



## DEFENSE INFORMATION SYSTEMS AGENCY

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

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

**24 Apr 12**

**SUBJECT:** Extension of the Special Interoperability Test Certification of the Enterasys S Series SSA Switches from release 7.41.01.0013 to release 7.41.02.0014

**References:** (a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2005  
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008  
(c) through (f), see Enclosure

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 Enterasys SSA-G1018-0652 (S150/155 series) Switch with release 7.41 was tested as a distribution switch and is hereinafter referred to as the System Under Test-G (SUT-G). The SUT-G meets all of its critical interoperability requirements and is certified for joint use within the Defense Information System Network (DISN) as an Assured Services Local Area Network (ASLAN) distribution and Layer 2 (L2)/Layer 3 (L3) access switch. The SUT-G is certified as interoperable for joint use with other ASLAN components listed on the Unified Capabilities (UC) Approved Products List (APL) with the following interfaces: 10/100/1000BaseT and 100/1000BaseX for access, 10/100/1000BaseT and 100/1000/10GBaseX for uplink. The SUT-G meets the critical interoperability requirements set forth in Reference (c), using test procedures derived from Reference (d).

The Enterasys SSA-T4068-0252 (S130 series) Switch with release 7.41 was tested as an access switch and is hereinafter referred to as the System Under Test-T (SUT-T). The SUT-T meets all of its critical interoperability requirements and is certified for joint use within the DISN as an Assured Services Local Area Network (ASLAN) L2/L3 access switch. The SUT-T is certified as interoperable for joint use with other ASLAN components listed on the Unified Capabilities (UC) Approved Products List (APL) with the following interfaces: 10/100/1000BaseT and 100/1000BaseX for access, 10/100/1000BaseT and 100/1000/10GBaseX for uplink. The SUT-T meets the critical interoperability requirements set forth in Reference (c), using test procedures derived from Reference (d). The Enterasys SSA-T1068-0652 (S150/155 series) employs the same software and similar hardware as the SUT-T. JITC analysis determined this system to be functionally identical to the SUT-T for interoperability certification purposes, and it is also certified for joint use.

The SUT is certified to support DISN Assured Services over Internet Protocol. If a component meets the minimum requirements for deployment in an ASLAN, it also meets the lesser requirements for deployment in a non-ASLAN. Non-ASLANs are "commercial grade" and

JITC Memo, JTE, Extension of the Special Interoperability Test Certification of the Enterasys S Series SSA Switches from release 7.41.01.0013 to release 7.41.02.0014

provide support to Command and Control (C2) (ROUTINE only calls) (C2(R)), or non-C2 voice subscribers. The SUT is certified for joint use deployment in a non-ASLAN for C2(R) and non-C2 traffic. When deployed in a non-ASLAN, the SUT may also be used to receive all levels of precedence but is limited to supporting calls that are originated at ROUTINE precedence only. Non-ASLANs do not meet the availability or redundancy requirements for C2 or Special C2 users and therefore are not authorized to support precedence calls originated above ROUTINE.

Testing of the SUT did not include video services or data applications; however, simulated preferred data, best effort data, and video traffic were generated during testing to determine the SUT's ability to prioritize and properly queue voice media and signaling traffic. No other configurations, features, or functions, except those cited within this document, are certified by JITC. This certification expires upon changes that affect interoperability but no later than three years from the date of the signed Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) approval Memorandum (12 December 2011).

3. The extension of this certification is based upon Desktop Review (DTR) 1. The original certification is based on interoperability testing conducted by the United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC TIC), review of the vendor's Letter(s) of Compliance (LoC), and the DISA CA Recommendation. Interoperability testing was conducted by the USAISEC TIC, Fort Huachuca, Arizona, from 18 July through 26 August 2011 and documented in Reference (e). Review of the vendor's LoC was completed on 17 August 2011. The DISA CA provided a positive recommendation on 17 October 2011, based on the security testing completed by USAISEC TIC-led Information Assurance (IA) test teams. Those test results are published in a separate report, Reference (f). This DTR was requested to include release 7.41.02.0014. This release includes minor software changes related to commercial functionality and doesn't affect Assured Services. Therefore, JITC approves this DTR. The IA posture has not changed. The original IA approval applies to this DTR.

4. Table 1 provides the SUT-G's and STU-T's interface status. The SUT-G's and STU-T's capability and functional requirements are listed in Table 2.

**Table 1. SUT Interface Status**

Interface	Applicability			CRs/FRs (See note 1.)	Status		
	Co	D	A		Co	D	A
<b>Network Management Interfaces for Core Layer Switches</b>							
EIA/TIA-232 (Serial)	R	R	R	EIA/TIA-232	Met	Met	Met
IEEE 802.3i (10BaseT UTP)	C	C	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Met	Met	Met
IEEE 802.3u (100BaseT UTP)	C	C	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Met	Met	Met
IEEE 802.3ab (1000BaseT UTP)	C	C	C	1, 6-15, 18-28, 31, 32-36, 48-53, 58-60, 65, 67-71	Met	Met	Met
<b>Uplink Interfaces for Core Layer Switches</b>							
IEEE 802.3u (100BaseT UTP)	R	R	C <sup>2</sup>	1-15, 16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met	Met	Met
IEEE 802.3u (100BaseFX)	C	C	C <sup>2</sup>	1-6, 11, 16, 18-24, 28-31, 40-41, 44-53, 55-60, 65-75	Met	Met	Met
IEEE 802.3ab (1000BaseT UTP)	C	C	C <sup>2</sup>	1-16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met	Met	Met
IEEE 802.3z (1000BaseX Fiber)	R	R	C <sup>2</sup>	1-5, 8-16, 18-24, 28-31, 40, 44-53, 55-60, 65-75	Met	Met	Met
IEEE 802.3ae (10GBaseX)	C	C	C <sup>2</sup>	1-5, 8-16, 18, 19, 40-41, 44-53, 55-60, 65-75	Met	Met	Met
<b>Access Interfaces for Core Layer Switches</b>							
IEEE 802.3i (10BaseT UTP)	C	C	C <sup>2</sup>	1-15, 18-24, 28-41, 44-54, 58-71	Met	Met	Met
IEEE 802.3u (100BaseT UTP)	R	R	C <sup>2</sup>	1-15, 18-24, 28-41, 44-54, 58-71	Met	Met	Met
IEEE 802.3u (100BaseFX)	C	C	C <sup>2</sup>	1-6, 11, 18-24, 28-31, 44-54, 58-71	Met	Met	Met
IEEE 802.3ab (1000BaseT UTP)	C	C	C <sup>2</sup>	1-15, 18-24, 28-41, 44-54, 58-71	Met	Met	Met
IEEE 802.3z (1000BaseX Fiber)	R	R	C <sup>2</sup>	1-6, 11, 18-24, 28-31, 44-54, 58-71	Met	Met	Met
<b>Generic Requirements for all Interfaces</b>							
Generic Requirements not associated with specific interfaces	R	R	R	30-32, 35, 36, 40, 69-71	Met	Met	Met
DoD IPv6 Profile Requirements	R	R	R	UCR Section 5.3.5.5	Met	Met	Met
Security	R	R	R	UCR Sections 5.3.1.3.8, 5.3.1.5, 5.3.1.6, and 5.4	Met <sup>3</sup>	Met <sup>3</sup>	Met <sup>3</sup>
<b>NOTES:</b>							
<p>1. The SUT's specific capability and functional requirement ID numbers depicted in the CRs/FRs column can be cross-referenced in Table 2. These requirements are for the following switch model, which is certified for Distribution and Layer 2/Layer 3 Access in the ASLAN: Enterasys <b>SSA-G1018-0652</b>. These requirements are also for the following switch models, which are certified for Layer 2/Layer 3 Access in the ASLAN: Enterasys <b>SSA-T4068-0252</b> and SSA-T1068-0652. The devices listed that are not bolded or underlined are in the same family series as the SUT but were not tested. However, they utilize the same OS software and similar hardware as the SUT, and JITC analysis determined them to be functionally identical for interoperability certification purposes.</p> <p>2. Access layer switches are required to support only one of the following IEEE interfaces: 802.3i, 802.3j, 802.3u, 802.3ab, or 802.3z.</p> <p>3. Security testing is accomplished via USAISEC TIC-led IA test teams, and the results are published in a separate report, Reference (f).</p>							
<b>LEGEND:</b>							
802.3ab	1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps)	D	Distribution				
802.3ae	10 Gbps Ethernet	DoD	Department of Defense				
802.3i	10BaseT Mbps over twisted pair	EIA	Electronic Industries Alliance				
802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps	EIA-232	Standard for defining the mechanical and electrical characteristics for connecting Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) data communications devices				
802.3z	Gigabit Ethernet Standard						
10BaseT	10 Mbps (Baseband Operation, Twisted Pair) Ethernet	FR	Functional Requirement				
100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet	IA	Information Assurance				
100BaseFX	100 Mbps Ethernet over fiber	ID	Identification				
1000BaseFX	1000 Mbps Ethernet over fiber	IEEE	Institute of Electrical and Electronics Engineers				
1000BaseT	1000 Mbps (Baseband Operation, Twisted Pair) Ethernet	IPv6	Internet Protocol version 6				
10GBaseX	10000 Mbps Ethernet over Category 5 Twisted Pair Copper	JITC	Joint Interoperability Test Command				
A	Access	OS	Operating System				
ASLAN	Assured Services Local Area Network	R	Required				
C	Conditional	SSA	S-series Stand Alone				
Co	Core	SUT	System Under Test				
CR	Capability Requirement	TIA	Telecommunications Industry Association				
		TIC	Technology Integration Center				
		UCR	Unified Capabilities Requirements				
		USAISEC	U.S. Army Information Systems Engineering Command				
		UTP	Unshielded Twisted Pair				

**Table 2. SUT Capability and Functional Requirements**

ID	Requirement (See note.)	UCR Reference
1	ASLAN components can have no single point of failure for >96 users for C2 and Special C2 users. Non-ASLAN components can have a single point of failure for C2(R) and non-C2 users. (R)	5.3.1.2.1, 5.3.1.7.7
2	Non-blocking of any voice or video traffic at 50% for core and distribution layer switches and 12.5% blocking for access layer switches. (R)	5.3.1.3
3	Maximum of 1 millisecond (ms) of jitter for voice and 10 ms for video for all ASLAN components. (R) Does not apply to preferred data and best effort data.	5.3.1.3
4	Maximum of 0.015% packet loss for voice and 0.05 % for video and preferred data for all ASLAN components. (R)	5.3.1.3
5	Maximum of 2 ms latency for voice, 10 ms for video, and 15 ms for preferred data for all ASLAN components. (R) Does not apply to best effort data.	5.3.1.3
6	100 Mbps IAW IEEE 802.3u and 1 Gbps IAW IEEE 802.3z for core and distribution layer components and only one of the following IEEE interfaces for access layer components: 802.3i, 802.3j, 802.3u, 802.3ab, or 802.3z. (R)	5.3.1.3.1
7	Force mode and auto-negotiation IAW IEEE 802.3, filtering IAW RFC 1812, and flow control IAW IEEE 802.3x. (R)	5.3.1.3.2
8	Port Parameter Requirements	Auto-negotiation IAW IEEE 802.3. (R)
9		Force mode IAW IEEE 802.3. (R)
10		Flow control IAW IEEE 802.3x. (R)
11		Filtering IAW RFC 1812. (R)
12		Link Aggregation IAW IEEE 802.3ad (output/egress ports only). (R)
13		Spanning Tree Protocol IAW IEEE 802.1D. (R)
14		Multiple Spanning Tree IAW IEEE 802.1s. (R)
15	Port Parameter Requirements (continued)	Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w. (R)
16	LACP link Failover and Link Aggregation IAW IEEE 802.3ad (uplink ports only) for core and distribution switches. (C)	5.3.1.3.2, 5.3.1.7.7.1
17	Class of Service Marking: Layer 3 DSCPs IAW RFC 2474 (R); Layer 2 3-bit user priority field of the IEEE 802.1Q 2-byte TCI field. (C)	5.3.1.3.3
18	VLAN capabilities IAW IEEE 802.1Q. (R)	5.3.1.3.4
19	Protocols IAW DISR profile (IPv4 and IPv6). IPv4 (R: LAN Switch, Layer 2 Switch): IPv6 (R: LAN Switch, C: Layer 2 Switch). Note: The Layer 2 switch is required to support only RFCs 2460, 5095, and 2464, and it must be able to queue packets based on DSCPs in accordance with (IAW) RFC 2474.	5.3.1.3.5
20	QoS Features	Shall support minimum of 4 queues. (R)
21		Must be able to assign VLAN tagged packets to a queue. (R)
22		Support DSCP PHBs per RFCs 2474, 2494, 2597, 2598, and 3246. (R: LAN Switch) Note: Layer 2 switch is required to support RFC 2474 only.
23		Support a minimum of one of the following: Weighted Fair Queuing (WFQ) IAW RFC 3662, Priority Queuing (PQ) IAW RFC 1046, Custom Queuing (CQ) IAW RFC 3670, or Class-Based WFQ IAW RFC 3366. (R)
24	Must be able to assign a bandwidth or a percentage of traffic to any queue. (R)	5.3.1.3.6
25	SNMP IAW RFCs 1157, 2206, 3410, 3411, 3412, 3413, and 3414. (R)	
26	SNMP traps IAW RFC 1215. (R)	
27	Remote monitoring IAW RFC 1281 and Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826. (R)	5.3.1.3.7
28	Product Requirements Summary IAW UCR 2008, Table 5.3.1-5. (R)	5.3.1.3.9
29	E2E Performance (Voice)	No more than 6 ms Latency over any 5-minute period measured under 100% congestion. (R)
		No more than 3 ms Jitter over any 5-minute period measured under 100% congestion. (R)
		Packet loss not to exceed .045% engineered (queuing) parameters over any 5-minute period under congestion. (R)
30	E2E Performance (Video)	No more than 30 ms Latency over any 5-minute period measured under 100% congestion. (R)
		No more than 30 ms Jitter over any 5-minute period measured under congestion. (R)
		Packet loss not to exceed 15% engineered (queuing) parameters over any 5-minute period under 100% congestion. (R)
31	E2E Performance (Data)	No more than 45 ms Latency over any 5-minute period measured under congestion. (R)
		Packet loss not to exceed engineered (queuing) parameters over any 5-minute period under congestion. (R)
32	LAN Network Management	Configuration Control for ASLAN and non-ASLAN. (R)
33		Operational Controls for ASLAN and non-ASLAN. (R)
34		Performance Monitoring for ASLAN and non-ASLAN. (R)
35		Alarms for ASLAN and non-ASLAN. (R)
36		Reporting for ASLAN and non-ASLAN. (R)

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

ID	Requirement (See note.)	UCR Reference	
37	Redundancy	5.3.1.7.7	
38			Redundant Power Supplies. (required on standalone redundant products)
39			Chassis Failover. (required on standalone redundant products)
40			Switch Fabric Failover. (required on standalone redundant products)
41			Non-LACP Link Failover. (R)
42			Fiber Blade Failover. (R)
43			Stack Failover. (C) (required if the stack supports more than 96 users)
44	CPU (routing engine) blade Failover. (R)	5.3.1.8.4.1	
45	MPLS may not add measurable Loss or Jitter to system. (C)	5.3.1.8.4.1	
46	MPLS conforms to RFCs in Table 5.3.1-14. (C)	5.3.1.8.4.2.1	
47	MPLS supports L2 and L3 VPNs. (C)	/2	
48	IPv6 Product Requirements: Dual Stack for IPv4 and IPv6 IAW RFC 4213 if routing functions are supported. (C)	5.3.5.4	
49	IPv6 System Requirements	5.3.5.4	
50		Support IPv6 IAW RFCs 2460 and 5095 if routing functions are supported. (C)	
51		Support IPv6 packets over Ethernet IAW RFC 2464. (R)	
52		Support MTU discovery IAW RFC 1981 if routing functions are supported. (R)	
53		Support a minimum MTU of 1280 IAW RFCs 2460 and 5095. (C)	
54		Shall support IPv6 addresses IAW RFC 4291. (R)	
55		Shall support IPv6 scoped addresses IAW RFC 4007. (R)	
56	If routing functions are supported: If DHCP is supported, it must be IAW RFC 3315; if DHCPv6 is supported, it shall be IAW RFC 3313. (C)	5.3.5.4.4	
55	IPv6 Router Advertisements	5.3.5.4.5.2	
56	If the system supports routing functions, the system shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link, shall log any inconsistent router advertisements, and shall prefer routers that are reachable over routers whose reachability is suspect or unknown. (C)	5.3.5.4.5.2	
57	IPv6 Router Advertisements (continued)	5.3.5.4.5.2	
58	IPv6 Neighbor Discovery	5.3.5.4.5	
59	If the system supports routing functions, the system shall include the MTU value in the router advertisement message for all links IAW RFC 2461 and RFC 4861. (C)	5.3.5.4.5.2	
60	IPv6 Neighbor Discovery	5.3.5.4.5	
61	IPv6 Neighbor Discovery	5.3.5.4.5	
62	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
63	IPv6 Neighbor Discovery	5.3.5.4.5	
64	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
65	IPv6 Neighbor Discovery	5.3.5.4.5	
66	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
67	IPv6 Neighbor Discovery	5.3.5.4.5	
68	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
69	IPv6 Neighbor Discovery	5.3.5.4.5	
70	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
71	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
72	IPv6 Neighbor Discovery	5.3.5.4.5	
73	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
74	IPv6 Neighbor Discovery	5.3.5.4.5	
75	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
76	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
77	IPv6 Neighbor Discovery	5.3.5.4.5	
78	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
79	IPv6 Neighbor Discovery	5.3.5.4.5	
80	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
81	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
82	IPv6 Neighbor Discovery	5.3.5.4.5	
83	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
84	IPv6 Neighbor Discovery	5.3.5.4.5	
85	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
86	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
87	IPv6 Neighbor Discovery	5.3.5.4.5	
88	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
89	IPv6 Neighbor Discovery	5.3.5.4.5	
90	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
91	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
92	IPv6 Neighbor Discovery	5.3.5.4.5	
93	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
94	IPv6 Neighbor Discovery	5.3.5.4.5	
95	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
96	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
97	IPv6 Neighbor Discovery	5.3.5.4.5	
98	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
99	IPv6 Neighbor Discovery	5.3.5.4.5	
100	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
101	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
102	IPv6 Neighbor Discovery	5.3.5.4.5	
103	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
104	IPv6 Neighbor Discovery	5.3.5.4.5	
105	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
106	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
107	IPv6 Neighbor Discovery	5.3.5.4.5	
108	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
109	IPv6 Neighbor Discovery	5.3.5.4.5	
110	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
111	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
112	IPv6 Neighbor Discovery	5.3.5.4.5	
113	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
114	IPv6 Neighbor Discovery	5.3.5.4.5	
115	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
116	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
117	IPv6 Neighbor Discovery	5.3.5.4.5	
118	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
119	IPv6 Neighbor Discovery	5.3.5.4.5	
120	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
121	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
122	IPv6 Neighbor Discovery	5.3.5.4.5	
123	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
124	IPv6 Neighbor Discovery	5.3.5.4.5	
125	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
126	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
127	IPv6 Neighbor Discovery	5.3.5.4.5	
128	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
129	IPv6 Neighbor Discovery	5.3.5.4.5	
130	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
131	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
132	IPv6 Neighbor Discovery	5.3.5.4.5	
133	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
134	IPv6 Neighbor Discovery	5.3.5.4.5	
135	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
136	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
137	IPv6 Neighbor Discovery	5.3.5.4.5	
138	The system shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the system is providing proxy service. (R)	5.3.5.4.5	
139	IPv6 Neighbor Discovery	5.3.5.4.5	
140	If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C)	5.3.5.4.5	
141	The system shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements. (R)	5.3.5.4.5	
142	IPv6 Neighbor Discovery		

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

ID	Requirement (See note.)		UCR Reference																																																																																																						
72	IPv6 Routing Functions	If the system supports routing functions, the system shall support the OSPF for IPv6 as described in RFC 5340. (C)	5.3.5.4.8																																																																																																						
73		If the system supports routing functions, the system shall support securing OSPF with Internet Protocol Security (IPSec) as described for other IPSec instances in UCR 2008, Section 5.4. (C)																																																																																																							
74		If the system supports routing functions, the system shall support OSPF for IPv6 as described in RFC 2740, router-to-router integrity using an IP authentication header with HMAC-SHA1-96 with ESP and AH as described in RFC 2404, and shall support OSPFv3 IAW RFC 4552. (C)																																																																																																							
75		If the system supports routing functions, the system shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810. (C)																																																																																																							
76	Site Requirements	Engineering Requirements: Physical Media for ASLAN and non-ASLAN. (R) (Site requirement)	5.3.1.7.1																																																																																																						
77		Battery back-up: two hours for non-ASLAN components and eight hours for ASLAN components. (R) (Site requirement)	5.3.1.7.5																																																																																																						
78		Availability of 99.999% (Special C2), 99.997% (C2) for ASLAN (R), and 99.9% (non-C2 and C2(R)) for non-ASLAN. (R) (Site requirement)	5.3.1.7.6																																																																																																						
79	IA Security Requirements	Port-Based Access Control IAW IEEE 802.1x and 802.3x. (R)	5.3.1.3.2																																																																																																						
80		Secure methods for network configuration: SSH2 instead of Telnet and support RFCs 4251-4254. Must use HTTPS instead of http and support RFCs 2660 and 2818 for ASLAN and non-ASLAN. (R)	5.3.1.6																																																																																																						
81		Security. (R)	5.3.1.3.8																																																																																																						
82		Must meet IA requirements IAW UCR 2008 Section 5.4 for ASLAN and non-ASLAN. (R)	5.3.1.5																																																																																																						
<p><b>NOTE:</b> All requirements are for core, distribution, and access layer components unless otherwise specified.</p> <p><b>LEGEND:</b></p> <table border="0"> <tr> <td>AH</td> <td>Authentication Header</td> <td>HMAC</td> <td>Hash-based Message</td> <td>MTU</td> <td>Maximum Transmission Unit</td> </tr> <tr> <td>ASLAN</td> <td>Assured Services Local Area Network</td> <td>HTTP</td> <td>Hypertext Transfer Protocol</td> <td>OSPF</td> <td>Open Shortest Path First</td> </tr> <tr> <td>C</td> <td>Conditional</td> <td>HTTPS</td> <td>Hypertext Transfer Protocol, Secure</td> <td>OSPFv3</td> <td>Open Shortest Path First Version 3</td> </tr> <tr> <td>C2</td> <td>Command and Control</td> <td>IA</td> <td>Information Assurance</td> <td>PHB</td> <td>Per Hop Behavior</td> </tr> <tr> <td>C2(R)</td> <td>Command and Control ROUTINE only</td> <td>IAW</td> <td>in accordance with</td> <td>QoS</td> <td>Quality of Service</td> </tr> <tr> <td>CPU</td> <td>Central Processing Unit</td> <td>ICMP</td> <td>Internet Control Message Protocol</td> <td>R</td> <td>Required</td> </tr> <tr> <td>DAD</td> <td>Duplicate Address Detection</td> <td>ICMPv6</td> <td>Internet Control Message Protocol for IPv6</td> <td>RFC</td> <td>Request for Comments</td> </tr> <tr> <td>DHCP</td> <td>Dynamic Host Configuration Protocol</td> <td>ID</td> <td>Identification</td> <td>SHA</td> <td>Secure Hash Algorithm</td> </tr> <tr> <td>DHCPv6</td> <td>Dynamic Host Configuration Protocol for IPv6</td> <td>IEEE</td> <td>Institute of Electrical and Electronics Engineers</td> <td>SLAAC</td> <td>Stateless Auto Address Configuration</td> </tr> <tr> <td>DISR</td> <td>Department of Defense Information Technology Standards Registry</td> <td>IPv4</td> <td>Internet Protocol version 4</td> <td>SNMP</td> <td>Simple Network Management Protocol</td> </tr> <tr> <td>DSCP</td> <td>Differentiated Services Code Point</td> <td>IPv6</td> <td>Internet Protocol version 6</td> <td>SSH2</td> <td>Secure Shell Version 2</td> </tr> <tr> <td>E2E</td> <td>End-to-End</td> <td>LACP</td> <td>Link Aggregation Control Protocol</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>ESP</td> <td>Encapsulating Security Payload</td> <td>LAN</td> <td>Local Area Network</td> <td>TCI</td> <td>Tag Control Information</td> </tr> <tr> <td>Gbps</td> <td>Gigabits per second</td> <td>LS</td> <td>LAN Switch</td> <td>UC</td> <td>Unified Capabilities</td> </tr> <tr> <td></td> <td></td> <td>Mbps</td> <td>Megabits per second</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> <tr> <td></td> <td></td> <td>MPLS</td> <td>Multiprotocol Label Switching</td> <td>VLAN</td> <td>Virtual Local Area Network</td> </tr> <tr> <td></td> <td></td> <td>ms</td> <td>millisecond</td> <td>VPN</td> <td>Virtual Private Network</td> </tr> </table>				AH	Authentication Header	HMAC	Hash-based Message	MTU	Maximum Transmission Unit	ASLAN	Assured Services Local Area Network	HTTP	Hypertext Transfer Protocol	OSPF	Open Shortest Path First	C	Conditional	HTTPS	Hypertext Transfer Protocol, Secure	OSPFv3	Open Shortest Path First Version 3	C2	Command and Control	IA	Information Assurance	PHB	Per Hop Behavior	C2(R)	Command and Control ROUTINE only	IAW	in accordance with	QoS	Quality of Service	CPU	Central Processing Unit	ICMP	Internet Control Message Protocol	R	Required	DAD	Duplicate Address Detection	ICMPv6	Internet Control Message Protocol for IPv6	RFC	Request for Comments	DHCP	Dynamic Host Configuration Protocol	ID	Identification	SHA	Secure Hash Algorithm	DHCPv6	Dynamic Host Configuration Protocol for IPv6	IEEE	Institute of Electrical and Electronics Engineers	SLAAC	Stateless Auto Address Configuration	DISR	Department of Defense Information Technology Standards Registry	IPv4	Internet Protocol version 4	SNMP	Simple Network Management Protocol	DSCP	Differentiated Services Code Point	IPv6	Internet Protocol version 6	SSH2	Secure Shell Version 2	E2E	End-to-End	LACP	Link Aggregation Control Protocol	SUT	System Under Test	ESP	Encapsulating Security Payload	LAN	Local Area Network	TCI	Tag Control Information	Gbps	Gigabits per second	LS	LAN Switch	UC	Unified Capabilities			Mbps	Megabits per second	UCR	Unified Capabilities Requirements			MPLS	Multiprotocol Label Switching	VLAN	Virtual Local Area Network			ms	millisecond	VPN	Virtual Private Network
AH	Authentication Header	HMAC	Hash-based Message	MTU	Maximum Transmission Unit																																																																																																				
ASLAN	Assured Services Local Area Network	HTTP	Hypertext Transfer Protocol	OSPF	Open Shortest Path First																																																																																																				
C	Conditional	HTTPS	Hypertext Transfer Protocol, Secure	OSPFv3	Open Shortest Path First Version 3																																																																																																				
C2	Command and Control	IA	Information Assurance	PHB	Per Hop Behavior																																																																																																				
C2(R)	Command and Control ROUTINE only	IAW	in accordance with	QoS	Quality of Service																																																																																																				
CPU	Central Processing Unit	ICMP	Internet Control Message Protocol	R	Required																																																																																																				
DAD	Duplicate Address Detection	ICMPv6	Internet Control Message Protocol for IPv6	RFC	Request for Comments																																																																																																				
DHCP	Dynamic Host Configuration Protocol	ID	Identification	SHA	Secure Hash Algorithm																																																																																																				
DHCPv6	Dynamic Host Configuration Protocol for IPv6	IEEE	Institute of Electrical and Electronics Engineers	SLAAC	Stateless Auto Address Configuration																																																																																																				
DISR	Department of Defense Information Technology Standards Registry	IPv4	Internet Protocol version 4	SNMP	Simple Network Management Protocol																																																																																																				
DSCP	Differentiated Services Code Point	IPv6	Internet Protocol version 6	SSH2	Secure Shell Version 2																																																																																																				
E2E	End-to-End	LACP	Link Aggregation Control Protocol	SUT	System Under Test																																																																																																				
ESP	Encapsulating Security Payload	LAN	Local Area Network	TCI	Tag Control Information																																																																																																				
Gbps	Gigabits per second	LS	LAN Switch	UC	Unified Capabilities																																																																																																				
		Mbps	Megabits per second	UCR	Unified Capabilities Requirements																																																																																																				
		MPLS	Multiprotocol Label Switching	VLAN	Virtual Local Area Network																																																																																																				
		ms	millisecond	VPN	Virtual Private Network																																																																																																				

5. In accordance with the Program Manager’s request, no detailed test report was developed. 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). STP is accessible by .mil/.gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to DISN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. 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 U.S. Government civilian or uniformed

JITC Memo, JTE, Extension of the Special Interoperability Test Certification of the Enterasys S Series SSA Switches from release 7.41.01.0013 to release 7.41.02.0014

military personnel at the Unified Capabilities Certification Office (UCCO); e-mail: [ucco@disa.mil](mailto:ucco@disa.mil).

6. The JITC point of contact is Mr. Edward Mellon, DSN 879-5159, commercial (520) 538-5159, FAX DSN 879-4347, or e-mail to [Edward.Mellon@disa.mil](mailto:Edward.Mellon@disa.mil). JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The Tracking Number for the SUT is 1035402.

FOR THE COMMANDER:

Enclosure a/s

  
for BRADLEY A. CLARK  
Chief  
Battlespace Communications Portfolio

DISTRIBUTION (electronic mail):

Joint Staff J-6

Joint Interoperability Test Command, Liaison, TE3/JT1

Office of Chief of Naval Operations, CNO N6F2

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

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

U.S. Marine Corps 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

**This page intentionally left blank.**

## **ADDITIONAL REFERENCES**

- (c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008, Change 2," 31 December 2010
- (d) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP), Change 2," 2 October 2006
- (e) Joint Interoperability Test Command, Memo, JTE, "Special Interoperability Test Certification of the Enterasys S Series SSA Switches with release 7.41.," 6 December 2011
- (f) U.S. Army Information Systems Engineering Command (HQUSAISEC), Technology Integration Center (TIC), "Information Assurance (IA) Assessment of Enterasys K Series Switches (Tracking Number 1035402)," 17 October 2011