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

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **15 Aug 11**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the Cisco Systems Lightweight Access Point (LAP) 1522 and LAP 1524 Wireless Products with Release 7.0.114.76

References: (a) DOD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
(c) through (f), see Enclosure 1

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.

2. The Cisco Systems LAP 1522 and 1524, with Release 7.0.114.76, hereinafter referred to as the Systems Under Test (SUTs), are certified for joint use in the Defense Information System Network as a Wireless Local Area Network Access System (WLAS) and Wireless Access Bridge (WAB). The US Army Information Systems Engineering Command Technology Integration Center (USAISEC TIC) conducted testing using wireless requirements derived from the Unified Capabilities Requirements (UCR), Reference (c), and wireless test procedures, Reference (d). The JITC will verify the SUT's certification status during operational deployment and evaluate any new discrepancy noted in the operational environment for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of Defense Information Systems Agency (DISA) via a vendor Plan of Actions and Milestones that addresses all new critical Test Discrepancy Reports (TDRs) within 120 days of identification. No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC. This certification expires upon changes that affect interoperability, but no later than three years from the date of the Department of Defense (DoD) Unified Capabilities Approved Product List approval memorandum.

3. This certification finding is based on interoperability testing conducted by the USAISEC TIC, a DoD Component Test Lab, review of the vendor's Letters of Compliance (LoCs), and DISA Information Assurance (IA) Certification Authority recommendation. The USAISEC TIC conducted IO testing from 29 November 2010 through 07 December 2010. Review of the vendor's LoC was completed on 21 December 2010. The USAISEC TIC conducted an IA-initiated verification and validation test 21 March 2011 through 23 March 2011 to close initial IA findings. The DISA IA CA recommendation was submitted on 2 June 2011. The IA test results for these products are published in a separate report, Reference (e). The JITC certifies that the SUTs meet UCR requirements for WLAS and WAB based on a review the DoD Component Test Laboratory results submitted with USAISEC TIC certification recommendation, Reference (f). Enclosure 2

documents their test results and describes the tested network and system configurations. Enclosure 3, System Functional and Capability Requirements, lists the Capability Requirements (CR) and Functional Requirements (FR).

4. The requirements for WLASs and WABs were established by Section 5.3.1 of Reference (c) and were used to evaluate the interoperability of the SUT. Tables 1 and 2 list the interface and CR/FR interoperability status of the SUT.

Table 1. SUT Interface Interoperability Status

Interface	Critical (See note 1.)	UCR Reference	Threshold CR/FR Requirements (See note 2.)	Status	Remarks
WLAS					
802.11a	No	5.3.1.7.2.3	1, 2, 3, 5, and 7	Certified	
802.11b	No	5.3.1.7.2.3	1, 2, 3, 5, and 7	Certified	
802.11g	No	5.3.1.7.2.3	1, 2, 3, 5, and 7	Certified	
802.16	No	5.3.1.7.2.3	1, 2, 3, 5, and 7	NA	
802.3i	No	5.3.1	1, 2, 3, 5, and 7	Certified	
802.3u	No	5.3.1	1, 2, 3, 5, and 7	Certified	
802.3 z	No	5.3.1	1, 2, 3, 5, and 7	Certified	See note 3.
802.3ab	No	5.3.1	1, 2, 3, 5, and 7	Certified	See note 3.
WAB					
802.11a	No	5.3.1.7.2.3	1, 2, 3, 6, and 7	Certified	
802.11b	No	5.3.1.7.2.3	1, 2, 3, 6, and 7	Certified	
802.11g	No	5.3.1.7.2.3	1, 2, 3, 6, and 7	Certified	
802.16	No	5.3.1.7.2.3	1, 2, 3, 6, and 7	NA	
802.3i	No	5.3.1	1, 2, 3, 6, and 7	Certified	
802.3u	No	5.3.1	1, 2, 3, 6, and 7	Certified	
802.3z	No	5.3.1	1, 2, 3, 6, and 7	Certified	See note 3.
802.3ab	No	5.3.1	1, 2, 3, 6, and 7	Certified	See note 3.
WEI					
802.11a	No	5.3.1.7.2.3	1, 3, and 4	NA	Products tested did not include WEIs.
802.11b	No	5.3.1.7.2.3	1, 3, and 4	NA	
802.11g	No	5.3.1.7.2.3	1, 3, and 4	NA	
802.16	No	5.3.1.7.2.3	1, 3, and 4	NA	

NOTES:
1. The UCR does not define any minimum interfaces. The SUT must minimally provide one of the wired interfaces (to the ASLAN) and wireless interfaces (subscriber).
2. The SUT need not provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CR/FR requirements. The detailed CR/FR requirements are listed in Enclosure 3, System Functional and Capability Requirements.
3. Supported on controllers using SFP transceivers.

LEGEND:

ASLAN	Assured Services LAN	SFP	Small Form-Factor Pluggable transceiver
CR	Capability Requirement	SUT	System Under Test
FR	Functional Requirement	UCR	Unified capabilities Requirements
ID	Identification	WAB	Wireless Access Bridge
LAN	Local Area Network	WEI	Wireless End Instrument
NA	Not Applicable	WLAS	Wireless LAN Access System

Table 2. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status	Remarks
1	**General Wireless Requirements**				
	IPv6	Required	5.3.1.7.2.1	Met	See note 2.
	WiFi Certified	Required (See note 3.)	5.3.1.7.2.1	Met	See note 4.
	Redundancy	Required	5.3.1.7.2.1	Met	See note 5
	FIPS 140-2 Level 1	Required	5.3.1.7.2.1	Met	See note 4.
	Latency	Required	5.3.1.7.2.1	Met	
	Traffic Prioritization	Required	5.3.1.7.2.1	Met	
	Wireless STIGs	Required	5.3.1.7.2.1	Met	See note 6.
2	**WIDS**				
	Continuous Scanning	Required	5.3.1.7.2.2	Met	See note 7.
	Location-sensing	Required	5.3.1.7.2.2	Met	See note 7.
3	**Wireless Interface Requirements**				
	Interface Standards	Required (See note 8.)	5.3.1.7.2.3	Met	
	802.11 Interface Standards	Required (See note 9.)	5.3.1.7.2.3	Met	
	802.16 Interface Standards	Required (See note 10.)	5.3.1.7.2.3	NA	See note 11.
	Fixed / Nomadic WEIs	Required (See note 12.)	5.3.1.7.2.3	NA	See note 13.
4	**Wireless End Instruments**				
	VoIP Solution	Required (See note 14.)	5.3.1.7.2.4	NA	The SUT tested does not include WEIs.
	Access Methods	Required (See note 15.)	5.3.1.7.2.4	NA	
	Call Control Authentication	Required (See note 16.)	5.3.1.7.2.4	NA	
	Call Termination	Required (See note 12.)	5.3.1.7.2.4	NA	
5	**WLAS Requirements**				
	Loss of Call upon WLAS failure	Required (See note 16.)	5.3.1.7.2.5	Met	See note 17.
	Maximum supported EIs	Required (See note 16.)	5.3.1.7.2.5	Met	See notes 16 and 18.
	MOS	Required (See note 16.)	5.3.1.7.2.5	Met	See notes 16 and 18.
	Roaming	Required (See note 17.)	5.3.1.7.2.5	Met	See notes 17.
6	**Wireless Access Bridge**				
	Individual Interface Standards	Required (See note 9.)	5.3.1.7.2.6	Met	
	Maximum Voice Calls Transported	Required (See note 9.)	5.3.1.7.2.6	Met	See notes 16 and 18.
	Voice MOS	Required (See note 9.)	5.3.1.7.2.6	Met	See notes 16 and 18.
	E2E BER	Required (See note 9.)	5.3.1.7.2.6	Met	
	Secure Voice Transmission	Required (See note 9.)	5.3.1.7.2.6	Met	See note 19.
	Call Signaling Transport	Required (See note 9.)	5.3.1.7.2.6	Met	See note 19.
	Latency	Required (See note 9.)	5.3.1.7.2.6	Met	
	Jitter	Required (See note 9.)	5.3.1.7.2.6	Met	
	WLAS/WAB Combination	Required (See note 9.)	5.3.1.7.2.6	Met	

Table 2. SUT Capability Requirements and Functional Requirements Status (continued)

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status	Remarks
7	**ASLAN Requirements Applicable to Wireless Products**				
	General Performance Parameters	Required	5.3.1.3	Met	

NOTES:
1. The SUT need not provide wireless capability. However, if wireless capability is present, the SUT must meet the wireless requirements (as applicable for product type WLAS, WAB, or WEI) in order to be certified.
2. Vendor demonstrated IPv6 QoS and IPv6 packet transfer via Ethernet.
3. Applies to 802.11 interfaces only.
4. Verified via vendor LoC.
5. A condition of fielding is to constrain to less than 96 telephony users. Controller transitions require client re-authentication prohibiting call continuance.
6. Vendor met STIG requirements with submitted mitigations.
7. Scanning conformed via management console on Cisco WCS.
8. Individual sub-requirements apply to specific interface types.
9. Applies to 802.11 interfaces only.
10. Applies to 802.16 interfaces only.
11. SUT does not provide an 802.16 (conditional) interface.
12. Applies to WEIs; not applicable to WLASs or WABs.
13. SUT does not include WEIs.
14. The WEI is certified in conjunction with a call-control agent (VoIP solution).
15. The WEI may be dedicated service (single traffic type) or shared service (voice, video, and data).
16. Specified requirements are applicable to WLAS products only.
17. Verified via emulated phone (Ixia).
18. The SUT supports the ability to limit the number of subscribers, thereby controlling the number of voice subscribers.
19. The USAISEC TIC did not test with secure instruments. This requirement was deemed to be met through use of test equipment to send emulated traffic.

LEGEND:

802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz
802.16	IEEE series of wireless broadband standards
BER	Bit Error Rate
CR	Capability Requirement
E2E	End-to-end
EIs	End Instruments
FIPS	Federal Information Processing Standard
FR	Functional Requirement
GHz	Gigahertz
IEEE	Institute of Electrical and Electronics Engineers
IPv6	Internet Protocol version 6
LAN	Local Area Network
MOS	Mean Opinion Score
STIG	Security Technical Implementation Guide
SUT	System Under Test
UCR	Unified Capabilities Requirements
VoIP	Voice over Internet Protocol
WAB	Wireless Access Bridge
WEI	Wireless End Instrument
WIDS	Wireless Intrusion Detection System
WiFi	Wireless Fidelity, trademark of the Wi-Fi Alliance that refers to a range of connectivity technologies, including WLAN
WLAN	Wireless LAN
WLAS	Wireless LAN Access System

5. In accordance with the Program Manager's request, the JITC did not prepare a detailed test report. The JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Non-secure Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet). Information related to Defense Switched Network (DSN) testing is on the Telecom Switched Services Interoperability website at http://jitc.fhu.disa.mil/tssi. All associated data is available on the Defense Information Systems

JITC Memo, JTE, Special Interoperability Test Certification of the Cisco Systems Lightweight Access Point (LAP) 1522 and LAP 1524 Wireless Products with Release 7.0.114.76

Agency Unified Capability Coordination Office (UCCO) website located at http://www.disa.mil/ucco/.

6. The JITC point of contact is Ms. Jacquelyn Mastin, commercial 301-744-2791 or DSN 312-354-2791; e-mail address is jackie.mastin@disa.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The UCCO tracking numbers are 1019005 and 1019007.

FOR THE COMMANDER:

3 Enclosures a/s

BRADLEY A. CLARK
Chief
Battlespace Communications Portfolio

Distribution (electronic mail):
Joint Staff J-6
Joint Interoperability Test Command, Liaison, TE3/JT1
Office of Chief of Naval Operations, CNO N6F2
Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)
Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ
U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I
DOT&E, Net-Centric Systems and Naval Warfare
U.S. Coast Guard, CG-64
Defense Intelligence Agency
National Security Agency, DT
Defense Information Systems Agency, TEMC
Office of Assistant Secretary of Defense (NII)/DoD CIO
U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68
Department of the Navy, SPAWAR, Atlantic, Bldg. 179 Marsh Road, Portsmouth, Virginia 23702-2737

(This page intentionally left blank.)

ADDITIONAL REFERENCES

(c) Office of the Assistant Secretary of Defense Document, "Department of Defense Unified Capabilities Requirements 2008, Change 2," December 2010

(d) Joint Interoperability Test Command Document, "Unified Capabilities Test Plan (UCTP)," November 2009

(e) United States Army Document, "Information Assurance (IA) Finding Summary for Cisco Systems Wireless Products, Release 7.0.114.76 (UC Tracking Numbers: 1019005, 1019007)" December 2010

(f) United States Army Information Systems Engineering Command Technology Integration Center Document, "UC APL IO Certification for Cisco Systems Lightweight Access Point (LAP) 1522, 1524 Products, Release 7.0.114.76 (UC Tracking Numbers: 1019005, 1019007)," December 2010

(This page intentionally left blank.)

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Cisco Systems Lightweight Access Point (LAP) 1522 and LAP 1524 Wireless Products with Release 7.0.114.76.

2. SPONSOR. Department of the Navy, Mr. Marquis E. Sailor, US Navy Space and Naval Warfare Systems Command (SPAWAR) Atlantic, Bldg. 179 Marsh Road, Portsmouth, Virginia 23702-2737; email: marquis.sailor@navy.mil.

3. SYSTEM POC. Mr. Josh Ament, Certification Test Manager, Cisco Systems, Inc., 7025 Kit Creek Road, PO Box 14987, Research Triangle Park, NC 27709.

4. TESTER. Testing conducted at Department of Army Distributed Testing Lab, United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC TIC), ATTN: James Hatch, Fort Huachuca, Arizona 85613; email: James.Hatch@us.army.mil

5. SYSTEM DESCRIPTION. Wireless Local Area Network (WLAN) implementations are considered extensions of the Local Area Network (LAN) physical layer. The Unified Capabilities Requirements (UCR) defines three wireless products: Wireless End Instruments (WEIs), Wireless LAN Access Systems (WLASs), and Wireless Access Bridges (WABs). The Cisco Systems LAP 1522 and LAP 1524 with Release 7.0.114.76, ereinafter referred to as the System under Test (SUT), provides the following wireless capabilities.

Cisco Wireless products unite the wired and wireless networks to provide a secure, scalable, and manageable platform for mobility services. This network integration enables unified security policies, intrusion prevention, Quality of Service (QoS), and location services. To administer wireless network resources, Cisco Wireless uses lightweight access points which are wirelessly-connected mesh access points associated to a Cisco Wireless Control System.

The authorized system management interface uses secure, web-based interactions, provided through the documented Apache Tomcat web server integrated in the Cisco Wireless Control System (WCS) management software. Administrators access the WCS via Secure Sockets Layer (SSL) network transactions. This management method satisfactorily addresses the security concerns detailed in the related IA report.

The WCS is the enterprise management console which parses out committed changes to affiliated Wireless LAN Controllers (WLCs) via the Simple Network Management Protocol (SNMP), Version 2c or 3.

Direct management of the WLCs is not authorized or recommended. Please refer to the IA concerns detailed in the related IA report. Use of the WCS for network management is the security mitigation.

The WLC secures all management of the access points (APs) via the Federal Information Processing Standards (FIPS)-certified Advanced Encryption Standard (AES) Datagram Transport Layer Security (DTLS) Control and Provisioning of Wireless Access Points (CAPWAP) management channel.

The SUTs are comprised of the following components:

a. The Cisco 4400 Series Wireless LAN Controllers are designed for medium-to-large enterprise facilities. The Cisco 4402 model has two Gigabit Ethernet (GbE) ports and is available in configurations that support 12, 25, and 50 access points.

b. The Cisco 4404 model has four GbE ports supporting 100 access points.

c. The Cisco 5508 model has eight GbE ports supporting 500 access points.

d. The Cisco Wireless Services Module (WiSM) integrates into Cisco Catalyst® 6500 Series and Cisco 7600 Series platforms. It communicates using the Lightweight Access Point Protocol (LWAPP) standard, establishing secure connectivity between access points and modules across Layer 3 networks. This protocol enables the automation of important WLAN configuration and management functions. The WiSM supports up to 300 access points.

e. The Cisco 3300 series mobility services engine (MSE) incorporates the Cisco Adaptive Wireless Intrusion Prevention System (wIPS) software. This wIPS performs rogue access point, rogue client, and ad-hoc connection detection and mitigation. It provides wireless security management and reporting information to the Wireless Control System (WCS). Use of the MSE with the WCS coordinates wIPS capabilities for scalable consistent wIPS features across the managed network. The MSE also provides location tracking and history for all Wi-Fi devices to the WCS. When used in conjunction with Cisco CleanAir APs it can specify the location of all Wi-Fi interferers.

f. The Cisco WCS supports WLAN design, radio frequency (RF) management, location tracking, intrusion protection systems, WLAN system configuration, monitoring, and management. It manages multiple WLAN controllers and their associated access points. This software package, installed on Microsoft Server 2003 for testing, provides features for detailed trending and analysis reports supporting network operations. The Cisco WCS provides network administrators the ability for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and WLAN system management.

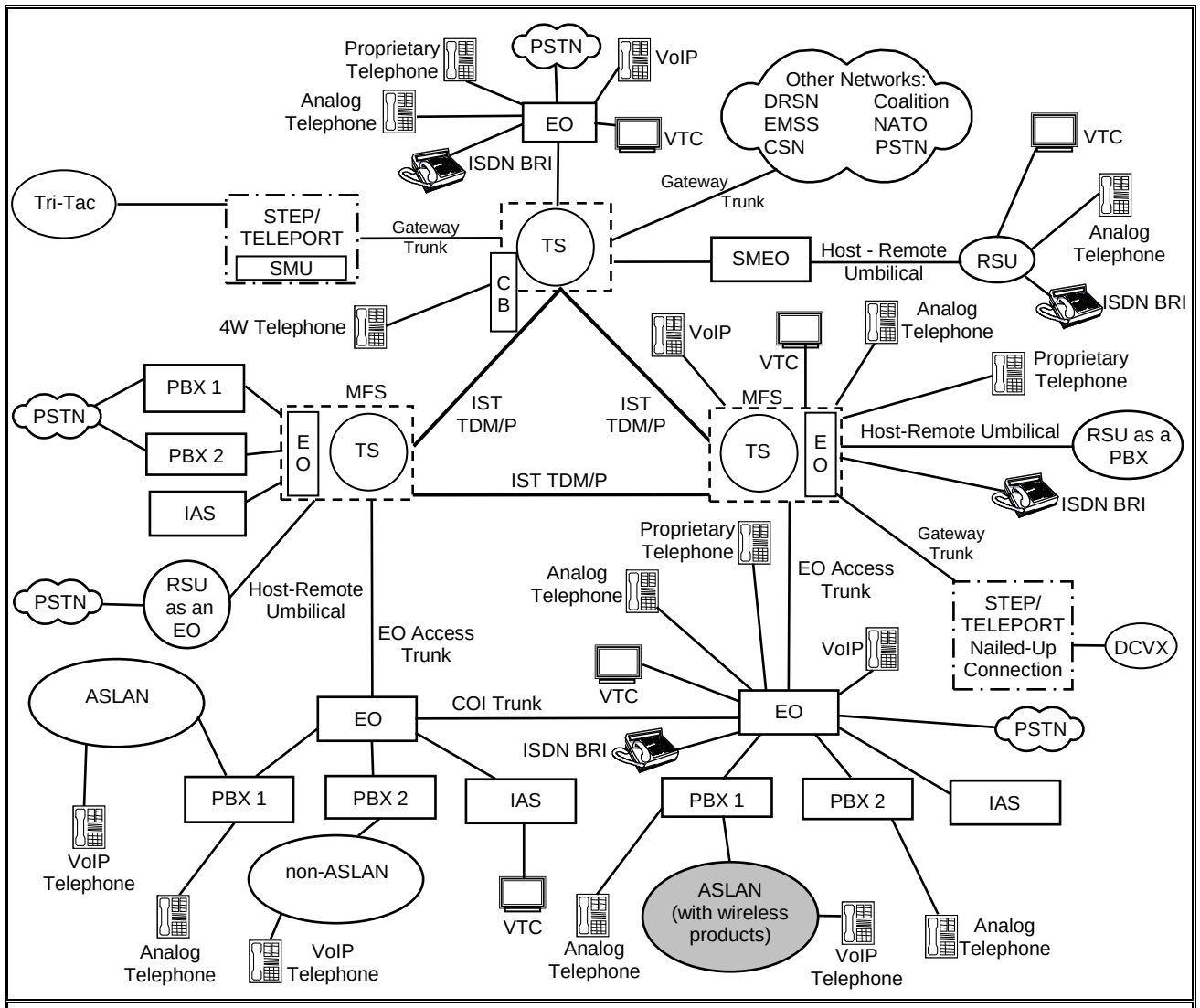
g. Lightweight Access Points (LAPs):

(1) The LAP 1524 Cisco Aironet AP offers secure, manageable wireless connectivity. This unit is Wi-Fi-certified for interoperability with a variety of wireless client devices. It supports Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g connectivity for indoor and outdoor environments. This AP has six, N-type

external antenna connectors which support 2.4- and 5-GHz antennas.

(2) The LAP 1522 Cisco Aironet AP offers secure, manageable wireless connectivity. This unit is Wi-Fi-certified for interoperability with a variety of wireless client devices. It supports Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g connectivity for indoor and outdoor environments. This AP has six, N-type external antenna connectors which support 2.4- and 5-GHz antennas.

6. OPERATIONAL ARCHITECTURE. The UCR DSN architecture in Figure 2-1 depicts the relationship of the SUTs to the DSN.



LEGEND:

4W	4-Wire	NATO	North Atlantic Treaty Organization
ASLAN	Assured Services Local Area Network	PBX	Private Branch Exchange
BRI	Basic Rate Interface	PBX 1	Private Branch Exchange 1
CB	Channel Bank	PBX 2	Private Branch Exchange 2
COI	Community of Interest	PSTN	Public Switched Telephone Network
CSN	Canadian Switch Network	RSU	Remote Switching Unit
DCVX	Deployable Cellular Voice Exchange	SMEO	Small End Office
DRSN	Defense Red Switch Network	SMU	Switched Multiplex Unit
DSN	Defense Switched Network	STEP	Standardized Tactical Entry Point
EMSS	Enhanced Mobile Satellite System	TDM/P	Time Division Multiplexing/Packetized
EO	End Office	Tri-Tac	Tri-Service Tactical Communications Program
IAS	Integrated Access Switch	TS	Tandem Switch
ISDN	Integrated Services Digital Network	VoIP	Voice over Internet Protocol
IST	Interswitch Trunk	VTC	Video Teleconferencing
MFS	Multifunction Switch	(oval)	System Under Test

Figure 2-1. DSN Architecture

7. INTEROPERABILITY REQUIREMENTS. The interface, Capability Requirements (CR), Functional Requirements (FR), Information Assurance (IA), and other requirements for wireless products are established by Section 5.3.1 of the Department of Defense Unified Capabilities Requirements 2008 (UCR 2008), Change 2, December 2010.

7.1 Interfaces. Wireless products connect to the Assured Services Local Area Network (ASLAN) infrastructure and other wireless devices (voice, video, and data). The threshold requirements for interfaces specific to the wireless products are listed in Table 2-1.

Table 2-1. Wireless Interface Requirements

Interface	Critical (See note 1.)	UCR Reference	Threshold CR/FR Requirements (See note 2.)	Criteria	Remarks
Wireless LAN Access System (WLAS)					
802.11a	No	5.3.1.7.2.3	1, 2, 3, and 5	Meets minimum CR/FRs and 802.11 interface standards.	Provides wireless subscriber access.
802.11b	No	5.3.1.7.2.3	1, 2, 3, and 5		
802.11g	No	5.3.1.7.2.3	1, 2, 3, and 5		
802.16	No	5.3.1.7.2.3	1, 2, 3, and 5	Meets minimum CR/FRs and 802.16 interface standards.	Provides wireless subscriber access.
802.3i	No	5.3.1	1, 2, 3, and 5	Meets minimum CR/FRs and 802.3 interface standards.	Provides wired ASLAN access and NM interface.
802.3u	No	5.3.1	1, 2, 3, and 5		
802.3 z	No	5.3.1	1, 2, 3, and 5		
802.3ab	No	5.3.1	1, 2, 3, and 5		
Wireless Access Bridge (WAB)					
802.11a	No	5.3.1.7.2.3	1, 2, 3, and 6	Meets minimum CR/FRs and 802.11 interface standards.	Provides wireless subscriber access.
802.11b	No	5.3.1.7.2.3	1, 2, 3, and 6		
802.11g	No	5.3.1.7.2.3	1, 2, 3, and 6		
802.16	No	5.3.1.7.2.3	1, 2, 3, and 6	Meets minimum CR/FRs and 802.16 interface standards.	Provides wireless subscriber access.
802.3i	No	5.3.1	1, 2, 3, and 6	Meets minimum CR/FRs and 802.3 interface standards.	Provides wired ASLAN access and NM interface.
802.3u	No	5.3.1	1, 2, 3, and 6		
802.3z	No	5.3.1	1, 2, 3, and 6		
802.3ab	No	5.3.1	1, 2, 3, and 6		
Wireless End Instrument WEI)					
802.11a	No	5.3.1.7.2.3	1, 3, and 4	Meets minimum CR/FRs and 802.11 interface standards.	Provides wireless subscriber access.
802.11b	No	5.3.1.7.2.3	1, 3, and 4		
802.11g	No	5.3.1.7.2.3	1, 3, and 4		
802.16	No	5.3.1.7.2.3	1, 3, and 4	Meets minimum CR/FRs and 802.16 interface standards.	Provides wireless subscriber access.

Table 2-1. Wireless Interface Requirements (continued)

NOTES:
1. "Required definition" means "conditionally required." The SUT need not provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CR/FR requirements.
2. The detailed CR/FR requirements are listed in Enclosure 3, System Functional and Capability Requirements.
3. The UCR references for each CR/FR are listed in Enclosure 3.

LEGEND:

ASLAN	Assured Services Local Area Network	UCR	Unified capabilities Requirements
CR	Capability Requirement	WAB	Wireless Access Bridge
FR	Functional Requirement	WEI	Wireless End Instrument
ID	Identification	WLAS	Wireless Local Area Network Access System
NA	Not Applicable	Y	Yes
SUT	System Under Test		

7.2 Capability Requirements (CR) and Functional Requirements (FR). Wireless products have required and conditional features and capabilities that are established by Section 5.3.1.7.2 of the UCR. The SUT does not need to provide non-critical (conditional) features and capabilities. If present, however, they must function according to the specified requirements. The wireless products' features, capabilities, and associated requirements are listed in Table 2-2. Detailed CR/FR requirements are provided in Table 3-1 of the System Functional and Capability Requirements.

Table 2-2. Wireless Capability Requirements and Functional Requirements

CR/FR ID	Capability/ Function	Applicability (See note 1.)	UCR Reference	Criteria	Remarks
1	**General Wireless Requirements**				
	IPv6	Required	5.3.1.7.2.1	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applicability per product type (WLAS, WAB, or WEI) is provided in Table 3-1 of Enclosure 3.
	Wi-Fi Certified	Required (See note 2.)	5.3.1.7.2.1		
	Redundancy	Required	5.3.1.7.2.1		
	FIPS 140-2 Level 1	Required	5.3.1.7.2.1		
	Latency	Required	5.3.1.7.2.1		
	Traffic Prioritization	Required	5.3.1.7.2.1		
	Wireless STIGs	Required	5.3.1.7.2.1		
2	**WIDS**				
	Continuous Scanning	Required	5.3.1.7.2.2	See Table 3-1 of Enclosure 3.	Applies to WLAS and WAB products.
	Location-sensing	Required	5.3.1.7.2.2		
3	**Wireless Interface Requirements**				
	Interface Standards	Required (See note 3.)	5.3.1.7.2.3	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applicability per product type (WLAS, WAB, or WEI) is provided in Table 3-1 of Enclosure 3.
	802.11 Interface Standards	Required (See note 4.)	5.3.1.7.2.3		
	802.16 Interface Standards	Required (See note 5.)	5.3.1.7.2.3		
	Fixed / Nomadic WEIs	Required (See note 6.)	5.3.1.7.2.3		

Table 2-2. Wireless Capability Requirements and Functional Requirements (continued)

CR/FR ID	Capability/ Function	Applicability (See note 1.)	UCR Reference	Criteria	Remarks
4	**Wireless End Instruments**				
	VoIP Solution	Required (See note 7.)	5.3.1.7.2.4	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applicability per product type (WLAS, WAB, or WEI) is provided in Table 3-1 of Enclosure 3.
	Access Methods	Required (See note 8.)	5.3.1.7.2.4		
	Call Control Authentication	Required (See note 6.)	5.3.1.7.2.4		
	Call Termination	Required (See note 6.)	5.3.1.7.2.4		
5	**WLAS Requirements**				
	Loss of Call upon WLAS failure	Required (See note 7.)	5.3.1.7.2.5	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applies to WLAS only.
	Maximum supported EIs	Required (See note 7.)	5.3.1.7.2.5		
	MOS	Required (See note 7.)	5.3.1.7.2.5		
	Roaming	Required (See note 7.)	5.3.1.7.2.5		
6	**Wireless Access Bridge**				
	Individual Interface Standards	Required (See note 8.)	5.3.1.7.2.6	Meet applicable UCR requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applies to WAB only.
	Maximum Voice Calls Transported	Required (See note 8.)	5.3.1.7.2.6		
	Voice MOS	Required (See note 8.)	5.3.1.7.2.6		
	E2E BER	Required (See note 8.)	5.3.1.7.2.6		
	Secure Voice Transmission	Required (See note 8.)	5.3.1.7.2.6		
	Call Signaling Transport	Required (See note 8.)	5.3.1.7.2.6		
	Latency	Required (See note 8.)	5.3.1.7.2.6		
	Jitter	Required (See note 8.)	5.3.1.7.2.6		
	WLAS/WAB Combination	Required (See note 8.)	5.3.1.7.2.6		
7	**ASLAN Requirements Applicable to Wireless Products**				
	General Performance Parameters	Required	5.3.1.3	See Table 3-1 of Enclosure 3.	

Table 2-2. Wireless Capability Requirements and Functional Requirements (continued)

NOTES:
1. Annotation of 'required' refers to high-level requirement category. Applicability of each sub-requirement is provided in enclosure 3.
2. Only applies to 802.11 interfaces.
3. Individual sub-requirements apply to specific interface types.
4. Applicable to 802.11 interfaces only.
5. Applicable to 802.16 interfaces only.
6. Applies to WEIs; not applicable to WLASs or WABs.
7. The WEI is certified in conjunction with a call-control agent (VoIP solution).
8. The WEI may be dedicated service (single traffic type) or shared service (voice, video, and data).

LEGEND:

802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz	MOS	Mean Opinion Score
802.16	IEEE series of wireless broadband standards	STIG	Security Technical Implementation Guide
ASLAN	Assured Services Local Area Network	SUT	System Under Test
BER	Bit Error Rate	UCR	Unified Capabilities Requirements
CR	Capability Requirement	VoIP	Voice over Internet Protocol
E2E	End-to-end	WAB	Wireless Access Bridge
EIs	End Instruments	WEI	Wireless End Instrument
FIPS	Federal Information Processing Standard	WIDS	Wireless Intrusion Detection System
FR	Functional Requirement	Wi-Fi	Wireless Fidelity, trademark of the Wi-Fi Alliance that refers to a range of connectivity technologies including Wireless Local Area Network
GHz	Gigahertz		
IEEE	Institute of Electrical and Electronics Engineers		
IPv6	Internet Protocol version 6	WLAS	Wireless Local Area Network Access System

7.3 Information Assurance. The IA requirements for wireless products are listed in Table 2-3 and were derived from the UCR Section 5.3.1, ASLAN Infrastructure, and UCR Section 5.4, IA Requirements.

Table 2-3. Wireless IA Requirements

Requirement	Critical (See Note.)	UCR Reference
Wi-Fi Alliance Certified (802.11 only)	Yes	5.3.1.7.2.1
FIPS 140-2 Level 1/2	Yes	5.3.1.7.2.1
Wireless STIG Requirements	Yes	5.3.1.7.2.1
WIDS Monitoring	Yes	5.3.1.7.2.1
General Requirements	Yes	5.4.6.2
Authentication	Yes	5.4.6.2.1
Integrity	Yes	5.4.6.2.2
Confidentiality	Yes	5.4.6.2.3
Non-repudiation	Yes	5.4.6.2.4
Availability	Yes	5.4.6.2.5

NOTE: Not all IA requirements from the referenced UCR Section apply. Refer to Table 3-1 in Enclosure 3, System Functional and Capability Requirements, for the specific IA requirements.

LEGEND:

FIPS	Federal Information Processing Standard	UCR	Unified Capabilities Requirements
IA	Information Assurance	WIDS	Wireless Intrusion Detection System
STIG	Secure Technical Implementation Guide	Wi-Fi	Wireless Fidelity

7.4 Other. None.

8. TEST NETWORK DESCRIPTION. The SUT was tested at the USAISEC TIC in a manner and configuration similar to that of the DSN operational environment. Testing of the system's required functions and features was conducted using the test configurations depicted in Figures 2-2 through 2-5.

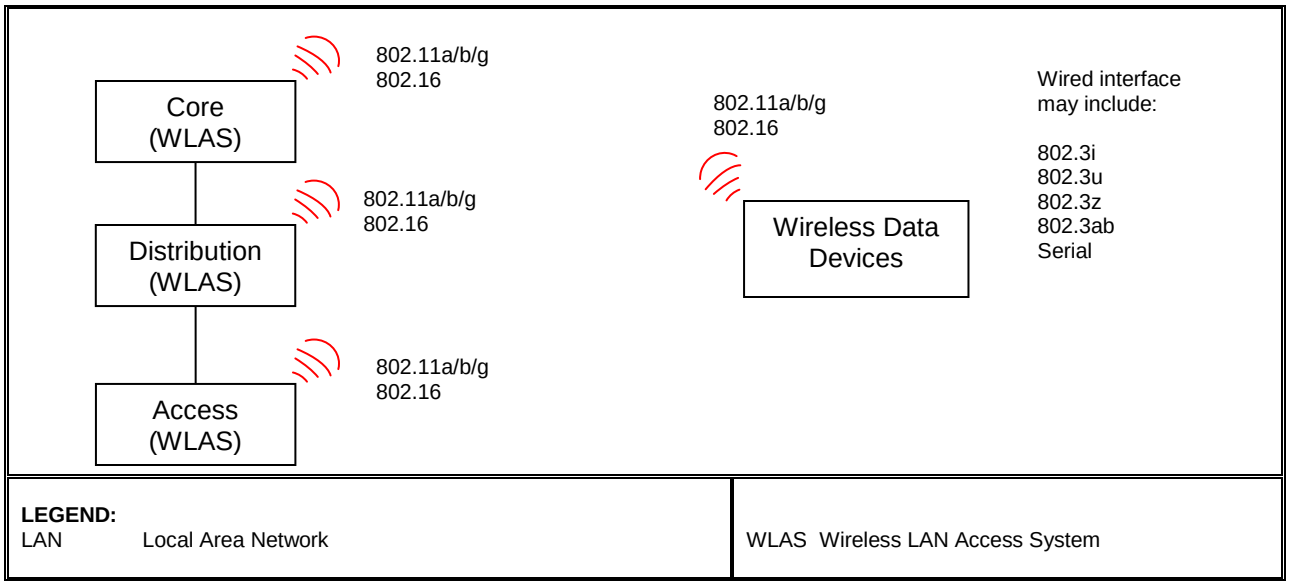


Figure 2-2. WLAS Test Configuration

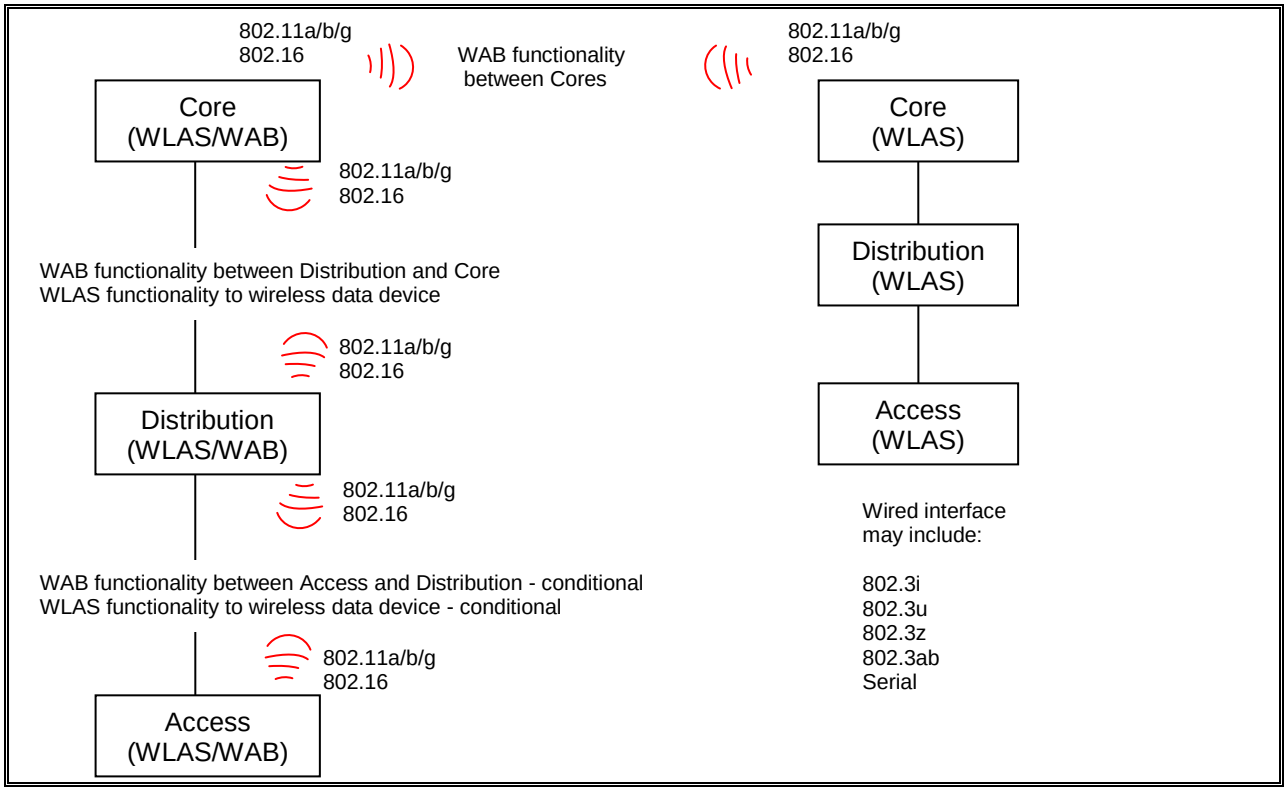
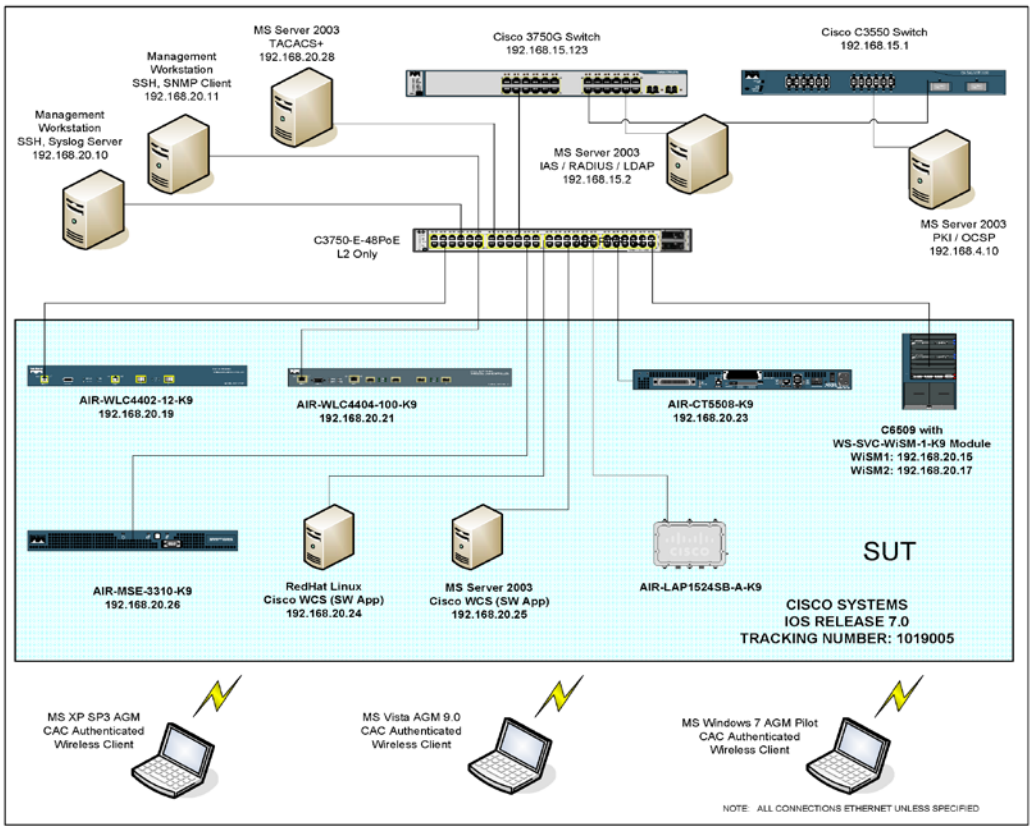


Figure 2-3. WAB Test Configuration

LEGEND:

LAN	Local Area Network	WLAS	Wireless LAN Access System
WAB	Wireless Access Bridge		

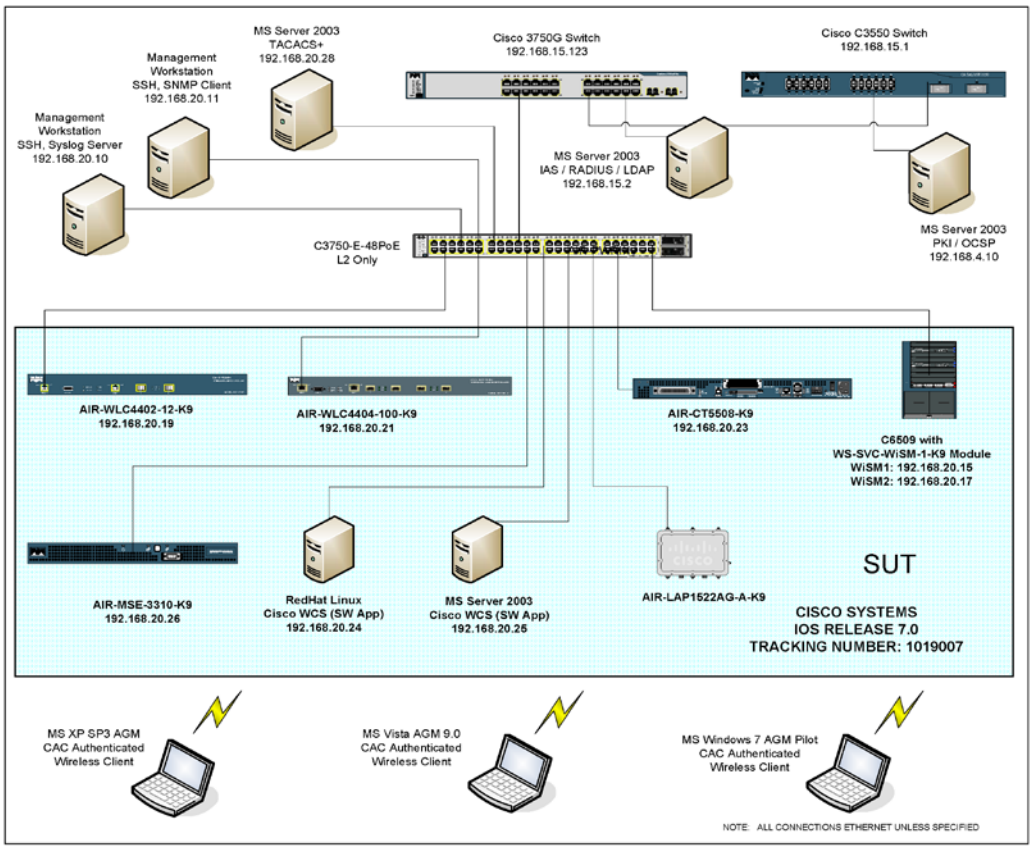
Figure 2-3. WAB Test Configuration (continued)



LEGEND:

ADDR	Address	MS	Microsoft
AGM	Army Golden Master	RADIUS	Remote Authentication Dial-in User Server
AP	Access Point	SP	Service Pack
CAC	Common Access Card	SUT	System Under Test
DHCP	Dynamic Host Configuration Protocol	SysLog	System Log
FIPS	Federal Information Processing Standards	TIC	Technology Integration Center
IAS	Internet Authentication Service	WC	Wireless Controller
LDAP	Lightweight Directory Access Protocol		

Figure 2-4. LAP 1524 Test Configuration



LEGEND:

ADDR	Address	MS	Microsoft
AGM	Army Golden Master	RADIUS	Remote Authentication Dial-in User Server
AP	Access Point	SP	Service Pack
CAC	Common Access Card	SUT	System Under Test
DHCP	Dynamic Host Configuration Protocol	SysLog	System Log
FIPS	Federal Information Processing Standards	TIC	Technology Integration Center
IAS	Internet Authentication Service	WC	Wireless Controller
LDAP	Lightweight Directory Access Protocol		

Figure 2-5. LAP 1522 Test Configuration

9. SYSTEM CONFIGURATIONS. Table 2-4 provides the system configurations and hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine its interoperability with a complement of ASLAN Infrastructure products. The ASLAN Infrastructure products listed are those used in the tested configuration. The list is not intended to identify only those ASLAN Infrastructure products that are certified for use with the SUT. The SUT is certified for use with any/all of the ASLAN Infrastructure products on the Unified Capabilities Approved Products List (UC APL).

Table 2-4. Tested System Configurations

System Name	Equipment		
Required Ancillary Equipment	Active Directory (AD)		
	Public Key Infrastructure (PKI)		
	RADIUS/TACACS+		
	SysLog Server		
Additional Equipment Needed	Management Workstation		
	LDAP Server		
System Name	**Equipment**		
	Hardware	**Cards**	**Software/Firmware**
Cisco Systems Wireless Products, Release 7.0.114.76 (Tracking Numbers: 1019005, 1019007) NOTE: The components bolded and underlined were tested. The other components in the family series were not tested; however, they utilize the same software and hardware, and analysis determined them to be functionally identical for interoperability certification purposes. They are also certified for joint use.	Cisco Systems **4402** Controller (AIR-WCL4402)	NA	7.0.114.76
	Cisco Systems **4404** Controller (AIR-WCL4404)	NA	7.0.114.76
	Cisco Systems **5508** Controller (AIR-WCL5508)	NA	7.0.114.76
	Cisco Systems **WiSM** Controller Card in C6509 (WS-SVC-WiSM)	WS-SVC-WiSM-1-K9	7.0.114.76
		Supervisor Card 720 WS-SUP720-38	
	Cisco Systems **MSE 3310** (AIR-MSE-3310)	NA	7.0.114.76
	Cisco Systems **WCS** (SW Application) (WCS)	NA	7.0.114.76
	Cisco Systems **AP 1524** (AIR-AP1524)	NA	7.0.114.76
	Cisco Systems **AP 1522** (AIR-AP1522)	NA	7.0.114.76

LEGEND:

AP	Access Point	SysLog	System Log
LC	Line Card	TACACS+	Terminal Access Controller Access Control System
LAP	Lightweight Access Point	TIC	Technology Integration Center
LDAP	Lightweight Directory Access Protocol	WC	Wireless Controller
RADIUS	Remote Authentication Dial-In User Server	WiSM	Wireless Services Module
SC	Supervisor Card	WCS	Wireless Control System

10. TESTING LIMITATIONS.

a. End instruments (EI) and DoD secure communications devices were not available to support testing and the USAISEC TIC did not conduct tests pertaining to those elements. Representative measurements were recorded in place of actual test results. These measurements indicate a link quality that is both suitably high and represents a reasonably low risk affiliated with the use of these products.

b. Testing of traffic parameters used up to 50 independent flow streams. Current test equipment licensing constrains the number of flows to 50. This level of network traffic exceeds the typical amount representative for loading an AP used in a dedicated voice network. Constraining traffic flows to this quantity represents a low risk in properly assessing the SUT's capabilities against the UCR.

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical interoperability requirements for WLAS in accordance with Section 5.3.1.7.2 of the UCR and is certified for joint use with other ASLAN Infrastructure Products listed on the UC APL. Additional discussion regarding specific testing results is contained in subsequent paragraphs.

11.1 Interfaces. The SUT's wireless interface statuses are provided in Table 2-5.

Table 2-5. Wireless Interface Requirements Status

Interface	Critical (See note 1.)	UCR Reference	Threshold CR/FR Requirements (See note 2.)	Status	Remarks
Wireless LAN Access System (WLAS)					
802.11a	No	5.3.1.7.2.3	1, 2, 3, 5, and 7	Certified	
802.11b	No	5.3.1.7.2.3	1, 2, 3, 5, and 7	Certified	
802.11g	No	5.3.1.7.2.3	1, 2, 3, 5, and 7	Certified	
802.16	No	5.3.1.7.2.3	1, 2, 3, 5, and 7	NA	
802.3i	No	5.3.1	1, 2, 3, 5, and 7	Certified	
802.3u	No	5.3.1	1, 2, 3, 5, and 7	Certified	
802.3 z	No	5.3.1	1, 2, 3, 5, and 7	Certified	See note 3.
802.3ab	No	5.3.1	1, 2, 3, 5, and 7	Certified	See note 3.
Wireless Access Bridge (WAB)					
802.11a	No	5.3.1.7.2.3	1, 2, 3, 6, and 7	Certified	
802.11b	No	5.3.1.7.2.3	1, 2, 3, 6, and 7	Certified	
802.11g	No	5.3.1.7.2.3	1, 2, 3, 6, and 7	Certified	
802.16	No	5.3.1.7.2.3	1, 2, 3, 6, and 7	NA	
802.3i	No	5.3.1	1, 2, 3, 6, and 7	Certified	
802.3u	No	5.3.1	1, 2, 3, 6, and 7	Certified	
802.3z	No	5.3.1	1, 2, 3, 6, and 7	Certified	See note 3.
802.3ab	No	5.3.1	1, 2, 3, 6, and 7	Certified	See note 3.

Table 2-5. Wireless Interface Requirements Status (continued)

Interface	Critical (See note 1.)	UCR Reference	Threshold CR/FR Requirements (See note 2.)	Status	Remarks
Wireless End Instrument (WEI)					
802.11a	No	5.3.1.7.2.3	1, 3, and 4	NA	Products tested did not include WEIs.
802.11b	No	5.3.1.7.2.3	1, 3, and 4	NA	
802.11g	No	5.3.1.7.2.3	1, 3, and 4	NA	
802.16	No	5.3.1.7.2.3	1, 3, and 4	NA	

NOTES:
1. The UCR does not define any minimum interfaces. The SUT must minimally provide one of the wired interfaces (to the ASLAN) and wireless interfaces (subscriber).
2. The SUT need not provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CR/FR requirements. The detailed CR/FR requirements are listed in Enclosure 3, System Functional and Capability Requirements.
3. The SUT does not support 802.16.
4. Supported on controllers using SFP transceivers.

LEGEND:

ASLAN	Assured Services Local Area Network	SUT	System Under Test
CR	Capability Requirement	UCR	Unified capabilities Requirements
FR	Functional Requirement	WAB	Wireless Access Bridge
NA	Not Applicable	WEI	Wireless End Instrument
SFP	Small Form-Factor Pluggable transceiver	WLAS	Wireless Local Area Network Access System

11.2 Capability Requirements (CR) and Functional Requirements (FR). The SUT's CR/FR statuses are listed in Table 2-6. The detailed CR/FR requirements are provided in Table 3-1 of the System Functional and Capability Requirements (Enclosure 3).

Table 2-6. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status	Remarks
1	**General Wireless Requirements**				
	IPv6	Required	5.3.1.7.2.1	Met	See note 2.
	WiFi Certified	Required (See note 3.)	5.3.1.7.2.1	Met	See note 4.
	Redundancy	Required	5.3.1.7.2.1	Met	See note 5.
	FIPS 140-2 Level 1	Required	5.3.1.7.2.1	Met	See note 4.
	Latency	Required	5.3.1.7.2.1	Met	
	Traffic Prioritization	Required	5.3.1.7.2.1	Met	
	Wireless STIGs	Required	5.3.1.7.2.1	Met	See note 6.
2	**WIDS**				
	Continuous Scanning	Required	5.3.1.7.2.2	Met	See note 7.
	Location-sensing	Required	5.3.1.7.2.2	Met	
3	**Wireless Interface Requirements**				
	Interface Standards	Required (See note 8.)	5.3.1.7.2.3	Met	
	802.11 Interface Standards	Required (See note 9.)	5.3.1.7.2.3	Met	
	802.16 Interface Standards	Required (See note 10.)	5.3.1.7.2.3	Not Tested	See note 11.
	Fixed/Nomadic WEIs	Required (See note 12.)	5.3.1.7.2.3	NA	See note 13.

Table 2-6. SUT Capability Requirements and Functional Requirements Status (continued)

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status	Remarks
4	**Wireless End Instruments**				
	VoIP Solution	Required (See note 14.)	5.3.1.7.2.4	NA	SUT does not include WEIs.
	Access Methods	Required (See note 15.)	5.3.1.7.2.4	NA	
	Call Control Authentication	Required (See note 14.)	5.3.1.7.2.4	NA	
	Call Termination	Required (See note 12.)	5.3.1.7.2.4	NA	
5	**WLAS Requirements**				
	Loss of Call upon WLAS Failure	Required (See note 16.)	5.3.1.7.2.5	Met	See notes 5 and 17.
	Maximum supported EIs	Required (See note 16.)	5.3.1.7.2.5	Met	See notes 17 and 18.
	MOS	Required (See note 16.)	5.3.1.7.2.5	Met	See notes 17 and 18.
	Roaming	Required (See note 16.)	5.3.1.7.2.5	Met	See note 17.
6	**Wireless Access Bridge**				
	Individual Interface Standards	Required (See note 9.)	5.3.1.7.2.6	Met	
	Maximum Voice Calls Transported	Required (See note 9.)	5.3.1.7.2.6	Met	See notes 17 and 18.
	Voice MOS	Required (See note 9.)	5.3.1.7.2.6	Met	See note 17.
	E2E BER	Required (See note 9.)	5.3.1.7.2.6	Met	See note 17.
	Secure Voice Transmission	Required (See note 9.)	5.3.1.7.2.6	Met	
	Call Signaling Transport	Required (See note 9.)	5.3.1.7.2.6	Met	
	Latency	Required (See note 9.)	5.3.1.7.2.6	Met	
	Jitter	Required (See note 9.)	5.3.1.7.2.6	Met	
	WLAS/WAB Combination	Required (See note 9.)	5.3.1.7.2.6	Met	
7	**ASLAN Requirements Applicable to Wireless Products**				
	General Performance Parameters	Required	5.3.1.3	Met	

Table 2-6. SUT Capability Requirements and Functional Requirements Status (continued)

NOTES:
1. The SUT need not provide wireless capability. However, if wireless capability is present, the SUT must meet the wireless requirements (as applicable for product type WLAS, WAB, or WEI) in order to be certified.
2. Vendor demonstrated IPv6 QoS and IPv6 packet transfer via Ethernet.
3. Only applies to 802.11 interfaces.
4. Verified via vendor LoC.
5. A condition of fielding is to constrain to less than 96 telephony users. Controller transitions require client re-authentication prohibiting call continuance.
6. Vendor met STIG requirements with submitted mitigations.
7. The SUT's scanning ability was conformed via Cisco WCS.
8. Individual sub-requirements apply to specific interface types.
9. Applicable to 802.11 interfaces only.
10. Applicable to 802.16 interfaces only.
11. SUT does not provide 802.16 (conditional) interface.
12. Applies to WEIs; not applicable to WLASs or WABs.
13. SUT does not include WEIs.
14. The WEI is certified in conjunction with a call-control agent (VoIP solution).
15. The WEI may be dedicated service (single traffic type) or shared service (voice, video, and data).
16. Specified requirements are only applicable to WLAS products.
17. Verified via emulated phone (Ixia).
18. The SUT supports the ability to limit the number of subscribers, thereby controlling number of voice subscribers.

LEGEND:

802.11	IEEE set of wireless standards in the 2.4,3.6, and 5 GHz
802.16	IEEE series of wireless broadband standards
ASLAN	Assured Services Local Area Network
BER	Bit Error Rate
CR	Capability Requirement
E2E	End-to-end
EIs	End Instruments
FIPS	Federal Information Processing Standard
FR	Functional Requirement
GHz	Gigahertz
IEEE	Institute of Electrical and Electronics Engineers
IPv6	Internet Protocol version 6
LoC	Letter of Compliance
MOS	Mean Opinion Score
QoS	Quality of Service
STIG	Security Technical Implementation Guide
SUT	System Under Test
UCR	Unified Capabilities Requirements
VoIP	Voice over Internet Protocol
WAB	Wireless Access Bridge
WCS	Wireless Control System
WEI	Wireless End Instrument
WIDS	Wireless Intrusion Detection System
Wi-Fi	Wireless Fidelity, trademark of the Wi-Fi Alliance that refers to a range of connectivity technologies including Wireless Local Area Network
WLAS	Wireless Local Area Network Access System

a. General Wireless Requirements

(1) Internet Protocol Version 6 (IPv6). The SUT WLAS (Figure 2-2) test configuration was used to investigate this requirement. Network testing confirms IPv6 packets are allowed to traverse the SUT in both WLAS and WAB configurations without issue. Tests conducted used the Ixia 250 test set and (wired and wireless) clients with LINUX operating systems connected at various locations to confirm the Layer 2 transport of the IPv6 packets. Since the SUT operates at an Open System Interconnection (OSI) Layer 2 level, all properly formatted Ethernet frames may traverse the system.

(2) Redundancy. The SUT WLAS (Figure 2-2) test configuration was used to confirm this requirement. The SUT supports wireless controller failover between primary and subordinate controllers. Testers confirmed that each wireless controller

listed was involved in a failed state and was also the responsible recovery unit. Similarly, testers confirmed all the SUT APs listed support failover recovery. AP and controller failovers are rapid and consistent. Testers confirmed assessment by observing a brief 1 ~ 2 Internet Control Message Protocol (ICMP) Ping interruption on the wireless clients pinging to other network entities. (Note: The Ping rate is one per second).

(3) Redundancy. The SUT supports wireless controller failover between primary and subordinate controllers. Testers confirmed that each wireless controller listed was involved in a failed state and was also the responsible recovery unit. Similarly, testers confirmed all the SUT APs listed support failover recovery. AP and controller failovers are rapid and consistent. Testers confirmed assessment by observing a brief 1 ~ 2 Internet Control Message Protocol (ICMP) Ping interruption on the wireless clients pinging to other network entities. (Note: The Ping rate is one per second).

(4) FIPS 140-2. FIPS 140-2. All wireless connections shall be FIPS 140-2 Level 1 certified (connections may either be WEI to WLAS if both support FIPS 140-2 Level 1, or WEI to a FIPS 140-2 compliant product through a WLAS if the WLAS is not capable of FIPS 140-2 Level 1). Wireless products that comprise the WLAN shall be secured in accordance with their wireless security profile. The SUT is Level 1 certified.

(5) Latency. The SUT WLAS (Figure 2-2) test configuration was used to confirm this requirement. Latency measurements for the SUT WLAS were measured at 2 milliseconds (ms), under optimal environmental conditions, when using the Ixia Performance Endpoints (software agents installed on wireless clients reporting back to the Ixia 250 test set).

(6) Traffic Prioritization. The SUT WLAS (Figure 2-2) test configuration was used to confirm this requirement. A suitable test environment was not available to assess fully the traffic prioritization features of the SUT. It is technically challenging to create a contention state adequate for the SUT to enforce traffic policing and shaping, given operations in the wireless RF domain. The 802.11 wireless protocols operate in a shared medium, half-duplex mode, regulating client access, thus mitigating wireless traffic contention. Testers confirmed the suitable transport of all appropriately marked Differentiated Services Code Point (DSCP) traffic types traversing the SUT in each test configuration at various network ingress and egress points. All encoded DSCP tags traversed the SUT properly in each test configuration. Testers used both the Ixia 250 test set and (wired and wireless) LINUX clients attached at various network ingress and egress points confirming appropriate traffic capabilities.

(7) Wireless STIG. The SUT meets Wireless STIG requirements with mitigations, as detailed in the IA Findings report for this UC submission.

b. WIDS Requirements. The Army IA APL testing in August 2009 confirmed Wireless Intrusion Detection System (WIDS) capabilities with the WCS for:

(1) Continuous Scanning.

(2) Location-Sensing WIDS.

c. Wireless Interface Requirements.

(1) Interfaces Supported. The SUT WLAS (Figure 2-2) test configuration was used to confirm this requirement. The SUT has current Wireless Protected Access 2 (WPA2) Certifications on file addressing the IEEE 802.11 a/b/g modes. This is also collaborated in the SUT vendor's LoC. Testers confirmed successful wireless associations and SUT interoperability with four different vendor wireless client interfaces. Tests were conducted successfully in each of the IEEE 802.11 a/b/g modes. The SUT does not support IEEE 802.16 interfaces.

(2) Standards. Tests were conducted successfully in each of the IEEE 802.11 a/b/g modes.

d. WEI Requirements. The SUT is not a WEI. Therefore, WEI requirements are not applicable.

e. WLAS Requirements.

(1) Loss of Calls. The SUT WLAS (Figure 2-2) test configuration was used to confirm this requirement. Testers successfully confirmed the SUT WLAS demonstrated the ability to maintain calls due to a failure of the WLAS (wireless controller and APs). Refer to similar testing performed in IO-3. Testers successfully confirmed Ixia performance endpoints by two methods: in conjunction with an Ixia 250 test set, and monitoring wireless client continuous ICMP Pings to various network elements.

(2) Max EIs. The SUT WLAS successfully supported 50 voice calls in accordance with the listing for Access IP Trunk Pair with a link size of 10 Megabits per second (Mbps). (Refer to UCR 2008, Table 5.3.1-10, LAN Voice over Internet Protocol (VoIP) Subscribers for Internet Protocol version 4 (IPv4) and IPv6. Testers determined the suitable product, link type, and link size to address the wireless IEEE 802.11 a/b/g interfaces properly.) Please reference the test limitations regarding EI availability and the 50-traffic-flow license constraint on the Ixia 250 test set. MOS 4.3 represents suitable operations at these loading levels. Suitably low latency, jitter, and packet loss measurements at higher traffic loading patterns confirm the trend for quality data transport using the SUT. This represents a low risk regarding the SUT's ability to support 96 simultaneous voice calls. Testers confirmed the test measurements were recorded using each of the wireless controllers and APs.

(3) Mean Opinion Score (MOS). The SUT WLAS successfully supported a MOS = 4.3 with 50 voice calls in accordance with the listing for Access IP Trunk Pair with a link size of 10 Mbps. Testers determined the suitable product, link type, and link size to address the wireless IEEE 802.11 a/b/g interfaces properly.

(4) Roaming Calls. The SUT successfully sustained calls during transitions between APs.

f. WAB Requirements.

(1) Interfaces. The SUT has current WPA2 Certifications on file addressing the IEEE 802.11 a/b/g. This is also collaborated in the SUT vendor's LoC. Testers confirmed successful wireless associations and SUT interoperability with four different vendor wireless client interfaces. Tests were conducted successfully in each of the IEEE 802.11 a/b/g modes.

(2) Max Voice Calls. The SUT WAB successfully supported 50 voice calls in accordance with the listing for Access IP Trunk Pair with a link size of 10 Mbps. (Refer to UCR 2008, Table 5.3.1-10, LAN VoIP Subscribers for IPv4 and IPv6. Testers determined the suitable product, link type, and link size to address the wireless IEEE 802.11 a/b/g interfaces properly.) Please reference the test limitations regarding EI availability and the 50-traffic-flow license constraint on the Ixia 250 test set. MOS 4.3 represents suitable operations at these loading levels. Suitably low latency, jitter, and packet loss measurements at higher traffic loading patterns confirm the trend for quality data transport using the SUT. This represents a low risk regarding the SUT's ability to support 96 simultaneous voice calls. Testers confirmed the test measurements were recorded using each of the wireless controllers.

(3) Mean Opinion Score (MOS). The SUT WAB successfully supported a MOS = 4.3 with 50 voice calls in accordance with the listing for Access IP Trunk Pair with a link size of 10 Mbps. Testers determined the suitable product, link type, and link size to address the wireless IEEE 802.11 a/b/g interfaces properly.

(4) Bit error rate (BER). The SUT WAB (Figure 2-3) test configuration was used to confirm this requirement. Test equipment characterized the quality of the data transport rather than a direct BER measurement. This is representative of transport. The data loss measurements are similar to BER measurements. Test duration = 9 hours, 0.038% byte loss (5.5×10^6 byte loss out of 14.4×10^9 bytes sent).

(5) DoD Secure Communication Devices (DSCD) Transmission. DSCDs were not available to support testing. Suitably low latency, jitter, and packet loss measurements at higher traffic loading patterns confirm the trend for quality data transport using the SUT. This represents a low risk regarding the SUT's ability to support DSCD transmission.

(6) Signaling Transport. The SUT is capable of supporting transport of signaling traffic.

(7) Latency. The SUT WAB (Figure 2-3) test configuration was used to confirm this requirement. The SUT WAB supports an average One Way Delay of 3 ms.

(8) Jitter. The SUT WAB (Figure 2-3) test configuration was used to confirm this requirement. Jitter was 30µs.

(9) WLAS/WAB Combination. The SUT WAB (Figure 2-3) test configuration was used to confirm this requirement. The SUT WAB, acting simultaneously as a WLAS, met the requirement for supporting Service-Class Tagging/QoS as specified in 5.3.1.7.2.7 (1). The SUT successfully transported the service-class-tagged traffic. All encoded DSCP tagged traffic traversed the SUT properly.

g. ASLAN Requirements Applicable to Wireless Products.

(1) The wireless products must meet the general performance parameters applicable for access devices in accordance with UCR 2008 Change 1 Section 5.3.1.3. The SUT met the appropriate requirements as detailed in the previous paragraphs for the wireless interfaces. The TIC testers verified connectivity and UCR requirements for the wired interlaces. The SUT met the requirements for 10/100/1000 Mbps wired interfaces.

11.3 Information Assurance. The IA Assessment Reports are published separately and are provided under separate cover.

11.4 Other. None.

12. TEST AND ANALYSIS REPORT. In accordance with the Program Manager's request, no detailed test report was developed. The JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System 2-7 Tracking Program (STP). The STP is accessible by .mil/.gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.

(This page left intentionally blank.)

SYSTEM FUNCTIONAL AND CAPABILITY REQUIREMENTS

The required and conditional features and capabilities for wireless products are established by Section 5.3.1.7.2 of the UCR. The SUT need not provide conditional features and capabilities; however, if they are present, they must function according to the specified requirements. The detailed Functional Requirements (FR) and Capability Requirements (CR) for wireless products are listed in Table 3-1.

Table 3-1. Wireless Products Capability/Functional Requirements

ID	Requirement	Reference	IO	IA	Remarks
Wireless Requirements					
1	Meet the IP requirements detailed in the DISA UCR 2008 IPv6 Requirements.	UCR 2008: 5.3.1.7.2.1 (1)	X		All TP IO-1 (see IDs 363-491)
2	802.11 wireless products must be WiFi Alliance-certified.	UCR 2008: 5.3.1.7.2.1 (2)		X	All TP IA-1
3	Wireless networks shall not be used to support special Command and Control (C2) users.	UCR 2008: 5.3.1.7.2.1 (3)	X		All TP IO-2
4	For wireless products that provide transport to more than 96 telephony users, the wireless products shall provide redundancy (single or dual).	UCR 2008: 5.3.1.7.2.1 (4)	X		WLAS/WAB TP IO-3
5	FIPS 140-2, Level 1/2	UCR 2008: 5.3.1.7.2.1 (5)		X	All Level 1 – secure room; Level 2 - open area (See ID 236-Table E-9 Test Case 342.)
6	The use of wireless in the LAN shall not increase latency by more than 10 ms above the specified maximum latency for a wired LAN.	UCR 2008: 5.3.1.7.2.1 (6)	X		All TP IO-4
7	Support LAN Traffic Prioritization: 802.11: 802.11e DSCP 802.16: 80216d and/or 802.16e.	UCR 2008: 5.3.1.7.2.1 (7)	X		All TP IO-5
8	Wireless products shall meet the WLAN security requirements as stipulated in the Wireless STIG, and all 802.11 components shall: - Use AES-CCMP using 802.11i - Implement Extensible Authentication Protocol – Transport Layer Security (EAP-TLS).	UCR 2008: 5.3.1.7.2.1 (8)		X	WLAS/WEI This requirement does not apply to connections between 802.11 WABs. TP IA-2
9	The WLAS and/or WAB wireless network shall be monitored by a Wireless Intrusion Detection System (WIDS) device under test.	UCR 2008: 5.3.1.7.2.2		X	WLAS/WAB TP IA-3
10	Wireless Interface Requirements: - All 802.11: Support 802.11e – Part 11and Amendments 6 and 8 - 802.11a: 802.11h - Part 11 and Amendment 5 - 802.16 (fixed): 802.16d or 802.16e and Amendment 2 - 802.16 (nomadic): 802.16e and Amendment 2.	UCR 2008: 5.3.1.7.2.3	X		All TP IO-6
11	WEIs shall: - Use 802.11 or 802.16 - Support dedicated or shared access method - Support authentication IAW IA - Provide telephone functionality identical to VoIP wired phone - Have a minimum certification level of FIPS 140-2, Level 1 - Have a VoIP timeout of 0-60sec; 5-sec default (VoIP Device Under Test Requirement).	UCR 2008: 5.3.1.7.2.4	X	X	WEI TP IO-7 For FIPs, see ID 236-Table E-9 Test Case 342.

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
Wireless Requirements					
12	WLAS must support: - No loss of calls for primary failover to secondary WLAS - Max EIs as defined by MOS when all telephones are off-hook simultaneously (table 5.3.1-9) - No drops of active calls when WEI roams from one WLAS to another.	UCR 2008: 5.3.1.7.2.5	X		WLAS/WEI Maximum Number of EIs allowed per WLAS, for converged or non-converged access for redundant and non-redundant WLAS; while not degrading any of the individual EIs' voice quality below the specified MOS scores for strategic and tactical situations, in an open air environment at a distance of 100 feet, except for the 5-second re-authentication as stated in item 1, (i.e., strategic MOS 4.0, strategic-to-tactical MOS 3.6, tactical-to- tactical MOS 3.2). TP IO-8
13	If the WAB supports 802.16, it must support 802.16d Part 16 or 802.16e part 16 and Amendment 2.	UCR 2008: 5.3.1.7.2.6 (1)	X		WAB TP IO-9
14	Max WAB voice calls IAW 5.3.1.7.3 Traffic engineering.	UCR 2008: 5.3.1.7.2.6 (2)	X		WAB TP IO-10
15	The introduction of a WAB(s) shall not cause the end-to-end average MOS to fall below appropriate levels (strategic 4.0, strategic-to-tactical 3.6, and tactical-to-tactical 3.2).	UCR 2008: 5.3.1.7.2.6 (3)	X		WAB As measured over any 5-minute time interval. TP IO-11
16	The introduction of a WAB(s) shall not exceed the end-to-end digital BER requirement of less than 1 error in 1x10-8 (averaged over a 9-hour period).	UCR 2008: 5.3.1.7.2.6 (4)	X		WAB TP IO-12
17	The introduction of a WAB(s) shall not degrade secure transmission for secure end products as defined in UCR 2008, Section 5.2.12.6, DOD Secure Communications Devices (DSCDs).	UCR 2008: 5.3.1.7.2.6 (5)	X		WAB TP IO-13
18	The WAB shall transport all call control signals transparently on an end-to-end basis.	UCR 2008: 5.3.1.7.2.6 (6)	X		WAB TP IO-14
19	The addition of a WAB(s) shall not cause the one-way delay measured from ingress to egress to increase by more than 3 ms for each WAB used, averaged over any 5-minute period.	UCR 2008: 5.3.1.7.2.6 (7)	X		WAB TP IO-15
20	The addition of the WAB shall not increase the LAN jitter requirements previously specified in this section.	UCR 2008: 5.3.1.7.2.6 (8)	X		WAB TP IO-16
21	WLAS/WAB combination shall support Service Class tagging/QoS. WAB may support special C2 calls, C2, C2(R), and non-C2 calls. All calls must meet other specified performance requirements for these users.	UCR 2008: 5.3.1.7.2.6	X		WLAS/WAB TP IO-17
ASLAN Requirements Applicable to Wireless Components					
22	All ASLAN Core/Data/Access (C/D/A) components must be non-blocking for a minimum of 50% rated output capacity.	UCR 2008: 5.3.1.3 (1)	X		WLAS/WAB TP IO-18
23	All ASLAN C/D/A components shall transport prioritized voice with no more than 2 ms latency.	UCR 2008: 5.3.1.3 (2)	X		WLAS/WAB Xref: IDs 6 and 19 (TPs IO-4 and IO-15)
24	All ASLAN C/D/A components shall transport prioritized voice with no more than 1 ms jitter.	UCR 2008: 5.3.1.3 (3)	X		WLAS/WAB Achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. XRef: ID 20 (TP IO-16)

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
ASLAN Requirements Applicable to Wireless Components					
25	All ASLAN C/D/A components shall transport prioritized voice with no more than 0.02 % (C/D) and 0.01% (A) packet loss.	UCR 2008: 5.3.1.3 (4)	X		WLAS/WAB Achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. TP IO-19
26	All ASLAN C/D/A components shall transport prioritized voice with a BER of no more than one (1) bit error in 10^6 bits.	UCR 2008: 5.3.1.3 (5)	X		WLAS/WAB Achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. TP IO-20
27	This test will demonstrate whether the device under test can receive alarms, policy violations, and performance issues.	UCR 2008: 5.3.1.6.4 & 5.3.2.17.3.1.5	X		WLAS/WAB TP IO-21
VoIP Device under Test Requirements Applicable to Wireless Components					
28	Support VoIP device under test Codec for WEIs (G.711 with 20 ms).	UCR 2008: 5.2.12.8.2.2	X		WEI TP IO-22
29	Support VoIP Multi-level Precedence and Pre-emption (MLPP).	UCR 2008: 5.2.12.8.2.3	X		WEI TP IO-23
30	VoIP Device under test latency 60 ms (+ 10 ms for wireless).	UCR 2008: 5.2.12.8.2.7	X		All XRef: ID 6**.** Averaged over any 5-minute period. The latency is to be measured from IP handset to egress from the VoIP device under test via a DSN trunk. TP IO-24
IA Requirements Applicable to Wireless Components ("Test case" refers to the RTS IATP test case.)					
31	The device under test shall be capable of being configured IAW all applicable DOD-approved security configuration guidelines (i.e., STIGs).	UCR 2008: 5.4.6.2 (1)		X	WLAS/WAB Table E-7, Test Case 1
32	Software patches shall only be installed if they originate from the device under test's manufacturer and are applied in accordance with the manufacturer's guidance. The device under test shall only accept automatic software updates if the software vendor cryptographically signs them.	UCR 2008: 5.4.6.2. (1.c and 1.c.1)		X	All Table E-7, Test Case 4 and 5
33	If the device under test uses public domain software, unsupported software, or other software, it shall be covered under that device under test's warranty.	UCR 2008: 5.4.6.2 (2) (Conditional)		X	All Table E-7, Test Case 6
34	The device under test shall only use open source software only if all licensing requirements are met.	UCR 2008: 5.4.6.2 (2.a)		X	All Table E-7, Test Case 7
35	The device under test shall not use mobile code technologies (e.g., Java, JavaScript, VBScript, and ActiveX) unless the mobile code technology is categorized and controlled in accordance with policy.	UCR 2008: 5.4.6.2 (3)		X	All Table E-7, Test Case 8
36	If Softphones are used in remote connectivity situations, the device under test shall be capable of supporting a VPN for Voice and Video over IP (VVoIP) traffic from the PC to the Enclave VPN access router/node. Note: The data from the PC and the VVoIP traffic from the PC Softphone must be separated into the appropriate VLANs at the earliest point in the path.	UCR 2008: 5.4.6.2 (4)		X	Conditional WEI Table E-7, Test Case 9
37	The device under test shall be capable of being located in physically secure areas.	UCR 2008: 5.4.6.2 (5)		X	WLAS/WAB Table E-7, Test Case 10

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
38	If the device under test has a speakerphone, the device under test shall be capable of disabling the speakerphone’s microphone. Note: Acceptable methods to meet this requirement include physically disabling the speakerphone or disabling the speakerphone using a configurable software parameter.	UCR 2008: 5.4.6.2 (6)		X	Conditional WEI Table E-7, Test Case 13
39	If the device under test is used in a sensitive area where National Security devices under test (NSS) are employed and/or within environments where National Security Information (NSI) is stored, processed, or transmitted, then the device under test shall be certified and accredited in accordance with the TSG 6, which is prepared by the National Telecommunications Security Working Group (NTSWG).	UCR 2008: 5.4.6.2 (7)		X	Conditional WEI Table E-7, Test Case 14
40	The device under test shall be capable of using a static IP address.	UCR 2008: 5.4.6.2 (8)	X	X	All Table E-7, Test Case 15 TP IO-25
41	If the device under test uses a Microsoft Windows-based operating system, the device under test shall support the installation and operation of the DOD-mandated Host Based Security System (HBSS) device under test.	UCR 2008: 5.4.6.2 (10)		X	Conditional WEI Table E-7, Test Case 17
42	The device under test shall be capable of displaying the latest DOD warning banners on all system management ingress ports accessed by administrators or users as part of a human-to-machine interface.	UCR 2008: 5.4.6.2.1.1 (1)		X	WLAS/WAB Table E-8, Test Case 18
43	At the first point of entry, the device under test shall have the capability to display a warning message of up to 20 lines by 80 characters (1600 characters) in length. As part of delivered software, the device under test shall be capable of providing an appropriate default message that warns against unauthorized access or use. The device under test’s banner shall be capable of being configured by authenticated and authorized personnel. The device under test shall be capable of displaying the banner to the administrator or user prior to a login attempt to the device under test.	UCR 2008: 5.4.6.2.1.1 (1.a -1.d)		X	WLAS/WAB Table E-8, Test Cases 18-22
44	The device under test shall be capable of displaying the following information upon successful access: the date and time of the administrator’s or user's last successful access to the device.	UCR 2008: 5.4.6.2.1.1 (1.f) UCR 2008: 5.4.6.2.1.1 (1.f.1)		X	WLAS/WAB Table E-8, Test Cases 25-26
45	The device under test shall be capable of displaying the number of unsuccessful attempts by that user-ID to gain access to the device under test (e.g., mistyped password) since the last successful access by that user-ID.	UCR 2008: 5.4.6.2.1.1 (1.f.2)		X	WLAS/WAB Table E-8, Test Case 27
46	The device under test shall be identified by an entity identifier that is unique within the domain of the appliance or application being connected to.	UCR 2008: 5.4.6.2.1.2 (1)		X	All Table E-8, Test Case 28
47	The device under test shall be capable of providing a primary access control method that is stronger than assigning passwords to specific actions (e.g., operations-related commands), although assigning passwords may be used to augment access control.	UCR 2008: 5.4.6.2.1.2 (1.a)		X	All Table E-8, Test Case 29
48	The device under test shall be capable of ensuring that all users and customer passwords are used in a secure manner.	UCR 2008: 5.4.6.2.1.2 (1.b)		X	WLAS/WAB Table E-8, Test Case 30
49	The device under test shall be capable of automatically suppressing or blotting out the clear text representation of a password on the data entry device.	UCR 2008: 5.4.6.2.1.2 (1.b.1)		X	All Table E-8, Test Case 31
50	The device under test shall ensure that passwords are safeguarded at the confidential level for sensitive but unclassified (SBU) devices under test.	UCR 2008: 5.4.6.2.1.2 (1.b.2)		X	All Table E-8, Test Case 32

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
51	The device under test shall be capable of storing access passwords (user and administrator) in a one-way encrypted form.	UCR 2008: 5.4.6.2.1.2 (1.b.2.a)		X	All Table E-8, Test Case 33
52	The device under test shall be capable of ensuring that passwords are not available in clear text to any user, including appropriate administrators. An appropriate administrator may be allowed to retrieve encrypted passwords. However, encrypted passwords shall not be available to any other user.	UCR 2008: 5.4.6.2.1.2 (1.b.3)		X	All Table E-8, Test Case 34
53	The device under test shall be capable of providing a mechanism for a password to be user-changeable. This mechanism shall require re-authentication of user identity.	UCR 2008: 5.4.6.2.1.2 (1.b.4)		X	All Table E-8, Test Case 35
54	The device under test shall be capable of ensuring that a new user password differs from the previous password by at least four characters.	UCR 2008: 5.4.6.2.1.2 (1.b.4.a)		X	All Table E-8, Test Case 36
55	The device under test shall be capable of having a password history to prevent password reuse. The default shall be configurable and shall be at least the past eight passwords or 180 days of password history.	UCR 2008: 5.4.6.2.1.2 (1.b.4.b)		X	All Table E-8, Test Case 37
56	After a password is assigned to a human user, when that user establishes a session for the first time, the device under test shall be capable of prompting the user to change the password and deny the session if the user does not comply.	UCR 2008: 5.4.6.2.1.2 (1.b.5)		X	WLAS/WAB Table E-8, Test Case 38
57	The device under test shall be capable of enforcing a configurable password aging interval (i.e., a password is required to be changed after a specified interval).	UCR 2008: 5.4.6.2.1.2 (1.b.6)		X	WLAS/WAB Table E-8, Test Case 39
58	The device under test shall be capable of defining a device-under-test-wide default password aging interval.	UCR 2008: 5.4.6.2.1.2 (1.b.6.a)		X	WLAS/WAB Table E-8, Test Case 40
59	If the device under test supports long-lived sessions (i.e., two signaling appliances continuously connected), the device under test shall be capable of providing the capability to set the password aging interval on a “per-user-ID” basis.	UCR 2008: 5.4.6.2.1.2 (1.b.6.b)		X	WLAS/WAB Table E-8, Test Case 41
60	The device under test shall be capable of setting the password aging interval on a “per-user-ID” basis.	UCR 2008: 5.4.6.2.1.2 (1.b.6.c)		X	WLAS/WAB Table E-8, Test Case 42
61	The device under test shall notify the user a specified period of time before the password expiration.	UCR 2008: 5.4.6.2.1.2 (1.b.6.c.i)		X	WLAS/WAB Table E-8, Test Case 42
62	The device under test shall notify the user upon password expiration but allow a specified additional number of subsequent logins within a specified time period before requiring a new password. The default for the number of subsequent logins shall not be greater than three. The default for the specified time period shall not be greater than 30 days.	UCR 2008: 5.4.6.2.1.2 (1.b.6.c.ii)		X	WLAS/WAB Table E-8, Test Case 42
63	The device under test shall not hard code the notification mechanism for password expiration to allow for variation in variables such as “early warning period,” “grace period,” and subsequent login after password expiration.	UCR 2008: 5.4.6.2.1.2 (1.b.6.c.iii)		X	WLAS/WAB Table E-8, Test Case 42
64	The device under test shall notify the user a specified period of time before the password expiration.	UCR 2008: 5.4.6.2.1.2 (1.b.6.d)		X	WLAS/WAB Table E-8, Test Case 43
65	The device under test shall notify the user upon password expiration but allow a specified additional number of subsequent logins within a specified time period before requiring a new password. The default for the number of subsequent logins shall not be greater than three. The default for the specified time period shall not be greater than 30 days.	UCR 2008: 5.4.6.2.1.2 (1.b.6.e, 1.b.6.e.1, and 1.b.6.e.2)		X	WLAS/WAB Table E-8, Test Cases 44-46
66	The device under test shall not hard code the notification mechanism for password expiration to allow for variation in variables such as “early warning period,” “grace period,” and subsequent login after password expiration.	UCR 2008: 5.4.6.2.1.2 (1.b.6.f)		X	WLAS/WAB Table E-8, Test Case 47

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
67	The device under test shall be capable of enforcing a configurable minimum period of waiting before an existing password can be updated (except for the first time update, which is required to be performed when the user logs in for the first time after being assigned a password). The default for the minimum waiting period shall be 24 hours without administrator intervention.	UCR 2008: 5.4.6.2.1.2 (1.b.7 and 1.b.7.a)		X	All Table E-8, Test Cases 48-49
68	The device under test shall be capable of ensuring that all user-entered passwords meet the following complexity requirements (so it cannot be “easily guessable”):	UCR 2008: 5.4.6.2.1.2 (1.b.8)		X	All Table E-8, Test Case 50
69	The device under test shall be capable of ensuring that all passwords including device under test security administrators, system administrators, and application administrator passwords consist of a mix of a minimum of 15 characters using at least two characters from each of the four character sets (i.e., upper-case letters, lower-case letters, numbers, and special characters).	UCR 2008: 5.4.6.2.1.2 (1.b.8.a and 1.b.8.b) & JTF-GNO Communications Tasking Order (CTO) 07-015		X	WLAS/WAB Table E-8, Test Cases 51-52
70	The device under test shall be capable of ensuring that the password does not contain, repeat, or reverse the associated user-ID.	UCR 2008: 5.4.6.2.1.2 (1.b.8.c)		X	All Table E-8, Test Case 53
71	The device under test shall be capable of ensuring that the password does not contain three of the same characters used consecutively.	UCR 2008: 5.4.6.2.1.2 (1.b.8.d)		X	All Table E-8, Test Case 54
72	The device under test shall be capable of ensuring that a "null" password is not possible.	UCR 2008: 5.4.6.2.1.2 (1.b.8.e)		X	All Table E-8, Test Case 55
73	The device-under-test-supplied passwords shall be “reasonably” resistant to brute-force password guessing attacks. The total number of device-under-test-generated passwords shall be on the same order of magnitude as the quantity that a user could generate using the rules specified for user-entered passwords.	UCR 2008: 5.4.6.2.1.2 (1.b.9, 1.b.9.a, 1.b.9.b, 1.b.9.c) (Conditional)		X	All Table E-8, Test Cases 56-59
74	The device under test shall ensure that it does not prevent a user from choosing (e.g. unknowingly) a password that is already associated with another user-ID. (Otherwise, an existing password may be divulged.)	UCR 2008: 5.4.6.2.1.2 (1.b.10)		X	All Table E-8, Test Case 60
75	The device under test shall not permit passwords to be embedded in device-under-test-defined access scripts or function keys.	UCR 2008: 5.4.6.2.1.2 (1.b.11)		X	All Table E-8, Test Case 61
76	The device under test shall have the capability to disable and enable the display of the “username of the last successful logon” feature.	UCR 2008: 5.4.6.2.1.2 (1.b.12)		X	All Table E-8, Test Case 62
77	If personal identification numbers (PINs) are used for passwords, the device under test shall have a configurable parameter for the PIN length, and the range shall be between four (4) and twenty (20) characters with a default of four (4).	UCR 2008: 5.4.6.2.1.2 (1.b.14) (Conditional)		X	All Table E-8, Test Case 64
78	If PINs are used for passwords, the device under test shall ensure that only numbers are allowed (i.e., no “#” or “*”).	UCR 2008: 5.4.6.2.1.2 (1.b.14.a) (Conditional)		X	All Table E-8, Test Case 65
79	If PINs (User-ID) are used for user identification (versus password), the device under test shall be capable of ensuring that only one individual is permitted to use an assigned PIN.	UCR 2008: 5.4.6.2.1.2 (1.c) (Conditional)		X	All Table E-8, Test Case 66
80	If PINs (User-ID) are used for user identification, the device under test shall have a configurable length between six (6) and twenty (20) characters, and the default shall be 6.	UCR 2008: 5.4.6.2.1.2 (1.c 1) (Conditional)		X	All Table E-8, Test Case 67
81	If PINs (User-ID) are used for user identification, the device under test shall only use numbers (i.e., no “#” or “*”) when assigning the PIN (User-ID).	UCR 2008: 5.4.6.2.1.2 (1.c.2) (Conditional)		X	All Table E-8, Test Case 68

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
82	The device under test shall be capable of supporting the non-ambiguity of a user-ID. This implies that the device under test shall prevent an appropriate administrator from creating (e.g., by mistake) a user-ID that already exists.	UCR 2008: 5.4.6.2.1.2 (1.d and 1.d.1)		X	All Table E-8, Test Cases 69-70
83	The device under test shall be capable of internally maintaining the identity of all user-IDs logged on at that time.	UCR 2008: 5.4.6.2.1.2 (1.e)		X	WLAS/WAB Table E-8, Test Case 71
84	The device under test shall be capable of associating a process that is invoked by a user or customer with the user-ID of that user.	UCR 2008: 5.4.6.2.1.2 (1.e.1)		X	WLAS/WAB Table E-8, Test Case 72
85	The device under test shall be capable of associating a process that is invoked by another process with the ID of the invoking process.	UCR 2008: 5.4.6.2.1.2 (1.e.2)		X	WLAS/WAB Table E-8, Test Case 73
86	The device under test shall be capable of associating autonomous processes (i.e., processes running without user or customer invocation) with an identification code (e.g., “system ownership”).	UCR 2008: 5.4.6.2.1.2 (1.e.3)		X	WLAS/WAB Table E-8, Test Case 74
87	A device under test shall have the capability to disable (as distinct from deleting) a user-ID after a configurable specified time interval if that user-ID has never been used during that time interval. This capability shall be either an autonomous disabling of the user-ID by the device under test, or an alarm/alert generated by the device under test for an appropriate administrator who then, depending on the policy, may disable the user-ID by using appropriate commands.	UCR 2008: 5.4.6.2.1.2 (1.f and 1.f.1)		X	WLAS/WAB Table E-8, Test Cases 75-76
88	A disabled login ID shall not be re-enabled by the user or another application user.	UCR 2008: 5.4.6.2.1.2 (1.f.2)		X	WLAS/WAB Table E-8, Test Case 77
89	The device under test shall have the capability to configure the default time interval for disabling a user-ID that has not been used during that time interval. The default time interval shall be 90 days. In addition to disabling the user, the device under test is capable of sending an alert to the device under test’s security administrator.	UCR 2008: 5.4.6.2.1.2 (1.g)		X	WLAS/WAB Table E-8, Test Case 78
90	The device under test shall be capable of verifying that a specified user (e.g., administrator) is only connected to the device under test a configurable number of times.	UCR 2008: 5.4.6.2.1.2 (1.h)		X	WLAS/WAB Table E-8, Test Case 79
91	Logon to the network a configurable number of times shall cause an alarm to be sent to the NMS unless an exception is granted per site policy.	UCR-2008: 5.4.6.2.1.2 (1.h.1)		X	WLAS/WAB Table E-8, Test Case 80
92	The device under test shall be capable of allowing the system security administrator to configure the number of consecutive failed logins for a user before the login procedure shall exit and end the attempted session. The number of times shall be between two and five, and the default shall be three.	UCR 2008: 5.4.6.2.1.2 (1.i)		X	All Table E-8, Test Case 81
93	The device under test shall be capable of immediately notifying the user of a failed login (i.e., “Login Failed”).	UCR 2008: 5.4.6.2.1.2 (1.i.1)		X	All Table E-8, Test Case 82
94	The device under test shall be capable of allowing a locked-out user to be re-enabled by a configurable timer or manually by an application security administrator, a system administrator, or a system security administrator. Default for the lockout duration shall be configurable, and the default shall be 60 seconds when the threshold for incorrect user-entered information has been exceeded.	UCR 2008: 5.4.6.2.1.2 (1.i.2. and 1.i.2.a)		X	All Table E-8, Test Cases 83-84
95	The device under test shall be capable of providing a mechanism to immediately notify (in real time) an appropriate administrator when the threshold for incorrect user-entered information is exceeded.	UCR 2008: 5.4.6.2.1.2 (1.i.3)		X	All Table E-8, Test Case 85
96	When the threshold for incorrect user-entered information has been exceeded, the device under test shall not, as a default arrangement, suspend the associated user-ID.	UCR 2008: 5.4.6.2.1.2 (1.i.4)		X	All Table E-8, Test Case 86

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
97	The device under test shall be capable of having different types of user roles. Note: Section 5.4.5.2.1, User Roles, defines the different types of user roles.	UCR 2008: 5.4.6.2.1.3 (1)		X	All Table E-8, Test Case 87
98	The device under test shall be capable of having at least three types of user roles: a system security administrator, a system administrator, and an application administrator.	UCR 2008: 5.4.6.2.1.3 (1.b)		X	WLAS/WAB Table E-8, Test Case 89
99	The device under test shall be capable of having at least three types of user roles: a system security administrator, a system administrator, and an application administrator.	UCR 2008: 5.4.6.2.1.3 (1.c)		X	WEI Table E-8, Test Case 90
100	The device under test shall be capable of setting the default user precedence VVoIP session origination capability as ROUTINE.	UCR 2008: 5.4.6.2.1.3 (1.d)		X	WEI Table E-8, Test Case 91
101	The device under test’s default user role shall be an application user.	UCR 2008: 5.4.6.2.1.3 (1.e)		X	WEI Table E-8, Test Case 92
102	The device under test’s default user role shall be a limited system administrator.	UCR 2008: 5.4.6.2.1.3 (1.f)		X	WLAS/WAB Table E-8, Test Case 93
103	The device under test shall be capable of working properly without Super User access privileges for any user application roles (system security administrator, system administrator, application administrator, and application user).	UCR 2008:5.4.6.2.1.3 (1.g)		X	All Table E-8, Test Case 94
104	The device under test shall support appropriate system administrator functions as “separate” from other user functions.	UCR 2008: 5.4.6.2.1.3 (1.h)		X	All Table E-8, Test Case 95
105	The security functions performed by an appropriate administrator shall be identified and documented.	UCR 2008: 5.4.6.2.1.3 (1.h.1)		X	All Table E-8, Test Case 96
106	If the ability to enable or disable the administrator’s account is an option of a device under test, the device under test shall not require that the account be enabled or activated during normal operation.	UCR 2008: 5.4.6.2.1.3 (1.h.2)		X	All Table E-8, Test Case 97
107	The Administrator shall have the capability to display all users currently logged onto the device under test.	UCR 2008: 5.4.6.2.1.3 (1.h.3); UCR 2008: 5.4.6.2.1.3 (1.h.3.a)		X	WLAS/WAB Table E-8, Test Cases 98-99
108	The Administrator shall have the capability to independently and selectively monitor (in real time) the actions of any one or more users, based on individual user identity.	UCR 2008: 5.4.6.2.1.3 (1.h.3.b)		X	WLAS/WAB Table E-8, Test Case 100
109	The Administrator shall have the capability to monitor the activities of a specific terminal, port, or network address in real time.	UCR 2008: 5.4.6.2.1.3 (1.h.3.c)		X	WLAS/WAB Table E-8, Test Case 101
110	The Administrator shall have the capability to authorize users.	UCR 2008: 5.4.6.2.1.3 (1.h.3.d)		X	WLAS/WAB Table E-8, Test Case 102
111	The Administrator shall have the capability to revoke users.	UCR 2008: 5.4.6.2.1.3 (1.h.3.e)		X	WLAS/WAB Table E-8, Test Case 103
112	The Administrator shall have the capability to lock out and restore a specific port or interface.	UCR 2008: 5.4.6.2.1.3 (1.h.3.f)		X	WLAS/WAB Table E-8, Test Case 104
113	The Administrator shall have the capability to identify all resources accessible to any specific user along with the associated privileges required to access them.	UCR 2008: 5.4.6.2.1.3 (1.h.3.g)		X	WLAS/WAB Table E-8, Test Case 105
114	The Administrator shall have the capability to deny the creation of a user-ID that is already in use.	UCR 2008: 5.4.6.2.1.3 (1.h.3.h)		X	WLAS/WAB Table E-8, Test Case 106
115	The Administrator shall have the capability to disable a user-ID after a specific period of time during which the user-ID has not been used.	UCR 2008: 5.4.6.2.1.3 (1.h.3.i)		X	WLAS/WAB Table E-8, Test Case 107
116	The Administrator shall have the capability to reinstate a disabled user-ID.	UCR 2008: 5.4.6.2.1.3 (1.h.3.j)		X	WLAS/WAB Table E-8, Test Case 108
117	The Administrator shall have the capability to delete a disabled user-ID.	UCR 2008: 5.4.6.2.1.3 (1.h.3.k)		X	WLAS/WAB Table E-8, Test Case 109
118	The Administrator shall have the capability to create or modify a password associated with a user-ID.	UCR 2008: 5.4.6.2.1.3 (1.h.3.l)		X	WLAS/WAB Table E-8, Test Case 110
119	The Administrator shall have the capability to delete a user-ID along with its password.	UCR 2008: 5.4.6.2.1.3 (1.h.3.m)		X	WLAS/WAB Table E-8, Test Case 111

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
120	The Administrator shall have the capability to define a password-aging interval.	UCR 2008: 5.4.6.2.1.3 (1.h.3.n)		X	WLAS/WAB Table E-8, Test Case 112
121	The Administrator shall have the capability to define the interval during which the user of an expired password shall be denied reusing a password.	UCR 2008: 5.4.6.2.1.3 (1.h.3.o)		X	WLAS/WAB Table E-8, Test Case 113
122	The Administrator shall have the capability to define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm.	UCR 2008: 5.4.6.2.1.3 (1.h.3.p)		X	WLAS/WAB Table E-8, Test Case 114
123	The Administrator shall have the capability to define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm.	UCR 2008: 5.4.6.2.1.3 (1.h.3.q)		X	WLAS/WAB Table E-8, Test Case 115
124	The Administrator shall have the capability to define the duration of session lock-out, which occurs when the threshold on the number of incorrect logins is exceeded.	UCR 2008: 5.4.6.2.1.3 (1.h.3.r)		X	WLAS/WAB Table E-8, Test Case 116
125	The Administrator shall have the capability to specify a customized advisory warning banner that is displayed upon valid test entry.	UCR 2008: 5.4.6.2.1.3 (1.h.3.s)		X	WLAS/WAB Table E-8, Test Case 117
126	The Administrator shall have the capability to define the duration of the time-out interval.	UCR 2008: 5.4.6.2.1.3 (1.h.3.t)		X	WLAS/WAB Table E-8, Test Case 118
127	The Administrator shall have the capability to define the privilege of a user to access a resource.	UCR 2008: 5.4.6.2.1.3 (1.h.3.u)		X	WLAS/WAB Table E-8, Test Case 119
128	The Administrator shall have the capability to define the privilege of an interface/port to be used to access a resource.	UCR 2008: 5.4.6.2.1.3 (1.h.3.v)		X	WLAS/WAB Table E-8, Test Case 120
129	The Administrator shall have the capability to permit post-collection audit analysis tools for report generation.	UCR 2008: 5.4.6.2.1.3 (1.h.3.w)		X	WLAS/WAB Table E-8, Test Case 121
130	The Administrator shall have the capability to permit the retrieval, copying, printing, or uploading of the security log.	UCR 2008: 5.4.6.2.1.3 (1.h.3.x)		X	WLAS/WAB Table E-8, Test Case 122
131	The Administrator shall have the capability to deny the ability to modify or delete the security log.	UCR 2008: 5.4.6.2.1.3 (1.h.3.y)		X	WLAS/WAB Table E-8, Test Case 123
132	The Administrator shall have the capability to provide a mechanism to specify the condition that would necessitate uploading the security log to avoid an overwrite in the buffer.	UCR 2008: 5.4.6.2.1.3 (1.h.3.z)		X	WLAS/WAB Table E-8, Test Case 124
133	The Administrator shall have the capability to provide a capability to validate the correct operation of the device under test.	UCR 2008: 5.4.6.2.1.3 (1.h.3.aa)		X	WLAS/WAB Table E-8, Test Case 125
134	The Administrator shall have the capability to provide a capability to monitor the device under test’s resources and their availabilities.	UCR 2008: 5.4.6.2.1.3 (1.h.3.bb)		X	WLAS/WAB Table E-8, Test Case 126
135	The Administrator shall have the capability to provide a capability to detect communication errors above an administrator- defined threshold.	UCR 2008: 5.4.6.2.1.3 (1.h.3.cc)		X	WLAS/WAB Table E-8, Test Case 127
136	The device under test shall only transmit passwords that are encrypted. Note: The Backbone Transport Services STIG requires that router administrative passwords are encrypted using Message Digest 5 (MD5).	UCR 2008: 5.4.6.2.1.3 (1.j)		X	WLAS/WAB Table E-8, Test Case 129
137	The device under test shall be capable of limiting user access based on a time-of-day interval (i.e., duty hours).	UCR 2008: 5.4.6.2.1.3 (1.k)		X	WLAS/WAB Table E-8, Test Case 130
138	A device under test that uses ancillary Authentication, Authorization, and Accounting (AAA) and syslog services shall do so in a secure manner.	UCR 2008: 5.4.6.2.1.4 (1) (Conditional)		X	All Table E-8, Test Case 131
139	A device under test that uses external Authentication, Authorization, and Accounting (AAA) services provided by the Diameter Base Protocol shall do so in accordance with RFC 3588.	UCR 2008:5.4.6.2.1.4 (1.a) (Conditional)		X	All Table E-8, Test Case 132
140	A device under test that acts as Diameter Agents shall be capable of being configured as Proxy Agents.	UCR 2008:5.4.6.2.1.4 (1.a.1) (Conditional)		X	All Table E-8, Test Case 133
141	A device under test that acts as Proxy Agents shall maintain session state.	UCR 2008: 5.4.6.2.1.4 (1.a.1.a) (Conditional)		X	All Table E-8, Test Case 134
142	All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field.	UCR 2008: 5.4.6.2.1.4 (1.a.2) (Conditional)		X	All Table E-8, Test Case 135

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
143	All Diameter implementations shall provide transport of their messages in accordance with the transport profile described in RFC 3539.	UCR 2008: 5.4.6.2.1.4 (1.a.3) (Conditional)		X	All Table E-8, Test Case 136
144	A device under test that uses the Extensible Authentication Protocol (EAP) within Diameter shall do so in accordance with RFC 4072.	UCR 2008: 5.4.6.2.1.4 (1.a.4) (Conditional)		X	All Table E-8, Test Case 137
145	A device under test that uses external AAA services provided by the Remote Authentication Dial In User Service (RADIUS) shall do so in accordance with RFC 2865.	UCR 2008: 5.4.6.2.1.4 (1.b) (Conditional)		X	All Table E-8, Test Case 138
146	A device under test that uses the Extensible Authentication Protocol (EAP) within RADIUS shall do so in accordance with RFC 3579.	UCR 2008: 5.4.6.2.1.4 (1.b.1) (Conditional)		X	All Table E-8, Test Case 139
147	If the device under test supports RADIUS-based accounting, it shall do so in accordance with RFC 2866.	UCR 2008: 5.4.6.2.1.4 (1.b.2) (Conditional)		X	All Table E-8, Test Case 140
148	If the device under test supports RADIUS, it shall support the use of Internet Protocol Security (IPSec) and/or TLS using non-null transforms as defined in the confidentiality section of this UCR 2008 (Section 5.4.6, Requirements).	UCR 2008: 5.4.6.2.1.4 (1.b.3) (Conditional)		X	All Table E-8, Test Case 141
149	If the device under test supports RADIUS and IPSec, it shall support the use of IKE for key management as defined in the confidentiality section of this UCR 2008 (Section 5.4.6, Requirements).	UCR 2008: 5.4.6.2.1.4 (1.b.4) (Conditional)		X	All Table E-8, Test Case 142
150	A device under test that uses external AAA services provided by the Terminal Access Controller Access Control System Plus (TACACS+) shall do so in accordance with the TACACS+ Protocol Specification 1.78 (or later).	UCR 2008: 5.4.6.2.1.4 (1.c) Conditional)		X	All Table E-8, Test Case 143
151	If the device under test supports TACACS+, it shall support the use of IPSec and/or TLS using non-null transforms as defined in the confidentiality section (Section 5.4.6, Requirements).	UCR 2008: 5.4.6.2.1.4 (1.c.1) (Conditional)		X	All Table E-8, Test Case 144
152	If the device under test supports TACACS+ and IPSec, it shall support the use of IKE for key management as defined in the confidentiality section (Section 5.4.6, Requirements).	UCR 2008: 5.4.6.2.1.4 (1.c.2) (Conditional)		X	All Table E-8, Test Case 145
153	Devices under test that use external address assignment services provided by the Dynamic Host Configuration Protocol (DHCP) shall do so in accordance with RFC 2131.	UCR 2008: 5.4.6.2.1.4 (1.d, 1.d.1, and 1.d.2) (Conditional)		X	WEI Table E-8, Test Cases146-148
154	A device under test that uses external AAA services provided by port-based network access control mechanisms shall do so in accordance with IEEE 802.1X-2004 in combination with a secure Extensible Authentication Protocol (EAP) type (EAP-TLS, EAP-TTLS, or PEAP).	UCR 2008: 5.4.6.2.1.4 (1.e) (Conditional)		X	All Table E-8, Test Case 149
155	A device under test that uses external EAP services provided by EAP shall do so in accordance with RFC 3748 and its RFC extensions.	UCR 2008: 5.4.6.2.1.4 (1.e.1) (Conditional)		X	All Table E-8, Test Case 150
156	A device under test that supports EAP as a minimum shall support authentication using shared secrets. Note: RFC 3748 requires that devices under test support Identity, Notification, NAK, and MD-5 Challenge Request/Response exchanges.	UCR 2008: 5.4.6.2.1.4 (1.e.1.a) (Conditional)		X	All Table E-8, Test Case 151
157	Devices under test that use external syslog services shall do so in accordance with RFC 3164. Devices under test that support syslog shall use UDP port 514 for the source port of the sender when using UDP for transport.	UCR 2008: 5.4.6.2.1.4 (1.f, 1.f.1-1.f.3) (Conditional)		X	WLAS/WAB Table E-8, Test Cases 152-155

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
158	If the originally-formed message has a TIMESTAMP in the HEADER , the timestamp shall be the local time of the device within its time zone. If the originally-formed message has a HOSTNAME field, it shall contain the hostname, as it knows itself. If the message does not have a hostname, the hostname field shall contain the message’s IP address. If the originally-formed message has a TAG value, it shall be the name of the program or process that generated the message.	UCR 2008: 5.4.6.2.1.4 (1.f.3.a-1.f.3.c) (Conditional)		X	WLAS/WAB Table E-8, Test Cases 156-158
159	If devices under test use TCP for the delivery of syslog events, then the device under test shall do so in accordance with the RAW profile defined in RFC 3195.	UCR 2008: 5.4.6.2.1.4 (1.f.4) (Conditional)		X	WLAS/WAB Table E-8, Test Case 159
160	The device under test shall be capable of authenticating users and appliances.	UCR 2008: 5.4.6.2.1.5 (1)		X	All Table E-8, Test Case 160
161	The device under test shall only allow authenticated users and appliances to access the device under test. The device under test shall ensure those authentication credentials are not transmitted in the “clear” (i.e., credentials shall be encrypted end-to-end).	UCR 2008: 5.4.6.2.1.5 (1.a and 1.a.1)		X	All Table E-8, Test Cases 161-162
162	The device under test shall be capable of ensuring that device under test access points that provide remote login facility also provide authentication services that are capable of utilizing authentication mechanisms that are stronger than usernames and passwords, i.e., using two factor authentication (strong authentication).	UCR 2008: 5.4.6.2.1.5 (1.a.2)		X	WLAS/WAB Table E-8, Test Case 163
163	The device under test shall be capable of authenticating the LSC using TLS (or its equivalent) (Threshold) with Public Key Infrastructure (PKI) certificates.	UCR 2008: 5.4.6.2.1.5 (1.a.4)		X	WEI Table E-8, Test Case 165
164	The device under test shall be capable of authenticating an appliance using the DOD PKI.	UCR 2008: 5.4.6.2.1.5 (1.b)		X	WLAS/WAB Table E-8, Test Case 166
165	If the device under test is Public Key Enabled (PKE), then the device under test shall use the DOD PKI certificates with the associated public key in the TLS certificate message for authenticating the appliance when using AS-SIP.	UCR 2008: 5.4.6.2.1.5 (1.b.1) (Conditional)			WEI Table E-8, Test Case 167
166	A device under test shall be capable of ensuring that user authentication for logging in, logging, and auditing of an appliance shall be at least as strong as a user-ID and the appropriate password/PIN (user-ID) entered over a previously established trusted path.	UCR 2008: 5.4.6.2.1.5 (1.c)		X	WLAS/WAB Table E-8, Test Case 169
167	The device under test shall not support ways to bypass the deployed authentication mechanism.	UCR 2008: 5.4.6.2.1.5 (1.d)		X	All Table E-8, Test Case 170
168	The device under test shall perform the entire user authentication procedure even if the user-ID entered is not valid.	UCR 2008: 5.4.6.2.1.5 (1.e)		X	All Table E-8, Test Case 171
169	The device under test shall protect (i.e., encrypt) all internal storage of authentication data to ensure confidentiality.	UCR 2008: 5.4.6.2.1.5 (1.f)		X	All Table E-8, Test Case 172
170	The device under test shall be capable of allowing users to place ROUTINE precedence and emergency calls without authentication.	UCR 2008: 5.4.6.2.1.5 (1.g)		X	WEI Table E-8, Test Case 173
171	The device under test shall only allow authenticated users to access the device under test for services above the ROUTINE precedence.	UCR 2008: 5.4.6.2.1.5 (1.h)		X	WEI Table E-8, Test Case 174
172	If the device under test uses SIP, the device under test shall use digest authentication as specified in RFC 3261 and/or with PKI certificates for authenticating user credentials to the LSC through the EI. The user authentication mechanism shall be software enabled or disabled.	UCR 2008: 5.4.6.2.1.5 (1.h.1 and 1.h.2)		X	WEI Table E-8, Test Cases 175-176
173	If the device under test is a Softphone, the device under test shall provide user authentication by presenting the CAC credentials of the user to the LSC. The device under test shall only allow an authenticated system administrator to perform configuration functions.	UCR 2008: 5.4.6.2.1.5 (1.h.2.a and .b)		X	WEI Table E-8, Test Cases 177-178

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
174	The device under test shall not display configuration information without proper authentication.	UCR 2008: 5.4.6.2.1.5 (1.i)		X	WEI Table E-8, Test Case 179
175	The device under test shall be capable of ensuring that all ports on a device under test that support operations related command inputs (e.g., SNMP SET commands) exercise strong authentication mechanisms for access control.	UCR 2008: 5.4.6.2.1.5 (1.j)		X	WLAS/WAB Table E-8, Test Case 180
176	The device under test shall be capable of ensuring that all appliances that support connection-oriented communications also support mutual authentication between the requestor and the provider.	UCR 2008: 5.4.6.2.1.5 (1.k)		X	WLAS/WAB Table E-8, Test Case 181
177	The device under test shall properly operate when auto-registration is disabled	UCR 2008: 5.4.6.2.1.5 (1.l)		X	WEI Table E-8, Test Case 182
178	The default authentication mechanism for SNMPv3 shall be HMAC-SHA-96.	UCR 2008: 5.4.6.2.1.5 (1.m)		X	WLAS/WAB Table E-8, Test Case 183
179	The device under test shall be capable of meeting the DOD Public Key Enabled (PKE) requirements for PKI-based authentication.	UCR 2008: 5.4.6.2.1.6 (1) and sub-paras (Conditional)		X	WEI Table E-8, Test Cases 184-231
180	The device under test shall be capable of providing authorization for services accessed on the device under test.	UCR 2008: 5.4.6.2.1.7 (1)		X	All Table E-8, Test Case 232
181	The device under test shall be capable of denying device under test access to any user unless identified with a user-ID and authenticated. Only authorized users shall be allowed access.	UCR 2008: 5.4.6.2.1.7 (1.a)		X	WLAS/WAB Table E-8, Test Case 233
182	The device under test shall be configured to not allow a user to access a resource unless that user’s user-ID has an appropriate privilege to access that resource.	UCR 2008: 5.4.6.2.1.7 (1.b)		X	All Table E-8, Test Case 234
183	The device under test shall be capable of regulating remote access by employing positive technical controls such as proxies and screened subnets.	UCR 2008: 5.4.6.2.1.7 (1.c)		X	WLAS/WAB Table E-8, Test Case 236
184	The device under test shall be capable of configuring proxies and screened subnets to limit access to only approved, network service classes and configured traffic levels for the authenticated users and end instruments.	UCR 2008: 5.4.6.2.1.7 (1.d)		X	WLAS/WAB Table E-8, Test Case 237
185	The device under test shall have the capability of controlling the flow of traffic across an interface to the network based on the source/destination IP address, source/destination port number, DSCP, and protocol identifier (“6 tuple”).	UCR 2008: 5.4.6.2.1.7 (1.d.1)		X	WLAS/WAB Table E-8, Test Case 238
186	The device under test shall be capable of utilizing VLANs to segregate VVoIP and data traffic. Servers requiring access to multiple VLANs shall be kept in a DMZ connected to the firewall and separating the two VLANs.	UCR 2008: 5.4.6.2.1.7 (1.d.2)		X	WLAS/WAB Table E-8, Test Case 242
187	The device under test shall be capable of supporting a minimum of five (5) distinct VLANs for VVoIP.	UCR 2008: 5.4.6.2.1.7 (1.d.2.a)		X	WLAS/WAB Table E-8, Test Case 243
188	The device under test shall be capable of ensuring that EIs (that do not contain a multi-port switch) and VVoIP appliances are only connected to switch ports with access to the VVoIP VLAN(s).	UCR 2008: 5.4.6.2.1.7 (1.d.2.b)		X	WLAS/WAB Table E-8, Test Case 244
189	If the device under test supports a data workstation, then the device under test shall be capable of supporting 802.1Q trunking to separate VVoIP and data traffic or shall have a separate NIC for the data and the VVoIP.	UCR 2008: 5.4.6.2.1.7 (1.d.2.c) (Conditional)		X	WEI Table E-8, Test Case 245
190	If the device under test supports a data workstation, then the device under test shall be capable of using separate 802.1Q VLAN tags for VVoIP and data or shall use separate NICs for the data and VVoIP interfaces.	UCR 2008: 5.4.6.2.1.7 (1.d.2.c.i) (Conditional)		X	WEI Table E-8, Test Case 245
191	If the device under test supports a data workstation, then the device under test shall be capable of routing the VVoIP and data traffic to the appropriate VLAN.	UCR 2008: 5.4.6.2.1.7 (1.d.2.c.ii) (Conditional)		X	WEI Table E-8, Test Case 245
192	The device under test shall be capable of configuring the maximum number of MAC addresses that can be dynamically configured on a given switch port (e.g., 1-3).	UCR 2008: 5.4.6.2.1.7 (1.d.2.d)		X	WLAS/WAB Table E-8, Test Case 246

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
193	The device under test shall be capable of notifying the NMS when the MAC address table’s threshold is reached to avoid an overflow.	UCR 2008: 5.4.6.2.1.7 (1.d.2.d.i)		X	WLAS/WAB Table E-8, Test Case 246
194	The device under test shall be capable of segregating soft phones to a dedicated VLAN.	UCR 2008: 5.4.6.2.1.7 (1.d.2.e)		X	WLAS/WAB Table E-8, Test Case 247
195	The device under test shall be capable of segregating flows to a dedicated VLAN.	UCR 2008: 5.4.6.2.1.7 (1.d.2.f -1.d.2.k)		X	WLAS/WAB Table E-8, Test Cases 248-253
196	The device under test shall have the capability to deploy on a dedicated IP network(s) or subnetwork(s) that utilizes address blocks that are separate from the normal data address blocks, thus allowing traffic and access control via firewalls and router ACLs.	UCR 2008: 5.4.6.2.1.7 (1.d.3)		X	WLAS/WAB Table E-8, Test Case 254
197	The device under test shall have the capability to be configured to ensure that the data network perimeter (i.e., data edge router or data perimeter firewall) blocks all external traffic destined to or sourced from the VVoIP VLANs and/or IP address space.	UCR 2008: 5.4.6.2.1.7 (1.d.3.b)		X	WLAS/WAB Table E-8, Test Case 260
198	The device under test shall have the capability to limit management appliance access to the IP addresses of appropriate workstations.	UCR 2008: 5.4.6.2.1.7 (1.d.3.c)		X	WLAS/WAB Table E-8, Test Case 261
199	If DHCP is used, the device under test shall have the capability to deploy different DHCP servers for VVoIP and non-VVoIP components, and the DHCP servers shall be located on physically diverse platforms from the routers and LAN switches.	UCR 2008: 5.4.6.2.1.7 (1.d.4) (Conditional)		X	WLAS/WAB Table E-8, Test Case 262
200	If DHCP is used, the device under test shall be capable of using 802.1X in combination with a secure EAP type (EAPTLS, EAP-TTLS, or PEAP) residing on the authentication server and within the operating device under test or application software of the EI in order to authenticate to the LAN.	UCR 2008: 5.4.6.2.1.7 (1.d.5.and .5a) (Conditional)		X	WLAS/WAB Table E-8, Test Cases 263-264
201	If 802.1X port authentication is used, the device under test shall ensure that all access ports start in unauthorized state. Note: The device under test should set AuthControlledPortControl equal to Auto mode for ports that will support VVoIP.	UCR 2008 5.4.6.2.1.7 (1.d.5.a.i) (Conditional)		X	WLAS/WAB Table E-8, Test Case 265
202	If 802.1X port authentication is used, the device under test shall ensure that reauthentication occurs every 60 minutes.	UCR 2008 5.4.6.2.1.7 (1.d.5.a.ii) (Conditional)		X	All Table E-8, Test Case 266
203	If 802.1X port authentication is used, the device under test shall also use 802.1AE and 802.1af to ensure a continuation of the authenticated relationship continues after the 802.1X authentication event to prevent parallel attacks.	UCR 2008 5.4.6.2.1.7 (1.d.5.a.iii) (Conditional)		X	All Table E-8, Test Case 267
204	The device under test’s documentation shall list all of the IP ports and protocols required by the device under test and the boundaries they transit as defined in the PPS Assurance Category Assignments List and which is maintained by DISA and is described in DODI 8551.1.	UCR 2008: 5.4.6.2.1.7 (1.e)		X	All Table E-8, Test Case 273
205	The devices under test shall not use IP ports and protocols deemed “red” as defined by the PPS Assurance Category Assignments List which is maintained by DISA and is described in DODI 8551.1.	UCR 2008: 5.4.6.2.1.7 (1.e.1)		X	All Table E-8, Test Case 274
206	The device under test that supports critical commands, operational commands, or critical objects shall be capable of establishing access privileges for these objects and commands. Critical objects include authentication data storage.	UCR 2008: 5.4.6.2.1.7 (1.f)		X	WLAS/WAB Table E-8, Test Case 275
207	The default policy on a device under test that supports operations-related or critical commands shall be capable of disallowing command issuance unless the issuer has been authenticated and authorized to use that command.	UCR 2008: 5.4.6.2.1.7 (1.f.1)		X	WLAS/WAB Table E-8, Test Case 276

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components (test cases refer to RTS IATP test case)					
208	Assigning passwords to specific actions shall not be used as a primary access method.	UCR 2008: 5.4.6.2.1.7 (1.f.1.a)		X	WLAS/WAB Table E-8, Test Case 277
209	All ports of a device under test that accepts operations-related or critical command inputs shall be capable of exercising device under test access control. This includes ports that provide direct access, dial-up access, access via a wireless interface, network access, and access via a Data Communications Channel (DCC).	UCR 2008: 5.4.6.2.1.7 (1.f.2)		X	WLAS/WAB Table E-8, Test Case 278
210	Depending on the application, if the system is to be accessed by administrative users who need to keep this access (including the fact that an access is being made) confidential from other administrative users, such as unauthorized B/P/C/S Director of Information Management (DOIM) employees (i.e., CALEA type requirements), the system shall be capable of providing a separate interface/port for such confidential access and shall be capable of ensuring that messages (including login requests) at this "special" interface/port are kept confidential from users logged on at other interfaces/ports.	UCR 2008: 5.4.6.2.1.7 (1.f.2.a)		X	WLAS/WAB Table E-8, Test Case 279
211	The device under test shall be capable of controlling access to resources over a given interface/port on the basis of privileges assigned to that interface/port.	UCR 2008: 5.4.6.2.1.7 (1.f.2.b)		X	WLAS/WAB Table E-8, Test Case 280
212	The device under test shall have the capability of monitoring the flow of traffic across an interface to the network.	UCR 2008: 5.4.6.2.1.7 (1.g)		X	WLAS/WAB Table E-8, Test Case 281
213	The NMS shall possess read-access and limited write/controlled access capabilities unless Service/agency operational command personnel are available to make changes 24X7 to all DOD IP VVoIP database tables (excluding tables associated with non-DISA controlled devices).	UCR 2008: 5.4.6.2.1.7 (1.i)		X	WLAS/WAB Table E-8, Test Case 286
214	If the device under test provides an emergency entry port (Emergency Action Interface) with device under test access control, the device under test shall have the capability to meet the requirements of using strong authentication; logging all access attempts in an audit log; and ensuring at least one, and not more than two, device under test security administrator accounts cannot be locked out due to login failures.	UCR 2008: 5.4.6.2.1.7 (1.l) (Conditional)		X	WLAS/WAB Table E-8, Test Case 290
215	The device under test shall be capable of using strong authentication.	UCR 2008: 5.4.6.2.1.7 (1.l.1)		X	WLAS/WAB Table E-8, Test Case 291
216	The device under test shall log all access attempts in an audit log.	UCR 2008: 5.4.6.2.1.7 (1.l.2)		X	WLAS/WAB Table E-8, Test Case 292
217	If the device under test provides an emergency entry port without device under test access control, then the following requirements shall be met: -The device under test emergency entry port shall recognize only those commands that perform device under test restoration (for example, from a disk) and no other operations commands. -The device under test shall generate a real-time alarm/alert when this port is used to gain access to the device under test and transmit that alarm to the appropriate NOC.	UCR 2008: 5.4.6.2.1.7 (1.m, 1.m.1, and 1.m.2) (Conditional)		X	WLAS/WAB Table E-8, Test Cases 294-296
218	The device under test shall have the capability to deny the establishment of any session via a port that is not designed to accept operations-related command inputs. For example, if the output port receives a login request, the device under test shall not respond.	UCR 2008: 5.4.6.2.1.7 (1.n)		X	WLAS/WAB Table E-8, Test Case 297
219	The device under test shall be capable of providing a time-out feature for users of the device under test.	UCR 2008: 5.4.6.2.1.7 (1.o, 1.o.1-1.o.3)		X	WLAS/WAB Table E-8, Test Cases 298-301
220	The device under test shall be capable of providing a mechanism to end a user session through a secure logoff procedure.	UCR 2008: 5.4.6.2.1.7 (1.p)		X	WLAS/WAB Table E-8, Test Case 302

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
221	The device under test shall be capable of dropping a port if a session is interrupted due to reasons such as time-out, power failure, link disconnection, etc., and the same login procedure as described above shall be required for a subsequent session request.	UCR 2008: 5.4.6.2.1.7 (1.q)		X	WLAS/WAB Table E-8, Test Case 303
222	If the device under test employs external modems to perform dial/dial-back: (1) The modem, after receiving a call from a session requester, shall disconnect the line before dialing the authorized number to reestablish the contact. (2) The dial-back shall be performed over a line different from the line over which the session request arrived at the modem. (3) A loss of power to the modem shall not cause the modem to fall back to a default password. (4) The password file in the modem shall not be readable by a user. (5) The modem shall prevent any modification of its stored configuration unless the user attempting this modification is properly authenticated and found to be authorized for this action.	UCR 2008: 5.4.6.2.1.7 (1.r, 1.r.1-1.r.5) (Conditional)		X	WLAS/WAB Table E-8, Test Cases 304-309
223	The device under test shall be capable of limiting the access to newly-created resources in conformance with the privilege of the creator of the resource. This should be the default configuration.	UCR 2008: 5.4.6.2.1.7 (1.s)		X	WLAS/WAB Table E-8, Test Case 310
224	If the application requires the device under test to provide different interfaces/ports for different functions, access to device under test resources over a given interface/port shall be controlled on the basis of privileges assigned to that interface/port.	UCR 2008: 5.4.6.2.1.7 (1.t) (Conditional)		X	WLAS/WAB Table E-8, Test Case 311
225	The device under test shall be capable of providing a level of granularity for any specified resource controlled by the device under test (to include precedence calls).	UCR 2008: 5.4.6.2.1.7 (1.u.1-1.u.8)		X	WLAS/WAB Table E-8, Test Cases 312-320
226	The device under test shall be capable of providing data and device under test integrity.	UCR 2008: 5.4.6.2.2 (1)		X	All Table E-9, Test Case 321
227	The device under test shall be capable of ensuring the integrity of signaling messages.	UCR 2008: 5.4.6.2.2 (1.a)			WEI Table E-9, Test Case 322
228	The device under test shall be capable of using TLS for providing integrity of AS-SIP messages. Note: The condition for the EI is the support of AS-SIP.	UCR 2008: 5.4.6.2.2 (1.a.1) (Conditional)		X	WEI Table E-9, Test Case 323
229	The device under test shall be capable of using HMAC-SHA1-160 with 160-bit keys.	UCR 2008: 5.4.6.2.2 (1.a.1.a) (Conditional)		X	WEI Table E-9, Test Case 324
230	If the device under test uses H.323, the system shall be capable of using H.235.1 Baseline Security Profile guidance for mutually authenticated shared keys and HMAC-SHA1-96 with 160-bit keys.	UCR 2008: 5.4.6.2.2 (1.a.2) (Conditional)		X	WEI Table E-9, Test Case 325
231	The device under test shall be capable of providing mechanisms to monitor system resources and their availabilities (e.g., overflow indication, lost messages, and buffer queues).	UCR 2008: 5.4.6.2.2 (1.d)		X	WLAS/WAB Table E-9, Test Case 335
232	The device under test shall be capable of providing mechanisms to detect communication errors (relevant to the system) above a specifiable threshold.	UCR 2008: 5.4.6.2.2 (1.e)		X	WLAS/WAB Table E-9, Test Case 336
233	The device under test shall be capable of providing data integrity of the bearer (Transport) packets.	UCR 2008: 5.4.6.2.2 (1.h)		X	WEI Table E-9, Test Case 339
234	The device under test shall be capable of using HMAC-SHA1-32 for the authentication tag, with 60-bit key length, as the default integrity mechanism for SRTP packets.	UCR 2008: 5.4.6.2.2 (1.h.1)		X	WEI Table E-9, Test Case 340
235	The device under test shall be capable of using HMAC-SHA1-80 for the authentication tag with 160-bit key length as the default integrity mechanism for SRTCP.	UCR 2008: 5.4.6.2.2 (1.h.2)		X	WEI Table E-9, Test Case 341

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
236	Devices that support remote network management functions and/or critical network resources and services shall be capable of providing appropriate standard (FIPS 140-2) cryptography-based data integrity services to protect and detect against unauthorized modification of messages.	UCR 2008: 5.4.6.2.2 (1.i)		X	WLAS/WAB Table E-9, Test Case 342
237	The device under test and its applications shall be capable of ensuring that it cannot be made to enter an insecure state because of the operation of non-privileged code.	UCR 2008: 5.4.6.2.2 (1.j)		X	All Table E-9, Test Case 343
238	The device under test shall be capable of ensuring that default user-IDs and passwords, previously modified by the administrator, do not revert to the vendor-delivered default user-IDs and passwords when the device under test is restarted unless configured to do so by an appropriate administrator.	UCR 2008:5.4.6.2.2 (1.k)		X	All Table E-9, Test Case 344
239	The device under test shall be capable of providing mechanisms to ensure the integrity of the data that is stored on the appliance and is used to support authentication processes. This includes protecting the information from malicious deletion, modification, or insertion. Note: Examples of the data stored would be private keys or certificates.	UCR 2008:5.4.6.2.2 (1.l)		X	All Table E-9, Test Case 345
240	The entire SNMPv3 message shall be checked for integrity and shall use HMAC-SHA1-96 with 160-bit key length.	UCR 2008:5.4.6.2.2 (1.n)		X	WLAS/WAB Table E-9, Test Case 347
241	If the device under test uses SSHv2, the system shall use HMAC-SHA1- 96 with 160-bit key length for data integrity.	UCR 2008:5.4.6.2.2 (1.o)		X	WLAS/WAB Table E-9, Test Case 348
242	If the device under test uses TLS, the system shall be capable of using TLS (SSLv3.1 or higher) in combination with HMAC-SHA1-160 with 160-bit keys to provide integrity for session packets.	UCR 2008:5.4.6.2.2 (1.p) (Conditional)		X	WEI Table E-9, Test Case 349
243	The device under test shall be capable of providing data and signaling confidentiality for all VVoIP traffic.	UCR 2008: 5.4.6.2.3 (1)		X	WLAS/WAB Table E-10, Test Case 350
244	The device under test shall implement FIPS 140-2, Level 1-validated cryptographic hardware modules or software toolkits operated in FIPS Mode for all encryption mechanisms.	UCR 2008: 5.4.6.2.3 (1.a)		X	WLAS/WAB Table E-10, Test Case 351
245	The device under test shall be capable of providing confidentiality for media streams using SRTP with AES_CM_128 encryption algorithm as the default or [Required FY12] AES 256-bit algorithm.	UCR 2008: 5.4.6.2.3 (1.b)		X	WEI Table E-10, Test Case 352
246	The device under test shall be capable of generating keys using a random source algorithm that meets the requirements of FIPS 186 to support SRTP.	UCR 2008: 5.4.6.2.3 (1.b.1)		X	WEI Table E-10, Test Case 353
247	The device under test shall be capable of distributing the Master Key and the Salt Key in the VVoIP signaling messages.	UCR 2008: 5.4.6.2.3 (1.b.2)		X	WEI Table E-10, Test Case 354
248	The device under test shall be capable of distributing the Master Key and the Salt Key in concatenated form.	UCR 2008: 5.4.6.2.3 (1.b.3)		X	WEI Table E-10, Test Case 355
249	The device under test shall use a Master Key of 128 bits in order to support 128-bit AES encryption. Note: This implies that the Master Salt Key may be null.	UCR 2008: 5.4.6.2.3 (1.b.4)		X	WEI Table E-10, Test Case 356
250	The Master Key and a random Master Salt Key shall be supported for SRTP sessions. Note: This is in addition to the 256-bit requirement.	UCR 2008: 5.4.6.2.3 (1.b.5)		X	WEI Table E-10, Test Case 357
251	The device under test shall be capable of providing confidentiality for signaling messages using TLS or IPSec using the AES 128-bit algorithm or AES 256-bit algorithm.	UCR 2008: 5.4.6.2.3 (1.c)		X	WEI Table E-10, Test Case 358
252	If H.323, MGCP, or H.248 (MEGACO) is used, the device under test shall be capable of using IPSec to provide confidentiality.	UCR 2008: 5.4.6.2.3 (1.c.1) (Conditional)		X	WEI Table E-10, Test Case 359

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
253	If IPSec is used, the device under test shall be capable of using Internet Key Exchange (IKE) for IPSec key distribution. [Required FY 10] IKE version 2. Note: IKEv2 requirements are found in UCR 2008, Section 5.3.5, IPv6 Requirements.	UCR 2008: 5.4.6.2.3 (1.c.1.c) (Conditional)		X	WEI Table E-10, Test Case 362
254	IKE version 1.	UCR 2008: 5.4.6.2.3 (1.c.1.c.i) (Conditional)		X	WEI Table E-10, Test Case 363
255	IKE version 2. Note: IKEv2 requirements are found in UCR 2008, Section 5.3.5, IPv6 Requirements.	UCR 2008: 5.4.6.2.3 (1.c.1.c.ii) (Conditional)		X	WEI Table E-10, Test Case 364
256	If IPSec is used, the device under test shall be capable of using the Revised Mode of public key encryption during Phase I of the Internet Security Association and Key Management Protocol (ISAKMP) negotiation for authentication.	UCR 2008: 5.4.6.2.3 (1.c.1.c.iii) (Conditional)		X	WEI Table E-10, Test Case 365
257	If IPSec is used, the device under test shall be capable of using the Quick Mode as the default Phase II authentication mechanism.	UCR 2008: 5.4.6.2.3 (1.c.1.c.iv) (Conditional)		X	WEI Table E-10, Test Case 366
258	If IPSec is used, the device under test shall be capable of using interpreting certificate requests for PKCS#7 wrapped certificates as a request for the whole path of certificates.	UCR 2008: 5.4.6.2.3 (1.c.1.c.v) (Conditional)		X	WEI Table E-10, Test Case 367
259	If IPSec is used, the system shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation.	UCR 2008: 5.4.6.2.3 (1.c.1.c.vi) (Conditional)		X	WEI Table E-10, Test Case 368
260	If IPSec is used, the device under test shall only support the following erroneous messages associated with a certificate request: Invalid key, Invalid ID, Invalid certificate encoding, Invalid certificate, Certificate type unsupported, Invalid CA, Invalid hash, Authentication failed, Invalid signature, Certificate unavailable.	UCR 2008: 5.4.6.2.3 (1.c.1.c.vi.a) (Conditional)		X	WEI Table E-10, Test Case 369
261	If IPSec is used, the device under test shall be capable of using Oakley Groups 1 and 2, as a minimum.	UCR 2008: 5.4.6.2.3 (1.c.1.c.vii) (Conditional)		X	WEI Table E-10, Test Case 370
262	If IPSec is used, the device under test shall be capable of using AES_128_CBC as the default encryption algorithm.	UCR 2008: 5.4.6.2.3 (1.c.1.d) (Conditional)		X	WEI Table E-10, Test Case 371
263	The device under test shall be capable of using TLS to provide confidentiality for the Assured Service - Session Initiation Protocol (AS-SIP). Note: The condition for the EI is the support of AS-SIP.	UCR 2008: 5.4.6.2.3 (1.c.2) (Conditional)		X	WEI Table E-10, Test Case 372
264	The underlying protocol for AS-SIP shall be the Transmission Control Protocol (TCP).	UCR 2008: 5.4.6.2.3 (1.c.2.a) (Conditional)		X	WEI Table E-10, Test Case 373
265	The device under test shall be capable of using as its default cipher either: [Conditional]TLS_RSA_WITH_AES_128_CBC_SHA or [Conditional, Required FY12] TLS_RSA_WITH_AES_256_CBC_SHA_	UCR 2008: 5.4.6.2.3 (1.c.2.b) (Conditional)		X	WEI Table E-10, Test Case 374
266	The device under test shall be capable of using a default of no compression for AS-SIP messages.	UCR 2008: 5.4.6.2.3 (1.c.2.c) (Conditional)		X	WEI Table E-10, Test Case 375
267	The device under test shall be capable of exchanging AS-SIP TLS messages in a single exchange or multiple exchanges.	UCR 2008: 5.4.6.2.3 (1.c.2.d) (Conditional)		X	WEI Table E-10, Test Case 376
268	The device under test shall be capable of distributing the SRTP Master Key and Salt Key in the AS-SIP message using the SDP cryptofield. Note: EI condition is whether it supports AS-SIP.	UCR 2008: 5.4.6.2.3 (1.c.2.e) (Conditional)		X	WEI Table E-10, Test Case 377
269	If TLS session resumption is used, a timer associated with TLS session resumption shall be configurable, and the default shall be one (1) hour. Note: This requirement is not associated with Network Management-related sessions.	UCR 2008: 5.4.6.2.3 (1.c.2.f) (Conditional)		X	WEI Table E-10, Test Case 378
270	The maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/ confidentiality/authorization process is one (1) hour.	UCR 2008: 5.4.6.2.3 (1.c.2.f.i) (Conditional)		X	WEI Table E-10, Test Case 379

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
271	If AS-SIP is used, the device under test shall only transmit packets that are secured with TLS and use port 5061. Note: The systems may use other signaling protocols for interfacing to MGs, EIs, etc.	UCR 2008: 5.4.6.2.3 (1.c.2.g) (Conditional)		X	WEI Table E-10, Test Case 380
272	The device under test shall reflect all received AS-SIP packets associated with port 5061 that are not secured with TLS. Note: This ensures that the system does not process UDP, SCTP, and TCP SIP packets that are not secured using a combination of TLS and TCP.	UCR 2008: 5.4.6.2.3 (1.c.2.h) (Conditional)		X	WEI Table E-10, Test Case 381
273	The device under test shall be capable of using SSHv2 or TLS (SSLv3.1) or higher for remote configuration of appliances. Note: EIs' remote manual configurations shall not be enabled, and all non-automatic processes shall be performed locally.	UCR 2008: 5.4.6.2.3 (1.e) (Conditional)		X	WLAS/WAB Table E-10, Test Case 384
274	If the device under test uses SSH, the system shall do so in a secure manner, as defined by the following subtended requirements. Note: EIs' remote manual configurations shall not be enabled, and all non-automatic processes shall be performed locally.	UCR 2008: 5.4.6.2.3 (1.g) (Conditional)		X	WLAS/WAB Table E-10, Test Case 391
275	If the device under test uses SSH, the system shall be capable of supporting the RSA 2,048-bit key algorithm.	UCR 2008: 5.4.6.2.3 (1.g.1) (Conditional)		X	WLAS/WAB Table E-10, Test Case 392
276	If the device under test uses SSH, the system shall use SSH in a secure manner.	UCR 2008: 5.4.6.2.3 (1.g.2) (Conditional)		X	WLAS/WAB Table E-10, Test Case 393
277	If the device under test uses SSH, a client shall close the session if the client receives a request to initiate an SSH session whose version is less than 2.0.	UCR 2008: 5.4.6.2.3 (1.g.2.a) (Conditional)		X	WLAS/WAB Table E-10, Test Case 394
278	If the device under test uses SSH, SSH sessions shall re-key at a minimum of every 2^{31} of transmitted data or every 60 minutes, whichever comes first.	UCR 2008: 5.4.6.2.3 (1.g.2.b) (Conditional)		X	WLAS/WAB Table E-10, Test Case 395
279	If the device under test uses SSH, SSH sessions shall transmit less than 2^{32} packets after a key exchange has occurred.	UCR 2008: 5.4.6.2.3 (1.g.2.c) (Conditional)		X	WLAS/WAB Table E-10, Test Case 396
280	If the device under test uses SSH, SSH sessions shall re-key at a minimum after receiving 2^{31} packets or every 60 minutes, whichever comes first.	UCR 2008: 5.4.6.2.3 (1.g.2.d) (Conditional)		X	WLAS/WAB Table E-10, Test Case 397
281	If the device under test uses SSH, SSH sessions shall accept less than 2^{32} packets after a key exchange has occurred. Note: These requirements are consistent with the SSHv2 recommendation formula for the number of packets to accept ($2^{L/4}$ where L is the key length – 128 bits).	UCR 2008: 5.4.6.2.3 (1.g.2.e) (Conditional)		X	WLAS/WAB Table E-10, Test Case 398
282	If the device under test uses SSH, SSH sessions shall use as the default encryption algorithm either AES 128-CBC or [conditional FY12] AES256-CBC.	UCR 2008: 5.4.6.2.3 (1.g.2.f) (Conditional)		X	WLAS/WAB Table E-10, Test Case 399
283	If the device under test uses SSH, SSH sessions shall use TCP as the underlying protocol.	UCR 2008: 5.4.6.2.3 (1.g.2.g) (Conditional)		X	WLAS/WAB Table E-10, Test Case 400
284	If the device under test uses SSH, the SSH packets shall have a configurable maximum uncompressed payload, and the default shall be 32,768 bytes. This does not preclude the system from automatically sizing the MTU if it is less than 32,768.	UCR 2008: 5.4.6.2.3 (1.g.2.h) (Conditional)		X	WLAS/WAB Table E-10, Test Case 401
285	If the device under test uses SSH, SSH packets shall have a maximum packet size of 35,000 bytes, including the packet length, padding length, payload, random padding, and MAC.	UCR 2008: 5.4.6.2.3 (1.g.2.h.i) (Conditional)		X	WLAS/WAB Table E-10, Test Case 402
286	If the device under test uses SSH, the appliance shall discard SSH packets that exceed the maximum packet size to avoid denial of service attacks or buffer overflow attacks.	UCR 2008: 5.4.6.2.3 (1.g.2.h.ii) (Conditional)		X	WLAS/WAB Table E-10, Test Case 403
287	If the device under test uses SSH, SSH packets shall use random bytes if packet padding is required.	UCR 2008: 5.4.6.2.3 (1.g.2.h.iii) (Conditional)		X	WLAS/WAB Table E-10, Test Case 404

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
288	If the device under test uses SSH, the system shall treat all SSH-encrypted packets sent in one direction as a single data stream. For example, the initialization vectors shall be passed from the end of one packet to the beginning of the next packet.	UCR 2008: 5.4.6.2.3 (1.g.2.i) (Conditional)		X	WLAS/WAB Table E-10, Test Case 405
289	If the device under test uses SSH, the system shall use Diffie-Hellman-Group2-SHA1 as the default key exchange mechanism for SSH.	UCR 2008: 5.4.6.2.3 (1.g.2.j) (Conditional)		X	WLAS/WAB Table E-10, Test Case 406
290	If the device under test uses SSH, the device using SSH shall be PKE and shall use the PKI to authenticate.	UCR 2008: 5.4.6.2.3 (1.g.2.k) (Conditional – FY12)		X	WLAS/WAB Table E-10, Test Case 407
291	If the device under test uses SSH, the device server using SSH shall have a host key.	UCR 2008: 5.4.6.2.3 (1.g.2.k.i) (Conditional – FY12)		X	WLAS/WAB Table E-10, Test Case 408
292	If the device under test uses SSH, the device shall certify and validate a server’s host key using the DOD PKI before connecting with an SSH session.	UCR 2008: 5.4.6.2.3 (1.g.2.k.ii) (Conditional – FY12)		X	WLAS/WAB Table E-10, Test Case 409
293	If the device under test uses SSH, the device shall certify and validate a server’s host key prior to connecting with an SSH session.	UCR 2008: 5.4.6.2.3 (1.g.2.k.iii) (Conditional – FY12)		X	WLAS/WAB Table E-10, Test Case 410
294	If the device under test uses SSH, the device shall disconnect a session if the authentication has not been accepted within 10 minutes.	UCR 2008: 5.4.6.2.3 (1.g.2.l) (Conditional)		X	WLAS/WAB Table E-10, Test Case 411
295	If the device under test uses SSH, the device shall disconnect if the number of failed authentication attempts for a single session exceeds a configurable parameter, and the default shall be three attempts.	UCR 2008: 5.4.6.2.3 (1.g.2.m) (Conditional)		X	WLAS/WAB Table E-10, Test Case 412
296	The device under test shall be capable of using SNMPv3 for all SNMP sessions. Note: If the device is using Version 1 or Version 2 (instead of SNMPv3) with all of the appropriate patches to mitigate the known security vulnerabilities, any findings associated with this requirement may be downgraded. In addition, if the device has also developed a migration plan to implement Version 3, any findings associated with this requirement may be further downgraded.	UCR 2008: 5.4.6.2.3 (1.h)		X	WLAS/WAB Table E-10, Test Case 413
297	The security level for SNMPv3 in the DOD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv.	UCR 2008: 5.4.6.2.3 (1.h.1)		X	WLAS/WAB Table E-10, Test Case 414
298	The SNMPv3 architecture shall be capable of allowing an appropriate administrator to manually configure the snmpEngineID from the operator console. A default-unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but this must be changeable.	UCR 2008: 5.4.6.2.3 (1.h.2)		X	WLAS/WAB Table E-10, Test Case 415
299	The security model for SMMPV3 shall be User-Based Security Model – snmpSecurity Model =3.	UCR 2008: 5.4.6.2.3 (1.h.3)		X	WLAS/WAB Table E-10, Test Case 416
300	If the device under test receives SNMP responses, the device shall conduct a timeliness check on the SNMPv3 message.	UCR 2008: 5.4.6.2.3 (1.h.3.a) (Conditional)		X	WLAS/WAB Table E-10, Test Case 417
301	An SNMPv3 engine shall perform time synchronization using authenticated messages.	UCR 2008: 5.4.6.2.3 (1.h.3.b)		X	WLAS/WAB Table E-10, Test Case 418
302	The message processing model shall be SNMPv3 – snmpMessage ProcessingModel=3.	UCR 2008: 5.4.6.2.3 (1.h.4)		X	WLAS/WAB Table E-10, Test Case 419
303	The default encryption cipher for SNMPv3 shall be CBC-DES-128 – usmDESPrivProtocol – CBCDES_128.	UCR 2008: 5.4.6.2.3 (1.h.5)		X	WLAS/WAB Table E-10, Test Case 420
304	If the device under test receives SNMP response messages, the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages.	UCR 2008: 5.4.6.2.3 (1.h.6) (Conditional)		X	WLAS/WAB Table E-10, Test Case 421
305	If the device under test receives SNMP responses, the SNMPv3 Command Generator Application shall discard any Response Class PDU for which there is no outstanding Confirmed Class PDU.	UCR 2008: 5.4.6.2.3 (1.h.7) (Conditional)		X	WLAS/WAB Table E-10, Test Case 422

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
306	When using msgID for correlating Response messages to outstanding Request messages, the SNMPv3 engine shall use different msgIDs in all such Request messages that it sends out during a 150-second Time Window.	UCR 2008: 5.4.6.2.3 (1.h.8)		X	WLAS/WAB Table E-10, Test Case 423
307	An SNMPv3 Command Generator or Notification Originator Application shall use different request-IDs in all Request PDUs that it sends out during a Time Window.	UCR 2008: 5.4.6.2.3 (1.h.9)		X	WLAS/WAB Table E-10, Test Case 424
308	When sending state-altering messages to a managed authoritative SNMPv3 engine, a Command Generator Application should delay sending successive messages to that managed SNMPv3 engine until a positive acknowledgement is received from the previous message or until the message expires.	UCR 2008: 5.4.6.2.3 (1.h.10)		X	WLAS/WAB Table E-10, Test Case 425
309	The device under test using SNMPv3 shall implement the key-localization mechanism.	UCR 2008: 5.4.6.2.3 (1.h.11)		X	WLAS/WAB Table E-10, Test Case 426
310	The device under test shall be capable of using a separate interface for management traffic. Note: The separate interface may be a logically- or physically-separate interface.	UCR 2008: 5.4.6.2.3 (1.j)		X	WLAS/WAB Table E-10, Test Case 428
311	The device under test shall be capable of protecting the management interface using filters. Note: Within a router, the filters may be achieved using ACLs. Within an appliance, the filters may include internal routing procedures to the different physical interfaces or VLAN tagging.	UCR 2008: 5.4.6.2.3 (1.j.1)		X	WLAS/WAB Table E-10, Test Case 429
312	The device under test shall be capable of using VLANs to segregate management traffic from other types of traffic, where feasible. Note: The LS will implement the VLAN, but the other appliances will have to tag the packets with the correct VLAN tag.	UCR 2008: 5.4.6.2.3 (1.j.2)		X	WLAS/WAB Table E-10, Test Case 430
313	The device under test shall re-key each encrypted session once the session has transmitted a maximum of $2^{L/4}$ blocks of data. “L” is the block length in bits (e.g., 128 for AES_128) and shall be configurable. Note: This is to prevent birthday property and other modes of attack.	UCR 2008: 5.4.6.2.3 (1.m)		X	WLAS/WAB Table E-10, Test Case 433
314	If the device under test is the originating party and receives a 181 message indicating that the call is being forwarded, then upon completion of the session establishment between the originating party and the forwarded-to party, the originating party must initiate a re-keying. Note: The re-keying is designed to prevent the forwarding party from having the key to the bearer session associated with the originating party and the forwarded-to party. If the forwarding party had the key to the bearer session, the forwarding party would be able to eavesdrop on the forwarded session. LSCs, MFSSs, and SSs may act as a B2BUA for an EI and would therefore originate the AS-SIP session on behalf of the EI.	UCR 2008: 5.4.6.2.3 (1.n) (Conditional)		X	WEI Table E-10, Test Case 434
315	If the EI acts as a bridge or an MCU, it shall establish a unique key for each EI connection.	UCR 2008: 5.4.6.2.3 (1.o) (Conditional)		X	WEI Table E-10, Test Case 435
316	The device under test shall be capable of providing non-repudiation and accountability services. Note: This assumes that authentication has already occurred as required previously.	UCR 2008: 5.4.6.2.4 (1)		X	WLAS/WAB Table E-11, Test Case 436
317	For user-accessible resources in the system that are created or modified by a user-ID via standard operations and maintenance procedures, the system shall be capable of providing a mechanism to identify the said user- ID, date, and time associated with the said resource creation or modification.	UCR 2008: 5.4.6.2.4 (1.a)		X	WLAS/WAB Table E-11, Test Case 437

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
318	The device under test shall be capable of auditing at the operating system and Database Management System (DBMS) levels and shall have a security log that contains information to support after-the-fact investigation of loss or impropriety and the appropriate management response.	UCR 2008: 5.4.6.2.4 (1.b)		X	WLAS/WAB Table E-11, Test Case 438
319	The security log entry of any request or activity that is invoked by a user-ID shall be capable of including that user-ID so it becomes possible to establish user accountability. Note: The term “user-ID” shall be interpreted for this requirement to include users as well as processes.	UCR 2008: 5.4.6.2.4 (1.b.1)		X	WLAS/WAB Table E-11, Test Case 439
320	The security log shall be capable of protecting itself from unauthorized access or destruction.	UCR 2008: 5.4.6.2.4 (1.b.2)		X	WLAS/WAB Table E-11, Test Case 440
321	The security log protection, at a minimum, shall be capable of providing access control based on user privileges and interface (logical or physical) privileges.	UCR 2008: 5.4.6.2.4 (1.b.2.a)		X	WLAS/WAB Table E-11, Test Case 441
322	The device under test shall have no mechanism for any external user (human or machine), including the administrator, to modify or delete the security log.	UCR 2008: 5.4.6.2.4 (1.b.2.b)		X	WLAS/WAB Table E-11, Test Case 442
323	The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).	UCR 2008: 5.4.6.2.4 (1.b.3)		X	WLAS/WAB Table E-11, Test Case 443
324	The device under test shall be capable of generating a security log alarm based upon specific conditions (e.g., percentage full by new entries since last upload, time interval elapsed since the last upload, disk space used). The alarm may necessitate uploading the security log (typically to some remote facility or other facility for long-term storage) to avoid an over-write in the buffer. This upload may be automatically performed by the system or by an appropriate administrator.	UCR 2008: 5.4.6.2.4 (1.b.3.a)		X	WLAS/WAB Table E-11, Test Case 444
325	Only the system security administrator role shall have the ability to retrieve, print, copy, and upload the security log(s).	UCR 2008: 5.4.6.2.4 (1.b.4)		X	WLAS/WAB Table E-11, Test Case 445
326	The device under test shall be capable of ensuring security log copies maintain time sequentially and include all records stored in the security log up to the initiation of the copy.	UCR 2008: 5.4.6.2.4 (1.b.4.a)		X	WLAS/WAB Table E-11, Test Case 446
327	The device under test security log shall survive system restart (e.g. via reloading).	UCR 2008: 5.4.6.2.4 (1.b.5)		X	WLAS/WAB Table E-11, Test Case 447
328	The security log shall be capable of recording any action that changes the security attributes and services, access controls, or other configuration parameters of devices; each login attempt and its result; and each logout or session termination (whether remote or console), to include the following events by default as a minimum:	UCR 2008: 5.4.6.2.4 (1.b.6)		X	WLAS/WAB Table E-11, Test Case 448
329	Invalid user authentication attempt.	UCR 2008: 5.4.6.2.4 (1.b.6.a)		X	WLAS/WAB Table E-11, Test Case 449
330	Unauthorized attempts to access system resources.	UCR 2008: 5.4.6.2.4 (1.b.6.b)		X	WLAS/WAB Table E-11, Test Case 450
331	Changes made in a user’s security profile and attributes.	UCR 2008: 5.4.6.2.4 (1.b.6.c)		X	WLAS/WAB Table E-11, Test Case 451
332	Changes made in security profiles and attributes associated with an interface/port.	UCR 2008: 5.4.6.2.4 (1.b.6.d)		X	WLAS/WAB Table E-11, Test Case 452
333	Changes made in access rights associated with resources (i.e., privileges required of a user and an interface/ports to access).	UCR 2008: 5.4.6.2.4 (1.b.6.e)		X	WLAS/WAB Table E-11, Test Case 453
334	Changes made in the system security configuration.	UCR 2008: 5.4.6.2.4 (1.b.6.f)		X	WLAS/WAB Table E-11, Test Case 454
335	Creation and modification of the system resources performed via standard operations and maintenance procedures.	UCR 2008: 5.4.6.2.4 (1.b.6.g)		X	WLAS/WAB Table E-11, Test Case 455
336	Disabling a user profile.	UCR 2008: 5.4.6.2.4 (1.b.6.h)		X	WLAS/WAB Table E-11, Test Case 456
337	Events associated with privileged users.	UCR 2008: 5.4.6.2.4 (1.b.6.i)		X	WLAS/WAB Table E-11, Test Case 457

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
338	If the device under test contains resources that are deemed mission critical (for example, a risk analysis classifies it as critical), then the device should log any events associated with access to those mission-critical resources.	UCR 2008: 5.4.6.2.4 (1.b.6.j)		X	WLAS/WAB Table E-11, Test Case 458
339	Successful login attempts.	UCR 2008: 5.4.6.2.4 (1.b.6.k)		X	WLAS/WAB Table E-11, Test Case 459
340	Failed login attempts to include the following:	UCR 2008: 5.4.6.2.4 (1.b.6.l)		X	WLAS/WAB Table E-11, Test Case 460
341	Failed login attempt due to an excessive number of logon attempts.	UCR 2008: 5.4.6.2.4 (1.b.6.l.i)		X	WLAS/WAB Table E-11, Test Case 461
342	Failed logon attempt due to blocking or blacklisting of a user-ID.	UCR 2008: 5.4.6.2.4 (1.b.6.l.ii)		X	WLAS/WAB Table E-11, Test Case 462
343	Failed logon attempt due to blocking or blacklisting of a terminal.	UCR 2008: 5.4.6.2.4 (1.b.6.l.iii)		X	WLAS/WAB Table E-11, Test Case 463
344	Failed logon attempt due to blocking or blacklisting of an access port.	UCR 2008: 5.4.6.2.4 (1.b.6.l.iv)		X	WLAS/WAB Table E-11, Test Case 464
345	The security log event record shall be capable of including the following information, at a minimum:	UCR 2008: 5.4.6.2.4 (1.b.7)		X	WLAS/WAB Table E-11, Test Case 465
346	Date and time of the event (both start and stop).	UCR 2008: 5.4.6.2.4 (1.b.7.a)		X	WLAS/WAB Table E-11, Test Case 466
347	User-ID, including associated terminal, port, network address, or communication device.	UCR 2008: 5.4.6.2.4 (1.b.7.b)		X	WLAS/WAB Table E-11, Test Case 467
348	Event type.	UCR 2008: 5.4.6.2.4 (1.b.7.c)		X	WLAS/WAB Table E-11, Test Case 468
349	Names of resources accessed.	UCR 2008: 5.4.6.2.4 (1.b.7.d)		X	WLAS/WAB Table E-11, Test Case 469
350	Success or failure of the event.	UCR 2008: 5.4.6.2.4 (1.b.7.e)		X	WLAS/WAB Table E-11, Test Case 470
351	The device under test shall have the capability to notify (e.g., via critical alarm, alert, or online report), within 30 seconds, an appropriate Network Operations Center (NOC) if the security log fails to record the events that are required to be recorded.	UCR 2008: 5.4.6.2.4 (1.b.8)		X	WLAS/WAB Table E-11, Test Case 471
352	The device under test shall not record actual or attempted passwords in the security log.	UCR 2008: 5.4.6.2.4 (1.b.9)		X	WLAS/WAB Table E-11, Test Case 472
353	The device under test shall ensure that security and audit logs are maintained separately from other audit logs (history or CDR audit logs).	UCR 2008: 5.4.6.2.4 (1.b.10)		X	WLAS/WAB Table E-11, Test Case 473
354	The device under test shall ensure that security and audit logs are maintained separately from other audit logs (history or CDR audit logs).	UCR 2008: 5.4.6.2.4 (1.b.11)		X	WLAS/WAB Table E-11, Test Case 474
355	If the device under test accesses other systems to pass on a request or activity that has a user-ID associated with it, the device shall have the capability to make that user-ID available to the other systems. Thus, if the other systems have the capability to accept the user-ID information, the said user can be traceable for the lifetime of the request or activity.	UCR 2008: 5.4.6.2.4 (1.c)		X	WLAS/WAB Table E-11, Test Case 475
356	The device under test shall be capable of providing post-collection audit analysis tools that can produce typical reports (e.g., exception reports, summary reports, and detailed reports) on specific data items, users, or communication facilities.	UCR 2008: 5.4.6.2.4 (1.d)		X	WLAS/WAB Table E-11, Test Case 476
357	The VVoIP device under test shall meet the availability requirements as stated in the UCR 2008, Section 5.3.2.2.3.8, System Quality Factors. Additional IA-specific IA availability requirements specified below are not covered in the System Quality Factors section of the UCR.	UCR 2008: 5.4.6.2.5 (1)		X	WLAS/WAB Table E-12, Test Case 477
358	The system shall have robustness through the maximum use of alternative routing, backup. Note: From a vendor’s perspective, this requirement is associated with meeting the reliability numbers for the system.	UCR 2008: 5.4.6.2.5 (1.a)		X	WLAS/WAB Table E-12, Test Case 478

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (“Test case” refers to the RTS IATP test case.)					
359	The device under test shall have mechanisms to allow “secure recovery” to reduce vulnerability due to failure or discontinuity, either of which makesit vulnerable to security compromise. Note: This requirement will ensure that as a device is re-established, it does not reboot in an unsecured mode such as with factory-set configurations.	UCR 2008: 5.4.6.2.5 (1.b)		X	WLAS/WAB Table E-12, Test Case 479
360	The device under test shall have the capability to rebuild the device to a base version and to permit subsequent vendor modification of that version, if that version and modification are currently in use.	UCR 2008: 5.4.6.2.5 (1.c)		X	WLAS/WAB Table E-12, Test Case 480
361	The device under test shall have the capability to provide adequate checkpoints in a process flow of the software system so that upon detection of service deterioration, a recovery to an acceptable level is facilitated.	UCR 2008: 5.4.6.2.5 (1.d)		X	WLAS/WAB Table E-12, Test Case 481
362	The device under test shall have a capability to define a threshold, e.g., percentage full by new entries since last upload, or time interval elapsed since last upload, to initiate a warning before a security log buffer overflow occurs.	UCR 2008: 5.4.6.2.5 (1.e)		X	WLAS/WAB Table E-12, Test Case 482
IPv6 Requirements Applicable to Wireless Components					
363	The device under test shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	UCR 2008: 5.3.5.3 (1)	X	X	WLAS/WAB Conditional -WEI Table E-13, Test Case 1 TP IO-26
364	If the device under test supports routing functions, the device shall support the manual tunnel requirements as described in RFC 4213.	UCR 2008: 5.3.5.3 (1.1) (Conditional)		X	WLAS/WAB Table E-13, Test Case 2
365	The device under test shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.	UCR 2008: 5.3.5.3 (2)	X	X	All Table E-13, Test Case 3 TP IO-27
366	The device under test shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464.	UCR 2008: 5.3.5.3 (3)	X	X	All Table E-13, Test Case 4 TP IO-28
367	The device under test shall support Path Maximum Transmission Unit (MTU) Discovery (RFC 1981).	UCR 2008: 5.3.5.3.1 (4)		X	WLAS/WAB Conditional -WEI Table E-13, Test Case 5
368	The device under test shall support a minimum MTU of 1280 bytes (RFC 2460 and updated by RFC 5095).	UCR 2008: 5.3.5.3.1 (5)		X	All Table E-13, Test Case 6
369	If Path MTU Discovery is used and a “Packet Too Big” message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, the device shall ignore the request for the smaller MTU and shall include a fragment header in the packet.	UCR 2008: 5.3.5.3.1 (6) (Conditional)		X	All Table E-13, Test Case 7
370	The device under test shall not use the Flow Label field as described in RFC 2460.	UCR 2008: 5.3.5.3.2 (7)		X	WEI Table E-13, Test Case 8
371	The device under test shall be capable of setting the Flow Label field to zero (0) when originating a packet.	UCR 2008: 5.3.5.3.2 (7.1)		X	WEI Table E-13, Test Case 9
372	The device under test shall not modify the Flow Label field when forwarding packets.	UCR 2008: 5.3.5.3.2 (7.2)		X	WEI Table E-13, Test Case 10
373	The device under test shall be capable of ignoring the Flow Label field when receiving packets.	UCR 2008: 5.3.5.3.2 (7.3)		X	WEI Table E-13, Test Case 11
374	The device under test shall support the IPv6 Addressing Architecture as described in RFC 4291.	UCR 2008: 5.3.5.3.3 (8)	X	X	All Table E-13, Test Case 12 TP IO-29
375	The device under test shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	UCR 2008: 5.3.5.3.3 (9)	X		All TP IO-30
376	If a scoped address (RFC 4007) is used, the device shall use a scope index value of zero (0) when the default zone is intended.	UCR 2008: 5.3.5.3.3 (9.1)	X		All TP IO-31

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components					
377	If a scoped address (RFC 4007) is used, the device shall use the syntax of <address>%<zone_id>/<prefix_length> when specifying an IPv6 non-global address. Note: "Address" is the IPv6 address and "%" and "/" are delimiters. If the zone id is zero (0) or default, the % and zone id may be omitted.	UCR 2008: 5.3.5.3.3 (9.2)	X		All TP IO-32
378	If the DHCP is supported within an IPv6 system, it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315.	UCR 2008: 5.3.5.3.3 (10) (Conditional)		X	All Table E-13, Test Case 13
379	If the device under test is a DHCPv6 client, the device shall discard any messages that contain options that are not allowed; these options are specified in Section 15 of RFC 3315.	UCR 2008: 5.3.5.3.3 (10.1) (Conditional)		X	WEI Table E-13, Test Case 14
380	The device under test shall support DHCPv6 as described in RFC 3315. Note: The following subtended requirements are predicated upon an implementation of DHCPv6 for the end instrument. It is not expected that other UC appliances will use DHCPv6.	UCR 2008: 5.3.5.3.3 (10.2)		X	WEI Table E-13, Test Case 15
381	If the device under test is a DHCPv6 client, and the first Retransmission Timeout has elapsed since the client sent the Solicit message and the client has received an Advertise message(s), but the Advertise message(s) does not have a preference value of 255, the client shall continue with a client-initiated message exchange by sending a Request message.	UCR 2008: 5.3.5.3.3 (10.2.1)		X	WEI Table E-13, Test Case 16
382	If the device under test is a DHCPv6 client and the DHCPv6 message exchange fails, it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a device-configurable timer, or a user-defined external event occurs. Note: The intent is to ensure that the DHCP client continues to restart the configuration process periodically until it succeeds.	UCR 2008: 5.3.5.3.3 (10.2.2)		X	WEI Table E-13, Test Case 17
383	If the device under test is a DHCPv6 client and sends an Information-Request message, it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server.	UCR 2008: 5.3.5.3.3 (10.2.3)		X	WEI Table E-13, Test Case 18
384	If the device under test is a DHCPv6 client, it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server prior to transmitting packets using that address for itself.	UCR 2008: 5.3.5.3.3 (10.2.4)		X	WEI Table E-13, Test Case 19
385	If the device under test is a DHCPv6 client, it shall log all reconfigure events.	UCR 2008: 5.3.5.3.3 (10.2.5)		X	WEI Table E-13, Test Case 20
386	If the device under test supports DHCPv6 and uses authentication, it shall discard unauthenticated DHCPv6 messages from UC systems and log the event. Note: This requirement assumes authentication is used as described in RFC 3118 (and extended in RFC 3315) but does not require authentication.	UCR 2008: 5.3.5.3.3 (10.3) (Conditional)		X	All Table E-13, Test Case 21
387	The device under test shall support Neighbor Discovery for IPv6 as described in RFC 2461 and RFC 4861 (FY10).	UCR 2008: 5.3.5.3.5 (11)	X	X	All Table E-13, Test Case 22 TP IO-33
388	The device under test shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements.	UCR 2008: 5.3.5.3.5 (11.1)		X	All Table E-13, Test Case 23
389	The device under test shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the device is providing proxy service.	UCR 2008: 5.3.5.3.5 (11.2)		X	All Table E-13, Test Case 24
390	If a valid neighbor advertisement is received by the device and the device neighbor cache does not contain the target's entry, the advertisement shall be silently discarded.	UCR 2008: 5.3.5.3.5 (11.3) (Conditional)		X	All Table E-13, Test Case 25

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components					
391	If a valid neighbor advertisement is received by the device under test, the device neighbor cache entry is in the INCOMPLETE state when the advertisement is received, and the link layer has addresses and no target link-layer option is included, the device under test shall silently discard the received advertisement.	UCR 2008: 5.3.5.3.5 (11.4) (Conditional)		X	All Table E-13, Test Case 26
392	If address resolution fails on a neighboring address, the entry shall be deleted from the device under test's neighbor cache.	UCR 2008: 5.3.5.3.5 (11.5) (Conditional)		X	All Table E-13, Test Case 27
393	The device under test shall support the ability to configure the system to ignore redirect messages.	UCR 2008: 5.3.5.3.5 (11.6)		X	WEI Table E-13, Test Case 28
394	The device under test shall only accept redirect messages from the same router that is currently being used for that destination.	UCR 2008: 5.3.5.3.5.1 (11.7)		X	All Table E-13, Test Case 29
395	If redirect messages are allowed, the device under test shall update its destination cache in accordance with the validated redirect message.	UCR 2008: 5.3.5.3.5.1 (11.7.1) (Conditional)		X	All Table E-13, Test Case 30
396	If the valid redirect message is allowed and no entry exists in the destination cache, the device under test shall create an entry.	UCR 2008: 5.3.5.3.5.1 (11.7.2) (Conditional)		X	All Table E-13, Test Case 31
397	If the device under test sends router advertisements, the device shall inspect valid router advertisements sent by other routers, verify that the routers are advertising consistent information on a link, and log any inconsistent router advertisements.	UCR 2008: 5.3.5.3.5.2 (11.8) (Conditional)		X	WLAS/WAB Table E-13, Test Case 32
398	The device under test shall prefer routers that are reachable over routers whose reachability is suspect or unknown.	UCR 2008: 5.3.5.3.5.2 (11.8.1)		X	WEI Table E-13, Test Case 33
399	If the device under test sends router advertisements, the device shall include the MTU value in the router advertisement message for all links, in accordance with RFC 2461 and RFC 4861 (FY10).	UCR 2008: 5.3.5.3.5.2 (11.9) (Conditional)		X	WLAS/WAB Table E-13, Test Case 34
400	If the device under test supports stateless IP address autoconfiguration, the device shall support IPv6 Stateless Address Auto- Configuration (SLAAC) for interfaces supporting UC functions, in accordance with RFC 2462 and RFC 4862 (FY10).	UCR 2008: 5.3.5.3.6 (12)		X	All (Softphone only) Table E-13, Test Case 35
401	The device under test shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless auto configuration.	UCR 2008: 5.3.5.3.6 (12.1)		X	All Table E-13, Test Case 36
402	The device under test shall support manual assignment of IPv6 addresses.	UCR 2008: 5.3.5.3.6 (12.2)		X	All Table E-13, Test Case 37
403	The device under test shall support stateful autoconfiguration (i.e., ManagedFlag=TRUE). Note: This requirement is associated with the earlier requirement for the EI to support DHCPv6.	UCR 2008: 5.3.5.3.6 (12.3)		X	WEI Table E-13, Test Case 38
404	If the device under test sends router advertisements, the device shall default to using the "managed address configuration" flag and the "other stateful" flag set to TRUE in the router advertisements when stateful autoconfiguration is implemented.	UCR 2008: 5.3.5.3.6 (12.3.1) (Conditional)		X	WLAS/WAB Table E-13, Test Case 39
405	If the device under test supports a subtended appliance behind it, the device shall ensure that the IP address assignment process of the subtended appliance is transparent to the UC components of the system and does not cause the device to attempt to change its IP address. Note: An example is a PC that is connected to the LAN through the hub or switch interface on a phone. The address assignment process of the PC should be transparent to the EI and should not cause the phone to attempt to change its IP address.	UCR 2008: 5.3.5.3.6 (12.4) (Conditional)		X	EI Table E-13, Test Case 40
406	If the device under test supports IPv6 SLAAC, the device shall have a configurable parameter that allows the function to be enabled and disabled.	UCR 2008: 5.3.5.3.6 (12.5) (Conditional)		X	EI Table E-13, Test Case 41

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components					
407	If the device under test supports SLAAC, and security constraints prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, IPSec-capable systems shall support privacy extensions for stateless address autoconfiguration as defined in RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6.	UCR 2008: 5.3.5.3.6 (12.6) (Conditional -Softphones)		X	EI Table E-13, Test Case 42
408	If the device under test supports stateless IP address autoconfiguration, the device shall support a configurable parameter to enable or disable manual configuration of the site-local and Global addresses (i.e., disable the "Creation of Global and Site-Local Addresses," as described in Section 5.5 of RFC 2462).	UCR 2008: 5.3.5.3.6 (12.7)		X	All WEI-Softphone Table E-13, Test Case 43
409	IPv6 nodes shall support link-local address configuration, and the Duplicate Address Detection (DAD) shall not be disabled, in accordance with RFC 2462 and RFC 4862 (FY10).	UCR 2008: 5.3.5.3.6 (12.8)		X	All Table E-13, Test Case 44
410	The device under test shall support the Internet Control Message Protocol for IPv6 (ICMPv6) as described in RFC 4443.	UCR 2008: 5.3.5.3.7 (14)	X	X	All Table E-13, Test Case 45 TP IO-34
411	The device under test shall have a configurable rate-limiting parameter for rate-limiting the forwarding of ICMP messages.	UCR 2008: 5.3.5.3.7 (14.1)	X	X	All Table E-13, Test Case 46 TP IO-35
412	The device under test shall support the capability to enable or disable the ability of the device to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.	UCR 2008: 5.3.5.3.7 (14.2)	X	X	All Table E-13, Test Case 47 TP IO-36
413	The device under test shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address.	UCR 2008: 5.3.5.3.7 (14.3)		X	All Table E-13, Test Case 48
414	The device under test shall validate ICMPv6 messages using the information contained in the payload prior to acting on them.	UCR 2008: 5.3.5.3.7 (14.4)		X	All Table E-13, Test Case 49
415	If the device under test supports routing functions, the device shall support the Open Shortest Path First (OSPF) for IPv6 as described in RFC 2740.	UCR 2008: 5.3.5.3.8 (15) (Conditional)	X	X	WLAS/WAB Table E-13, Test Case 50 TP IO-37
416	If the device under test supports routing functions, the device shall support securing OSPF with Internet Protocol Security (IPSec) as described for other IPSec instances in UCR 2008, Section 5.4, and Information Assurance.	UCR 2008: 5.3.5.3.8 (15.1) (Conditional)		X	WLAS/WAB Table E-13, Test Case 51
417	If the device under test supports routing functions, the device shall support router-to-router integrity using the IP Authentication Header with HMAC-SHA1-128 as described in RFC 4302.	UCR 2008: 5.3.5.3.8 (15.2) (Conditional)		X	WLAS/WAB Table E-13, Test Case 52
418	If the device under test supports routing functions, the system shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810. Note: The FY08 VVoIP design does not utilize multicast, but routers supporting VVoIP also support data applications that may utilize multicast. A Softphone will have non-routing functions that require MLDv2.	UCR 2008: 5.3.5.3.8 (20)		X	EI-Softphone Conditional-WLAS/WAB Table E-13, Test Case 58
419	The device under test shall support MLD as described in RFC 2710. Note: This requirement was added in order to ensure that Neighbor Discovery multicast requirements are met. Routers are not included in this requirement since they must meet RFC 2710 in the preceding requirement.	UCR 2008: 5.3.5.3.8 (21)		X	All Table E-13, Test Case 59
420	If the device under test uses IPSec, the device shall support the Security Architecture for the IP RFC 2401 and RFC 4301 (FY10). In FY08, RFC 2401 (and its related RFCs) is the Threshold requirement as described in UCR 2008, Section 5.4, Information Assurance. In addition, the interfaces required to use IPSec are defined in UCR 2008, Section 5.4, Information Assurance.	UCR 2008: 5.3.5.3.8 (22)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 60

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components					
421	If RFC 4301 is supported, the device under test shall support binding of a security association (SA) with a particular context.	UCR 2008: 5.3.5.3.8 (22.1)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 61
422	If RFC 4301 is supported, the device under test shall be capable of disabling the BYPASS IPSec processing choice. Note: The intent of this requirement is to ensure that no packets are transmitted unless they are protected by IPSec.	UCR 2008: 5.3.5.3.8 (22.2)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 62
423	If RFC 4301 is supported, the device under test shall not support the mixing of IPv4 and IPv6 in a security association.	UCR 2008: 5.3.5.3.8 (22.3)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 63
424	If RFC 4301 is supported, the device under test's security association database (SAD) cache shall have a method to uniquely identify a SAD entry. Note: The concern is that a single SAD entry will be associated with multiple security associations. RFC 4301, Section 4.4.2, describes a scenario in which this could occur.	UCR 2008: 5.3.5.3.8 (22.4)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 64
425	If RFC 4301 is supported, the device under test shall be capable of correlating the Differentiated Services Code Point (DSCP) for a VVoIP stream to the security association, in accordance with UCR 2008, Section 5.3.2, Assured Services Requirements; and Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, plain text DSCP plan. For a more detailed description of the requirement, please see Section 4-1 of RFC 4301 - Security Architecture for the Internet Protocol.	UCR 2008: 5.3.5.3.8 (22.5)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 65
426	If RFC 4301 is supported, the device under test shall implement IPSec to operate with both integrity and confidentiality.	UCR 2008: 5.3.5.3.8 (22.6)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 66
427	If RFC 4301 is supported, the device under test shall be capable of enabling and disabling the ability of the device to send an ICMP message informing the sender that an outbound packet was discarded.	UCR 2008: 5.3.5.3.8 (22.7)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 67
428	If an ICMP outbound packet message is allowed, the device under test shall be capable of rate-limiting the transmission of ICMP Responses.	UCR 2008: 5.3.5.3.8 (22.7.1)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 68
429	If RFC 4301 is supported, the device under test shall be capable of enabling or disabling the propagation of the Explicit Congestion Notification (ECN) bits.	UCR 2008: 5.3.5.3.8 (22.8)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 69
430	If RFC 4301 is supported, the device under test's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.	UCR 2008: 5.3.5.3.8 (22.9)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 70
431	If RFC 4301 is supported, and the device under test receives a packet that does not match any SPD cache entries and determines it should be discarded, the device shall log the event and include the date/time; Security Parameter Index (SPI), if available; IPSec protocol, if available; source and destination of the packet, and any other selector values of the packet.	UCR 2008: 5.3.5.3.8 (22.10)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 71
432	If RFC 4301 is supported, the device under test shall include a management control to allow an administrator to enable or disable the ability of the system to send an Internet Key Exchange (IKE) notification of INVALID_SELECTORS.	UCR 2008: 5.3.5.3.8 (22.11)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 72
433	If RFC 4301 is supported, the device under test shall support the Encapsulating Security Payload (ESP) Protocol in accordance with RFC 4303.	UCR 2008: 5.3.5.3.9 (22.12)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 73
434	If RFC 4303 is supported, the device under test shall be capable of enabling anti-replay.	UCR 2008: 5.3.5.3.9 (22.12.1)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 74

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components					
435	If RFC 4303 is supported, the device under test shall check, as its first check after a packet has been matched to its SA, whether the packet contains a Sequence Number that does not duplicate the Sequence Number of any other packet received during the life of the security association.	UCR 2008: 5.3.5.3.9 (22.12.2)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 75
436	If RFC 4301 is supported, the device under test shall support the cryptographic algorithms as defined in RFC 4308 for Suite Virtual Private Network (VPN)-B.	UCR 2008: 5.3.5.3.9 (22.13)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 76
437	If RFC 4301 is supported, the device under test shall support the use of AES-CBC with 128-bit keys for encryption.	UCR 2008: 5.3.5.3.9 (22.13.1)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 77
438	If RFC 4301 is supported, the device under test shall support the use of HMAC-SHA1- 96 for (Threshold) and AES-XCBC-MAC-96 (FY2010).	UCR 2008: 5.3.5.3.9 (22.13.2)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 78
439	If RFC 4301 is supported, the device under test shall support IKE Version 1 (IKEv1) (Threshold), as defined in RFC 2409; and IKE Version 2 (IKEv2) (FY2010), as defined in RFC 4306. Note: Internet Key Exchange version 1 (IKEv1) requirements are found in UCR 2008, Section 5.4, Information Assurance.	UCR 2008: 5.3.5.3.9 (22.14)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 79
440	If the device under test supports IKEv2, it shall be capable of configuring the maximum User Datagram Protocol (UDP) message size.	UCR 2008: 5.3.5.3.9 (22.14.1) (Conditional)		X	All Table E-13, Test Case 80
441	If IKEv2 is supported, the device under test shall support the use of the ID_IPv6_ADDR and ID_IPV4_ADDR Identification Type.	UCR 2008: 5.3.5.3.9 (22.14.2) (Conditional)		X	All Table E-13, Test Case 81
442	If the device under test supports IKEv2, the device shall be capable of ignoring subsequent SA setup response messages after the receipt of a valid response.	UCR 2008: 5.3.5.3.9 (22.14.3) (Conditional)		X	All Table E-13, Test Case 82
443	If the device under test supports IKEv2, the device shall be capable of sending a Delete payload to the other end of the security association.	UCR 2008: 5.3.5.3.9 (22.14.4) (Conditional)		X	All Table E-13, Test Case 83
444	If the device under test supports IKEv2, the device shall reject initial IKE messages unless they contain a Notify payload of type COOKIE.	UCR 2008: 5.3.5.3.9 (22.14.5) (Conditional)		X	All Table E-13, Test Case 84
445	If the device under test supports IKEv2, the device shall close an SA instead of rekeying when its lifetime expires if there has been no traffic since the last rekey.	UCR 2008: 5.3.5.3.9 (22.14.6) (Conditional)		X	All Table E-13, Test Case 85
446	If the system supports IKEv2, the system shall not use the Extensible Authentication Protocol (EAP) method for IKE authentication.	UCR 2008: 5.3.5.3.9 (22.14.7) (Conditional)		X	All Table E-13, Test Case 86
447	If the device under test supports IKEv2, the device shall limit the frequency with which it responds to messages on UDP port 500 or 4500 when outside the context of a security association known to it.	UCR 2008: 5.3.5.3.9 (22.14.8) (Conditional)		X	All Table E-13, Test Case 87
448	If the device under test supports IKEv2, the device shall not support temporary IP addresses or respond to such requests.	UCR 2008: 5.3.5.3.9 (22.14.9) (Conditional)		X	All Table E-13, Test Case 88
449	If the device under test supports IKEv2, the device shall support the IKEv2 cryptographic algorithms defined in RFC 4307.	UCR 2008: 5.3.5.3.9 (22.14.10) (Conditional)		X	All Table E-13, Test Case 89
450	If the device under test supports IKEv2, the device shall support the VPN-B Suite as defined in RFC 4308 and RFC 4869 (FY2010).	UCR 2008: 5.3.5.3.9 (22.14.11) (Conditional)		X	All Table E-13, Test Case 90
451	If RFC 4301 is supported, the device under test shall support extensions to the Internet IP Security Domain of Interpretation for the ISAKMP as defined in RFC 2407.	UCR 2008: 5.3.5.3.9 (22.15)		X	All Table E-13, Test Case 91
452	If RFC 4301 is supported, the device under test shall support the ISAKMP as defined in RFC 2408.	UCR 2008: 5.3.5.3.9 (22.16)		X	All Table E-13, Test Case 92
453	If the device under test supports the IPSec Authentication Header Mode, the device under test shall support the IP Authentication Header (AH) as defined in RFC 4302.	UCR 2008: 5.3.5.3.9 (22.17)		X	All Table E-13, Test Case 93

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components					
454	If RFC 4301 is supported, the device under test shall support manual keying of IPSec.	UCR 2008: 5.3.5.3.9 (22.18)		X	All Table E-13, Test Case 94
455	If RFC 4301 is supported, the device under test shall support the ESP and AH cryptographic algorithm implementation requirements as defined in RFC 4305 and RFC 4835 (FY10).	UCR 2008: 5.3.5.3.9 (22.19)		X	All Table E-13, Test Case 95
456	If RFC 4301 is supported, the device under test shall support the IKEv1 security algorithms as defined in RFC 4109.	UCR 2008: 5.3.5.3.9 (22.21)		X	All Table E-13, Test Case 96
457	The device under test shall comply with the Management Information Base (MIB) for IPv6 textual conventions and general group as defined in RFC 4293. Note: The requirements to support SNMPv3 are found in UCR 2008, Section 5.3.2.17.3.1.5, SNMP Version 2 and Version 3 Format Alarm messages; and UCR 2008, Section 5.4, Information Assurance.	UCR 2008: 5.3.5.3.10 (23)	X	X	WLAS/WAB Table E-13, Test Case 97 TP IO-38
458	If the device under test performs routing functions, the device shall support the SNMP management framework as described in RFC 3411.	UCR 2008: 5.3.5.3.10 (23.1)		X	WLAS/WAB Table E-13, Test Case 98
459	If the device under test performs routing functions, the device shall support SNMP message processing and dispatching as described in RFC 3412.	UCR 2008: 5.3.5.3.10 (23.2)		X	WLAS/WAB Table E-13, Test Case 99
460	If the device under test performs routing functions, the device shall support the SNMP applications as described in RFC 3413.	UCR 2008: 5.3.5.3.10 (23.3)		X	WLAS/WAB Table E-13, Test Case 100
461	The device under test shall support the ICMPv6 MIBs as defined in RFC 4293.	UCR 2008: 5.3.5.3.10 (24)	X	X	WLAS/WAB Table E-13, Test Case 101 TP IO-39
462	The device under test shall support the Transmission Control Protocol (TCP) MIBs as defined in RFC 4022.	UCR 2008: 5.3.5.3.10 (25)	X	X	WLAS/WAB Table E-13, Test Case 102 TP IO-40
463	The device under test shall support the UDP MIBs as defined in RFC 4113.	UCR 2008: 5.3.5.3.10 (26)	X	X	WLAS/WAB Table E-13, Test Case 103 TP IO-41
464	If the device under test performs routing functions, the device shall support IP tunnel MIBs as described in RFC 4087.	UCR 2008: 5.3.5.3.10 (27)		X	WLAS/WAB Table E-13, Test Case 104
465	If the device under test performs routing functions, the device shall support the IP Forwarding MIB as defined in RFC 4292.	UCR 2008: 5.3.5.3.10 (28)		X	WLAS/WAB Table E-13, Test Case 105
466	If the device under test supports mobile users, the device shall support the Mobile IP Management MIBs as described in RFC 4295.	UCR 2008: 5.3.5.3.10 (29)		X	WLAS/WAB Table E-13, Test Case 106
467	If the device under test supports SNMP and supports routing functions, the device shall support the textual conventions for IPv6 flow labels as described in RFC 3595.	UCR 2008: 5.3.5.3.10 (30) (Conditional)		X	WLAS/WAB
468	If the device under test supports SNMP and IPSec, the device shall support the IPSec security policy database as described in RFC 4807.	UCR 2008: 5.3.5.3.10 (31)		X	WLAS/WAB Table E-13, Test Case 107
469	If the device under test uses Uniform Resource Identifiers (URIs), the device shall use the URI syntax described in RFC 3986.	UCR 2008: 5.3.5.3.10 (32)		X	All Table E-13, Test Case 108
470	If the device under test uses the Domain Name System (DNS), the device shall conform to RFC 3596 for DNS queries. Note: DNS is primarily used for NM applications.	UCR 2008: 5.3.5.3.10 (33)		X	All Table E-13, Test Case 109
471	For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 Kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 Kbps) resulting in a 250-byte bearer packet plus 10 Kbps for signaling, Ethernet Interframe Gap, and the SRTCP overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.	UCR 2008: 5.3.5.3.11 (34)	X		WLAS/WAB TP IO-42

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components					
472	The number of VoIP subscribers per link size for IPv6 is the same as for IPv4 and is defined in UCR 2008, Section 5.3.1, Assured Services Local Area Network Infrastructure Product Requirements.	UCR 2008: 5.3.5.3.11 (35)	X		WLAS/WAB TP IO-43
473	The number of video subscribers per link size for IPv6 is the same as for IPv4 and is defined in UCR 2008, Section 5.3.1, Assured Services Local Area Network Infrastructure Product Requirements.	UCR 2008: 5.3.5.3.11 (36)	X		WLAS/WAB TP IO-44
474	The device under test shall use the Alternative Network Address Types (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091 when establishing media streams from dual-stacked appliances for AS-SIP signaled sessions.	UCR 2008: 5.3.5.3.12 (38)		X	WEI Table E-13, Test Case 111
475	The device under test shall prefer any IPv4 address to any IPv6 address when using ANAT semantics.	UCR 2008: 5.3.5.3.12 (38.1)	X		WEI TP IO-45
476	The device under test shall place the SDP-ANAT option-tag in a required header field when using ANAT semantics in accordance with RFC 4092.	UCR 2008: 5.3.5.3.12 (38.2)		X	WEI Table E-13, Test Case 112
477	The device under test shall place the SDP-ANAT option-tag in a required header field when using ANAT semantics in accordance with RFC 4092.	UCR 2008: 5.3.5.3.12 (38.3)		X	WEI Table E-13, Test Case 113
478	The device under test shall place the SDP-ANAT option-tag in a required header field when using ANAT semantics in accordance with RFC 4092.	UCR 2008: 5.3.5.3.12 (38.3)		X	WEI Table E-13, Test Case 113
479	If the device under test is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is a unicast address, the system shall support generation and processing of unicast IPv6 addresses having the following formats: x:x:x:x:x:x:x:x (where x is the hexadecimal value of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A:x:x:x:x:x:x:d.d.d.d (where x is the hexadecimal value of the six high-order 16-bit pieces of the address, and d is the decimal value of the four low-order 8-bit pieces of the address (standard IPv4 representation). Example: 1080:0:0:0:8:800:16.23.135.22	UCR 2008: 5.3.5.3.13 (39) (Conditional)	X		WEI TP IO-46
480	If the device under test is using AS-SIP, the system shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats: • x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A • x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22 • compressed zeros: 1080::8:800:200C:417A	UCR 2008: 5.3.5.3.13 (40) (Conditional)	X		WEI TP IO-47
481	If the device under test is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is a multicast group address (i.e., the two most significant hexadecimal digits are FF), the device shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.	UCR 2008: 5.3.5.3.13 (41) (Conditional)	X		WEI TP IO-48
482	If the device under test is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is an IPv6 multicast group address, the multicast connection address shall not have a TTL value appended to the address as IPv6 multicast does not use TTL scoping.	UCR 2008: 5.3.5.3.13 (43) (Conditional)	X		WEI TP IO-49
483	If the device under test is using AS-SIP, the device shall support the processing of IPv6 multicast group addresses having the <number of address> field and may support generating the <number of address> field. This field has the identical format and operation as the IPv4 multicast group addresses.	UCR 2008: 5.3.5.3.13 (44) (Conditional)	X		WEI TP IO-50
484	The device under test shall support default address selection for IPv6 as defined in RFC 3484 (except for Section 2.1).	UCR 2008: 5.3.5.3.13 (46)		X	WEI - Softphone Table E-13, Test Case 115

Table 3-1. Wireless Products Capability/Functional Requirements (continued)

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components					
485	If the device under test supports Remote Authentication Dial In User Service (RADIUS) authentication, the system shall support RADIUS in the manner defined in RFC 3162.	UCR 2008: 5.3.5.3.14 (47)		X	WLAS/WAB Table E-13, Test Case 116
486	If the device under test supports Mobile IP version 6 (MIPv6), the system shall provide mobility support as defined in RFC 3775.	UCR 2008: 5.3.5.3.14 (48)		X	WEI - Softphone Table E-13, Test Case 117
487	If the device under test supports Mobile IP version 6 (MIPv6), the system shall provide a secure manner to signal between mobile nodes and home agents in manner described in RFC 3776 and RFC 4877 (FY10).	UCR 2008: 5.3.5.3.14 (49)		X	WEI - Softphone Table E-13, Test Case 119
488	If the device under test supports network mobility (NEMO), the system shall support the function as defined in RFC 3963.	UCR 2008: 5.3.5.3.14 (51)		X	WEI - Softphone Table E-13, Test Case 120
489	The device under test shall support Differentiated Services as Described in RFC 2474 and RFC 5072 (FY10) for a voice and video stream.	UCR 2008: 5.3.5.3.14 (52)	X	X	All Table E-13, Test Case 121 TP IO-51
490	If the device under test acts as an IPv6 tunnel broker, the device shall support the function in the manner defined in RFC 3053.	UCR 2008: 5.3.5.3.14 (53)		X	WEI - Softphone Table E-13, Test Case 122
Other UCR Requirements					
491	For NM, LAN products shall use Secure Shell 2 (SSH2). Due to its increased security, the SSH2 protocol shall be used instead of Telnet. The LAN products shall support RFC 4251 through RFC 4254, inclusive.	UCR 2008: 5.3.1.6 (1)		X	WLAS/WAB TP IA-
492	For NM, LAN products shall use HyperText Transfer Protocol, Secure (HTTPS). Due to its increased security, HTTPS shall be used instead of HTTP, as described in RFC 2660. The LAN products shall support RFC 2818.	UCR 2008: 5.3.1.6 (2)		X	WLAS/WAB TP IA-
493	All LAN components shall be capable of providing status changes 99 percent of the time (with 99.9 percent as an Objective Requirement) by means of an automated capability in near real time (NRT).	UCR 2008: 5.3.1.6.3		X	WLAS/WAB TP IA-
494	All LAN components shall be capable of providing SNMP alarm indications to an NMS. Alarms shall be reported as TRAPs via SNMP in NRT. More than 99.95 percent of alarms shall be reported in NRT. NRT is defined as within 5 seconds of detecting the event, excluding transport time.	UCR 2008: 5.3.1.6.4		X	WLAS/WAB TP IA-
Wireless STIGs					
495	The device under test shall support MAC address filtering.	Wireless STIG WIR0160: CAT III 2.2.3.3		X	All TP IA-
496	The device under test shall support VLANs.	Wireless STIG WIR0290: CAT II 2.2.3.8 2.2.1.2		X	All TP IA-
497	The device under test shall support disabling SSID broadcast mode.	Wireless STIG WIR0150: CAT II		X	All TP IA-
498	SSIDs not set to default.	Wireless STIG, WIR0105: CAT III Wireless STIG, WIR0140: CAT III		X	All TP IA-

This page intentionally left blank.