



DEFENSE INFORMATION SYSTEMS AGENCY

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

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

4 Aug 14

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Callware Technologies Callegra.Unified Communications (UC)™ Server with Software Release 6.15-Joint Interoperability Test Command (JITC) Service Pack 1 (SP1)

- 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 UC products.
2. Conditions of Certification. The Callware Callegra.UC with Software Release 6.15 JITC SP1; 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 a CPE without any conditions (see Table 1). This certification expires upon changes that affect interoperability, but no later than three years from the date of the UC Approved Products List (APL) memorandum.

Table 1. Conditions

Table with 3 columns: Condition, Operational Impact, Remarks. Content: Not applicable; the Callware Technologies Callegra.Unified Communications (UC)™ Server with Software Release 6.15-Joint Interoperability Test Command (JITC) Service Pack 1 (SP1) 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 the UC APL product summary.

JITC Memo, JTE, Joint Interoperability Certification of the Callware Technologies Callegra.Unified Communications (UC)TM Server with Software Release 6.15-Joint Interoperability Test Command (JITC) Service Pack 1 (SP1)

Table 2. SUT Interface Status

Interface	Threshold CR/FR Requirements (See note 1.)	Status	Remarks																								
Interfaces																											
Serial TIA-232F	1	Met	The SUT met the critical CRs and FRs for this interface.																								
IEEE 802.3-2002	1, 2, 3	Met	The SUT met the critical CRs and FRs for this interface. (See note 2.)																								
2-Wire Analog Loop Start Line	1	Met	The SUT met the critical CRs and FRs for the interface. (See note 2.)																								
Avaya CS1000M 2-Wire Proprietary Digital Line	1 (See note 5.)	Met	The SUT met the critical CRs and FRs for the interface. (See note 2.)																								
Avaya CS2100 2-Wire Proprietary Digital Line	1	Met	The SUT met the critical CRs and FRs for the interface. (See note 2.)																								
<p>NOTES:</p> <p>1. The UCR does not identify interface CR/FR applicability.</p> <p>2. The conditional IPv6 compliance was met with the vendor's LoC because the switches and Local Session Controllers only support IPv4 for Network Management. Network Management requirements were tested and verified using IPv4.</p> <p>3. The UCR does not identify interface CR/FR applicability.</p> <p>4. The SUT interface to this interface is bridged only and not directly connected.</p> <p>5. The UCR does not include requirements for proprietary interfaces. The SUT interface to the M3905 digital phone was tested using the Avaya CS1000M 2-wire proprietary digital interface as depicted in Figure 2-2</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 20%;">CRs</td> <td style="width: 30%;">Capability Requirements</td> <td style="width: 20%;">LoC</td> <td style="width: 30%;">Letters of Compliance</td> </tr> <tr> <td>FRs</td> <td>Functional Requirements</td> <td>Mbps</td> <td>Megabits per second</td> </tr> <tr> <td>IEEE 802.3-2002</td> <td>Institute of Electrical and Electronics Engineers</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>IP</td> <td>Internet Protocol</td> <td>TIA</td> <td>Telecommunications Industry Association</td> </tr> <tr> <td>IPv4</td> <td>Internet Protocol version 4</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>				CRs	Capability Requirements	LoC	Letters of Compliance	FRs	Functional Requirements	Mbps	Megabits per second	IEEE 802.3-2002	Institute of Electrical and Electronics Engineers	SUT	System Under Test	IP	Internet Protocol	TIA	Telecommunications Industry Association	IPv4	Internet Protocol version 4	UCR	Unified Capabilities Requirements	IPv6	Internet Protocol version 6		
CRs	Capability Requirements	LoC	Letters of Compliance																								
FRs	Functional Requirements	Mbps	Megabits per second																								
IEEE 802.3-2002	Institute of Electrical and Electronics Engineers	SUT	System Under Test																								
IP	Internet Protocol	TIA	Telecommunications Industry Association																								
IPv4	Internet Protocol version 4	UCR	Unified Capabilities Requirements																								
IPv6	Internet Protocol version 6																										

Table 3. SUT Capability Requirements and Functional Requirements 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												
<p>NOTE: The annotation of "required" refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.</p> <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 20%;">CR</td> <td style="width: 30%;">Capability Requirement</td> <td style="width: 20%;">R</td> <td style="width: 30%;">Required</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> </table>				CR	Capability Requirement	R	Required	FR	Functional Requirement	SUT	System Under Test	ID	Identification	UCR	Unified Capabilities Requirements
CR	Capability Requirement	R	Required												
FR	Functional Requirement	SUT	System Under Test												
ID	Identification	UCR	Unified Capabilities Requirements												

JITC Memo, JTE, Joint Interoperability Certification of the Callware Technologies Callegra.Unified Communications (UC)TM Server with Software Release 6.15-Joint Interoperability Test Command (JITC) Service Pack 1 (SP1)

Table 4. UC APL Product Summary

Product Identification			
Product Name	Callware Callegra.UC		
Software Release	6.15 Joint Interoperability Test Command (JITC) Service Pack (SP1)		
UC Product Type(s)	CPE		
Product Description	Voice Mail, Auto Attendant		
Product Components (See note.)	Component Name	Version	Remarks
VMWare server	ESXi Server (VMWare)	5.1.0	
Data server	Data Server	6.15-JITC, Microsoft Windows 2008 Server R2	
Database server	Database Server	6.15-JITC, SQL Server 2008 R2	
Telephony server	Telephony Server	6.15-JITC, Microsoft Windows 2008 Server R2	
Media server	Media Server	6.15-JITC, RedHat Enterprise Linux (RHEL) 6.5/2.6.32 Kernel	
Dialogic card	Dialogic Card	5.0.34 Service Update – 5.0.34	
NOTE: The detailed component and subcomponent list is provided in Enclosure 3.			
LEGEND:			
APL	Approved Products List	SQL	Structured Query Language
CPE	Customer Premise Equipment	VM	Virtual Machine
R2	Release 2	UC	Unified Capabilities

4. Test Details. This certification is based on interoperability testing, review of the vendor’s Letters of Compliance (LoC), and DISA Certifying Authority (CA) Recommendation for inclusion on the UC Approved Products List (APL). Testing was conducted at JITC’s Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 17 through 27 February 2014 using test procedures derived from Reference (d). Review of the vendor’s LoC was completed on 27 January 2014. Information Assurance (IA) testing was conducted by DISA-led IA test teams and the results are 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 the interface, capability, and functional requirements.

5. Additional Information. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Sensitive but Unclassified 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>.

JITC Memo, JTE, Joint Interoperability Certification of the Callware Technologies Callegra.Unified Communications (UC)TM Server with Software Release 6.15-Joint Interoperability Test Command (JITC) Service Pack 1 (SP1)

6. **Point of Contact (POC).** The JITC point of contact is Ms. Anita Brown, commercial telephone (520) 538-5164, DSN telephone 879-5164, FAX DSN 879-4347; e-mail address anita.l.brown53.civ@mail.mil; mailing address Joint Interoperability Test Command, ATTN: JTE (Ms. Anita Brown) P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The UCCO tracking number for the SUT is 1320001.

FOR THE COMMANDER:


for RIC HARRISON
Chief
Networks/Communications and UC Portfolio

3 Enclosures a/s

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, Errata 1," 1 July 2013

(d) Joint Interoperability Test Command, "Unified Capabilities Test Plan (UCTP)," Draft

(e) Joint Interoperability Test Command, "Information Assurance Finding Summary For Callware Technologies Inc. (CTI), Callegra.Unified Communications (UC) Release (Rel.) 6.15 Service Pack (SP) 1 Joint Interoperability Test Command (JITC) (Tracking Number 1320001)," Draft

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The Callware Technologies Callegra.Unified Communications (UC)TM Server with Software Release 6.15-Joint Interoperability Test Command (JITC) Service Pack 1 (SP1) 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	United States Navy		
Sponsor Point of Contact	Jon Marcy, e-mail: jon.marcy.ctr@navy.mil		
Vendor Point of Contact	Chris Toomer, Callware Technologies, 9100 South 500 West Sandy,Utah 84070, e-mail:ctoomer@callware.com		
System Name	Callware Callegra.UC		
Increment and/or Version	6.15 JITC SP1		
Product Category	Customer Premise Equipment		
System Background			
Previous certifications	Previous JITC certification 6.14		
Tracking			
UCCO ID	1320001		
System Tracking Program ID	STP System # 4733, Test/Activity # 11728		
Requirements Source			
Unified Capabilities Requirements	Unified Capabilities Requirements 2013, Errata 1		
Remarks			
Test Organization(s)	JITC		
LEGEND:			
AO	Action Officer	SP	Service Pack
ID	Identification	UC	Unified Capabilities
JITC	Joint Interoperability Test Command	UCCO	Unified Capabilities Connection Office

2. SYSTEM DESCRIPTION. The SUT offers an integrated automated attendant (Auto Attendant) and voice messaging (Voicemail) solution that expands to include speech recognition. The SUT also offers additional unified messaging advantages such as fax services, browser-based voice and fax messaging, and e-mail integration including text-to-speech. The SUT was designed with an extensible markup language based N-tier (N denotes any number; i.e., 2, 3, 10, etc.), object-oriented, distributed architecture allowing it to scale from a full-featured four-port voicemail system up to a very large network of unified communication installations. Client applications are supported on the desktop versions of Microsoft Windows that are approved for use within the Department of Defense. The SUT utilizes a graphical interface for system setup and administration.

The SUT offers both an integrated Auto Attendant and Voicemail functionality, and includes the following optional applications: CallegraVOICETM, CallegraFAXTM, CallegraINBOXTM, CallegraCOMMUNITYTM, CallegraWEBTM, and CallegraTTSTM. The SUT also offers the Callegra.UC SDKTM application, which was not tested and is not covered under this certification. All Callware applications run on the Callegra.UCTM Server and are administered using the included Microsoft Management Console (MMC) module. CallegraADMINTM for MMC is an

integral part of the SUT. The SUT consists of the Callegra Client Workstation, CWDataCenter, CWTelephonyServer, CWDataCenter-CallegraRECOVERY(Principal), CWDataCenter-CallegraRECOVERY(Mirror), and Data Distribution Device. The following are descriptions of the applications covered by this certification:

The Callegra.UC™ Server offers integrated Auto Attendant and Voicemail and expands to include speech recognition. The following features are supported by this application:

- Multiple Private Branch Exchange (PBX) integration methods across multiple PBX manufacturers
- Diagnostic tracing
- Multi-tenanting
- Multi-site networking
- On-line help and documentation
- Fax tone auto-transfer
- Box alias table (inbound routing)
- Dial string translation (outbound routing)

The Auto Attendant can be used as the primary reception, answering all incoming calls, or it can be set up to provide overflow or secondary support for a live receptionist. The following features are supported by this application:

- “0” for operator or another extension
- Multiple call routing options. Audiotext boxes within Callegra systems can offer up to 250 distinct call routing options per box. Audiotext boxes are used mainly for auto attendant trees and can also be used for unlimited announcement applications, general information, and call routing capabilities without messaging capability
- Direct to voice mail transfer
- Directory look-up
- Scheduled greetings
- Holiday greetings
- Message edit and delivery options
- Auto transfers

CallegraADMIN™ for MMC is an integral part of the SUT. All Callware applications run on the Callegra.UC™ Server and are administered using the included MMC module. The following features are offered by this application:

- Local or remote access for Callegra administrators
- Real time dynamic box administration
- Global distribution lists
- System utilities

CallegraVOICE™ brings speech-enabled call routing and auto attendant functionality to the SUT through the use of speech recognition technology. The following features are supported by this application:

- Voice activated call routing
- Speech enabled employee directory

- Speech enabled directory for box owners

CallegraFAX™ module allows incoming faxes to be delivered to the SUT. The following features are supported by this application:

- Message waiting indicator
- Pager notification
- Telephone notification
- Directory look-up
- E-mail notification including Short Message Service (SMS) paging to compatible devices

CallegraWEB™ for Internet Explorer is a browser-based Internet client giving the SUT the ability to access and control voice and fax messages over the Internet. The following features are supported by this application:

- Accessing voice messages via the internet
- Accessing faxes via the internet
- Sending voice messages via the internet
- Sending faxes via the internet

CallegraINBOX™ for Microsoft Outlook provides complete voice and fax integration with Microsoft Outlook. The following features are supported by this application:

- Microsoft Outlook 2000 and XP
- Windows 98, ME, NT4.0, 2000, XP
- Mail server independent
- Callegra options menu
- Passcode protected
- Telephone and multimedia support
- Intuitive visual message control
- Send and forward as e-mail
- Confidential and urgent messaging
- Integrated Callegra address book
- Fax print driver
- Fax viewers
- Xerox TextBridge Optical Character Recognition
- Sent fax log
- Message store controls
- Personal greeting controls
- Remote Internet Protocol (IP) access
- Notification control

CallegraCOMMUNITY™ provides a method of sending voice messages from one Callegra.UC™ system to another in a Callegra Voice Profile for Internet Mail (CVPIM) network environment. CallegraCOMMUNITY™ will allow a network of independent Callegra.UC™ systems to exchange messages in a loosely-coupled environment. This message exchange will

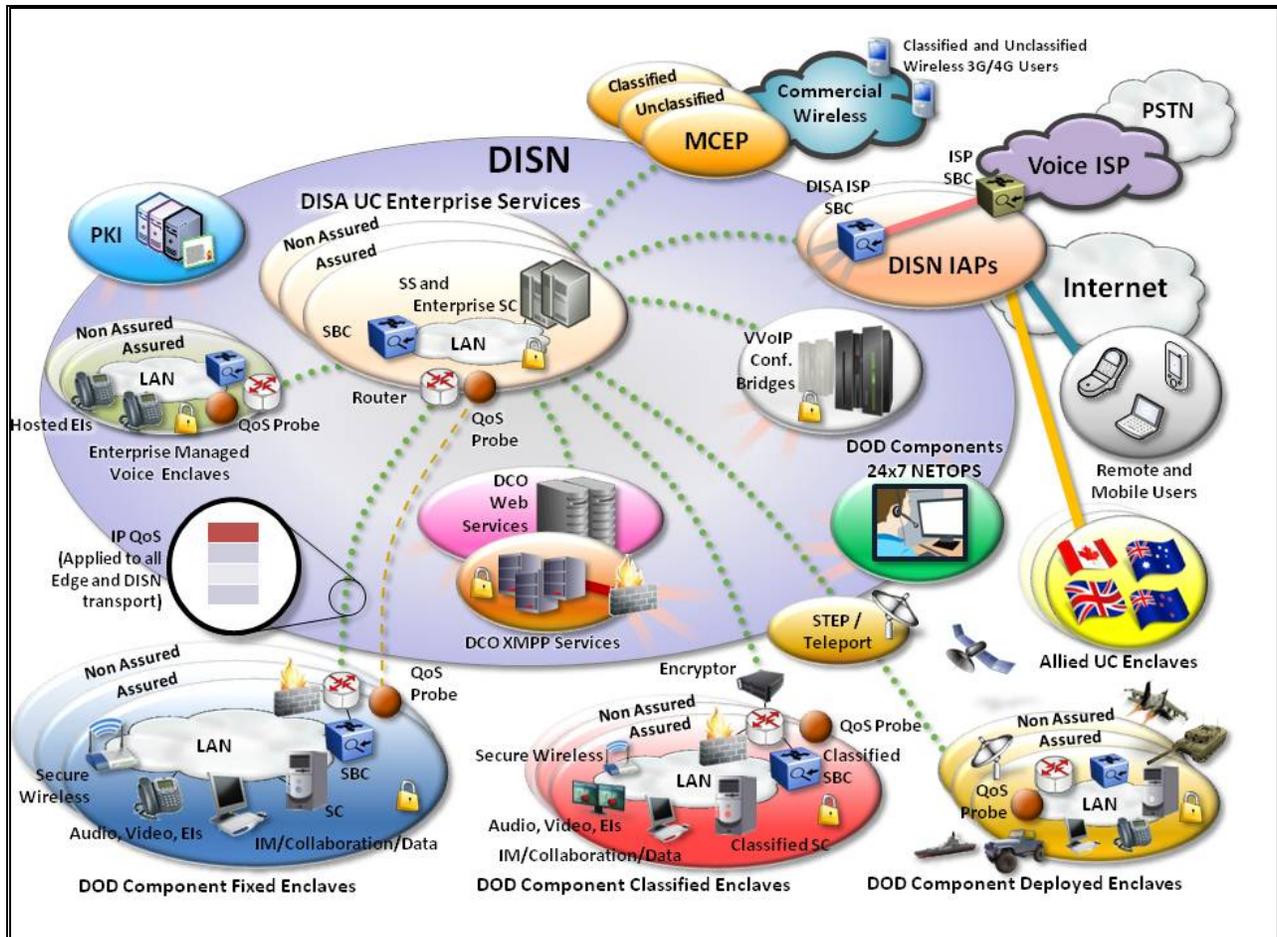
be achieved through CVPIM. CVPIM is a method for encoding voicemail messages as data, enabling travel via the Simple Mail Transfer Protocol (SMTP) mail protocol over IP networks.

CallegraTTS™ provides callers with the ability to call into the Callegra.UC voice mail system and listen to their e-mail messages as they are converted from text to speech via the Telephone User Interface (TUI). CallegraTTS™ also plays the distributed Datacenter server names when using CallegraCOMMUNITY™ in a CVPIM IP network and outputs the information over the TUI.

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 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 (POA&M), which will address all new critical Test Discrepancy Reports (TDRs) 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 Instrument	SBC	Session Border Controller
IAP	Internet 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

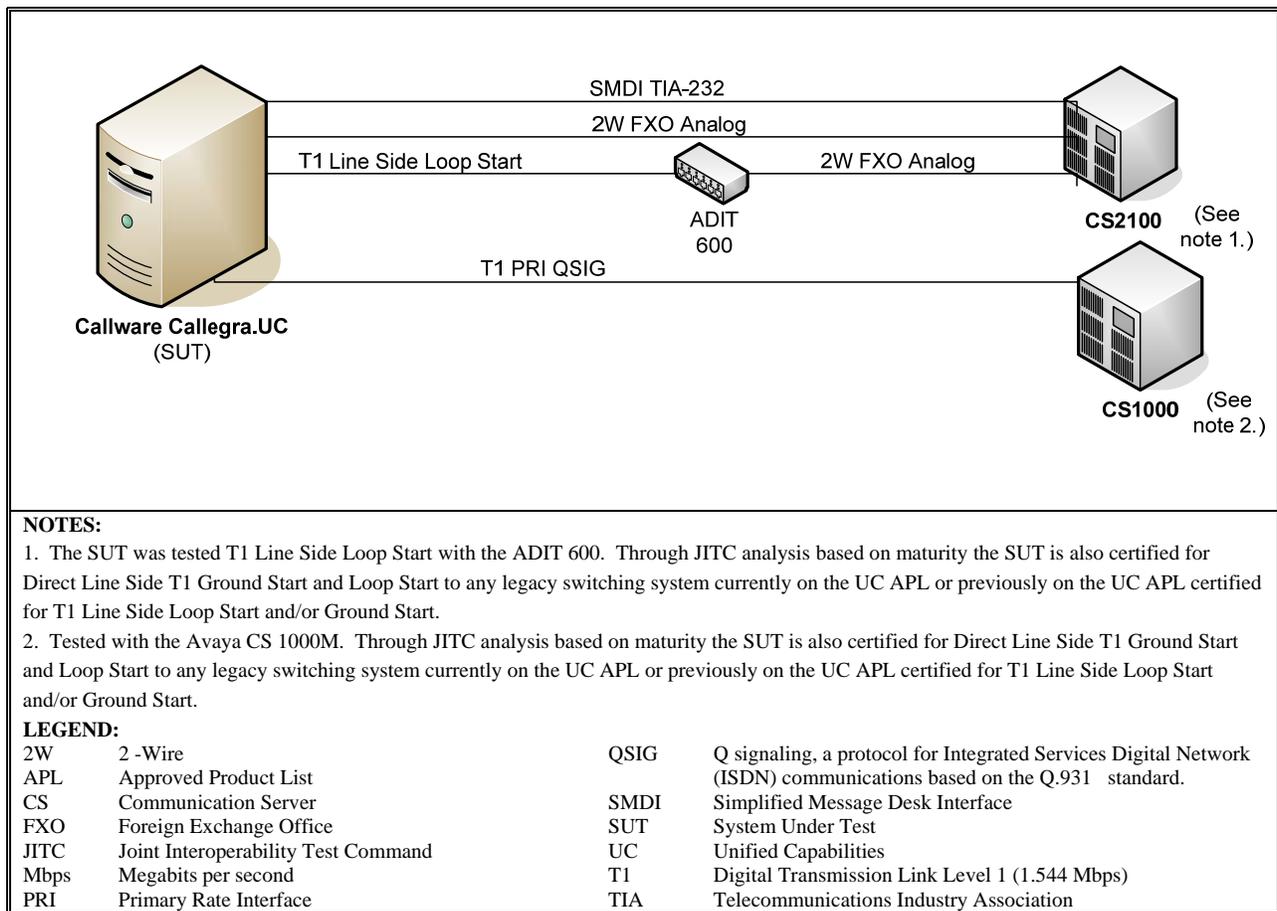


Figure 2-2. SUT Test Configuration

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

a. CPE Requirements

(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. 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 (ACTA). 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, Multilevel Precedence and Preemption, before “answer” supervision is provided. The SUT met 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” 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 met this conditional requirement.

(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. Although the SUT supports this conditional requirement, it was not tested and is not covered under this certification.

(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. Although the SUT supports this conditional requirement, it was not tested and is not covered under this certification.

(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 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. This functionality is not a feature of the SUT, but rather the local base switch and the E911 (tandem) emergency services switch in accordance with Telcordia Technologies GR-529-CORE. Additionally, the FCC regulations regarding 911 and E911 must be considered.

b. Differentiated Services Code Point (DSCP) Requirements. Products that support 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). RFC 2474 defines the DS field. In IPv4, it defines the layout of the Type of Service (TOS) octet. In 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 NA/SS in UCR Section 5, IPv6. The SUT met this requirement with the vendor’s LoC. The SUT was tested using IPv4. The interfaces to the Avaya CS1000M, CS2100 and NEC 3C series switches.

d. 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. None.

8. CONCLUSION(S). The SUT meets the critical interoperability requirements for a CPE in accordance with the UCR and is certified for joint use with other UC Products listed on the Approved Products List (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 1.)	Status	Remarks																								
Interfaces																											
Serial TIA-232F	1	Met	The SUT met the critical CRs and FRs for this interface.																								
IEEE 802.3-2002	2, 3	Met	The SUT met the critical CRs and FRs for this interface. (See note 2.)																								
2-Wire Analog Loop Start Line	3	Met	The SUT met the critical CRs and FRs for the interface. (See note 2.)																								
Avaya CS1000M 2-Wire Proprietary Digital Line	3 (See note 5.)	Met	The SUT met the critical CRs and FRs for the interface. (See note 2.)																								
Avaya CS2100 2-Wire Proprietary Digital Line		Met	The SUT met the critical CRs and FRs for the interface. (See note 2.)																								
<p>NOTES:</p> <ol style="list-style-type: none"> 1. The UCR does not identify interface CR/FR applicability. 2. The conditional IPv6 compliance was met with the vendor's LoC because the switches and Local Session Controllers only support IPv4 for Network Management. Network Management requirements were tested and verified using IPv4. 3. The UCR does not identify interface CR/FR applicability. 4. The SUT interface to this interface is bridged only and not directly connected. 5. The UCR does not include requirements for proprietary interfaces. The SUT interface to the M3905 digital phone was tested using the Avaya CS1000M 2-wire proprietary digital interface as depicted in Figure 2-2 <p>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 25%;">CRs</td> <td style="width: 50%;">Capability Requirements</td> <td style="width: 25%;">LoC</td> <td style="width: 25%;">Letters of Compliance</td> </tr> <tr> <td>FRs</td> <td>Functional Requirements</td> <td>Mbps</td> <td>Megabits per second</td> </tr> <tr> <td>IEEE 802.3-2002</td> <td>Institute of Electrical and Electronics Engineers</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>IP</td> <td>Internet Protocol</td> <td>TIA</td> <td>Telecommunications Industry Association</td> </tr> <tr> <td>IPv4</td> <td>Internet Protocol version 4</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>				CRs	Capability Requirements	LoC	Letters of Compliance	FRs	Functional Requirements	Mbps	Megabits per second	IEEE 802.3-2002	Institute of Electrical and Electronics Engineers	SUT	System Under Test	IP	Internet Protocol	TIA	Telecommunications Industry Association	IPv4	Internet Protocol version 4	UCR	Unified Capabilities Requirements	IPv6	Internet Protocol version 6		
CRs	Capability Requirements	LoC	Letters of Compliance																								
FRs	Functional Requirements	Mbps	Megabits per second																								
IEEE 802.3-2002	Institute of Electrical and Electronics Engineers	SUT	System Under Test																								
IP	Internet Protocol	TIA	Telecommunications Industry Association																								
IPv4	Internet Protocol version 4	UCR	Unified Capabilities Requirements																								
IPv6	Internet Protocol version 6																										

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																
<p>NOTES: 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>LEGEND:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 25%;">CR</td> <td style="width: 50%;">Capability Requirement</td> <td style="width: 25%;">IPv4</td> <td style="width: 25%;">Internet Protocol version 4</td> </tr> <tr> <td>DISA</td> <td>Defense Information Systems Agency</td> <td>IPv6</td> <td>Internet Protocol version 6</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> </table>				CR	Capability Requirement	IPv4	Internet Protocol version 4	DISA	Defense Information Systems Agency	IPv6	Internet Protocol version 6	FR	Functional Requirement	SUT	System Under Test	ID	Identification	UCR	Unified Capabilities Requirements
CR	Capability Requirement	IPv4	Internet Protocol version 4																
DISA	Defense Information Systems Agency	IPv6	Internet Protocol version 6																
FR	Functional Requirement	SUT	System Under Test																
ID	Identification	UCR	Unified Capabilities Requirements																

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

Component	Release	Sub-component	Function
ESXi Server (VMWare)	5.1.0	Not Applicable	VMWare server
Data Server	6.15-JITC, Microsoft Windows 2008 Server R2	Not Applicable	Data server
Database Server	6.15-JITC, SQL Server 2008 R2	Not Applicable	Database Server
Telephony Server	6.15-JITC, Microsoft Windows 2008 Server R2	Not Applicable	Telephony Server
Media Server	6.15-JITC, RedHat Enterprise Linux (RHEL) 6.5/2.6.32 Kernel	Not Applicable	Media Server
Dialogic Analog Card (D/120 JCT) Dialogic Card (D/480JCT-2T1)	5.0.34 Service Update – 5.0.34	Not Applicable	Dialogic Card
LEGEND:			
APL	Approved Products List	SQL	Structured Query Language
CPE	Customer Premise Equipment	VM	Virtual Machine
R2	Release 2	UC	Unified Capabilities

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

Callware Callegra.UC	Software Release 6.15 SP1	Voicemail, Autoattendant	
Required Ancillary Equipment (site provides)			
Public Key Infrastructure			
Active Directory			
Test Network Components			
Avaya CS2100 w/SMDI	SE09.1	MFSS	
Avaya CS1000M	Succession DSN 5.0	SMEO	
NEC 3C	Version 8.5.	LSC	
ADIT 600	Not Applicable	Channel Bank	
LEGEND:			
DSN	Defense Switched Network	SMDI	Simplified Message Desk Interface
LSC	Local Session Controller	SMEO	Small End Office
MFSS	Multifunction Softswitch	SP	Service Pack
SE	Succession Enterprise	UC	Unified Capabilities

Table 3-5. Products Capability/Functional Requirements

CR/FR ID	Requirement	UCR Ref (UCR 2013 Errata 1)	LoC/ TP ID	R/O/C
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 IO-1	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 IO-2	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 IO-3	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/T IO-4	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/T IO-5	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/T IO-5	C
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/T IO-6	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-7	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	L/T IO-8	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

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

LEGEND:			
C	Conditional	ITU	International Telecommunication Union
CPE	Customer Premise Equipment	L	LoC Item
DoD	Department of Defense	LoC	Letter(s) of Compliance
DSN	Defense Switched Network	LSSGR	Local Access and Transport Area (LATA) Switching
DTMF	Dual Tone Multi Frequency		Systems Generic Requirements
EIA	Electronic Industries Alliance	MLPP	Multi-level Precedence and Preemption
FCC	Federal Communications Commission	NA/SS	Network Appliance/Simple Server
GR	Generic Requirement	R	Required
ID	Identification	TIA	Telecommunications Industry Association
IEEE	Institute of Electrical and Electronics Engineers	TP	Test Plan
IP	Internet Protocol	UC	Unified Capabilities
IPv6	Internet Protocol version 6	UCR	Unified Capabilities Requirements

Table 3-6. IPv6 Requirements

ID	Requirement	UCR Ref (UCR 2013 Errata 1)	LoC/ TP ID	CPE
1	5.2 – IPv6 Requirements			
1-1	The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	5.2.1 IP6-000010	L/T	R
1-2	Dual-stack end points or Call Connection Agents (CCAs) shall be configured to choose IPv4 over IPv6.	5.2.1 IP6-000020	L/T	R
1-3	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/T	R
1-4	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 and the feature parity is limited to the functionality tested in accordance with the distributed test laboratory approved test procedures for the category of the product.	5.2.1 IP6-000050	L/T	R
1-5	The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.	5.2.1 IP6-000060	L	R
1-6	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
2	5.2.1.1 – Maximum Transmission Unit			
2-1	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
2-2	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	5.2.1.2 – Flow Label			
3-1	The product shall not use the Flow Label field as described in RFC 2460.	5.2.1.2 IP6-000110	L	R
3-2	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
3-3	The product shall be capable of ignoring the Flow Label field when receiving packets.	5.2.1.2 IP6-000140	L	R
4	5.2.1.3 – Address			
4-1	The product shall support the IPv6 Addressing Architecture as described in RFC 4291.	5.2.1.3 IP6-000150	L	R
4-2	The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	5.2.1.3 IP6-000160	L	R
4-3	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

Table 3-6. IPv6 Requirements (continued)

ID	Requirement	UCR Ref (UCR 2013 Errata 1)	LoC/ TP ID	CPE
5	5.2.1.4 – Dynamic Host Configuration Protocol			
5-1	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
5-2	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
5-3	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
5-4	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
5-5	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
5-6	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
5-7	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
5-8	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
6	5.2.1.5 – Neighbor Discovery			
6-1	The product shall support Neighbor Discovery for IPv6 as described in RFC 4861.	5.2.1.5 IP6-000280	L	R
6-2	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
6-3	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
6-4	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
6-5	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
6-6	The product shall support the ability to configure the product to ignore Redirect messages.	5.2.1.5.1 IP6-000340	L	R
6-7	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
6-8	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
6-9	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
6-10	If redirects are supported, then the device shall support the ability to disable this functionality.	5.2.1.5.1 IP6-000380	L	C
6-11	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
7	5.2.1.6 – Stateless Address Autoconfiguration and Manual Address Assignment			
7-1	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
7-2	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

Table 3-6. IPv6 Requirements (continued)

ID	Requirement	UCR Ref (UCR 2013 Errata 1)	LoC/ TP ID	CPE
7-3	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
7-4	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
7-5	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
7-6	The product shall support manual assignment of IPv6 addresses.	5.2.1.6 IP6-000470	L	R
8	5.2.1.7 – Internet Control Message Protocol			
8-1	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
8-2	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
8-3	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
8-4	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
9	5.2.1.8 – Routing Functions			
9-1	The product shall support MLD as described in RFC 2710.	5.2.1.8 IP6-000680	L	R
10	5.2.1.9 – IP Security			
10-1	If the product uses IPSec, then the product shall be compatible with the Security Architecture for the IPSec described in RFC 4301. a. If RFC 4301 is supported, then the product shall support binding of a SA with a particular context. b. If RFC 4301 is supported, then the product shall be capable of disabling the BYPASS IPSec processing choice.	5.2.1.9 IP6-000690	L	C
10-2	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
10-3	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
10-4	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
10-5	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
10-6	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
10-7	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
10-8	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
10-9	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
10-10	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
10-11	If RFC 4303 is supported, then the product shall be capable of enabling anti-replay.	5.2.1.9 IP6-000790	L	C

Table 3-6. IPv6 Requirements (continued)

ID	Requirement	UCR Ref (UCR 2013 Errata 1)	LoC/ TP ID	CPE
10-12	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
10-13	If RFC 4301 is supported, then the product shall support IKEv1 as defined in RFC 2409.	5.2.1.9 IP6-000810	L	C
10-14	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
10-15	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
10-16	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
10-17	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
10-18	If RFC 4301 is supported, then the product shall support manual keying of IPSec.	5.2.1.9 IP6-000860	L	C
10-19	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
10-20	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
11	5.2.1.10 – Network Management			
11-1	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
11-2	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
12	5.2.1.11 – Traffic Engineering			
12-1	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
13	5.2.1.12 – IP Version Negotiation			
13-1	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
13-2	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
13-3	The product shall prefer any IPv4 address to any IPv6 address when using ANAT semantics.	5.2.1.12 IP6-001050.a	L	R
13-4	The product shall place the option tag “SDP-ANAT” in a Required header field when using ANAT semantics in accordance with RFC 4092.	5.2.1.12 IP6-001050.b	L/T	R
14	5.2.1.13 – Services Session Initiation Protocol IPv6 Unique Requirements			
14-1	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: <ul style="list-style-type: none"> x: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

Table 3-6. IPv6 Requirements (continued)

ID	Requirement	UCR Ref (UCR 2013 Errata 1)	LoC/ TP ID	CPE
14-2	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: <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
14-3	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.	5.2.1.13 IP6-001080	L	C
14-4	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.	5.2.1.13 IP6-001090	L	C
14-5	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.	5.2.1.13 IP6-001100	L	C
14-6	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.	5.2.1.13 IP6-001110	L	C
15	5.2.1.14 – Miscellaneous			
15-1	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.	5.2.1.14 IP6-001150	L	R
15-2	If the product acts as an IPv6 tunnel broker, then the product shall support the function as defined in RFC 3053.	5.2.1.14 IP6-001160	L	C
RFC #	RFC Title	UCR Ref (UCR 2013 Errata 1)	LoC/TP ID	R/O/C (See Note 1)
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

Table 3-6. IPv6 Requirements (continued)

RFC #	RFC Title	UCR Ref (UCR 2013 Errata 1)	LoC/TP ID	R/O/C (See Note 1)																																												
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																																												
<p>NOTE: 1. All CPE IPv6 capabilities are in accordance with NA/SS IPv6 applicability.</p> <p>LEGEND:</p> <table> <tr> <td>C</td> <td>Conditional</td> <td>L</td> <td>LoC Item</td> </tr> <tr> <td>CPE</td> <td>Customer Premise Equipment</td> <td>LoC</td> <td>Letter(s) of Compliance</td> </tr> <tr> <td>DoD</td> <td>Department of Defense</td> <td>LSSGR</td> <td>Local Access and Transport Area (LATA) Switching Systems Generic Requirements</td> </tr> <tr> <td>DSN</td> <td>Defense Switched Network</td> <td>MLPP</td> <td>Multi-level Precedence and Preemption</td> </tr> <tr> <td>DTMF</td> <td>Dual Tone Multi Frequency</td> <td>R</td> <td>Required</td> </tr> <tr> <td>EIA</td> <td>Electronic Industries Alliance</td> <td>TIA</td> <td>Telecommunications Industry Association</td> </tr> <tr> <td>FCC</td> <td>Federal Communications Commission</td> <td>TP</td> <td>Test Plan</td> </tr> <tr> <td>GR</td> <td>Generic Requirement</td> <td>UC</td> <td>Unified Capabilities</td> </tr> <tr> <td>ID</td> <td>Identification</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> <td></td> <td></td> </tr> <tr> <td>ITU</td> <td>International Telecommunication Union</td> <td></td> <td></td> </tr> </table>					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		
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																																															