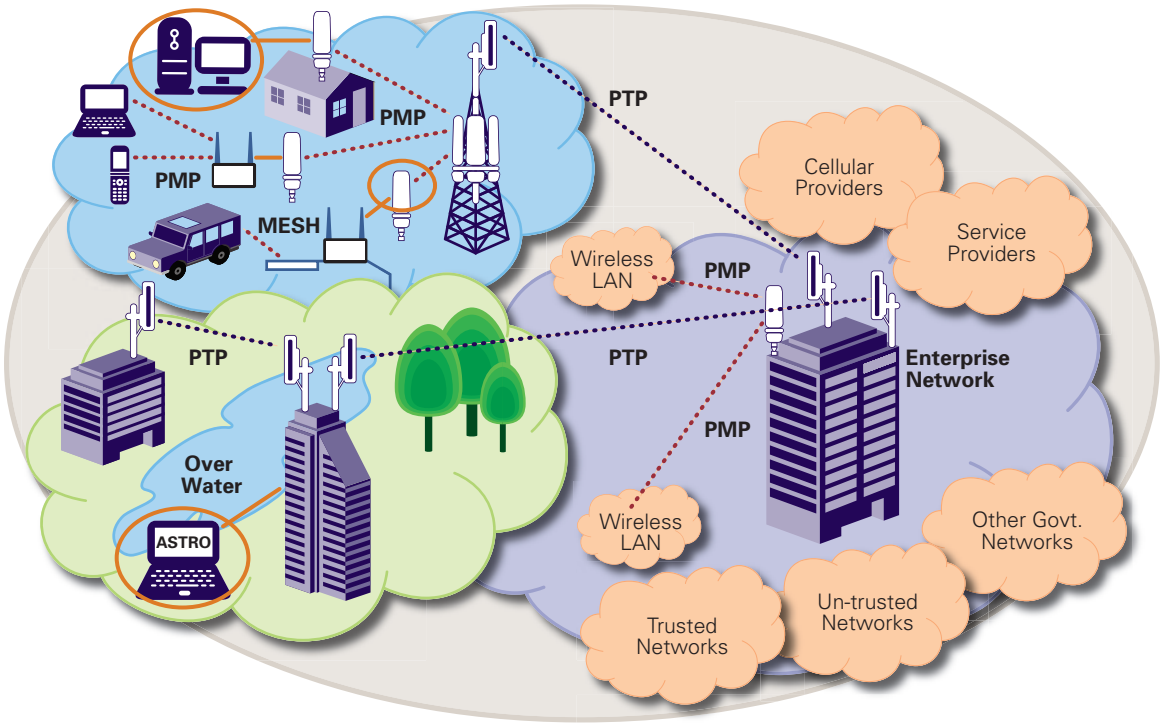

Figure 1
IP infrastructure with wireless point-to-point links for connectivity and backhaul as well as point-to-multipoint and mesh communications.

Enterprise networks for organizations such as:
- Businesses
- Federal agencies
- DoD and NATO agencies
- County and state governments
- Municipalities
- Schools and universities
- Healthcare providers
- Public safety agencies
- Transportation agencies
- Utility companies

Motorola has been addressing customers' communications requirements for more than 80 years and has an unwavering commitment to providing robust, state-of-the-art security capabilities for its wireless solutions. That commitment extends to Motorola's family of point-to-point wireless solutions. This paper explains the technological capabilities and recommended policies and procedures that are available to protect these point-to-point communication networks.

Introduction

The push for anytime, anywhere access to information has been the primary driving factor for the growth of wireless communications worldwide. The agility, convenience and cost-effectiveness that wireless connectivity offers are compelling arguments for implementing wireless technology. However, the perception that wireless communications are not secure has been a deterrent for wireless adoption in many organizations.

In reality, security technology, policies and processes can effectively protect wireless equipment and data transmissions from malicious attacks. While there is no computer network that is 100% secure, today's wireless networks can be equipped with robust, multi-layered security that provides safe and secure wireless network access anytime and anywhere.

As "anywhere" signifies, information access is not limited to inside the building. Today's users need access to information both from inside and outside the building. Whether a request for information comes from across the parking lot or across the state, the wireless communication travels over the air by radio waves. Motorola's point-to-point wireless connectivity solutions are designed to seamlessly integrate with Information Assurance (IA) policies, procedures and processes to:

- Secure over-the-air transmissions
- Protect the radios which send and receive data
- Guard against internal and external threats

Information Assurance

Information Assurance (IA) is closely linked to information security. In fact, the terms are often used interchangeably. However, IA encompasses a broader strategy for protecting information and information systems. While several organizations have contributed to the development and refinement of the "Five Pillars" IA model, all organizations define IA in basically the same manner:

Information Assurance protects and defends information and information systems by ensuring ***availability, integrity, authentication, confidentiality and non-repudiation***. In addition, IA incorporates detection, prevention and response capabilities to provide for the restoration of damaged or compromised information systems.

Each attribute plays an important role in executing the IA model:

- **Availability:** Timely and reliable access to data and information services for authorized users
- **Integrity:** Protection against unauthorized modification or destruction of information as well as the physical and electronic systems
- **Authentication:** A means of identifying users (e.g., passwords, fingerprints, PINs) as recognized individuals who have authorized access to network and system elements
- **Confidentiality:** Assurance that information is not disclosed to unauthorized individuals, processes or devices
- **Non-Repudiation:** Proof of sender's and recipient's identities so that neither party can later deny having been part of the transaction

Simply put, IA is a set of policies, procedures and processes that safeguard data moving on the network, data processed by applications and data residing on any type of digital storage medium. Ultimately, to safeguard digital information in all of its various states, IA also has to protect the IP network and any related IT infrastructure.

Although IA is typically very data-centric, it is not confined to computer systems and is not limited to information in electronic or machine-readable forms. IA applies to all important information and data within the enterprise, in whatever form it exists. For example, giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

By protecting information, devices and IT operations, IA uniquely supports secure wireless communications that are potentially highly interoperable with partner organizations and other relevant entities such as government agencies, accounting firms, insurance companies, financial institutions and contractors.

Introduction continued

To safeguard information production, transport and storage within a wireless infrastructure, an IA program employs a number of policies, processes and procedures that guide an organization's security management efforts and many related areas of IT operations. These programs are effective to the degree that they enable convergence and integration of several key disciplines, including:

- Regulatory and policy compliance
- IT and network security
- Physical security
- Business continuity and disaster recovery
- Identity and access management
- IT life cycle and project management
- Intelligence gathering and analysis

When deployed as a strategic function, IA becomes an important cross-functional platform for the unification of various governance, policy and operational capabilities that might otherwise be fragmented and isolated.

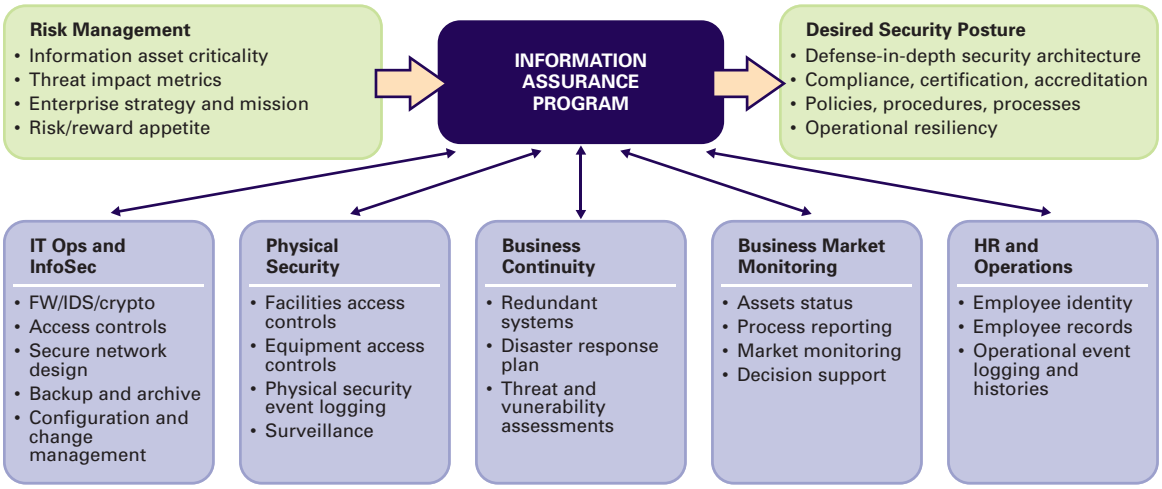

Figure 2
IA decision-making process and related enterprise impact

BlueCross BlueShield Chattanooga, TN Feb. 12, 2010	57 hard drives were stolen from a leased facility for BlueCross BlueShield. The drives contained data including protected health information of customers of its health plan. The insurer sent out 220,133 notifications to tier 3 customers indicating that their personal information was included on the stolen drives. This information included name, address, BlueCross member ID number, diagnosis, Social Security number and date of birth. **Records containing sensitive personal information involved in security breaches in the U.S. since January 2005: 350,387,036** (as of this paper's publication) Source: Privacy Rights Clearinghouse (www.privacyrights.org)

Motorola's Information Assurance Initiative

Motorola is fully committed to the ongoing implementation, management and enhancement of IA best practices for all its wireless solutions, including the PTP family of products. The Company's IA strategy is based on a comprehensive approach which emphasizes the importance and value of establishing a defense-in-depth program that encompasses people, policies, processes and technology.

The mission is to deliver state-of-the-art, system-wide solutions that assure availability, integrity, authentication, confidentiality and non-repudiation by implementing hardware, software and services that prevent, detect and respond to potential and real threats.

The table below lists Motorola's key IA discipline areas across the global organization covering three key functional areas of security control:

- Technology: Safeguards and countermeasures that are primarily implemented and executed by the information system through mechanisms contained in the system hardware, software or firmware
- Operational: Safeguards and countermeasures that are primarily implemented and executed by people
- Management: Risk management and the management of information system security

MOTOROLA'S KEY IA DISCIPLINE AREAS		
Area	**Discipline**	**Addressing Such Topics As:**
Technology	Network	Network topology and architecture, transport equipment hardening, network services, approved ports and protocols, network boundary protection and wireless security
	Platform	Commercial OS hardening and configuration, common middleware, desktop applications and host-based protections
	Database	Database hardening and configuration, secure mechanisms to achieve database availability, data confidentiality and integrity, identity and access control, auditing and event management
	Application	Secure coding standards, identity and access control, web-enabled applications, proxies, auditing and event management, and host-based protections
	Cryptography	Approved algorithms, key management including PKI and appropriate usage of cryptography
	Identity and Access Management	Identification, authentication, authorization, entitlements, account and access management, and approved mechanisms
	Vulnerability Management	Vulnerability scanning, patching, security alerts and advisories
	Auditing and Event Management	Incident response and points of contact, remediation, forensics and documentation, reporting and alert reporting
	Disaster Recovery	Backup, restore, time to recover, time to return to operation and point of recovery
Operational	Incident Response	Incident response process, points of contact, remediation, forensics and documentation
	Change Control	Definition of controlled environments, tracking of change requests, approvals, implementation, testing and acceptance
	Asset and Configuration Management	Asset inventory, secure baseline configuration, monitoring, access control and change control
	Training and Awareness	Training and skills, awareness training for general population, customer focused training
	Operational Support Lifecycle	Lifecycle management security issues such as remote service access, remote system monitoring, field upgrades, system staging and provisioning, and debugging tools
	Product Development Lifecycle	Lifecycle management security issues such as permit-to-build, architecture review boards, secure development lifecycle, separation of development, testing and production systems, secure development environments and security testing
	Information Classification and Handling	Definition and protection of sensitive data with references to organizational policy, identification of linkages to the product development and operational support lifecycles

MOTOROLA'S KEY IA DISCIPLINE AREAS		
Area	**Discipline**	**Addressing Such Topics As:**
Management	Third-Party Vendor Management	Service and support agreements, hardware and software sourcing and development, legal ramifications, engagement through supplier selection, acceptance, lifecycle management, underpinning contracts, vulnerability identification, disclosure and remediation
	Compliance and Risk Management	Risk assessments, risk rankings, risk treatment and management, compliance monitoring and independent security assessments
	Roadmaps	Linkage to customer voice, review frequency, synchronization identification with appropriate regulatory requirements, plan for adoption of disciplines and initiatives across the global organization
	Policies and Standards	Risk ownership, authoritative guidance and common solutions

These security capabilities are components within Motorola's overall Information Assurance strategy. This strategy comprises more than a series of technical controls, providing a comprehensive approach to information assurance that extends to the people, policies, and processes that touch the wireless network.

PTP Security and Compliance

Motorola has made a significant investment in security technologies, compliance testing and certification procedures to provide its customers with robust, reliable and cost-effective security programs for its Wireless Network Solutions. The following information describes the risks, security features and compliance procedures that specifically relate to PTP systems. Within Motorola's defined IA discipline areas, the applicable IA disciplines for PTP systems are:

- Network
- Cryptography
- Identity and event management
- Vulnerability management
- Audit and event management
- Disaster recovery

Non-technical (Operational and Management) disciplines and the Application discipline within Motorola's IA strategy are not covered in this paper.

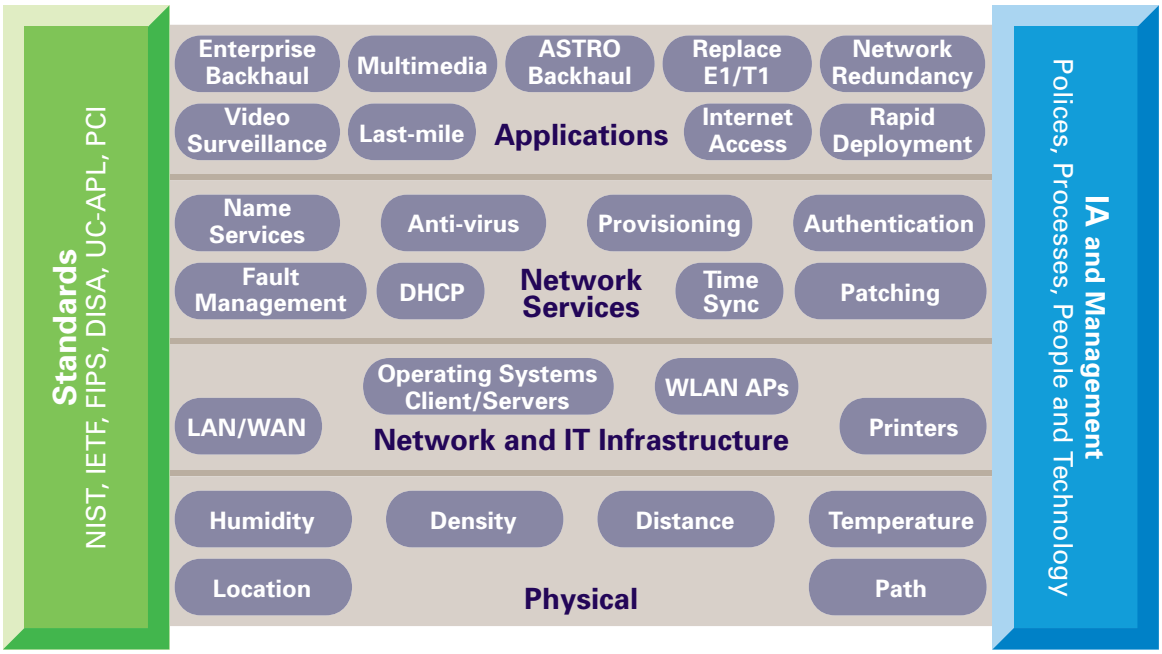

Figure 3
Defense-in-depth security architecture

The defense-in-depth security model is a series of interconnected layers of security in which Information Assurance policies and controls are applied at all levels of the technology stack

Potential Threats in Point-to-Point Deployments

Today's attackers are looking for vulnerabilities everywhere in the IT infrastructure, including:

- Attacks on physical facilities and equipment
- Eavesdropping, masquerading and denial of service at the network level
- Corruption and control of applications and operating systems
- Violation of the confidentiality, integrity and availability of user data

Analyzing the risks presented by connecting to and sharing information with internal teams, external partners and related business entities is a critical step when deploying a defense-in-depth wireless security program. By analyzing the risks, you can pinpoint the areas of vulnerability and implement the appropriate countermeasures.

With PTP wireless connectivity, over-the-air transmissions and "man-in-the-middle" attacks represent the greatest threats to information confidentiality. Connecting wireless outdoor devices to the computer network and managing the wireless network also present potential risks. In addition, most organizations have to cope with both internal and external threats, with the greatest internal threats coming from employees who access the Internet for job-related activities and/or break-time surfing activities.

IA Disciplines Specific to PTP Systems

While all PTP systems are engineered to be inherently secure, Motorola has enhanced these systems with several robust security features and compliance certifications to protect wireless communications and meet regulatory requirements.

PTP IA Discipline Areas: While each PTP security feature is categorized by its IA discipline area, the combination of these security features working together addresses all five IA attributes.

- **Network**
  All PTP bridges support standard management protocols: HTTP, SNMPv1 and v2c, and TFTP. PTP bridges utilize these protocols over standard Transmission Control Protocol (TCP/IP) and User Datagram Protocol (UDP/IP) port interfaces. Several PTP products support the following secure versions of these protocols:

  > **HTTPS/TLS (IA Authentication, Confidentiality and Non-Repudiation)**
  Transport Layer Security (TLS) is a cryptographic protocol that provides security and data integrity for communications over TCP/IP networks such as the Internet. It is an Internet Engineering Task Force (IETF) standard track protocol which was last updated in RFC[1] 5246. Several versions of the protocols are in wide-spread use in applications like Web browsing, electronic mail, Internet faxing, instant messaging and voice-over-IP (VoIP).

  In PTP bridges, TLS encrypts segments of the Transport Layer protocols in use for an end-to-end connection. Hypertext Transfer Protocol Secure (HTTPS) is a combination of HTTP and TLS. Motorola has implemented HTTPS/TLS on certain PTP bridges and uses it to protect the management interface on those devices. HTTPS/TLS requires the purchase of an AES license key.

  PTP bridges support installation of user-provided X.509 digital certificates, allowing the operator to install the certificates they currently use. In addition, PTP systems support strong cyber-suite algorithms as approved by NIST (National Institute of Standards and Technology) pursuant to FIPS 140-2, Level 2.

  > **SNMPv3 (IA Authentication and Confidentiality)**
  Simple Network Management Protocol (SNMP)v3 is defined by RFC 3411-RFC 3418. SNMPv3 adds security and remote configuration enhancements to SNMP and is the current SNMP standard as of 2004. The IETF has designated SNMPv3 as a full Internet Standard, the highest maturity level for an RFC memorandum. In addition to the SNMPv1 and v2 protocols, SNMPv3 support is provided on several PTP bridges. In certain cases, a license key is required.

- **Cryptography – 128/256-Bit AES Encryption (IA Confidentiality)**
  In the "no encryption" mode, data security for PTP systems is provided by the mechanisms used to transmit data over the RF band. To transmit data over a radio spectrum, the data is packed into airside packets and an error correction code is applied. In the case of PTP systems with *intelligent* Orthogonal Frequency Division Multiplexing (*i*-OFDM), the data is also interleaved (spread) over many frequencies. These airside packets do not align with the payload packets. While snooping and unscrambling is possible, it would require that the attacker obtain a great deal of knowledge and resources to achieve that state.

  To provide an added layer of security, many PTP systems support implementation of Federal Information Processing Standard (FIPS) 197 compliant 128-bit and 256-bit Advanced Encryption Standard (AES) approved algorithms. AES is a block cipher adopted as an encryption standard by the U.S. Government. It has been analyzed extensively and is now used worldwide. Today, AES is one of the most popular algorithms used in symmetric key cryptography and is available in many different encryption packages. It is the first publicly accessible and open cipher approved by the U.S. National Security Agency (NSA) for top secret information. For FIPS 140-2 compliance, AES encryption must be enabled. (See the Compliance Certifications section.)

  On PTP 100 and 200 links, AES encryption is included as a feature in specified models. For PTP 300, 500, 600 and 800 links, AES encryption is a PTP system option which can be enabled by purchasing and applying an upgrade license key to the radio units. AES link encryption can be configured using the PTP Security Wizard which uses a "key of keys" approach to encrypt all defined IA discipline areas. A FIPS-approved key generator is used to create a key of keys. PTP license keys with 128-bit AES encryption require a 128-bit key of keys. Similarly, license keys with 256-bit AES require a 256-bit key of keys. Once a key of keys is generated, erasing it will render PTP IA disciplines inaccessible.

- **Identity and Event Management (IA Authentication)**

[1] In computer network engineering, a Request for Comments (RFC) is a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.

Identity-based user accounts can be enabled to control user access to PTP radios in accordance with security policies. Several models can be configured with the following user account options:

> Best practice passwords
> Auto logout period
> Maximum number of login attempts
> Login attempt lockout period
> Password expiration period
> Minimum password change period

Up to ten users may be permitted access to a PTP radio, and each user can be configured with different levels of access. Defined access levels are security officer, system administrator and read only. Every time a user attempts to login to the wireless unit, a user security banner is generated and displayed.

License keys must be obtained and enabled for most PTP encryption, throughput and capacity upgrades. Because those license keys are tied to each device's Media Access Control (MAC) address as a unique identifier, entitlements cannot be stolen. For FIPS 140-2 compliance, identity-based user accounts must be enabled. (See the Compliance Certifications section.)

- **Vulnerability Management (IA Availability and Integrity)**
  Using commercially-available tools, Motorola regularly scans its PTP solutions for vulnerabilities. After scanning, vulnerabilities are evaluated. Those vulnerabilities that pose significant risk to the customer are resolved.

- **Auditing and Event Management (IA Availability and Integrity)**
  When abnormal conditions are detected, a number of diagnostic messages can be sent via SNMP to an operator or a network management system such as Motorola's Wireless Manager. Some examples of these messages are:
  - Disabled wireless or fiber link
  - Disabled data port
  - Change in wireless or fiber link status
  - Change in TDD status

- **Disaster Recovery (IA Availability and Integrity)**
  The "Save and Restore" feature on PTP bridges allows the system administrator to backup the operating configuration of the wireless unit. The system administrator should back up the operating configuration immediately after a successful PTP installation or prior to any software upgrade. Then the administrator can restore the unit's configuration by simply restoring the saved configuration file. The backup configuration file can also be used when swapping out a faulty wireless unit by capturing the saved configuration file from the faulty unit and uploading it to the new unit. When the system administrator restores a configuration, the system will validate the integrity of the configuration file and alert you to any changes to the file.

  Obtaining a Group Access license key is a way to speed up deployment of a new unit when a device is damaged or lost. In classically-deployed links, each PTP link requires that the Master and Slave radios are pre-matched via software configuration. By obtaining and applying a Group Access license key, you can associate any Slave radio in a defined group to any Master radio in the group without pre-matching the radios. As a result, a new radio can be installed and be operational very quickly.

  Group Access capability is recommended where radios are deployed at great distances or in difficult to reach locations such as a snowy mountaintop or on a building which is located on the opposite side of a large body of water. In such instances, the time it would take to reach the opposite end of a link or the extreme site conditions can make on-site configuration difficult or even impossible. For difficult-to-service radio sites, obtaining a Group Access license key can make replacing damaged or lost units much faster and easier, often significantly reducing installation man-hours.

Motorola's Wireless Manager
Flexibility is one of the hallmarks of Motorola's wireless solutions, especially when it comes to managing the wireless network. Network operators can easily integrate with an existing third-party network management system; manage the wireless network remotely via the Internet and a Web browser; and/or use Wireless Manager, Release 2.2 or higher as the wireless network management system.

Wireless Manager (WM) helps organizations manage their wireless networks for maximum reliability and uptime. With WM, Point-to-Point, Point-to-Multipoint and Mesh sites as well as any other SNMP-enabled devices can be monitored and managed from one live Google™ map-based view. Real-time polled network performance metrics and alarms shown on a unified map enable faster and more efficient issue response.

When paired with Motorola's PTP solutions, WM adds these capabilities to PTP bridges:

- **Status Monitoring:** WM uses an SNMP status ping to determine if PTP devices in the WM inventory are still responsive and reachable via the network. Failed status checks result in a major alarm, which is prominently displayed. An alarm can alert you to failed, destroyed and/or stolen hardware, including problems such as denial-of-service attacks that make a device effectively offline.
- **Configuration Monitoring:** WM checks the configuration of each PTP device on a regular basis, and compares that configuration to the expected settings. If a discrepancy is detected – due to unauthorized tampering with the device, as an example – the system administrator is notified so that investigative and corrective action can be taken.
- **Access Control:** WM users can be limited in the scope of their WM activities, including limits on the devices they can view and manage as well as limits on the features they can use (e.g., read-only inventory listings versus writing configuration settings). Password access provides further control.
- **Audit Trail:** WM records the configuration actions of its own users, so that a history is maintained of what users changed the settings on each PTP device and when the changes were made. In the event of a problem with settings on a device, the system administrator can determine which user is responsible and assess the reasoning behind the changed configuration.

Compliance Certifications
Various PTP bridges have been or are in the process of being tested by the appropriate regulatory agencies to certify compliance to the following regulatory standards:

- **FIPS 140-2**
  The Federal Information Processing Standard (FIPS) 140 is a series of publications numbered 140 which are U.S. Government computer security standards that specify requirements for cryptography modules. The current version of the standard is FIPS 140-2 which was issued on May 25, 2001, and updated as of December, 2006.

  Motorola offers a FIPS 140-2 Level 2 mode for certain PTP solutions. This mode meets regulatory requirements for cryptographic algorithms, key security and tamper evidence. All PTP links equipped with FIPS 140-2 must also have 128-bit or 256-bit AES encryption. Together, the AES encryption and FIPS 140-2 protection provide robust security to protect IP communications from malicious incidents.

- **UC-APL**
  Currently, Motorola is pursuing DoD UC-APL compliance for certain PTP systems. The U.S. Department of Defense (DoD) United Capabilities Approved Product List (UC-APL) was established to maintain a single consolidated list of products that have completed Interoperability (IO) and Information Assurance (IA) testing and certification. DoD organizations are required to fulfill their system needs by purchasing only APL-listed products, providing one of the listed products meets their needs. This means the APL must be consulted prior to purchasing a system or product.

  With testing conducted by the Joint Interoperability Test Command (JITC), UC compliance is validated to ensure interoperability between DoD command and services systems that will be deployed together both in peacetime and war. During the testing and certification process, IA capabilities are validated against the Defense Information Systems Agency (DISA) Security Technology Implementation Guide (STIG) and IO against Unified Capabilities Requirements (UCR) 2008.

DISA defines interoperability as:
"the ability to provide and accept data, information, material and services…includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange, as required for mission accomplishment."

Summary

Motorola has made a significant investment in developing security features, policies and processes to reassure customers that its PTP solutions are secure. That commitment to best practices and technological innovation is an ongoing effort designed to detect, prevent and respond to potential threats. The Company continually expands and enhances security capabilities and compliance certifications to aggressively defend customers' wireless networks from those who are continually working to attack them.

The following table provides a snap-shot view of the PTP security features and certifications that are in operation today or are in the process of development and/or certification.

PTP SECURITY FEATURES and COMPLIANCE CERTIFICATIONS							
Security Features	**PTP 100**	**PTP 200**	**PTP 250**	**PTP 300/500**	**PTP 600**	**PTP 800**	**Wireless Manager**
DES 56-bit	●	●	—	—	—	—	—
AES 128-bit[2]	●	●	●	●	●	●	Future Release
AES 256-bit[2]	—	—	—	●	●	●	Future Release
SNMPv3[3]	Future Release	Future Release	●	Release 04-00	●	Future Release	●
HTTPS/TLS	Future Release	Future Release	Future Release	Under Evaluation	●	Future Release	Under Evaluation
Identity-based User Accounts	Future Release	Future Release	Future Release	Under Evaluation	●	Under Evaluation	●
Vulnerability Scanning	●	●	Planned	●	●	●	●
Diagnostic Alarms	●	●	●	●	●	●	●
Disaster Recovery	●	●	●	●	●	●	●
Link Name Security	—	—	—	—	Future Release	●	—
Compliance Certifications	**PTP 100**	**PTP 200**	**PTP 250**	**PTP 300/500**	**PTP 600**	**PTP 800**	**Wireless Manager**
FIPS 140-2 Compliance[4]	—	—	—	Under Evaluation	●	Under Evaluation	Under Evaluation
FIPS 197 Compliance	●	●	Future Release	●	●	●	Future Release
UC-APL Compliance[5]	—	—	—	Under Evaluation	Future Release	Under Evaluation	Under Evaluation
To comply with current export restrictions, a Point-to-Point AES or FIPS license key is required to access all high-grade cryptographic algorithms.							

[2] For PTP 300/500, 600 and 800 systems, AES encryption is an optional feature which can be enabled by purchasing a license key. On PTP 100 and 200 systems, AES is included in specified models. The AES encryption product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

[3] SNMPv3 is available on AES-enabled radios.

[4] FIPS 140-2 Level 2 mode is an optional feature which is compatible with new and existing systems, although some hardware restrictions may apply. Confirm FIPS 140-2 certification status online at: http://csrc.nist.gov/groups/STM/cmvp/inprocess.html

[5] Confirm UC-APL certification status online at: http://jitc.fhu.disa.mil/apl/dsn.html

About Motorola

As a global communications leader, Motorola has been at the forefront of communication inventions and innovations for more than 80 years. Our communication solutions allow people, businesses and governments to be more connected and more mobile. We hold a market-leading position in WiMAX deployments around the world and are at the forefront on 4G telecommunications. Plus, our unique combination of innovative PTP technologies has earned Motorola the market leadership position in the global unlicensed Ethernet market.

Wireless Network Solutions

Motorola delivers seamless connectivity that puts real-time information in the hands of users, giving customers the agility they need to grow their business or better protect and serve the public. Working seamlessly together with its world-class devices, Motorola's unrivalled wireless network solutions include indoor WLAN, outdoor wireless mesh, point-to-multipoint, point-to-point networks and voice over WLAN solutions. Combined with powerful software for wireless network design, security, management and troubleshooting, Motorola's solutions deliver trusted networking and anywhere access to organizations across the globe.

Figure 4
PTP Product Family

MOTOROLA

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