National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Aruba Mobility Controller and Access Point Series

Report Number: CCEVS-VR-VID10348-2011
Dated: 27 June 2011
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

James Donndelinger

The Aerospace Corporation
Columbia, MD

Ralph Broom

Noblis, Inc.
Falls Church, VA

Common Criteria Testing Laboratory

SAIC
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the Aruba Mobility Controller and Access Point Series product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in May 2011. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The SAIC evaluation team determined that the product is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 4 augmented with ALC_FLR.2. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The TOE is a Wireless Local Area Network (WLAN) access system comprising Aruba Mobility Controllers, Access Points, and the ArubaOS. The Aruba Mobility Controller (MC) appliances are wireless switches that provide a wide range of wireless and wired network mobility services, security, centralized management, auditing, authentication, and remote access. The Aruba Access Point (AP) appliances service wireless clients (part of the operational environment) and can monitor radio frequency spectrums to detect intrusions, denial of service (DoS) attacks, and other vulnerabilities. The ArubaOS is a suite of mobility applications that runs on all Aruba MCs and APs and allows administrators to configure and manage the wireless and mobile user environment.

The products, when configured as specified in the guidance documentation, satisfy all of the security functional requirements stated in the Aruba Mobility Controller and Access Point Series Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	Aruba Mobility Controller and Access Point Series, comprising: o Aruba Mobility Controllers: Aruba MC 200, MC 800, MC 3200, MC3400, MC3600 and MC 6000. o Aruba Access Points: Aruba AP-60, AP-61, AP-65, AP-70, AP-85, AP-120, AP-121, AP-124 and AP-125. o ArubaOS version 3.4.2.3
Sponsor:	Aruba Networks, Inc. 1344 Crossman Avenue Sunnyvale, CA 94089-1113

Developer:	Aruba Networks, Inc. 1344 Crossman Avenue Sunnyvale, CA 94089-1113
CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	21 August 2009
Completion Date:	9 May 2011
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 2, September 2007.
Evaluation Class:	EAL 4 augmented with ALC_FLR.2
Description:	Aruba Mobility Controller and Access Point Series provides a Wireless Local Area Network (WLAN) access system supporting a wide range of wireless and wired network mobility services, security, centralized management, auditing, authentication, remote access, and wireless intrusion detection.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Aruba Mobility Controller and Access Point Series product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	US Government Wireless Local Area Network (WLAN) Access System For Basic Robustness Environments Protection Profile, Version 1.1, 25 July 2007
Evaluation Personnel:	Science Applications International Corporation: Anthony J. Apted Dawn Campbell Katie Sykes
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its IT environment are intended to counter:

- An administrator may incorrectly install or configure the TOE, resulting in ineffective security mechanisms.
- A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
- A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
- Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
- Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
- The developer or tester performs insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may occur, resulting in incorrect TOE behavior being undiscovered leading to flaws that may be exploited by a mischievous user or program.
- A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
- A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
- A user may gain unauthorized access to an unattended session.
- A user may gain access to services (either on the TOE or by sending data through the TOE) for which they are not authorized according to the TOE security policy.
- An unauthorized user or process may gain access to an administrative account.

1.4 Organizational Security Policies

The ST identifies the following organizational security policies that the TOE and its IT environment are intended to fulfill:

- The TOE shall display an initial banner for administrator logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
- The authorized users of the TOE shall be held accountable for their actions within the TOE.
- The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.

- Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).
- The TOE shall provide the capability to encrypt/decrypt wireless network traffic between the TOE and those wireless clients that are authorized to join the network.
- In accordance with the DOD Wireless Policy, there will be no ad hoc 802.11 or 802.15 networks allowed.

2 Identification

The evaluated product is **Aruba Mobility Controller and Access Point Series**, comprising:

- Aruba Mobility Controllers: Aruba MC 200, MC 800, MC 3200, MC3400, MC3600 and MC 6000.
- Aruba Access Points: Aruba AP-60, AP-61, AP-65, AP-70, AP-85, AP-120, AP-121, AP-124 and AP-125.
- ArubaOS version 3.4.2.3

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the Aruba Mobility Controller and Access Point Series security policy has been extracted and reworked from the Aruba Mobility Controller and Access Point Series ST and Final ETR.*

3.1 Security Audit

The TOE is capable of auditing security relevant events such as logins, administrator actions, use of trusted channel and path, cryptographic operations, resource limitation exceeded, etc. Each audit event includes the date and time of the event, the type of event, the subject identity (if applicable), and the outcome of the event. The administrator can include and exclude events to be audited based on specific criteria. The TOE can detect security event/violation based on signature and perform the appropriate action such as alerting the administrator or denying access.

3.2 Cryptographic Support

The TOE has been certified as a FIPS 140-2 cryptographic module (FIPS 140-2 certified Certificates #:1297, #1116, #1109, #1077, and #1075) at Security Level 2. When in FIPS mode, the cryptographic module only employs FIPS-approved RNG, key generation, establishment, zeroization, encryption, digital signature, and hashing algorithms.

3.3 User Data Protection

The TOE provides both policies and access control lists (ACLs) to control information flow. Firewall policies identify specific characteristics about a data packet and specify the action to take based on that identification. ACLs provide a method of restricting certain types of traffic on a physical port based on IP address, port, protocol, etc. Administrators can apply firewall policies to user roles and give differential treatment to different users on the same network, or to physical ports and apply the same policy to all traffic through the port. The TOE can also group wireless

clients into separate virtual LANs (VLANs). The TOE protects the data between itself and the wireless clients using AES or TDES. The TOE ensures any previous information content is made unavailable upon the allocation of a memory buffer to a network packet.

3.4 Identification and Authentication

The TOE can maintain administrator and user attributes, including credentials such as username and password for administrators and session key and role for remote authenticated users (username and password can be stored in the TOE's internal database or in an authentication server in the operational environment). The TOE requires identification and authentication (either locally or remotely through external authentication server, internally, or both) of administrators managing the TOE. The TOE provides various mechanisms for identifying and authenticating wireless clients, including captive portal and 802.1X. After an administrator-specified number of failed authentication attempts, the user account is locked out. In addition, the password mechanism can be configured to have a minimum length of six characters.

3.5 Security Management

The TOE provides the capability to manage auditing, cryptographic operations, intrusion protection functions, password minimum length enforcement, user accounts, policies & ACLs rules, advisory banner, and timeout (inactivity threshold) value. The management functions are restricted to an administrator role. The role must have the appropriate access privileges or access will be denied. The wireless user role has no access to the management interfaces. The information flow policy blocks packets by default and only administrators can change the default values. The FIPS-validated TOE ensures that only secure values are accepted for security attributes.

3.6 Protection of the TSF

The TOE provides integrity protection for all communication between its components. This prevents unauthorized modification of TSF data during transmission. The TOE also provides self-tests to ensure the correct operation of the cryptographic functions and TSF hardware. There is an option for the administrator to verify the integrity of stored TSF executable code. The communication between the TOE and another trusted IT product (e.g., NTP, syslog, RADIUS) is protected through a trusted channel. The communication between the TOE and remote administrators is protected through a trusted path.

3.7 Resource Utilization

The TOE can enforce maximum usage quotas on the number of concurrent sessions available to each named group of users.

3.8 TOE Access

The TOE allows administrators to configure a period of inactivity for a user's session. Once that time period has been reached while the session has no activity, the session is terminated. A warning banner is displayed at the management interfaces (Web GUI and CLI) to advise users on appropriate use and penalty for misuse of the system.

3.9 Trusted Path/Channels

The TOE provides an encrypted channel between itself and third-party trusted IT entities in the operating environment. The TOE also provides a protected communication path between itself and wireless users.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- Administrators are non-hostile, appropriately trained and follow all administrator guidance.
- There are no general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) available on the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- Wireless clients are configured so that information cannot flow between a wireless client and any other wireless client or host networked to the TOE without passing through the TOE.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 4 augmented with ALC_FLR.2).
2. This evaluation only covers the specific model numbers and software version identified in this document, and not any earlier or later versions released or in process.
3. The TOE must be configured in FIPS mode in the evaluated configuration.
4. The following add-on software modules, which are not part of the ArubaOS base software package and require separate product licenses, are included in the scope of evaluation and required in the evaluated configuration:
    a. Policy Enforcement Firewall—provides identity-based security for wired and wireless clients.
    b. Wireless Intrusion Protection—detects, classifies and limits designated wireless security threats such as rogue APs, denial of service attacks, malicious wireless attacks, impersonations, and unauthorized intrusions.
    c. VPN Server—enables controllers to provide Virtual Private Network (VPN) tunnel termination to local and remote clients, and provides site-to-site VPN tunnels between controllers and third-party VPN concentrators.
5. The TOE utilizes third-party software and hardware components in its operational environment, as follows:
    a. syslog server to store audit records

b. authentication server to authenticate users (RADIUS, LDAP, and TACACS+ are supported)

c. Network Time Protocol (NTP) server to obtain reliable time stamps

d. SNMP server to capture SNMP traps. For security reasons, only SNMPv3 is allowed in the evaluated configuration.

e. The remote administrator can use a web browser to access the Web GUI interface and/or use SSH client to access the CLI. Note that Telnet cannot be used to access the CLI in the CC evaluated configuration.

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and design documentation.

At a high level, Aruba Mobility Controllers consist of two main components:

- Control Plane (CP)—implements functions which can be handled at lower speeds such as Mobility Controller system management (CLI and Web GUI), user authentication (e.g. 802.1X, RADIUS, LDAP, captive portal), Internet Key Exchange (IKE), auditing/logging (SYSLOG), Wireless IDS (WIDS), and termination of protocols operating at the system level (e.g. SSH, TLS, NTP, etc.).
- Data Plane (DP)—implements functions that must be handled at high speeds such as high-speed switching functions (forwarding, VLAN tagging/enforcement, bridging), termination of 802.11 associations/sessions, tunnel termination (GRE, IPsec), firewall/ACL and deep packet inspection functions, and cryptographic acceleration.

The CP runs the Linux OS, along with various custom user-space applications which provide CP functions. This suite of custom user-space applications, which constitutes ArubaOS, provides the following functions:

- Monitoring and managing critical system resources, including processes, memory, and flash
- Sending and receiving PAPI[1] protocol messages to and from managed APs as well as other mobility controllers
- Managing system configuration and licensing
- Managing an internal database used to store licenses, user authentication information, etc
- Providing network anomaly detection, hardware monitoring, mobility management, wireless management, and radio frequency management services
- Providing a Command Line Interface (CLI) for the MC
- Providing a web-based management UI for the MC, as well as an optional captive portal login page for wireless users
- Providing various WLAN station and AP management functions

[1] PAPI is an Aruba-proprietary WLAN management protocol and provides no direct security.

- Providing authentication services for the system management interfaces (CLI, web GUI) and wireless users
- Providing IPSec key management services for remote APs, VPN users, and connections with other Aruba mobility controllers
- Providing Network Time Protocol service for APs, point-to-point tunneling protocol services for users, layer 2 tunneling protocol services for users, file transfer protocol services for users, serial over Ethernet connection services for administration of directly-connected APs, SSH services for incoming management connections, SNMP client/agent services, and protocol independent multicast (routing) services for the controller
- Providing syslog services by sending logs to the operating environment.

The DP is further subdivided into two subcomponents: Fast Path (FP) and Slow[2] Path (SP). The FP implements high-speed packet forwarding based on various proprietary tables, and on table miss will send the packets to SP. The SP manages all DP tables such as user, ACL, station, tunnel, route, ARP cache, session, bridge, VLAN, and port. The SP also performs deep packet inspection and cryptographic processing.

The Linux OS running on the CP is MontaVista's Embedded Linux. Linux is a soft real-time, multi-threaded operating system that supports memory protection between processes. Only Aruba provided interfaces are used, and the CLI is a restricted command set. For the 3000 series, this OS implements both the control and data planes.

For all but the 3000 series, the data plane is primarily implemented on the SiByte platform[3]. A lightweight, Aruba-proprietary OS called SOS runs on the SiByte platform. SOS contains an Ethernet driver, a serial driver, a logging facility, semaphore support, and a crypto driver. In the MC 6000 controller, a Field Programmable Gate Array (FPGA) is used to control and monitor the switch fabric, MACs, PHYs, SoE, and PoE and provide security functionality such as filtering.

The DP and CP run on different hardware platforms but the security functionality remains the same, regardless of the model. The differences in the platforms are in the processors, memory capacity, physical interfaces, FPGA implementation, etc., and are based on performance and scalability requirements. The table below shows the different models based on maximum number of APs and users supported.

Table 2 – Mobility Controller Specifications

Product	Max. # of APs	Max. # of Users	Typical Deployment
MC 6000	2,048	32,768	Headquarters/ Large Campus
MC 3000 Series	128	2,048	Medium/Large Enterprise/Campus
MC 800	16	256	Branch Office
MC 200	6	100	Small Offices/ Retail Store

Each Aruba AP is a wireless hardware device that is enclosed in a plastic encasing. The ArubaOS provides the security functionality for the APs. The ArubaOS runs on an embedded Linux kernel.

[2] The entire DP (including both FP and SP elements) is a high-speed packet processor, so the SP designation should be understood to be relative.

[3] SiByte refers to the hardware architecture of the TOE which includes Broadcom SiByte MIPS processors and cryptographic processor.

Similar to the controllers, the security functionality of the different models are the same with differences in platforms based on performance and scalability requirements only. At a high level, the APs consist of the following subsystems:

- Processor subsystem—performs the packet processing functions on the packet
- Memory subsystem—contains memory which supports the Processor subsystem
- Ethernet Controller subsystem—includes integrated Ethernet MAC for transfer of 10/100 Ethernet packets between the AP and the wired network
- Radio Controller subsystem—there are two radio controllers, 802.11a (5 GHz range) and 802.11b/g (2.4 GHz range)
- Wireless Antenna subsystem—interface between the wireless world and the AP. The antenna handles both 5 GHz and 2.4 GHz ranges
- PoE (Power over Ethernet) subsystem—receives 48V power over the Ethernet
- SoE (Serial over Ethernet) subsystem—contains the RS-232 serial port circuitry for communicating with the switch connected to the 10/100 port
- USB subsystem—the AP-70 supports one USB V2.0 compliant port (up to 480 Mbps). A PCI to USB 2.0 controller is used to interface to the system host
- Serial subsystem—the AP-120 supports a serial console port on the front panel that utilizes a RJ45 jack and connects directly to serial port 0 via the RS232 transceiver.

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and therefore delivered with the TOE is as follows:

- *Aruba AP-120 Series Indoor Access Point Installation Guide*, Apr 2009
- *Aruba AP-60/61 Access Point Installation Guide*, Apr 2008
- *Aruba AP-65 Wireless Access Point Installation Guide*, 20 Aug 2008
- *Aruba AP-70 Access Point Installation Guide*, Nov 2009
- *Aruba AP-85 Outdoor Access Point Series Installation Guide*, Feb 2010
- *ArubaOS 3.4.2.2-FIPS Release Notes*, Apr 2010
- *ArubaOS 3.4.2 Command Line Interface Reference Guide*, Dec 2009
- *ArubaOS 3.4.2 MIB Reference Guide*, Jun 2008
- *ArubaOS 3.4.2 Quick Start Guide*, Dec 2009
- *ArubaOS 3.4.2 User Guide*, Dec 2009
- *ArubaOS 3.4.2 Software Upgrade Guide*, Dec 2009
- *Aruba Common Criteria EAL4 Addendum*, Apr 2010
- *Aruba 200 Mobility Controller Installation Guide*, May 2006

- *Aruba 3000 Multi Service Mobility Controller Series Installation Guide*, Sep 2007
- *Aruba 6000 Series Mobility Controller Installation Guide*, May 2006
- *Aruba 800 Series Mobility Controller Installation Guide*, Jan 2006
- *ArubaOS 3.4.2 Syslog Messages Reference Guide*, Aug 2009

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for Aruba Mobility Controller and Access Point Series.

Evaluation team testing was conducted at the vendor's development site April 11 through April 14, 2011.

7.1 Developer Testing

The vendor's approach to testing is based primarily on comprehensive testing of the network protocols forming the majority of the TSFI. Much of the testing is automated using a dedicated security analyzer (the Mu-4000) to thoroughly exercise the TSFI. Additional manual testing is also performed to demonstrate capabilities specified in the SFRs that are not directly discernible through protocol testing, and to generate specific audit records or packet streams for capture and subsequent analysis. The vendor has developed a test suite comprising interface tests specific to each TSFI described in the functional specification.

The vendor's test documentation additionally includes security conformance tests for the following protocols and associated RFCs:

- EAP TLS Authentication Protocol (RFC 2716)
- EAP Tunneled TLS Authentication Protocol (RFC 5281)
- HTTP over TLS (RFC 2818)
- IPsec/IKE (RFC 2408, RFC 2409)
- IPsec/ESP (RFC 4303)
- Protected EAP (PEAP) Version 0
- RADIUS (RFC 2138, RFC 2869, RFC 3579, RFC 3580)
- SSH (RFC 4251, RFC 4252, RFC 4253, RFC 4254).

Each protocol or (for protocols defined by multiple RFCs) RFC has a test case specification that describes the test cases for testing each conformance statement in the corresponding RFC conformance document. Each test case maps to one or more test identifiers, which identify the specific conformance statements tested.

The vendor ran the TOE test suites in various configurations, consistent with the test environment described in the testing documentation, and provided the evaluation team with the actual results. The test configurations were representative of the Mobility Controller and Access Point appliances included in the evaluated configuration. All tests passed.

7.2 Evaluation Team Independent Testing

The evaluation team executed a sample of the vendor test suite, per the evaluated configuration as described in the Aruba Mobility Controller and Access Point Series Security Target. The tests were run on a selection of the test configurations described in the various interface test documents.

The developer's test documentation describes different test configurations for each of the TSFI that is tested. The documentation identifies different models of the TOE components that were used in the test configurations. The evaluation team performed its tests on two test bed configurations as follows:

- An MC-3400 Mobility Controller with an AP-125 Access Point. The MC-3400 is a high-end mobility controller based on the XLR architecture described in the Architecture Overview, while the AP-120 series of access points (which includes the AP-125) are the only access points in the valuated configuration that include a hardware cryptographic module.
- An MC-800 Mobility Controller and an AP-70 Access Point. The MC-800 is a low-end Mobility Controller based on the legacy architecture described in the Architecture Overview.

All MCs run the same MC code base, all APs run the same AP code base, and all MCs and APs in the evaluated configuration are also FIPS 140-2 validated.

The test environment included the following IT components that are external to the TOE but are required in the TOE's operational environment:

- Client computers to support remote administration—in the test environment, these comprised laptops equipped with Windows XP or Linux. On the Windows XP platforms, Putty was used to provide access to the CLI using SSH and either Internet Explorer or Mozilla Firefox was used to provide access to the WebUI using HTTPS, while on the Linux platforms Openssh was used to access the CLI and Mozilla Firefox was used to access the WebUI.
- Wireless clients—in the test environment, these comprised laptops equipped with Windows XP and Odyssey Access Client to provide wireless client access to the TOE.
- A RADIUS server to support remote authentication of wireless client users.
- An NTP server to provide a synchronized timestamp to the network components.
- An SNMP server to receive traps generated by the TOE.

The test environment provided by the vendor included the following tools used in a number of the vendor's tests:

- Wireshark—used to capture and examine packet streams
- Colasoft Packet Builder—used to craft or modify network packets
- MG-SOFT MIB browser—an SNMP browser used to monitor network-attached devices when testing SNMP
- OpenSSL—used in manual testing of the TOE's TLS implementation

- Paros proxy—used to intercept and modify HTTP/HTTPS data transmitted between a client and server
- Backtrack4—provides a large collection of security-related tools ranging from port scanners to password crackers
- IxANVL (Automated Network Validation Library) software from Ixia—used to demonstrate RFC conformance of specific protocols
- Mu-4000 security analyzer—used to exercise the TOE's implementation of specific protocols.

The evaluation team performed the following additional functional tests:

- **Audit Data Generation**—the evaluation team confirmed, through examination and analysis of the audit trail produced by running the vendor test sample and the evaluation team's own tests, that all audit records specified in the ST can be generated by the TOE.
- **Audit Function Management**—the evaluation team determined, through testing and examination of the developer's guidance documentation, that the security audit function is always enabled when the TOE is operating and there is no command provided to disable the audit function.
- **Selective Audit**—the evaluation team confirmed the descriptions in the ST that the administrator is able to include and exclude auditable events from the set of audited events based on specified criteria.
- **Administrator Login**—the evaluation team confirmed the behavior of the identification and authentication mechanisms for remote administrators.
- **Password Constraints**—the evaluation team confirmed the TOE enforces a minimum password length of 6 characters for all passwords, and that the administrator can configure a Management Password policy to set a minimum password length in the range 6..64 and specify additional restrictions, based on password composition rules.
- **Information Flow at AP**—the evaluation team confirmed the Access Point components of the TOE enforce information flow (firewall) rules and NAT policy when configured in remote bridge mode.
- **Security Management**—the evaluation team confirmed that all management capabilities specified and described in the ST are described accurately and are limited to appropriate security management roles.
- **Maximum Simultaneous Sessions**—the evaluation team confirmed the TOE enforces the maximum number of sessions specified for a defined user role.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE, identifying a number of vulnerabilities reported against earlier versions of ArubaOS or third-party libraries that are incorporated within ArubaOS. The evaluation team determined, through analysis of vulnerability descriptions and consideration of the method of use of the TOE, that two of these reported vulnerabilities are not relevant to the TOE in its evaluated configuration—one relates to SNMP, which must be configured for SNMPv3 in the evaluated configuration, and the other is a documented feature, which has appropriate guidance associated with it in the product guidance documentation. The evaluators additionally confirmed, through examination of the vendor's CM

records, that the other vulnerabilities have had fixes developed and applied to ArubaOS and do not exist in the evaluated version of the TOE.

The evaluation team also performed a port scan of the TOE using Nmap. The evaluation team confirmed all open ports identified by the scan were identified in the TOE guidance as ports that are open by default, but only on the trusted side of the network.

In addition to the open source search and port scan, the evaluation team considered other potential vulnerabilities, based on a focused search of the evaluation evidence. Some of the ideas for vulnerability tests identified by the evaluation team were already covered by vendor functional tests or by the independent functional tests devised by the evaluation team. Others were determined, through analysis, not to present exploitable vulnerabilities. The evaluation team performed tests to confirm:

- The TOE accepts only SSHv2 connections. Attempts to connect to the CLI using SSHv1 are refused.
- The TOE does not allow MIB values to be modified via SNMP—they can only be read. In addition, when SNMPv3 is configured, all SNMP packet data is encrypted, and any attempt to execute an SNMP request must specify the correct authentication and privacy credentials.

8 Evaluated Configuration

The evaluated version of the TOE is identified as: Aruba Mobility Controller and Access Point Series, comprising:

- Aruba Mobility Controllers: Aruba MC 200, MC 800, MC 3200, MC3400, MC3600 and MC 6000.
- Aruba Access Points: Aruba AP-60, AP-61, AP-65, AP-70, AP-85, AP-120, AP-121, AP-124 and AP-125.
- ArubaOS version 3.4.2.3.

The TOE is a Wireless Local Area Network (WLAN) access system comprising Aruba Mobility Controllers, Access Points, and the ArubaOS. The Aruba Mobility Controller (MC) appliances are wireless switches that provide a wide range of wireless and wired network mobility, security, centralized management, auditing, authentication, and remote access. The Aruba Access Point (AP) appliances service wireless clients (part of the operational environment) and can monitor radio frequency spectrums to detect intrusions, denial of service (DoS) attacks, and other vulnerabilities. The ArubaOS is a suite of mobility applications that runs on all Aruba MCs and APs and allows administrators to configure and manage the wireless and mobile user environment.

The TOE relies on third-party software and hardware components in the operating environment. The TOE can utilize an external audit server (support syslog) to store audit records and external authentication server (support RADIUS, LDAP, TACACS+) to authenticate users. In addition, the TOE uses an external Time server (support NTP) to obtain reliable time stamps and external SNMP server to capture SNMP traps. For security reasons, only SNMPv3 is allowed in the evaluated configuration. The remote administrator can use a web browser to access the Web GUI interface and/or use SSH client to access the CLI. The local administrator can use the serial port to access the CLI. Neither the web browser or SSH client is part of the TOE. Note that Telnet cannot be used to access the CLI in the CC evaluated configuration.

9 Results of the Evaluation

The evaluation was conducted based upon version 3.1 Revision 2 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL4 augmented with ALC_FLR.2" certificate rating be issued for Aruba Mobility Controller and Access Point Series.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table.

Table 3 – TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security Architecture Description
ADV_FSP.4	Complete Functional Specification
ADV_IMP.1	Implementation Representation of the TOE
ADV_TDS.3	Basic Modular Design
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.4	Production Support, Acceptance Procedures and Automation
ALC_CMS.4	Problem Tracking CM Coverage
ALC_DEL.1	Delivery Procedures
ALC_DVS.1	Identification of Security Measures
ALC_FLR.2	Flaw Reporting Procedures
ALC_LCD.1	Developer Defined Life-cycle Model
ALC_TAT.1	Well-defined Development Tools
ATE_COV.2	Analysis of Coverage
ATE_DPT.2	Testing: Security Enforcing Modules
ATE_FUN.1	Functional Testing
ATE_IND.2	Independent Testing – Sample
AVA_VAN.3	Focused Vulnerability Analysis

10 Validator Comments/Recommendations

1. The TOE does not support authenticated NTP for time synchronization. The TOE end-user must ensure that the communications path for NTP and the time server is trusted.
2. The TOE permits configuration of key sizes smaller than required in the Protection Profile. TOE users should select the required key sizes during configuration.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is **Aruba Mobility Controller and Access Point Series Security Target,** Version 1.0, dated May 6, 2011.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 1, September 2006, CCIMB-2006-09-001.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-002.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-003.
4. Common Methodology for Information Technology Security: Evaluation methodology, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-004.
5. Aruba Mobility Controller and Access Point Series Security Target, Version 1.0, May 6, 2011.