DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) 26 June 2024

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Aruba, a Hewlett Packard Enterprise company, Mobility Gateways (7000/7200 and 9000/9200 series), Mobility Conductors (Hardware/Virtual), and specified Remote Access Points, with Software Release Aruba Operating System (AOS) 8.10

References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013, Change 2," September 2017
(c) through (d), see Enclosure 1

1. Certification Authority. Reference (a) establishes the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for Department of Defense Information Network (DoDIN) products, Reference (b).

2. Conditions of Certification. The Aruba, a Hewlett Packard Enterprise company, Mobility Gateways (7000/7200 and 9000/9200 series), Mobility Conductors (Hardware/Virtual), and specified Remote Access Points, with Software Release Aruba Operating System (AOS) 8.10, is hereinafter referred to as the System Under Test (SUT). The SUT meets the requirements of the Unified Capabilities Requirements, Reference (b), as a Virtual Private Network (VPN) and is certified for joint use with the conditions described in Table 1.

This certification expires upon changes which affect interoperability, but no later than the expiration date specified in the DoDIN Approved Products List (APL) memorandum.

Table 1. Conditions

Description		Operational Impact	Remarks
UCR Waivers			
None.			
TDR#	**Conditions of Fielding**		
ANI-1828-001	SEC-000120: The SUT cannot record network traffic at the layer in which it is operating. CoF: The site shall provide a local capture device for capturing real time data to meet this requirement. The SUT should have a mirror port configured to support the capture.	Minor with CoF	On 30 April 2024, DISA adjudicated this discrepancy as minor with a CoF.

(Table continues next page.)

Table 1. Conditions (continued)

Description		Operational Impact	Remarks
TDR#	**Conditions of Fielding** (continued)		
ANI-1828-002	SEC-000330: The SUT moves VPN at 1/3rd of the published rate. CoF: When configured for use on the DoD network, throughput is 1/4th to 1/3rd of the Vendor's published rate.	Minor with CoF	On 30 April 2024, DISA adjudicated this discrepancy as minor with a CoF.
TDR#	**Open Test Discrepancies**		
	None.		

LEGEND:

CoF	Condition of Fielding	TDR	Test Discrepancy Report
DISA	Defense Information Systems Agency	UCR	Unified Capabilities Requirements
DoD	Department of Defense	VPN	Virtual Private Network
SUT	System Under Test		

3. Interoperability Status. Table 2 provides the SUT Interface Status, Table 3 provides the Capability Requirements and Functional Requirements status, and Table 4 provides a DoDIN APL Product Summary, to include subsequent Desktop Review (DTR) updates.

Table 2. SUT Interface Status

Interface (See note 1.)	Applicability: (R), (O), (C)	Status	Remarks
	VPN		
Network Management Interfaces (See note 2.)			
10 Mbps	C	Not Tested (See note 3.)	IAW IEEE 802.3i or 802.3j.
100 Mbps	C	Met	IAW IEEE 802.3u
1000 Mbps	C	Met	IAW IEEE 802.3ab or 802.3z
Serial (EIA/TIA)	C	Met	
Network Interfaces (See note 4.)			
10 Mbps	C	Met	IAW IEEE 802.3i or 802.3j
100 Mbps	C	Met	IAW IEEE 802.3u
1000 Mbps	C	Met	IAW IEEE 802.3ab or 802.3z
10 Gbps	O	Not Tested (See note 3.)	IAW IEEE 802.3ae or 802.3an.
25 Gbps	O	Met	IAW IEEE 802.3by-2016
40/100 Gbps	O	Met	IAW IEEE 802.3ba or 802.3bm
2.5/5 Gbps	O	Not Tested (See note 3.)	IAW IEEE 802.3bz.

NOTE(S):
1. The UCR 2013 Change 2, Section 13, does not identify individual interface requirements for security devices. The SUT must minimally provide Ethernet interfaces that meet the requirements in Section 2.7.1.
2. The SUT shall provide at least one of the specified management interfaces.
3. The SUT does not support this optional or conditional interface.
4. The SUT shall support at least of the wired network interfaces (802.3).

(Table continues next page.)

Table 2. SUT Interface Status (continued)

LEGEND:			
802.3ab	1000BaseT Gbps Ethernet over twisted pair	C	Conditional
802.3ae	10 Gbps Ethernet	CSMA	Carrier Sense Multiple Access
802.3an	10 GBaseT Ethernet over unshielded twisted	EIA	Electronic Industries Alliance
802.3ba	40/100 Gbps Ethernet	Gbps	Gigabits per second
802.3bm	40/100 Gbps Ethernet for Optical Fiber	GBaseT	Gigabit (Baseband Operation, Twisted Pair) Ethernet
802.3bz	2.5/5 GBaseT over twisted pair	IAW	In accordance with
802.3i	10BaseT Mbps over twisted pair	IEEE	Institute of Electrical and Electronics Engineers
802.3j	10BaseF over Fiber-Optic	Mbps	Megabits per second
802.3u	Standard for CSMA with collision detection at 100 Mbps	O	Optional
802.3by	25 Gbps Ethernet Standard twisted pair	R	Required
802.3z	Gigabit Ethernet Standard	SUT	System Under Test
BaseF	Megabit Ethernet over fiber	TIA	Telecommunications Industry Association
BaseT	Megabit (Baseband Operation, Twisted Pair) Ethernet	VPN	Virtual Private Network

Table 3. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (See note 1.)	UCR 2013 Change 2 Reference	Status
1	Cybersecurity (R)	See note 2.	Met (See note 2.)
2	IPv6 (R)	5.2	Met
3	Security Device Requirements (R)	13.2	Partially Met (See note 3.)

NOTE(S):
1. The annotation of "required" refers to a high-level requirement category. Enclosure 3 provides the applicability of each sub-requirement.
2. A JITC-led Cybersecurity test team conducted Cybersecurity testing and published the results in a separate report, Reference (d).
3. The SUT met the requirements in this section, with the following exceptions:
   - The SUT partially met the Conformance requirements in Section 13.2.1. The SUT moves VPN at 1/3rd of the published rate. DISA adjudicated this discrepancy as minor with CoF, as noted in Table 1.
   - The SUT partially met the Performance requirements in Section 13.2.3. The SUT cannot record the traffic at the layer at which it is created. DISA adjudicated this discrepancy as minor with CoF, as noted in Table 1.

LEGEND:

CoF	Condition of Fielding	JITC	Joint Interoperability Test Command
CR	Capability Requirement	R	Required
DISA	Defense Information Systems Agency	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements
ID	Identification	VPN	Virtual Private Network
IPv6	Internet Protocol version 6		

Table 4. DoDIN APL Product Summary

Product Identification	
Product Name	Mobility Gateways (7000/7200 and 9000/9200 Series), Mobility Conductors (Hardware and Virtual), and specified Remote Access Points
Software Release	AOS 8.10
UCR Product Type(s)	VPN
Product Description	The Aruba mobility gateway appliance provides secure remote access to web applications, client/server applications, and file shares for employees, business partners, and customers. All traffic is encrypted using Internet Protocol Security (IPSec) to secure the data. This appliance makes secure remote access possible using a Web interface for a wide range of platforms and mobile devices.

(Table continues next page.)

Table 4. DoDIN APL Product Summary (continued)

DoDIN Certified Function	Component/Sub-Component Name (See notes 1 and 2.)	Tested Version	Hardware Chipset	Remarks
VPN	**7000 and 7200 Series Gateways**			
	7024 7005 7008 7205 7210 7220 7240XM 7280	AOS 8.10	Broadcom XLP	VPN Concentrator Appliance
	9000 Series and 9200 Series Gateways			
	9004 9012	AOS 8.10	Intel Atom	VPN Concentrator Appliance
	9240		Intel Xeon	
	RAPs			
	AP-203RP AP-203R	AOS 8.10	Broadcom BCM40000	Secure Connector
	AP-303H		Qualcomm IPQ4000	
	AP-314 **AP-315**		Qualcomm IPQ8000	
	Managed/Standalone Virtual Gateway	AOS 8.10 ESXi 7.0.3 (build 22348816) ActivClient 7.4.1.5	NA	VPN Concentrator Appliance
	MCR-HW-1K MCR-HW-5K MCR-HW-10K	AOS 8.10	Intel Xeon	Management appliance physical product
	MCR-VA-1K MCR-VA-50 MCR-VA-500 MCR-VA-5K MCR-VA-10K	AOS 8.10 ESXi 7.0.3 (build 22348816) ActivClient 7.4.1.5	NA	Management appliance virtual
	Management Workstation (site-provided)	Windows 11 ActivClient 7.4.1.5	NA	System management

NOTE(S):
1. Table 3-3 in Enclosure 3 provides additional details for the initially tested components/subcomponents.
2. Components bolded and underlined were tested. The other components in the family series were not tested; however, JITC certified the other components for joint use because they have similar hardware and operate on the same software as the tested and certified components and JITC analysis determined they were functionally identical for interoperability certification purposes.

LEGEND:

AOS	Aruba Operating System	JITC	Joint Interoperability Test Command
AP	Access Point	MCR	Mobility Conductor
APL	Approved Products List	NA	Not Applicable
DoDIN	Department of Defense Information Network	RAP	Remote Access Point
ESXi	Elastic Sky X integrated.	UCR	Unified Capabilities Requirements
IPsec	Internet Protocol Security	VPN	Virtual Private Network

4. Test Details. This certification is based on interoperability (IO) testing, Defense Information Systems Agency (DISA) adjudication of open test discrepancy reports (TDRs), review of the Vendor's Letter of Compliance (LoC), and the DISA Certifying Authority Recommendation for inclusion on the DoDIN APL. JITC completed review of the Vendor's LoC on 29 March 2024

JITC Memo, JTE, Joint Interoperability Certification of the Aruba, a Hewlett Packard Enterprise company, Mobility Gateways (7000/7200, and 9000/9200 series), Mobility Conductors (Hardware/Virtual), and specified Remote Access Points with Software Release Aruba Operating System (AOS) 8.10

and conducted IO testing at the JITC Global Network Test Facility (GNTF), Fort Huachuca, Arizona, from 1 April through 10 April 2024, using test procedures derived from Reference (c). A JITC-led Cybersecurity (CS) test team conducted CS testing from 18 March to 29 March 2024 and published the results in a separate report, Reference (d). Enclosure 2 documents the test results and describes the test network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

5. Additional Information. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Sensitive but Unclassified Internet Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at https://stp.jitc.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Industry Toolkit (JIT) at https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the CS Assessment Package containing the approved configuration and deployment guide must be requested directly from the Approved Products Certification Office (APCO) by e-mail: disa.meade.peo-transport.list.approved-products-certification-of@mail.mil. All associated information is available on the DISA APCO website located at https://aplits.disa.mil/.

6. Point of Contact (POC). JITC POC: Ms. Jenna Valenzuela; commercial phone 520-533-5442; DSN 879-5442; email: jenna.s.valenzuela.civ@mail.mil; mailing address: Joint Interoperability Test Command, C/O JTE-Ms. Jenna Valenzuela, 2001 Brainard Road (MB59), Fort Huachuca, Arizona 85613. The APCO tracking number for the SUT is 2319901.

FOR THE COMMANDER:

DORN.LAWRENCE.T.1168371930 Digitally signed by DORN.LAWRENCE.T.1168371930 Date: 2024.06.26 04:46:14 -07'00'

3 Enclosures a/s

LAWRENCE T. DORN
Chief
Specialized Test Division

JITC Memo, JTE, Joint Interoperability Certification of the Aruba, a Hewlett Packard Enterprise company, Mobility Gateways (7000/7200, and 9000/9200 series), Mobility Conductors (Hardware/Virtual), and specified Remote Access Points with Software Release Aruba Operating System (AOS) 8.10

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS
ISG Secretariat, DISA, JT
U.S. Strategic Command, J66
USSOCOM J65
USTRANSCOM J6
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6, SAIS-CBC
US Air Force, SAF/A6SA
US Marine Corps, MARCORSYSCOM, SEAL, CERT Division
US Coast Guard, CG-64
DISA/ISG REP
OUSD Intel, IS&A/Enterprise Programs of Record
DLA, Test Directorate, J621C
NSA/DT
NGA, Compliance and Assessment Team
DOT&E
Medical Health Systems, JMIS PEO T&IVV
HQUSAISEC, AMSEL-IE-ME
APCO

ADDITIONAL REFERENCES

(c) Joint Interoperability Test Command (JITC), "Virtual Private Network (VPN) Test Procedures Version 1.1 for Unified Capabilities Requirements (UCR) 2013 Change 2," January 2023 (Draft)
(d) JITC, "Cybersecurity Assessment Report for Aruba, a Hewlett Packard Enterprise company Mobility Gateways (7000/7200 and 9000/9200 series), Mobility Conductors, and specified Remote Access Points (RAPs), Virtual Private Network (VPN) Concentrator, Software Release Aruba Operating System (AOS) 8.10, Tracking Number (TN) 2319901," May 2024

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The Aruba, a Hewlett Packard Enterprise company, Mobility Gateways (7000/7200 and 9000/9200 series), Mobility Conductors, and specified Remote Access Points, with Software Release Aruba Operating System (AOS) 8.10, is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT identifying information and requirements source.

Table 2-1. System and Requirements Identification

System Identification	
Sponsor	Defense Information Systems Agency J6
Sponsor Point of Contact	Hung Tran, Email: hung.v.tran14.civ@mail.mil Phone: 301-225-8842
Vendor Point of Contact	Carmody Rauch, Email: carmody.rauch@hpe.com; Phone: 520-447-1544
System Name(s)	Aruba, a Hewlett Packard Enterprise company, Mobility Gateways (7000/7200 and 9000/9200 series), Mobility Conductors, and specified Remote Access Points
Increment and/or Version	Aruba Operating System (AOS) 8.10
Product Category	Virtual Private Network
System Background	
Previous certifications	None
Tracking	
APCO ID	Tracking Number 2319901
System Tracking Program ID	8384
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013, Change 2, Section 13
Remarks	None
Test Organization(s)	Joint Interoperability Test Command, Fort Huachuca, Arizona
LEGEND: AOS Aruba Operating System APCO Approved Products Certification Office ID Identification	

2. SYSTEM DESCRIPTION. The Department of Defense (DoD) Information Network (DoDIN) services include transport, data, voice, video, messaging, and other capabilities along with ancillary enterprise services. A key component of the DoDIN transport is the Security Device (SD). SDs are generally considered to be "cybersecurity and cybersecurity-enabled information technology (IT) Information Assurance Products" in accordance with (IAW) DoD Directive (DoDD) 8500.1. The cybersecurity (CS) and CS-enabled product requirements include network-based Firewalls (FWs), Intrusion Prevention Systems (IPSs), Virtual Private Network (VPN) servers, and Network Access Controllers (NACs), for example. More information on SDs can be found in Section 13 of the Unified Capabilities Requirements (UCR) 2013 Change 2, SDs.

A VPN extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it directly connects to the private network, while benefitting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to point connection to a proxy server using dedicated connections, encryption, or a combination of the two.

A VPN connection across the Internet is similar to a wide area network link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from the private network. VPNs allow employees to securely access their company's intranet while traveling outside the office. Similarly, VPNs securely and cost effectively connect geographically disparate offices of an organization creating one cohesive virtual network. VPN technology is also used by ordinary Internet users to connect to proxy servers for protecting one's identity.

The SUT is certified for joint use as VPN. The Aruba Mobility Gateway appliance provides secure remote access to web applications, client/server applications, and file shares for employees, business partners, and customers. All traffic is encrypted using Internet Protocol (IP) Security (sec) (IPsec) to secure the data. This appliance makes secure remote access possible using a Web interface for a wide range of platforms and mobile devices. The Mobility Gateway can be used to:

- Create a remote access connection that gives remote employees secure access to private company applications such as email via a web interface.
- Create a business partner connection that provides designated suppliers with access to an internal supply chain application via a web interface.

The user/administrator determines the user policies. The Mobility Gateway appliance applies those policies to control access methods appropriate for users.

The system consists of the following components:

- Gateway: 7000 Series, 7200 Series, 9000 Series, 9200 Series, Managed Virtual Gateway or Standalone Virtual Gateway
- Remote Access Point (RAP) (x3)
- Conductor; Mobility Conductor or Virtual Conductor

The Aruba Wireless Access Points were used as a text fixture for this test but were not certified under this event.

Gateways: 7000 Series, 7200 Series, 9000 Series, 9200 Series, Managed Virtual and Standalone Virtual. Mobility Gateways (physical and virtual) are wireless local-area network (WLAN) controllers and VPN concentrators that support IPsec VPN connections to RAPs as well as site-to-site IPsec VPN connections to other Mobility Gateways. The Gateways also manage the secure WLAN supported on the RAP.

The 7000 and 7200 Series Gateways include the 7005, 7008, 7024, 7205, 7210, 7220, 7240XM, and 7280 models. JITC tested the 7024 model under AOS 8.10. The 7000 and 7200 Series models perform the role of a VPN concentrator. They utilize the Broadcom XLP chipset, are a compact form factor of 1 Rack Unit, or less, and cover a broad range of maximum users and functional bandwidth.

The 9000 and 9200 Series Gateways include the 9004, 9012, and 9240 models. JITC tested the 9004 and 9240 models under AOS 8.10. The 9000 and 9200 Series models perform the role of a VPN concentrator. The 9000 and 9012 models utilize the Intel Atom chipset. The 9240 model is a higher scale product utilizing the Intel Xeon chipset. They are a compact form factor of 1 Rack Unit, or less, and cover a broad range of maximum users and functional bandwidth.

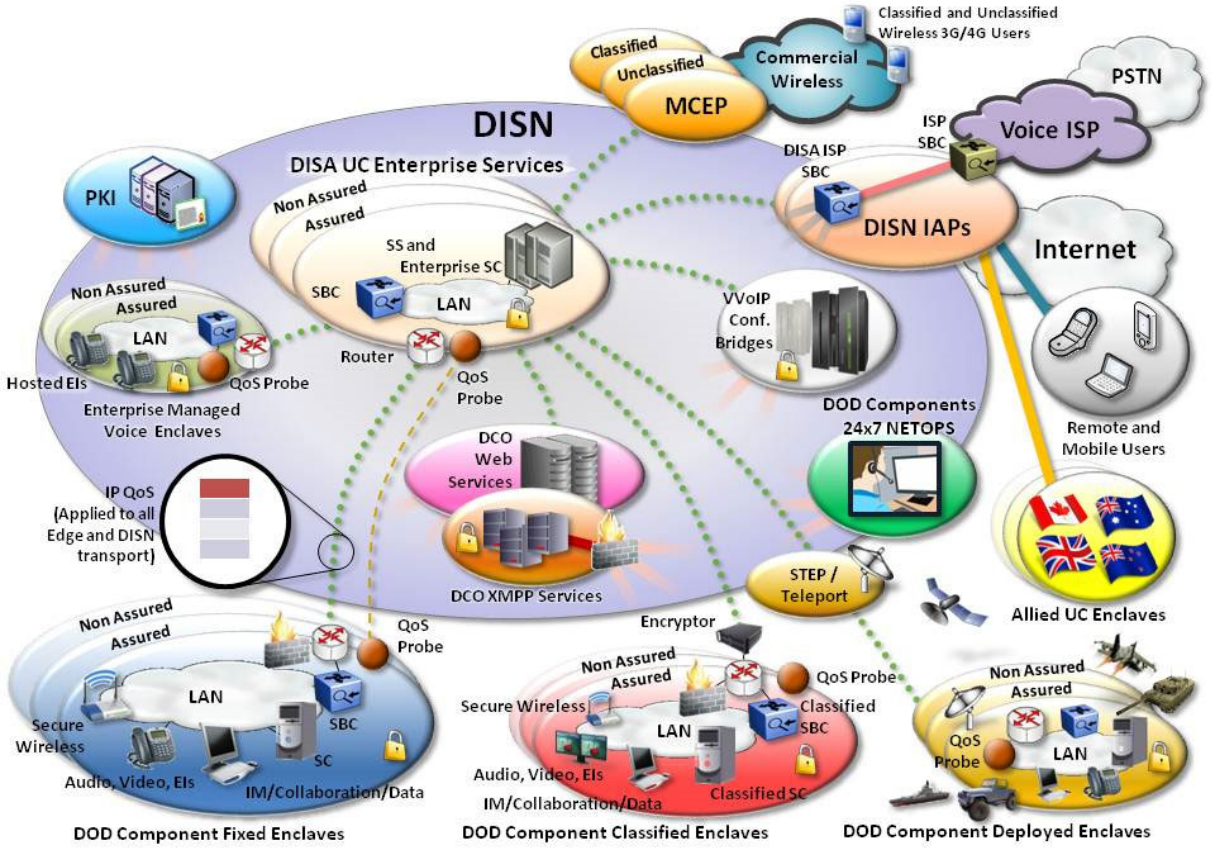
RAP (x3). The RAPs include Access Point (AP)-203R, AP-203RP, AP-303H, AP-314, and AP-315. JITC tested AP-203-RP, AP-303H, and AP-315 under AOS 8.10. The RAPs provide secure wireless or wired and wireless connections to end users. Once provisioned, the RAP will build a secure IPsec VPN connection back to a Mobility Gateway over the Internet or untrusted network. All traffic from the end user (wired or wireless) is sent over the VPN tunnel to the Gateway and then onto the trusted network.

Conductors: Mobility Conductor - Hardware (MCR-HW) and Mobility Conductor-Virtual Appliance (MCR-VA). Mobility Conductors (physical and virtual) provide an optional way to manage Mobility Gateways. Mobility Conductors use a centralized, multi-tiered architecture. Network configurations can be made and distributed from the Mobility Conductor automatically to all managed Mobility Gateways to eliminate onsite configuration, while still allowing for site or Gateway-specific configuration items. The management connection between the Mobility Conductor and Mobility Gateway is secured with an IPsec VPN.

Management Description. The SUT is managed using console access with a Secure Shell (SSH) terminal session, or web graphical user interface (GUI) using Hypertext Transfer Protocol Secure (HTTPS). The AOS supports using an authentication server with username/password or certificate-based authentication. The AOS Mobility Gateway devices can be managed directly, by implementing and using Mobility Conductors, or by AirWave (currently listed under tracking number 1804401). Management access is used to configure and manage AOS devices. AOS can send logs to a central syslog service.

3. OPERATIONAL ARCHITECTURE. The DoD Information Network (DoDIN) architecture is a two-level network hierarchy consisting of Defense Information Systems Network backbone switches and Service/Agency installation switches. The DoD Chief Information Officer and Joint Staff policy and subscriber mission requirements determine the type of switch allowable at a particular location. The DoDIN architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the Notional Operational DoDIN Architecture in which the SUT may be used. Figure 2-2 depicts the DoDIN SD functional model.

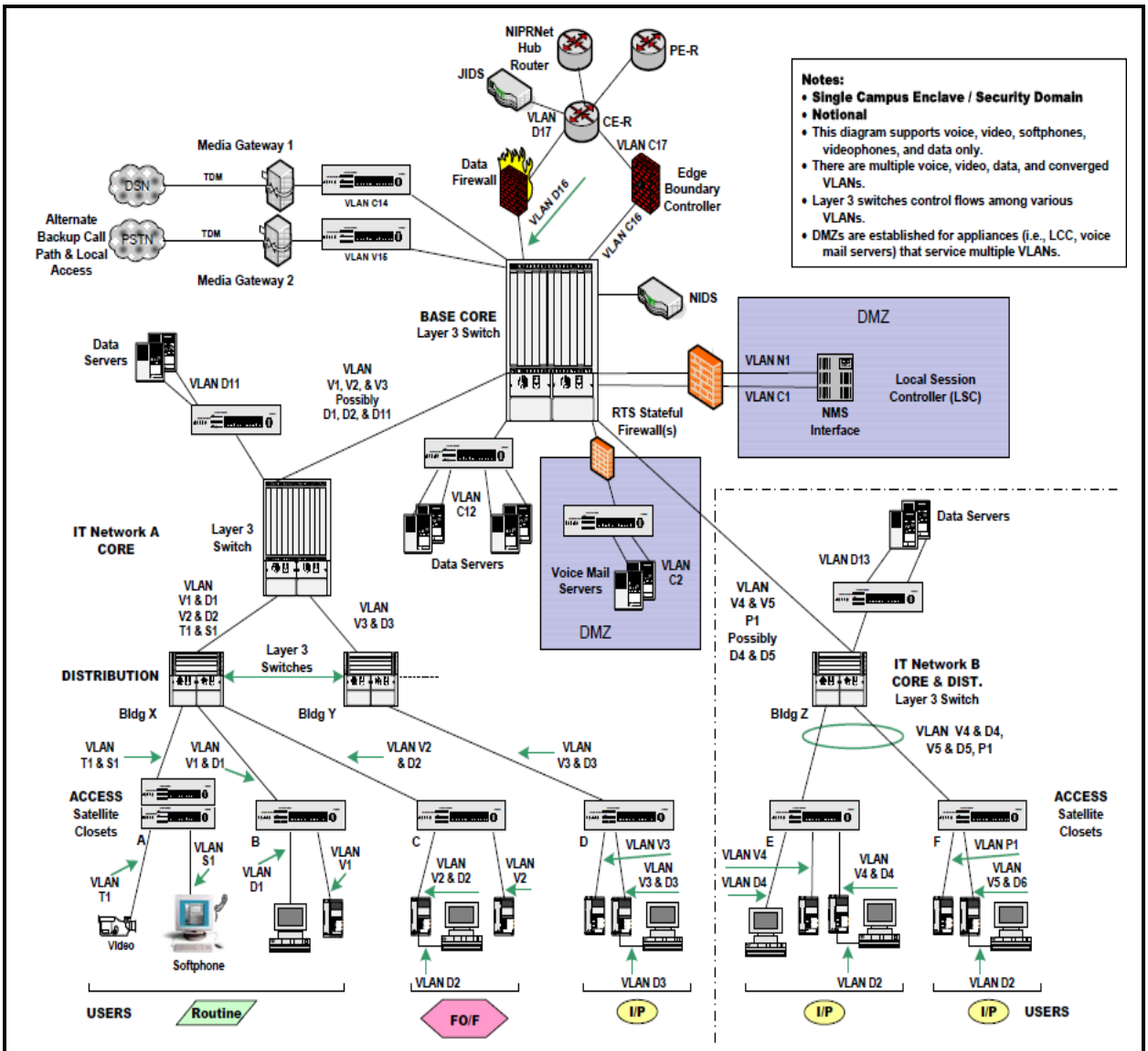
4. TEST CONFIGURATION. The Joint Interoperability Test Command (JITC) test team tested the SUT at the Global Network Test Facility, Fort Huachuca, Arizona, in a manner and configuration similar to that of a notional operational environment depicted in Figure 2-1. The test team tested the SUT's required interoperability functions and features using the test configuration depicted in Figure 2-3. The test configuration used for Cybersecurity (CS) testing is documented in a separate report, Reference (d)."



LEGEND:

DCO	Defense Connection Online	NETOPS	Network Operations
DISA	Defense Information Systems Agency	PKI	Public Key Infrastructure
DISN	Defense Information Systems Network	PSTN	Public Switched Telephone Network
DoD	Department of Defense	QoS	Quality of Service
DoDIN	DoD Information Network	SBC	Session Border Controller
EI	End Instrument	SC	Session Controller
IAP	Internet Access Point	SS	Softswitch
IM	Instant Messaging	STEP	Standardized Tactical Entry Point
IP	Internet Protocol	UC	Unified Capabilities
ISP	Internet Service Provider	VVoIP	Voice and Video over IP
LAN	Local Area Network	XMPP	Extensible Messaging and Presence Protocol
MCEP	Multi Carrier Entry Point		

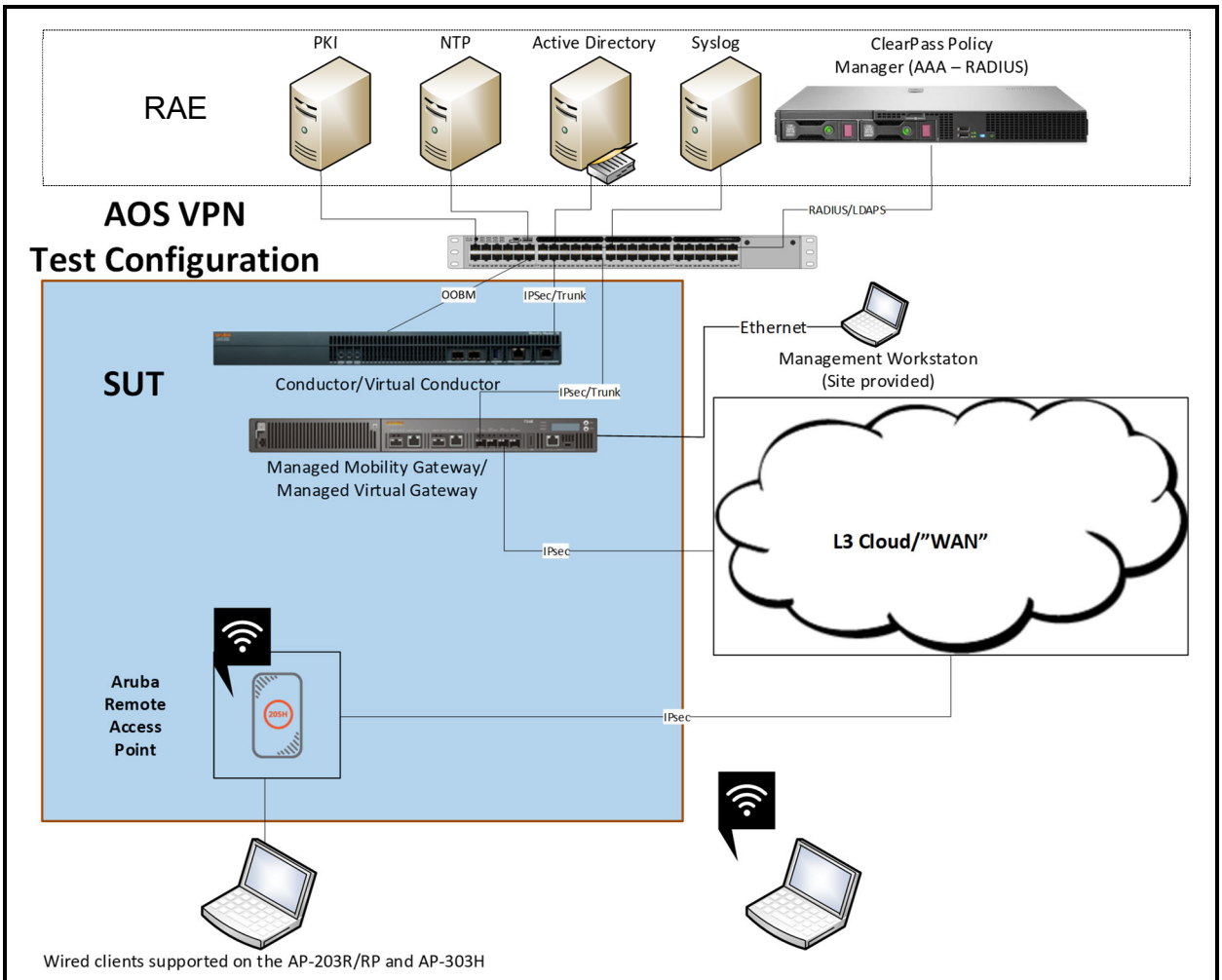
Figure 2-1. Notional DoDIN Architecture



LEGEND:

Bldg	Building	LSC	Local Session Controller
C	Carrier	NIDS	Network Intrusion Detection System
CE-R	Core Edge Router	NIPRNet	Unclassified-But-Sensitive Internet Protocol Router Network
D	Data	NMS	Network Management System
Dist	Distribution	PE-R	Perimeter Edge Router
DMZ	Demilitarized Zone	PSTN	Public Switched Telephone Network
DoDIN	Department of Defense Information Network	RTS	Real Time Service
DSN	Defense Switched Network	S	Softphone
FO/F	Flash Override/Flash	SUT	System Under Test
I/P	Internet Protocol	T	Video
IT	Information Technology	TDM	Time Division Multiplexing
JIDS	Joint Intrusion Detection System	V	Voice
LCC	Low-Cost Carrier	VLAN	Virtual Local Area Network

Figure 2-2. DoDIN Security Device Functional Model



LEGEND:

AAA	Authentication, Authorization, and Accounting	OOBM	Out-of-Band Management
AOS	Aruba Operating System	PKI	Public Key Infrastructure
AP	Access Point	R/RP	Component/Model name
H	component/model name	RADIUS	Remote Authentication Dial-In User Service
IPSec	Internet Protocol Security	SUT	System Under Test
L3	Layer 3	VPN	Virtual Private Network
LDAPS	Lightweight Directory Access Protocol Secure	WAN	Wide Area Network
NTP	Network Time Protocol		

Figure 2-3. SUT Interoperability Test Configuration

5. METHODOLOGY. JITC conducted testing of the SUT components IAW VPN requirements derived from the Unified Capabilities Requirements (UCR) 2013, Change 2, Reference (b), and using VPN test procedures derived from Reference (c). In addition to testing, an analysis of the Vendor's Letter of Compliance (LoC) verified the SUT met letter "R" requirements. Test Discrepancy Reports (TDRs) documented any noted discrepancies. The Vendor submitted Plan of Action and Milestones (POA&M) as required. The Defense Information Systems Agency (DISA) adjudicated two TDRs recorded during initial testing as minor with condition of fielding (CoF), as noted in Table 1. DISA will evaluate any new discrepancy noted in the operational environment for impact on the existing certification. DISA

will evaluate these discrepancies via a Vendor POA&M, which will address all new critical TDRs within 120 days of identification.

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS.
The UCR 2013, Change 2, Sections 2, 5, and 13, established the interface, Capability Requirements (CRs) and Functional Requirements (FRs), CS, and other requirements for SDs. In Enclosure 3, Table 3-1 provides the SUT interface status and Table 3-2 provides the CR and FR status. The sub-paragraphs below provide testing details and results. Optional and/or conditional requirements are not included in the test results unless otherwise noted.

a. The UCR 2013, Change 2, Section 5.2, includes the IPv6 Requirements.

1) Section 5.2.1 of UCR 2013 provided the detailed IPv6 product requirements for SDs: Maximum Transmission Unit, Flow Label, Address, Neighbor Discovery, Stateless Address Autoconfiguration and Manual Address Assignment, Internet Control Message Protocol, Traffic Engineering, IP Version Negotiation. The SUT met these requirements with testing and the Vendor's LoC.

2) Section 5.2.2 of UCR 2013 provided the detailed Mapping of Request For Comments to DoDIN Profile Categories product requirements for SDs. The SUT met these requirements with testing and the Vendor's LoC.

b. The UCR 2013, Change 2, Section 13.2, includes the SD Requirements.

1) Section 13.2.1 of UCR 2013 provided the conformance requirements for VPN. Note: This section is applicable to only a VPN. The SUT met the requirements in this section with testing and the Vendor's LoC, with the following exception: The SUT moves VPN at 1/3rd of the published rate. DISA adjudicated this discrepancy as minor with CoF, as noted in Table 1.

2) Section 13.2.2 of UCR 2013 provided the general requirements for Firewall (FW), Intrusion Prevention System (IPS), VPN, Network Access Controller (NAC), and Wireless Intrusion Detection System (WIDS). The SUT met the VPN requirements with testing and the Vendor's LoC.

3) Section 13.2.3 of UCR 2013 provided the performance requirements for FW, IPS, and VPN. SDs are intended to mitigate the threats enclaves face from external sources while permitting transmission of legitimate traffic in both directions. Performance tests attempt to validate an SD's ability to maintain that legitimate traffic stream while the network is under attack. The SUT met the VPN requirements in this section with testing and the Vendor's LoC, with the following exception: The SUT cannot record the traffic at the layer at which it is created. DISA adjudicated this discrepancy as minor with CoF, as noted in Table 1.

4) In addition to Section 4, the UCR 2013 Section 13.2.4 also specifies functional requirements for "SD-unique" products such as network-based FWs, IPSs, VPN concentrators, Integrated Security System (ISSs), WIDS, and NACs. The SUT met the VPN requirements with testing and the Vendor's LoC.

5) Section 13.2.4.1.1 of UCR 2013 provided policy requirements for FW and VPN. This section identifies the need for an SD to respond to policy-based actions set by a System Administrator. Note: This section is only applicable to FW or VPN. The SUT met the VPN requirements with testing and the Vendor's LoC.

6) Section 13.2.4.1.2 of UCR 2013 provided filtering requirements for FW to perform basic filtering functions. The SD's controlled interface must support and filter communications protocols/services from outside the perimeter of the interconnected Information Systems (ISs) according to IS-appropriate needs (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications). Filtering is defined as having the ability to block on a per-interface basis, defaulting to block, and defaulting to disabled, if supported on the SD itself. Note: This section is only applicable to FW. The SUT is a VPN; therefore, these FW requirements do not apply to the SUT.

7) Section 13.2.4.2 of UCR 2013 provided functionality requirements for IPS. The SUT is a VPN' therefore, these IPS requirements do not apply to the SUT.

8) Section 13.2.4.3 of UCR 2013 listed requirements for ISS systems that provide the functionality of more than one CS device in one integrate device. Note: This section is only applicable to ISSs. The SUT is a VPN; therefore, these ISS requirements do not apply to the SUT.

9) Section 13.2.4.5 of UCR 2013 provided requirements for NAC. The NAC attempts to control access to a network with policies including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. A system is composed of many elements and is not a single device. Note: This section is only applicable for NAC. The SUT is a VPN; therefore, the NAC requirements do not apply to the SUT.

7. HARDWARE/SOFTWARE/FIRMWARE VERSION IDENTIFICATION. Table 3-3 provides the SUT components' hardware, software, and firmware tested. JITC tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

8. TESTING LIMITATIONS. Attack hardware was not available for test procedures requiring replay attacks. Some attacks were simulated via crafted Ixia traffic which ensured some categories of disallowed traffic was blocked. As a result, the ability for the SUT to protect itself from attacks as well as replay attacks was not verified via testing. The vendor did assert compliance for these security features in their LoC. In addition, software clients for laptop computers were not provided for this test; therefore, software clients were not tested during this test event and are not certified for use within the DoDIN.

9. CONCLUSION(S). The SUT meets the critical interoperability requirements for a VPN IAW the UCR, Reference (b), and is certified for joint use with other products listed on the DoDIN Approved Products List (APL). The SUT is certified for use with the interfaces depicted in Table 3-1.

DATA TABLES

Table 3-1. SUT Interface Status

Interface (See note 1.)	Applicability: (R), (O), (C) VPN	Status	Remarks
Network Management Interfaces (See note 2.)			
10 Mbps	C	Not Tested (See note 3.)	IAW IEEE 802.3i or 802.3j.
100 Mbps	C	Met	IAW IEEE 802.3u
1000 Mbps	C	Met	IAW IEEE 802.3ab or 802.3z
Serial (EIA/TIA)	C	Met	
Network Interfaces (See note 4.)			
10 Mbps	C	Met	IAW IEEE 802.3i or 802.3j
100 Mbps	C	Met	IAW IEEE 802.3u
1000 Mbps	C	Met	IAW IEEE 802.3ab or 802.3z
10 Gbps	O	Not Tested (See note 3.)	IAW IEEE 802.3ae or 802.3an.
25 Gbps	O	Met	IAW IEEE 802.3by-2016
40/100 Gbps	O	Met	IAW IEEE 802.3ba or 802.3bm
2.5/5 Gbps	O	Not Tested (See note 3.)	IAW IEEE 802.3bz.

NOTE(S):
1. The UCR 2013 Change 2, Section 13, does not identify individual interface requirements for security devices. The SUT must minimally provide Ethernet interfaces that meet the requirements in Section 2.7.1.
2. The SUT shall provide at least one of the specified management interfaces.
3. The SUT does not support this conditional or optional interface.
4. The SUT shall support at least of the wired network interfaces (802.3).

LEGEND:

802.3ab	1000BaseT Gbps Ethernet over twisted pair	C	Conditional
802.3ae	10 Gbps Ethernet	CSMA	Carrier Sense Multiple Access
802.3an	10 GBaseT Ethernet over unshielded twisted	EIA	Electronic Industries Alliance
802.3ba	40/100 Gbps Ethernet	Gbps	Gigabits per second
802.3bm	40/100 Gbps Ethernet for Optical Fiber	GBaseT	Gigabit (Baseband Operation, Twisted Pair) Ethernet
802.3bz	2.5/5 GBaseT over twisted pair	IAW	In accordance with
802.3i	10BaseT Mbps over twisted pair	IEEE	Institute of Electrical and Electronics Engineers
802.3j	10BaseF over Fiber-Optic	Mbps	Megabits per second
802.3u	Standard for CSMA with collision detection at 100 Mbps	O	Optional
802.3by	25 Gbps Ethernet Standard twisted pair	R	Required
802.3z	Gigabit Ethernet Standard	SUT	System Under Test
BaseF	Megabit Ethernet over fiber	TIA	Telecommunications Industry Association
BaseT	Megabit (Baseband Operation, Twisted Pair) Ethernet	VPN	Virtual Private Network

Table 3-2. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/ Function	Applicability (See note 1.)	UCR 2013 Change 2 Reference	Status
1	**Cybersecurity Requirements**		See note 2.	Met
2	**Internet Protocol Version 6 Requirements**			
	Product Requirements	R	5.2.1	Met
	Mapping of RFCs to DoDIN Profile Categories	R	5.2.2	Met
3	**Security Device Requirements**			
	Conformance	R	13.2.1	Partially Met (See note 3.)
	General	R	13.2.2	Met
	Performance	R	13.2.3	Partially Met (See note 4.)
	Functionality	R	13.2.4	Met
	FW/VPN	R	13.2.4.1	Met
	IPS	R	13.2.4.2	Not Tested (See note 5.)
	ISS	R	13.2.4.3	Not Tested (See note 6.)
	NAC	R	13.2.4.5	Not Tested (See note 7.)

NOTE(S):

1. The annotation of 'required' refers to a high-level requirement category. Refer to Appendix (c) for the applicability of each sub-requirement. The SUT does not need to provide conditional requirements. However, if a capability is provided, it must function according to the specified requirements.
2. A JITC-led Cybersecurity test team conducted Cybersecurity testing and published the results in a separate report, Reference (d).
3. The SUT met the requirements in this section with the following exception: The SUT moves VPN at 1/3rd of the published rate. DISA adjudicated this discrepancy as minor with CoF, as noted in Table 1.
4. The SUT met the requirements in this section with the following exception: The SUT cannot record the traffic at the layer at which it is created. DISA adjudicated this discrepancy as minor with CoF, as noted in Table 1.
5. The SUT is a VPN; therefore, the IPS Functionality requirements in UCR 2013, Change 2, Section 13.2.4.2, do not apply to the SUT.
6. The SUT is a VPN; therefore, the ISS requirements in UCR 2013, Change 2, Section 13.2.4.3, do not apply to the SUT.
7. The SUT is a VPN; therefore, the NAC requirements in UCR 2013, Change 2, Section 13.2.4.5, do not apply to the SUT.

LEGEND:

CoF	Condition of Fielding	ISS	Integrated Security System
CR	Capability Requirement	JITC	Joint Interoperability Test Command
DISA	Defense Information Systems Agency	NAC	Network Access Controller
DoDIN	Department of Defense Information Network	R	Required
FR	Functional Requirement	RFC	Request for Comments
FW	Firewall	SUT	System Under Test
ID	Identification	UCR	Unified Capabilities Requirements
IPS	Intrusion Prevention System	VPN	Virtual Private Network

Table 3-3. SUT Hardware/Software/Firmware Version Identification

Component (See note.)	Release	Hardware Chipset	Description
7000 and 7200 Series Gateways			
7005 7008 **7024** 7205 7210 7220 7240XM 7280	AOS 8.10	Broadcom XLP	The 7000 and 7200 Series Gateways include the 7005, 7008, 7024, 7205, 7210, 7220, 7240XM, and 7280 models. JITC tested the 7024 model under AOS 8.10. The 7000 and 7200 Series models perform the role of a VPN concentrator. They utilize the Broadcom XLP chipset, are a compact form factor of 1 Rack Unit, or less, and cover a broad range of maximum users and functional bandwidth.
9000 Series and 9200 Series Gateways			
9004 9012	AOS 8.10	Intel Atom	The 9000 and 9200 Series Gateways include the 9004, 9012, and 9240 models. JITC tested the 9004 and 9240 models under AOS 8.10. The 9000 and 9200 Series models perform the role of a VPN concentrator. The 9000 and 9012 models utilize the Intel Atom chipset. The 9240 model is a higher scale product utilizing the Intel Xeon chipset. They are a compact form factor of 1 Rack Unit, or less, and cover a broad range of maximum users and functional bandwidth.
9240		Intel Xeon	
RAP (x3)			
AP-203R **AP-203RP**	AOS 8.10	Broadcom BCM40000	The RAPs include AP-203R, AP-203RP, AP-303H, AP-314, and AP-315. JITC tested AP-203RP, AP-303H, and AP-315 under AOS 8.10. The RAPs provide secure wireless or wired and wireless connections to end users. Once provisioned, the RAP will build a secure IPsec VPN connection back to a Mobility Gateway over the Internet or untrusted network. All traffic from the end user (wired or wireless) is sent over the VPN tunnel to the Gateway and then onto the trusted network
AP-303H		Qualcomm IPQ4000	
AP-314 **AP-315**		Qualcomm IPQ8000	
Managed/Standalone Virtual Gateway	AOS 8.10	NA	Mobility Gateways (physical and virtual) are WLAN controllers and VPN concentrators that support IPsec VPN connections to RAPs as well as site-to-site IPsec VPN connections to other Mobility Gateways. The Gateways also manage the secure WLAN supported on the RAP.
	ESXi 7.0.3 (build 22348816)		
	ActivClient 7.4.1.5		
Mobility Conductor Hardware Appliance **MCR-HW-1K** MCR-HW-5K MCR-HW-10K	AOS 8.10	Intel Xeon	Mobility Conductors (physical and virtual) provide an optional way to manage Mobility Gateways. Mobility Conductors use a centralized, multi-tiered architecture. Network configurations can be made and distributed from the Mobility Conductor automatically to all managed Mobility Gateways to eliminate onsite configuration, while still allowing for site or Gateway-specific configuration items. The management connection between the Mobility Conductor and Mobility Gateway is secured with an IPsec VPN.
Mobility Conductor Virtual Conductor **MCR-VA-1K** MCR-VA-50 MCR-VA-500 MCR-VA-5K MCR-VA-10K	AOS 8.10	NA	
	ESXi 7.0.3 (build 22348816)		
	ActivClient 7.4.1.5		
Management Workstation (site-provided)	Windows 11	NA	The SUT is managed using console access with a Secure Shell (SSH) terminal session, or web GUI using HTTPS. The AOS supports using an authentication server with username/password or certificate-based authentication. The AOS Mobility Gateway devices can be managed directly, by implementing and using Mobility Conductors, or by AirWave (currently listed under tracking number 1804401). Management access is used to configure and manage AOS devices. AOS can send logs to a central syslog service.
	ActivClient 7.4.1.5		

NOTE(S): JITC tested the bolded and underlined components. The other components in the product series were not tested; however, JITC certified the other components for joint use because they utilize the same software and similar hardware as tested and certified components and analysis determined they were functionally identical for interoperability certification purposes.

(Table continues next page.)

Table 3-3. SUT Hardware/Software/Firmware Version Identification (continued)

LEGEND:			
AP	Access Point	NA	Not Applicable
AOS	Aruba Operating System	RAP	Remote Access Point
GUI	Graphical User Interface	SSH	Secure Shell
HTTPS	Hypertext Transfer Protocol Secure	SUT	System Under Test
IPsec	Internet Protocol Security	VPN	Virtual Private Network
JITC	Joint Interoperability Test Command	WLAN	Wireless Local-Area Network
MCR	Mobility Conductor	XLP	eXtreme Low Power

Table 3-4. Test Infrastructure Hardware/Software/Firmware Version Identification

System Name	Software Release	Function
Required Ancillary Equipment		
ClearPass Policy Manager	ARBAs Linux vm (arba-cppm-001v)	Public Key Infrastructure (OCSP)
NTP Server	Cisco Catalyst 9300 IOS 17.9.4a	NTPv3 Server
Active Directory	Microsoft Server 2019	Server
Kiwi Syslog Server	Microsoft Server 2019 with Kiwi Syslog Server 9.8.405	Logging
RADIUS	Cisco Identify Service Engine 3.0.1.518	Authentication
LDAPS	Windows 2016 (2 and 3)	Manage directory information services
Test Network Components		
Workstation	Windows 11	Management
Wireshark	2.0.2 (Windows)	Protocol Analyzer
Nessus Scanner	10.7.2	Vulnerability Scanner
Switch	Cisco 9500-48Y IOS-XE 17.9.4a	Switch

LEGEND:			
LDAPS	Lightweight Directory Access Protocol Secure	RADIUS	Remote Authentication Dial-In User Service
NTP/v3	Network Time Protocol/version 3	Syslog	System Log
OCSP	Online Certificate Status Protocol	vm	virtual machine