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

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **8 Nov 13**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Amcom Software Inc, MediaSTAR™, Software Release 13.4.0.44

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, MediaSTAR™, Software Release 13.4.0.44; 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 certified for use with the Avaya Communication Server (CS) 1000M Defense Switched Network (DSN) Release 5.0. JITC analysis determined the SUT is also certified for use with any CS1000E or related switch currently or previously on the UC Approved Products List (APL). The SUT was also tested and certified with the Avaya S8720 CM 4 with Application Enabled (AE) Services Release 6.2. JITC analysis determined any Avaya switches certified with software version CM4 or CM6 are functionally identical to the S8720 CM4 relative to the SUT. Therefore, the SUT is certified for use with any Avaya CM 4 and CM 6 switches that have been or are on the UC APL and are configured with the Avaya AE Services Release 6.2. The certification also includes proprietary digital interfaces utilized by these certified systems. This certification expires upon changes that affect interoperability, but no later than three years from the date of this memorandum.

**Table 1. Conditions**

| Condition | Status | Operational Impact | Remarks |
|---|---|---|---|
| Not applicable; MediaSTAR™, Software Release 13.4.0.44 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 Unified Capabilities (UC) Approved Products List (APL) product summary.

**Table 2. SUT Interface Status**

| Interface | Threshold CR/FR Requirements (See note 1.) | Status | Remarks |
|---|---|---|---|
| **Interfaces (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 3.) | Met | The SUT met the critical CRs and FRs for the interface. (See note 2.) |
| Avaya S8720 Communications Manager 2-Wire Proprietary Digital Line | 1 (See note 4.) | Met | The SUT met the critical CRs and FRs for the interface. (See note 2.) |
| IP (See note 5.) | 2, 3 | Met | The SUT met the critical CRs and FRs for this interface. |

**NOTES:**
1. The UCR does not identify interface CR/FR applicability.
2. The SUT interface to this interface is bridged only and not directly connected.
3. 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.
4. The UCR does not include requirements for proprietary interfaces. The SUT interface to the Avaya 2420 digital phone was tested using the Avaya S8720 Communications Manager 2-wire proprietary digital interface as depicted in Figure 2-2.
5. The SUT provided an IP intra-enclave interface between the MediaSTAR Engine and MediaSTAR Inspector

**LEGEND:**

| | | | |
|---|---|---|---|
| CPE | Customer Premise Equipment | FR | Functional Requirement |
| CR | Capability Requirement | IP | Internet Protocol |
| CS | Communication Server | SUT | System Under Test |

**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 (See note 2.) |
| 3 | Internet Protocol version 6 Requirements (C) | Table 5.2-1 | Met (See note 2.) |

**NOTES:**
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.
2. The IP connectivity of the SUT only exists between the client and the server intra enclave.

**LEGEND:**

| | | | |
|---|---|---|---|
| C | Conditional | R | Required |
| CR | Capability Requirement | SUT | System Under Test |
| FR | Functional Requirement | UCR | Unified Capabilities Requirements |
| ID | Identification | | |

**Table 4. UC APL Product Summary**

| **Product Identification** | | | |
|---|---|---|---|
| Product Name | Amcom Software MediaSTAR$^{TM}$ | | |
| Software Release | Software Release 13.4.0.44 | | |
| UC Product Type(s) | Customer Premise Equipment (CPE) | | |
| Product Description | Passive call logging and recording solution | | |
| **Product Components (See note.)** | **Component Name** | **Version** | **Remarks** |
| MediaSTAR Inspector | Dell Optiplex XE | Windows 7 Professional SP1 with MediaSTARinspector version 13.4.0.42 | |
| MediaSTAR Engine | Dell Power Edge R720 | Windows 2008 Server R2 SP2 MediaSTARengine version 13.4.0.44 | |
| **NOTE:** The detailed component and subcomponent list is provided in Enclosure 3.<br>**LEGEND:**<br>APL Approved Products List<br>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 APL. Testing was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 22 through 26 July 2013 using test procedures derived from Reference (d). Review of the vendor's LoC was completed on 30 August 2013. The DISA CA provided a positive Recommendation on 30 October 2013 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 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.

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 1233802.

FOR THE COMMANDER:

J. T. Schutte

3 Enclosures a/s

for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

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, MARCORSYSCOM, 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, “MediaSTAR CPE Test Procedures,” Draft
(e) Joint Interoperability Test Command, “Information Assurance (IA) Findings Summary For Amcom Software, Inc. MediaSTAR Software Release 13.4.0 (Tracking Number 1233802),” Draft

# CERTIFICATION SUMMARY

**1. SYSTEM AND REQUIREMENTS IDENTIFICATION.** Amcom Software Inc, MediaSTAR$^{TM}$, Software Release 13.4.0.44 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 Prarie, Minnesota 55343, e-mail: berdman@amcomsoft.com |
| System Name | Amcom Software Inc, MediaSTAR$^{TM}$ |
| Increment and/or Version | 13.4.0.44 |
| Product Category | Customer Premise Equipment |
| **System Background** | |
| Previous certifications | None. |
| **Tracking** | |
| UCCO ID | 1233802 |
| System Tracking Program ID | 4743 |
| **Requirements Source** | |
| Unified Capabilities Requirements | Unified Capabilities Requirements 2013 |
| Remarks | |
| **Test Organization(s)** | Joint Interoperability Test Command, Fort Huachuca, Arizona |
| **LEGEND:**<br>ID Identification | <br>UCCO Unified Capabilities Connection Office |

**2. SYSTEM DESCRIPTION.** The SUT is a passive call logging and recording solution, which can improve call center management by providing supervisors with the ability to:

- View operator activity
- See which agents are idle
- View the length of time agents are on a call
- Record all calls to/from agents automatically
- Listen to live phone conversations
- Listen to calls that have been recorded and saved.

The SUT supports traditional call logging and recording system features. The SUT only records analog or digital station side extensions. Calls are recorded along with an embedded date, time, and call duration. Once recorded, calls are searchable in many ways such as position, call duration, date, time, or any comments or flags that have been applied. The SUT accomplishes this via a non-intrusive high-impedance tap to the switch as depicted in the test configuration. The SUT consists of the following components: MediaSTAR Inspector and MediaSTAR Engine. MediaSTAR Inspector and MediaSTAR Engine work together to form the application MediaSTAR.

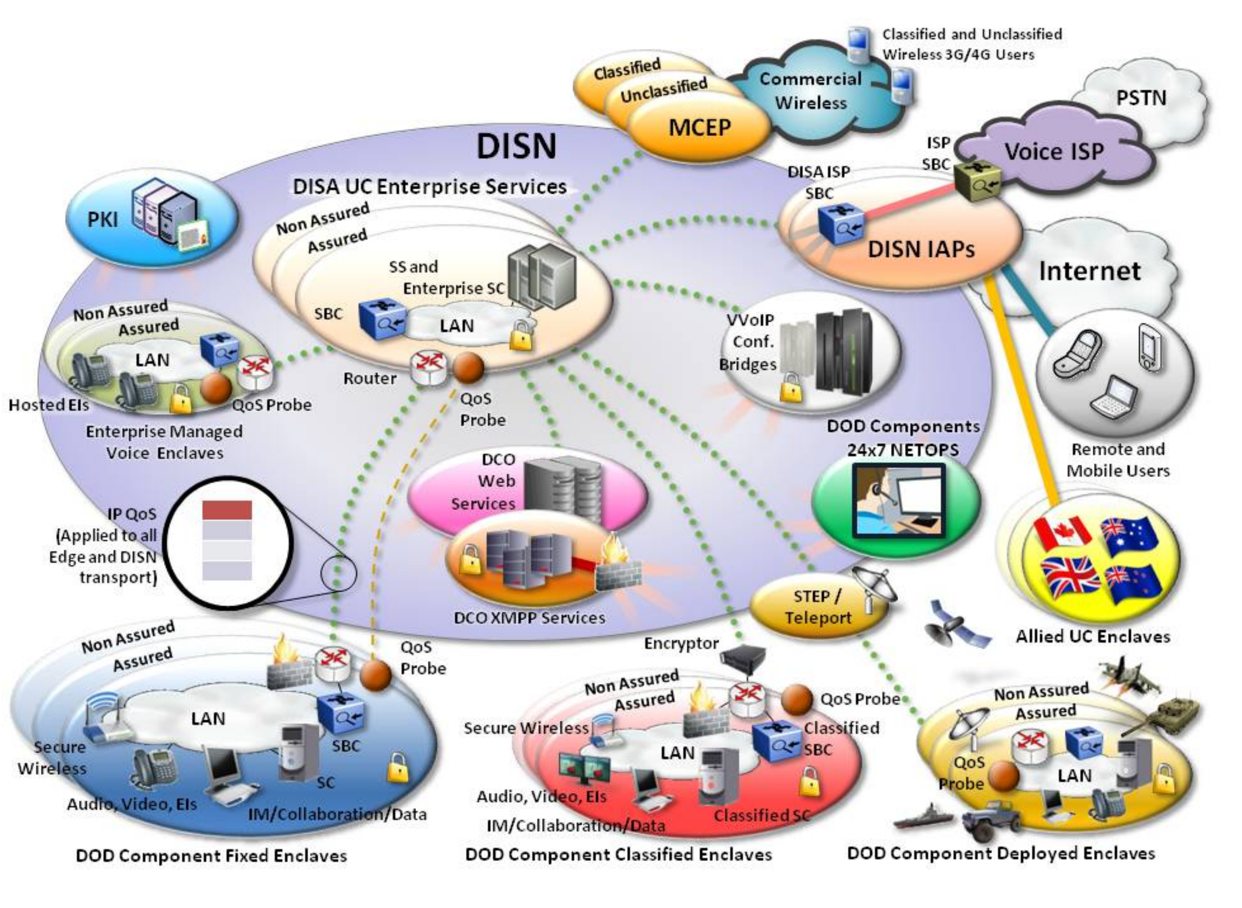
MediaSTAR Inspector. The Inspector module provides a real time user interface for communication between the supervisors and the telephone network. It allows supervisors to monitor telephone line activity by listening in real-time to conversations on selected lines, listening to previously recorded conversations, and displaying statistics, including historical data. The number of Inspectors on the network is unlimited. The MediaSTAR Instpector is loaded on a Microsoft Windows 7 Professional with latest service pack release.

The MediaSTAR Engine is a stand-alone application that can be used to record telephone conversations. The engine monitors telephone line activity, writes all telephone line events to the database, records conversations to disk files in ".wav" format, which can be played back later with any standard audio player, and provides all this information to the MediaSTAR Inspectors in real time via TCP/IP. The MediaSTAR Engine is loaded on a Microsoft Windows® 2008 Server R2 with latest service packs release.

**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.

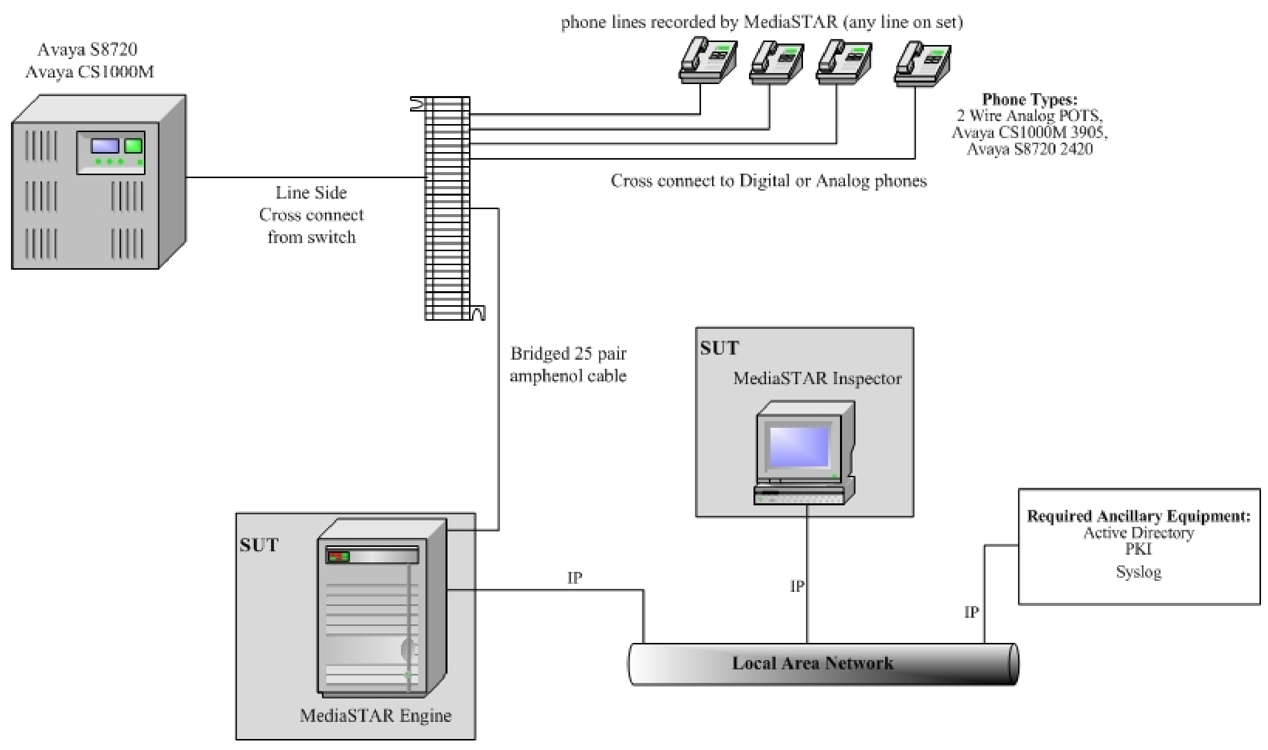
**5. METHODOLOGY.** Testing was conducted using CPE requirements derived from the Unified Capabilities Requirements (UCR) 2013, Reference (c), and CPE test procedures, Reference (d). Any discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These 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 |
| DISA | Defense Information Systems Agency |
| DISN | Defense Information Systems Network |
| DoD | Department of Defense |
| EI | End Item |
| IAP | Integrated Access Point |
| IM | Instant Messaging |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| LAN | Local Area Network |
| MCEP | Multi-Carrier Entry Point |
| NETOPS | Network Operations |
| PKI | Public Key Infrastructure |
| PSTN | Public Switched Telephone Network |
| QoS | Quality of Service |
| SBC | Session Border Controller |
| SC | Session Controller |
| SS | Softswitch |
| UC | Unified Capabilities |
| VVoIP | Voice and Video over IP |
| XMPP | Extensible Messaging and Presence Protocol |

**Figure 2-1. Notional UC Network Architecture**



**LEGEND:**

| | | | |
|---|---|---|---|
| CS | Communication Server | PKI | Public Key Infrastructure |
| IP | Internet Protocol | POTS | Plain Old Telephone Service |
| Mbps | Megabits per second | SUT | System Under Test |

**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 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” 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 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 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 Tagging.** 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). 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 intra-enclave IP connection between the MediaSTAR Engine and the MediaSTAR Inspector. 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 vendor’s letter of compliance and testing the intra-enclave IP connection between the MediaSTAR Engine and the MediaSTAR Inspector.

**d. Functionality testing.** There are no specific functionality requirements in the UCR for this type of CPE. However, testers conducted functionality testing on the SUT. Testers placed calls of varying durations (10, 20, 30, 40, and 50 seconds) from various telephones monitored by the SUT. The SUT was able to monitor each call as it occurred from the MediaSTAR Work Station. The engineer selected and played back .wav files for each of the calls and verified that the recorded timestamps matched the call durations. In addition, testers verified voice quality based on Table 2-2. Each call received a rating of 5 (Excellent) on the Voice and Video Subjective Quality Scale.

**Table 2-2. Voice and Video Subjective Quality Scale**

| Rating | Reference | Definition |
|---|---|---|
| 1 | *Unusable* | Quality is unusable. Voice and video may be heard and seen but is unrecognizable. |
| 2 | *Poor* | Quality is unusable. Words and phrases are not fully understandable or video cannot be properly identified. |
| 3 | *Fair* | Quality is seriously affected by distortion. Repeating words and phrases are required to convey speech or video is seriously impacted and barely recognizable. |
| 4 | *Good* | Quality is usable. Audio or video is not impaired but some distortion is noticeable |
| 5 | *Excellent* | Quality is unaffected. No discernable problems with either audio or video. |
| **NOTE:** Audio and video quality during a conference will receive a subjective rating on the Data Collection Form. A rating of lower than 4 on this reference scale is considered a failure. | | |

**e. 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.** 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 any Avaya CS1000M, CS1000E, or functionally similar switch and any Avaya switch certified with software versions Communication Manager (CM) 4 or CM 6 that is configured with AE Services Release 6.2 Session Controller. This certification applies to the previously identified Avaya switches that are currently or have been 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 1.) | Status | Remarks |
|---|---|---|---|
| **Interfaces (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 3.) | Met | The SUT met the critical CRs and FRs for the interface. (See note 2.) |
| Avaya S8720 Communications Manager 2-Wire Proprietary Digital Line | 1 (See note 4.) | Met | The SUT met the critical CRs and FRs for the interface. (See note 2.) |
| IP (See note 5.) | 2, 3 | Met | The SUT met the critical CRs and FRs for this interface. |

**NOTES:**

1. The UCR does not identify interface CR/FR applicability.
2. The SUT interface to this interface is bridged only and not directly connected.
3. 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.
4. The UCR does not include requirements for proprietary interfaces. The SUT interface to the Avaya 2420 digital phone was tested using the Avaya S8720 Communications Manager 2-wire proprietary digital interface as depicted in Figure 2-2.
5. The SUT provided an IP intra-enclave interface between the MediaSTAR Engine and MediaSTAR Inspector

**LEGEND:**

| | | | |
|---|---|---|---|
| CPE | Customer Premise Equipment | FR | Functional Requirement |
| CR | Capability Requirement | IP | Internet Protocol |
| CS | Communication Server | 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 (See note 2.) |
| 3 | Internet Protocol version 6 Requirements (R) | Table 5.2-1 | Met (See note 3.) |

**NOTES:**

1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Table 3-5.
2. The requirement was met by testing intra-enclave connection between the MediaSTAR Engine and the MediaSTAR Inspector using IPv4 and IPv6.
3. The requirement was met by testing intra-enclave connection between the MediaSTAR Engine and the MediaSTAR Inspector using IPv6.

**LEGEND:**

| | | | |
|---|---|---|---|
| CR | Capability Requirement | IPv6 | Internet Protocol version 6 |
| FR | Functional Requirement | R | Required |
| ID | Identification | SUT | System Under Test |
| IPv4 | Internet Protocol version 4 | UCR | Unified Capabilities Requirements |

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

| Component | Release | Sub-component | Function |
|---|---|---|---|
| MediaSTAR Engine Server (Dell Edge R720) | Application: 13.4.0.44<br>Microsoft Windows Server 2008 R2<br>Microsoft SQL 2008 R2 | Audio Codes NGX800 PCIe Board with Smartworks 5.3.1.765 Firmware 1032 | Monitoring telephone line activity |
| | | Audio Codes LD809 PCIe Board Smartworks 5.3.1.765 Firmware 1032 | |
| MediaSTAR Inspector Client (Dell Optiplex XE) | Application: 13.4.0.22<br>Microsoft Windows 7 Professional SP1 | N/A | Customer Monitoring System |

**LEGEND:**

| | | | |
|---|---|---|---|
| N/A | Not Applicable | SP | Service Pack |
| 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 | | |
| **Test Network Components** | | |
| Avaya CS1000 | Succession DSN 5.0 | SMEO |
| Avaya S8720 | Communication Manager (CM) 4.0<br>(R014x.00.2.731.7: Super Patch 14419) | SMEO |
| 2-wire analog phones | Not applicable | phone |
| Avaya M3905 digital phone | Not applicable | phone |
| Avaya 2420 digital phone | Not applicable | phone |

**LEGEND:**

| | | | |
|---|---|---|---|
| CS | Communication Server | MFSS | Multifunction Softswitch |
| DSN | Defense Switched Network | SMEO | Small End Office |

## 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<br>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<br>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<br>AUX-006160 | T | 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** | | | |
| 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<br>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<br>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<br>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<br>AUX-006200 | L | 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:<br>Serial interfaces shall be in accordance with one of the following standards:<br>ITU-T Recommendation V.35.<br>TIA-232-F.<br>EIA-449-1.<br>TIA-530-A.<br>Ethernet interfaces shall be in accordance with IEEE 802.3-2002. | 3.7.2<br>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<br>AUX-006220 | L/T<br>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<br>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 Systems Generic Requirements |
| DSN | Defense Switched Network | | |
| 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<br>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<br>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<br>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<br>IP6-000050 | L | R |

## Table 3-6.  IPv6 Requirements (continued)

| ID | 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<br>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<br>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<br>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<br>IP6-000100 | L | C |
| 3-9 | The product shall not use the Flow Label field as described in RFC 2460. | 5.2.1.2<br>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<br>IP6-000120 | L | R |
| 3-11 | The product shall be capable of ignoring the Flow Label field when receiving packets. | 5.2.1.2<br>IP6-000140 | L | R |
| 3-12 | The product shall support the IPv6 Addressing Architecture as described in RFC 4291. | 5.2.1.3<br>IP6-000150 | L | R |
| 3-13 | The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007. | 5.2.1.3<br>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<br>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<br>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<br>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<br>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<br>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<br>IP6-000240 | L | C |

## Table 3-6. IPv6 Requirements (continued)

| ID | 5.2 – IPv6 Requirements (continued) | | | |
|---|---|---|---|---|
| 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<br>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<br>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<br>IP6-000270 | L | C |
| 3-23 | The product shall support Neighbor Discovery for IPv6 as described in RFC 4861. | 5.2.1.5<br>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<br>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<br>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<br>IP6-000320 | L | R |
| 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<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>IP6-000460 | L | R |
| 3-39 | The product shall support manual assignment of IPv6 addresses. | 5.2.1.6<br>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<br>IP6-000520 | L | R |

## Table 3-6.  IPv6 Requirements (continued)

| ID | 5.2 – IPv6 Requirements (continued) | | | |
|---|---|---|---|---|
| 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<br>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<br>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<br>IP6-000560 | L | R |
| 3-44 | The product shall support MLD as described in RFC 2710. | 5.2.1.8<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>IP6-000750 | L | C |
| 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<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>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<br>IP6-000850 | L | C |
| 3-62 | If RFC 4301 is supported, then the product shall support manual keying of IPSec. | 5.2.1.9<br>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<br>IP6-000870 | L | C |

## Table 3-6.  IPv6 Requirements (continued)

| ID | 5.2 – IPv6 Requirements (continued) | | | |
|---|---|---|---|---|
| 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<br>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<br>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<br>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<br>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<br>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<br>IP6-001050 | L | R |
| 3-70 | 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:<br>• 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.<br>• x: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<br>IP6-001060 | L | C |
| 3-71 | 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:<br>• x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A.<br>• x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22.<br>• compressed zeros: 1080::8:800:200C:417A. | 5.2.1.13<br>IP6-001070 | L | C |
| 3-72 | 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<br>IP6-001080 | L | C |
| 3-73 | 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<br>IP6-001090 | L | C |
| 3-74 | 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<br>IP6-001100 | L | C |
| 3-75 | 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<br>IP6-001110 | L | C |
| 3-76 | 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<br>IP6-001150 | L | R |
| 3-77 | 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<br>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 | | |
| DTMF | Dual Tone Multi Frequency | MLPP | Multi-level Precedence and Preemption |
| EIA | Electronic Industries Alliance | R | Required |
| FCC | Federal Communications Commission | TIA | Telecommunications Industry Association |
| GR | Generic Requirement | TP | Test Plan |
| ID | Identification | UC | Unified Capabilities |
| IEEE | Institute of Electrical and Electronics Engineers | UCR | Unified Capabilities Requirements |
| ITU | International Telecommunication Union | | |