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

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) 6 Dec 11

SUBJECT: Special Interoperability Test Certification of the Enterasys K Series Switches with release 7.41.

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 (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 Enterasys K10 and K6 Switches with release 7.41 are 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 Information System Network (DISN) as an Assured Services Local Area Network (ASLAN) distribution and Layer 3 access switch. The SUT 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 meets the critical interoperability requirements set forth in Reference (c), using test procedures derived from Reference (d).

The SUT is certified to support Defense Information System Network (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 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.

3. This finding 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 Letters 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. 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 (e).

4. Table 1 provides the SUT's interface status. The SUT'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 |
| **Network Management Interfaces for Core Layer Switches** | | | | | | | |
| 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 |
| **Uplink Interfaces for Core Layer Switches** | | | | | | | |
| IEEE 802.3u (100BaseT UTP) | R | R | C[2] | 1-15, 16, 18-24, 28-31, 40, 44-53, 55-60, 65-75 | Met | Met | Met |
| IEEE 802.3u (100BaseFX) | C | C | C[2] | 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[2] | 1-16, 18-24, 28-31, 40, 44-53, 55-60, 65-75 | Met | Met | Met |
| IEEE 802.3z (1000BaseX Fiber) | R | R | C[2] | 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[2] | 1-5, 8-16, 18, 19, 40-41, 44-53, 55-60, 65-75 | Met | Met | Met |
| **Access Interfaces for Core Layer Switches** | | | | | | | |
| IEEE 802.3i (10BaseT UTP) | C | C | C[2] | 1-15, 18-24, 28-41, 44-54, 58-71 | Met | Met | Met |
| IEEE 802.3u (100BaseT UTP) | R | R | C[2] | 1-15, 18-24, 28-41, 44-54, 58-71 | Met | Met | Met |
| IEEE 802.3u (100BaseFX) | C | C | C[2] | 1-6, 11, 18-24, 28-31, 44-54, 58-71 | Met | Met | Met |
| IEEE 802.3ab (1000BaseT UTP) | C | C | C[2] | 1-15, 18-24, 28-41, 44-54, 58-71 | Met | Met | Met |
| IEEE 802.3z (1000BaseX Fiber) | R | R | C[2] | 1-6, 11, 18-24, 28-31, 44-54, 58-71 | Met | Met | Met |
| **Generic Requirements for all Interfaces** | | | | | | | |
| 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[3] | Met[3] | Met[3] |

## Table 1. SUT Interface Status (continued)

**NOTES:**

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 models, which are certified for Distribution and Access in the ASLAN: Enterasys **K10**, **K6.**
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.
3 Security testing is accomplished via USAISEC TIC-led IA test teams, and the results are published in a separate report, Reference (e).

**LEGEND:**

| | |
|---|---|
| 802.3ab | 1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps) |
| 802.3ae | 10 Gbps Ethernet |
| 802.3i | 10BaseT Mbps over twisted pair |
| 802.3u | Standard for carrier sense multiple access with collision detection at 100 Mbps |
| 802.3z | Gigabit Ethernet Standard |
| 10BaseT | 10 Mbps (Baseband Operation, Twisted Pair) Ethernet |
| 100BaseT | 100 Mbps (Baseband Operation, Twisted Pair) Ethernet |
| 100BaseFX | 100 Mbps Ethernet over fiber |
| 1000BaseFX | 1000 Mbps Ethernet over fiber |
| 1000BaseT | 1000 Mbps (Baseband Operation, Twisted Pair) Ethernet |
| 10GBaseX | 10000 Mbps Ethernet over Category 5 Twisted Pair Copper |
| A | Access |
| ASLAN | Assured Services Local Area Network |
| C | Conditional |
| Co | Core |
| CR | Capability Requirement |
| D | Distribution |
| DoD | Department of Defense |
| EIA | Electronic Industries Alliance |
| 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 |
| FR | Functional Requirement |
| IA | Information Assurance |
| ID | Identification |
| IEEE | Institute of Electrical and Electronics Engineers |
| IPv6 | Internet Protocol version 6 |
| JITC | Joint Interoperability Test Command |
| OS | Operating System |
| R | Required |
| SUT | System Under Test |
| 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) | 5.3.1.3.2 |
| 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) | |

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

| ID | Requirement (See note.) | | UCR Reference |
|---|---|---|---|
| 15 | Port Parameter Requirements (continued) | Rapid Reconfiguration of Spanning Tree IAW IEEE 802.1w. (R) | 5.3.1.3.2 |
| 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 IAW RFC 2474. | | 5.3.1.3.5 |
| 20 | QoS Features | Shall support minimum of 4 queues. (R) | 5.3.1.3.6 |
| 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) | |
| 25 | Network Monitoring | SNMP IAW RFCs 1157, 2206, 3410, 3411, 3412, 3413, and 3414. (R) | 5.3.1.3.7 |
| 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) | |
| 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) | 5.3.1.4.1 |
| | | 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) | 5.3.1.4.2 |
| | | 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) | 5.3.1.4.3 |
| | | 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) | 5.3.1.6.1 |
| 33 | | Operational Controls for ASLAN and non-ASLAN. (R) | 5.3.1.6.2 |
| 34 | | Performance Monitoring for ASLAN and non-ASLAN. (R) | 5.3.1.6.3 |
| 35 | | Alarms for ASLAN and non-ASLAN. (R) | 5.3.1.6.4 |
| 36 | | Reporting for ASLAN and non-ASLAN. (R) | 5.3.1.6.5 |
| 37 | Redundancy | Redundant Power Supplies. (required on standalone redundant products) | 5.3.1.7.7 |
| 38 | | Chassis Failover. (required on standalone redundant products) | |
| 39 | | Switch Fabric Failover. (required on standalone redundant products) | |
| 40 | | Non-LACP Link Failover. (R) | |
| 41 | | Fiber Blade Failover. (R) | |
| 42 | | Stack Failover. (C) (required if the stack supports more than 96 users) | |
| 43 | | CPU (routing engine) blade Failover. (R) | |
| 44 | MPLS | MPLS may not add measurable Loss or Jitter to system. (C) | 5.3.1.8.4.1 |
| 45 | | MPLS conforms to RFCs in Table 5.3.1-14. (C) | 5.3.1.8.4.1 |
| 46 | | MPLS supports L2 and L3 VPNs. (C) | 5.3.1.8.4.2.1/2 |
| 47 | IPv6 Product Requirements: Dual Stack for IPv4 and IPv6 IAW RFC 4213 if routing functions are supported. (C) | | 5.3.5.4 |
| 48 | IPv6 System Requirements | Support IPv6 IAW RFCs 2460 and 5095 if routing functions are supported. (C) | 5.3.5.4 |
| 49 | | Support IPv6 packets over Ethernet IAW RFC 2464. (R) | 5.3.5.4 |
| 50 | | Support MTU discovery IAW RFC 1981 if routing functions are supported. (R) | 5.3.5.4.1 |
| 51 | | Support a minimum MTU of 1280 IAW RFCs 2460 and 5095. (C) | 5.3.5.4.1 |
| 52 | | Shall support IPv6 addresses IAW RFC 4291. (R) | 5.3.5.4.3 |
| 53 | | Shall support IPv6 scoped addresses IAW RFC 4007. (R) | 5.3.5.4.3 |
| 54 | | 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 Advertise-ments | 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 |

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

| ID | Requirement (See note.) | | UCR Reference |
|---|---|---|---|
| 56 | IPv6 Router Advertisements (continued) | 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 |
| 57 | | IPv6 Neighbor Discovery: 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) | |
| 58 | IPv6 Neighbor Discovery | If routing functions are supported: Neighbor Discovery IAW RFCs 2461 and 4861. (C) | 5.3.5.4.5 |
| 59 | | 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) | |
| 60 | | 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) | |
| 61 | IPv6 SLAAC and Manual Address Assignment | If the system supports stateless IP address Auto-configuration, the system shall support IPv6 SLAAC for interfaces supporting UC functions IAW RFC 2462 and RFC 4862. (C) | 5.3.5.4.6 |
| 62 | | If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the function to be enabled and disabled. (C) | |
| 63 | | If the product supports IPv6 SLAAC, 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 auto-configuration. (C) | |
| 64 | | If the product supports stateless IP address auto-configurations, including those provided for the commercial market, the DAD shall be disabled IAW RFC 2462 and RFC 4862. (R) | |
| 65 | | The system shall support manual assignment of IPv6 addresses. (R) | |
| 66 | | If the system provides routing functions, the system shall default to using the "managed address configuration" flag and the "other stateful" flag set to TRUE in the router advertisements when stateful auto-configuration is implemented. (C) | |
| 67 | IPv6 ICMP | The system shall support the ICMPv6 as described in RFC 4443. (R) | 5.3.5.4.7 |
| 68 | | The system shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages. (R) | |
| 69 | | The system shall support the capability to enable or disable the ability of the system to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. (R) Required if LS supports routing functions. | |
| 70 | | The system 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. (R) | |
| 71 | | The system shall validate ICMPv6 messages, using the information contained in the payload, prior to acting on them. (R) | |
| 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 |

**NOTE:** All requirements are for core, distribution, and access layer components unless otherwise specified.

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

**LEGEND:**

| | |
|---|---|
| AH | Authentication Header |
| ASLAN | Assured Services Local Area Network |
| C | Conditional |
| C2 | Command and Control |
| C2(R) | Command and Control ROUTINE only |
| CPU | Central Processing Unit |
| DAD | Duplicate Address Detection |
| DHCP | Dynamic Host Configuration Protocol |
| DHCPv6 | Dynamic Host Configuration Protocol for IPv6 |
| DISR | Department of Defense Information Technology Standards Registry |
| DSCP | Differentiated Services Code Point |
| E2E | End-to-End |
| ESP | Encapsulating Security Payload |
| Gbps | Gigabits per second |
| HMAC | Hash-based Message Authentication Code |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol, Secure |
| IA | Information Assurance |
| IAW | in accordance with |
| ICMP | Internet Control Message Protocol |
| ICMPv6 | Internet Control Message Protocol for IPv6 |
| ID | Identification |
| IEEE | Institute of Electrical and Electronics Engineers |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| LACP | Link Aggregation Control Protocol |
| LAN | Local Area Network |
| LS | LAN Switch |
| Mbps | Megabits per second |
| MPLS | Multiprotocol Label Switching |
| ms | millisecond |
| MTU | Maximum Transmission Unit |
| OSPF | Open Shortest Path First |
| OSPFv3 | Open Shortest Path First Version 3 |
| PHB | Per Hop Behavior |
| QoS | Quality of Service |
| R | Required |
| RFC | Request for Comments |
| SHA | Secure Hash Algorithm |
| SLAAC | Stateless Auto Address Configuration |
| SNMP | Simple Network Management Protocol |
| SSH2 | Secure Shell Version 2 |
| SUT | System Under Test |
| TCI | Tag Control Information |
| UC | Unified Capabilities |
| UCR | Unified Capabilities Requirements |
| VLAN | Virtual Local Area Network |
| 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 military personnel at the Unified Capabilities Certification Office (UCCO); e-mail: 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. JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The Tracking Number for the SUT is 1035405.

JITC Memo, JTE, Special Interoperability Test Certification of the Enterasys K Series Switches with release 7.41

FOR THE COMMANDER:

2 Encls as

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 MARCORSYSCOM, 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) U.S. Army Information Systems Engineering Command (HQUSAISEC), Technology Integration Center (TIC), "Information Assurance (IA) Assessment of Enterasys K Series Switches (Tracking Number 1035405)," 17 October 2011

**This page intentionally left blank.**

## CERTIFICATION TESTING SUMMARY

**1. SYSTEM TITLE**. Enterasys K Series Switches with release 7.41; hereinafter referred to as the system under test (SUT).

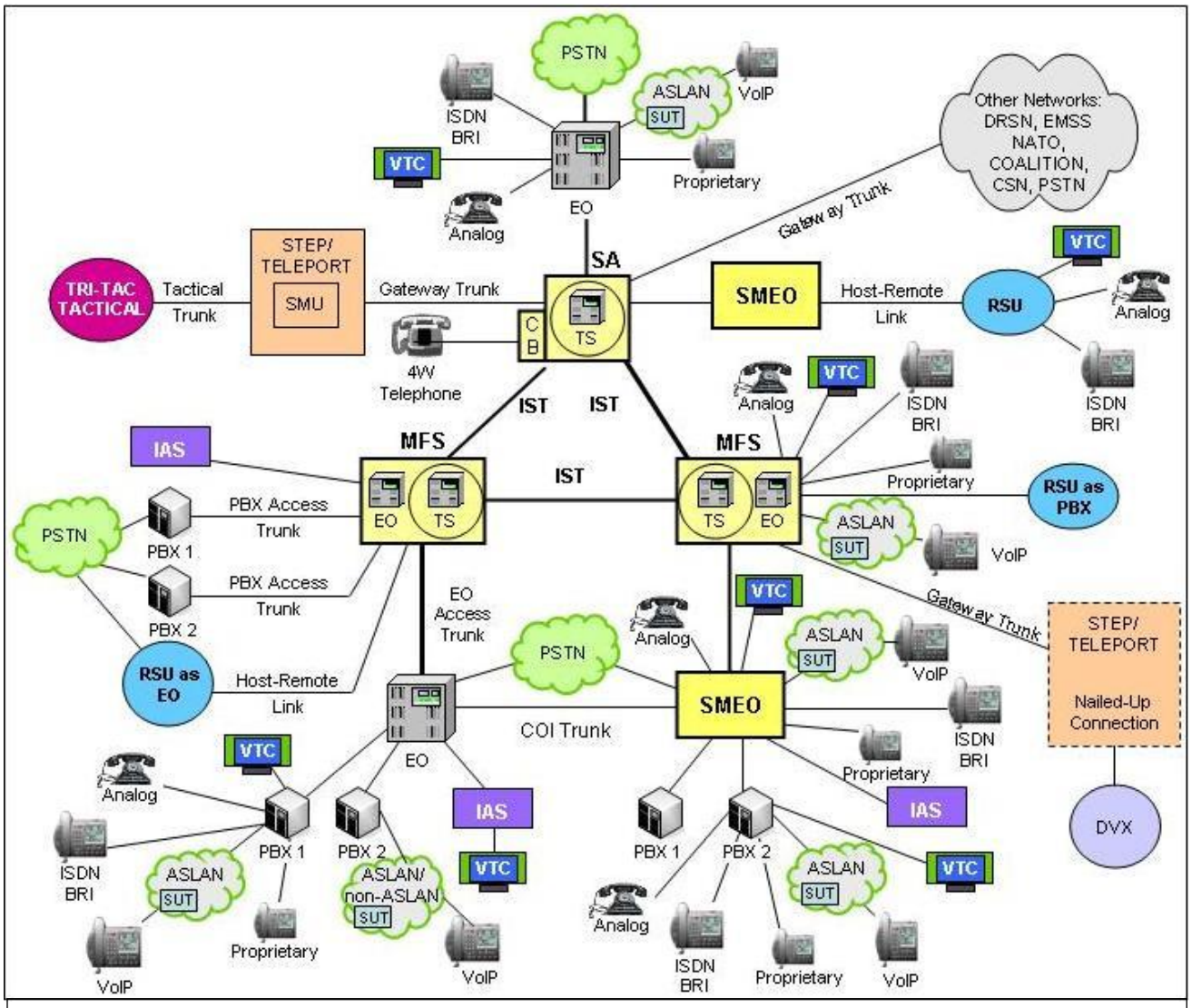
**2. PROPONENT.** Headquarters, United States Army Information Systems Engineering Command (HQ USAISEC).

**3. PROGRAM MANAGER (PM) Installation Information Infrastructure Modernization Program (I3MP), POC:** Mr. Jordan Silk, United States Army Information Systems Engineering Command, Technology Integration Center (USAISEC-TIC), Building 53302, Fort Huachuca, AZ 85613; e-mail: jordan.r.silk.civ@mail.mil.

**4. TESTER.** USAISEC-TIC, Fort Huachuca, Arizona.

**5. SYSTEM UNDER TEST DESCRIPTION.** The SUT is used to transport voice signaling and media as part of an overall Voice over Internet Protocol (VoIP) system. The SUT provides availability, security, and Quality of Service (QoS) to meet the operational requirements of the network and Assured Services for the Warfighter. The SUT is certified as a Distribution and Layer 3 (L3) Access switch and is interoperable for joint use with other Assured Services Local Area Network (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 K10 and K6 switches were the system tested.

**6. OPERATIONAL ARCHITECTURE.** The Defense Information System Network (DISN) architecture is a two-level network hierarchy consisting of DISN backbone switches and Service/Agency installation switches. Service/Agency installation switches have been authorized to extend voice services over Internet Protocol (IP) infrastructures. The Unified Capabilities Requirements (UCR) operational DISN Architecture, shown in Figure 2-1, depicts the relationship of the ASLAN and non-ASLAN to the DISN switch types.




**LEGEND:**

| | | | |
|---|---|---|---|
| 4W | 4-Wire | NATO | North Atlantic Treaty Organization |
| ASLAN | Assured Services Local Area Network | PBX | Private Branch Exchange |
| BRI | Basic Rate Interface | PBX 1 | Private Branch Exchange 1 |
| CB | Channel Bank | PBX 2 | Private Branch Exchange 2 |
| COI | Community of Interest | PC | Personal Computer |
| CSN | Canadian Switch Network | PSTN | Public Switched Telephone Network |
| DRSN | Defense Red Switch Network | RSU | Remote Switching Unit |
| DSN | Defense Switched Network | SMEO | Small End Office |
| DVX | Deployable Voice Exchange | SMU | Switched Multiplex Unit |
| EMSS | Enhanced Mobile Satellite System | STEP | Standardized Tactical Entry Point |
| EO | End Office | TDM/P | Time Division Multiplex/Packetized |
| IAS | Integrated Access Switch | Tri-Tac | Tri-Service Tactical Communications Program |
| IP | Internet Protocol | TS | Tandem Switch |
| ISDN | Integrated Services Digital Network | VoIP | Voice over Internet Protocol |
| IST | Interswitch Trunk | VTC | Video Teleconferencing |
| MFS | Multifunction Switch | SUT | System Under Test |

**Figure 2-1. DISN Architecture**

**7. REQUIRED SYSTEM INTERFACES**. The SUT's capability and functional requirements are listed in Table 2-1. These requirements are derived from the *UCR 2008, Change 2,* and have been verified by means of JITC testing and a review of the vendor's Letters of Compliance (LoC).

**Table 2-1. 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 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) | 5.3.1.3.2 |
| 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 | | 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 IAW RFC 2474. | | 5.3.1.3.5 |
| 20 | QoS Features | Shall support minimum of 4 queues. (R) | 5.3.1.3.6 |
| 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: The 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) | |
| 25 | Network Monitoring | SNMP IAW RFCs 1157, 2206, 3410, 3411, 3412, 3413, and 3414. (R) | 5.3.1.3.7 |
| 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) | |
| 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) | 5.3.1.4.1 |
| | | No more than 3 ms Jitter over any 5-minute period measured under 100% congestion. (R) | |
| | | Packet loss not to exceed 0.045% 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) | 5.3.1.4.2 |
| | | 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) | |

## Table 2-1. SUT Capability and Functional Requirements (continued)

| ID | Requirement (See note.) | | UCR Reference |
|---|---|---|---|
| 31 | E2E Performance (Data) | No more than 45 ms Latency over any 5-minute period measured under congestion. (R) | 5.3.1.4.3 |
| | | 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) | 5.3.1.6.1 |
| 33 | | Operational Controls for ASLAN and non-ASLAN. (R) | 5.3.1.6.2 |
| 34 | | Performance Monitoring for ASLAN and non-ASLAN. (R) | 5.3.1.6.3 |
| 35 | | Alarms for ASLAN and non-ASLAN. (R) | 5.3.1.6.4 |
| 36 | | Reporting for ASLAN and non-ASLAN. (R) | 5.3.1.6.5 |
| 37 | Redundancy | Redundant Power Supplies. (Required on standalone redundant products.) | 5.3.1.7.7 |
| 38 | | Chassis Failover. (Required on standalone redundant products.) | |
| 39 | | Switch Fabric Failover. (Required on standalone redundant products.) | |
| 40 | | Non-LACP Link Failover. (R) | |
| 41 | | Fiber Blade Failover. (R) | |
| 42 | | Stack Failover. (C) (Required if the stack supports more than 96 users.) | |
| 43 | | CPU (routing engine) blade Failover. (R) | |
| 44 | MPLS | MPLS may not add measurable Loss or Jitter to system. (C) | 5.3.1.8.4.1 |
| 45 | | MPLS conforms to RFCs in Table 5.3.1-14. (C) | 5.3.1.8.4.1 |
| 46 | | MPLS supports L2 and L3 VPNs. (C) | 5.3.1.8.4.2.1/2 |
| 47 | IPv6 Product Requirements: Dual Stack for IPv4 and IPv6 IAW RFC 4213 if routing functions are supported. (C) | | 5.3.5.4 |
| 48 | IPv6 System Requirements | Support IPv6 IAW RFCs 2460 and 5095 if routing functions are supported. (C) | 5.3.5.4 |
| 49 | | Support IPv6 packets over Ethernet IAW RFC 2464. (R) | 5.3.5.4 |
| 50 | | Support MTU discovery IAW RFC 1981 if routing functions are supported. (R) | 5.3.5.4.1 |
| 51 | | Support a minimum MTU of 1280 IAW RFCs 2460 and 5095. (C) | 5.3.5.4.1 |
| 52 | | Shall support IPv6 addresses IAW RFC 4291. (R) | 5.3.5.4.3 |
| 53 | | Shall support IPv6 scoped addresses IAW RFC 4007. (R) | 5.3.5.4.3 |
| 54 | | 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 | 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 and 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 |
| 56 | | 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). | |
| 57 | | IPv6 Neighbor Discovery: 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) | |
| 58 | IPv6 Neighbor Discovery | If routing functions are supported, Neighbor Discovery IAW RFCs 2461 and 4861. (C) | 5.3.5.4.5 |
| 59 | | 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) | |
| 60 | | 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) | |
| 61 | IPv6 SLAAC and Manual Address Assignment | If the system supports stateless IP address Auto-configuration, the system shall support IPv6 SLAAC for interfaces supporting UC functions IAW RFC 2462 and RFC 4862. (C) | 5.3.5.4.6 |
| 62 | | If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the function to be enabled and disabled. (C) | |
| 63 | | If the product supports IPv6 SLAAC, 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 auto-configuration. (C) | |
| 64 | | If the product supports stateless IP address auto-configurations, including those provided for the commercial market, the DAD shall be disabled IAW RFC 2462 and RFC 4862. (R) | |
| 65 | | The system shall support manual assignment of IPv6 addresses. (R) | |
| 66 | | If the system provides routing functions, the system shall default to using the “managed address configuration” flag and the “other stateful” flag set to TRUE in the router advertisements when stateful auto-configuration is implemented. (C) | |

## Table 2-1. SUT Capability and Functional Requirements (continued)

| ID | Requirement (See note.) | | UCR Reference |
|---|---|---|---|
| 67 | IPv6 ICMP | The system shall support the ICMPv6 as described in RFC 4443. (R) | 5.3.5.4.7 |
| 68 | | The system shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages. (R) | |
| 69 | | The system shall support the capability to enable or disable the ability of the system to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. (R) (Required if LS supports routing functions) | |
| 70 | | The system 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. (R) | |
| 71 | | The system shall validate ICMPv6 messages using the information contained in the payload prior to acting on them. (R) | |
| 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 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 |

**NOTE:** All requirements are for Core, Distribution, and Access Layer components unless otherwise specified.

**LEGEND:**

| | | | | | |
|---|---|---|---|---|---|
| ASLAN | Assured Services Local Area Network | HTTP | Hypertext Transfer Protocol | MTU | Maximum Transmission Unit |
| C | Conditional | HTTPS | Hypertext Transfer Protocol, Secure | OSPF | Open Shortest Path First |
| C2 | Command and Control | IA | Information Assurance | OSPFv3 | Open Shortest Path First Version 3 |
| C2(R) | Command and Control ROUTINE only | IAW | In accordance with | PHB | Per Hop Behavior |
| CPU | Central Processing Unit | ICMP | Internet Control Message Protocol | QoS | Quality of Service |
| DAD | Duplicate Address Detection | ICMPv6 | Internet Control Message Protocol for IPv6 | R | Required |
| DHCP | Dynamic Host Configuration Protocol | ID | Identification | RFC | Request for Comments |
| DHCPv6 | Dynamic Host Configuration Protocol for IPv6 | IEEE | Institute of Electrical and Electronics Engineers | SHA | Secure Hash Algorithm |
| DISR | Department of Defense Information Technology Standards Registry | IPv4 | Internet Protocol version 4 | SLAAC | Stateless Auto Address Configuration |
| DSCP | Differentiated Services Code Point | IPv6 | Internet Protocol version 6 | SNMP | Simple Network Management Protocol |
| E2E | End-to-End | LACP | Link Aggregation Control Protocol | SSH2 | Secure Shell Version 2 |
| Gbps | Gigabits per second | LAN | Local Area Network | SUT | System Under Test |
| HMAC | Hash-based Message Authentication Code | LS | LAN Switch | TCI | Tag Control Information |
| | | Mbps | Megabits per second | UC | Unified Capabilities |
| | | MPLS | Multiprotocol Label Switching | UCR | Unified Capabilities Requirements |
| | | ms | millisecond | VLAN | Virtual Local Area Network |
| | | | | VPN | Virtual Private Network |

**8. TEST NETWORK DESCRIPTION.** The SUT was tested at the USAISEC TIC, a Department of Defense (DoD) Component Test Lab, in a manner and configuration similar to those of the DISN's operational environment. A notional diagram of the SUT within an ASLAN VoIP architecture is depicted in Figure 2-2, and the notional non-ASLAN VoIP architecture is depicted in Figure 2-3. The notional ASLAN and non-ASLAN combined VoIP architecture is depicted in Figure 2-4. The ASLAN test configuration used to test the SUT in a homogeneous network is depicted in Figure 2-5, and the heterogeneous test network configuration is depicted in Figures 2-6 and 2-7.

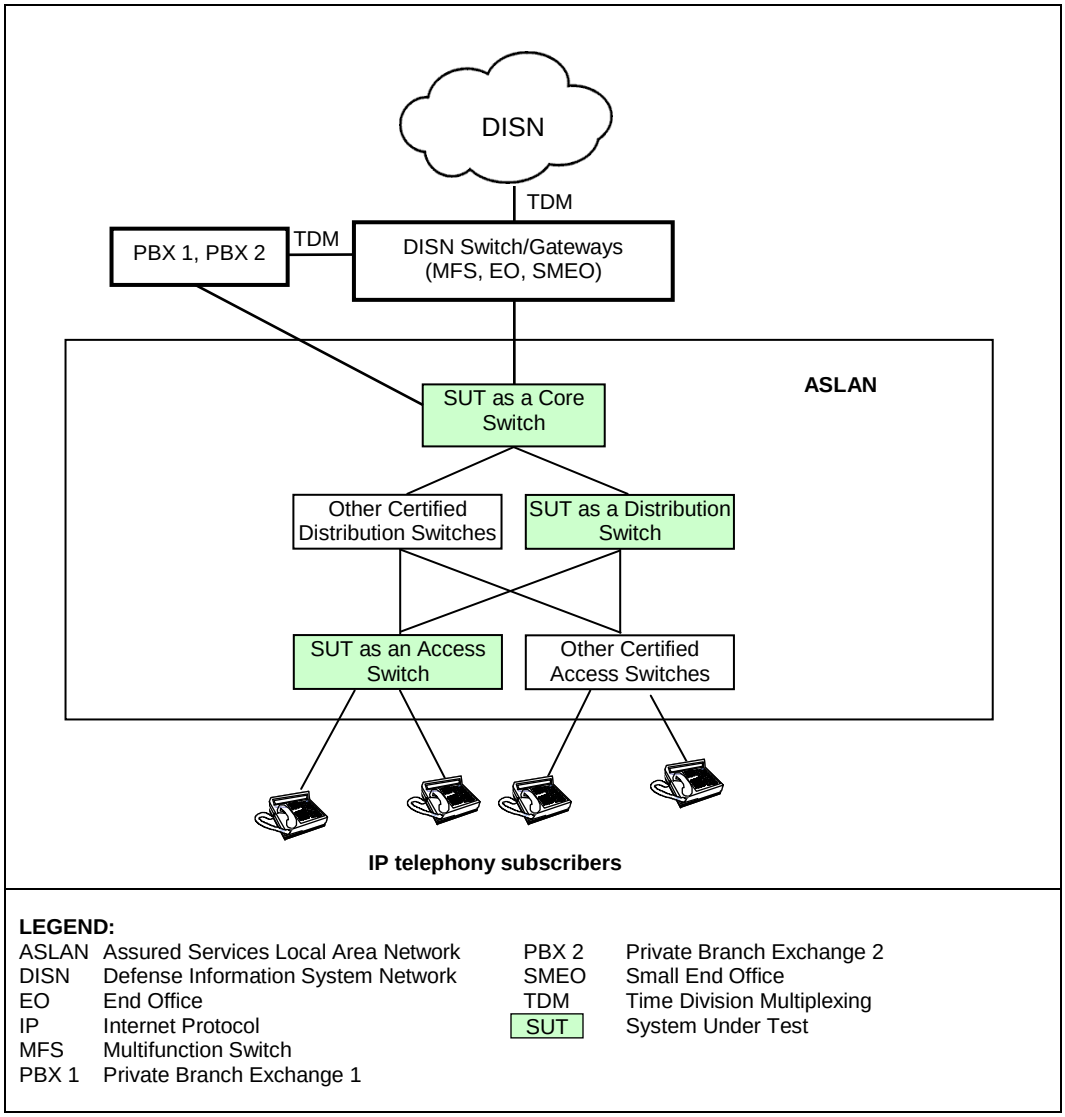
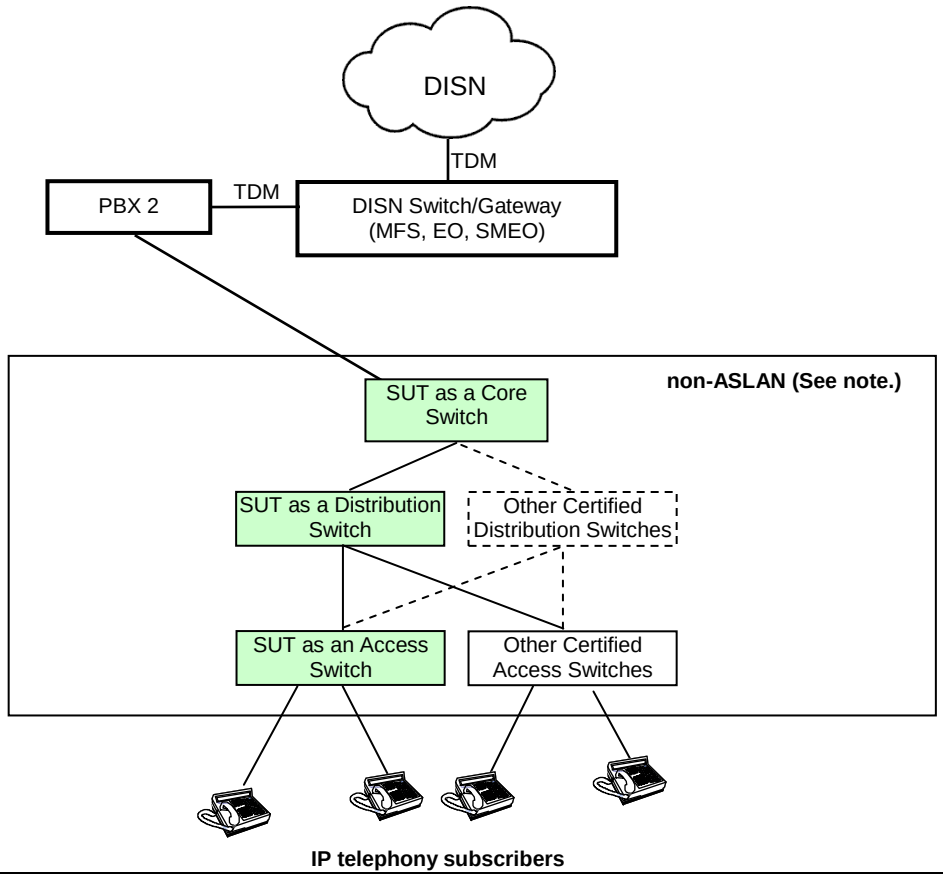



**Figure 2-2. SUT Notional ASLAN VoIP Architecture**

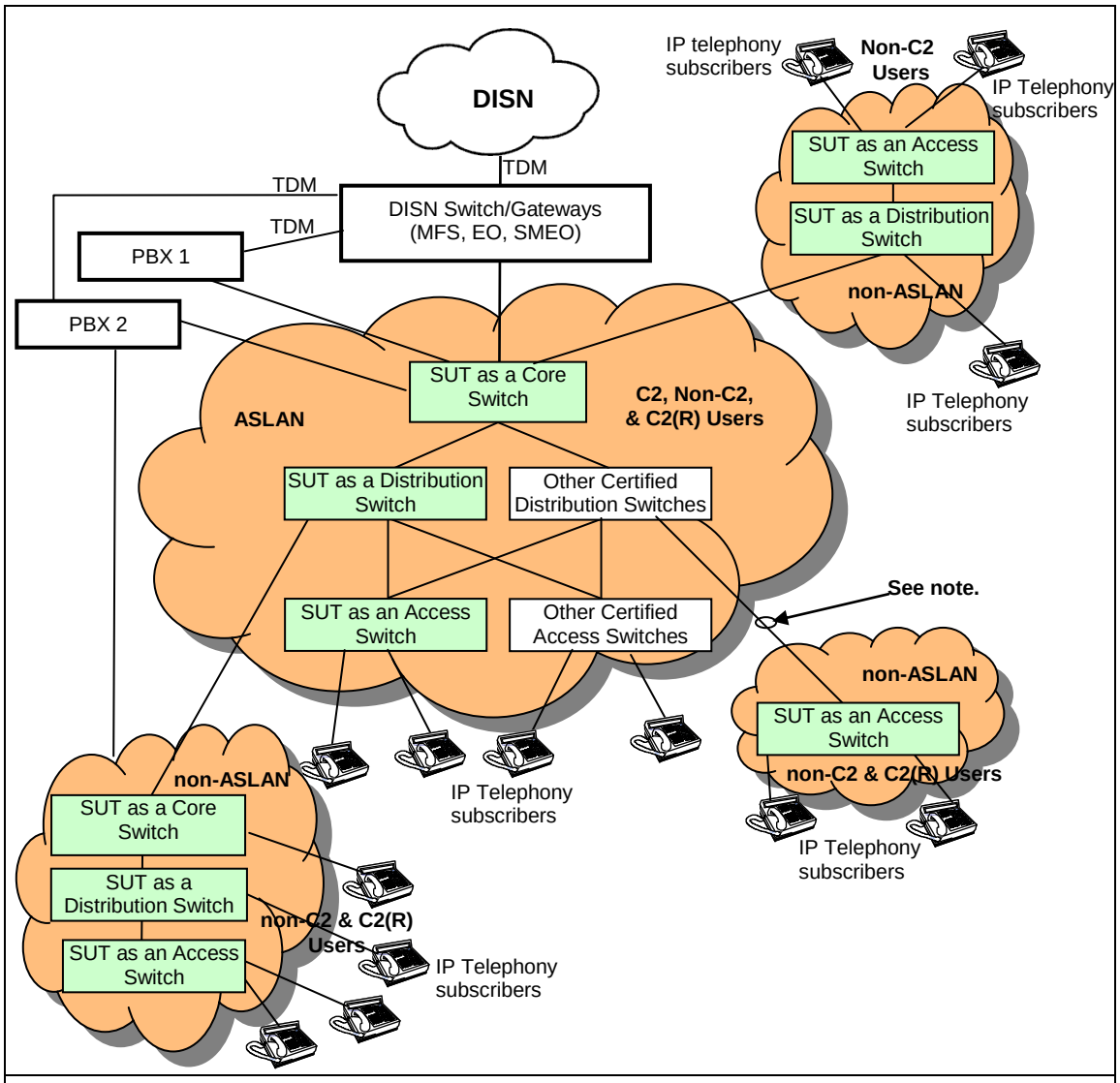



**NOTE:** Dotted lines denote optional links/components not required for a non-ASLAN. A single point of failure which could impact more than 96 telephony subscribers is permitted, and switch modularity is not required.

**LEGEND:**

| | | | |
|---|---|---|---|
| ASLAN | Assured Services Local Area Network | PBX 2 | Private Branch Exchange 2 |
| DISN | Defense Information System Network | SMEO | Small End Office |
| EO | End Office | TDM | Time Division Multiplexing |
| IP | Internet Protocol | | |
| MFS | Multifunction Switch | SUT | System Under Test |

**Figure 2-3. SUT Notional Non-ASLAN VoIP Architecture**

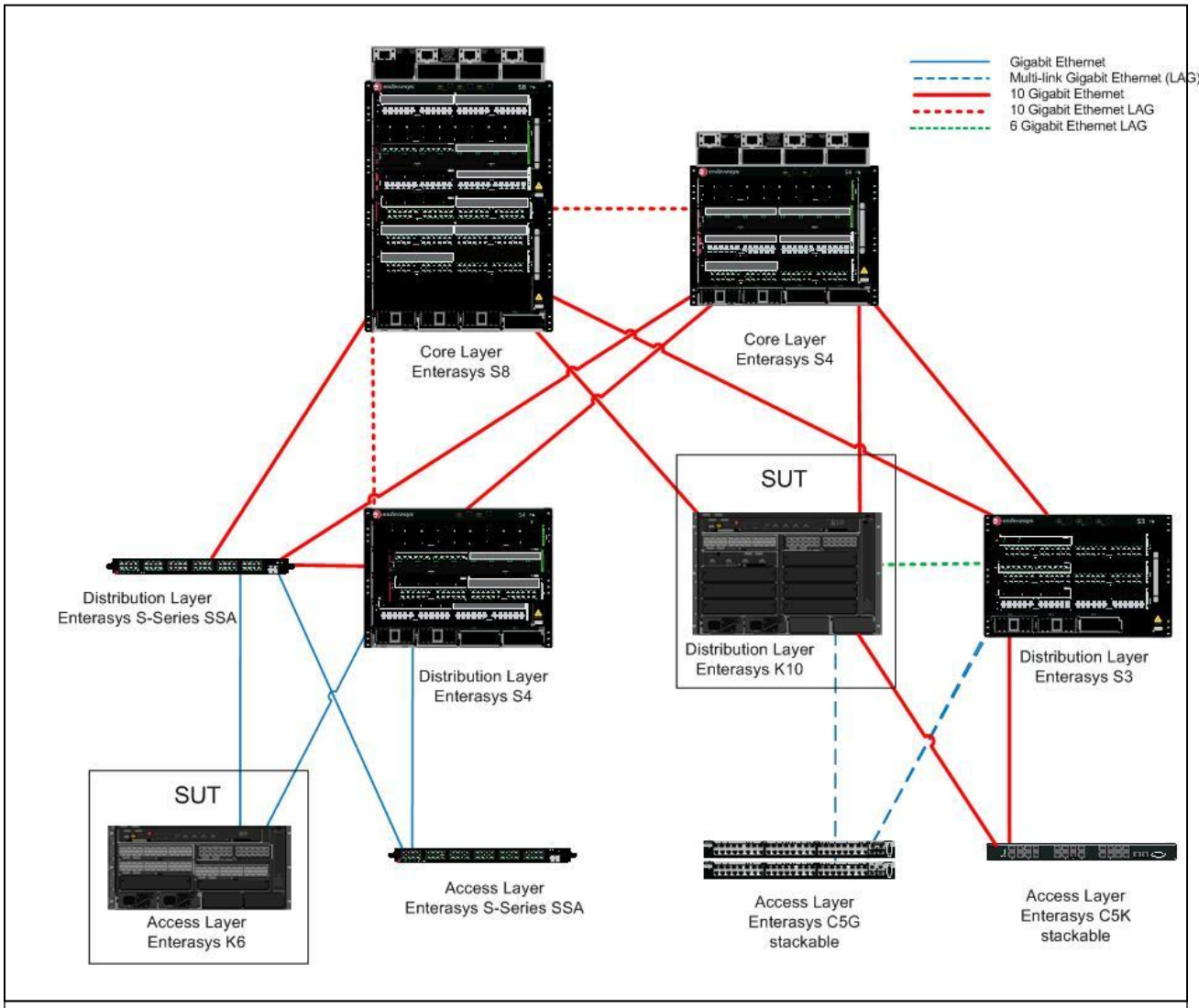



**NOTE:** A non-ASLAN switch can connect to an ASLAN switch at any layer provided that the connection does not cause the ASLAN to exceed the traffic engineering limits. A single point of failure which could impact more than 96 telephony subscribers is permitted, and switch modularity is not required.

**LEGEND:**

| | | | |
|---|---|---|---|
| ASLAN | Assured Services Local Area Network | PBX 1 | Private Branch Exchange 1 |
| C2 | Command and Control | PBX 2 | Private Branch Exchange 2 |
| C2(R) | Command and Control ROUTINE Only | SMEO | Small End Office |
| DISN | Defense Information System Network | TDM | Time Division Multiplexing |
| EO | End Office | | |
| IP | Internet Protocol | SUT | System Under Test |
| MFS | Multifunction Switch | | |

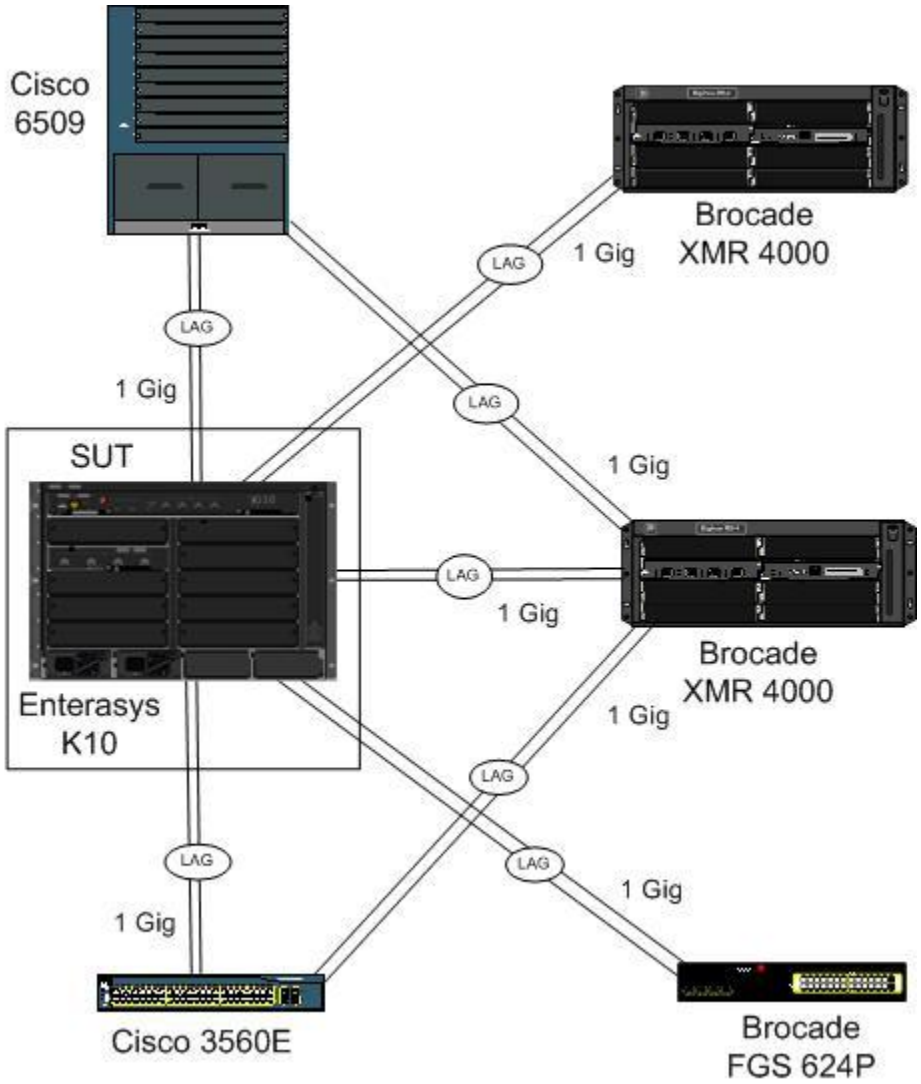
**Figure 2-4. SUT Notional ASLAN and non-ASLAN Combined VoIP Architecture**




**LEGEND:**

| | |
|---|---|
| LAG | Link Aggregation Group |
| SSA | S-series Stand Alone |
| SUT | System Under Test |

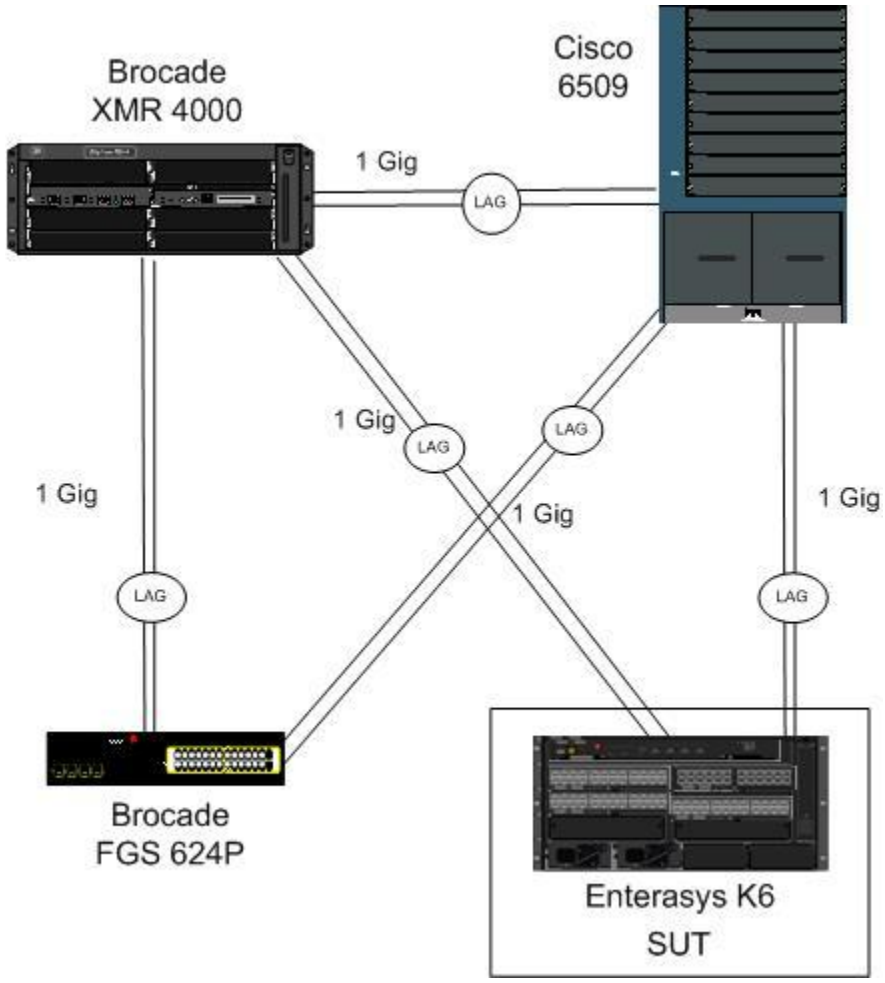
**Figure 2-5. Enterasys Homogeneous Test Configuration**




**LEGEND:**

| | |
|---|---|
| Gig | Gigabit |
| LAG | Link Aggregation Group |
| SUT | System Under Test |

**Figure 2-6. Heterogeneous Distribution Test Configuration with Brocade and Cisco**




**LEGEND:**

| | |
|---|---|
| Gig | Gigabit |
| LAG | Link Aggregation Group |
| SUT | System Under Test |

**Figure 2-7. Heterogeneous Access Test Configuration with Brocade and Cisco**

**9. SYSTEM CONFIGURATIONS**. Table 2-2 provides the system configurations, hardware, and software components tested with the SUT. The SUT is certified with other IP systems listed on the UC APL that are certified for use with an ASLAN or non-ASLAN.

**Table 2-2. Tested System Configuration**

| System Name | Release |
|---|---|
| Enterasys S8 (155/150 130 series) | 7.41.01.0013 |
| Enterasys S4 (155/150 series) | 7.41.01.0013 |
| Enterasys S4 (150 series) | 7.41.01.0013 |
| Enterasys S3 (130 series) | 7.41.01.0013 |
| Enterasys S-Series Standalone (SSA, 150/155 series) | 7.41.01.0013 |
| Enterasys SSA (130 series) | 7.41.01.0013 |
| Enterasys C5G124-xx stackable | 6.51.01.0018 |
| Enterasys C5K125/175-xx stackable | 6.51.01.0018 |
| Brocade NetIron XMR 4000 | FI 4.0.0f |
| Brocade FastIron GS 624P | FI 4.3.02a |
| Cisco 6509 | IOS 12.2(33)SXI2 |
| Cisco 3560E | IOS 12.2(46)SE |

| SUT (See note.) | Release | Function | Sub-component (See note.) | Description |
|---|---|---|---|---|
| **Enterasys K10-CHASSIS**<br>**Enterasys K6-CHASSIS** | 7.41.01.0013 | Distribution, Access L3 | **KK2008-0204-F2G** | **K10 Mgmt/Fabric with (4) 10GB via SFP+** |
| | | | **KK2008-0204-F1G** | **K6 Mgmt/Fabric with (4) 10GB via SFP+** |
| | | | **KT2006-0224-G** | **K-series 24 port 10/100/1000BaseT via RJ45 with PoE (802.3at)** |
| | | | **KG2001-0224-G** | **K-series 24 port 1000Base-X via SFP** |
| | | | **KK2008-0204-G** | **K-series 4 port 10GBASE-X via SFP+** |
| | | | KT2010-0224-G | K-Series 24 Port 10/100/1000BaseT via Mini-RJ21 with PoE |

**NOTE:** Components bolded and underlined were tested by USAISEC TIC. The other components in the family series were not tested; however, they utilize the same software and hardware, and JITC analysis determined them to be functionally identical for interoperability certification purposes. As such, they are also certified for joint use.

**LEGEND:**

| | | | |
|---|---|---|---|
| GB | Gigabyte | SFP | Small Form Factor Pluggable |
| IOS | Internetworking Operating System | SSA | S-series Stand Alone |
| JITC | Joint Interoperability Test Command | SUT | System Under Test |
| L3 | Layer 3 | USAISEC TIC | U.S. Army Information Systems Engineering Command Technology Integration Center |
| OS | Operating System | | |
| PoE | Power over Ethernet | | |

**10. TESTING LIMITATIONS.** None.

**11. TEST RESULTS.**

**a. Test Conduct.** The SUT was tested as a Distribution and L3 Access switch in both homogeneous and heterogeneous ASLAN configurations. It met all of the

requirements by means of testing and/or the vendor's LoC, as outlined in the subparagraphs below. All requirements are for Core, Distribution, and Access Layer components, unless otherwise specified.

(1) The *UCR 2008, Change 2*, paragraphs 5.3.1.2.1, 5.3.1.7.7, 5.3.1.7.7.1, and 5.3.1.7.7.2, state that ASLAN components can have no single point of failure for more than 96 users for C2 and Special C2 users. The *UCR 2008, Change 2,* paragraph 5.3.1.7.7, states the following redundancy requirements: Redundancy can be met if the product itself provides redundancy internally or if a secondary product is added to the ASLAN to provide redundancy to the primary product. Single-product redundancy may be met with a modular chassis that, at a minimum, provides the following: dual power supplies, dual processors, termination sparing, redundancy protocol, no single point of failure, and switch fabric or backplane redundancy. In the event of a component failure in the network, all calls that are active shall not be disrupted (loss of existing connection requiring redialing), and the path through the network shall be restored within five seconds. If a secondary product has been added to provide redundancy to a primary product, the failover to the secondary product must meet the same requirements. Non-ASLAN components can have a single point of failure for C2(R) and non-C2 users. The SUT supports more than 96 users and is equipped with redundant uplinks. A standard load of 100 percent of the total bandwidth was used with 50 percent each of IPv4 and IPv6 traffic. Non-Link Aggregation Control Protocol (LACP) link failover was achieved within 497 milliseconds (ms) for the K10 switch, and within 2899 ms for the K6 switch. In a heterogeneous network using Brocade switches, the maximum Non-LACP link failover time was 2010 ms or less for both SUTs. In a heterogeneous network using Cisco switches, the maximum non-LACP failover was 1648 ms or less for both SUTs. Maximum LACP failover times for the K10 switch were 1016 ms in a homogeneous network, 4127 ms in a heterogeneous network using Brocade switches, and 1397 ms in a heterogeneous network using Cisco switches. Maximum LACP failover times for the K6 switch were 352 ms in a homogeneous network, 367 ms in a heterogeneous network using Brocade switches, and 780 ms in a heterogeneous network using Cisco switches. The chassis failover times for the K10 switch were 4437 ms in a homogeneous network, 2780 ms in a heterogeneous network with Brocade switches, and 461 ms in a heterogeneous network with Cisco switches. Chassis failover for the K6 switch was not measured because it is a like device to the K10 switch.

(2) The *UCR 2008, Change 2,* paragraph 5.3.1.3 states that the ASLAN infrastructure components shall meet the requirements in the subparagraphs below. The SUT was tested using 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data; operations, administration, and maintenance (OAM); and video traffic; 20.9 percent voice traffic; and 2 percent each of network management and voice/video signaling.

(a) The Core and Distribution products shall be non-blocking for a minimum of 50 percent, and Access products shall be non-blocking for 12.5 percent

(maximum voice and video traffic) of their respective maximum rated output capacity for egress ports that interconnect (trunk) the product to other products. Non-blocking is defined as the capability to send and receive 64- to 1,518-byte packets at full duplex rates from ingress ports to egress ports without losing any packets. The SUT met this requirement for all of the test cases by ensuring that higher-priority traffic was queued above lower-priority traffic and best effort data.

(b) The SUT shall have the capability to transport prioritized voice packets (media and signaling) with jitter of no more than 1 ms across all switches. All ASLAN infrastructure components shall have the capability to transport prioritized video packets (media and signaling) with jitter of no more than 10 ms across all switches. The jitter shall be achievable over any five-minute period measured from ingress ports to egress ports under congested conditions. The SUTs met this requirement with a measured jitter of 0.02 ms or less for both voice and video packets.

(c) All Core, Distribution, and Access products shall have the capability to transport prioritized voice packets with no more than 0.015 percent packet loss. All Core, Distribution, and Access products shall have the capability to transport prioritized video and preferred data packets with no more than 0.05 percent packet loss. The packet loss shall be achievable over any five-minute period measured from ingress ports to egress ports under congested conditions. The SUTs met this requirement with a measured packet loss of 0.00 percent for all traffic types.

(d) The SUT shall have the capability to transport prioritized voice packets (media and signaling), with latency of no more than 2 ms. All ASLAN infrastructure components shall have the capability to transport prioritized video packets (media and signaling) with latency of no more than 10 ms. The latency shall be achievable over any five-minute period measured from ingress ports to egress ports under congested conditions. The SUTs met this requirement with a measured latency of 0.332 ms or less for both voice and video packets.

(3) The *UCR 2008, Change 2,* paragraph 5.3.1.3.1 states that, at a minimum, Core and Distribution products shall provide the following interface rates: 100 Mbps IAW IEEE 802.3u, and 1 Gbps IAW IEEE 802.3z. Other rates may be provided as conditional interfaces. At a minimum, Access products shall provide one of the following interface rates: 10 Mbps IAW IEEE 802.3i, 100 Mbps IAW IEEE 802.3u, or 1000 Mbps IAW IEEE 802.3ab and IEEE 802.3z. Other rates may be provided as conditional interfaces. Refer to Table 2-3 for a detailed list of the interfaces that were tested. The SUTs met these requirements.

## Table 2-3. SUT Interface Status

| Interface | Applicability | | | CRs/FRs (See note 1.) | Status | | |
|---|---|---|---|---|---|---|---|
| | Co | D | A | | Co | D | A |
| **Network Management Interfaces for Core Layer Switches** | | | | | | | |
| 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 |
| **Uplink Interfaces for Core Layer Switches** | | | | | | | |
| IEEE 802.3u (100BaseT UTP) | R | R | C[2] | 1-15, 16, 18-24, 28-31, 40, 44-53, 55-60, 65-75 | Met | Met | Met |
| IEEE 802.3u (100BaseFX) | C | C | C[2] | 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[2] | 1-16, 18-24, 28-31, 40, 44-53, 55-60, 65-75 | Met | Met | Met |
| IEEE 802.3z (1000BaseX Fiber) | R | R | C[2] | 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[2] | 1-5, 8-16, 18, 19, 40-41, 44-53, 55-60, 65-75 | Met | Met | Met |
| **Access Interfaces for Core Layer Switches** | | | | | | | |
| IEEE 802.3i (10BaseT UTP) | C | C | C[2] | 1-15, 18-24, 28-41, 44-54, 58-71 | Met | Met | Met |
| IEEE 802.3u (100BaseT UTP) | R | R | C[2] | 1-15, 18-24, 28-41, 44-54, 58-71 | Met | Met | Met |
| IEEE 802.3u (100BaseFX) | C | C | C[2] | 1-6, 11, 18-24, 28-31, 44-54, 58-71 | Met | Met | Met |
| IEEE 802.3ab (1000BaseT UTP) | C | C | C[2] | 1-15, 18-24, 28-41, 44-54, 58-71 | Met | Met | Met |
| IEEE 802.3z (1000BaseX Fiber) | R | R | C[2] | 1-6, 11, 18-24, 28-31, 44-54, 58-71 | Met | Met | Met |
| **Generic Requirements for all Interfaces** | | | | | | | |
| 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[3] | Met[3] | Met[3] |

**NOTES:**

1. The SUT's specific capability and functional requirement ID numbers listed in the CRs/FRs column can be cross-referenced in Table 2-2. These requirements apply to the following Enterasys switches which are certified in the ASLAN Distribution and Access layers: **K10**, **K6**. The devices listed in Table 2-2 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.
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.
3. Security testing is accomplished via USAISEC TIC-led Information Assurance test teams, and the results are published in a separate report, Reference (e).

**Table 2-3. SUT Interface Status**
**(continued)**

**LEGEND:**

| | | | |
|---|---|---|---|
| 802.3ab | 1000BaseT Gbps Ethernet over twisted pair at 1 Gbps (125 Mbps) | Co | Core |
| | | CR | Capability Requirement |
| 802.3ae | 10 Gbps Ethernet | D | Distribution |
| 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 | FR | Functional Requirement |
| 10BaseT | 10 Mbps (Baseband Operation, Twisted Pair) Ethernet | ID | Identification |
| | | IEEE | Institute of Electrical and Electronics Engineers |
| 100BaseT | 100 Mbps (Baseband Operation, Twisted Pair) Ethernet | IPv6 | Internet Protocol version 6 |
| | | JITC | Joint Interoperability Test Command |
| 100BaseFX | 100 Mbps Ethernet over fiber | OS | Operating System |
| 1000BaseFX | 1000 Mbps Ethernet over fiber | R | Required |
| 1000BaseT | 1000 Mbps (Baseband Operation, Twisted Pair) Ethernet | SUT | System Under Test |
| | | TIA | Telecommunications Industry Association |
| 10GBaseX | 10000 Mbps Ethernet over Category 5 Twisted Pair Copper | TIC | Technology Integration Center |
| | | UCR | Unified Capabilities Requirements |
| A | Access | USAISEC | U.S. Army Information Systems Engineering Command |
| ASLAN | Assured Services Local Area Network | UTP | Unshielded Twisted Pair |
| C | Conditional | | |

(4) The *UCR 2008, Change 2,* paragraph 5.3.1.3.2, states that the ASLAN infrastructure components shall provide the following parameters on a per port basis: auto-negotiation, force mode, flow control, filtering, link aggregation, Spanning Tree Protocol, multiple spanning tree, rapid reconfiguration of spanning tree, and port-based access control. The SUT met these requirements by means of testing and the vendor's LoC.

(5) The *UCR 2008, Change 2,* paragraph 5.3.1.3.3, states that the ASLAN infrastructure components shall support Differentiated Services Code Points (DSCP) IAW RFC 2474 as stated in the subparagraphs below.

(a) The ASLAN infrastructure components shall be capable of accepting any packet with a DSCP value between 0 and 63 on an ingress port and assigning that packet to a QoS behavior listed in Section 5.3.1.3.6. Using an IP traffic generator, the SUT prioritized the traffic described below for queuing from lowest to highest with distinct IPv4 DSCP values. The IP load included 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OAM, and video traffic; 20.9 percent voice traffic; and 2 percent each of network management and voice/video signaling. The IP traffic generator/measurement tool recorded that the SUT had properly queued higher-prioritized traffic above the lower-prioritized best effort traffic. In addition, per the vendor's LoC, the SUT is capable of assigning a DSCP value from 0-63 for each type of traffic, thus meeting the requirement.

(b) The ASLAN infrastructure components shall be capable of accepting any packet with a DSCP value between 0 and 63 on an ingress port and reassigning that packet to any new DSCP value (0-63). The current DSCP values are provided in Section 5.3.3.3.2. This requirement was met through testing and per the vendor's LoC.

(c) The ASLAN infrastructure components must be able to support the prioritization of aggregate service classes with queuing IAW Section 5.3.1.3.6. Using an IP traffic generator, the SUT prioritized the traffic described below for queuing from lowest to highest with distinct IPv6 service class values. The IP load included 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OAM, and video traffic; 20.9 percent voice traffic; and 2 percent each of network management and voice/video signaling. The IP traffic generator tool recorded that the SUT had properly queued higher-prioritized traffic above the lower-prioritized best effort traffic.

(d) The ASLAN infrastructure components may support the 3-bit user priority field of the IEEE 802.1Q 2-byte Tag Control Information (TCI) field. Default values are provided in Table 5.3.1-4. If the field is supported, the following Class of Service (CoS) requirements shall apply: The ASLAN infrastructure components shall be capable of accepting any frame with a user priority value (0-7) on an ingress port and assigning that frame to a QoS behavior listed in Section 5.3.1.3.6. The ASLAN infrastructure components shall be capable of accepting any frame with a user priority value (0-7) on an ingress port and reassigning that frame to any new user priority value (0-7). This requirement was met per the vendor's LoC.

(6) The *UCR 2008, Change 2,* paragraph 5.3.1.3.4, states that the ASLAN infrastructure components shall be capable of Virtual LAN (VLAN) capabilities IAW IEEE 802.1Q. Using the IP loader, the SUT was configured with a pre-set VLAN ID tag. The load was captured at the egress and ingress points to ensure that the SUT assigned the VLAN ID in the proper VLAN. The data was not modified or misplaced, and the assigned VLAN traffic was not lost. In addition, the SUT has the capability to assign any value from 1 through 4094 to any VLAN ID, per the vendor's LoC.

(7) The *UCR 2008, Change 2,* paragraph 5.3.1.3.5, states that the ASLAN infrastructure components shall meet the Department of Defense Information Technology Standards Registry (DISR) protocol requirements for IPv4 and IPv6. Using an IP traffic generator, the SUT prioritized the traffic described below for queuing from lowest to highest with distinct IPv4 DSCP values and IPv6 service class values. The SUT was tested using 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OAM, and video traffic; 20.9 percent voice traffic; and 2 percent each of network management and voice/video signaling. The IP traffic generator/measurement tool recorded that the SUT properly queued higher-prioritized traffic above the lower-prioritized best effort traffic. The IPv4 and IPv6 DISR RFC protocol requirements were met by the vendor's LoC.

(8) The *UCR 2008, Change 2,* paragraph 5.3.1.3.6, states that the ASLAN infrastructure components shall be capable of providing the following QoS features:

(a) Provide a minimum of four queues. The SUT has the ability to support up to eleven queues, per the vendor's LoC.

(b) Assign a DSCP or Traffic Class value to any of the queues. The SUT met this requirement through the vendor's LoC.

(c) Support Differentiated Services (DiffServ) per hop behaviors (PHBs) in accordance with RFCs 2474, 2597, 2598, 3140, and 3246. The SUT met this requirement through testing of the queuing process.

(d) Support, at a minimum, 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. The SUT supports RFCs 3662 and 1046 per the vendor's LoC.

(e) All queues shall be capable of having a bandwidth assigned. The bandwidth or traffic percentage shall be fully configurable per queue from 0 to full bandwidth or 0 to 100 percent. The sum of configured queues shall not exceed full bandwidth or 100 percent of traffic. Using an IP traffic generator, the SUT prioritized the traffic described below for queuing from lowest to highest with distinct IPv4 DSCP values and IPv6 service class values. The SUT was tested using 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OAM, and video traffic; 20.9 percent voice traffic; and 2 percent each of network management and voice/video signaling. The IP traffic generator/measurement tool recorded that the SUT had properly queued higher-prioritized traffic above the lower-prioritized best effort traffic. The IP traffic generator/measurement tool also recorded that the SUT had properly queued higher-prioritized traffic above the lower-prioritized best effort traffic at the assigned bandwidth per queue. The captured video throughput measured by the IP traffic generator/measurement tool was 23.96 percent of the line rate for the K10 switch and 24.76 percent for the K6 switch; both results are within the allowable window of 25 percent +/- 2 percent.

(9) The *UCR 2008, Change 2,* paragraph 5.3.1.3.7, states that the ASLAN infrastructure components shall be capable of providing the following Network Monitoring features:

(a) Simple Network Management Protocol (SNMP) IAW RFCs 1157, 2206, 3410, 3411, 3412, 3413, and 3414. The SUT met the requirements for all of the RFCs through the vendor's LoC with the exception of RFC 2206. RFC 2206 is Not

Applicable (NA) since the devices do not support the Resource Reservation Protocol (RSVP), and the RSVP is not a requirement for ASLANs.

(b) SNMP traps IAW RFC 1215. The SUT met this requirement through testing. The SilverCreek SNMP Test Suite was used to capture SNMP traps. For the port configuration change test, the speed of an individual port on each switch was changed from 1000 to 100 and back again for the port configuration change test.

(c) Remote Monitoring (RMON) IAW RFC 2819. The SUT met this requirement through the vendor's LoC.

(d) Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework IAW RFC 3584. The SUT met this requirement through the vendor's LoC.

(e) Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model IAW RFC 3826. Security is tested by USAISEC TIC-led IA test teams, and the results are published in a separate report, Reference (e).

(10) The *UCR 2008, Change 2*, paragraph 5.3.1.3.9, states that all switches shall meet Product Requirements IAW *UCR 2008, Change 2,* Table 5.3.1-5. The SUT met the requirements listed in Table 5.3.1-5 by means of testing and/or the vendor's LoC, as stipulated throughout this document.

(11) The *UCR 2008, Change 2,* section 5.3.1.4, states that the ASLAN infrastructure components shall be capable of meeting the End-to-End (E2E) performance requirements for voice, video, and data services. End-to-end performance across a LAN is measured from the traffic ingress point to the traffic egress point. The requirements are measured over any five-minute period under congested conditions. A "congested condition" is defined as using 100 percent of the total aggregate uplink bandwidth with 50 percent each of IPv4 and IPv6 traffic. The test included 24.9 percent each of best effort data, OAM, and video traffic; 20.9 percent voice traffic; and 2 percent each of network management and voice/video signaling. The test also included 100 percent of the link capacities as defined by baseline traffic engineering: 25 percent voice/signaling, 25 percent video, 25 percent preferred data, and 25 percent best effort traffic. The E2E requirements are ASLAN requirements. When included within an ASLAN, the SUT met all of the E2E voice, video, and data services performance requirements. Refer to paragraphs 11.b.(2)(b), 11.b.(2)(c), and 11.b.(2)(d).

(12) The *UCR 2008, Change 2,* section 5.3.1.6, states that LAN infrastructure components must meet the requirements in the subparagraphs below. Near Real Time (NRT) is defined as within five seconds of detecting the event, excluding transport time.

(a) Local area networks shall have the ability to perform remote network product configuration/reconfiguration of objects that have existing DoD Global Information Grid (GIG) management capabilities. The network management system

(NMS) shall report configuration change events in NRT, whether or not the change was authorized. The system shall report the success or failure of authorized configuration change attempts in NRT. The SUT met this requirement through testing.

(b) Local area network infrastructure components must provide metrics to the NMS to allow it to make decisions on managing the network. Network management systems shall have an automated NM capability to obtain the status of networks and associated assets in NRT 99 percent of the time (with 99.9 percent as an Objective Requirement). Specific metrics are defined in the *UCR 2008, Change 2,* sections 5.3.2.17 and 5.3.2.18. The SUT met this requirement with the vendor's LoC.

(c) Local area network components shall be capable of providing status changes in NRT 99 percent of the time (with 99.9 percent as an Objective Requirement) by means of an automated capability. An NMS will have an automated NM capability to obtain the status of networks and associated assets in NRT 99 percent of the time (with 99.9 percent as an Objective Requirement). The NMS shall collect statistics and monitor bandwidth utilization, delay, jitter, and packet loss. The SUT met this requirement with the vendor's LoC.

(d) Local area network components shall be capable of providing SNMP alarm indications to an NMS. The NMS will have the NM capability to perform automated fault management of the network, to include problem detection, fault correction, fault isolation and diagnosis, problem tracking until corrective actions are completed, and historical archiving. Alarms will be correlated to eliminate those that are duplicate or false, initiate tests, and perform diagnostics to isolate faults to a replaceable component. Alarms shall be reported as traps via SNMP in NRT. More than 99.95 percent of alarms shall be reported in NRT. The SUT met this requirement with the vendor's LoC.

(e) An NMS will have the NM capability of automatically generating and providing an integrated/correlated presentation of a network and all its associated networks. The SUT fully supports SNMP Management Information Bases (MIBs) that can be used to build visual representations of the network using an NMS.

(13) The *UCR 2008 Change 2,* paragraphs 5.3.1.3.8, 5.3.1.5, and 5.3.1.6 state that ASLAN components must meet security requirements. Security is tested by USAISEC TIC-led IA test teams, and the results are published in a separate report, Reference (e).

(14) The *UCR 2008 Change 2,* paragraph 5.3.1.7.6 states that ASLAN components must meet an availability of 99.999 percent for Special C2 users and 99.997 percent for C2 users. The SUT met this requirement with the vendor's LoC.

**b. System Interoperability Results.** The SUT is certified for Joint use within the DISN as a Distribution and Access Layer Switch. It is also certified with any digital

switching systems listed on the UC APL which are certified for use with an ASLAN or non-ASLAN.

**12. TEST AND ANALYSIS REPORT.** 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) containing the approved configuration and deployment guide must be requested directly from U.S. Government civilian or uniformed military personnel in the Unified Capabilities Certification Office (UCCO); e-mail: ucco@disa.mil.

**This page intentionally left blank**.