

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
Section 5 IPv6.....	5-1
5.1 Introduction.....	5-1
5.2 IPv6.....	5-1
5.2.1 Product.....	5-6
5.2.1.1 Maximum Transmission Unit.....	5-6
5.2.1.2 Flow Label.....	5-7
5.2.1.3 Address.....	5-7
5.2.1.4 Dynamic Host Configuration Protocol.....	5-8
5.2.1.5 Neighbor Discovery.....	5-9
5.2.1.6 Stateless Address Autoconfiguration and Manual Address Assignment.....	5-10
5.2.1.7 Internet Control Message Protocol.....	5-13
5.2.1.8 Routing Functions.....	5-14
5.2.1.9 IP Security.....	5-16
5.2.1.10 Network Management.....	5-18
5.2.1.11 Traffic Engineering.....	5-19
5.2.1.12 IP Version Negotiation.....	5-20
5.2.1.13 Services Session Initiation Protocol IPv6 Unique Requirements.....	5-21
5.2.1.14 Miscellaneous.....	5-22
5.2.2 Mapping of RFCs to UC Profile Categories.....	5-23

LIST OF TABLES

<u>TABLE</u>		<u>PAGE</u>
Table 5.2-1.	IPv6 Requirements for UC Products.....	5-2
Table 5.2-2.	UCR Policy for Manual, Stateful, and Stateless IPv6 Address Configuration	5-13
Table 5.2-3.	UC End Instruments (EIs).....	5-23
Table 5.2-4.	UC Network Appliances and Simple Servers (NA/SS).....	5-24
Table 5.2-5.	UC Router (R).....	5-25
Table 5.2-6.	LAN Switch (LS).....	5-27
Table 5.2-7.	UC Information Assurance Security Devices (SD)	5-29

SECTION 5

IPV6

5.1 INTRODUCTION

This section describes the IPv6 requirements for Sensitive but Unclassified (SBU) Unified Capabilities (UC) subsets provided by all products and technologies used to send and receive or to support voice, video, or data across Department of Defense (DoD) networks that provide UC services.

5.2 IPV6

The system requirements specified in Section 2, Session Control Products, are the minimum set of requirements necessary for the system to be Internet protocol (IP) version 6 (IPv6) capable for Video and Voice over IP (VVoIP). An implementer may choose to specify additional IPv6 requirements based on its non-VVoIP or unique VVoIP requirements. Also, a vendor may choose to implement additional IPv6 functions based on its commercial market. This section focuses on the “deltas” between an IPv6 implementation and an IPv4 implementation, and does not address consistencies or inconsistencies between IPv4 and IPv6.

When the [Alarm] tag appears after a requirement’s applicability statement, the guidance from Section 4.2.1, The [Alarm] Tag: Generation of Alarms, is to be followed.

The requirements defined in Section 2, Session Control Products, are associated with the external interfaces of the UC products or network appliances. For defining each requirement, the terms “UC products” and “Network Appliance (NA)” are shortened to “system.” As shown in Figure 2.1-1, High-Level DISN Assured Services Network Model, the external interfaces for an NA are generally considered to be interfaces that connect to and interact with the Assured Services Local Area Network (ASLAN) or the non-ASLAN. The primary interfaces associated with the IPv6 requirements are the signaling: UC Session Initiation Protocol (SIP) and bearer: Secure Real-Time Transport Protocol (SRTP) interfaces.

Whenever a reference to a specific Request for Comments (RFC) appears in a UC Requirements (UCR) requirement, the specific language of the UCR document and its subtended requirements should be understood within the context of the RFC.

Finally, the acronyms used for designating the various UC Products are shown in [Table 5.2-1](#), IPv6 Requirements for UC Products.

Table 5.2-1. IPv6 Requirements for UC Products

UC PRODUCT	IPV6 REQUIREMENTS
SBU IP-Based UC Product	
Softswitch (SS)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Session Controller (SC) including Master SC (MSC), Subtended SC (SSC), and Deployable SC (DSC)	The SC/Call Connection Agent (CCA) application in conjunction with the VVoIP EI and Media Gateway (MG) must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Router (R)	Must be IPv6-capable. Use guidance in Table 5.2-5 for Routers.
Customer Edge (CE) Router (CE-R)	Must be IPv6-capable. Use guidance in Table 5.2-5 for Routers.
Assured Services (AS) Session Initiation Protocol (SIP) (AS-SIP) End Instrument (AEI)	The EI in conjunction with the Call Connection Agent (CCA) application must be IPv6-capable. Use guidance in Table 5.2-3 for EI.
Secure End Instrument (SEI)	Same as AEI, above.
Extensible Messaging and Presence Protocol (XMPP) Server/Client	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
AS-SIP Time Division Multiplexing (TDM) gateway (AS-SIP TDM GW)	If the AS-SIP TDM GW has an IP interface, then the AS-SIP TDM GW must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
AS-SIP IP Gateway (AS-SIP IP GW)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Collaboration Product (Server Component)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Collaboration Product (Client Component)	Must be IPv6-capable. Use guidance in Table 5.2-3 for EI.
LAN Product	
LAN Switch (LS)	Must be IPv6-capable. Use guidance in Table 5.2-6 .
LAN Access Switch	Must be IPv6-capable. Use guidance in Table 5.2-6 Part 1 for LAN Access Switch and Section 7.2.1.5, Protocols.
LAN Distribution Switch	Must be IPv6-capable. Use guidance in Table 5.2-6 Part 2 for LAN Distribution Switches and Section 7.2.1.5, Protocols.
LAN Core Switch	Must be IPv6-capable. Use guidance in Table 5.2-6 Part 3 for LAN Core Switches and Section 7.2.1.5, Protocols.
Wireless LAN Product	

UC PRODUCT	IPv6 REQUIREMENTS
Wireless LAN Access Switch (WLAS)	Must be IPv6-capable. Use guidance in Table 5.2-6 Part 1 for LAN Access Switch.
Wireless LAN Access Bridge (WAB)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Wireless End Instrument (WEI)	Must be IPv6-capable. Same as AEI, above.
Peripheral Products	
Customer Premises Equipment (CPE)	If the CPE has an IP interface, then the CPE must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Integrated Access Switch (IAS)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
AS-SIP IP Gateway (GW)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
AS-SIP TDM Gateway (GW)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Signaling Multipoint Control Unit (SMCU)	If the SMCU has an IP interface, then the SMCU must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
DoD Secure Communications Device (DSCD)	Same as SEI, above.
UC Conference System (UCCS)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
UC External Adjunct Devices	UC External Adjunct Devices that are not covered under CPE [such as a Lightweight Directory Access Protocol (LDAP) server, local directory services server] are to be covered under DoD IPv6 Profile for Net App or Simple Server. Use guidance in Table 5.2-4 for NA/SS.
Network monitoring for IPv6 data/voice networks	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Instant Messaging, Chat, and Presence/Awareness Features	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Real-Time Services (RTS) Routing Database	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
UC Tool Suite	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
E911 Management System	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Network Infrastructure Products	
Multiservice Provisioning Platform (MSPP)	If the MSPP has an IP interface, then the MSPP must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Optical Digital Cross-Connect (ODXC)	If the ODXC has an IP interface, then the ODXC must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Provider Router/Provider Edge Router (P/PE Router)	Must be IPv6-capable. Use guidance in Table 5.2-5 for Router.
DISN Optical Transport Switch (OTS)	If the OTS has an IP interface, then the OTS must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.

UC PRODUCT	IPv6 REQUIREMENTS
Transport Switch Function (TSF)	If the TSF has an IP interface, then the TSF must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Aggregate Grooming Function (AGF)	If the AGF has an IP interface, then the AGF must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Access Aggregation (AAG) Function	If the AAG has an IP interface, then the AAG must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Timing and Synchronization (T&S)	If the T&S has an IP interface, then the T&S must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Tactical UC Product	
Deployable Network Element (D-NE)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Deployable LAN (DLAN) Products and infrastructure	Must be IPv6-capable. Use guidance from LAN Products, above.
Deployed Tactical Radio (DTR)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Deployable Cellular Voice Exchange (DCVX)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Multifunction Mobile Devices	
Multifunction Mobile Device	Must be IPv6-capable. Use guidance in Table 5.2-3 for EI.
Multifunction Mobile Device Backend Support System (MBSS)	Must be IPv6-capable. Use guidance in Table 5.2-3 for EI.
Security Devices (SDs)	
High Assurance IP Encryptor (HAIPE)	Must be IPv6-capable. Use guidance in Table 5.2-7 .
Link Encryptor Family (LEF)	Must be IPv6-capable. Use guidance in Table 5.2-7 .
Session Border Controller (SBC)	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Firewall (FW)	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Intrusion Protection System (IPS) and Intrusion Detection System (IDS)	Must be IPv6-capable and must be capable of inspecting IPv4 and IPv6 packets simultaneously, and those packets contained within tunnels that are not encrypted (e.g., GRE, IPSec AH, IP in IP) or shall support the capability to alarm if tunneled packets are detected that could not be inspected further. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Virtual Private Network (VPN) Concentrator	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Network Access Control (NAC)	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Integrated Security Solution (ISS)	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Information Assurance Tools (IATs)	Must be IPv6-capable. Use guidance in UCR 2013, Section 13, Security Devices.

UC PRODUCT	IPV6 REQUIREMENTS
RTS Stateful Firewall (RSF)	Must be IPv6-capable. Use guidance in Table 5.2-7 and in UCR 2013, Section 13, Security Devices.
Storage Devices	
Data Storage Controller (DSC)	Must be IPv6 capable. Use guidance in Table 5.2-4 for NA/SS.
Network Elements	
Assured Services Network Element (AS-NE)	Must be IPv6 capable. Use guidance in Table 5.2-4 for NA/SS.
Defense Switched Network (DSN) Fixed Network Element (F-NE)	Must be IPv6-capable. Use guidance in Table 5.2-4 for NA/SS.
Classified Products	
Classified Session Controller (SC)	Same as SC, above.
Classified Core Switch	Same as LAN Core Switch, above.
Classified Distribution Switch	Same as LAN Distribution Switch, above.
Classified Access Switch	Same as LAN Access Switch, above.
Classified Session Border Controller (SBC)	Same as SBC, above.
Classified CE-R	Same as CE-R, above.
Secure UC Conference System (UCCS)	Same as UCCS, above.
Secure Multi Signaling Multipoint Control Unit (SMCU)	Same as SMCU, above.
Network Management	
Element Management System (EMS)	Conditional, dependent on the vendor's decision to use IPv6 for NM.
VVoIP EMS	Conditional, dependent on the vendor's decision to use IPv6 for NM.

5.2.1 Product

IP6-000010 [Required: EI, NA/SS, R, SD] The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213. **[Conditional: LS]** If the Local Area Network (LAN) Switch (LS) also supports a routing function, then the product shall also support dual IPv4 and IPv6 stacks as described in RFC 4213.

NOTE: The tunnel requirements are associated only with appliances that provide IP routing functions (e.g., routers). The primary intent of these requirements is to (1) require dual stacks on all UC appliances and (2) allow dual stacks and tunneling on routers.

IP6-000020 [Required: EI, NA/SS, LS, SD] Dual-stack end points or Call Connection Agents (CCAs) shall be configured to choose IPv4 over IPv6.

IP6-000030 [Required: EI, NA/SS, R, LS, SD] 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.

IP6-000040 [Conditional: R, LS] If the LS supports a routing function, then the product shall support the manual tunnel requirements as described in RFC 4213.

IP6-000050 [Required: EI, NA/SS, R, LS, SD] 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.

IP6-000060 [Required: EI, NA/SS, R, SD] The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095. **[Conditional: LS]** If the LS also supports a routing function, then the product shall support RFC 2460 and be updated by RFC 5095.

IP6-000070 [Required: EI, NA/SS, R, LS, SD] 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.

5.2.1.1 *Maximum Transmission Unit*

IP6-000080 [Required: EI (Softphone Only), R, LS, SD] The product shall support Path Maximum Transmission Unit (MTU) Discovery as described in RFC 1981.

IP6-000090 [Required: EI, NA/SS, R, LS, SD] The product shall support a minimum MTU of 1280 bytes as described in RFC 2460 and updated by RFC 5095.

NOTE: Guidance on MTU requirements and settings can be found in Section 6.11.4.2, Layer 2 – Data Link Layer.

IP6-000100 [Conditional: EI, NA/SS, SD] 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.

NOTE: Unlike IPv4, fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path.

5.2.1.2 *Flow Label*

IP6-000110 [Required: EI, NA/SS, R, LS, SD] The product shall not use the Flow Label field as described in RFC 2460.

IP6-000120 [Required: EI, NA/SS, R, LS, SD] The product shall be capable of setting the Flow Label field to zero when originating a packet.

IP6-000130 [Required: R, LS] The product shall not modify the Flow Label field when forwarding packets.

IP6-000140 [Required: EI, NA/SS, R, LS, SD] The product shall be capable of ignoring the Flow Label field when receiving packets.

5.2.1.3 *Address*

IP6-000150 [Required: EI, NA/SS, R, LS, SD] The product shall support the IPv6 Addressing Architecture as described in RFC 4291.

NOTE 1: According to “DoD IPv6 Standard Profiles For IPv6-capable Products-Supplemental Guidance” version 6.0, the use of “IPv4-mapped” addresses “on-the-wire” is discouraged due to security risks raised by inherent ambiguities.

NOTE 2: As noted in National Institute of Standards and Technology (NIST) Special Publication (SP) 500-267 25, “A Profile for IPv6 in the U.S. Government – Version 1.0”:

The use of the old Site-Local address type (RFC3879) is deprecated. The Unique Local IPv6 Unicast Addresses (ULA) (RFC 4193) mechanism has been designed to fulfill a similar requirement. While Private Addresses are widely used in IPv4 networks, generalized ULA use and support in IPv6 are not as mature nor is their architectural desirability as well understood.

For these reasons, the UC products are not required to support ULA at this time.

NOTE 3: An end site is defined as an end-user (subscriber) edge network domain that requires multiple subnets/64. Therefore, vendors will not be required to support anything greater than /64, such as /116 or /126 subnet.

IP6-000160 [Required: EI, NA/SS, R, LS, SD] The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.

IP6-000170 [Conditional: EI, NA/SS, R, LS, SD] 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.

5.2.1.4 *Dynamic Host Configuration Protocol*

IP6-000180 [Required: EI] [Conditional: NA/SS, R] 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.

IP6-000190 [Conditional: LS] If the LS supports DHCP and a routing function, then the product shall support RFC 3315.

IP6-000200 [Conditional: EI, NA/SS] 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).

IP6-000210 [Required: EI] The product shall support DHCPv6 as described in RFC 3315.

NOTE: The following subtended requirements are predicated upon an implementation of DHCPv6 for the EI. It is not expected that other UC appliances will use DHCPv6.

IP6-000220 [Required: EI] [Conditional: NA/SS] 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.

IP6-000230 [Required: EI] [Conditional: NA/SS] 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.

NOTE: The intent is to ensure that the DHCP client continues to restart the configuration process periodically until it succeeds.

IP6-000240 [Required: EI] [Conditional: NA/SS] 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.

IP6-000250 [Required: EI] [Conditional: NA/SS] 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.

IP6-000260 [Required: EI] [Conditional: NA/SS] [Alarm] 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).

IP6-000270 [Conditional: EI, NA/SS, R, LS] [Alarm] If the product supports DHCPv6 and uses authentication, then it shall discard unauthenticated DHCPv6 messages from UC products and log the event.

NOTE: Some systems may not be able to log all this information (e.g., the system may not have access to this information).

5.2.1.5 Neighbor Discovery

IP6-000280 [Required: EI, NA/SS, R, SD] The product shall support Neighbor Discovery for IPv6 as described in RFC 4861.

IP6-000290 [Conditional: LS] If the LS also supports a routing function, then the product shall support RFC 4861.

IP6-000300 [Required: NA/SS, R, LS, SD] 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.

IP6-000310 [Required: EI, NA/SS, R, LS, SD] 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.

IP6-000320 [Required: EI, NA/SS, R, LS, SD] 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.

IP6-000330 [Required: EI, NA/SS, R, LS, SD] When address resolution fails on a neighboring address, the entry shall be deleted from the product’s neighbor cache.

5.2.1.5.1 *Redirect Messages*

IP6-000340 [Required: EI, NA/SS, SD] The product shall support the ability to configure the product to ignore Redirect messages.

IP6-000350 [Required: EI, NA/SS, SD] The product shall only accept Redirect messages from the same router as is currently being used for that destination.

NOTE: The intent of this requirement is that if a node is sending its packets destined for location A to router X, that it can only accept a Redirect message from router X for packets destined for location A to be sent to router Z.

IP6-000360 [Conditional: EI, NA/SS] If “Redirect” messages are allowed, then the product shall update its destination cache in accordance with the validated Redirect message.

IP6-000370 [Conditional: EI, NA/SS] If the valid “Redirect” message is allowed and no entry exists in the destination cache, then the product shall create an entry.

IP6-000380 [Conditional: EI, NA/SS] If redirects are supported, then the device shall support the ability to disable this functionality.

NOTE: The default setting is “disabled” so that the redirect functions must explicitly be “enabled.”

5.2.1.5.2 *Router Advertisements*

IP6-000390 [Required: R] [Conditional: LS] [Alarm] If the product supports routing functions, then the product shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link and shall log any inconsistent router advertisements.

NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).

IP6-000400 [Required: EI, NA/SS, SD] The product shall prefer routers that are reachable over routers whose reachability is suspect or unknown.

IP6-000410 [Required: R] [Conditional: LS] If the product supports routing functions, then the product shall be capable of supporting the MTU value in the router advertisement message for all links in accordance with RFC 4861.

5.2.1.6 *Stateless Address Autoconfiguration and Manual Address Assignment*

IP6-000420 [Conditional: EI, NA/SS, R, LS, SD] 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.

NOTE 1: RFC 4862 has replaced the now-obsolete RFC 2462. The scope of RFC 2462, Section 5.5, is Creation of Global and Site-Local Addresses. The scope of RFC 4862, Section 5.5, is Creation of Global Addresses.

NOTE 2: “DoD IPv6 Standard Profiles for IPv6-capable Products-Supplemental Guidance” defines Host as a PC or other end-user computer or workstation running a general-purpose operating system.

NOTE 3: The UC EI platform (on which the softphone is located) may be certified to the DoD IPv6 Profile and required to support autonomous configuration, either SLAAC or DHCPv6 client.

IP6-000430 [Conditional: EI, NA/ SS, R, LS, SD] 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.

IP6-000440 [Conditional: EI (except softphones), NA/ SS, R, LS, SD] If the product supports IPv6 SLAAC, then the product shall have the configurable parameter set not to perform stateless autoconfiguration.

NOTE: The objective of this requirement is to prevent a product from using stateless auto configuration. Stateless address autoconfiguration is focused solely on softphones since they reside on PCs.

IP6-000450 [Required: EI, NA/SS, R, LS, SD] 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.

IP6-000460 [Required: EI, NA/SS, R, LS, SD] 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.

NOTE: Network Infrastructure Security Technical Implementation Guide (STIG) states the following:

The use of Duplicate Address Detection opens up the possibility of denial of service attacks. Any node can respond to Neighbor Solicitations for a tentative address,

causing the other node to reject the address as a duplicate. This attack is similar to other attacks involving the spoofing of Neighbor Discovery messages.

Further, RFC 4862 states the following:

By default, all addresses should be tested for uniqueness prior to their assignment to an interface for safety. The test should individually be performed on all addresses obtained manually, via stateless address autoconfiguration, or via DHCPv6. To accommodate sites that believe the overhead of performing Duplicate Address Detection outweighs its benefits, the use of Duplicate Address Detection can be disabled through the administrative setting of a per-interface configuration flag.

The products may include an administrative setting to disable DAD.

IP6-000470 [Required: EI, NA/SS, R, LS, SD] The product shall support manual assignment of IPv6 addresses.

IP6-000480 [Required: EI (Softphones only)] The product shall support stateful autoconfiguration (i.e., ManagedFlag=TRUE) as described in RFC 4862.

NOTE: This requirement is associated with the earlier Requirement 10.2 for the EI to support DHCPv6.

IP6-000490 [Required: R] [Conditional: LS] If the product provides routing functions, then the product shall default to using the “managed address configuration” flag and the “other stateful flag” set to TRUE in their router advertisements when stateful autoconfiguration is implemented.

IP6-000500 [Conditional: EI] If the product supports a subtended appliance behind it, then the product shall ensure that the IP address assignment process of the subtended appliance is transparent to the UC components of the product and does not cause the product to attempt to change its IP address.

NOTE: An example is a PC that is connected to the LAN through the hub or switch interface on a phone. The address assignment process of the PC should be transparent to the EI and should not cause the phone to attempt to change its IP address.

IP6-000510 [Conditional: EI (Softphones only)] If the product supports SLAAC and security constraints prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, then Internet Protocol Security (IPSec)-capable products shall support privacy extensions for stateless address autoconfiguration as defined in RFC 4941.

[Table 5.2-2](#), UCR Policy for Manual, Stateful, and Stateless IPv6 Address Configuration, summarizes the policy for configuring Manual, DHCP, and SLAAC for IPv6 address for the various UC Products.

Table 5.2-2. UCR Policy for Manual, Stateful, and Stateless IPv6 Address Configuration

UC PRODUCT	MANUAL IPV6 CONFIGURATION	IPV6 STATEFUL CONFIGURATION VIA DHCPV6	IPV6 SLAAC
Softphones	Yes, Requirement 12.3	Yes, Requirement 10	Yes, Requirement 12.4
EI (except softphones)	Yes, Requirement 12.3	Yes, Requirement 10	No, Requirement 12.1.1
NA/SS	Yes, Requirement 12.3	No for SC, SS, MG, Requirement 10, Note 1. Yes for all others if RFC 3315 is supported, Requirement 10	No, Requirement 12.1.1
R	Yes, Requirement 12.3	Conditionally Yes if RFC 3315 is supported, Requirement 10	No, Requirement 12.1.1
LS	Yes, Requirement 12.3	Conditionally Yes if RFC 3315 and routing functions are supported, Requirement 10	No, Requirement 12.1.1
SD	Yes, Requirement 12.3	No, Requirement 10	No, Requirement 12.1.1

Where “No” could be (1) not installed, (2) removed from Operating System, or (3) disabled by parameter.

5.2.1.7 Internet Control Message Protocol

IP6-000520 [Required: EI, NA/SS, R, LS, SD] The product shall support the Internet Control Message Protocol (ICMP) for IPv6 as described in RFC 4443.

IP6-000530 [Required: R, LS] The product shall have a configurable rate-limiting parameter for rate limiting the ICMP error messages it originates.

IP6-000540 [Required: NA/SS, R, LS, SD] 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.

NOTE: In lieu of the RFC 4443 paragraph 3.1 requirement to prohibit routers from forwarding a code 3 (address unreachable) message on point-to-point link back onto the arrival link, vendors may alternatively use a prefix length of 127 on Inter-Router Links to address ping-pong issues on non-Ethernet interfaces (the ping-pong issue is not present on Ethernet interfaces).

IP6-000550 [Required: EI, NA/SS, R, LS, SD] 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.

NOTE: The number of responses may be traffic conditioned to limit the effect of a denial of service attack.

IP6-000560 [Required: EI, NA/SS, R, LS, SD] The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them.

NOTE: The actual validation checks are specific to the upper layers and are out of the scope of this UCR. Protecting the upper layer with IPsec mitigates these attacks.

5.2.1.8 Routing Functions

IP6-000570 [Required: R] [Conditional: LS] If the product supports routing functions, then the product shall support the Open Shortest Path First (OSPF) for IPv6 as described in RFC 5340.

IP6-000580 [Required: R] [Conditional: LS] If the product supports routing functions, then the product shall support securing OSPF with IPsec as described for other IPsec instances in Section 4, Information Assurance.

IP6-000590 [Required: R] [Conditional: LS] If the product supports routing functions, then the product shall support router-to-router integrity using the IP Authentication Header with HMAC-SHA1-96 within Encapsulating Security Payload (ESP) and Authentication Header (AH) as described in RFC 2404.

NOTE: NIST Special Publication 500-267, "A Profile for IPv6 in the U.S. Government," forwards the following guidance:

Although HMAC-SHA-1 (RFC 2404) is still considered secure, the Internet Engineering Task Force (IETF) is encouraging the standardization of HMAC-SHA-256 to ensure an orderly transition to a more secure Message Authentication Code (MAC).

IP6-000600 [Required: R] [Conditional: LS] If the product supports interior routing functions of OSPFv3, then the product shall support RFC 4552.

NOTE: RFC 4552 relies on manual key exchange (pre-configuration) and may not be appropriate in a dynamic Tactical environment. Router acquisitions for Tactical deployment are exempt from this requirement.

IP6-000610 [Conditional: R, LS] If the product supports the Intermediate System to Intermediate System (IS-IS) routing protocol used in DoD backbone networks, then the product shall support the IS-IS for IPv6 as described in RFC 5308.

NOTE: IS-IS is the primary routing protocol in the Defense Information Systems Network (DISN) backbone for handling the infrastructure (non-customer) routes. The Provider (P), Classified CE-R (C-PE), Unclassified CE-R (U-PE), and Aggregation Router (AR) devices all have instances of the routing protocol. The IS-IS is also used on the RED side across the Generic Routing Encapsulation (GRE) tunnels.

IP6-000620 [Conditional: R, LS] If the product supports IS-IS routing architecture (for IPv6-only or dual-stack operation), then the product shall support RFC 5304 and RFC 5310 and shall support RFC 6119 for IPv6 traffic engineering.

IP6-000630 [Conditional: R, LS] If the product acts as a CE Router (CE-R), then the product shall support the use of Border Gateway Protocol (BGP) as described in RFC 1772 and RFC 4271.

- a. If the product acts as a CE-R, then the product shall support the use of BGP4 multiprotocol extensions for IPv6 inter-domain routing as described in RFC 2545.

NOTE: The requirement to support BGP4 is in Section 6, Network Infrastructure End-to-End Performance.

IP6-000640 [Conditional: R, LS] If the product acts as a CE-R, then the product shall support multiprotocol extensions for BGP4 in RFC 4760.

NOTE: The requirement to support BGP4 is in Section 6, Network Infrastructure End-to-End Performance.

IP6-000650 [Conditional: R] If the product acts as a CE-R, then the product shall support the GRE as described in RFC 2784.

IP6-000660 [Conditional: R] If the product acts as a CE-R, then the product shall support the Generic Packet Tunneling in IPv6 Specification as described in RFC 2473.

NOTE 1: Tunneling is provided for data applications and is not needed as part of the VVoIP architecture.

NOTE 2: Section 13, Security Devices, requires that Firewall (FW) and Intrusion Protection System (IPS) shall conform to all of the MUST requirements found in RFC 2473.

IP6-000670 [Required: EI (Softphone Only), R] [Conditional: LS] If the product supports routing functions, then the product shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810.

NOTE: The current VVoIP design does not use multicast, but routers supporting VVoIP also support data applications that may use multicast. A softphone will have non-routing functions that require MLDv2.

- a. If the product supports MLD process as described in RFC 2710 and extended in RFC 3810, then the product shall support RFC 2711.

IP6-000680 [Required: EI, NA/SS, SD] The product shall support MLD as described in RFC 2710.

NOTE: This requirement was added to ensure that Neighbor Discovery multicast requirements are met. Routers are not included in this requirement since they have to meet RFC 2710 in the preceding requirement.

5.2.1.9 IP Security

IP6-000690 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If the product uses IPSec, then the product shall be compatible with the Security Architecture for the IPSec described in RFC 4301.

NOTE 1: RFC 4301 mandates support for several features for which support is available in Internet Key Exchange (IKE) version 2 (IKEv2) but not in IKEv1, e.g., negotiation of a Security Association (SA) representing ranges of local and remote ports or negotiation of multiple SAs with the same selectors.

However, at this time the UCR does not require the use of IKEv2. Therefore, implementation at this time of RFC 4301 will include only those features which are compatible with the use of IKEv1.

NOTE 2: The interfaces required to use IPSec are defined in Section 4, Information Assurance.

- b. If RFC 4301 is supported, then the product shall support binding of a SA with a particular context.
- c. If RFC 4301 is supported, then the product shall be capable of disabling the BYPASS IPSec processing choice.

NOTE: The intent of this requirement is to ensure that no packets are transmitted unless they are protected by IPSec.

IP6-000700 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4301 is supported, then the product shall not support the mixing of IPv4 and IPv6 in a SA.

IP6-000710 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4301 is supported, then the product's security association database (SAD) cache shall have a method to uniquely identify a SAD entry.

NOTE: The concern is that a single SAD entry will be associated with multiple security associations. RFC 4301, Section 4.4.2, Security Association Database (SAD), describes a scenario where this could occur.

IP6-000720 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4301 is supported, then the product shall implement IPSec to operate with both integrity and confidentiality.

IP6-000730 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] 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.

IP6-000740 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If an ICMP outbound packet message is allowed, then the product shall be capable of rate limiting the transmission of ICMP responses.

IP6-000750 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4301 is supported, then the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.

IP6-000760 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] [Alarm] 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.

NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).

IP6-000770 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] [Alarm] 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.

NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).

IP6-000780 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4301 is supported, then the product shall support the ESP Protocol in accordance with RFC 4303.

IP6-000790 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4303 is supported, then the product shall be capable of enabling anti-replay.

IP6-000800 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] 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.

IP6-000810 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4301 is supported, then the product shall support IKEv1 as defined in RFC 2409.

NOTE: The IKEv1 requirements are found in Section 4, Information Assurance.

IP6-000820 [Conditional: EI, NA/SS, R, LS, SD] 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.

IP6-000830 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] 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.

IP6-000840 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4301 is supported, then the product shall support the ISAKMP as defined in RFC 2408.

IP6-000850 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If the product supports the IPsec Authentication Header Mode, then the product shall support the IP Authentication Header (AH) as defined in RFC 4302.

IP6-000860 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4301 is supported, then the product shall support manual keying of IPsec.

IP6-000870 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4301 is supported, then the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined RFC 4835

IP6-000880 [Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, SD] If RFC 4301 is supported, then the product shall support the IKEv1 security algorithms as defined in RFC 4109.

5.2.1.10 Network Management

IP6-000890 [Conditional: R, LS] If IPv6-compatible nodes are managed via Simple Network Management Protocol (SNMP) using IPv6, then the product shall comply with the Management Information Base (MIB) for IPv6 textual conventions and general group as defined in RFC 4293.

NOTE: The requirements to support SNMPv3 are found in Section 4, Information Assurance.

IP6-000900 [Conditional: R, LS] If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support the SNMPv3 management framework as described in RFC 3411.

IP6-000910 [Conditional: R, LS] If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support SNMPv3 message processing and dispatching as described in RFC 3412.

IP6-000920 [Conditional: R, LS] If the product performs routing functions and if IPv6-capable nodes are managed via SNMP management using IPv6, then the product shall support the SNMPv3 applications as described in RFC 3413.

IP6-000930 [Conditional: R, LS] If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the IP MIBs as defined in RFC 4293.

IP6-000940 [Conditional: R, LS] If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the Transmission Control Protocol (TCP) MIBs as defined in RFC 4022.

IP6-000950 [Conditional: R, LS] If IPv6-compatible nodes are managed via SNMP using IPv6, then the product shall support the User Datagram Protocol (UDP) MIBs as defined in RFC 4113.

IP6-000960 [Conditional: R, LS] If IPv6-compatible nodes are managed via SNMP using IPv6, and the product performs routing functions and tunneling functions, then the product shall support IP tunnel MIBs as described in RFC 4087.

IP6-000970 [Conditional: R, LS] If the product performs routing functions and is managed by SNMP using IPv6, then the product shall support the IP Forwarding MIB as defined in RFC 4292.

IP6-000980 [Conditional: R, LS] If the product supports routing functions, and the IPsec policy database is configured through SNMPv3 using IPv6, then the product shall support RFC 4807.

IP6-000990 [Required: EI (Softphone only)] [Conditional: EI, NA/SS, R, LS, SD] If the product uses Uniform Resource Identifiers (URIs) in combination with IPv6, then the product shall use the URI syntax described in RFC 3986.

IP6-001000 [Conditional: EI, NA/SS] 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.

5.2.1.11 Traffic Engineering

IP6-001010 [Required: NA/SS, R, LS, SD] 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.

IP6-001020 [Required: R, LS] Despite the differences in IPv6 and IPv4 packet sizes, for planning purposes, the number of VoIP subscribers per link size for IPv6 should be assumed to

be approximately the same as for IPv4 and is defined in Table 7.6-2, LAN VoIP Subscribers for IPv4 and IPv6, in Section 7, Network Edge Infrastructure.

IP6-001030 [Required: R, LS] Despite the differences in IPv6 and IPv4 packet sizes, for planning purposes, the number of video subscribers per link size for IPv6 should be assumed to be approximately the same as for IPv4 and is defined in Section 7, Network Edge Infrastructure.

5.2.1.12 IP Version Negotiation

IP6-001040 [Required: NA/SS, SD] The product shall forward packets using the same IP version as the version in the received packet.

NOTE: If the packet was received as an IPv6 packet, then the appliance will forward it as an IPv6 packet. If the packet was received as an IPv4 packet, then the appliance will forward the packet as an IPv4 packet. This requirement is primarily associated with the signaling packets to ensure that translation does not occur.

IP6-001050 [Required: EI, NA/SS] 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. Also, the following conditional requirements would apply.

NOTE 1: Guidance on clarification on the use of ANAT for related media is located in the AS-SIP 2013, Section 5.2.5, Clarification on the Use of ANAT for Related Media Streams.

NOTE 2: Guidance on SIP syntax and encoding rules for IPv6 Augmented Backus-Naur Form (ABNF) per RFC 5954 is located in AS-SIP 2013, Section 4.1.3, Basic Requirements for AS-SIP Signaling Appliances and AS-SIP EI.

IP6-001050.a [Required: EI, NA/SS] The product shall prefer any IPv4 address to any IPv6 address when using ANAT semantics.

NOTE: This requirement will result in all AS-SIP sessions being established using IPv4.

IP6-001050.b [Required: EI, NA/SS] The product shall place the option tag “SDP-ANAT” in a Required header field when using ANAT semantics in accordance with RFC 4092.

IP6-001050.c [Required: EI] The products shall include the IPv4 and IPv6 addresses within the SDP of the SIP INVITE message when the INVITE contains the SDP.

5.2.1.13 *Services Session Initiation Protocol IPv6 Unique Requirements*

IP6-001060 [Conditional: EI, NA/SS, SD] 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 (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: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.

IP6-001070 [Conditional: EI, NA/SS, SD] 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 format: 1080:0:0:0:8:800:200C:417A.
- 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.

IP6-001080 [Conditional: EI, NA/SS, SD] 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.

IP6-001090 [Conditional: EI, NA/SS, SD] 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.

IP6-001100 [Conditional: EI, NA/SS, SD] 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.

IP6-001110 [Conditional: EI, NA/SS, SD] 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.

IP6-001120 [Required: SD] The product shall be able to provide topology hiding [e.g., Network Address Translation (NAT)] for IPv6 packets as described in Section 4, Information Assurance.

NOTE: Deployments requiring the network topology hiding that IPv4 NAT provided as a side-effect should consider RFC 4864 – Local Network Protection (LNP) for IPv6.

IP6-001130 [Required: EI (Softphone Only)] The product shall support default address selection for IPv6 as defined in RFC 3484 (except for Section 2.1).

NOTE: It is assumed that an IPv6 appliance will have as a minimum an IPv6 link local and an IPv4 address, and will have at least two addresses.

5.2.1.14 *Miscellaneous*

IP6-001140 [Conditional: R, SD] If the product supports Remote Authentication Dial-in User Service (RADIUS) authentication, then the product shall support RADIUS as defined in RFC 3162. **[Conditional: LS]** If the LS supports a routing function and supports RADIUS authentication, then the product shall support RADIUS as defined in RFC 3162.

NOTE 1: RFC 3162 defines only the additional attributes of RADIUS that are unique to IPv6 implementations. For the base RADIUS requirements, other RFCs are required, such as RFC 2865.

NOTE 2: Because RFC 3162 cites the Network Access Server (NAS) functions would be on the Access Point (router), this function should be a feature of the router.

IP6-001150 [Required: EI, NA/SS, R, LS, SD] 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.

IP6-001160 [Conditional: NA/SS] If the product acts as an IPv6 tunnel broker, then the product shall support the function as defined in RFC 3053.

IP6-001170 [Conditional: R] If the product supports roaming (as defined within RFC 4282), then the product shall support this function as described by RFC 4282.

IP6-001180 [Conditional: R] If the product supports the Point-to-Point Protocol (PPP), then the product shall support PPP as described in RFC 5072.

IP6-001190 [Required: LS] [Conditional: R] To support ASLAN assured services, all LAN switches that provide layer 3 functionality to the access layer shall support Virtual Router Redundancy protocol (VRRP) for IPv6 as detailed in RFC 5798.

NOTE: This applies to products only in the ASLAN.

IP6-001200 [Conditional: R, LS] If the product supports ECN, then the product shall support RFC 3168 for the incorporation of ECN to TCP and IP, including ECN's use of two bits in the IP header.

NOTE: This applies to the Core, Distribution, and Access products as identified in Section 7.2.1.5, Protocols. The use of RFC 3168 is Conditional for these products.

5.2.2 Mapping of RFCs to UC Profile Categories

Tables 5.2-3 through 5.2-7 map RFCs and requirements applicability to the various UC profile categories.

Table 5.2-3. UC End Instruments (EIs)

RFC NUMBER	RFC TITLE	REQUIRED – R * CONDITIONAL – C
1981	Path MTU Discovery for IP Version 6	R-8
2407	The Internet IP Security Domain of Interpretation for ISAKMP	R-8; C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	R-8; C
2409	The Internet Key Exchange (IKE)	R-8; C
2460	Internet Protocol, Version 6 (IPv6) Specification	R-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
2710	Multicast Listener Discovery (MLD) for IPv6	R-8
2711	IPv6 Router Alert Option	R-8
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	R
3484	Default Address Selection for Internet Protocol Version 6 (IPv6)	R-8
3596	DNS Extensions to Support IPv6	C
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R-8
3986	Uniform Resource Identifier (URI): Generic Syntax	R-8; C
4007	IPv6 Scoped Address Architecture	R
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	R-8; C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	R-8; C
4302	IP Authentication Header	R-8; C
4303	IP Encapsulating Security Payload (ESP)	R-8; C
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R

RFC NUMBER	RFC TITLE	REQUIRED – R * CONDITIONAL – C
4566	SDP: Session Description Protocol	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R-8, C
4861	Neighbor Discovery for IP Version 6 (IPv6)	R
4862	IPv6 Stateless Address Autoconfiguration	R-8; C
4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	C-8
5095	Deprecation of Type 0 Routing Headers in IPv6	R
Notes:		
C/R-1: Meets only the dual-stack requirements of this RFC.		
C/R-2: Meets only the IPv6 formatting requirements of this RFC.		
R-3: Meets only the framing format aspects of RFC.		
R-4: Requirement covered in Section 6, Network Infrastructure End-to-End Performance.		
C-5: Condition is that product acts as a router.		
C-6: Applies only to MGs.		
C-7: Requirements apply only if the product acts as a CE-R.		
C/R-8: EI (softphones only).		
* This column can have (1) softphones only, e.g., R-8, (2) EI, e.g., R-3; or (3) Softphones only and EI, e.g., R-8; C.		

Table 5.2-4. UC Network Appliances and Simple Servers (NA/SS)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C
2409	The Internet Key Exchange (IKE)	C
2460	Internet Protocol, Version 6 (IPv6) Specification	R-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
2710	Multicast Listener Discovery (MLD) for IPv6	R-8
3053	IPv6 Tunnel Broker	C
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3596	DNS Extensions to Support IPv6	C
3986	Uniform Resource Identifier (URI): Generic Syntax	C
4007	IPv6 Scoped Address Architecture	R
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	C
4302	IP Authentication Header	C
4303	IP Encapsulating Security Payload (ESP)	C
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C
4861	Neighbor Discovery for IP Version 6 (IPv6)	R
4862	IPv6 Stateless Address Autoconfiguration	C
5095	Deprecation of Type 0 Routing Headers in IPv6	R
Notes:		
C/R-1: Meets only the dual-stack requirements of this RFC.		
C/R-2: Meets only the IPv6 formatting requirements of this RFC.		
R-3: Meets only the framing format aspects of RFC.		
R-4: Requirement covered in Section 6, Network Infrastructure End-to-End Performance.		
C-5: Condition is that product acts as a router.		
C-6: Applies only to MGs.		
C-7: Requirements apply only if the product acts as a CE-R.		
C/R-8: EI (softphones only).		

Table 5.2-5. UC Router (R)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1772	Application of the Border Gateway Protocol in the Internet	C-7
1981	Path MTU Discovery for IPv6	R
2404	The Use of HMAC-SHA-1-96 within ESP and AH	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	R
2408	Internet Security Association and Key Management Protocol (ISAKMP)	R
2409	The Internet Key Exchange (IKE)	R
2460	Internet Protocol, Version 6 (v6) Specification	R-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2473	Generic Packet Tunneling in IPv6 Specification	C-7
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	C-7

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2710	Multicast Listener Discovery (MLD) for IPv6	R
2711	IPv6 Router Alert Option	R
2784	Generic Router Encapsulation	C-7
3162	RADIUS and IPv6	C
3168	The Addition of Explicit Congestion Notification (ECN) to IP	C
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	C
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	C
3413	Simple Network Management Protocol (SNMP) Applications	C
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R
3986	Uniform Resource Identifier (URI): Generic Syntax	C
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	C
4087	IP Tunnel MIB	C
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	R
4113	Management Information Base for the User Datagram Protocol (UDP)	C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4271	A Border Gateway Protocol 4 (BGP-4)	C-7
4282	The Network Access Identifier	C
4291	IP Version 6 Addressing Architecture	R
4292	IP Forwarding MIB	C
4293	Management Information Base for the Internet Protocol (IP)	C
4301	Security Architecture for the Internet Protocol	R
4302	IP Authentication Header	R
4303	IP Encapsulating Security Payload (ESP)	R
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4552	Authentication Confidentiality for OSPFv3	R
4760	Multiprotocol Extensions for BGP-4	C-7, C
4807	IPSec Security Policy Database Configuration MIB	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R
4861	Neighbor Discovery for IP Version 6 (IPv6)	R

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4862	IPv6 Stateless Address Autoconfiguration	C
5072	IP Version 6 over PPP	C
5095	Deprecation of Type 0 Routing Headers in IPv6	R
5304	IS-IS Cryptographic Authentication	C
5308	Routing IPv6 with IS-IS	C
5310	IS-IS Generic Cryptographic Authentication	C
5340	OSPF for IPv6	R
5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	C
Notes:		
C/R-1: Meets only the dual-stack requirements of this RFC.		
C/R-2: Meets only the IPv6 formatting requirements of this RFC.		
R-3: Meets only the framing format aspects of RFC.		
R-4: Requirement covered in Section 6, Network Infrastructure End-to-End Performance.		
C-5: Condition is that product acts as a router.		
C-6: Applies only to MGs.		
C-7: Requirements apply only if the product acts as a CE-R.		
C/R-8: EI (softphones only)		

Table 5.2-6. LAN Switch (LS)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
Part 1 LAN Access Switch		
1981	Path MTU Discovery for IPv6	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C
2409	The Internet Key Exchange (IKE)	C
2460	Internet Protocol, Version 6 (v6) Specification	C-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
3168	The Addition of Explicit Congestion Notification (ECN) to IP	C
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	C
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	C
3413	Simple Network Management Protocol (SNMP) Applications	C
3986	Uniform Resource Identifier (URI): Generic Syntax	C
4007	IPv6 Scoped Address Architecture	R

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4022	Management Information Base for the Transmission Control Protocol (TCP)	C
4087	IP Tunnel MIB	C
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C
4113	Management Information Base for the User Datagram Protocol (UDP)	C
4291	IP Version 6 Addressing Architecture	R
4292	IP Forwarding MIB	C
4293	Management Information Base for the Internet Protocol (IP)	C
4301	Security Architecture for the Internet Protocol	C
4302	IP Authentication Header	C
4303	IP Encapsulating Security Payload (ESP)	C
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4807	IPSec Security Policy Database Configuration MIB	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C
4862	IPv6 Stateless Address Autoconfiguration	C
5095	Deprecation of Type 0 Routing Headers in IPv6	C
Part 2 LAN Distributed L3 Switch Requirements from Part 1 above, plus the below		
1981	Path MTU Discovery for IPv6	C-5
2404	The Use of HMAC-SHA-1-96 within ESP and AH	C-5
2710	Multicast Listener Discovery (MLD) for IPv6	C-5
2711	IPv6 Router Alert Option	C-5
3162	RADIUS and IPv6	C-5
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C-5, C-9
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	C-5
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	C-1, C-5
4552	Authentication Confidentiality for OSPFv3 (Routing protocol authentication only)	C-5
4861	Neighbor Discovery for IP Version 6 (IPv6)	C-5
5304	IS-IS Cryptographic Authentication	C-5
5308	Routing IPv6 with IS-IS	C-5
5310	IS-IS Generic Cryptographic Authentication	C-5
5340	OSPF for IPv6	C-5
5798	Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	R

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
Part 3 LAN Core L3 Switch Requirements from Part 2 above, plus the below		
1772	Application of the Border Gateway Protocol in the Internet	C-7
2473	Generic Packet Tunneling in IPv6 Specification	C-7
2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	C-7
4271	A Border Gateway Protocol 4 (BGP-4)	C-7
4760	Multiprotocol Extensions for BGP-4	C-7
Notes:		
C/R-1: Meets only the dual-stack requirements of this RFC.		
C/R-2: Meets only the IPv6 formatting requirements of this RFC.		
R-3: Meets only the framing format aspects of RFC.		
R-4: Requirement covered in Section 6, Network Infrastructure End-to-End Performance.		
C-5: Condition is that product acts as a router.		
C-6: Applies only to MGs.		
C-7: Requirements apply only if the product acts as a CE-R.		
C/R-8: EI (softphones only).		
C-9: Condition is that product supports DHCP.		

Table 5.2-7. UC Information Assurance Security Devices (SD)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1981	Path MTU Discovery for IPv6	R
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C
2409	The Internet Key Exchange (IKE)	C
2460	Internet Protocol, Version 6 (v6) Specification	R-2
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	R-4
2710	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R
3162	RADIUS and IPv6	C
3986	Uniform Resource Identifier (URI): Generic Syntax	C
4007	IPv6 Scoped Address Architecture	R
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	R-1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	C
4302	IP Authentication Header	C

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4303	IP Encapsulating Security Payload (ESP)	C
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C
4861	Neighbor Discovery for IP version 6 (IPv6)	R
4862	IPv6 Stateless Address Autoconfiguration	C
5095	Deprecation of Type 0 Routing Headers in IPv6	R

Notes:

C/R-1: Meets only the dual-stack requirements of this RFC.

C/R-2: Meets only the IPv6 formatting requirements of this RFC.

R-3: Meets only the framing format aspects of RFC.

R-4: Requirement covered in Section 6, Network Infrastructure End-to-End Performance.

C-5: Condition is that product acts as a router.

C-6: Applies only to MGs.

C-7: Requirements apply only if the product acts as a CE-R.

C/R-8: EI (softphones only).