Lucent Technologies
Bell Labs Innovations

Access Point 600

FIPS 140-1 Non-Proprietary Security Policy

Level 2 Validation

February 25, 2002

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Access Point 600 from Lucent Technologies. This security policy describes how the Access Point 600 meets the security requirements of FIPS 140-1 and how to operate the Access Point 600 in a secure FIPS 140-1 mode. This policy was prepared as part of the Level 2 FIPS 140-1 validation of the Access Point 600.

FIPS 140-1 (Federal Information Processing Standards Publication 140-1 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-1 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

1.2 References

This document deals only with operations and capabilities of the Access Point 600 in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the Access Point 600 and the entire Access Point series from the following sources:

- The Lucent Technologies website (www.lucent.com) contains information on the full line of products from Lucent Technologies.

- The NIST Validated Modules website (http://csrc.ncsl.nist.gov/cryptval/): contains contact information for answers to technical or sales-related questions for the Access Point 600

1.3 Document Organization

The Security Policy document is one document in complete FIPS 140-1 Submission Package. In addition to this document, the complete Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Module Software Listing
- Other supporting documentation as additional references

This document provides an overview of the Access Point 600 and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the Access Point 600. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

This Security Policy and other Certification Submission Documentation was produced by Corsec Security, Inc. under contract to Lucent Technologies. With the exception of this Non-Proprietary Security Policy, the FIPS 140-1 Certification Submission Documentation is proprietary to Lucent

Technologies and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Lucent Technologies.

2 Access Point 600

The Access Point 600 is a next-generation, high performance IP services router optimized for service providers wishing to quickly introduce high-demand managed IP services at their enterprise customer premises locations. The Access Point 600 is purpose-built to deliver new revenue-generating IP services with multi-access routing, Quality of Service (QoS) with Class-Based Queuing (CBQ), secure Virtual Private Networks (VPN), firewall security, and policy management. The service provider has the advantages of easy deployment to multi-size customer premise locations and the implementation of flexible management facilities that can be both customer and/or service provider managed.

Users can migrate from basic IP access to more advanced VPN and Service Level Agreement (SLA) managed IP services with a single, purpose-built IP services platform. The integrated traffic measurement and monitoring capabilities allow service level monitoring, enhanced network planning, and billing support. As a fully Simple Network Management Protocol (SNMP) managed system, Access Point 600 is targeted to support small to medium size regional and branch offices while easily integrating into existing network management systems and back-office services. And service providers can quickly deploy new revenue-generating IP services at minimum expenditures, without disrupting or reengineering existing service provider core network infrastructure.

2.1 Cryptographic Modules

The case of the Access Point 600 is the cryptographic boundary. All functionality discussed in this document is contained within the cryptographic boundary. No components of the module are excluded from FIPS 140-1 requirements.

2.2 Module Interfaces

The physical interfaces include a power plug and power switch. Various network interfaces are available (see Table 1 below) for the Access Point 600 to help customize the module to meet specific needs. Each network interface option is a FIPS 140-1 physical interface, and each is classified as a *data input interface* and *data output interface*. Network interfaces do not affect the cryptographic processing of the module, nor are they privy to any security parameters contained in the module's cryptographic software. Each network interface module listed below was tested for FIPS 140-1 compliance; therefore, and card or combination of cards may be used in a FIPS mode of operation.

Part Number	Label	Description
AP-PMC-01	10/100 Enet	10/100 Mbps Ethernet
AP-SP-PMC-01	10/100 Enet	10/100 Mbps Ethernet
AP-PMC-03	ATM DS3	ATM DS3
AP-SP-PMC-03	ATM DS3	ATM DS3
AP-PMC-04	ATM OC-3 MMF	ATM OC-3 multimode fiber
AP-SP-PMC-04	ATM OC-3 MMF	ATM OC-3 multimode fiber
AP-PMC-07	ATM OC-3 SMF-LR	ATM OC-3 single-mode fiber — long range
AP-SP-PMC-07	ATM OC-3 SMF-LR	ATM OC-3 single-mode fiber — long range
AP-PMC-05	ATM OC-3 SMF-IR	ATM OC-3 single-mode fiber — intermediate range

Part Number	Label	Description
AP-SP-PMC-05	ATM OC-3 SMF-IR	ATM OC-3 single-mode fiber — intermediate range
AP-PMC-0D	DS3	Frame-based DS3
AP-SP-PMC-0D	DS3	Frame-based DS3
AP-PMC-02	HSSI	High Speed Synchronous Interface
AP-SP-PMC-02	HSSI	High Speed Synchronous Interface
AP-PMC-0S	ISDN S/T	Integrated Services Digital Network S/T Interface
AP-SP-PMC-0S	ISDN S/T	Integrated Services Digital Network S/T Interface
AP-PMC-0U	ISDN U	Integrated Services Digital Network U Interface
AP-SP-PMC-0U	ISDN U	Integrated Services Digital Network U Interface
AP-PMC-08	MSSI	Medium Speed Synchronous Interface
AP-SP-PMC-08	MSSI	Medium Speed Synchronous Interface
AP-PMC-06	QUAD T1/E1	Quad T1/E1 with integrated CSU/DSU's
AP-SP-PMC-06	QUAD T1/E1	Quad T1/E1 with integrated CSU/DSU's

Table 1 – Network Interfaces

The module's status interfaces are located on the front and rear panels. These LEDs provide overall status of the module's operation. Descriptions for these LEDs are in Table 2 and Table 3, respectively.

LED	Indication	Description
Power	Green	On-board power is within tolerance
Alert	Amber	Operator attention required
Error	Red	System Fault
Fan OK	Green	All fans working properly
Fan Fail	Amber	One or more fans failed
Over Temp	Red	System is over its temperature threshold and as been reset
PMC Status	Green	Operational interface module is in the associated slot
	Amber	Interface module in the associated slot has failed
	None	No interface module detected in associated slot

Table 2 – Front Panel LEDs

The following table provides detailed information about the LEDs found on the back panel:

LED	Indication	Description
PWR	Green	On-board power is within tolerance
ALERT	Amber	Operator attention required
ERROR	Red	System Fault
FANOK	Green	All fans working properly
FAN FAIL	Amber	One or more fans failed
OVER TEMP	Red	System is over its temperature threshold and as been reset
LNK	Green	An Ethernet link is established
ACT	Amber	Slot 1 port is transmitting/receiving data
10/100	Amber	Slot 1 is transmitting data at 100 Mbps
	None	Slot 1 is transmitting data at 10 Mbps

Table 3 – Rear Panel LEDs

The module's physical interfaces are separated into the FIPS 140-1 logical interfaces as described in the following table:

AP600 Physical Interface	FIPS 140-1 Logical Interface
LAN/WAN Interfaces* Console Port Auxiliary Port**	Data Input Interface
LAN/WAN Interfaces* Console Port Auxiliary Port**	Data Output Interface
Power Switch Reset Switch Console Port Auxiliary Port**	Control Input Interface
LAN/WAN Interfaces* LEDs Console Port Auxiliary Port**	Status Output Interface
Power Plug	Power Interface

Table 4 – FIPS 140-1 Logical Interfaces

* See Table 1 – Network Interfaces
** The auxiliary port will be disabled in FIPS mode (see Section 3 of this document).

2.3 Roles and Services

The Access Point 600 supports role-based authentication and has two roles available: the Crypto Officer role and the User role. The services for each respective role are detailed below.

2.3.1 Crypto Officer Services

The Crypto Officer is responsible for the following services:

- Manage the module
  - Set up Telnet
  - Configure SNMP
  - Configure operator authentication
- Configure the module:
  - Define IP address
  - Enable/disable interfaces
  - Enable/disable network services
  - Display the configuration
  - Zeroize keys
- Set encrypt/bypass parameters
  - Set keys and algorithms to be used
  - Configure certain IPs to allow plaintext packets
  - Encrypt and decrypt packets based on configuration file settings
- Reset and power-off the module

2.3.2 User Services

The User is responsible for the following services:

- Initiating diagnostic network services
  - Ping
  - Traceroute
- Displaying full status of the module
- Manage system events
  - Display the module log table
  - Set and display filtering options

Basic FIPS operations such as encrypt and decrypt are performed dynamically by the module. The Crypto Officer configures the module and sets encryption/bypass parameters. The module itself will check incoming/outgoing packets against the configuration file to determine whether packets are encrypted or decrypted.

Roles are authenticated by username and password, and an operator connects to the Access Point 600 through a secure telnet session or via the console port with a terminal (or terminal emulation software). See Section 3 of this document for more details.

2.4 Physical Security

The router is entirely encased by a thick steel chassis. Once the Access Point 600 has been configured to meet FIPS 140-1 Level 2 requirements (see Section 3 of this document), tamper-evidence labels need to be placed to ensure that the module's case will indicate tampering. The tamper-evidence labels should be placed as follows:

1. Clean the case of any grease, dirt, or oil before applying the tamper-evidence labels (alcohol-based cleaning pads are recommended).
2. Place one label over the back network interface panel and the top cover as shown in Figure 1
3. Place one label over the back network interface panel and the bottom cover as shown in Figure 1
4. Place one label over the back power panel and the top cover as shown in Figure 1
5. Place one label over the back power panel and the bottom cover as shown in Figure 1
6. Place one label over the Aux port as shown in Figure 1
7. Place one label over the top cover and the front panel as shown in Figure 3

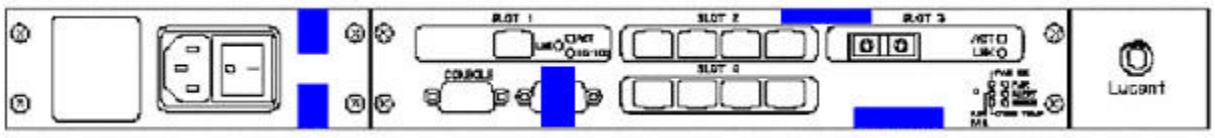

Figure 1 – Tamper-evidence label placement on back panel

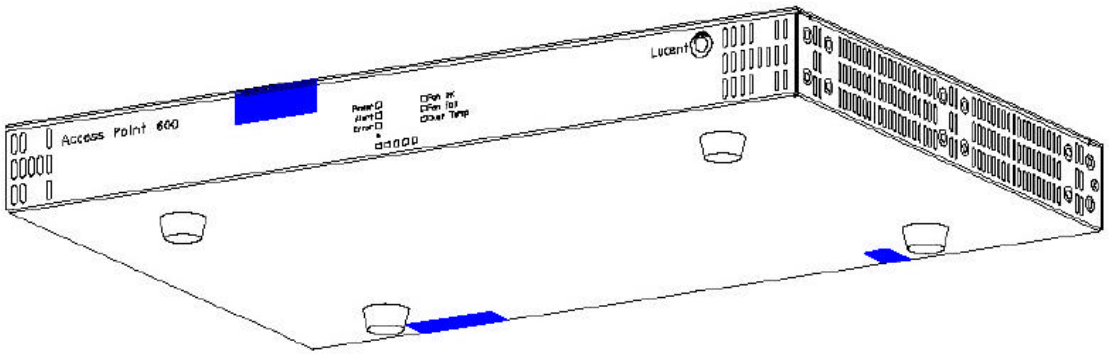

Figure 2 – Tamper-evidence label placement on front panel/bottom

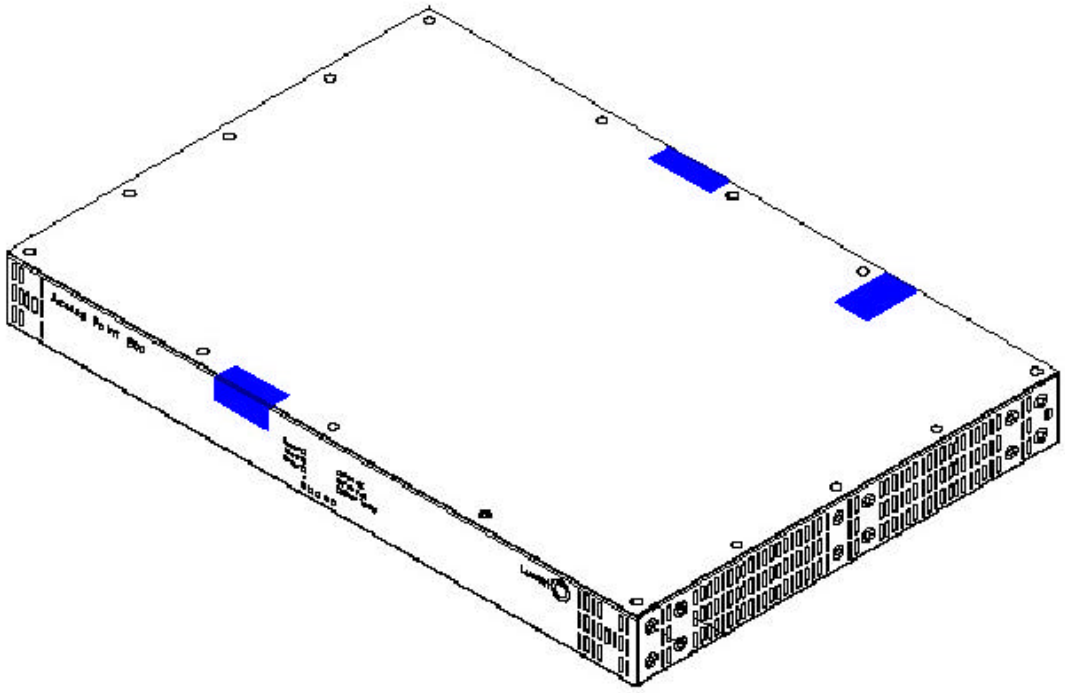

Figure 3 – Tamper-evidence label placement on front panel/top

The placement of the labels should be consistent with the instructions and the images above. The tamper evidence seals have a special adhesive backing to adhere to the module's painted surface.

Removing the power panel, network interface panel, bottom cover or top cover will damage the tamper evidence seals. Tamper evidence labels can be inspected for signs of tampering, which include the following: curled corners, bubbling, and rips. The word "Opened" may appear on the label if it was peeled away from the surface of the module. The tamper evidence labels have individual, unique serial numbers, and the labels may be inspected periodically and compared against the applied serial numbers to verify that the fresh labels have not been applied to a tampered module.

2.5 Cryptographic Key Management

The router securely administers cryptographic keys and other critical security parameters (e.g., passwords). The tamper-evidence seals provide physical protection for all keys. Keys are also password protected and can be zeroized by the Crypto Officer. Keys are exchanged and entered manually via manual key exchange or Internet Key Exchange (IKE). The Access Point 600 provides DES and 3DES IPSec encryption as well as SHA-1 hashing and DSA key generation, and RSA signatures. Specifically, the module supports the following keys:

- Pre-shared keys to perform IKE
- Signing keys to perform IKE
- Public keys to perform IKE
- SA keys negotiated to perform IPSEC

2.6 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The module has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules. Thus, the module meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for Business use (Class A). The module is labeled in accordance with FCC requirements with the appropriate FCC warnings.

2.7 Self-Tests

The Access Point 600 runs self-tests during startup and periodically during operations. The self-tests run at power-up include cryptographic known answer tests (KAT) on the FIPS-approved cryptographic algorithms (DES, 3DES) and on the message digest algorithm (SHA-1), as well as pairwise consistency tests run on DSA and RSA. The module also runs a software integrity test using a CRC-32 at startup. If the module is in FIPS-mode, then the bootstrap verifies that the CRC-32 of the compressed OS image is correct before booting from flash. If the image is valid, the OS is uncompressed and boots. Otherwise, the OS load is aborted.

A bypass mode test performed conditionally prior to executing IPSec. Whenever the Access Point Operating System writes to the Configuration File, a CRC-32 is calculated only for the area in NVRAM that is being used for the configuration data. This value is stored in the file header for the configuration file in NVRAM. Whenever the Configuration File is read from NVRAM to place data into RAM, the CRC-32 is calculated and then compared with the CRC-32 stored in the file header. The read continues if the values match; otherwise, the file is presumed to be corrupted and it is cleared.

The module also supports a manual key entry test for all key entries. The operator is required to enter the command line for key entry twice (the "up-arrow" command to re-enter the previous

CLI entry is disabled in FIPS mode). If the two commands and their respective keys do not match, the operator must try to enter the key again.

The module also supports the following conditional tests: a pairwise consistency test on all public and private key pairs and a test on the output of the random number generator. Whenever a public and private key pair is generated, the module will test this key pair to ensure proper calculation and verification of a digital signature. A continuous random number generator test is also performed on the output of the ANSI X9.17 pseudo-random number generator to ensure that output does not match a previous output value.

3 Secure Operation of the Access Point 600

3.1 Initial Setup

The Crypto Officer must apply tamper-evidence labels as described in Section 2.4 - Physical Security.

The Crypto Officer must securely store tamper evidence labels before use. After applying the tamper-evidence labels, the Crypto Officer must securely store any unused labels.

3.2 System Initialization and Configuration

The Access Point 600 is validated with version 2.6 of the OS image. No other image may be used with the Access Point 600.

The FIPS 140-1 validation does not include the optional hardware encryption acceleration card. Installing and using this card will violate FIPS 140-1 compliance.

The Crypto Officer must enter the following command to put the Access Point 600 in FIPS mode: **config system fips fips-mode enabled**.

The Crypto Officer must change the default username/password from "admin/*no password*" to a password that is at least 8 characters.

3.3 FIPS Approved Algorithms

The module supports the following FIPS approved algorithms:

- DES
- 3DES
- SHA-1
- RSA
- DSA

3.4 Non-FIPS Approved Algorithms

The following algorithms are implemented in the module but cannot be used in FIPS-mode of operation:

- MD-5
- SSL
- HMAC MD-5
- HMAC SHA-1
- Diffie-Hellman (may be used in FIPS mode of operation)

3.5 Protocols

The following protocols and network services must not be configured for FIPS mode of operation:

- CHAP
- PAP
- RADIUS

SNMPv3 over a secure IPSec tunnel may be employed for authenticated, secure SNMP *gets* and *sets*.

3.6 Remote Access

Auxiliary terminal services must be disabled. Use of the Auxiliary port is not allowed in FIPS mode.

Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto Officer must configure the module so that any remote connections via telnet are secured through IPSec.

The operator is not allowed to configure the module via the web interface. Use of the web interface for configuration is not allowed in FIPS mode.