



## DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 4502  
ARLINGTON, VIRGINIA 22204-4502

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

**10 Dec 2009**

### MEMORANDUM FOR DISTRIBUTION

**SUBJECT:** Special Interoperability Test Certification of General Dynamics C4 Systems Sectéra® vIPer™ Release 1.0.2

References: (a) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004  
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008  
(c) through (e), see Enclosure 1

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

2. The General Dynamics C4 Systems Sectéra® vIPer™ Release 1.0.2 is hereinafter referred to as the system under test (SUT). The SUT meets all of its critical interoperability requirements and is certified for joint use within the Defense Switched Network (DSN) as a Department of Defense (DoD) Secure Communications Device (DSCD). The SUT is certified with any Cisco CallManager solution on the Unified Capabilities (UC) Approved Product List (APL) with the following limitation: the Cisco CallManager solutions must be configured with 2800, 3700, or 3800 series gateways that are loaded with the appropriate certified Internetwork Operating System (IOS) versions. The appropriate certified versions are IOS 12.4(22)T2 or later for the 2800 series gateways and IOS 12.4(15) T8 or later for the 3700 and 3800 series gateways. No other configurations, features, or functions, except those cited within this report, are certified by the JITC. This certification expires upon changes that could affect interoperability, but no later than three years from the date of this memorandum.

3. This finding is based on interoperability testing conducted by JITC, DISA adjudication of open test discrepancy reports, review of the vendor's Letters of Compliance (LoC), Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG) accreditation, and National Security Agency (NSA) Type I Accreditation. Interoperability testing of the SUT was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 27 April through 29 May 2009. Review of vendor's LoC was completed on 29 May 2009. The SUT NSA Type I accreditation was granted on 7 September 2007, Reference (c). DISA adjudication of outstanding test discrepancy reports was completed on 18 October 2008. The DSAWG grants accreditation based on the security testing completed by DISA-led Information Assurance test teams and published in a separate report, Reference (d).

The DSAWG accreditation was granted on 1 October 2009. Enclosure 2 documents the test results and describes the tested network and system configurations.

4. The interoperability test summary of the SUT is indicated in Table 1. The Unified Capabilities Requirement DSCD Interoperability Requirements are listed in Table 2. This interoperability test status is based on the SUT’s ability to meet:

- a. DSN services for Network and Applications specified in Reference (e).
- b. DSCD interface and signaling requirements as specified in Reference (f) verified through JITC testing and/or vendor submission of LoC.
- c. DSCD Capability Requirements (CRs)/Feature Requirements (FRs) specified in Reference (f) verified through JITC testing and/or vendor submission of LoC.
- d. The overall system interoperability performance derived from test procedures listed in Reference (g).

**Table 1. SUT Interoperability Test Summary**

DSCD Interoperability Requirements																															
Interface & Signaling	Critical	Status	Remarks																												
Ethernet 100BaseT (SCCP)	Yes	Certified	Met all Critical CRs and FRs. with the following minor exceptions: The SUT during registration incorrectly tags the TFTP packets at 0. <sup>1</sup> When the SUT security soft key is pressed it deregisters. <sup>2</sup> The SUT redial key redials the wrong number. <sup>3</sup> The SUT does not meet IPv6 requirements. <sup>4</sup>																												
Security	Yes	Certified	See note 5.																												
<p><b>NOTES:</b></p> <p>1 When the SUT is registering, it incorrectly tags TFTP packets with a DSCP tag of 0 (best effort). However, after the registration is completed, TFTP packets are correctly tagged. This discrepancy was adjudicated by DISA on 14 July 2009 as having a minor operational impact.</p> <p>2 When the SUT is off hook and the subscriber presses the security soft key, the SUT deregisters and all incoming ROUTINE calls placed to the SUT receive a busy signal and above ROUTINE calls divert to the alternate Directory Number. This discrepancy was adjudicated by DISA on 14 July 2009 as having a minor operational impact.</p> <p>3 The SUT redial key, when pressed after a call is placed, redials the wrong number. This discrepancy was adjudicated by DISA on 14 July 2009 as having a minor operational impact with the vendor’s commitment to fix this discrepancy in the next release.</p> <p>4 The UCR, section 5.2.12.8.2.8, states that the VoIP systems (a combination of call control and End Instruments) must meet IPv6 capability requirements as defined in UCR 2008, Section 5.3.5. The SUT does not support IPv6; however, this requirement was waived for the SUT by the Assistant Secretary of Defense on 3 August 2009.</p> <p>5 Security is tested by DISA-led Information Assurance test teams and published in a separate report, Reference (d).</p> <p><b>LEGEND:</b></p> <table border="0"> <tr> <td>100BaseT</td> <td>100 Mbps (Baseband Operation, Twisted Pair) Ethernet</td> <td>IPv6</td> <td>Internet Protocol version 6</td> </tr> <tr> <td>CRs</td> <td>Capability Requirements</td> <td>Mbps</td> <td>Megabits per second</td> </tr> <tr> <td>DISA</td> <td>Defense Information Systems Agency</td> <td>SCCP</td> <td>Skinny Call Control Protocol</td> </tr> <tr> <td>DoD</td> <td>Department of Defense</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>DSCD</td> <td>DoD Secure Communications Devices</td> <td>TFTP</td> <td>Trivial File Transfer Protocol</td> </tr> <tr> <td>DSCP</td> <td>Differentiated Services Code Point</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>FRs</td> <td>Feature Requirements</td> <td>VoIP</td> <td>Voice over Internet Protocol</td> </tr> </table>				100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IPv6	Internet Protocol version 6	CRs	Capability Requirements	Mbps	Megabits per second	DISA	Defense Information Systems Agency	SCCP	Skinny Call Control Protocol	DoD	Department of Defense	SUT	System Under Test	DSCD	DoD Secure Communications Devices	TFTP	Trivial File Transfer Protocol	DSCP	Differentiated Services Code Point	UCR	Unified Capabilities Requirements	FRs	Feature Requirements	VoIP	Voice over Internet Protocol
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IPv6	Internet Protocol version 6																												
CRs	Capability Requirements	Mbps	Megabits per second																												
DISA	Defense Information Systems Agency	SCCP	Skinny Call Control Protocol																												
DoD	Department of Defense	SUT	System Under Test																												
DSCD	DoD Secure Communications Devices	TFTP	Trivial File Transfer Protocol																												
DSCP	Differentiated Services Code Point	UCR	Unified Capabilities Requirements																												
FRs	Feature Requirements	VoIP	Voice over Internet Protocol																												

**Table 2. DSCD UCR Interoperability Requirements**

DSN Line Interface																																													
Interface	Critical	Requirements Required or Conditional	References																																										
Ethernet 100BaseT (SCCP)	Yes	<ul style="list-style-type: none"> <li>Type Approved by NSA (R)</li> <li>DSCDs that establish secure sessions on IP networks using FNBDT/SCIP shall satisfy all of the end point requirements described SCIP-215 and SCIP-216 (C)</li> <li>DSCD devices that use an IP interface shall meet the end instrument requirements as specified in Section 5.2.12.8 (C)</li> <li>Shall go secure with at least an 85% call completion rate (R)</li> <li>Shall establish secure call within 60 seconds for duration of secure call (R)</li> <li>Shall operate in a network that has an end-to-end latency of up to 600 milliseconds (R)</li> <li>Maintain secure voice connection with MOS of 3.0 (R)</li> <li>Process new key with 95% rekey completion rate (R)</li> <li>Supports data and facsimile transmission rate of 9.6 kbps or better (C)</li> </ul>	<ul style="list-style-type: none"> <li>UCR Section 5.2.12.6.6</li> <li>UCR Section 5.2.12.6.6</li> <li>UCR Section 5.2.12.8</li> <li>UCR Section 5.2.12.6.6</li> </ul>																																										
Security		<ul style="list-style-type: none"> <li>GR-815, STIGs, and DoDI 8510.bb (DIACAP) (R)</li> </ul>	<ul style="list-style-type: none"> <li>UCR Section 3</li> </ul>																																										
<b>LEGEND:</b> <table border="0"> <tr> <td>100BaseT</td> <td>100 Mbps (Baseband Operation, Twisted Pair) Ethernet</td> <td>FNBDT</td> <td>Future Narrowband Digital Terminal</td> <td>NSA</td> <td>National Security Agency</td> </tr> <tr> <td>C</td> <td>Conditional</td> <td>GR</td> <td>Generic Requirement</td> <td>R</td> <td>Required</td> </tr> <tr> <td>DIACAP</td> <td>DoD Information Assurance Certification and Accreditation Process</td> <td>GR-815</td> <td>Generic Requirements For Network Element/Network System (NE/NS) Security</td> <td>SCCP</td> <td>Skinny Call Control Protocol</td> </tr> <tr> <td>DoD</td> <td>Department of Defense</td> <td>IP</td> <td>Internet Protocol</td> <td>SCIP</td> <td>Secure Communications Internet Protocol</td> </tr> <tr> <td>DoDI</td> <td>DoD Instruction</td> <td>kbps</td> <td>kilobits per second</td> <td>STIGs</td> <td>Security Technical Implementation Guides</td> </tr> <tr> <td>DSCD</td> <td>DoD Secure Communications Device</td> <td>Mbps</td> <td>Megabits per second</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td>DSN</td> <td>Defense Switched Network</td> <td>MOS</td> <td>Mean Opinion Score</td> <td></td> <td></td> </tr> </table>				100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	FNBDT	Future Narrowband Digital Terminal	NSA	National Security Agency	C	Conditional	GR	Generic Requirement	R	Required	DIACAP	DoD Information Assurance Certification and Accreditation Process	GR-815	Generic Requirements For Network Element/Network System (NE/NS) Security	SCCP	Skinny Call Control Protocol	DoD	Department of Defense	IP	Internet Protocol	SCIP	Secure Communications Internet Protocol	DoDI	DoD Instruction	kbps	kilobits per second	STIGs	Security Technical Implementation Guides	DSCD	DoD Secure Communications Device	Mbps	Megabits per second	UCR	Unified Capabilities Requirements	DSN	Defense Switched Network	MOS	Mean Opinion Score		
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	FNBDT	Future Narrowband Digital Terminal	NSA	National Security Agency																																								
C	Conditional	GR	Generic Requirement	R	Required																																								
DIACAP	DoD Information Assurance Certification and Accreditation Process	GR-815	Generic Requirements For Network Element/Network System (NE/NS) Security	SCCP	Skinny Call Control Protocol																																								
DoD	Department of Defense	IP	Internet Protocol	SCIP	Secure Communications Internet Protocol																																								
DoDI	DoD Instruction	kbps	kilobits per second	STIGs	Security Technical Implementation Guides																																								
DSCD	DoD Secure Communications Device	Mbps	Megabits per second	UCR	Unified Capabilities Requirements																																								
DSN	Defense Switched Network	MOS	Mean Opinion Score																																										

5. No detailed test report was developed in accordance with the Program Manager’s request. The JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.125> (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>.

6. The JITC point of contact is Ms. Anita Bickler, DSN 879-5164, commercial (520) 538-5164, FAX DSN 879-4347, or e-mail to [anita.bickler@disa.mil](mailto:anita.bickler@disa.mil). The JITC’s mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 0813501.

FOR THE COMMANDER:

2 Enclosures a/s

  
 for RICHARD A. MEADOR  
 Chief  
 Battlespace Communications Portfolio

JITC Memo, JTE, Extension of the Special Interoperability Test Certification of General Dynamics C4 Systems Sectéra® vIPer™ Release 1.0.2

Distribution (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)

Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ

U.S. Marine Corps MARCORSSYSCOM, SIAT, MJI Division I

DOT&E, Net-Centric Systems and Naval Warfare

U.S. Coast Guard, CG-64

Defense Intelligence Agency

National Security Agency, DT

Defense Information Systems Agency, TEMC

Office of Assistant Secretary of Defense (NII)/DOD CIO

U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68

Defense Information Systems Agency, GS23

## **ADDITIONAL REFERENCES**

- (c) National Security Agency, "Information Assurance Directorate," 7 September 2007
- (d) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of General Dynamics (GD) Sectera vPer (Tracking Number 0813501)," 1 October 2009
- (e) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C, "Policy for Department of Defense Voice Services with Real Time Services (RTS)," 9 November 2007
- (f) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008," 22 January 2009
- (g) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP), Change 2," 2 October 2006

## CERTIFICATION TESTING SUMMARY

- 1. SYSTEM TITLE.** General Dynamics C4 Systems Sectéra® vIPer™ Release 1.0.2; hereinafter referred to as the System Under Test (SUT).
- 2. PROPONENT.** U.S. Army Communications-Electronics Command.
- 3. PROGRAM MANAGER.** Mr. John Kahler, EA-TJTN/GS13, Building 1210 Rittko Ave, Fort Monmouth, NJ, 07703, E-mail: john.kahler@us.army.mil.
- 4. TESTER.** Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.
- 5. SYSTEM UNDER TEST DESCRIPTION.** The SUT is a Department of Defense (DoD) Secure Communications Device (DSCD) that provides voice communications for both secure (National Security Agency [NSA] Accredited Type 1) and non secure communications between other Voice over Internet Protocol (VoIP) and Time Division Multiplex end instruments. Incorporating Secure Communication Internet Protocol (SCIP) technology with integrated security and PIN-based access controls.

The SUT is compatible with Cisco VoIP systems using Cisco Skinny Call Control Protocol (SCCP). The SUT is Enhanced Fire Fly capable and does not require a crypto card. The SUT is certified with any Cisco CallManager Solution on the Unified Capabilities (UC) Approved Product List (APL) with the following gateway Internetwork Operating System (IOS) stipulations:

- The SUT is certified only with 3700 and 3800 series gateways with IOS 12.4(15) T8 or above listed on the UC APL.
- The SUT is certified only with 2800 series gateways with IOS 12.4(22)T2 or above listed on the UC APL.

**6. OPERATIONAL ARCHITECTURE.** The Defense Switched Network (DSN) architecture is a two-level network hierarchy consisting of DSN backbone switches and Service/Agency installation switches. Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The DSN architecture, therefore, consists of several categories of switches, including Private Branch Exchanges (PBX)s. The Unified Capabilities Requirements (UCR) operational DSN Architecture is depicted in Figure 2-1.



**7. REQUIRED SYSTEM INTERFACES.** The SUT Interoperability Test Summary is shown in Table 2-1 and the Capability and Feature Requirements used to evaluate the interoperability of the SUT are indicated in Table 2-2. These requirements are derived from the UCR and verified through JITC testing and review of the vendor's Letters of Compliance (LoC).

**Table 2-1. SUT Interoperability Test Summary**

DSCD Interoperability Requirements			
Interface & Signaling	Critical	Status	Remarks
Ethernet 100BaseT (SCCP)	Yes	Certified	Met all Critical CRs and FRs. with the following minor exceptions: The SUT during registration incorrectly tags the TFTP packets at 0. <sup>1</sup> When the SUT security soft key is pressed it deregisters. <sup>2</sup> The SUT redial key redials the wrong number. <sup>3</sup> The SUT does not meet IPv6 requirements. <sup>4</sup>
Security	Yes	Certified	See note 5.

**NOTES:**

- 1 When the SUT is registering, it incorrectly tags TFTP packets with a DSCP tag of 0 (best effort). However, after the registration is completed, TFTP packets are correctly tagged. This discrepancy was adjudicated by DISA on 14 July 2009 as having a minor operational impact.
- 2 When the SUT is off hook and the subscriber presses the security soft key, the SUT deregisters and all incoming ROUTINE calls placed to the SUT receive a busy signal and above ROUTINE calls divert to the alternate Directory Number. This discrepancy was adjudicated by DISA on 14 July 2009 as having a minor operational impact.
- 3 The SUT redial key, when pressed after a call is placed, redials the wrong number. This discrepancy was adjudicated by DISA on 14 July 2009 as having a minor operational impact with the vendor's commitment to fix this discrepancy in the next release.
- 4 The UCR, section 5.2.12.8.2.8, states that the VoIP systems (a combination of call control and End Instruments) must meet IPv6 capability requirements as defined in UCR 2008, Section 5.3.5. The SUT does not support IPv6; however, this requirement was waived for the SUT by the Assistant Secretary of Defense on 3 August 2009.
- 5 Security is tested by DISA-led Information Assurance test teams and published in a separate report, Reference (d).

**LEGEND:**

100BaseT	100 Mbps (Baseband Operation, Twisted Pair)	IPv6	Internet Protocol version 6
CRs	Capability Requirements	Mbps	Megabits per second
DISA	Defense Information Systems Agency	SCCP	Skinny Call Control Protocol
DoD	Department of Defense	SUT	System Under Test
DSCD	DoD Secure Communications Devices	TFTP	Trivial File Transfer Protocol
DSCP	Differentiated Services Code Point	UCR	Unified Capabilities Requirements
FRs	Feature Requirements	VoIP	Voice over Internet Protocol

**Table 2-2. DSCD UCR Interoperability Requirements**

DSN Line Interface			
Interface	Critical	Requirements Required or Conditional	References
Ethernet 100BaseT (SCCP)	Yes	<ul style="list-style-type: none"> <li>• Type Approved by NSA (R)</li> <li>• DSCDs that establish secure sessions on IP networks using FNBDT/SCIP shall satisfy all of the end point requirements described SCIP-215 and SCIP-216 (C)</li> <li>• DSCD devices that use an IP interface shall meet the end instrument requirements as specified in Section 5.2.12.8 (C)</li> <li>• Shall go secure with at least an 85% call completion rate (R)</li> <li>• Shall establish secure call within 60 seconds for duration of secure call (R)</li> <li>• Shall operate in a network that has an end-to-end latency of up to 600 milliseconds (R)</li> <li>• Maintain secure voice connection with MOS of 3.0 (R)</li> <li>• Process new key with 95% rekey completion rate (R)</li> <li>• Supports data and facsimile transmission rate of 9.6 kbps or better (C)</li> </ul>	<ul style="list-style-type: none"> <li>• UCR Section 5.2.12.6.6</li> <li>• UCR Section 5.2.12.6.6</li> <li>• UCR Section 5.2.12.8</li> <li>• UCR Section 5.2.12.6.6</li> </ul>
Security		<ul style="list-style-type: none"> <li>• GR-815, STIGs, and DoDI 8510.bb (DIACAP) (R)</li> </ul>	<ul style="list-style-type: none"> <li>• UCR Section 3</li> </ul>

**Table 2-2. DSCD UCR Interoperability Requirements (continued)**

<b>LEGEND:</b>					
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	DSN	Defense Switched Network	MOS	Mean Opinion Score
C	Conditional	FNBBDT	Future Narrowband Digital Terminal	NSA	National Security Agency Required
DIACAP	DoD Information Assurance Certification and Accreditation Process	GR	Generic Requirement	SCCP	Skinny Call Control Protocol
DoD	Department of Defense	GR-815	Generic Requirements For Network Element/Network System (NE/NS) Security	SCIP	Secure Communications Internet Protocol
DoDI	DoD Instruction	IP	Internet Protocol	STIGs	Security Technical Implementation Guides
DSCD	DoD Secure Communications Device	kbps	kilobits per second	UCR	Unified Capabilities Requirements
		Mbps	Megabits per second		

**8. TEST NETWORK DESCRIPTION.** The SUT was tested at JITC’s Global Information Grid Network Test Facility in a manner and configuration similar to that of the DSN operational environment. Testing of the SUT required functions and features was conducted using the test configurations depicted in Figures 2-2 through 2-9. Figures 2-2 through 2-8 simulate actual DoD operationally deployed network to strategic core network test configuration strings. Figure 2-9 depicts the test configuration used to test shared access with the SUT. The SUT was tested with other DSCD devices between the various test points denoted in each figure.



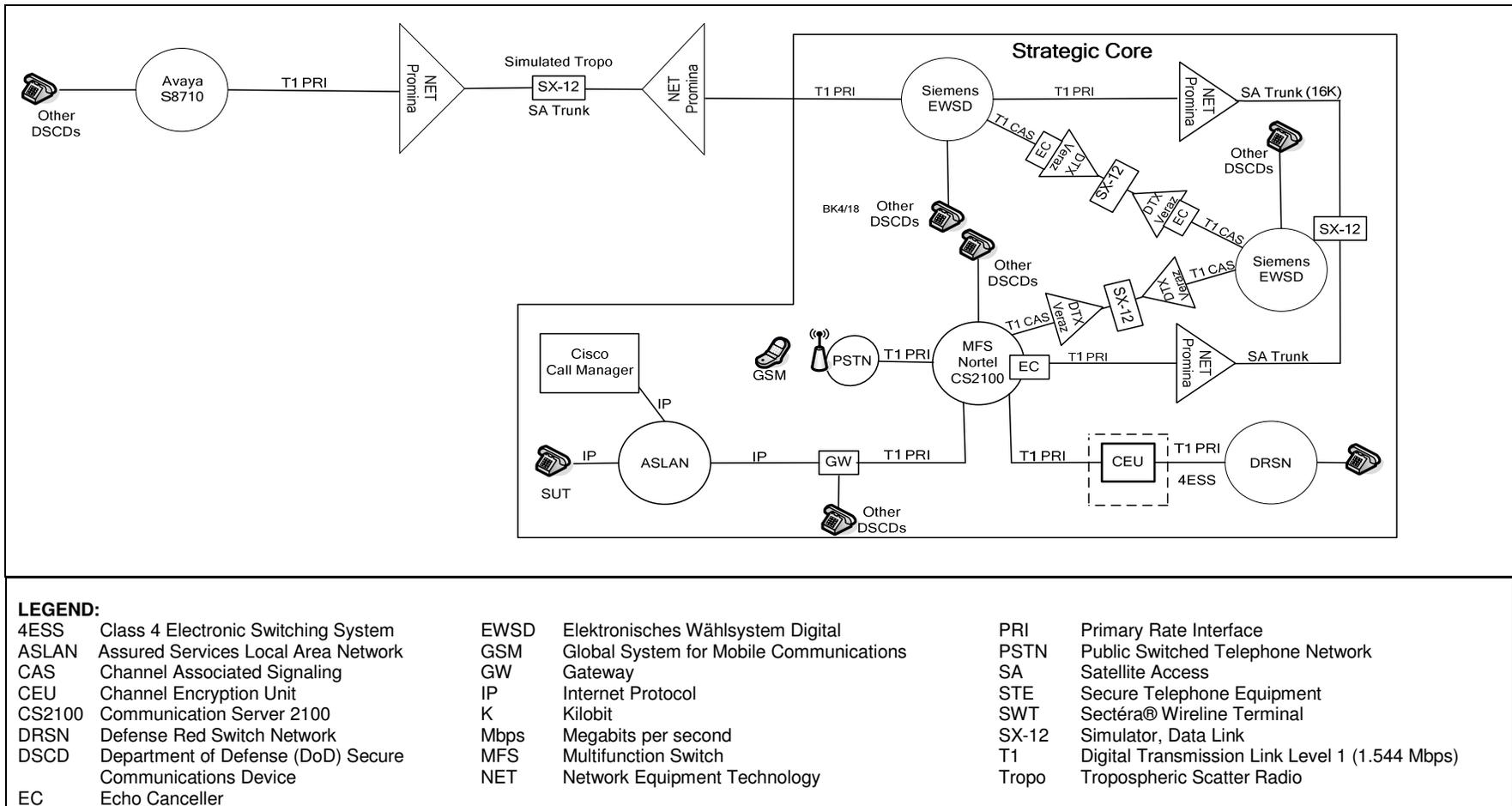


Figure 2-3. Air Force Composite Test Diagram

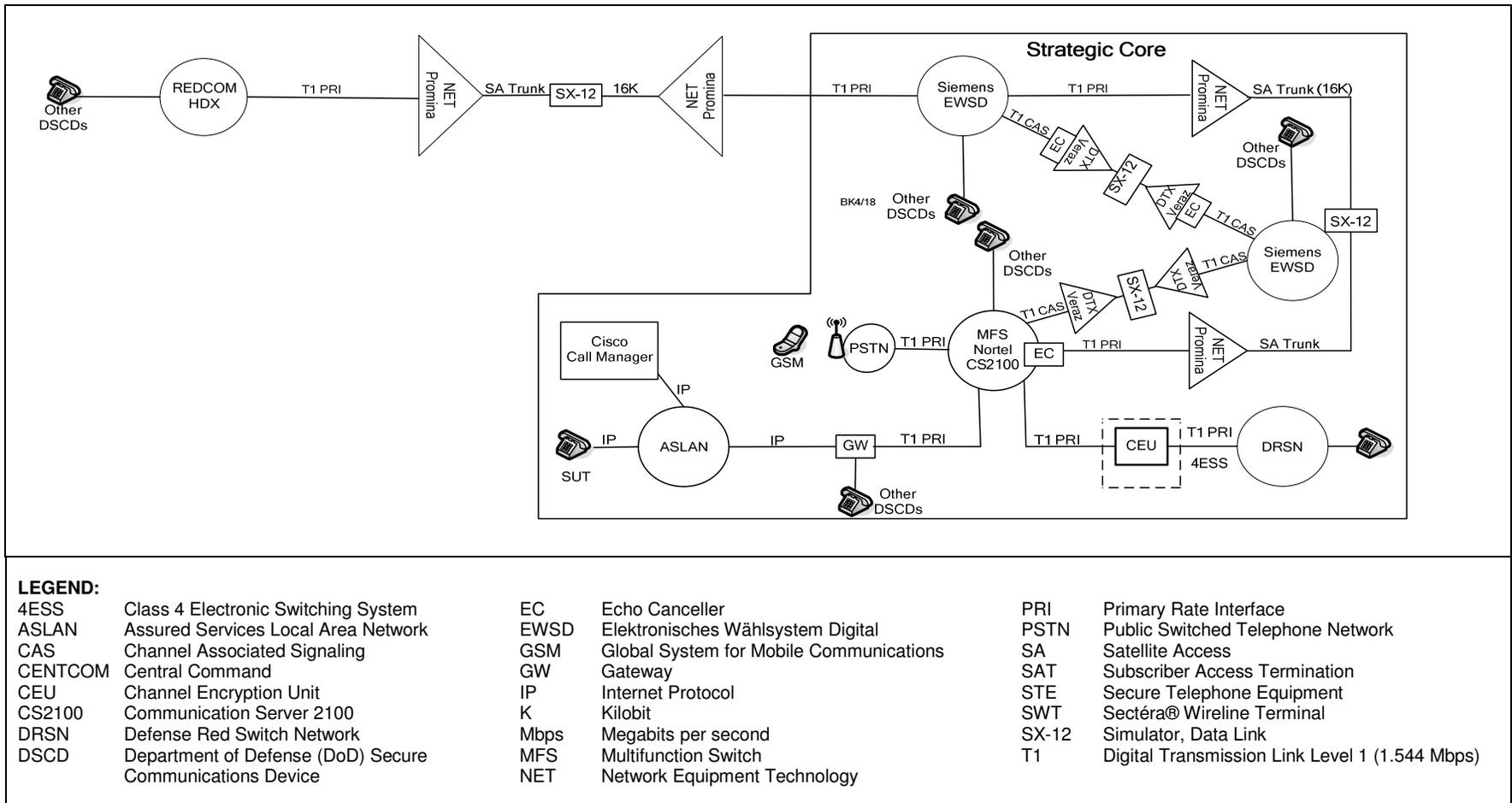


Figure 2-4. CENTCOM Dual Hop Composite Test Diagram

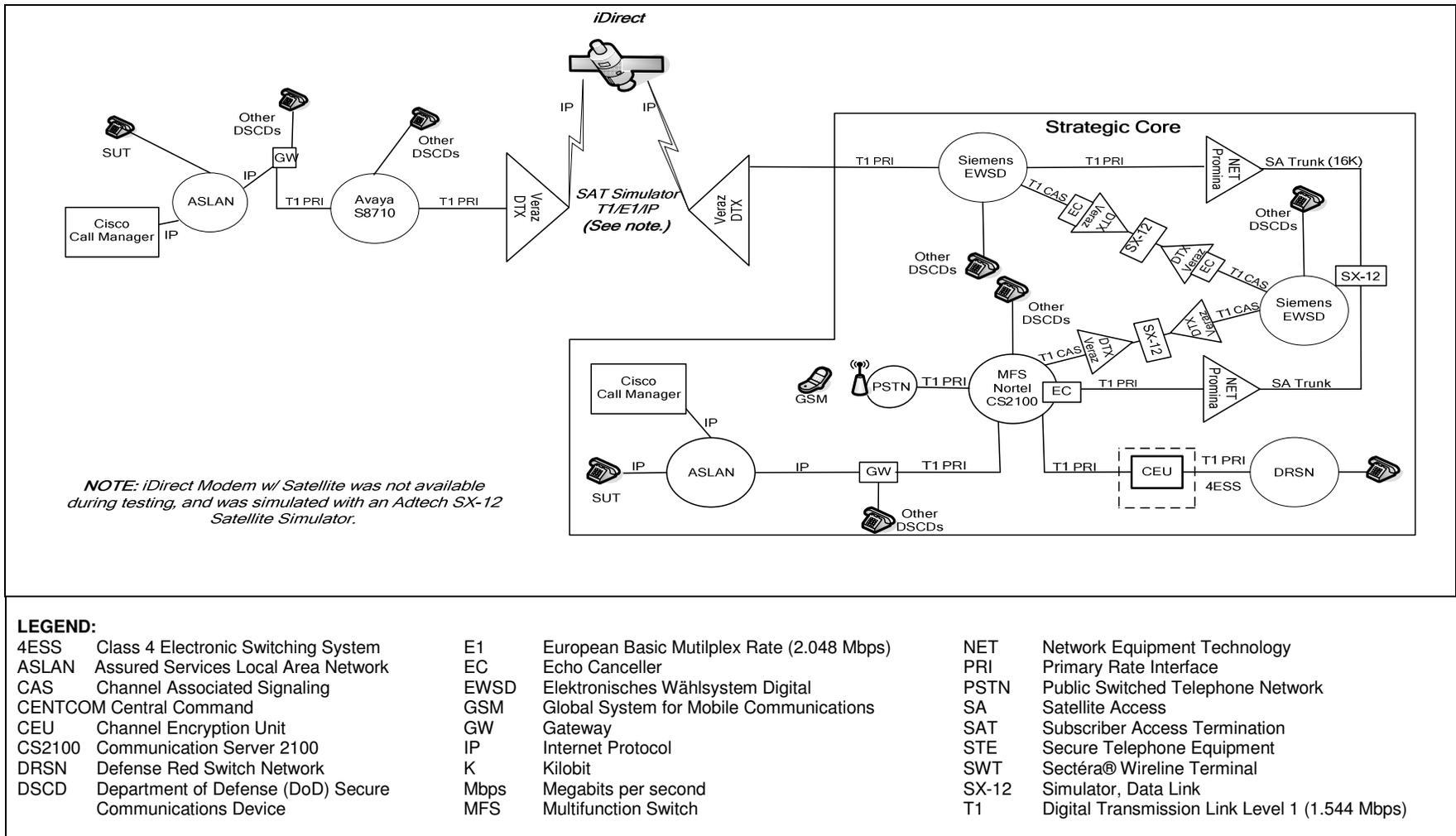


Figure 2-5. CENTCOM Composite Test Diagram

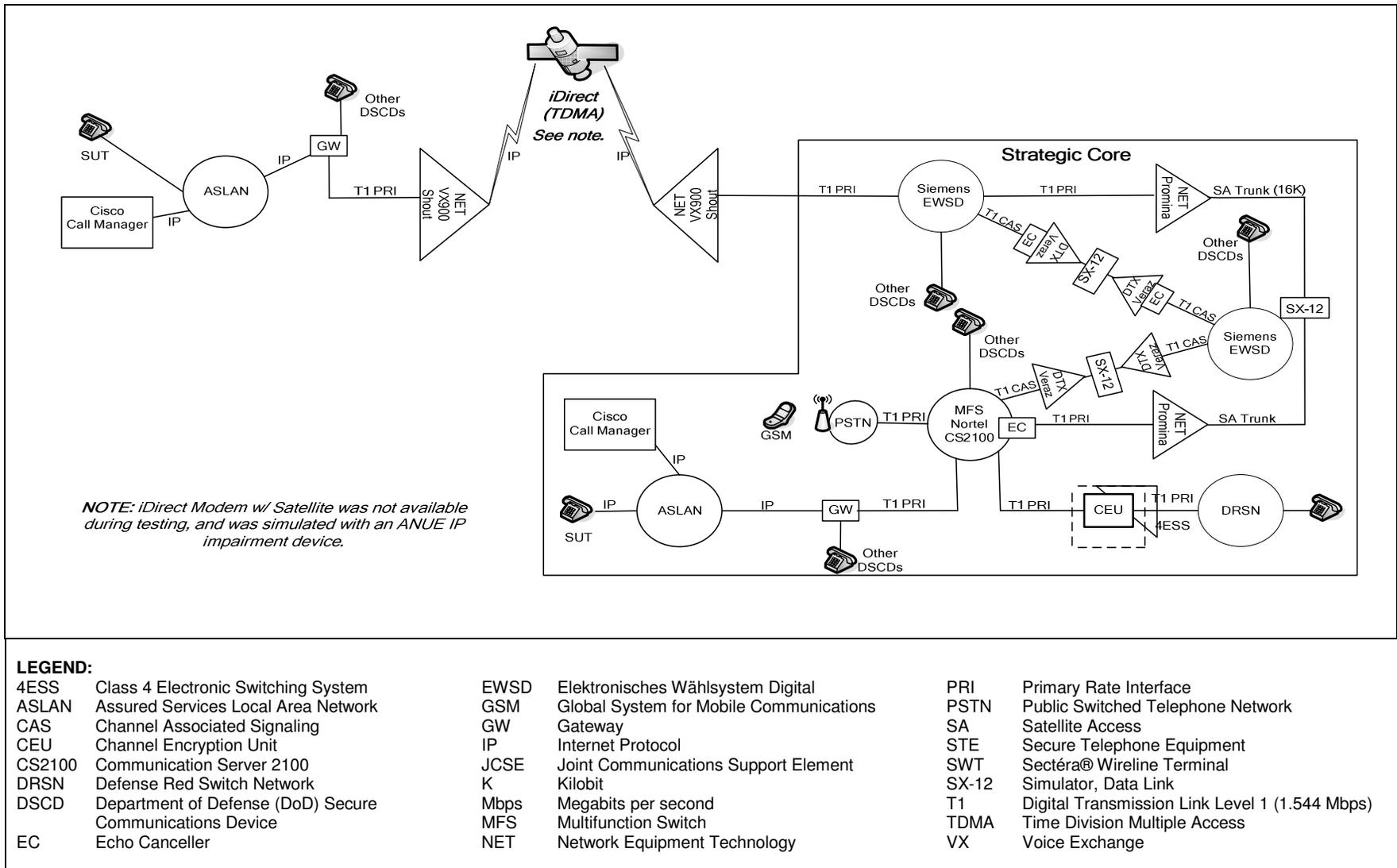
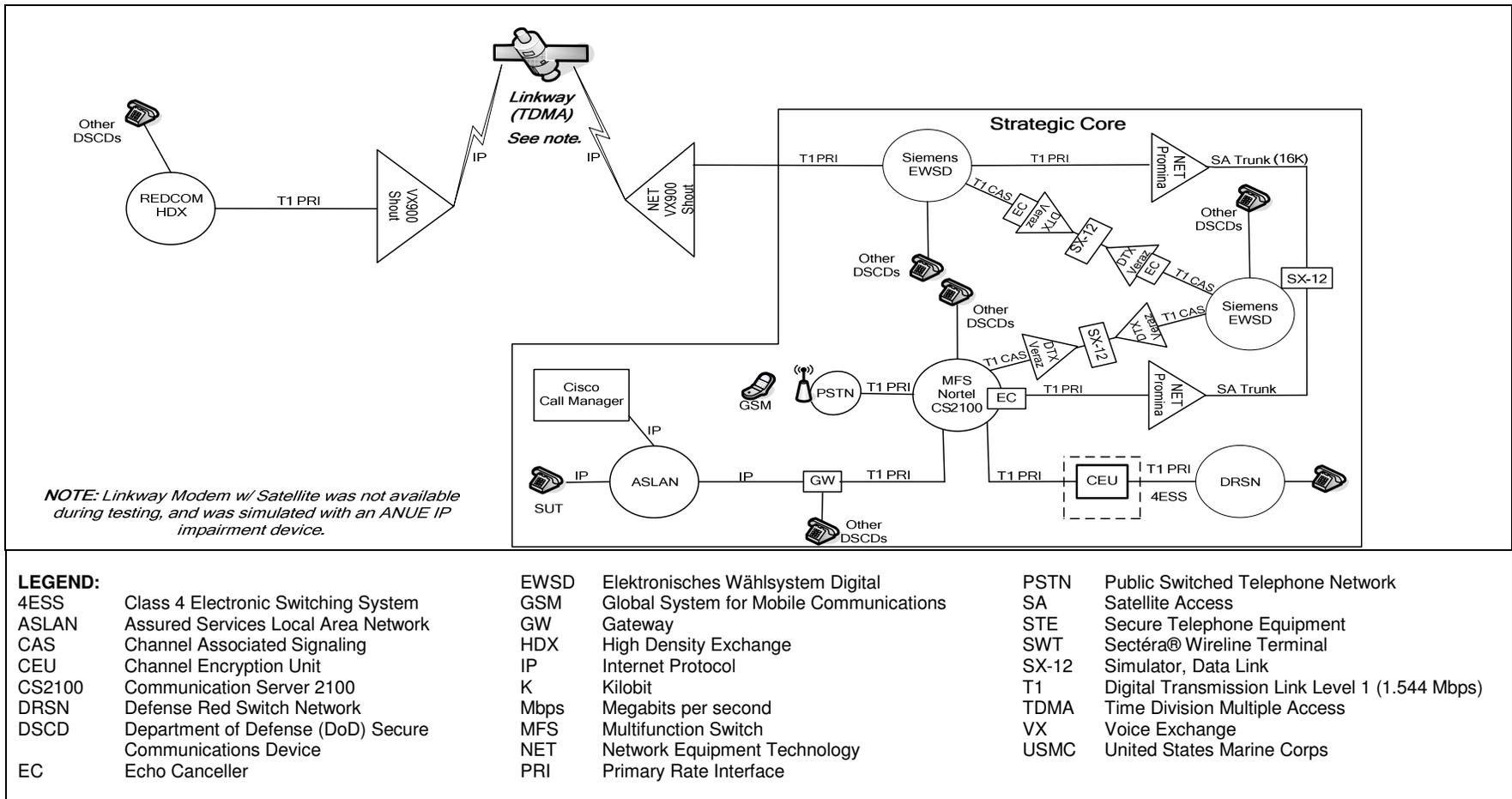
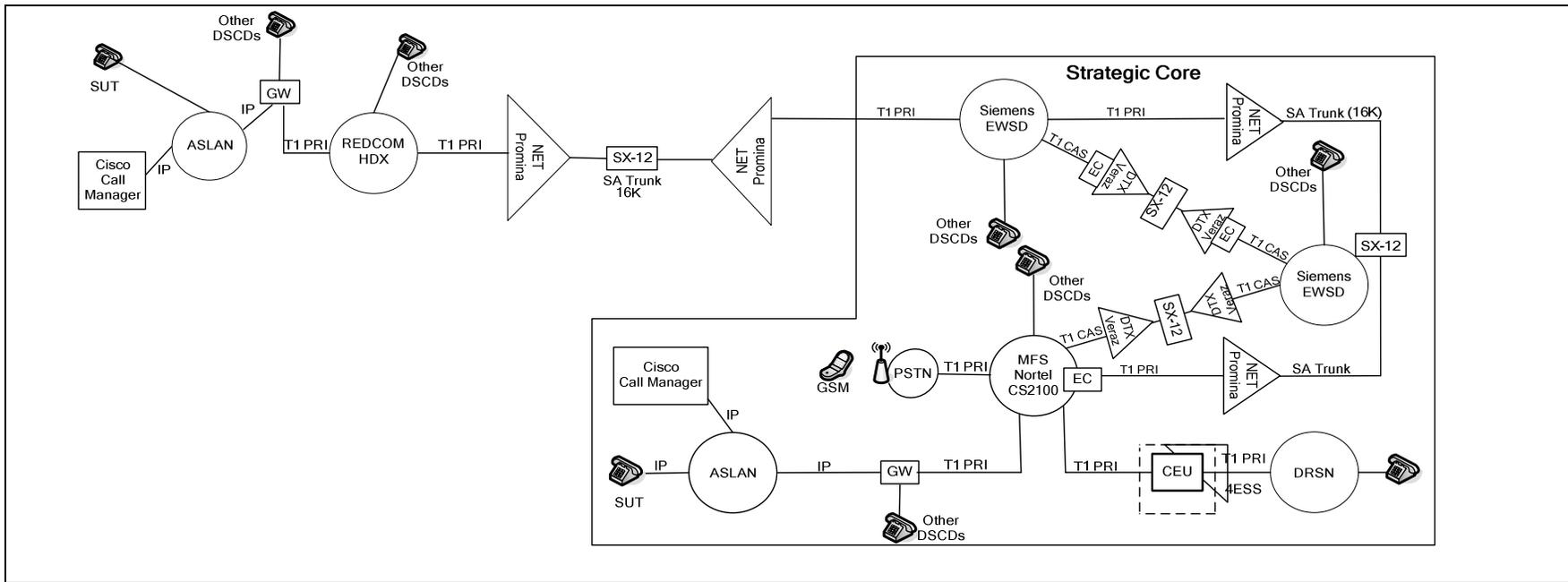


Figure 2-6. JCSE DSCD Composite Test Diagram



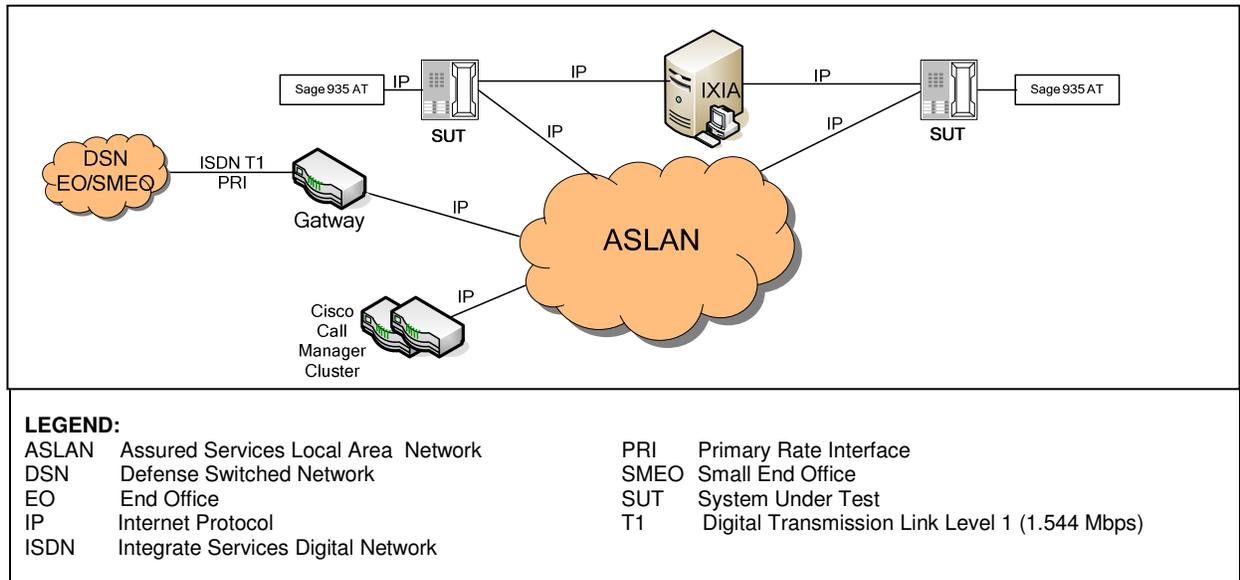
**Figure 2-7. USMC Composite Test Diagram**



**LEGEND:**

4ESS	Class 4 Electronic Switching System	EC	Echo Canceller	NET	Network Equipment Technology
ASLAN	Assured Services Local Area Network	EWSD	Elektronisches Wählsystem Digital	PRI	Primary Rate Interface
BRI	Basic Rate Interface	GSM	Global System for Mobile Communications	PSTN	Public Switched Telephone Network
CAS	Channel Associated Signaling	GW	Gateway	SA	Satellite Access
CEU	Channel Encryption Unit	HDX	High Density Exchange	STE	Secure Telephone Equipment
CS2100	Communication Server 2100	IP	Internet Protocol	SWT	Sectéra® Wireline Terminal
DRSN	Defense Red Switch Network	K	Kilobit	SX-12	Simulator, Data Link
DSCD	Department of Defense (DoD) Secure Communications Device	Mbps	Megabits per second	T1	Digital Transmission Link Level 1 (1.544 Mbps)
		MFS	Multifunction Switch	WIN-T	Warfighter Information Network - Tactical

**Figure 2-8. WIN-T Composite Test Diagram**



**Figure 2-9. SUT Shared Access Test Configuration Diagram**

**9. SYSTEM CONFIGURATIONS.** Table 2-2 provides the system configurations, hardware, and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine interoperability with a complement of DSN switches, network elements, and comparable DSCD end instruments noted in Table 2-2. Table 2-2 lists the DSN switches and Network Elements which depict the tested configuration and is not intended to identify the only switches and Network Elements that are certified with the SUT. The SUT is certified with any Cisco CallManager Solution on the UC APL with the following gateway IOS stipulations:

- The SUT is certified only with 3700 and 3800 series gateways with IOS 12.4(15) T8 or above listed on the UC APL.
- The SUT is certified only with 2800 series gateways with IOS 12.4(22)T2 or above listed on the UC APL.

**Table 2-2. Tested System Configurations**

System Name	Software Release
Nortel CS2100 (MFS)	Succession Enterprise (SE) 09.1
Nokia-Siemens EWSD (MFS)	19d with Patch Set 46
Avaya S8710 (SMEO)	Communication Manager (CM) 4.0 (R014x.00.2.731.7: Super Patch 14419)
Avaya G3CSI (PBX 1)	Communication Manager (CM) 3.0 (R013i.00.0.340.5: Patch 8893.1.0.7)
Cisco Unified CallManager (PBX 1)	Version 4.3(2) Service Release (SR) 1b, with Internetwork Operating System (IOS) Software Release 12.4(15) T7
REDCOM High Density Exchange (HDX) (SMEO)	Release 3.0A Revision 3, with Specified Patch Group 0 (3.0A R3P0)
Raytheon Channel Encryption Unit (CEU)	Release Version (v) 2.01.08 with LogiTel Mesh Router (MR) 1060 Release Version (v) 1.01.0205
L3 Communications STE and STE-R	2.6 with KOV14

**Table 2-2. Tested System Configurations (continued)**

System Name		Software Release	
L3 Communications Omni Secure Wireline Terminal		5.07	
NET Promina 800 and 400		4.x.2.02 Version 92.45	
General Dynamics Sectéra® Wireline Terminal		12.05	
NET VX900		4.3.5 Version 55	
Veraz DTX 600		JITC022.1	
SUT	SUT Hardware	SUT Processor	Software Version
	General Dynamics IP vIPer (Model SVT1000SM) with Software Release 1.0.2	Secure Control Processor (SCP) Operational	D006.0005.0000
		Secure Voice Processor (VP) Operational	D001.0006.0000
		Telecommunications Network Processor Operational	D005.C009.0000
		Human Machine Interface (HMI) Processor Operational	D006.0002.0000
		Secure Control Processor Boot	D005.0010.0000
		Voice Processor Boot	D001.0004.0000
		Telecommunications Network Processor Boot	D001.0007.0000
		Telecommunications Network Processor CURE	D001.0007.0000
		Human Machine Interface (HMI) Processor Boot	D005.0000.0000
Field Programmable Gate Array		03	
<b>LEGEND:</b>			
CS	Communication Server	MFS	Multifunction Switch
CURE	Code Upgrade Recovery	NET	Network Equipment Technologies
EWSD	Elektronisches Wählsystem Digital	PBX 1	Private Branch Exchange 1
IP	Internet Protocol	SMEO	Small End Office
JITC	Joint Interoperability Test Command	STE	Secure Terminal Equipment
KOV	Key Operating Variable	STE-R	Secure Terminal Equipment Red Switch
Mbps	Megabits per second	SUT	System Under Test

**10. TESTING LIMITATIONS.** None.

**11. TEST RESULTS**

**a. Discussion**

(1) The UCR, section 5.2.12.6.6, states that DSCD shall be only those that are Type Approved by the NSA and are listed on the NSA Secure Product Web site. Each DSCD must support at least one NSA approved secure protocol. If the DSCD supports more than one secure protocol, it must meet all the requirements for at least one of the secure protocols, and must minimally support the other protocols that are provided on the DSCD. The SUT received an NSA Type I approval for SCIP on 7 June 2007, which meets this requirement.

(2) The UCR, section 5.2.12.6.6, states that DSCDs that establish secure sessions on Internet Protocol (IP) networks using SCIP shall satisfy all of the end point requirements described SCIP-215 and SCIP-216. This requirement was met with vendor submission of a LoC.

(3) The UCR, section 5.2.12.8, states that DSCD devices that use an IP interface shall meet the end instrument requirements as specified in Section 5.2.12.8. The SUT met the requirements in accordance with section 5.2.12.8 as described below:

- The UCR, section 5.2.12.8.2.7, states the VoIP systems shall not be greater than 60 milliseconds (ms) averaged over any five-minute period. The latency is to be measured from IP handset to egress from the VoIP system via a DSN trunk. The SUT met this requirement with a measured one-way latency of 59.9 ms from handset to the Digital Transmission Link Level 1 (T1) Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) gateway trunk egress.

- The UCR, section 5.2.12.8.2.8, states that the VoIP systems (a combination of call control and End Instruments) must meet Internet Protocol Version 6 (IPv6) capability requirements as defined in UCR 2008, Section 5.3.5. The SUT does not support IPv6; however, this requirement was waived for the SUT by the Assistant Secretary of Defense on 3 August 2009.

- The UCR, section 5.2.12.8.2.9, states that the VoIP system shall meet the service class tagging requirements as provided in UCR 2008, Section 5.3.1. In accordance with this reference, the SUT is required to tag layer 3 Internet Protocol version 4 (IPv4) IP traffic with a Differentiated Services Code Point (DSCP) tag any value 0 through 63 distinctively for voice media and voice signaling. The SUT has the ability to set DSCP voice media and voice signaling distinctively any value 0 to 63 which meets this requirement with one minor exception. When the SUT is registering, it incorrectly tags trivial file transfer protocol (TFTP) packets with a DSCP tag of 0 (best effort). However, after the registration is completed TFTP packets are correctly tagged. This discrepancy was adjudicated by Defense Information Systems Agency (DISA) as having a minor operational impact. In addition, with shared access the SUT, data traffic from the data port is untagged with a DSCP value of 0 (best effort) which also meets this requirement. The SUT was tested for shared access as depicted in Figure 2-9. The Ixia IP load device was used to generate 100 percent of the SUT shared access bandwidth of 100 Megabits per Second (Mbps). In addition, while the Ixia shared access load was generated through the SUT, a voice call was successfully placed between two SUTs as depicted in Figure 2-9. Furthermore, the Sage 935AT was connected to the SUT handsets to measure packet loss and determine that the SUT is properly prioritizing and queuing voice media and signaling packets above data. The Sage 935AT recorded no packet loss which, meets this requirement.

(3) The UCR, section 5.2.12.6.6, states that a DSCD device that supports one of the required signaling modes shall interoperate with and establish secure session with other compatible devices with at least a 85 percent secure call completion rate. A total of 800 secure calls were placed with the SUT to other DSCD secure devices listed in Table 2-2 over the test configurations depicted in Figures 2-2 through 2-8 with a secure call completion rate of 92 percent, which meets this requirement.

(4) The UCR, section 5.2.12.6.6, states that the DSCD shall be capable of using the protocols provided to establish a secure session within 60 seconds and must maintain secure communications for the duration of the secure portion of the call. The SUT setup secure calls over the test configurations depicted in Figures 2-2 through 2-8.

All calls established a secure connection within 37 seconds and maintained calls until sessions were ended, which meets this requirement.

(5) The UCR, section 5.2.12.6.6, states that the DSCD shall operate in a network that has an end-to-end latency of up to 600 ms. The SUT was able to establish secure calls over the test configurations depicted in Figures 2-2 through 2-8. The maximum end-to-end latency was 1000 ms, which meets this requirement.

(6) The UCR, section 5.2.12.6.6, states that the DSCD shall achieve and maintain a secure voice connection with a minimum Mean Opinion Score (MOS) of 3.0. In the non-secure mode, the SUT is required to maintain a non-secure voice connection with a minimum a MOS of 4.0 or better. A SAGE 935AT was used to measure MOS from the handset of the SUT. The SUT non-secure voice connection measured a MOS between 4.2 and 4.49 with an average of 4.4. The SUT secure voice connection at 9.6 kilobits per second (kbps) Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-A CELP) measured a MOS from 3.87 to 3.95 for an average of 3.91, which meets this requirement.

(7) The UCR, section 5.2.12.6.6, states that once connected to the rekey center, the DSCD shall obtain a new key and properly process that new key with a 95 percent rekey completion rate. The SUT rekey completion rate over test configurations depicted in Figures 2-2 through 2-8 was 100 percent for a total of 12 rekey calls attempted, which meets this requirement.

(8) Security. The security requirements for DSCD devices with IP interfaces are satisfied with a NSA Type I accreditation and Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG) accreditation. The SUT NSA Type I accreditation was granted on 7 September 2007. The DSAWG accreditation was granted on 1 October 2009.

**12. TEST AND ANALYSIS REPORT.** No detailed test report was developed in accordance with the Program Manager's request. The JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet), or <http://199.208.204.125> (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>.