



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

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

27 Nov 13

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Amcom Software Inc., Internet Protocol (IP) Phone Tracking Gateway Release 3.4.12

- References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) DoD CIO, Memorandum, "Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)," 27 March 2012
(c) through (e), see Enclosure 1

1. Certification Authority. References (a) and (b) establish the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for the Unified Capabilities (UC) products.

2. Conditions of Certification. The Amcom Software Inc., IP Phone Tracking Gateway Release 3.4.12; hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements (UCR), Reference (c), and is certified for joint use as Customer Premise Equipment (CPE) without any conditions (see Table 1). The SUT was tested and is certified with the Amcom Software Inc., Personal Computer/Public Safety Answering Point (PC/PSAP™) Release 11.11.0.21. JITC analysis determined that the SUT is certified with any Amcom Software Inc. PC/PSAP™ that has been or is on the Unified Capabilities (UC) Approved Products List (APL). The SUT was tested with an Assured Services Local Area Network (ASLAN) access layer switch and is certified with any ASLAN access switch that has been or is on the UC APL. This certification expires upon changes that affect interoperability, but no later than three years from the date of this memorandum.

Table 1. Conditions

Table with 4 columns: Condition, Status, Operational Impact, Remarks. Row 1: Not applicable; the Amcom Software Inc., IP Phone Tracking Gateway Release 3.4. meets all of the Unified Capabilities Requirements (UCR), Reference (c) joint critical interoperability requirements.

3. Interoperability Status. Table 2 provides the SUT interface interoperability status and Table 3 provides the Capability Requirements (CR) and Functional Requirements (FR) status. Table 4 provides a UC APL product summary.

The DISA CA provided a positive Recommendation on 27 November 2013 for a period of one year based on the security testing completed by DISA-led IA test teams and the results published in a separate report, Reference (e). Enclosure 2 documents the test results and describes the tested network and system configurations. Enclosure 3 provides a detailed list of interface, capability, and functional requirements in Table 3-1 through Table 3-6.

5. Additional Information. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Sensitive but Unclassified IP Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at <https://stp.fhu.disa.mil/>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <https://jit.fhu.disa.mil/>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil. All associated information is available on the DISA UCCO website located at <http://www.disa.mil/Services/Network-Services/UCCO>.

6. Point of Contact (POC). The JITC point of contact is Ms. Sibylle Gonzales, commercial telephone (520) 538-5483, DSN telephone 879-5483, FAX DSN 879-4347; e-mail address sibylle.j.gonzales.civ@mail.mil; mailing address Joint Interoperability Test Command, ATTN: JTE (Ms. Sibylle Gonzales) P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 1300906.

FOR THE COMMANDER:



for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

3 Enclosures a/s

JITC Memo, JTE, Joint Interoperability Certification of the Amcom Software Inc., Internet Protocol (IP) Phone Tracking Gateway Release 3.4.12

Distribution (electronic mail):

DoD CIO

Joint Staff J-6, JCS

USD(AT&L)

ISG Secretariat, DISA, JTA

U.S. Strategic Command, J665

US Navy, OPNAV N2/N6FP12

US Army, DA-OSA, CIO/G-6 ASA(ALT), SAIS-IOQ

US Air Force, A3CNN/A6CNN

US Marine Corps, MARCORSSYSCOM, SIAT, A&CE Division

US Coast Guard, CG-64

DISA/TEMC

DIA, Office of the Acquisition Executive

NSG Interoperability Assessment Team

DOT&E, Netcentric Systems and Naval Warfare

Medical Health Systems, JMIS IV&V

HQUSAISEC, AMSEL-IE-IS

UCCO

ADDITIONAL REFERENCES

- (c) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013," 1 March 2013
- (d) Joint Interoperability Test Command, "IP Phone Tracker CPE Test Procedures," Draft
- (e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of Amcom Software, Inc. Voice over Internet Protocol (VoIP) Phone Tracking Gateway Release (Rel.) 3.4.12 (Tracking Number 1300906)," Draft

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The Amcom Software Inc., IP Phone Tracking Gateway Rel 3.4.12 is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT identifying information and requirements source.

Table 2-1. System and Requirements Identification

System Identification	
Sponsor	Headquarters United States Army Information Systems Engineering Command (HQUSAISEC)
Sponsor Point of Contact	Mr. Robert Adkins, USAISEC ELIE-ISE-ES, Building 53301, Fort Huachuca, Arizona 85613, e-mail: robert.h.adkins.civ@mail.mil
Vendor Point of Contact	Amcom Software, Inc., 10400 Yellow Circle Drive, Eden Prairie, Minnesota 55343, e-mail: berdman@amcomsoft.com
System Name	Amcom Software Inc., IP Phone Tracking Gateway
Increment and/or Version	3.4.12
Product Category	Customer Premise Equipment
System Background	
Previous certifications	None.
Tracking	
UCCO ID	1300906
System Tracking Program ID	4744
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013
Remarks	
Test Organization(s)	Joint Interoperability Test Command, Fort Huachuca, Arizona
LEGEND:	
ID	Identification
UCCO	Unified Capabilities Connection Office

2. SYSTEM DESCRIPTION. The SUT keeps track of the current location for authorized Voice over Internet Protocol (VoIP) terminal phones, authorized VoIP soft phones, and any other authorized VoIP telephony devices. VoIP soft phones are not tested and are not included in this certification. An authorized VoIP telephony device is characterized by a Media Access Control (MAC) address and extension number that is registered with the Call Server (i.e., IP Public Branch Exchange). The location is based on the Client-defined mapping of Ethernet switch port ranges to physical locations. The extension/direct inward dialing number, Switch Internet Protocol (IP) address, switch port, and Emergency Response Location (ERL) that is the location associated with the switch and switch port are integrated directly into the Amcom Personal Computer (PC)/Public Safety Answering Point (PSAP) VoIP database tables. An ERL is the building address and the specific location within the building (i.e., Third Floor, Room 305).

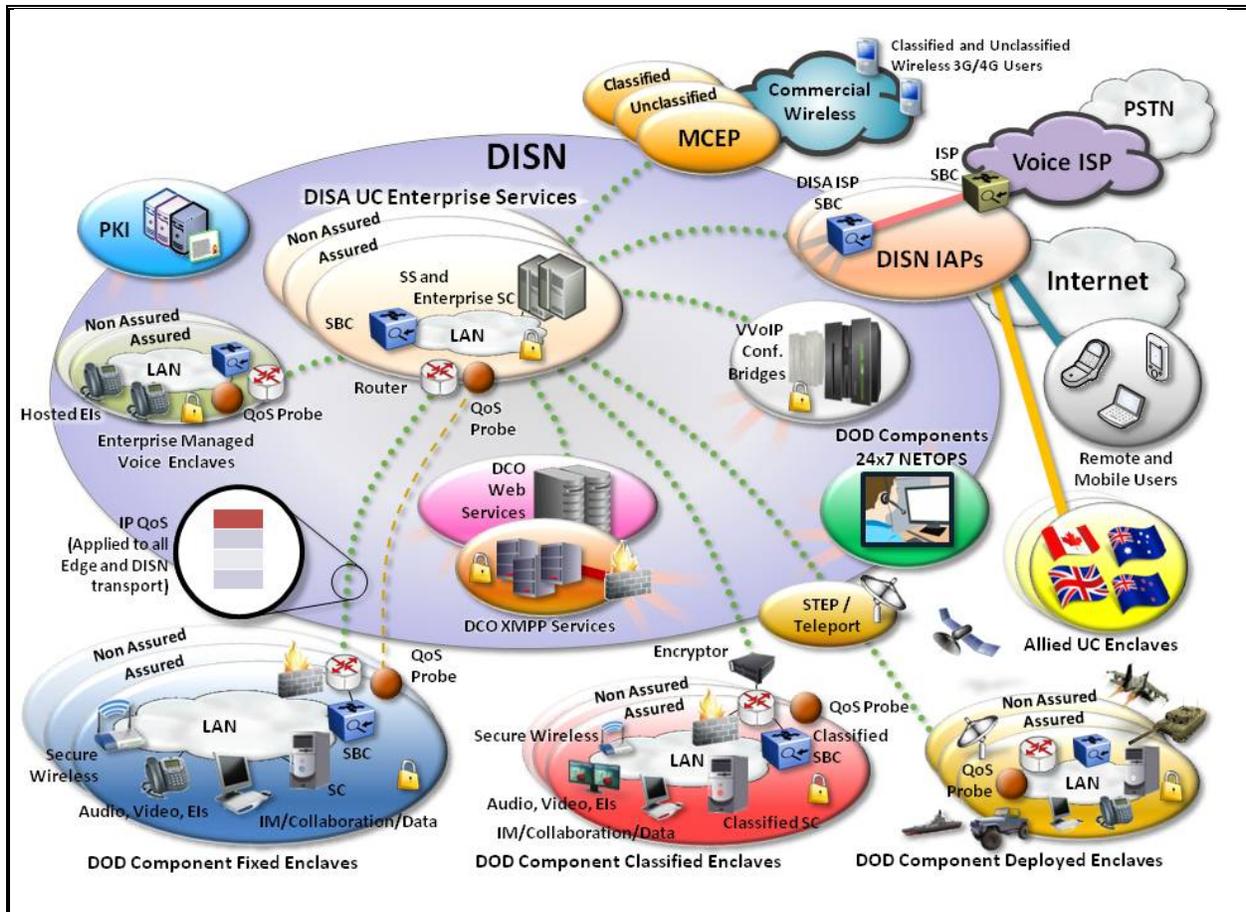
The location of the wired VoIP End Instrument (EI) is determined by querying the Management Information Base (MIB) of the site-provided Assured Services Local Area Network (ASLAN) access layer switch that the VoIP EI is connected to identifying the switch, switch port, and MAC address of the VoIP EI connected to each switch port. As a device is connected to a switch port, there is an option for the switch to be configured to generate a Simple Network Management Protocol (SNMP) trap or configured to a management system that relays the trap to the SUT. In response to the trap, the SUT determines the switch port (and therefore the location)

to which a VoIP telephony device that caused the trap is connected via SNMP querying. Optionally, a periodic scheduled MIB scan on all data switches can be performed as a means of ensuring that device connections are determined even when a SNMP trap is lost. As a result, the VoIP tracking gateway has the location of the device and the phone number to associate with the device.

3. OPERATIONAL ARCHITECTURE. The Unified Capabilities (UC) architecture is a two-level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and Service/Agency installation switches. The Department of Defense (DoD) Chief Information Officer (CIO) and Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The UC architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the notional operational UC architecture in which the SUT may be used.

4. TEST CONFIGURATION. The test team tested the SUT at JITC, Fort Huachuca, Arizona in a manner and configuration similar to that of a notional operational environment. Testing of the system's required functions and features was conducted using the test configuration depicted in Figure 2-2. Information Assurance testing used the same configuration.

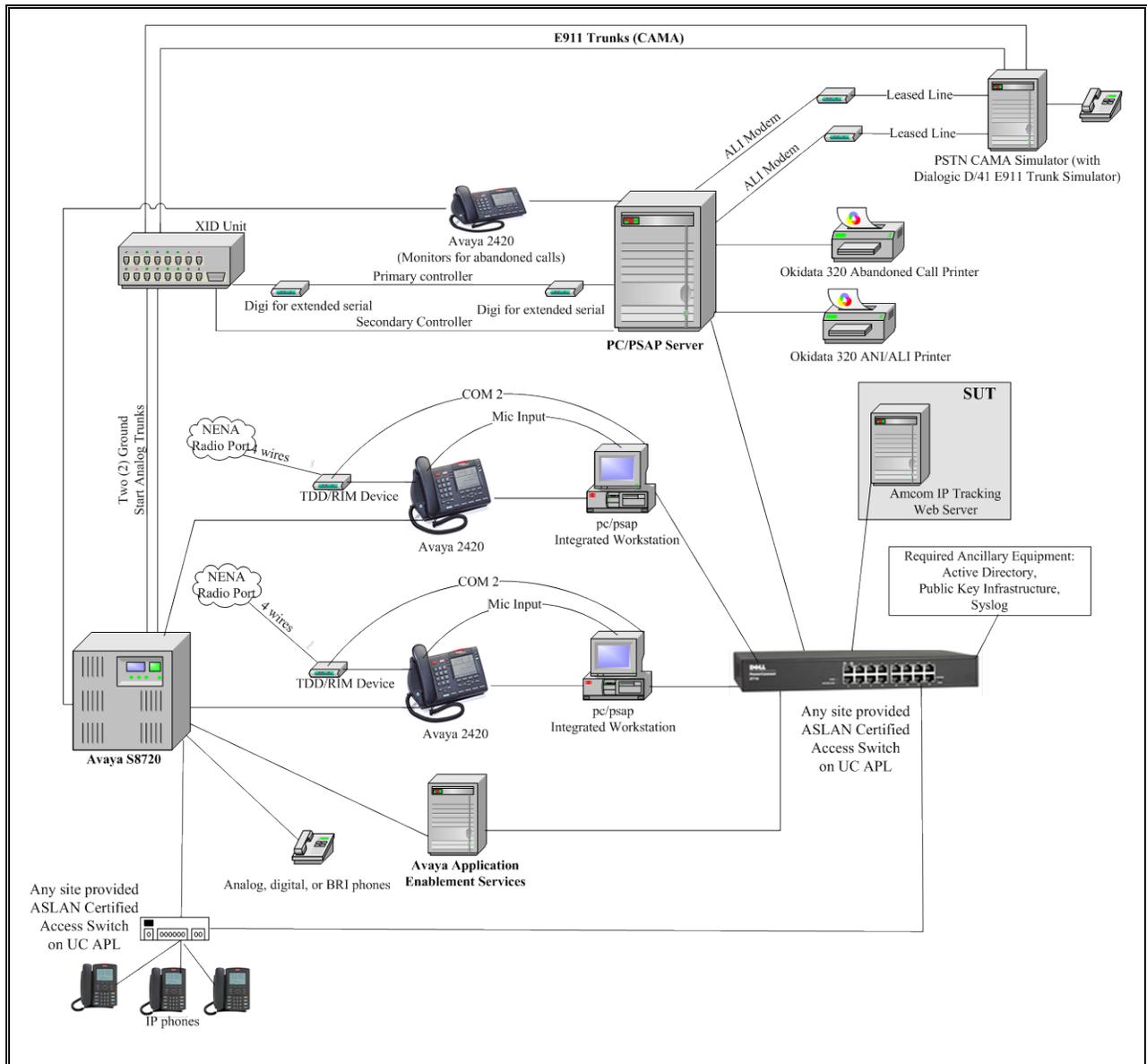
5. METHODOLOGY. Testing was conducted using Customer Premises Equipment (CPE) requirements derived from the Unified Capabilities Requirements (UCR) 2013, Reference (c), and CPE test procedures, Reference (d). Any discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of DISA via a vendor Plan of Action and Milestones, which will address all new critical Test Discrepancy Reports within 120 days of identification.



LEGEND:

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

Figure 2-1. Notional UC Network Architecture



LEGEND:

AES	Application Enablement Services	Mbps	Megabits per second
ALI	Automatic Location Information	Mic	Microphone
ANI	Automatic Number Indication	NENA	National Emergency Number Association
APL	Approved Products List	PC/PSAP	Personal Computer/Public Safety Answering Point
ASLAN	Assured Services Local Area Network	PSTN	Public Switched Telephone Network
BRI	Basic Rate Interface	RIM	Radio Interface Module
CAMA	Centralized Automatic Message Accounting	SUT	System Under Test
COM	Communications Port	TDD	Telecommunications Devid for the Deaf
CS	Communication Server	UC	Unified Capabilities
E911	Enhanced 911 Service	XID	Trunk Interface Device
IP	Internet Protocol		

Figure 2-2. SUT Test Configuration with the Avaya S8720

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS. The interface, Capability Requirements (CR), and Functional Requirements (FR) for UC Customer Premise Equipment (CPE) are established by UCR 2013, section 3.7.2.

a. Requirements

(1) If a CPE device supports Multilevel Precedence and Preemption (MLPP), then that device shall do so in accordance with the requirements listed in Section 2.25.2, MLPP, and shall not affect the Defense Switch Network (DSN) interface features and functions associated with line supervision and control. The SUT does not support this conditional requirement.

(2) All DSN CPE, at a minimum, must meet the requirements of Part 15 and Part 68 of the Federal Communications Commission (FCC) Rules and Regulations, and the Administrative Council for Terminal Attachments. The SUT met this requirement with the vendor's Letters of Compliance (LoC).

(3) If a CPE device supports autoanswer, then that device shall have an "autoanswer" mode feature allowing the autoanswer mode to be set to a "time" more than the equivalency of four ROUTINE precedence ring intervals, in accordance with Section 2.25.2, MLPP, before "answer" supervision is provided. The SUT does not support this conditional requirement.

(4) If a CPE device is required to support precedence calls above ROUTINE precedence, then that device shall respond properly to an incoming alerting (ringing) precedence call cadence, as described in Section 2.9.1.2.1, UC Ringing Tones, Cadences, and Information Signals. The SUT does not support this conditional requirement.

(5) If a CPE device can "out dial" Dual Tone Multi Frequency (DTMF) and/or dial pulse (DP) digits (automatic and/or manual), then that device shall comply with the requirements as specified in Telcordia Technologies GR-506-CORE, LSSGR: Signaling for Analog Interfaces, Issue 1, June 1996, paragraph 10. That device shall also be capable of outpulsing and interpretation of DTMF digits on outgoing and two-way trunks as specified in Telcordia Technologies GR-506-CORE, LSSGR: Signaling for Analog Interfaces, Issue 1, June 1996, paragraph 15, and Table 3.7-1. The SUT does not support this conditional requirement.

(6) If a CPE device contains a modem or facsimile machine, then that modem or facsimile machine shall be compatible with International Telecommunications Union (ITU) and Telcordia standards, as applicable. The SUT does not support this conditional requirement.

(7) If a CPE device contains a facsimile device, then that facsimile device, at a minimum, shall meet the requirements in accordance with applicable DoD Information Technology (IT) Standards Registry (DISR) standards. The SUT does not support this conditional requirement.

(8) If Configuration Management and/or Fault Management is provided by the CPE device so that it can be managed by the Advanced DSN Integrated Management Support System (ADIMSS) or other management systems, then the management information for that CPE device shall be provided by one or more of the following serial or Ethernet interfaces:

(a) Serial interfaces shall be in accordance with one of the following standards:

1. ITU-T Recommendation V.35
2. TIA-232-F
3. EIA-449-1
4. TIA-530-A

(b) Ethernet interfaces shall be in accordance with Institute of Electrical and Electronics Engineers (IEEE) 802.3-2002.

The SUT does not support this conditional requirement.

(9) If a CPE device supports 911 and E911 emergency services, then, at a minimum, the 911 and the E911 (tandem) emergency services shall have the capability to “hold” (prevent) the originating subscriber or caller from releasing the call, via the “switch supervision interaction for line and trunk control by the called party” feature, in accordance with Telcordia Technologies GR-529-CORE. Additionally, the FCC regulations regarding 911 and E911 must be considered. The SUT does not support this conditional requirement.

b. Differentiated Services Code Point (DSCP) Requirements. Products that supports IP interfaces shall support the DSCP plan, as shown in Table 7.2-3. Differentiated Services (DS) assignments shall be software configurable for the full range of six bit values (0-63 Base10). Request For Comments (RFC) 2474 defines the DS field. In IP version 4 (IPv4), it defines the layout of the Type of Service (TOS) octet. In IP version 6 (IPv6), it defines the layout in the Traffic Class octet. This requirement was met with testing. The Wireshark test tool was used to capture the DSCP values. The SUT successfully demonstrated it could configure DSCP values from 0-63 for both IPv4 and IPv6.

c. IPv6 Requirements. UCR 2013, section 5, Table 5.2-1 states that if a CPE device supports IP interfaces, then the CPE shall support the IPv6 requirements as defined for Network Appliance/Simple Server in UCR Section 5, IPv6. The SUT server is based on the Microsoft 2008 operating system which fully supports IPv6; however, due to limitations in our test network we were not able to test IPv6 end-to-end. Although the SUT was not tested using IPv6, the requirements were met with the vendor’s LoC.

d. Functionality Testing. There are no specific functionality requirements in the UCR for this type of CPE. JITC tested and verified the IP Phone Tracking Gateway’s ability to provide ALI database updates to the AMCOM Inc., PC/PSAP when changes to IP EI switch locations in real time. The test included updating the ALI database with the required the IP EI location

information, such as MAC address, the port number, physical address, building number, room number, 10-digit phone number, and changing the port numbers. The initial information and port number connection changes for the IP EI was verified on the PC/PSAP workstation display when PSAP agent answered the emergency call from the IP EI.

Changes to the port numbers were accomplished by moving the connection from port 4 to port 5 and back to its original configuration on the same access switch to simulate a move or relocation. The changes in port numbers and associated location changes were verified on the PC/PSAP workstation display when PSAP agent answered emergency calls from the associated IP EI.

f. Hardware/Software/Firmware Version Identification: Table 3-3 provides the SUT components' hardware, software, and firmware tested. The JITC tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

7. TESTING LIMITATIONS. JITC test teams noted the following testing limitations including the impact they may have on interpretation of the results and conclusions. Any untested requirements are also included in the testing limitations.

The SUT requirement to meet IPv6 based on the NA/SS IPv6 profile was only met by vendor's LoC. The SUT server is based on the Microsoft 2008 operating system which fully supports IPv6 and the ability to configure the DSCP value to any value from 0-63; however, due to limitations in our test network we were not able to test IPv6 end-to-end.

8. CONCLUSION(S). The SUT meets the critical interoperability requirements for a UC CPE in accordance with the UCR and is certified for joint use with any Amcom Inc. PC/PSAP listed on the Approved Products List (APL). The SUT is also certified for use with any ASLAN access layer switch that has been or is on the UC APL. The SUT meets the interoperability requirements for the interfaces listed in Table 3-1.

DATA TABLES

Table 3-1. Interface Status

Interface	Threshold CR/FR Requirements (See note.)	Status	Remarks												
Interfaces															
IEEE 802.3u (10/100 BaseT)	1, 2, 3	Met	The SUT met the critical CRs and FRs for this interface.												
<p>NOTE: The UCR does not identify interface CR/FR applicability. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column are cross-referenced with Table 3.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 15%;">CR</td> <td style="width: 40%;">Capability Requirements</td> <td style="width: 15%;">ID</td> <td style="width: 30%;">Identification</td> </tr> <tr> <td>FR</td> <td>Functional Requirements</td> <td>IP</td> <td>Internet Protocol</td> </tr> <tr> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> <td>SUT</td> <td>System Under Test</td> </tr> </table>				CR	Capability Requirements	ID	Identification	FR	Functional Requirements	IP	Internet Protocol	IEEE	Institute of Electrical and Electronics Engineers	SUT	System Under Test
CR	Capability Requirements	ID	Identification												
FR	Functional Requirements	IP	Internet Protocol												
IEEE	Institute of Electrical and Electronics Engineers	SUT	System Under Test												

Table 3-2. Capability and Functional Requirements and Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status																
1	Customer Premise Equipment Requirements (R)	3.7.2	Met																
2	Differentiated Services Code Point Tagging Requirements (R)	Table 7.2-3	Met																
3	Internet Protocol version 6 Requirements (R)	Table 5.2-1	Met (See note 2.)																
<p>NOTES:</p> <p>1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Table 3-5.</p> <p>2. The IPv6 requirements were met with the vendor's LoC. The IPv6 requirements were not validated through testing due to limitations of the test network.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 15%;">CR</td> <td style="width: 30%;">Capability Requirement</td> <td style="width: 15%;">LoC</td> <td style="width: 40%;">Letter of Compliance</td> </tr> <tr> <td>FR</td> <td>Functional Requirement</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>IPv6</td> <td>Internet Protocol version 6</td> <td></td> <td></td> </tr> </table>				CR	Capability Requirement	LoC	Letter of Compliance	FR	Functional Requirement	SUT	System Under Test	ID	Identification	UCR	Unified Capabilities Requirements	IPv6	Internet Protocol version 6		
CR	Capability Requirement	LoC	Letter of Compliance																
FR	Functional Requirement	SUT	System Under Test																
ID	Identification	UCR	Unified Capabilities Requirements																
IPv6	Internet Protocol version 6																		

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

Component	Release	Sub-component	Function								
IP Phone Tracking Gateway Server (Dell Power Edge R320)	3.4.12	Windows 2008 Server R2 SP2 Microsoft SQL 2008 R2 XnEtrack version 3.4.20 NetworkTrapService version 1.0.3.0 SwitchTracking version 1.5.2.0 AvayaPush version 1.3 AvayaInventory version 1.3.0.7	Application/Database Server								
<p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 15%;">IP</td> <td style="width: 30%;">Internet Protocol</td> <td style="width: 15%;">SP2</td> <td style="width: 40%;">Service Pack 2</td> </tr> <tr> <td>R2</td> <td>Release 2</td> <td>SUT</td> <td>System Under Test</td> </tr> </table>				IP	Internet Protocol	SP2	Service Pack 2	R2	Release 2	SUT	System Under Test
IP	Internet Protocol	SP2	Service Pack 2								
R2	Release 2	SUT	System Under Test								

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

System Name	Software Release	Function
Required Ancillary Equipment		
Active Directory		
Public Key Infrastructure		
SysLog Server		

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

System Name	Software Release	Function																				
Test Network Components																						
Avaya S8720	Communication Manager (CM) 4.0 (R014x.00.2.731.7: Super Patch 14419)	SMEO																				
Amcom PC/PSAP (See note 1.)	11.11.0.21	PC/PSAP																				
Avaya 9620	Ha 96XXr3_171bs.bin	IP End Instrument																				
Cisco CP7960G	P00308010200	IP End Instrument																				
Dell PowerConnect 3524 (See note 2.)	2.0.0.29	Access switch																				
Cisco Catalyst 3560	IOS 12.2(35) SE5	Access switch																				
<p>NOTES:</p> <p>1. The SUT was tested and is certified with the Amcom PC/PSAP Release 11.11.0.21. JITC analysis determined that the SUT is certified with any Amcom PC/PSAP that has been or is on the UC APL.</p> <p>2. The SUT was tested with an ASLAN access layer switch and is therefore certified with any ASLAN access switch that has been or is on the UC APL.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 33%;">APL</td> <td style="width: 33%;">Approved Products List</td> <td style="width: 33%;">PC/PSAP</td> <td style="width: 33%;">Personal Computer/Public Safety Answering Point</td> </tr> <tr> <td>ASLAN</td> <td>Assured Services Local Area Network</td> <td>SMEO</td> <td>Small End Office</td> </tr> <tr> <td>IOS</td> <td>Internetwork Operating System</td> <td>UC</td> <td>Unified Capabilities</td> </tr> <tr> <td>IP</td> <td>Internet Protocol</td> <td></td> <td></td> </tr> <tr> <td>JITC</td> <td>Joint Interoperability Test Command</td> <td></td> <td></td> </tr> </table>			APL	Approved Products List	PC/PSAP	Personal Computer/Public Safety Answering Point	ASLAN	Assured Services Local Area Network	SMEO	Small End Office	IOS	Internetwork Operating System	UC	Unified Capabilities	IP	Internet Protocol			JITC	Joint Interoperability Test Command		
APL	Approved Products List	PC/PSAP	Personal Computer/Public Safety Answering Point																			
ASLAN	Assured Services Local Area Network	SMEO	Small End Office																			
IOS	Internetwork Operating System	UC	Unified Capabilities																			
IP	Internet Protocol																					
JITC	Joint Interoperability Test Command																					

Table 3-5. Products Capability/Functional Requirements

ID	Requirement	UCR Ref (UCR 2013)	LoC/TP ID	CPE
1	3.7.2 – CPE Requirements			
1-1	If a CPE device supports MLPP, then that device shall do so in accordance with the requirements listed in Section 2.25.2, Multilevel Precedence and Preemption, and shall not affect the DSN interface features and functions associated with line supervision and control.	3.7.2 AUX-006140	T	C
1-2	All DSN CPE, at a minimum, must meet the requirements of Part 15 and Part 68 of the FCC Rules and Regulations, and the Administrative Council for Terminal Attachments (ACTA).	3.7.2 AUX-006150	L	R
1-3	If a CPE device supports autoanswer, then that device shall have an “autoanswer” mode feature allowing the autoanswer mode to be set to a “time” more than the equivalency of four ROUTINE precedence ring intervals, in accordance with Section 2.25.2, Multilevel Precedence and Preemption, before “answer” supervision is provided.	3.7.2 AUX-006160	T	C
1-4	If a CPE device is required to support precedence calls above ROUTINE precedence, then that device shall respond properly to an incoming alerting (ringing) precedence call cadence, as described in Section 2.9.1.2.1, UC Ringing Tones, Cadences, and Information Signals.	3.7.2 AUX-006170	L/T	C
1-5	If a CPE device can “out dial” DTMF and/or dial pulse (DP) digits (automatic and/or manual), then that device shall comply with the requirements as specified in Telcordia Technologies GR-506-CORE, LSSGR: Signaling for Analog Interfaces, Issue 1, June 1996, paragraph 10. That device shall also be capable of outpulsing and interpretation of DTMF digits on outgoing and two-way trunks as specified in Telcordia Technologies GR-506-CORE, LSSGR: Signaling for Analog Interfaces, Issue 1, June 1996, paragraph 15, and Table 3.7-1.	3.7.2 AUX-006180	L	C
1-6	If a CPE device contains a modem or facsimile machine, then that modem or facsimile machine shall be compatible with ITU and Telcordia standards, as applicable.	3.7.2 AUX-006190	L	C
1-7	If a CPE device contains a facsimile device, then that facsimile device, at a minimum, shall meet the requirements in accordance with applicable DoD Information Technology (IT) Standards Registry (DISR) standards.	3.7.2 AUX-006200	L	C

Table 3-5. Products Capability/Functional Requirements (continued)

ID	Requirement	UCR Ref (UCR 2013)	LoC/TP ID	CPE
1	3.7.2 – CPE Requirements (continued)			
1-8	If Configuration Management and/or Fault Management is provided by the CPE device so that it can be managed by the Advanced DSN Integrated Management Support System (ADIMSS) or other management systems, then the management information for that CPE device shall be provided by one or more of the following serial or Ethernet interfaces: Serial interfaces shall be in accordance with one of the following standards: ITU-T Recommendation V.35. TIA-232-F. EIA-449-1. TIA-530-A. Ethernet interfaces shall be in accordance with IEEE 802.3-2002.	3.7.2 AUX-006210	L	C
1-9	If a CPE device supports 911 and E911 emergency services, then, at a minimum, the 911 and the E911 (tandem) emergency services shall have the capability to “hold” (prevent) the originating subscriber or caller from releasing the call, via the “switch supervision interaction for line and trunk control by the called party” feature, in accordance with Telcordia Technologies GR-529-CORE. Additionally, the FCC regulations regarding 911 and E911 must be considered.	3.7.2 AUX-006220	L/T IO-1	C
2	Table 7.2-3 – DSCP Tagging Requirements			
2-1	Products that supports IP interfaces shall support the DSCP plan, as shown in Table 7.2-3. Differentiated Services (DS) assignments shall be software configurable for the full range of six bit values (0-63 Base10).	7.2.1 EDG-000160	T	R
3	5.2 – IPv6 Requirements			
3-1	If a CPE device supports IP interfaces, then the CPE shall support the IPv6 requirements as defined for NA/SS in UCR Section 5, IPv6. Refer to Table 3-6.	Table 5.2-1	L	R
LEGEND:				
C	Conditional	ITU	International Telecommunication Union	
CPE	Customer Premise Equipment	L	LoC Item	
DoD	Department of Defense	LoC	Letter(s) of Compliance	
DSCP	Differentiated Services Code Point	LSSGR	Local Access and Transport Area (LATA) Switching	
DSN	Defense Switched Network		Systems Generic Requirements	
DTMF	Dual Tone Multi Frequency	MLPP	Multi-level Precedence and Preemption	
EIA	Electronic Industries Alliance	NA/SS	Network Appliance/Simple Server	
FCC	Federal Communications Commission	R	Required	
GR	Generic Requirement	TIA	Telecommunications Industry Association	
ID	Identification	TP	Test Plan	
IEEE	Institute of Electrical and Electronics Engineers	UC	Unified Capabilities	
IP	Internet Protocol	UCR	Unified Capabilities Requirements	
IPv6	Internet Protocol version 6			

Table 3-6. IPv6 Requirements

ID	5.2 – IPv6 Requirements			
3-1	The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	5.2.1 IP6-000010	L	R
3-2	Dual-stack end points or Call Connection Agents (CCAs) shall be configured to choose IPv4 over IPv6.	5.2.1 IP6-000020	L	R
3-3	All nodes and interfaces that are “IPv6-capable” must be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a deliberate transition strategy. This includes the stateless autoconfiguration of link-local addresses. Nodes with multiple network interfaces may need to be separately configured per interface.	5.2.1 IP6-000030	L	R
3-4	The system shall provide the same (or equivalent) functionality in IPv6 as in IPv4 consistent with the requirements in the UCR for its Approved Products List (APL) category. NOTE: This requirement applies only to products that are required to perform IPv6 functionality.	5.2.1 IP6-000050	L	R

Table 3-6. IPv6 Requirements (continued)

5.2 – IPv6 Requirements (continued)				
3-5	The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.	5.2.1 IP6-000060	L	R
3-6	The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464. NOTE: This requirement does not mandate that the remaining sections of RFC 2464 have to be implemented.	5.2.1 IP6-000070	L	R
3-7	The product shall support a minimum MTU of 1280 bytes as described in RFC 2460 and updated by RFC 5095.	5.2.1.1 IP6-000090	L	R
3-8	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, then the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet.	5.2.1.1 IP6-000100	L	C
3-9	The product shall not use the Flow Label field as described in RFC 2460.	5.2.1.2 IP6-000110	L	R
3-10	The product shall be capable of setting the Flow Label field to zero when originating a packet.	5.2.1.2 IP6-000120	L	R
3-11	The product shall be capable of ignoring the Flow Label field when receiving packets.	5.2.1.2 IP6-000140	L	R
3-12	The product shall support the IPv6 Addressing Architecture as described in RFC 4291.	5.2.1.3 IP6-000150	L	R
3-13	The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	5.2.1.3 IP6-000160	L	R
3-14	If a scoped address (RFC 4007) is used, then the product shall use a scope index value of zero when the default zone is intended.	5.2.1.3 IP6-000170	L	C
3-15	If Dynamic Host Configuration Protocol (DHCP) is supported within an IPv6 environment, then it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315.	5.2.1.4 IP6-000180	L	C
3-16	If the product is a DHCPv6 client, then the product shall discard any messages that contain options that are not allowed to appear in the received message type (e.g., an Identity Association option in an Information-Request message).	5.2.1.4 IP6-000200	L	C
3-17	If the product 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, then the client shall continue with a client-initiated message exchange by sending a Request message.	5.2.1.4 IP6-000220	L	C
3-18	If the product is a DHCPv6 client and the DHCPv6 solicitation message exchange fails, then it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event occurs.	5.2.1.4 IP6-000230	L	C
3-19	If the product is a DHCPv6 client and it sends an Information-Request message, then it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server.	5.2.1.4 IP6-000240	L	C
3-20	If the product is a DHCPv6 client, then it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server before transmitting packets using that address for itself.	5.2.1.4 IP6-000250	L	C
3-21	If the product is a DHCPv6 client, then it shall log all reconfigure events. NOTE: Some systems may not be able to log all this information (e.g., the system may not have access to this information).	5.2.1.4 IP6-000260	L	C
3-22	If the product supports DHCPv6 and uses authentication, then it shall discard unauthenticated DHCPv6 messages from UC products and log the event.	5.2.1.4 IP6-000270	L	C
3-23	The product shall support Neighbor Discovery for IPv6 as described in RFC 4861.	5.2.1.5 IP6-000280	L	R
3-24	The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for any cast addresses or solicited proxy advertisements.	5.2.1.5 IP6-000300	L	R
3-25	When a valid “Neighbor Advertisement” message is received by the product and the product neighbor cache does not contain the target’s entry, the advertisement shall be silently discarded.	5.2.1.5 IP6-000310	L	R
3-26	When a valid “Neighbor Advertisement” message is received by the product and the product 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 product shall silently discard the received advertisement.	5.2.1.5 IP6-000320	L	R

Table 3-6. IPv6 Requirements (continued)

ID	5.2 – IPv6 Requirements (continued)			
3-27	When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache.	5.2.1.5 IP6-000330	L	R
3-28	The product shall support the ability to configure the product to ignore Redirect messages.	5.2.1.5.1 IP6-000340	L	R
3-29	The product shall only accept Redirect messages from the same router as is currently being used for that destination.	5.2.1.5.1 IP6-000350	L	R
3-30	If "Redirect" messages are allowed, then the product shall update its destination cache in accordance with the validated Redirect message.	5.2.1.5.1 IP6-000360	L	C
3-31	If the valid "Redirect" message is allowed and no entry exists in the destination cache, then the product shall create an entry.	5.2.1.5.1 IP6-000370	L	C
3-32	If redirects are supported, then the device shall support the ability to disable this functionality.	5.2.1.5.1 IP6-000380	L	C
3-33	The product shall prefer routers that are reachable over routers whose reachability is suspect or unknown.	5.2.1.5.2 IP6-000400	L	R
3-34	If the product supports stateless IP address autoconfiguration including those provided for the commercial market, then the product shall support IPv6 Stateless Address Autoconfiguration (SLAAC) for interfaces supporting UC functions in accordance with RFC 4862.	5.2.1.6 IP6-000420	L	C
3-35	If the product supports IPv6 SLAAC, then the product shall have a configurable parameter that allows the function to be enabled and disabled. Specifically, the product 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 autoconfiguration.	5.2.1.6 IP6-000430	L	C
3-36	If the product supports IPv6 SLAAC, then the product shall have the configurable parameter set not to perform stateless autoconfiguration.	5.2.1.6 IP6-000440	L	C
3-37	While nodes are not required to autoconfigure their addresses using SLAAC, all IPv6 Nodes shall support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862. In accordance with RFC 4862, DAD shall be implemented and shall be on by default. Exceptions to the use of DAD are noted in the following text.	5.2.1.6 IP6-000450	L	R
3-38	A node MUST allow for autoconfiguration-related variable to be configured by system management for each multicast-capable interface to include DupAddrDetectTransmits where a value of zero indicates that DAD is not performed on tentative addresses as specified in RFC 4862.	5.2.1.6 IP6-000460	L	R
3-39	The product shall support manual assignment of IPv6 addresses.	5.2.1.6 IP6-000470	L	R
3-40	The product shall support the Internet Control Message Protocol (ICMP) for IPv6 as described in RFC 4443.	5.2.1.7 IP6-000520	L	R
3-41	The product shall support the capability to enable or disable the ability of the product to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.	5.2.1.7 IP6-000540	L	R
3-42	The product 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.	5.2.1.7 IP6-000550	L	R
3-43	The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them.	5.2.1.7 IP6-000560	L	R
3-44	The product shall support MLD as described in RFC 2710.	5.2.1.8 IP6-000680	L	R
3-45	If the product uses IPSec, then the product shall be compatible with the Security Architecture for the IPSec described in RFC 4301.	5.2.1.9 IP6-000690	L	C
3-46	If RFC 4301 is supported, then the product shall not support the mixing of IPv4 and IPv6 in a SA.	5.2.1.9 IP6-000700	L	C
3-47	If RFC 4301 is supported, then the product's security association database (SAD) cache shall have a method to uniquely identify a SAD entry.	5.2.1.9 IP6-000710	L	C
3-48	If RFC 4301 is supported, then the product shall implement IPSec to operate with both integrity and confidentiality.	5.2.1.9 IP6-000720	L	C
3-49	If RFC 4301 is supported, then the product shall be capable of enabling and disabling the ability of the product to send an ICMP message informing the sender that an outbound packet was discarded.	5.2.1.9 IP6-000730	L	C
3-50	If an ICMP outbound packet message is allowed, then the product shall be capable of rate limiting the transmission of ICMP responses.	5.2.1.9 IP6-000740	L	C
3-51	If RFC 4301 is supported, then the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.	5.2.1.9 IP6-000750	L	C

Table 3-6. IPv6 Requirements (continued)

ID	5.2 – IPv6 Requirements (continued)			
3-52	If RFC 4301 is supported, and the product receives a packet that does not match any SPD cache entries, and the product determines it should be discarded, then the product 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.	5.2.1.9 IP6-000760	L	C
3-53	If RFC 4301 is supported, then the product should include a management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECTORS.	5.2.1.9 IP6-000770	L	C
3-54	If RFC 4301 is supported, then the product shall support the ESP Protocol in accordance with RFC 4303.	5.2.1.9 IP6-000780	L	C
3-55	If RFC 4303 is supported, then the product shall be capable of enabling anti-replay.	5.2.1.9 IP6-000790	L	C
3-56	If RFC 4303 is supported, then the product 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.	5.2.1.9 IP6-000800	L	C
3-57	If RFC 4301 is supported, then the product shall support IKEv1 as defined in RFC 2409.	5.2.1.9 IP6-000810	L	C
3-58	To prevent a Denial of Services (DoS) attack on the initiator of an IKE_SA, the initiator shall accept multiple responses to its first message, treat each as potentially legitimate, respond to it, and then discard all the invalid half-open connections when it receives a valid cryptographically protected response to any one of its requests. Once a cryptographically valid response is received, all subsequent responses shall be ignored whether or not they are cryptographically valid.	5.2.1.9 IP6-000820	L	C
3-59	If RFC 4301 is supported, then the product shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.	5.2.1.9 IP6-000830	L	C
3-60	If RFC 4301 is supported, then the product shall support the ISAKMP as defined in RFC 2408.	5.2.1.9 IP6-000840	L	C
3-61	If the product supports the IPSec Authentication Header Mode, then the product shall support the IP Authentication Header (AH) as defined in RFC 4302.	5.2.1.9 IP6-000850	L	C
3-62	If RFC 4301 is supported, then the product shall support manual keying of IPSec.	5.2.1.9 IP6-000860	L	C
3-63	If RFC 4301 is supported, then the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined RFC 4835.	5.2.1.9 IP6-000870	L	C
3-64	If RFC 4301 is supported, then the product shall support the IKEv1 security algorithms as defined in RFC 4109.	5.2.1.9 IP6-000880	L	C
3-65	If the product uses Uniform Resource Identifiers (URIs) in combination with IPv6, then the product shall use the URI syntax described in RFC 3986.	5.2.1.10 IP6-000990	L	C
3-66	If the product uses the Domain Name Service (DNS) resolver for IPv6 based queries, then the product shall conform to RFC 3596 for DNS queries.	5.2.1.10 IP6-001000	L	C
3-67	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 Secure Real-Time Transport Control Protocol (SRTCP) overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.	5.2.1.11 IP6-001010	L	R
3-68	The product shall forward packets using the same IP version as the version in the received packet.	5.2.1.12 IP6-001040	L	R
3-69	When the product is establishing media streams from dual-stacked appliances for AS-SIP signaled sessions, the product shall use the Alternative Network Address Type (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091.	5.2.1.12 IP6-001050	L	R

Table 3-6. IPv6 Requirements (continued)

ID	5.2 – IPv6 Requirements (continued)			
3-70	<p>If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a unicast address, then the product shall support generation and processing of unicast IPv6 addresses having the following formats:</p> <ul style="list-style-type: none"> • x:x:x:x:x:x:x (where x is the hexadecimal values of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A. • x:x:x:x:x:d.d.d.d (where x is the hexadecimal values of the six high-order 16-bit pieces of the address, and d is the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). For example, 1080:0:0:0:8:800:116.23.135.22. 	5.2.1.13 IP6-001060	L	C
3-71	<p>If the product is using AS-SIP, then the product shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats:</p> <ul style="list-style-type: none"> • x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A. • 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. 	5.2.1.13 IP6-001070	L	C
3-72	<p>If the product 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), then the product shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.</p>	5.2.1.13 IP6-001080	L	C
3-73	<p>If the product is using AS-SIP, and the <addrtype> is IPv6, then the product shall support the use of RFC 4566 for IPv6 in SDP as described in AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs.</p>	5.2.1.13 IP6-001090	L	C
3-74	<p>If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is an IPv6 multicast group address, then the multicast connection address shall not have a Time To Live (TTL) value appended to the address as IPv6 multicast does not use TTL scoping.</p>	5.2.1.13 IP6-001100	L	C
3-75	<p>If the product is using AS-SIP, then the product 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.</p>	5.2.1.13 IP6-001110	L	C
3-76	<p>The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 2, Session Control Products, and Section 6, Network Infrastructure End-to-End Performance, plain text DSCP plan.</p>	5.2.1.14 IP6-001150	L	R
3-77	<p>If the product acts as an IPv6 tunnel broker, then the product shall support the function as defined in RFC 3053.</p>	5.2.1.14 IP6-001160	L	C

Table 3-6. IPv6 Requirements (continued)

ID	5.2 – IPv6 Requirements (continued)				
3-78	If the CPE has an IP interface, then the CPE must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.		Table 5.2-1	L	R
	RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP	Table 5.2-4	L	C
	RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)	Table 5.2-4	L	C
	RFC 2409	The Internet Key Exchange (IKE)	Table 5.2-4	L	C
	RFC 2460	Internet Protocol, Version 6 (IPv6) Specification	Table 5.2-4	L	R-2
	RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Table 5.2-4	L	R-3
	RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	Table 5.2-4	L	R-4
	RFC 2710	Multicast Listener Discovery (MLD) for IPv6	Table 5.2-4	L	R-8
	RFC 3053	IPv6 Tunnel Broker	Table 5.2-4	L	C
	RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	Table 5.2-4	L	C
	RFC 3596	DNS Extensions to Support IPv6	Table 5.2-4	L	C
	RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	Table 5.2-4	L	C
	RFC 4007	IPv6 Scoped Address Architecture	Table 5.2-4	L	R
	RFC 4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	Table 5.2-4	L	R
	RFC 4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	Table 5.2-4	L	R
	RFC 4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	Table 5.2-4	L	C
	RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	Table 5.2-4	L	R-1
	RFC 4291	IP Version 6 Addressing Architecture	Table 5.2-4	L	R
	RFC 4301	Security Architecture for the Internet Protocol	Table 5.2-4	L	C
	RFC 4302	IP Authentication Header	Table 5.2-4	L	C
RFC 4303	IP Encapsulating Security Payload (ESP)	Table 5.2-4	L	C	
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Table 5.2-4	L	R	
RFC 4566	SDP: Session Description Protocol	Table 5.2-4	L	C	
RFC 4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	Table 5.2-4	L	C	
RFC 4861	Neighbor Discovery for IP Version 6 (IPv6)	Table 5.2-4	L	R	
RFC 4862	IPv6 Stateless Address Autoconfiguration	Table 5.2-4	L	C	
RFC 5095	Deprecation of Type 0 Routing Headers in IPv6	Table 5.2-4	L	R	
LEGEND:					
C	Conditional	L	LoC Item		
CPE	Customer Premise Equipment	LoC	Letter(s) of Compliance		
DoD	Department of Defense	LSSGR	Local Access and Transport Area (LATA) Switching Systems Generic Requirements		
DSN	Defense Switched Network	MLPP	Multi-level Precedence and Preemption		
DTMF	Dual Tone Multi Frequency	R	Required		
EIA	Electronic Industries Alliance	TIA	Telecommunications Industry Association		
FCC	Federal Communications Commission	TP	Test Plan		
GR	Generic Requirement	UC	Unified Capabilities		
ID	Identification	UCR	Unified Capabilities Requirements		
IEEE	Institute of Electrical and Electronics Engineers				
ITU	International Telecommunication Union				