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

IN REPLY
REFER TO: Joint Interoperability Test Command (JTE) **24 Nov 14**

MEMORANDUM FOR DISTRIBUTION Revision 1

SUBJECT: Joint Interoperability Certification of the NetApp, Inc. FAS3220 Data ONTAP 7-Mode with Version 8.2.1

References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) DoD CIO, Memorandum, "Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)," 27 March 2012
(c) through (e), see Enclosure 1

1. **Certification Authority.** References (a) and (b) establish the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for the UC products.

2. **Conditions of Certification.** The NetApp, Inc. FAS3220 Data ONTAP 7-Mode with Version 8.2.1; hereinafter referred to as the System Under Test (SUT), meets the critical requirements of the Unified Capabilities Requirements (UCR), Reference (c), and is certified for joint use as a Data Storage Controller (DSC) with the conditions described in Table 1. The FAS3220 was the model tested; however, the models listed in Table 4 utilize the same software and similar hardware. JITC analyses determined these systems to be functionally identical to the FAS3220 and therefore, they are covered under this certification. This certification expires upon changes that affect interoperability, but no later than three years from the date of the UC Approved Products List (APL) memorandum.

Table 1. Conditions

Condition	Operational Impact	Remarks
UCR Waivers		
None.		
Conditions of Fielding		
The SUT does not support the GNS/single name space requirement. The SUT only supports in-band single name space functionality and is not certified for out-of-band global name space support.	Minor	See note 1.
Open Test Discrepancies		
The SUT does not support enabling or disabling the ability of the product to generate a Destination Unreachable message for reasons other than congestion.	Minor	See note 2.
The SUT does not support the enabling or disabling of sending an Echo Reply message in response to an Echo Request message.	None	See note 3.
The SUT does not support MLD as described in the RFC 2710.	None	See note 3.
The SUT does not support the ability to configure the product to ignore Redirect messages.	None	See note 3.

Table 1. Conditions (continued)

Condition	Operational Impact	Remarks
The SUT does not support being configured to only accept Redirect messages from the same router as is currently being used for that destination.	Minor	See note 2.
The SUT does not support Differentiated Services as described in RFC 2474 for preferred data in accordance with Section 2, Session Control Products, and Section 6, Network Infrastructure End-to-End Performance, plain text DSCP plan.	Minor	See note 2.
The SUT does not support DNS client-side Load Balancing. This requirement does not apply to the SUT because the SUT has a single DNS connection and this requirement applies to multiple DNS connections.	None	
The SUT does not support the required CoS and QoS marking on egress traffic at Layer 3 per Section 6, Network Infrastructure End-to-End Performance or the optional CoS and QoS at Layer 2.	Minor	See note 3.

NOTES:
1. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact with a condition of fielding. The SUT does not support disparate and remote network based file systems because the GNS exists within a DSC cluster which must be co-located in a campus type environment. The SUT supports only "in-band" (local) single namespace functionality. The SUT is not certified for "out-of-band" Global Namespace support.
2. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact.
3. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact. In addition, DISA stated the intent to change this requirement in the next version of the UCR.

LEGEND:

CoS	Class of Service	MLD	Multicast Listener Discovery
DISA	Defense Information Systems Agency	POA&M	Plan of Action and Milestones
DNS	Domain Name Service	QoS	Quality of Service
DSC	Data Storage Controller	RFC	Requests for Comment
DSCP	Differentiated Services Code Point	SUT	System Under Test
GNS	Global Name Service	UCR	Unified Capabilities Requirements

3. **Interoperability Status.** Table 2 provides the SUT interface interoperability status and Table 3 provides the Capability Requirements (CR) and Functional Requirements (FR) status. Table 4 provides a UC APL product summary.

Table 2. SUT Interface Status

Interface	Threshold CR/FR Requirements (See note.)	Status	Remarks
Network Attached Storage (NAS) Interfaces			
1 GbE (Ethernet) (R)	1	Met	
10 GbE (Ethernet) (R)	1	Met	
Storage Array Net (SAN) Interfaces			
Fibre Channel (FC)	1	Met	
FC Protocol (FCP)	1	Met	
Out-of-band Management Interfaces			
10 Mbps Ethernet (R)	1	Met	
100 Mbps Ethernet (R)	1	Met	
Converged Network Adapter (CNA) Interfaces			
10 GbE (Ethernet) (R)	1	Met	
100 Mbps Ethernet (R)	1	Met	

NOTE: The UCR does not identify interface CR/FR applicability. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column are cross-referenced with Table 3.

LEGEND:

CR	Capability Requirement	Mbps	Megabits per second
FR	Functional Requirement	R	Required
GbE	Gigabit Ethernet	SUT	System Under Test
ID	Identification	UCR	Unified Capabilities Requirements

Table 3. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status
1	Data Storage Controller (DSC) (R)	Section 14	Partially Met (See notes 2 and 3.)

NOTES:
1. The annotation of "required" refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3.
2. The SUT met the requirements with the exceptions noted in Table 1. DISA adjudicated these exceptions as minor.
3. Security testing is accomplished by DISA-led Information Assurance test teams and the results published in a separate report, Reference (e).

LEGEND:

CR	Capability Requirement	R	Required
DISA	Defense Information Systems Agency	SUT	System Under Test
FR	Functional Requirement	UCR	Unified Capabilities Requirements

Table 4. UC APL Product Summary

Product Identification			
Product Name	NetApp, Inc. FAS3220 Data ONTAP 7-Mode		
Software Release	Version 8.2.1		
UC Product Type(s)	Data Storage Controller		
Product Description	The SUT performs data replication, mirroring, back-up, continuance of operation, and disaster recovery functions.		
Product Components (See note 1.)	**Component Name (See note 2.)**	**Version**	**Remarks**
Primary and Secondary Data Storage Controller (x2)	FAS2220, FAS2240-2, FAS2240-4, FAS3140, V3140, FAS3160, V3160, FAS3170, V3170, FAS3210, V3210, **FAS3220**, FAS3220 w/ IOXM, V3220, V3220 w/ IOXM, FAS3240, FAS3240 w/ IOXM, V3240, V3240 w/ IOXM, FAS3250 w/ IOXM, V3250 w/ IOXM, FAS3270, FAS3270 w/ IOXM, V3270, V3270 w/ IOXM, SA320 w/ IOXM, FAS6040, V6040, FAS6080, V6080, SA600, FAS6210, V6210, FAS6220, V6220, FAS6240 w/ IOXM, V6240 w/ IOXM, FAS6250 w/ IOXM, V6250 w/ IOXM, FAS6280 w/ IOXM, V6280 w/ IOXM, FAS6290 w/ IOXM, V6290 w/ IOXM, SA620, FAS8020, FAS8040, FAS8060, CBvM100 (Edge), FSvM100 (Edge-T)	8.2.1	See notes 3 and 4.

NOTES:
1. The detailed component and subcomponent list is provided in Enclosure 3.
2. Components bolded and underlined were tested by JITC. The other components in the family series were not tested, but are also certified for joint use. JITC certifies those additional components because they utilize the same software and similar hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes.
3. Expanded I/O products have a dual enclosure and 12 PCIe expansion slots instead of a single enclosure and 4 PCIe expansion slots.
4. The FAS8020, FAS8040, FAS8060, CBvM100 (Edge), and FSvM100 (Edge-T) components are certified for joint use. See Enclosure 4 for details.

LEGEND:

APL	Approved Products List	PCIe	Peripheral Component Interconnect Express
I/O	Input/Output	SUT	System Under Test
IOXM	I/O Expansion Module	UC	Unified Capabilities
JITC	Joint Interoperability Test Command		

4. **Test Details.** This certification is based on interoperability testing, review of the vendor's Letters of Compliance (LoC), and DISA adjudication of open test discrepancy reports (TDRs) for inclusion on the UC APL. Testing was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 7 through 11 July 2014 using test procedures derived from Reference (d). Review of the vendor's LoC was completed on 8 July 2014. DISA adjudication of outstanding TDRs was completed on 18 August 2014. Information Assurance (IA) testing was conducted by DISA-led IA test teams and the results are published in a separate report, Reference (e). Enclosure 2 documents the test results and describes the tested network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements. Enclosure 4 provides a detailed JITC Revision History.

5. **Additional Information.** JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Sensitive but Unclassified IP Data (formerly known as NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at https://stp.fhu.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil. All associated information is available on the DISA UCCO website located at http://www.disa.mil/Services/Network-Services/UCCO

6. **Point of Contact (POC).** The JITC point of contact is Ms. Anita Brown, commercial telephone (520) 538-5164, DSN telephone 879-5164, FAX DSN 879-4347; e-mail address anita.l.brown53.civ@mail.mil; mailing address Joint Interoperability Test Command, ATTN: JTE (Ms. Anita Brown) P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The UCCO tracking number for the SUT is 1324201.

FOR THE COMMANDER:

4 Enclosures a/s

for RIC HARRISON
Chief
Networks/Communications and UC Portfolio

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS USD(AT&L)
ISG Secretariat, DISA, JTA
U.S. Strategic Command, J665 US
Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA(ALT), SAIS-IOQ

US Air Force, A3CNN/A6CNN
Distribution (electronic mail) (continued):
US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division US Coast Guard, CG-64
DISA/TEMC
DIA, Office of the Acquisition Executive NSG Interoperability Assessment Team
DOT&E, Netcentric Systems and Naval Warfare
Medical Health Systems, JMIS IV&V HQUSAISEC, AMSEL-IE-IS
UCCO

ADDITIONAL REFERENCES

(c) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013, Errata-1," July 2013
(d) Joint Interoperability Test Command, "Data Storage Controller (DSC) Test Procedures For Unified Capabilities Requirements (UCR) 2013," Draft
(e) Joint Interoperability Test Command, "Information Assurance Assessment Report for NetApp, Inc.FAS3220 Data ONTAP - 7-Mode 8.2.1 (Tracking Number 1324201)," Draft

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The NetApp, Inc. FAS3220 Data ONTAP 7-Mode with Version 8.2.1 is hereinafter referred to as the System Under Test (SUT). Table 2-1 depicts the SUT identifying information and requirements source.

Table 2-1. System and Requirements Identification

System Identification	
Sponsor	United States Army
Sponsor Point of Contact	Jordan Silk, jordan.r.silk.civ@mail.mil, 520-533-7218
Vendor Point of Contact	Jeremy Duncan, jduncan@tachyondynamics.com, 540-440-1193
System Name	NetApp FAS3220 Data ONTAP 7-Mode
Increment and/or Version	8.2.1
Product Category	Data Storage Controller
System Background	
Previous certifications	Not Applicable
Tracking	
UCCO ID	1324201
System Tracking Program ID	4544
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013, Errata-1
Remarks	
Test Organization(s)	Joint Interoperability Test Command, Fort Huachuca, Arizona
LEGEND:	
ID Identification	UCCO Unified Capabilities Connection Office

2. SYSTEM DESCRIPTION. A Data Storage Controller (DSC) is a specialized multiprotocol computer system with an attached disk array that serves in the role of a disk array controller and end node in Base/Post/Camp/Station (B/P/C/S) networks. The DSC is typically a Military Department (MILDEP) asset connected to the Assured Services Local Area Network (ASLAN); however, the DSC is not considered part of the ASLAN.

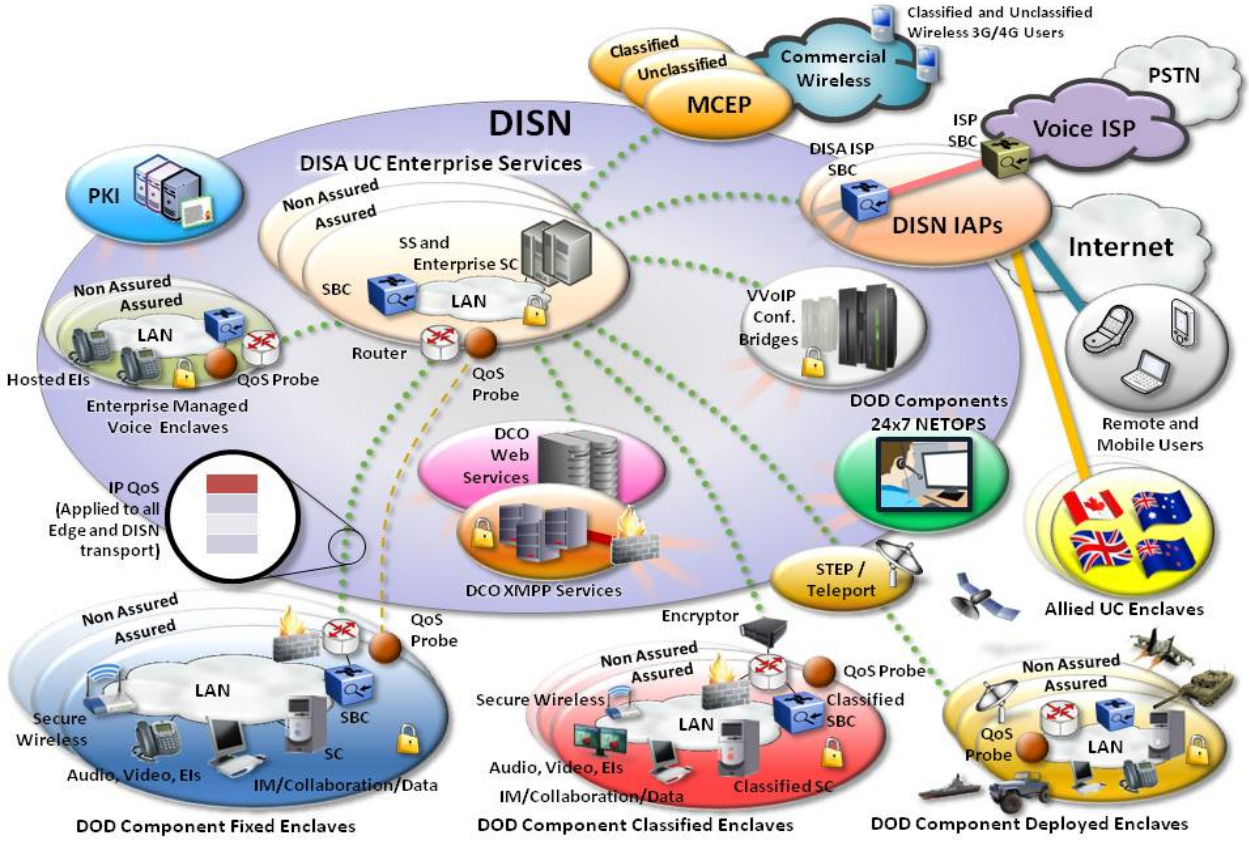
a. General Description. The SUT is a cross-platform hardware- and software-based data storage and retrieval system. The SUT responds to network requests from clients and fulfills them by writing data to or retrieving data from the disk arrays. The SUT provides a modular hardware architecture running the Data ONTAP operating system and WAFL (Write Anywhere File Layout) software. Data ONTAP is the operating system for all NetApp storage systems. The SUT provides a complete set of storage management tools through a command-line interface, through System Manager and FilerView, through the DataFabric Manager (which requires a license), and through the remote management device such as the Service Processor (SP), the Remote Local Area Network (LAN) Module (RLM), or the Baseboard Management Controller (BMC) form data storage system.

b. Management Description. The SUT is managed with a site-provided, Security Technical Implementation Guide (STIG)-compliant, Common Access Card (CAC)-enabled workstation.

3. OPERATIONAL ARCHITECTURE. The Unified Capabilities (UC) architecture is a two-level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and Service/Agency installation switches. The Department of Defense (DoD) Chief Information Officer (CIO) and Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The UC architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the notional operational UC architecture in which the SUT may be used and Figure 2-2 the DSC functional model.

4. TEST CONFIGURATION. The test team tested the SUT at JITC, Fort Huachuca, Arizona in a manner and configuration similar to that of a notional operational environment. Testing of the system's required functions and features was conducted using the test configurations depicted in Figures 2-3 and 2-4. Information Assurance testing used the same configurations. Enclosure 4 provides a list of errata changes to this certification since the original signature date.

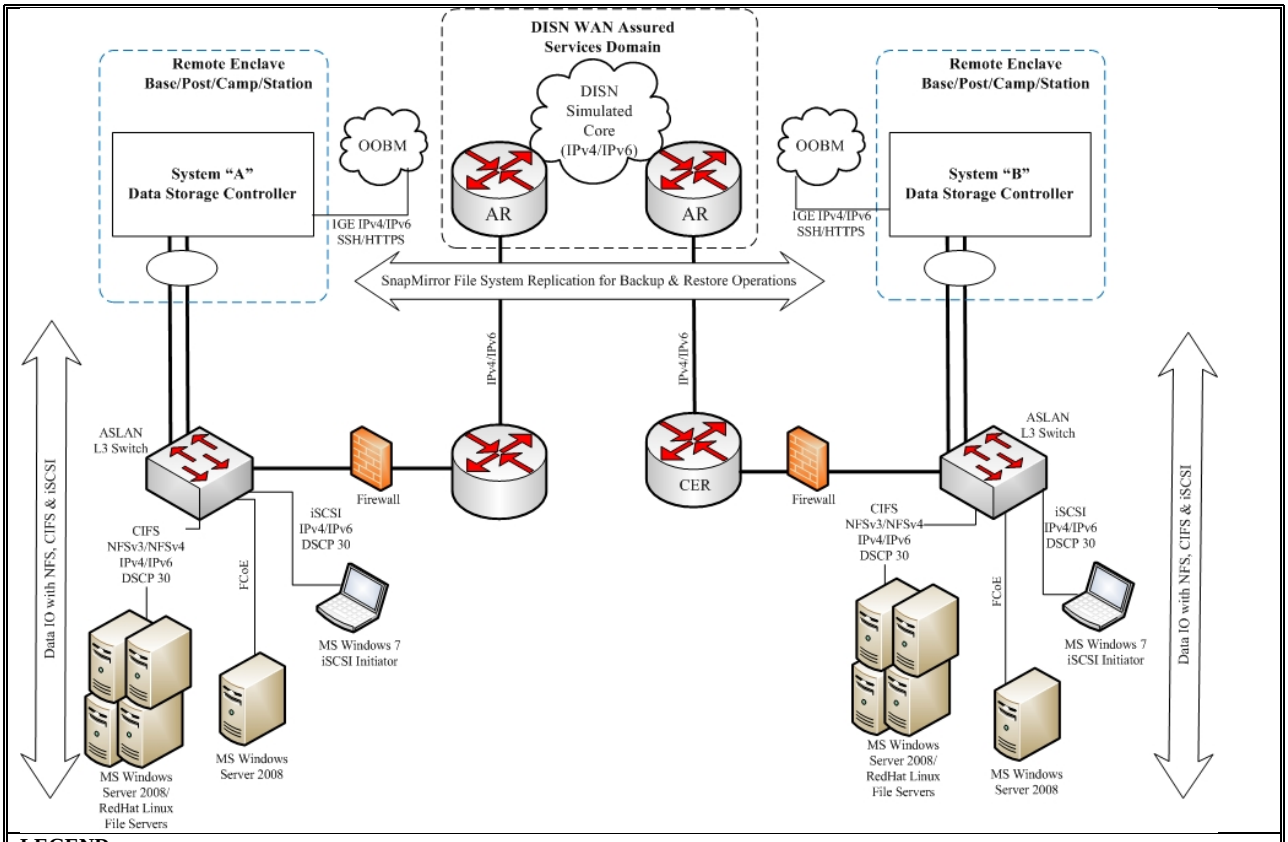
5. METHODOLOGY. Testing was conducted using DSC requirements derived from the Unified Capabilities Requirements (UCR) 2013, Reference (c), and DSC test procedures, Reference (d). Any discrepancies noted were written up in Test Discrepancy Reports (TDRs). The vendor submitted Plan of Action and Milestones (POA&M) as required. The remaining open TDRs were adjudicated by DISA as minor. Any new discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of DISA via a vendor POA&M, which will address all new critical TDRs within 120 days of identification.



LEGEND:

DCO	Defense Connection Online	NETOPS	Network Operations
DISA	Defense Information Systems Agency	PKI	Public Key Infrastructure
DISN	Defense Information Systems Network	PSTN	Public Switched Telephone Network
DoD	Department of Defense	QoS	Quality of Service
EI	End Instrument	SBC	Session Border Controller
IAP	Internet Access Point	SC	Session Controller
IM	Instant Messaging	SS	Softswitch
IP	Internet Protocol	STEP	Standardized Tactical Entry Point
ISP	Internet Service Provider	UC	Unified Capabilities
LAN	Local Area Network	VVoIP	Voice and Video over IP
MCEP	Multi Carrier Entry Point	XMPP	Extensible Messaging and Presence Protocol

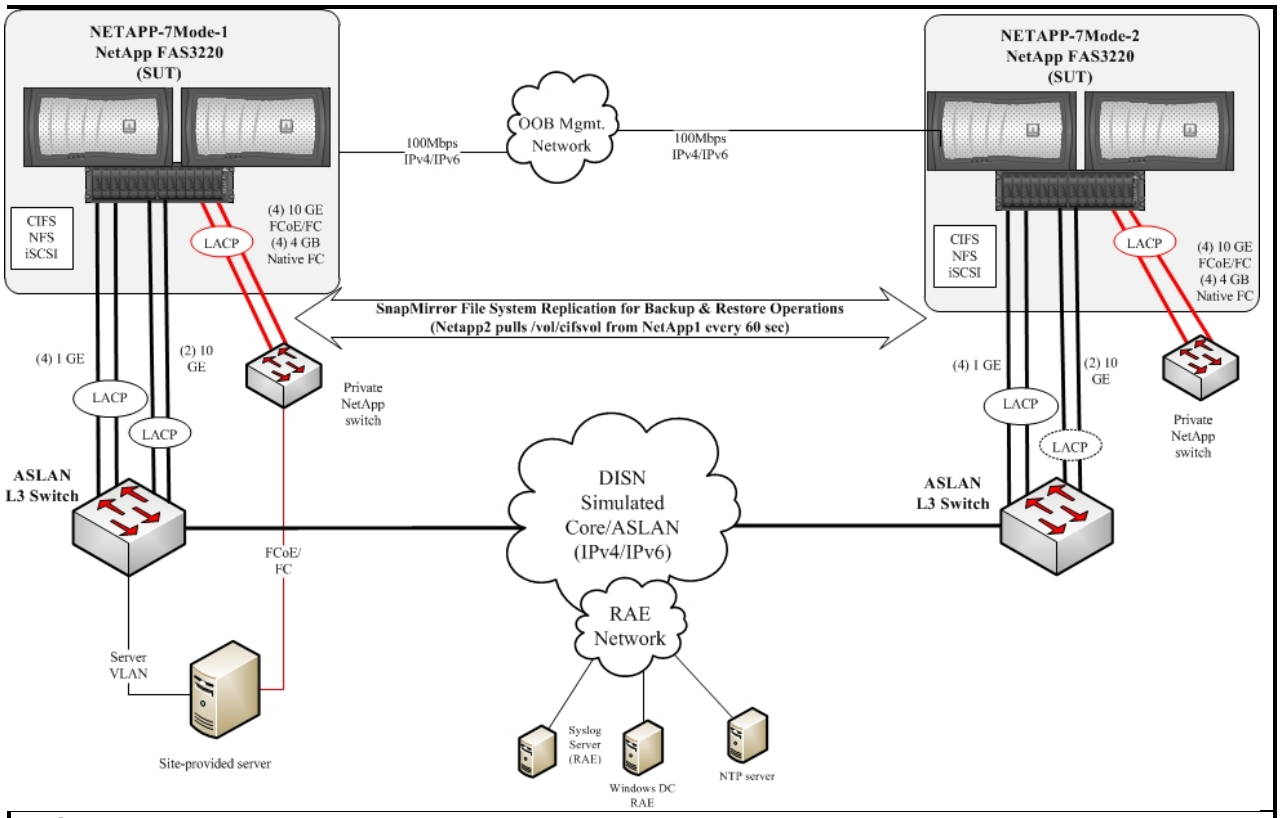
Figure 2-1. Notional UC Network Architecture



LEGEND:

AR	Aggregation Router	IPv6	Internet Protocol version 6
ASLAN	Assured Services Local Area Network	iSCSI	Internet Small Computer Systems Interface
CER	Customer Edge Router	L3	Layer 3
CIFS	Common Internet File System	MS	Microsoft
DISN	Defense Information Systems Network	NFSv3	Network File System version 3
DSCP	Differentiated Services Code Point	NFSv4	Network File System version 4
FCoE	Fibre Channel Over Ethernet	OOBM	Out of Band Management
GE	Gigabit Ethernet	SSH	Secure Shell
HTTPS	Hypertext Transfer Protocol	WAN	Wide Area Network
IPv4	Internet Protocol version 4		

Figure 2-2. Data Storage Controller Functional Reference Model



LEGEND:			
ASLAN	Assured Services Local Area Network	L3	Layer 3
CIFS	Common Internet File System	LACP	Link Aggregation Control Protocol
DC	Domain Controller	Mbps	Megabits per second
DISN	Defense Information Systems Network	Mgmt	Management
FC	Fiber Channel	NFS	Network File System
FCoE	Fiber Channel over Ethernet	NTP	Network Time Protocol
GB	Gigabyte	OOB	Out of Band
GE	Gigabit Ethernet	RAE	Required Ancillary Equipment
IPv4	Internet Protocol version 4	sec	seconds
IPv6	Internet Protocol version 6	SUT	System Under Test
iSCSI	Internet Small Computer System Interface	VLAN	Virtual Local Area Network

Figure 2-3. SUT Test Configuration

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS. The interface, Capability Requirements (CR) and Functional Requirements (FR), and other requirements for DSCs are established by UCR 2013, Errata 1, sections 14, 5, and 4.

a. Interface Status. The JITC testing interface status of the SUT is provided in Table 3-1. The DSC shall provide physical interfaces for, as a minimum, Gigiabit Ethernet (GbE) and 10 GbE in conformance with Institute of Electrical and Electronics Engineers (IEEE) 802.3 for Ethernet LAN interfaces. The SUT met the 1 GbE and 10 GbE Ethernet LAN interfaces requirements with testing. The system shall provide physical interfaces for out-of-band management (OOBM) access and services with 10/100 Megabit per second (Mbps) Ethernet interfaces as a minimum. Services shall include remote access with at least one of the following protocols: SSHv2, Secure Socket Layer (SSL), HTTPS, and SNMP version 3; and the protocols shall be secured in accordance with Section 4, Information Assurance. The SUT met this

requirement with testing. The system may optionally provide Fiber Channel (FC) physical interfaces and FC Protocol (FCP) interfaces and services as per American National Standards Institute (ANSI) X3.230, X3.297, and X3.303. The SUT met this optional requirement with the testing. The system shall provide physical interfaces for FC over Ethernet (FCoE) services over a 10GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA). The SUT met this requirement with testing.

b. Capability and Functional Requirements and Status.

(1) The UCR 2013, section 14.2 includes the Storage System requirements in the subparagraphs below.

(a) The system shall provide a Redundant Array of Independent Disks (RAID) for multiple disk drives. The system shall provide a configuration option to select the specific RAID level to be provisioned in the disk array. The RAID levels available for use shall be subject to the specific vendor implementation. At a minimum, the RAID level shall be dual parity RAID-6 for Serial Advanced Technology Attachment (SATA) drives and RAID-5 for Serial Attached Small Computer Systems Interface (SCSI) and FC drives, although stronger RAID levels are acceptable. The SUT utilizes dual parity RAID-6 drives. The SUT met this requirement with testing. Testing included removing two of the RAID drives while writing data to Common Internet File System (CIFS) share using the FCoE interface. The missing drives were displayed in the system status.

(b) The system shall be capable of 99.9 percent availability. The SUT met this requirement with the vendor's Letter of Compliance (LoC), redundant equipment including but not limited to power supplies, data storage controllers, dual parity RAID-6, and vendor product availability documentation.

(c) The system shall provide a management control function for low-level system monitoring and control functions, interface functions, and remote management. The management control function shall provide an Ethernet physical interface(s) for connection to the owner's (i.e., MILDEP) management network/LAN and also provide status. The monitoring shall include an initial system check, system cooling fans, temperatures, power supplies, voltages, and system power state tracking and logging. The SUT met this requirement with testing. Testing included a powering off one of the two power supplies. The SUT displayed the correct status and continued working. The system health status was captured prior and after the power supply was powered off.

(d) The system shall provide data storage replication (e.g., mirroring) services [Internet protocol (IP) version 4 (IPv4) and version 6 (IPv6)] between systems that are configured as source and destination replication pairs. The replication operations shall provide capabilities for data backup replication, system replication and migration, and system disaster recovery (DR) services in support of continuity of operations (COOP) planning. The SUT met this requirement with testing. Testing included data backup, replication, system replication and migration, and data recovery operations for IPv4 and IPv6.

(e) When the system interfaces to an Integrated Data Protection (IDP) service and the IDP makes copies of data storage information on to another DSC for periodic data storage backup, DR/COOP, migration, and data archiving operation, the system replication service shall complete the replication regardless of the host connection protocols used between the application servers and the DSC. The SUT met this requirement with testing. The SUT was able to copy data storage information on to another DSC and make the data available for data archiving operation and the system replication service.

(f) The system replication and migration services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for migrating data storage information. The SUT met this requirement with testing. Data storage and configuration information was replicated onto a standby DSC using regular scheduled backup operation, asynchronous replication.

(g) The system DR services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for DR/COOP. The SUT met this requirement with testing. Testing included backing up and replicating data storage and configuration information onto a standby DSC. The data on the standby DSC was accessible for DR/COOP.

(h) The system shall provide configurable modes for replication (mirroring) operations between the source DSC and the destination DSC. During replication, both the source and the destination must be in a known good state. The configurable modes shall be Asynchronous or Synchronous and are depicted in UCR 2013, Errata 1, Table 14.2-1, Replication Operation Modes. The SUT met this requirement with the Asynchronous mode only. Testing included replicating data utilizing incremental block based replication occurring once per minute and manually entering a command that triggered the replication.

(2) The UCR 2013, section 14.3 includes the Storage Protocol requirements in the subparagraphs below.

(a) The system shall provide a Network File System version 3 (NFSv3) server for file systems data input/output (I/O). The SUT met this requirement with tested using Red Hat Linux. The SUT currently does not support NFS for Windows and therefore NFS for Windows is not included in this certification.

(b) The system shall provide a NFS version 4 (NFSv4) server for file systems data I/O. This optional requirement was not tested and therefore is not included in this certification.

(c) The system shall provide a NFS version 4.1 (NFSv4.1) server, including support for parallel NFS for file systems data I/O. This optional requirement was not tested and therefore is not included in this certification.

(d) The system shall provide a CIFS version 1.0 (CIFSv1.0) server for file systems data I/O. The SUT met this requirement with testing using a Windows based client. Wireshark captures showed protocol features such as protocol version negotiation, file locking, file read/write, etc.

(e) The system shall provide a CIFS version 2.0 (CIFSv2.0) server for file systems data I/O. The SUT met this optional requirement with testing using a Windows based client. Wireshark captures showed protocol features such as protocol version negotiation, file locking, file read/write, etc.

(f) The system shall provide Internet Small Computer Systems Interface (iSCSI) server (target) operations for data I/O of Logical Units (LUNs) to clients (initiators). The SUT met this optional requirement with testing using a Windows based client. Testing included the creation of LUNs, copying data files from the client machine to one of the LUNs, editing and reading copied files.

(g) The system shall provide FCP server (target) operations for data I/O of FCP LUNs to clients (initiators). The SUT met this optional requirement with testing using a Windows based client. Testing included the creation of LUNs, copying data files from the client machine to one of the LUNs, editing and reading copied files using FCP only. All interfaces except the FCP interface were disconnected during the test.

(h) The system shall provide FCoE server (target) operations for data I/O of FCP LUNs to clients (initiators). The SUT met this optional requirement with testing using a Windows based client. Testing included the creation of LUNs, copying data files from the client machine to one of the LUNs, editing and reading copied files using FCoE only. All interfaces except the FCoE interface were disconnected during the test.

(i) The system shall provide a HTTPS server for file system data I/O and management access to the storage controller operating system. The session shall be secured with SSL or Transport Layer Security (TLS), per Internet Engineering Task Force (IETF) Request for Comment (RFC) 5246, and shall comply with Section 4, Information Assurance, for that protocol. Although the SUT supports HTTPS server file system Input/Output, this optional requirement was not tested and therefore is not included in this certification.

(j) The system shall provide SSHv2 or SSL for management access to the storage controller operating system. The SSHv2 or SSL implementation shall comply with Section 4, Information Assurance, for that protocol. The SUT met this requirement with testing. SSHv2 was used to management access to the storage controller operating system.

(k) The system shall provide Web-based Distributed Authoring and Versioning (WebDAV), per IETF RFC 4918, in support of Cloud-based virtualized storage infrastructures. The SUT does not support this optional requirement.

(l) The system shall implement the Representational State Transfer (REST) software architecture for distributed hypermedia systems and Cloud-based virtualized storage infrastructures. The SUT does not support this optional requirement.

(m) The system shall implement the Storage Networking Industry Association (SNIA) Cloud Data Management Interface (CDMI) standard. The SUT does not support this optional requirement.

(n) The system shall provide Global Name Space (GNS) or single name space functionality. The GNS functionality shall provide the capability to aggregate disparate and remote network-based file systems to provide a consolidated view to reduce complexities of localized file management and administration. The GNS functionality shall provide large (i.e., 14 Petabyte [PB] or greater) working pools of disks, transparent data migration, and it shall serve to reduce the number of storage mount points and shares. Each system shall have a dedicated and unique GNS. The SUT does not support this requirement. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact with a condition of fielding. The SUT does not support disparate and remote network based file systems because the GNS exists within a DSC cluster which must be co-located in a campus type environment. The SUT supports only "in-band" (local) single namespace functionality. The SUT is not certified for "out-of-band" Global Namespace support.

(3) The UCR 2013, section 14.4 includes the Network Attached Storage Interface requirements in the subparagraphs below.

(a) The system shall provide physical interfaces for Gigabit Ethernet (GbE) and 10 Gigabit Ethernet (10 GbE) services in conformance with Institute of Electrical and Electronics Engineers (IEEE) 802.3 for Ethernet LAN interfaces. The SUT met this requirement with testing. The 1 GbE and 10 GbE interfaces were used throughout the test. Wireshark captures showed no anomalies.

(b) The system shall be able to provision, monitor, and detect faults, and to restore Ethernet services in an automated fashion. The SUT met this requirement with the vendor's LoC, system logs, and system monitoring tool.

(c) The system shall provide physical interfaces for out-of-band management (OOBM) access and services with 10/100 Mbps Ethernet interfaces as a minimum. Services shall include remote access with at least one of the following protocols: SSHv2, SSL, HTTPS, and SNMPv3; and the protocols shall be secured in accordance with Section 4, Information Assurance (IA). The SUT met this requirement with testing the remote access using SSHv2. IA testing is accomplished by a DISA-led IA test team and the results published in a separate report, Reference (e).

(d) When the system uses Ethernet, Fast Ethernet, GbE, and 10GbE interfaces, the interfaces shall be autosensing, auto-detecting, and auto-configuring with incoming and corresponding Ethernet link negotiation signals. Autosensing, auto-detecting, and auto-configuring only applies to interfaces below 10GbE interfaces. The SUT met this requirement with testing for all interfaces below10GbE. Testing included changing the data rate and switching between full and duplex.

(e) Ethernet services of the system and the Logical Link Interworking Function (IWF) of the system shall terminate the Media Access Control (MAC) layer of Ethernet as described in Ethernet Standard IEEE 802.3. The SUT met this requirement with testing. No anomalies were identified in the Wireshark data captured during testing.

(f) Ethernet services of the system shall support jumbo frames with a configurable Maximum Transmission Unit (MTU) of 9000 bytes or greater, excluding Ethernet encapsulation. When Ethernet encapsulation is included in the frame size calculation, an additional 22 bytes must be included for the MAC header (14 bytes), the Virtual LAN (VLAN) tag (4 bytes), and the Cyclical Redundancy Check (CRC) Checksum (4 bytes) fields in the Ethernet frame, resulting in a maximum of 9022 bytes or greater. The system shall also support a configurable MTU between 1280 bytes and 1540 bytes to ensure packets can transit type 1 encryptors. The system default MTU shall be 1540 bytes. The SUT met this requirement with the vendor LoC.

(g) Ethernet services of the system shall allocate a unique Ethernet MAC address to each Ethernet interface associated with a VLAN, as per IEEE 802.1Q. The SUT met this requirement with testing which included assigning unique Ethernet MAC address to Ethernet interface associated with a VLAN.

(h) Ethernet services of the system shall support "Link Aggregation," as per IEEE 802.3ad or IEEE 802.1AX-2008, and use with the Link Aggregation Control Protocol. The SUT met this requirement with the vendor LoC and using LACP for the 10 Gb interfaces used during the test.

(i) Ethernet services of the system shall provide Link Layer Discovery Protocol (LLDP), as per IEEE 802.1AB. The SUT does not support this optional requirement.

(4) The UCR 2013, section 14.5, states the system shall provide Fibre Channel (FC) physical interfaces and FCP interfaces and services as per American National Standards Institute (ANSI) X3.230, X3.297, and X3.303. The SUT met this requirement with the vendor's LoC and testing.

(5) The UCR 2013, section 14.6 includes the Converged Network Adapter Interface requirements in the subparagraphs below.

(a) The system shall provide physical interfaces for FCoE services over a 10GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA). The SUT met this requirement with the vendor's LoC and testing. Test included copying files from one DSC to another using the 10GbE FCoE interfaces.

(b) The system shall provide physical interfaces for Data Center Bridging [DCB, also known as Converged Enhanced Ethernet (CEE)] features, and functionality, per the standards depicted in Table 14.6-1, Physical Interfaces for Data Center Bridging. Although the SUT supports the DCB requirement, this optional requirement was not tested and therefore is not included in this certification.

(6) The UCR 2013, section 14.7 includes the IP Networking requirements in the subparagraphs below.

(a) The system shall meet the IPv6 requirements defined in Section 5.2.2, Mapping of RFCs to UC Profile Categories, for a simple server/network appliance. The SUT met the critical IPv6 requirements with the vendor's LoC with the exceptions listed in the subparagraphs below.

1. The SUT does not support the capability to enable or disable the ability of the product to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact.

2. The SUT does not 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. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact. In addition, DISA stated the intent to change this requirement in the next version of the UCR.

3. The SUT does not support Multicast Listener Discovery (MLD) as described in RFC 2710. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact. In addition, DISA stated the intent to change this requirement in the next version of the UCR.

4. The SUT does not support the ability to configure the product to ignore Redirect messages. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact. In addition, DISA stated the intent to change this requirement in the next version of the UCR.

5. The SUT does not support being configured to only accept Redirect messages from the same router as is currently being used for that destination. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact.

(b) The system shall provide statically provisioned or dynamically adjusted large IP packet receive buffers for replication (mirroring) session traffic received on the Ethernet physical interfaces. The receive buffers may be statically provisioned or the operating system of the system may dynamically self-adjust the packet receive buffer size based on measurements of the E2E path bandwidth, Maximum Segment Size (MSS), Round Trip Time (RTT), and the percentage of packet loss. The system shall provide a default and minimum IP packet receive buffer size of 2048 KB per replication (mirroring) session. The system shall provide a statically provisioned or dynamically adjusting maximum IP packet receive buffer size of up to 8192 KB per replication (mirroring) session. The SUT met this requirement with the vendor's LoC and

testing. Receive buffer were successfully provisioned to the required minimum and maximum IP packet receive buffer size. The receive buffer size was verified using Wireshark data captures.

(c) The system shall provide an optimized congestion control (congestion avoidance) algorithm in Transmission Control Protocol (TCP) for avoidance of traffic loss on communications paths in high-speed networks with high latency or large bandwidth-delay products. The SUT met this requirement with the vendor's LoC.

(7) The UCR 2013, section 14.8 includes the Name Services requirements in the subparagraphs below.

(a) The system shall provide Lightweight Directory Access Protocol (LDAP) directory services per IETF RFC 4510. The SUT met this requirement with the vendor's LoC.

(b) The system shall provide Kerberos authentication service per IETF RFC 4120. The SUT does not support this requirement. The SUT met this requirement with the vendor's LoC.

(c) The system shall provide Domain Name System (DNS) client functionality. The SUT met this requirement with testing. The functionality was verified by finding a host name when entering an IP address and finding an IP address when entering a host name.

(d) The system shall provide DNS client-side Load Balancing. The SUT does not support this requirement. This requirement does not apply to the SUT because the SUT has a single DNS connection and this requirement applies to multiple DNS connections.

(e) The system shall provide Network Information Service (NIS) client directory service functionality. Although the SUT supports the NIS requirement, this optional requirement was not tested because a NIS server was not available and therefore is not included in this certification. There is no operational impact of not testing NIS. The SUT uses DNS and Cisco's native discovery protocol for client-server directory services.

(f) The system shall provide NIS Netgroups client directory service functionality. This requirement is not applicable. Although the SUT supports the NIS server, this requirement was not tested because a NIS server was not available and therefore is not included in this certification. There is no operational impact of not testing NIS. The SUT provides DNS and Cisco's native discovery protocol for client-server directory services.

(g) The system shall provide Network Basic Input/Output System (NETBIOS) over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS). The SUT does not support this optional requirement. Although the SUT supports WINS, this optional requirement was not tested because a WINS server was not available and therefore is not included in this certification. There is no operational impact since the SUT provides DNS functionality. DNS has replaced WINS since Microsoft made changes to NetBIOS, allowing it to use the TCP/IP stack to perform its job (NetBIOS over TCP/IP) and most DNS servers are able to handle NetBIOS requests.

(h) The system shall provide Internet Storage Name Service (iSNS) client functionality per IETF RFC 4171. Although the SUT supports iSNS client functionality, this requirement was not tested because an iSNS server was not available for test and therefore is not included in this certification. There is no operational impact since the SUT was able to provide discovery, management and configuration of iSCSI and Fibre Channel devices on the TCP/IP network without the use of an iSNS server.

(i) If the system has a FC interface then the system shall provide FC Name and Zone Service. The SUT met this conditional requirement with testing. Testing included creating a zone with several members in one Virtual Storage Area Network (VSAN) allowing those members belonging to that zone to communicate. Next, a new zone was created within the same VSAN and a couple of members were moved from the original zone to the new zone. The members moved to the new zone were no longer able to communicate with the member in the original zone. In addition, access control for different VSAN was also verified. Members in one VSAN were not able to communicate with members in another VSAN.

(8) The UCR 2013, section 14.9 includes the Security Services requirements in the subparagraphs below.

(a) The system shall provide IPSec per RFC 4301. The SUT does not support this optional requirement and therefore is not included in this certification.

(b) The system shall provide Encapsulating Security Payload (ESP) per RFC 4303. The SUT does not support this optional requirement and therefore is not included in this certification.

(c) The system shall provide Internet Key Exchange version 2 (IKEv2) per RFC 4306. The SUT does not support this optional requirement and therefore is not included in this certification.

(d) The system shall provide a configurable Packet Filter (Firewall) service to block unauthorized access (for intrusion prevention) while permitting authorized communications. The Packet Filter service shall use a “stateless” design that does not degrade performance and shall filter all packets received based on interface, source IP address, protocol, port, Type of Service (TOS), or Time To Live (TTL). The Packet Filter service shall provide a configuration policy for defining combinations of multiple packet match rules and processing actions. The SUT does not support this optional requirement and therefore is not included in this certification.

(e) The system shall provide encryption of data at rest at a minimum of AES-256 in accordance with Federal Information Processing Standard (FIPS) 140-2 level 1 or higher to provide the following capabilities:

1. Rapid crypto-shredding (destruction) of data, in accordance with National Institute of Standards and Technology (NIST) 800-88, for tactical systems that operate in harm's way and may fall into enemy hands. The met this requirement with the vendor's LoC.

2. Rapid recovery from sensitive data spills, where the wrong data is accidentally written to the wrong place. The SUT met this requirement with the vendor's LoC.

(f) The system shall comply with all appropriate STIGs to include the Database Security Technical Implementation Guide. Security testing is accomplished by a DISA-led IA test team and the results published in a separate report, Reference (e).

(9) The UCR 2013, section 14.10, states the system shall provide an Application Programming Interface (API) to enable interaction with other software and systems. The interactions shall include routines, data structures, object classes, and protocols used to communicate between the consumer and implementer of the API. The API protocol and message format (e.g., Extensible Markup Language [XML]) shall be subject to the specific vendor system operating system implementation. The SUT met this requirement with the vendor's LoC.

(10) The UCR 2013, section 14.11 includes the Class of Service and Quality of Service requirements in the subparagraphs below.

(a) The system shall provide Class of Service (CoS) and Quality of Service (QoS) marking on egress traffic at layer 2 per IEEE 802.1p and, Section 7.2.1.3, Class of Service Markings, and Section 7.2.1.4, Virtual LAN Capabilities. Traffic classification and marking must occur before the egress transmission of the Ethernet frame with a rule or policy engine that matches on various storage and management protocol types as offered by the system. The SUT does not support this optional requirement and therefore is not included in this certification.

(b) The system shall provide CoS and QoS marking on egress traffic at layer 3 per Section 6, Network Infrastructure End-to-End Performance. Traffic classification and marking must occur before the egress transmission of the IP packet with a rule or policy engine that matches on various storage and management protocols that occur within the system, such as those listed in Table 14.11-1. The IP packets are marked in the TOS field of the IPv6 packet header with Differentiated Services Code Point (DSCP) values from 0 and 63, inclusive. These are to be used in the ASLAN, non-ASLAN, and extended networks for per-hop CoS and QoS traffic conditioning by the network elements. The SUT does not support this requirement. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact. In addition, DISA stated the intent to change this requirement in the next version of the UCR.

(11) The UCR 2013, section 14.12 includes the Virtualization requirements in the subparagraphs below. The SUT does not support the optional vDSC capabilities. Therefore, the requirements in the following subparagraphs do not apply and therefore are not included in this certification. There is no impact of the SUT not supporting this optional requirement.

(a) The system shall provide virtualized Data Storage Controller (vDSC) functionality and individual protocol server processes. The vDSC shall meet all the requirements of a DSC with minor exceptions that are related to design and technical limitations associated with the complete virtualization of an operating system, which include internal counters for attributes of the physical system, QoS traffic processing, and per vDSC Mobile IP correspondent node binding cache limitations.

(b) The vDSC capability within the system shall provide secure, Private Networking Domains (PNDs) for Ethernet, VLANs, and IP that isolate the network domains of system units. The PND shall support the use of duplicate IP addresses and IP subnet address ranges among those of any other configured vDSC in the system. The PND shall provide a dedicated IP Forwarding Information Base (FIB) per vDSC.

(c) The vDSC shall provide an individual Command Line Interface (CLI) context with the full command set of the system, with the scope of the commands limited to the individual vDSC CLI context.

(d) The vDSC shall provide a programmatic API with the full command set of the system with the scope of the API commands limited to the individual vDSC context.

(e) The vDSC capability within the system shall provide an individual GNS unique from the system or shall provide a single name space that provides the capability to aggregate disparate hardware and storage architectures into a single file system. The GNS shall provide the capability to aggregate disparate and remote network-based file systems, providing a consolidated view to reduce complexities of localized file management and administration. The GNS shall provide large working pools of disks and transparent data migration, and shall serve to reduce the number of storage mount points and shares. The single name space shall be spread across multiple physical network access server heads all representing the same file system without replication. The single name space shall include the ability to tier data automatically within the same file system.

c. Hardware/Software/Firmware Version Identification. Table 3-3 provides the SUT components' hardware, software, and firmware tested. The JITC tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

7. TESTING LIMITATIONS. JITC test teams noted the following testing limitations including the impact they may have on the interpretation of the results and conclusions:

a. Although the SUT supports the NIS requirement, this optional requirement was not tested because a NIS server was not available and therefore is not included in this certification. There is no operational impact of not testing NIS. The SUT uses DNS and Cisco's version of LDAP for client-server directory services.

b. Although the SUT supports the NIS server, this requirement was not tested because a NIS server was not available and therefore is not included in this certification. There is no operational impact of not testing NIS. The SUT provides DNS and Cisco's version of LDAP for client-server directory services.

c. Although the SUT supports WINS, this optional requirement was not tested because a WINS server was not available and therefore is not included in this certification. There is no operational impact since the SUT provides DNS functionality. DNS has replaced WINS since Microsoft made changes to NetBIOS, allowing it to use the TCP/IP stack to perform its job (NetBIOS over TCP/IP) and most DNS servers are able to handle NetBIOS requests.

d. Although the SUT supports iSNS client functionality, this requirement was not tested because an iSNS server was not available and therefore is not included in this certification. There is no operational impact since the SUT was able to provide discovery, management and configuration of iSCSI and Fibre Channel devices on the TCP/IP network without the use of an iSNS server.

8. CONCLUSION(S). The SUT meets the critical interoperability requirements for a Data Storage Controller in accordance with the UCR and is certified for joint use with other UC Products listed on the Approved Products List (APL). The SUT meets the interoperability requirements for the interfaces listed in Table 3-1.

DATA TABLES

Table 3-1. SUT Interface Status

Interface	Threshold CR/FR Requirements (See note.)	Status	Remarks
Network Attached Storage (NAS) Interfaces			
1 GbE (Ethernet) (R)	1	Met	
10 GbE (Ethernet) (R)	1	Met	
Storage Array Net (SAN) Interfaces			
Fibre Channel (FC)	1	Met	
FC Protocol (FCP)	1	Met	
Out-of-band Management Interfaces			
10 Mbps Ethernet (R)	1	Met	
100 Mbps Ethernet (R)	1	Met	
Converged Network Adapter (CNA) Interfaces			
10 GbE (Ethernet) (R)	1	Met	
100 Mbps Ethernet (R)	1	Met	

NOTE: The UCR does not identify interface CR/FR applicability. The SUT high-level CR and FR ID numbers depicted in the Threshold CRs/FRs column are cross-referenced with Table 3-2.

LEGEND:

CR	Capability Requirement	Mbps	Megabits per second
FR	Functional Requirement	R	Required
GbE	Gigabit Ethernet	SUT	System Under Test
ID	Identification	UCR	Unified Capabilities Requirements

Table 3-2. Capability and Functional Requirements and Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status
1	Data Storage Controller (DSC) (R)		
	Storage System (R)	14.2	Met (See note 2.)
	Storage Protocol (R)	14.3	Partially Met (See notes 3 - 6.)
	Network Attached Storage Interface (R)	14.4	Met (See note 7.)
	Storage Array Network Interface (O)	14.5	Met
	Converged Network Adapter Interface (O)	14.6	Met (See note 8.)
	IP Networking (R)	14.7	Partially Met (See notes 9 - 14.)
	Name Services (R)	14.8	Met (See notes 15 - 18.)
	Security Services (R)	14.9	Met (See notes 19 - 22.)
	Interoperability (R)	14.10	Met
	Class of Service and Quality of Service (R)	14.11	Not Met (See note 23.)
	Virtualization (O)	14.12	Not Tested (See note 24.)

NOTES:

1. The annotation of "required" refers to a high-level requirement category. The applicability of each sub-requirement is provided in Table 3-5.
2. The optional synchronous mode was not tested and therefore is not included in this certification.
3. The optional requirements for NFSv4 and NFSv1 server for file system I/O were not tested and therefore these requirements are not included in the certification.
4. Although, the SUT supports a HTTPS server, this optional requirement was not tested and therefore this requirement is not included in this certification.
5. The SUT does not support the optional requirements for WebDAV and REST and therefore these requirements are not included in this certification.
6. The SUT does not the GNS/single name space requirement. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor with condition of fielding.
7. The SUT does not support the optional LLDP requirement and therefore this requirement is not included in the certification.

Table 3-2. Capability and Functional Requirements and Status (continued)

NOTES (continued):

8. Although the SUT supports the DCB requirement, this optional requirement was not tested and therefore is not included in this certification.
9. The SUT does not support enabling or disabling the ability of the product to generate a Destination Unreachable message for reasons other than congestion. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact.
10. The SUT does not support the enabling or disabling of sending an Echo Reply message in response to an Echo Request message. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact. In addition, DISA stated the intent to change this requirement in the next version of the UCR.
11. The SUT does not support MLD as described in the RFC 2710. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact. In addition, DISA stated the intent to change this requirement in the next version of the UCR.
12. The SUT does not support the ability to configure the product to ignore Redirect messages. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact. In addition, DISA stated the intent to change this requirement in the next version of the UCR.
13. The SUT does not support being configured to only accept Redirect messages from the same router as is currently being used for that destination. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact.
14. The SUT does not support Differentiated services as described in RFC 2474 for preferred data in accordance with Section 2, Session Control Products, and Section 6, Network Infrastructure End-to-End Performance, plain text DSCP plan. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact.
15. The SUT does not support DNS client-side Load Balancing. This requirement does not apply to the SUT because the SUT has a single DNS connection and this requirement applies to multiple DNS connections.
16. A NIS server was not available for testing NIS client directory and Netgroup client directory.
17. A WINS server was not available for testing optional NBT Name Resolution and WINS server requirement.
18. An iSNS server was not available to test the iSNS client functionality.
19. The SUT does not support the optional IPSec per RFC 4301 requirement and therefore is not included in the certification.
20. The SUT does not support the optional Encapsulating Security Payload (ESP) per RFC 4303 requirement and therefore it is not included in the certification.
21. The SUT does not support the optional Internet Key Exchange version 2 (IKEv2) per RFC 4306 requirement and therefore it is not included in the certification.
22. Security testing is accomplished by DISA-led Information Assurance test teams and the results published in a separate report, Reference (e).
23. The SUT does not support the required CoS and QoS marking on egress traffic at Layer 3 per Section 6, Network Infrastructure End-to-End Performance or the optional CoS and QoS at Layer 2. DISA has accepted and approved the vendor's POA&M and adjudicated this discrepancy as having a minor operational impact. In addition, DISA stated the intent to change this requirement in the next version of the UCR.
24. The SUT does not support the optional vDSC requirements and therefore are not included in the certification.

LEGEND:

CoS	Class of Service	LAN	Local Area Network
CR	Capability Requirement	LLDP	Link Layer Discovery Protocol
DCB	Data Center Bridging	MLD	Multicast Listener Discovery
DSC	Data Storage Controller	NBT	NETBIOS over TCP/IP
DISA	Defense Information Systems Agency	NFS	Network File System
DNS	Domain Name Service	NIS	Network Information Service
DSCP	Differentiated Services Code Point	PO&AM	Plan of Action and Milestones
FR	Functional Requirement	QoS	Quality of Service
GNS	Global Name Space	REST	Representational State Transfer
HTTPS	Hypertext Transfer Protocol Secure	RFC	Request for Comment
ICMP	Internet Control Message Protocol	SUT	System under Test
IEEE	Institute of Electrical and Electronics Engineers	TCP/IP	Transmission Control Protocol/Internet Protocol
I/O	Input/Output	UCR	Unified Capabilities Requirements
IP	Internet Protocol	v	Version
IPSec	Internet Protocol Security	vDSC	Virtualized Data Storage Controller
iSNS	Internet Storage Name Service	WebDAV	Web Based Distributed Authoring and Versioning
		WINS	Windows Internet Name Service

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

Component (See notes 1 and 2.)	Release	Sub-component	Function
FAS2220, FAS2240-2, FAS2240-4, FAS3140, V3140, FAS3160, V3160, FAS3170, V3170, FAS3210, V3210, **FAS3220**, FAS3220 w/ IOXM, V3220, V3220 w/ IOXM, FAS3240, FAS3240 w/ IOXM, V3240, V3240 w/ IOXM, FAS3250 w/ IOXM, V3250 w/ IOXM, FAS3270, FAS3270 w/ IOXM, V3270, V3270 w/ IOXM, SA320 w/ IOXM, FAS6040, V6040, FAS6080, V6080, SA600, FAS6210, V6210, FAS6220, V6220, FAS6240 w/ IOXM, V6240 w/ IOXM, FAS6250 w/ IOXM, V6250 w/ IOXM, FAS6280 w/ IOXM, V6280 w/ IOXM, FAS6290 w/ IOXM, V6290 w/ IOXM, SA620	Data ONTAP Release 8.2.1	Not Applicable	Primary and Secondary DSCs

NOTES:
1. Components bolded and underlined were tested by JITC. The other components in the family series were not tested, but are also certified for joint use. JITC certifies those additional components because they utilize the same software and similar hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes.
2. Expanded I/O products have a dual enclosure and 12 PCIe expansion slots instead of a single enclosure and 4 PCIe expansion slots.

LEGEND:

I/O	Input/Output	PCIe	Peripheral Component Interconnect Express
IOXM	I/O Expansion Module	SUT	System Under Test
JITC	Joint Interoperability Test Command		

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

System Name	Software Release	Function
Required Ancillary Equipment		
Active Directory		
Public Key Infrastructure		
SysLog Server		
Test Network Components		
Cisco Nexus 5010	NX OS 5.2(1)N1(1)	Switch for Primary DSC
Cisco Nexus 5010	NX OS 5.2(1)N1(1)	Switch for Secondary DSC
Fujitsu RX300S6 Server	Windows Servers 2008 R2 Standard Service	Management Server (See note 1)
Fujitsu T901 Laptop	Linux	NFS Client Server (See note 1)
Window 2003 Server	Windows Server 2003 with Service Pack 1	DNS Server
Windows 2003 Server	Windows Server 2003 with Service Pack 2	DNS Server
Cisco 6509	IOS 15.1(1)	Edge Switch
Cisco 7606	IOS 15.2(1)	UC WAN Router

LEGEND:

COOP	Continuity of Operations
IOS	Internetwork Operating System

Table 3-5. DSC Capability/Functional Requirements

ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	DSC
1	**14.2 – Storage System**			
1-1	The system shall provide a Redundant Array of Independent Disks (RAID) for multiple disk drives. The system shall provide a configuration option to select the specific RAID level to be provisioned in the disk array. The RAID levels available for use shall be subject to the specific vendor implementation. At a minimum, the RAID level shall be dual parity RAID-6 for Serial Advanced Technology Attachment (SATA) drives and RAID-5 for Serial Attached Small Computer Systems Interface (SCSI) and Fiber Channel (FC) drives, although stronger RAID levels are acceptable.	14.2 DAT-000010	T IO-4	R
1-2	The system shall be capable of 99.9 percent availability.	14.2 DAT-000020	L/T	R
1-3	The system shall provide a management control function for low-level system monitoring and control functions, interface functions, and remote management. The management control function shall provide an Ethernet physical interface(s) for connection to the owner's (i.e., MILDEP) management network/Local Area Network (LAN) and also provide status. The monitoring shall include an initial system check, system cooling fans, temperatures, power supplies, voltages, and system power state tracking and logging.	14.2 DAT-000030	T IO-12	R
1-4	The system shall provide data storage replication (e.g., mirroring) services [Internet protocol (IP) version 4 (IPv4) and version 6 (IPv6)] between systems that are configured as source and destination replication pairs. The replication operations shall provide capabilities for data backup replication, system replication and migration, and system disaster recovery (DR) services in support of continuity of operations (COOP) planning.	14.2 DAT-000040	T IO-3	R
1-5	When the system interfaces to an Integrated Data Protection (IDP) service and the IDP makes copies of data storage information on to another DSC for periodic data storage backup, DR/COOP, migration, and data archiving operation, the system replication service shall complete the replication regardless of the host connection protocols used between the application servers and the DSC.	14.2 DAT-000050	T IO-3	R
1-6	The system replication and migration services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for migrating data storage information.	14.2 DAT-000060	T IO-3	R
1-7	The system DR services shall provide capabilities to replicate data storage and configuration information onto another standby DSC system for DR/COOP.	14.2 DAT-000070	T IO-3	R
1-8	The system shall provide configurable modes for replication (mirroring) operations between the source DSC and the destination DSC. During replication, both the source and the destination must be in a known good state. The configurable modes shall be Asynchronous or Synchronous and are depicted in Table 14.2-1, Replication Operation Modes.	14.2 DAT-000080	T IO-5	R
2	**14.3 – Storage Protocol**			
2-1	The system shall provide a Network File System version 3 (NFSv3) server for file systems data input/output (I/O).	14.3 DAT-000090	T IO-1	R
2-2	The system shall provide a Network File System version 4 (NFSv4) server for file systems data I/O.	14.3 DAT-000100	T IO-1	O
2-3	The system shall provide a Network File System version 4.1 (NFSv4.1) server, including support for parallel NFS for file systems data I/O.	14.3 DAT-000110	T IO-1	O
2-4	The system shall provide a Common Internet File System version 1.0 (CIFSv1.0) server for file systems data I/O.	14.3 DAT-000120	T IO-2	R
2-5	The system shall provide a Common Internet File System version 2.0 (CIFSv2.0) server for file systems data I/O.	14.3 DAT-000130	T IO-2	O
2-6	The system shall provide Internet Small Computer Systems Interface (iSCSI) server (target) operations for data I/O of Logical Units (LUNs) to clients (initiators).	14.3 DAT-000140	T IO-6	O
2-7	The system shall provide Fibre Channel Protocol (FCP) server (target) operations for data I/O of FCP LUNs to clients (initiators).	14.3 DAT-000150	T	O
2-8	The system shall provide Fibre Channel over Ethernet (FCoE) server (target) operations for data I/O of FCP LUNs to clients (initiators).	14.3 DAT-000160	T	O
2-9	The system shall provide a HyperText Transfer Protocol Secure (HTTPS) server for file system data I/O and management access to the storage controller operating system. The session shall be secured with Secure Socket Layer (SSL) or Transport Layer Security (TLS), per Internet Engineering Task Force (IETF) Request for Comment (RFC) 5246, and shall comply with Section 4, Information Assurance, for that protocol.	14.3 DAT-000170	L/T	O
2-10	The system shall provide Secure Shell version 2 (SSHv2) or SSL for management access to the storage controller operating system. The SSHv2 or SSL implementation shall comply with Section 4, Information Assurance, for that protocol.	14.3 DAT-000180	T IO-13	R

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

ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	DSC
2-11	The system shall provide Web-based Distributed Authoring and Versioning (WebDAV), per IETF RFC 4918, in support of Cloud-based virtualized storage infrastructures.	14.3 DAT-000190	L/T	O
2-12	The system shall implement the Representational State Transfer (REST) software architecture for distributed hypermedia systems and Cloud-based virtualized storage infrastructures.	14.3 DAT-000200	L/T	O
2-13	The system shall implement the Storage Networking Industry Association (SNIA) Cloud Data Management Interface (CDMI) standard.	14.3 DAT-000210	L/T IO-7	O
2-14	The system shall provide Global Name Space (GNS) or single name space functionality. The GNS functionality shall provide the capability to aggregate disparate and remote network-based file systems to provide a consolidated view to reduce complexities of localized file management and administration. The GNS functionality shall provide large (i.e., 14 Petabyte [PB] or greater) working pools of disks, transparent data migration, and it shall serve to reduce the number of storage mount points and shares. Each system shall have a dedicated and unique GNS. NOTE: A GNS functionality is provided with the assumption that it will only be used in deployments where latency is less than 200 ms.	14.3 DAT-000220	T IO-8, IO-14	R
3	**14.4 – Network Attached Storage Interface**			
3-1	The system shall provide physical interfaces for Gigabit Ethernet (GbE) and 10 Gigabit Ethernet (10 GbE) services in conformance with Institute of Electrical and Electronics Engineers (IEEE) 802.3 for Ethernet LAN interfaces.	14.4 DAT-000230	T IO-10	R
3-2	The system shall be able to provision, monitor, and detect faults, and to restore Ethernet services in an automated fashion.	14.4 DAT-000240	T IO-9, IO-15	R
3-3	The system shall provide physical interfaces for out-of-band management (OOBM) access and services with 10/100 Mbps Ethernet interfaces as a minimum. Services shall include remote access with at least one of the following protocols: SSHv2, SSL, HTTPS, and SNMPv3; and the protocols shall be secured in accordance with Section 4, Information Assurance.	14.4 DAT-000250	T IO-16	R
3-4	When the system uses Ethernet, Fast Ethernet, Gigabit Ethernet (GbE), and 10GbE interfaces, the interfaces shall be autosensing, autodetecting, and autoconfiguring with incoming and corresponding Ethernet link negotiation signals.	14.4 DAT-000260	T IO-11	R
3-5	Ethernet services of the system and the Logical Link Interworking Function (IWF) of the system shall terminate the Media Access Control (MAC) layer of Ethernet as described in Ethernet Standard IEEE 802.3.	14.4 DAT-000270	L/T IO-17	R
3-6	Ethernet services of the system shall support jumbo frames with a configurable Maximum Transmission Unit (MTU) of 9000 bytes or greater, excluding Ethernet encapsulation. When Ethernet encapsulation is included in the frame size calculation, an additional 22 bytes must be included for the MAC header (14 bytes), the Virtual LAN (VLAN) tag (4 bytes), and the Cyclical Redundancy Check (CRC) Checksum (4 bytes) fields in the Ethernet frame, resulting in a maximum of 9022 bytes or greater. The system shall also support a configurable MTU between 1280 bytes and 1540 bytes to ensure packets can transit type 1 encryptors. The system default MTU shall be 1540 bytes.	14.4 DAT-000280	T IO-18	R
3-7	Ethernet services of the system shall allocate a unique Ethernet MAC address to each Ethernet interface associated with a VLAN, as per IEEE 802.1Q.	14.4 DAT-000290	T IO-19	R
3-8	Ethernet services of the system shall support "Link Aggregation," as per IEEE 802.3ad or IEEE 802.1AX-2008, and use with the Link Aggregation Control Protocol.	14.4 DAT-000300	T	R
3-9	Ethernet services of the system shall provide Link Layer Discovery Protocol (LLDP), as per IEEE 802.1AB.	14.4 DAT-000310	T IO-20	O
4	**14.5 –Storage Array Network Interface**			
4-1	The system shall provide Fibre Channel (FC) physical interfaces and FCP interfaces and services as per American National Standards Institute (ANSI) X3.230, X3.297, and X3.303.	14.5 DAT-000320	L/T IO-21	O
5	**14.6 –Converged Network Adapter Interface**			
5-1	The system shall provide physical interfaces for FCoE services over a 10GbE physical interface in conformance with the ANSI T11 FC-BB-5 standard for FCoE with a Converged Network Adapter (CNA).	14.6 DAT-000330	L/T IO-22	O
5-2	The system shall provide physical interfaces for Data Center Bridging [DCB, also known as Converged Enhanced Ethernet (CEE)] features, and functionality, per the standards depicted in Table 14.6-1, Physical Interfaces for Data Center Bridging.	14.6 DAT-000340	L/T	O

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

ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	DSC
6	**14.7 – IP Networking**			
6-1	The system shall meet the IPv6 requirements defined in Section 5.2.2, Mapping of RFCs to UC Profile Categories, for a simple server/network appliance.	14.7 DAT-000350	L/T IO-23	R
6-2	The system shall provide statically provisioned or dynamically adjusted large IP packet receive buffers for replication (mirroring) session traffic received on the Ethernet physical interfaces. The receive buffers may be statically provisioned or the operating system of the system may dynamically self-adjust the packet receive buffer size based on measurements of the E2E path bandwidth, Maximum Segment Size (MSS), Round Trip Time (RTT), and the percentage of packet loss. The system shall provide a default and minimum IP packet receive buffer size of 2048 KB per replication (mirroring) session. The system shall provide a statically provisioned or dynamically adjusting maximum IP packet receive buffer size of up to 8192 KB per replication (mirroring) session. These IP packet receive buffer size requirements are conceptually based on either the Satellite or Transoceanic and Terrestrial Fiber Optic Cable E2E IP transport path models as depicted in Table 14.7-1, IP End-to-End Transport Path Models.	14.7 DAT-000360	L/T	R
6-3	The system shall provide an optimized congestion control (congestion avoidance) algorithm in Transmission Control Protocol (TCP) for avoidance of traffic loss on communications paths in high-speed networks with high latency or large bandwidth-delay products.	14.7 DAT-000370	L/T IO-24	R
7	**14.8 – Name Services**			
7-1	The system shall provide Lightweight Directory Access Protocol (LDAP) directory services per IETF RFC 4510.	14.8 DAT-000380	L/T IO-25	R
7-2	The system shall provide Kerberos authentication service per IETF RFC 4120.	14.8 DAT-000390	L/T IO-25	R
7-3	The system shall provide Domain Name System (DNS) client functionality.	14.8 DAT-000400	T IO-26	R
7-4	The system shall provide DNS client-side Load Balancing.	14.8 DAT-000410	T IO-26	R
7-5	The system shall provide Network Information Service (NIS) client directory service functionality.	14.8 DAT-000420	T IO-27	R
7-6	The system shall provide NIS Netgroups client directory service functionality.	14.8 DAT-000430	T IO-27	R
7-7	The system shall provide Network Basic Input/Output System (NETBIOS) over TCP/IP (NBT) Name Resolution and Windows Internet Name Service (WINS).	14.8 DAT-000440	T	O
7-8	The system shall provide Internet Storage Name Service (iSNS) client functionality per IETF RFC 4171.	14.8 DAT-000450	L/T IO-28	R
7-9	If the system has a Fiber Channel (FC) interface then the system shall provide FC Name and Zone Service.	14.8 DAT-000460	T IO-29	C
8	**14.9 – Security Services**			
8-1	The system shall provide IPSec per RFC 4301.	14.9 DAT-000470	IA IO-30	O
8-2	The system shall provide Encapsulating Security Payload (ESP) per RFC 4303.	14.9 DAT-000480	IA	O
8-3	The system shall provide Internet Key Exchange version 2 (IKEv2) per RFC 4306.	14.9 DAT-000490	IA	O
8-4	The system shall provide a configurable Packet Filter (Firewall) service to block unauthorized access (for intrusion prevention) while permitting authorized communications. The Packet Filter service shall use a "stateless" design that does not degrade performance and shall filter all packets received based on interface, source IP address, protocol, port, Type of Service (TOS), or Time To Live (TTL). The Packet Filter service shall provide a configuration policy for defining combinations of multiple packet match rules and processing actions.	14.9 DAT-000500	IA	O
8-5	The system shall provide encryption of data at rest at a minimum of AES-256 in accordance with Federal Information Processing Standard (FIPS) 140-2 level 1 or higher to provide the following capabilities: • Rapid crypto-shredding (destruction) of data, in accordance with National Institute of Standards and Technology (NIST) 800-88, for tactical systems that operate in harm's way and may fall into enemy hands. • Rapid recovery from sensitive data spills, where the wrong data is accidentally written to the wrong place.	14.9 DAT-000510	IA	R

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

ID	Requirement	UCR Ref (UCR 2013)	LoC/ TP ID	DSC
8-6	The system shall comply with all appropriate STIGs to include the Database Security Technical Implementation Guide.	14.9 DAT-000520	IA	R
9	**14.10 – Interoperability**			
9-1	The system shall provide an Application Programming Interface (API) to enable interaction with other software and systems. The interactions shall include routines, data structures, object classes, and protocols used to communicate between the consumer and implementer of the API. The API protocol and message format (e.g., Extensible Markup Language [XML]) shall be subject to the specific vendor system operating system implementation.	14.10 DAT-000530	T IO-32	R
10	**14.11 – Class of Service and Quality of Service**			
10-1	The system shall provide Class of Service (CoS) and Quality of Service (QoS) marking on egress traffic at layer 2 per IEEE 802.1p and, Section 7.2.1.3, Class of Service Markings, and Section 7.2.1.4, Virtual LAN Capabilities. Traffic classification and marking must occur before the egress transmission of the Ethernet frame with a rule or policy engine that matches on various storage and management protocol types as offered by the system. Examples of Storage Protocols and Management Protocols are listed in Table 14.11-1, Example Storage and Management Protocols. The marking is made in Ethernet VLAN tags by setting the priority value to between zero and seven, inclusive for various traffic classes. These are to be used in the ASLAN, non-ASLAN, and extended networks for per-hop CoS and QoS traffic conditioning by the network elements.	14.11 DAT-000540	T	O
10-2	The system shall provide CoS and QoS marking on egress traffic at layer 3 per Section 6, Network Infrastructure End-to-End Performance. Traffic classification and marking must occur before the egress transmission of the IP packet with a rule or policy engine that matches on various storage and management protocols that occur within the system, such as those listed in Table 14.11-1. NOTE: The IP packets are marked in the TOS field of the IPv6 packet header with Differentiated Services Code Point (DSCP) values from 0 and 63, inclusive. These are to be used in the ASLAN, non-ASLAN, and extended networks for per-hop CoS and QoS traffic conditioning by the network elements.	14.11 DAT-000550	T IO-33	R
11	**14.12 – Virtualization**			
11-1	The system shall provide virtualized Data Storage Controller (vDSC) functionality and individual protocol server processes. The vDSC shall meet all the requirements of a DSC with minor exceptions that are related to design and technical limitations associated with the complete virtualization of an operating system, which include internal counters for attributes of the physical system, QoS traffic processing, and per vDSC Mobile IP correspondent node binding cache limitations.	14.12 DAT-000560	T	O
11-2	The vDSC capability within the system shall provide secure, Private Networking Domains (PNDs) for Ethernet, VLANs, and IP that isolate the network domains of system units. The PND shall support the use of duplicate IP addresses and IP subnet address ranges among those of any other configured vDSC in the system. The PND shall provide a dedicated IP Forwarding Information Base (FIB) per vDSC.	14.12 DAT-000570	T	O
11-3	The vDSC shall provide an individual Command Line Interface (CLI) context with the full command set of the system, with the scope of the commands limited to the individual vDSC CLI context.	14.12 DAT-000580	T	O
11-4	The vDSC shall provide a programmatic API with the full command set of the system with the scope of the API commands limited to the individual vDSC context.	14.12 DAT-000590	T	O
11-5	The vDSC capability within the system shall provide an individual GNS unique from the system or shall provide a single name space that provides the capability to aggregate disparate hardware and storage architectures into a single file system. The GNS shall provide the capability to aggregate disparate and remote network-based file systems, providing a consolidated view to reduce complexities of localized file management and administration. The GNS shall provide large working pools of disks and transparent data migration, and shall serve to reduce the number of storage mount points and shares. The single name space shall be spread across multiple physical Network Access Server (NAS) heads all representing the same file system without replication. The single name space shall include the ability to tier data automatically within the same file system.	14.12 DAT-000600	T	O
12	**5.2 – IPv6 Requirements**			
12-1	If a DSC supports IP interfaces, then the DSC shall support the IPv6 requirements as defined for NA/SS in UCR Section 5, IPv6. Refer to Table 3-6.	Table 5.2-1	L	R

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

LEGEND:			
ANSI	American National Standards Institute	L	LoC Item
API	Application Programming Interface	LoC	Letter(s) of Compliance
C	Conditional	LUN	Logical Unit
COOP	Continuity of Operations	MAC	Media Access Control
CoS	Class of Service	NA/SS	Network Appliance/Simple Server
DSC	Data Storage Controller	O	Optional
FCP	Fibre Channel Protocol	QoS	Quality of Service
Gb	Gigabit	PND	Private Networking Domain
GbE	Gigabit Ethernet	R	Required
GNS	Global Name Service	RAID	Redundant Array of Independent Disks
ID	Identification	RFC	Requests for Comment
IEEE	Institute of Electrical and Electronics Engineers	STIG	Security Technical Implementation Guides
IETF	Internet Engineering Task Force	T	Test Item
I/O	input/output	TOS	Type of Service
IO-	interoperability test identification number	TP	Test Plan
IP	Internet Protocol	UC	Unified Capabilities
IPSec	Internet Protocol Security	UCR	Unified Capabilities Requirements
IPv6	Internet Protocol version 6	vDSC	virtualized Data Storage Controller

Table 3-6. IPv6 Requirements

ID	Requirement	UCR Ref (UCR 2013)	LoC/TP ID	C/R
v6-1	The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	5.2.1 IP6-000010	L	R
v6-2	Dual-stack end points or Call Connection Agents (CCAs) shall be configured to choose IPv4 over IPv6.	5.2.1 IP6-000020	L	R
v6-3	All nodes and interfaces that are "IPv6-capable" must be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a deliberate transition strategy. This includes the stateless autoconfiguration of link-local addresses. Nodes with multiple network interfaces may need to be separately configured per interface.	5.2.1 IP6-000030	L	R
v6-4	The system shall provide the same (or equivalent) functionality in IPv6 as in IPv4 consistent with the requirements in the UCR for its Approved Products List (APL) category. NOTE: This requirement applies only to products that are required to perform IPv6 functionality.	5.2.1 IP6-000050	L	R
v6-5	The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.	5.2.1 IP6-000060	L	R
v6-6	The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464. NOTE: This requirement does not mandate that the remaining sections of RFC 2464 have to be implemented.	5.2.1 IP6-000070	L	R
v6-7	The product shall support a minimum MTU of 1280 bytes as described in RFC 2460 and updated by RFC 5095.	5.2.1.1 IP6-000090	L	R
v6-8	If Path MTU Discovery is used and a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, then the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet.	5.2.1.1 IP6-000100	L	C
v6-9	The product shall not use the Flow Label field as described in RFC 2460.	5.2.1.2 IP6-000110	L	R
v6-10	The product shall be capable of setting the Flow Label field to zero when originating a packet.	5.2.1.2 IP6-000120	L	R
v6-11	The product shall be capable of ignoring the Flow Label field when receiving packets.	5.2.1.2 IP6-000140	L	R
v6-12	The product shall support the IPv6 Addressing Architecture as described in RFC 4291.	5.2.1.3 IP6-000150	L	R
v6-13	The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	5.2.1.3 IP6-000160	L	R
v6-14	If a scoped address (RFC 4007) is used, then the product shall use a scope index value of zero when the default zone is intended.	5.2.1.3 IP6-000170	L	C

Table 3-6. IPv6 Requirements (continued)

ID	Requirement	UCR Ref (UCR 2013)	LoC/TP ID	C/R
v6-15	If Dynamic Host Configuration Protocol (DHCP) is supported within an IPv6 environment, then it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315.	5.2.1.4 IP6-000180	L	C
v6-16	If the product is a DHCPv6 client, then the product shall discard any messages that contain options that are not allowed to appear in the received message type (e.g., an Identity Association option in an Information-Request message).	5.2.1.4 IP6-000200	L	C
v6-17	If the product is a DHCPv6 client and the first retransmission timeout has elapsed since the client sent the Solicit message and the client has received an Advertise message(s), but the Advertise message(s) does not have a preference value of 255, then the client shall continue with a client-initiated message exchange by sending a Request message.	5.2.1.4 IP6-000220	L	C
v6-18	If the product is a DHCPv6 client and the DHCPv6 solicitation message exchange fails, then it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a system configurable timer, or a user defined external event occurs.	5.2.1.4 IP6-000230	L	C
v6-19	If the product is a DHCPv6 client and it sends an Information-Request message, then it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server.	5.2.1.4 IP6-000240	L	C
v6-20	If the product is a DHCPv6 client, then it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server before transmitting packets using that address for itself.	5.2.1.4 IP6-000250	L	C
v6-21	If the product is a DHCPv6 client, then it shall log all reconfigure events. NOTE: Some systems may not be able to log all this information (e.g., the system may not have access to this information).	5.2.1.4 IP6-000260	L	C
v6-22	If the product supports DHCPv6 and uses authentication, then it shall discard unauthenticated DHCPv6 messages from UC products and log the event.	5.2.1.4 IP6-000270	L	C
v6-23	The product shall support Neighbor Discovery for IPv6 as described in RFC 4861.	5.2.1.5 IP6-000280	L	R
v6-24	The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for any cast addresses or solicited proxy advertisements.	5.2.1.5 IP6-000300	L	R
v6-25	When a valid “Neighbor Advertisement” message is received by the product and the product neighbor cache does not contain the target’s entry, the advertisement shall be silently discarded.	5.2.1.5 IP6-000310	L	R
v6-26	When a valid “Neighbor Advertisement” message is received by the product and the product neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the product shall silently discard the received advertisement.	5.2.1.5 IP6-000320	L	R
v6-27	When address resolution fails on a neighboring address, the entry shall be deleted from the product’s neighbor cache.	5.2.1.5 IP6-000330	L	R
v6-28	The product shall support the ability to configure the product to ignore Redirect messages.	5.2.1.5.1 IP6-000340	L	R
v6-29	The product shall only accept Redirect messages from the same router as is currently being used for that destination.	5.2.1.5.1 IP6-000350	L	R
v6-30	If “Redirect” messages are allowed, then the product shall update its destination cache in accordance with the validated Redirect message.	5.2.1.5.1 IP6-000360	L	C
v6-31	If the valid “Redirect” message is allowed and no entry exists in the destination cache, then the product shall create an entry.	5.2.1.5.1 IP6-000370	L	C
v6-32	If redirects are supported, then the device shall support the ability to disable this functionality.	5.2.1.5.1 IP6-000380	L	C
v6-33	The product shall prefer routers that are reachable over routers whose reachability is suspect or unknown.	5.2.1.5.2 IP6-000400	L	R
v6-34	If the product supports stateless IP address autoconfiguration including those provided for the commercial market, then the product shall support IPv6 Stateless Address Autoconfiguration (SLAAC) for interfaces supporting UC functions in accordance with RFC 4862.	5.2.1.6 IP6-000420	L	C
v6-35	If the product supports IPv6 SLAAC, then the product shall have a configurable parameter that allows the function to be enabled and disabled. Specifically, the product shall have a configurable parameter that allows the “managed address configuration” flag and the “other stateful configuration” flag to always be set and not perform stateless autoconfiguration.	5.2.1.6 IP6-000430	L	C

Table 3-6. IPv6 Requirements (continued)

ID	Requirement	UCR Ref (UCR 2013)	LoC/TP ID	C/R
v6-36	If the product supports IPv6 SLAAC, then the product shall have the configurable parameter set not to perform stateless autoconfiguration.	5.2.1.6 IP6-000440	L	C
v6-37	While nodes are not required to autoconfigure their addresses using SLAAC, all IPv6 Nodes shall support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862. In accordance with RFC 4862, DAD shall be implemented and shall be on by default. Exceptions to the use of DAD are noted in the following text.	5.2.1.6 IP6-000450	L	R
v6-38	A node MUST allow for autoconfiguration-related variable to be configured by system management for each multicast-capable interface to include DupAddrDetectTransmits where a value of zero indicates that DAD is not performed on tentative addresses as specified in RFC 4862.	5.2.1.6 IP6-000460	L	R
v6-39	The product shall support manual assignment of IPv6 addresses.	5.2.1.6 IP6-000470	L	R
v6-40	The product shall support the Internet Control Message Protocol (ICMP) for IPv6 as described in RFC 4443.	5.2.1.7 IP6-000520	L	R
v6-41	The product shall support the capability to enable or disable the ability of the product to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.	5.2.1.7 IP6-000540	L	R
v6-42	The product shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address.	5.2.1.7 IP6-000550	L	R
v6-43	The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them.	5.2.1.7 IP6-000560	L	R
v6-44	The product shall support MLD as described in RFC 2710.	5.2.1.8 IP6-000680	L	R
v6-45	If the product uses IPSec, then the product shall be compatible with the Security Architecture for the IPSec described in RFC 4301.	5.2.1.9 IP6-000690	L	C
v6-46	If RFC 4301 is supported, then the product shall not support the mixing of IPv4 and IPv6 in a SA.	5.2.1.9 IP6-000700	L	C
v6-47	If RFC 4301 is supported, then the product's security association database (SAD) cache shall have a method to uniquely identify a SAD entry.	5.2.1.9 IP6-000710	L	C
v6-48	If RFC 4301 is supported, then the product shall implement IPSec to operate with both integrity and confidentiality.	5.2.1.9 IP6-000720	L	C
v6-49	If RFC 4301 is supported, then the product shall be capable of enabling and disabling the ability of the product to send an ICMP message informing the sender that an outbound packet was discarded.	5.2.1.9 IP6-000730	L	C
v6-50	If an ICMP outbound packet message is allowed, then the product shall be capable of rate limiting the transmission of ICMP responses.	5.2.1.9 IP6-000740	L	C
v6-51	If RFC 4301 is supported, then the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.	5.2.1.9 IP6-000750	L	C
v6-52	If RFC 4301 is supported, and the product receives a packet that does not match any SPD cache entries, and the product determines it should be discarded, then the product shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet.	5.2.1.9 IP6-000760	L	C
v6-53	If RFC 4301 is supported, then the product should include a management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECTORS.	5.2.1.9 IP6-000770	L	C
v6-54	If RFC 4301 is supported, then the product shall support the ESP Protocol in accordance with RFC 4303.	5.2.1.9 IP6-000780	L	C
v6-55	If RFC 4303 is supported, then the product shall be capable of enabling anti-replay.	5.2.1.9 IP6-000790	L	C
v6-56	If RFC 4303 is supported, then the product shall check, as its first check, after a packet has been matched to its SA whether the packet contains a sequence number that does not duplicate the sequence number of any other packet received during the life of the security association.	5.2.1.9 IP6-000800	L	C
v6-57	If RFC 4301 is supported, then the product shall support IKEv1 as defined in RFC 2409.	5.2.1.9 IP6-000810	L	C

Table 3-6. IPv6 Requirements (continued)

ID	Requirement	UCR Ref (UCR 2013)	LoC/TP ID	C/R
v6-58	To prevent a Denial of Services (DoS) attack on the initiator of an IKE_SA, the initiator shall accept multiple responses to its first message, treat each as potentially legitimate, respond to it, and then discard all the invalid half-open connections when it receives a valid cryptographically protected response to any one of its requests. Once a cryptographically valid response is received, all subsequent responses shall be ignored whether or not they are cryptographically valid.	5.2.1.9 IP6-000820	L	C
v6-59	If RFC 4301 is supported, then the product shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.	5.2.1.9 IP6-000830	L	C
v6-60	If RFC 4301 is supported, then the product shall support the ISAKMP as defined in RFC 2408.	5.2.1.9 IP6-000840	L	C
v6-61	If the product supports the IPSec Authentication Header Mode, then the product shall support the IP Authentication Header (AH) as defined in RFC 4302.	5.2.1.9 IP6-000850	L	C
v6-62	If RFC 4301 is supported, then the product shall support manual keying of IPSec.	5.2.1.9 IP6-000860	L	C
v6-63	If RFC 4301 is supported, then the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined RFC 4835.	5.2.1.9 IP6-000870	L	C
v6-64	If RFC 4301 is supported, then the product shall support the IKEv1 security algorithms as defined in RFC 4109.	5.2.1.9 IP6-000880	L	C
v6-65	If the product uses Uniform Resource Identifiers (URIs) in combination with IPv6, then the product shall use the URI syntax described in RFC 3986.	5.2.1.10 IP6-000990	L	C
v6-66	If the product uses the Domain Name Service (DNS) resolver for IPv6 based queries, then the product shall conform to RFC 3596 for DNS queries.	5.2.1.10 IP6-001000	L	C
v6-67	For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 kbps) resulting in a 250-byte bearer packet plus 10 kbps for signaling, Ethernet Interframe Gap, and the Secure Real-Time Transport Control Protocol (SRTCP) overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.	5.2.1.11 IP6-001010	L	R
v6-68	The product shall forward packets using the same IP version as the version in the received packet.	5.2.1.12 IP6-001040	L	R
v6-69	When the product is establishing media streams from dual-stacked appliances for AS-SIP signaled sessions, the product shall use the Alternative Network Address Type (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091.	5.2.1.12 IP6-001050	L	R
v6-70	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a unicast address, then the product shall support generation and processing of unicast IPv6 addresses having the following formats: • x:x:x:x:x:x:x:x (where x is the hexadecimal values of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A. • x:x:x:x:x:x:d.d.d.d (where x is the hexadecimal values of the six high-order 16-bit pieces of the address, and d is the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). For example, 1080:0:0:0:8:800:116.23.135.22.	5.2.1.13 IP6-001060	L	C
v6-71	If the product is using AS-SIP, then the product shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats: • x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A. • x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22. • compressed zeros: 1080::8:800:200C:417A.	5.2.1.13 IP6-001070	L	C
v6-72	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a multicast group address (i.e., the two most significant hexadecimal digits are FF), then the product shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.	5.2.1.13 IP6-001080	L	C
v6-73	If the product is using AS-SIP, and the <addrtype> is IPv6, then the product shall support the use of RFC 4566 for IPv6 in SDP as described in AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs.	5.2.1.13 IP6-001090	L	C
v6-74	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is an IPv6 multicast group address, then the multicast connection address shall not have a Time To Live (TTL) value appended to the address as IPv6 multicast does not use TTL scoping.	5.2.1.13 IP6-001100	L	C

Table 3-6. IPv6 Requirements (continued)

ID	Requirement		UCR Ref (UCR 2013)	LoC/TP ID	C/R
v6-75	If the product is using AS-SIP, then the product shall support the processing of IPv6 multicast group addresses having the <number of address> field and may support generating the <number of address> field. This field has the identical format and operation as the IPv4 multicast group addresses.		5.2.1.13 IP6-001110	L	C
v6-76	The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 2, Session Control Products, and Section 6, Network Infrastructure End-to-End Performance, plain text DSCP plan.		5.2.1.14 IP6-001150	L	R
v6-77	If the product acts as an IPv6 tunnel broker, then the product shall support the function as defined in RFC 3053.		5.2.1.14 IP6-001160	L	C
v6-78	If the DSC has an IP interface, then the DSC must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.		Table 5.2-1	L	R
	RFC 2407	The Internet IP Security Domain of Interpretation for ISAKMP	Table 5.2-4	L	C
	RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)	Table 5.2-4	L	C
	RFC 2409	The Internet Key Exchange (IKE)	Table 5.2-4	L	C
	RFC 2460	Internet Protocol, Version 6 (IPv6) Specification	Table 5.2-4	L	R-2
	RFC 2464	Transmission of IPv6 Packets over Ethernet Networks	Table 5.2-4	L	R-3
	RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	Table 5.2-4	L	R-4
	RFC 2710	Multicast Listener Discovery (MLD) for IPv6	Table 5.2-4	L	R-8
	RFC 3053	IPv6 Tunnel Broker	Table 5.2-4	L	C
	RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	Table 5.2-4	L	C
	RFC 3596	DNS Extensions to Support IPv6	Table 5.2-4	L	C
	RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	Table 5.2-4	L	C
	RFC 4007	IPv6 Scoped Address Architecture	Table 5.2-4	L	R
	RFC 4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	Table 5.2-4	L	R
	RFC 4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	Table 5.2-4	L	R
	RFC 4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	Table 5.2-4	L	C
	RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	Table 5.2-4	L	R-1
	RFC 4291	IP Version 6 Addressing Architecture	Table 5.2-4	L	R
	RFC 4301	Security Architecture for the Internet Protocol	Table 5.2-4	L	C
	RFC 4302	IP Authentication Header	Table 5.2-4	L	C
	RFC 4303	IP Encapsulating Security Payload (ESP)	Table 5.2-4	L	C
	RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Table 5.2-4	L	R
	RFC 4566	SDP: Session Description Protocol	Table 5.2-4	L	C
	RFC 4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	Table 5.2-4	L	C
	RFC 4861	Neighbor Discovery for IP Version 6 (IPv6)	Table 5.2-4	L	R
	RFC 4862	IPv6 Stateless Address Autoconfiguration	Table 5.2-4	L	C
	RFC 5095	Deprecation of Type 0 Routing Headers in IPv6	Table 5.2-4	L	R

Table 3-6. IPv6 Requirements (continued)

LEGEND:

AH	Authentication Header	ISAKMP	Internet Security Association and Key Management Protocol
AS-SIP	Assured Services Session Initiation Protocol		
C	Conditional	kbps	kilobits per second
DAD	Duplicate Address Detection	L	LoC Item
DHCP	Dynamic Host Configuration Protocol	LoC	Letter(s) of Compliance
DHCPv6	Dynamic Host Configuration Protocol for IPv6	MLD	Multicast Listener Discovery
DNS	Domain Name Service	MTU	Maximum Transmission Unit
DSC	Data Session Controller	R	Required
DSCP	Differentiated Services Code Point	RFC	Request For Comment
ESP	Encapsulating Security Protocol	SAD	Security Association Database
ICMP	Internet Control Message Protocol	SDP	Session Description Protocol
ICMPv6	Internet Control Message Protocol for IPv6	SLAAC	Stateless Address Autoconfiguration
ID	Identification	SPD	Security Policy Database
IKE	Internet Key Exchange	TP	Test Plan
IPSec	Internet Protocol Security	UC	Unified Capabilities
IPv4	Internet Protocol version 4	UCR	Unified Capabilities Requirements
IPv6	Internet Protocol version 6		

Joint Interoperability Certification Revision History

Revision	Date	Approved By	Comments
NA	24 November 2014	Brad Clark	This is the original Joint Interoperability Certification.
1	19 February 2015	Anita Brown	The following components were added to Table 4, UC APL Product Summary. These components were not tested, however, are also certified for joint use. JITC certifies those additional components because they utilize the same software and similar hardware and JITC analysis determined them to be functionally identical for interoperability certification purposes. FAS8020, FAS8040, FAS8060, CBvM100 (Edge), FSvM100 (Edge-T)

LEGEND:
NA Not Applicable
SUT System Under Test