Lucent Technologies
Bell Labs Innovations

Access Point 300

FIPS 140-1 Non-Proprietary Security Policy

Level 1 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 300 from Lucent Technologies. This security policy describes how the Access Point 300 meets the security requirements of FIPS 140-1 and how to operate the Access Point 300 in a secure FIPS 140-1 mode. This policy was prepared as part of the Level 1 FIPS 140-1 validation of the Access Point 300.

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 300 in the technical terms of a FIPS 140-1 cryptographic module security policy. More information is available on the Access Point 300 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 300

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 300 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 300. 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 300

The Access Point 300 is a next-generation, high performance IP Services router optimized for service providers wishing to quickly introduce high demand managed IP services at small to medium-sized enterprise customer premises locations. The Access Point 300 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 premises 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 solutions 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 300 is easily integrated into existing management systems and back-office services.

Service providers can quickly deploy new revenue-generating IP services at minimum expenditures, without disrupting or reengineering existing service provider core network infrastructure. All five Access Point 300 configurations employ an advanced system architecture that achieves high-speed packet forwarding while applying advanced services at very fine granularity. With data forwarding rates of up to 50 Mbps and 3DES encrypted traffic forwarding rates of up to 5 Mbps, Access Point 300 sets new price and performance standards for small and medium-sized branch office IP services routers.

The Access Point 300 is part of a family of IP services routers that are all built-to-purpose to deliver IP services. Supported WAN interface modules and protocols, routing performance, and applications capabilities differentiate the models IP services characteristics. The family also includes Access Point QVPN Builder, a software management product for deployment and management of revenue-generating, IP VPN and QoS services.

2.1 Cryptographic Modules

The case of the Access Point 300 is the cryptographic boundary. All functionality discussed in this document is contained within the cryptographic boundary, and no components of the module are excluded from FIPS 140-1 requirements. The module meets overall requirements for Level 1; it meets Level 2 requirements in every section except Physical Security.

2.2 Module Interfaces

The physical interfaces include a power plug and power switch. The Access Point 300 has a variety of network interface configurations available, as the following table shows:

Product Number	Configuration
AP-300-ST	2 10/100 Ethernet, ISDN BRI S/T
AP-300-M-ST	2 10/100 Ethernet, MSSI, ISDN BRI S/T
AP-300-2M-ST	2 10/100 Ethernet, 2 MSSI, ISDN BRI S/T
AP-300-M-U	2 10/100 Ethernet, MSSI, ISDN BRI U

Product Number	Configuration
AP-300-2T1E1-ST	2 10/100 Ethernet, 2 T1/E1, ISDN BRI S/T
AP-300-2T1E1-U	2 10/100 Ethernet, 2 T1/E1, ISDN BRI U

Table 1 – Access Point 300 Product Numbers and Descriptions

Various network interfaces are available (see Table 2 – Network Interfaces below) for the Access Point 300 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 are simply external interfaces, similar to the 10/100BaseT LAN ports. 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 model listed in Table 1 – Access Point 300 Product Numbers and Descriptions was tested for FIPS 140-1 compliance.

Label	Description
1 or 2 x MSSI (up to 8 Mbps) (V.35 or X.21)	High speed serial interface
2 x T1/E1 with integrated DSU/CSUs	T1/E1 interface
1 x ISDN BRI S/T	ISDN BRI with S/T interface
1 x ISDN BRU U	ISDN BRI with U interface

Table 2 – Network Interfaces

The module's status interface LEDs are located on the front panel and provide overall status of the module's operation. Each model has different LEDs, and descriptions for the cumulative LEDs are in the following tables:

LED	Indication	Description
Power	Green	On-board power is within tolerance
Alert	Amber	Operator attention required
Error	Red	System Fault

Table 3 – SYS LEDs

LED	Indication	Description
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 4 – LAN LEDs

LED	Indication	Description
L1	Green	The associated link is operational
	Red	A cable is not found or an error exists on the system
L2	Amber	The port is in loopback

Table 5 – MSSI LEDs

LED	Indication	Description
Lnk	Green	The link is up
	Amber	The link is active
	Red	The system is not receiving a signal from the remote end
Alm	Yellow	Problem with the remote end

Table 6 – T1/E1 LEDs

Indication			Description
S1	**S2**	**S4**	
Lit	Dark	Dark	Inactive
Dark	Lit	Dark	Sensing
Lit	Lit	Dark	Deactivated
Dark	Dark	Lit	Awaiting signal
Lit	Dark	Lit	Identifying input
Dark	Lit	Lit	Synchronized
Lit	Lit	Lit	Activated
Dark	Dark	Dark	Lost synchronization

Table 7 – ISDN S/T LEDs

LED	Indication	Description
ACT	Dark	The U interface is inactive if the other LEDs indicate Deactivated
	Fast Blinking	The U interface is not synchronized
	Slow Blinking	The U interface is synchronized, but the internal S/T bus is not synchronized
	Solid	All interfaces are fully synchronized if the other LEDs are solid yellow or solid green

Table 8 – ISDN U LED

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

AP300 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 9 – FIPS 140-1 Logical Interfaces

* See Table 1 – Access Point 300 Product Numbers and Descriptions and Table 2 – 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 300 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 300 through a secure telnet session or via the console port with a terminal (or terminal emulation software). See Section 3 - Secure Operation of the Access Point 300 for more details.

2.4 Physical Security

The module meets all Level 1 FIPS 140-1 requirements for physical security, providing a multiple-chip stand-alone cryptographic module with production grade equipment, industry standard passivation, and a strong molded plastic cover.

2.5 Cryptographic Key Management

The router securely administers cryptographic keys and other critical security parameters (e.g., passwords). 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 300 provides DES and 3DES IPSec encryption as well as SHA-1 hashing, 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 300 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), 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 300

3.1 System Initialization and Configuration

The Access Point 300 is validated with version 2.6 of the OS image. No other image may be used with the Access Point 300.

The Crypto Officer must enter the following command to put the Access Point 300 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.

3.2 FIPS Approved Algorithms

The module supports the following FIPS approved algorithms:

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

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

3.4 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*.

3.5 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.