www.defenseelectronicsmag.com

Defense Electronics

A Special Section to **Penton's Design Engineering & Sourcing Group**

ELECTRONICALLY REPRINTED FROM FEBRUARY/MARCH 2013

BACKHAUL SOLUTIONS Earn DoD APPROVAL

ROB MILLER, DIRECTOR OF FEDERAL MARKETS
Cambium Networks, 3800 Golf Rd., Ste. 360, Rolling Meadows, IL 60008
+ 1 (813) 505-5481 email: rob.miller@cambiumnetworks.com
www.cambiumnetworks.com.

Backhaul Solutions Earn DoD's JITC Approval

Cambium Networks' Point-to-Point (PTP) 600 Series Solutions Are Interoperability and Information Assurance Tested and Certified by the DoD's UCCO.

Microwave backhaul systems such as the PTP 600 series of wireless Ethernet bridges from Cambium Networks Ltd. (www.cambiumnetworks.com) are invaluable for both licensed and unlicensed links. Designed for licensed use in the 2.5-, 4.5-, and 4.9-GHz bands (with license holders such as NATO) and unlicensed use in the 5.4-, 5.8, and 5.9-GHz bands, these point-to-point (P2P) systems support data rates to 300 Mb/s at distances to 124 miles.

2. At higher frequencies the PTP 800 Outdoor Radio Unit, Indoor RF unit, and compact modem work to provide secure backhaul communications.

Of particular significance to secure communications, the PTP series of links are especially well suited for Department of Defense (DoD) applications; they have gone through a two-year development and testing program, met and exceeded Unified Capabilities Certification Office (UCCO) certification, and earned a place on the official DoD Unified Capabilities Approved Products List (UC APL). In fact, the PTP 600 system is the first and only UC-APL-certified microwave backhaul solution for use by the DoD. It provides reliable communications for any number of government and law-enforcement agencies requiring the reassurance of a secure solution.

1. PTP 600 Integrated and Connectorized Outdoor Radio Units.

PTP 600 Series radios (**Fig. 1**) are wireless Ethernet bridges encased in ruggedized, commercial-grade metal housings. Their primary purpose is to provide secure Internet Protocol (IP) data, voice, and video communications, even in non-line-of-sight (NLOS) environments, over water and desert terrain, and in extreme weather conditions.

Because Cambium Networks (formerly a division of Motorola Solutions) had deployed thousands of radios throughout the DoD since 2004, PTP 600 radios had become the predominant backhaul choice for DoD and numerous federal agencies. In addition to good NLOS performance in the 4- and 5-GHz bands, these backhaul systems feature small, simple form factors, high system gain of 167 to 199 dB, and orthogonal-frequency-division-multiplex (OFDM) capability with 1024 subcarriers. They are wind tested to 202 mph for durability and have received IP 66/67 certification. In addition, PTP 600 Series radios have a built-in spectrum analyzer with dynamic spectrum optimization to ensure reliable radio performance.

The DoD's UC APL is established in accordance with the UC's requirements document, UCR 2008, Change 3, which is available at the agency's website (www.disa.mil/ucco/). The purpose of the UC APL is to establish a single list of products that have Interoperability (IO) and Information Assurance (IA) certification. The DoD's UC APL helps to simplify the design and maintenance of DoD network infrastructure equipment. The UC APL is the only listing of equipment by the DoD to be fielded in DoD networks.

DoD network systems must be supported by purchasing APL products, pro-

Table 1: FIPS 140-2 security-level specifications.

Cambium PTP 600 security-level compliance	
Security requirements section	**FIPS 140-2 Level**
Cryptographic module specification	3
Module ports and interfaces	2
Roles, services, and authentication	3
Finite state model	2
Physical security	2
Operational environment	NA
Cryptographic key management	2
EMI/EMC	2
Self-tests	2
Design assurance	3
Mitigation of other attacks	NA

3. Anti-tamper labels are strategically located on a PTP 600 ODU with connectors.

vided that a product on the list meets the system's requirements. This means the APL must be consulted prior to purchasing a system or product.

The UCCO serves as the staff element for the NS2 Capabilities Center to manage acquisition of products from the UC APL. The UCC provides process guidance, coordination, information, and support to vendors and government sponsors throughout the entire process, from the registration phase to the attainment of DoD UC APL status. The UCCO also manages the APL End of Life (EOL) List (available on www.disa.mil/services), which consists of products that have been removed from the DoD's UC APL. As NS2 moves towards a distributed testing environment, the UCCO will be the primary point of contact (POC) for scheduling and coordination of partnering Testing Centers of Excellence locations.

Products to be considered for UC APL certification require sponsorship by a DoD program. The UC APL certification also requires that the products receive Federal Information Processing Standards (FIPS) 140-2 Level 2 regulatory requirements for cryptographic algorithms. DoD organizations and many Federal agencies require FIPS 140-2 validation to secure sensitive data, voice, and video communications. Because PTP 600 systems are deployed by so many DoD groups, the Installation Information Infrastructure Modernization Program (I3MP) sponsored the PTP 600 and confirmed that it was worthy of APL consideration.

With I3MP's sponsorship, Cambium began multi-faceted testing efforts in 2009 and completed the process in 2011. Tests for all UC APL requirements were performed in Cambium's core development center, which is equipped and staffed for RF/microwave testing as well as network, intrusion, and vulnerability testing. FIPS 140 testing and validation was completed first, involving cryptographic algorithm evaluation via the National Institute for Standards and Technology (NIST) Cryptographic Algorithm Validation Program (CMVP), independent source code inspection by a NIST-certified test house, and extensive cryptographic self tests. **Table 1** shows the compliance levels validated during the FIPS 140 testing process.

After receiving I3MP sponsorship and FIPS 140-2 validation for the PTP 600, Cambium received the Security Technical Implementation Guides (STIGs) which formed the DoD's Joint Interoperability Test Command (JITC) test specifications for UC APL certification. Thousands of STIG requirements had to be analyzed, tested, and certified as compliant with the DoD's strict IA and IO specifications.

Table 2: FIPS 140-2 validated security standards for the PTP 600.

FIPS 140-2 validated security standards for the PTP 600			
Security standard	**Requirement**	**Operational environment**	**Validation description**
Secure hash standard (SHS)	SHA hashing functions conform to the secure hash algorithms as specified in FIPS 180-3	T1 C6414 DSP	Validation No. 1101
Digital signature algorithm (DSA)	DSA conforms to the digital signature algorithm as specified in FIPS 186-2 and FIPS 186-3	T1 C6414 DSP	Validation No. 399
Advanced encryption standard (AES) algorithm	AES conforms to the AES algorithm as specified in FIPS 197	VRTX 2	Validation No. 708 – wireless link encryption (Firmware) CFB128 (e only; 128, 192, 256)
		T1 C6414 DSP	Validation No. 1144 –TLS/ SNMP payload encryption (Firmware) ECB (e/d; 128, 192, 256) CBC (e/d; 128, 192, 256) CTR (ext only; 128, 192, 256
Keyed-hash message authentication code (HMAC)	Conforms to HMAC as specified in FIPS Publication 198	T1 C6414 DSP	Validation No. 700 (Firmware) HMAC-SHA1 (Key Sizes Ranges Tested: KS = BS) SHS Validation No.1101
Deterministic random bit generator (DRBG) Algorithm	Conforms to DRBG algorithm as specified in Special Publication 800-90, recommendation for random number generation using deterministic random bit generators	T1 C6414 DSP	Validation No. 21 (Firmware) CTR_DRBG: Prediction Resistance Tested: Not Enabled BlockCipher_Use_df: AES-128 AES Validation No.1144
Triple data encryption algorithm (DES)	Conforms to triple DES algorithm as specified in FIPS Publication 46-3, data encryption standard	T1 C6414 DSP	Validation No. 863 (Firmware) TCBC (e/d; KO 1,2) TCBCI (e/d; KO 1,2)

By being validated to FIPS 140-2 Security Level 2 specifications,[1] operators are assured of the security of their information. Security Level 1 is the minimum requirement for UC APL certification. It requires that at least one Approved security function must be implemented in an Approved mode of operation but does not provide protection of Critical Security Parameters (CSPs) used or generated by the module. Level 1 allows the software components of a cryptographic module to be executed on a general-purpose computing system using an unevaluated operating system. No specific physical security mechanisms are required. FIPS 140-2 Security Level 2 enhances the physical security mechanisms of a Level 1 cryptographic module by adding the requirement for tamper evidence, including the use of tamper-evident coatings or seals, or for pick-resistant locks on removable module covers or doors. Tamper-evident coatings or seals are placed on a cryptographic module so that the coating or seal must be broken to attain physical access to the CSPs within the module.

Level 2 also requires role-based authentication in which a cryptographic module authenticates and verifies the authorization of an operator to assume a specific role and to perform a corresponding set of services. This protects against unauthorized execution, modification, and reading of cryptographic software.

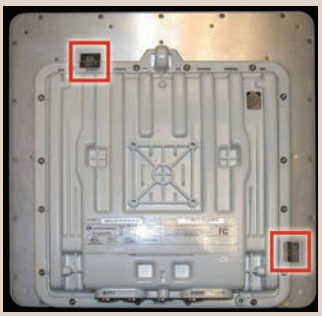
Achieving FIPS 140-2 also requires testing and gaining approval for six key algorithms. Each algorithm must be subjected to thousands of cryptographic tests on the target platform. Test results for the PTP 600 system were submitted to InfoGard/NIST for validation, with details for those approved algorithms for the PTP 600 system shown in **Table 2.** In addition to the PTP 600 systems, Cambium's higher-frequency Ethernet-based PTP 800 Wireless Licensed Microwave solutions **(Fig. 2)** are also FIPS 140-2 validated.[2] The PTP 800 systems operate in frequency bands from 6 to 38 GHz, for applications where licensed exclusivity is desired, can be deployed with full confidence that sensitive communications will be secure.

For additional protection, the PTP 600 systems meet key security validation requirements. The key-of-keys is stored as a 128/256-b Advanced Encryption Standard (AES) key and is read during the initialization procedure. The key of keys can be configured or erased only by a user with the security officer role.

The systems must also meet rigorous requirements for exposing any evidence of tampering. The cryptographic boundary of each wireless unit is the PTP 600's external casing. There are two product variants that have different casing arrangements. The integrated unit has an integrated RF antenna. A model with connectors is identical to the integrated version, except that the antenna is replaced by a metal plate with two N-type RF connectors for an external antenna.

Anti-tamper labels are installed on the metal cases to allow the modules to operate in a FIPS-approved mode of operation. Tamper-evident labels must go through rigorous testing at a NIST-approved lab before being declared fit for DoD purposes. Each PTP 600 radio is delivered with anti-tamper labels applied. A PTP 600 module with connectors **(Fig. 3)** has two labels wrapping around the enclosures edge, with one label on the top (horizontal) and one label on the left side (vertical). A PTP 600 integrated module has two labels on the underside of the enclosure **(Fig. 4)**, with the top label (horizontal) and the side label (vertical).

Security Technical Implementation Guides (STIGs)[3] provide configuration standards for DoD IA and IA-enabled devices or systems. The guides contain technical guidance to secure information systems and software that might otherwise be vulnerable to malicious computer attack. In the first phase of meeting the STIG requirements, Cambium was required to provide specific responses to all STIG requirements. This procedure entailed in-house testing of STIG requirements to determine what, if any, PTP 600 enhancements would be needed to obtain UC APL certification. Based on the in-house analysis, Cambium added several software features, including the use of a secure network time protocol (NTP) to prevent an attacker from modifying a PTP 600's perception of time; and Remote Authentication Dial-In User Service (RADIUS), to remotely authenticate users and their levels of access based on an organization's network policies; and control user accounts via configurable password rules.



4. This PTP 600 Integrated ODU shows the location of its anti-tamper labels.

After the required enhancements were made, STIG testing was conducted by the DoD's JITC (www.jitc.fhu.disa.mil/) with a Cambium engineer on premises at the JITC lab. The process involved two weeks of IA testing which included extensive network intrusion, penetration, and vulnerability scanning. Another week of Ethernet, T1, and VoIP network testing was conducted to comply with interoperability requirements.

Following the two-year testing, development, and certification process, the PTP 600 Series backhaul solutions received UC APL certification, allowing all DoD agencies to purchase and operate UC-certified systems over a DoD network. The listing can be confirmed at https://aplits.disa.mil/processAPList.do/. The certification is especially crucial for the thousands of strategic and tactical communications vital to DoD and Federal agencies worldwide, including for battlefield communications; training and simulation networks; backhaul from telemetry and land mobile radios (LMRs); border patrol; sensor and security backhaul; ship-to-ship and ship-to-shore communications; satellite local-area-network (LAN) extensions; LTE and WiMAX backhaul; law enforcement; and test range communications. In addition to UC APL certification, PTP 600 radios have also passed MIL-STD 461 testing for electromagnetic interference, qualifying them for use on US Navy ships. **DE**

References

1. FIPS 140-2 validation can be confirmed at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1515.
2. FIPS 140-2 certification status can be confirmed at http://csrc.nist.gov/groups/STM/cmvp/inprocess.html.
3. More information on STIGs is available at http://iase.disa.mil/stigs/index.html.

Cambium Networks™