Changes to UCR 2008, Change 1, Section 5.3.5, IPv6 Requirements

SECTION	CORRECTION	EFFECTIVE DATE
5.3.5.1	Description of relationship between DISR Version 3.0 and the Change 1 is added with differences between the two documents defined.	No action required
5.3.5.2	New section added to define the system characteristics for Change 1.	No action required
5.3.5.3	New IPv6 Rules of Engagement (ROE)	Immediately
5.3.5.3.1	Note added re: Default IPv4 for Dual Stack end-points.	Immediately
5.3.5.3.1	Note added re: IA conditions for “IPv6-capable” nodes.	Immediately
5.3.5.3.2	Change LS requirement to Conditional from Required.	Immediately
5.3.5.3.3.8	Note added re: ULA.	Immediately
5.3.5.3.3.8.1	Note added re: the size of subnets that vendor’s products are required to support.	Immediately
5.3.5.3.3.9.2	Delete requirement on syntax of scoped address.	Immediately
5.3.5.3.4.10.2.5	Added note that logging may be impractical and the logging requirement would not apply.	Immediately
5.3.5.3.4.10.3	Added note that logging may be impractical and the logging requirement would not apply.	Immediately
5.3.5.3.5.11	Change LS requirement to Conditional from Required.	Immediately
5.3.5.3.5.11	Add note about “Neighbor Discovery” functions.	Immediately
5.3.5.3.5.11.2	Delete requirement for setting override flag bit.	Immediately
5.3.5.3.5.11.3	Change requirement to Required from Conditional for purposes of clarification.	Immediately
5.3.5.3.5.11.4	Change requirement to Required from Conditional for purposes of clarification.	Immediately
5.3.5.3.5.11.5	Change requirement to Required from Conditional for purposes of clarification.	Immediately
5.3.5.3.5.2.11.8	Delete Conditional requirement for EBC.	Immediately
5.3.5.3.5.2.11.8	Added note that logging may be impractical and the logging requirement would not apply.	Immediately
5.3.5.3.5.2.11.9	Delete Conditional requirement for EBC.	Immediately

SECTION	CORRECTION	EFFECTIVE DATE
5.3.5.3.6.12	Delete Required requirement for R, LS, EI (softphones only)	Immediately
5.3.5.3.6.12	Add note on definition of Host.	Immediately
5.3.5.3.6.12	Add note on DOD IPv6 Profile certification of UC EI.	Immediately
5.3.5.3.6.12	Add note on scopes of RFCs 2462 and 4862.	Immediately
5.3.5.3.6.12.1	Requirement is re-numbered from the same requirement as in UCR 2008.	No action required
5.3.5.3.6.12.1	Add note that the SLAAC function may be removed from the Operating System.	Immediately
5.3.5.3.6.12.1.1	Change requirement to Conditional from Required for EI, NA/SS, R, LS, EBC. Also, requirement is re-numbered from the same requirement as in UCR 2008.	Immediately
5.3.5.3.6.12.2	Change requirement to Conditional from Required for EI, NA/SS, R, LS, EBC. Also, requirement is re-numbered from the same requirement as in UCR 2008.	Immediately
5.3.5.3.6.12.2	Add note that requirement is derived from DOD IPv6 Profile.	No action required
5.3.5.3.6.12.2	Add note the requirement on restricting DAD parameter.	18 Month Rule
5.3.5.3.6.12.4.1	Delete Conditional requirement for EBC.	Immediately
5.3.5.3.6.(12.7)	Delete requirement for disabling manual configuration. This requirement is numbered in accordance with UCR 2008 as shown in the parentheses.	Immediately
5.3.5.3.7.14	Change requirement to Conditional from Required for LS.	Immediately
5.3.5.3.7.14.1	Change requirement to Conditional from Required for LS.	Immediately
5.3.5.3.7.14.2	Change requirement to Conditional from Required for LS.	Immediately
5.3.5.3.7.14.3	Change requirement to Conditional from Required for LS.	Immediately
5.3.5.3.7.14.4	Change requirement to Conditional from Required for LS.	Immediately
5.3.5.3.8.15.2	Delete reference to RFC 4302.	Immediately
5.3.5.3.8.15.2	Add reference to RFC 2404.	18 Month Rule
5.3.5.3.8.15.2	Add note about RFC 2404.	No action required
5.3.5.3.8.15.3	Add Required for R and Conditional for LS requirement for RFC 4552 Authentication Confidentiality for OSPFv3.	18 Month Rule
5.3.5.3.8.15a	Add Required for R and Conditional for LS requirement for RFC 5308.	18 Month Rule

SECTION	CORRECTION	EFFECTIVE DATE
5.3.5.3.8.15a.1	Add Required for R and Conditional for LS requirement for RFC 5304 and RFC 5310.	18 Month Rule
5.3.5.3.8.16	Add Conditional requirement for RFC 1772 and RFC 4271 for LS.	18 Month Rule
5.3.5.3.8.16.1	Add Conditional requirement for RFC 2545 for LS.	18 Month Rule
5.3.5.3.9.22.10	Added note that logging may be impractical and the logging requirement would not apply.	Immediately
5.3.5.3.9.22.11	Added note that logging may be impractical and the logging requirement would not apply.	Immediately
5.3.5.3.9.22.14.2	Delete this subtended requirement from UCR 2008.	Immediately
5.3.5.3.9.22.14.3	Subtended requirement re-worded for clarity.	Immediately
5.3.5.3.9.22.14.4	Delete this subtended requirement from UCR 2008.	Immediately
5.3.5.3.10.23	The Required requirement for SS, NA, EBC, R, and LS is changed to Conditional requirement for R and LS.	Immediately
5.3.5.3.10.23.1	The Required requirement for R is changed to Conditional requirement for R and LS.	Immediately
5.3.5.3.10.23.2	The Required requirement for R is changed to Conditional requirement for R and LS.	Immediately
5.3.5.3.10.23.3	The Required requirement for R is changed to Conditional requirement for R and LS.	Immediately
5.3.5.3.10.24	The Required requirement for SS, NA, EBC, R, and LS is changed to Conditional requirement for R and LS.	Immediately
5.3.5.3.10.25	The Required requirement for SS, NA, EBC, R, and LS is changed to Conditional requirement for R and LS.	Immediately
5.3.5.3.10.26	The Required requirement for SS, NA, EBC, R, and LS is changed to Conditional requirement for R and LS.	Immediately
5.3.5.3.10.27	The Required requirement for R is changed to Conditional requirement.	Immediately
5.3.5.3.10.29	The effective date for RFC 4295 has been delayed to UCR 2010 at the earliest.	Immediately
5.3.5.3.10.32	Note added that RFC 3596 has been deleted by DOD IPv6 Profile version 4.0.	Immediately
5.3.5.3.12.37	Add Required requirement to NA.	18 Month Rule

SECTION	CORRECTION	EFFECTIVE DATE
5.3.5.3.12.38.1	Add Note about starting AS SIP sessions.	Immediately
5.3.5.3.13.42	Add Conditional requirement for EI, NA/SS, EBC for RFC 3266.	18 Month Rule
5.3.5.3.14.47	Add Note clarifying the RADIUS applications.	Immediately
5.3.5.3.14.48	The effective date for RFC 3775 has been delayed to UCR 2010 at the earliest.	Immediately
5.3.5.3.14.48.1	The effective date for RFC 3775 has been delayed to UCR 2010 at the earliest.	Immediately
5.3.5.3.14.51	The Conditional requirement for LS has been deleted and the effective date for RFC 3963 has been delayed to UCR 2010 at the earliest.	Immediately Immediately
5.3.5.14.52 5.3.5.3.14.52.1	Delete RFC 5072 from this requirement. The Required requirement for LS has been changes to Conditional requirement for RFC 2474.	Immediately Immediately
5.3.5.3.14.55	The Conditional requirement for RFC 5072 has been included for implementation in UCR 2010 at the earliest.	18 Month Rule
Table 5.3.5-2 UC Host/Workstation (EI (Softphone))	This table summarizes the corrections identified above for UC Host/Workstations.	Various
Table 5.3.5-3 UC Simple Server (LSC, MFSS)/UC Network Appliance (MG)	This table summarizes the corrections identified above for UC Simple Server/Network Appliance.	Various
Table 5.3.5-4 UC Router (R)	This table summarizes the corrections identified above for UC Router.	Various
Table 5.3.5-5 LAN Switch (LS)	This table summarizes the corrections identified above for LAN Switch.	Various
Table 5.3.5-6 UC Information Assurance Device (EBC)	This table summarizes the corrections identified above for UC EBC.	Various

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF TABLES

TABLE **PAGE**

5.3.5 IPv6 Requirements

Section 5.3.5 describes the IPv6 requirements for SBU UC subsets provided by the DSN, DVS, circuit emulation, and/or short, latency sensitive C2 messages.

5.3.5.1 Introduction

The DISR baseline is updated to ensure that DoD Capabilities for building and buying IT products are based on a current and effective set of IT NSS standards. "DoD IPv6 Standard Profiles for IPv6-Capable Products" Version 3.0 (Ref: DoD memorandum, sub: Department of Defense IT Standards Registry Baseline Release 08-2.0, dated July 14, 2008.) is approved for distribution via the DISR for IPv6 for DoD IT equipments, including those for UC, providing a seamless integration of voice, video, and data applications. However, version 4.0 of the "DoD IPv6 Standard Profiles for IPv6-Capable Products" has been approved (Ref: DoD memorandum, sub: Department of Defense IT Standards Registry Baseline Release 09-2.0, dated July 30, 2009) and has already deprecated version 3.0. Unless specifically addressed in this section, all UCR products shall comply with version 4.0 of the "DoD IPv6 Standard Profiles for IPv6-Capable Products".

"DoD IPv6 Standard Profiles for IPv6-Capable Products" version 4.0 is included at the end of Section 5.3.5.

The sole exemption at this time is the VVoIP products defined in this section. The VVoIP products addressed by this exemption are defined in table 5.3.5-1 and the associated IPv6 requirements are based on the DoD IPv6 Profile, Version 3.0, with five exceptions as follows:

1. If the DoD IPv6 Profile, Version 4.0, has identified an Information Assurance risk that must be mitigated with a new requirement.

2. If the DoD IPv6 Profile, Version 4.0, has deleted a requirement, which is cited in Version 3.0.

3. If the DoD IPv6 Profile, Version 3.0, cites an RFC with SHOULD for the product class while the UCR cites a REQUIRED in this case.

4. If there is a UCR unique requirement that is levied on the UCR product and is not included in the DoD IPv6 Profile.

5. If the DoD IPv6 Profile, Version 3.0, cites a mandatory requirement for an RFC and the UCR cites a conditional requirement for the same RFC.

In Tables 5.3.5-2 to 5.3.5-6, these exceptions are identified with an asterisk ($*^{(n)}$) where *n* is one of these five exceptions.

In some cases, DoD IPv6 Profile, Version 3.0, will identify RFCs which will be deprecated. For example, in DoD IPv6 Profile, Version 4.0, RFC 2740 "Open Shortest Path First (OSPF) for IPv6," will be superseded by RFC 5340 in 2010. In the text of UCR 2008, Change 1, this case is denoted by: "RFC 2740 and RFC 5340 (UCR 2010)." This is to be interpreted to mean that:

1. Under UCR 2008, Change 1, the use of either RFC 2740 or RFC 5340 is acceptable.

2. Under UCR 2010, the requirement for RFC 5340 will be mandatory.

Also, UCR 2008, Change 1, includes some specific subtended requirements to the underlining RFCs for reasons of Information Assurance or Interoperability

If there are differences between this UCR and the "DoD IPv6 Standard Profiles for IPv6-Capable Products," Version 3.0, the UCR takes precedence over the DoD IPv6 Profile, version 3.0. However, for any appliance that is not defined in the UCR 2008, Change 1, the vendor is to follow DoD IPv6 Profile version 4.0.

The DoD IPv6 Profile includes Network Appliance and Simple Server, and notes that the distinction between them results in no real difference in requirements or testing. Hence, the product class is identified as "Net App or Simple Server." UCR 2008, Change 1, will follow the DoD IPv6 Profile guidance and identify the product class as "NS/SS."

For the DoD IPv6 Profile, Information Assurance devices include firewall, IDS, authentication server, security gateway, HAIPE, and VPN concentrator. The UC IPv6 requirements for an EBC are specified in the UCR. Guidance for UC IPv6 requirements for Intrusion Protection System (IPS), IDS, firewall, and VPN can be found in DoD IPv6 Profile, Version 4.0.

5.3.5.2 Characteristics

The system requirements specified in Section 5.3.2, Assured Services Requirements, are the minimum set of requirements necessary for the system to be IPv6-capable for Video and 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. The requirements are CY 2009 requirements unless specifically stated that the requirement applies to a different timeframe. The terms used within UCR are defined in Appendix A, Definitions, Abbreviations and Acronyms, and References.

Requirements may be designated as "Required," "Conditional, or "Objective" requirements. The terms are defined in UCR, Appendix A. To illustrate the use of "Conditional," the statement "**[Conditional: R, LS]** If the product supports mobile users, the product shall support the Mobile IP Management MIBs as described in RFC 4295 (UCR 2010)" should be read to mean that the requirement to support the sections of the RFC 4295 would not be mandatory for all IPv6 routers and LAN switches, but is mandatory for products that are intended to support mobile users.

The requirements defined in Section 5.3.2, Assured Services Requirements, are associated with the external interfaces of the UC products or network appliances (NAs). For defining each requirement, the terms "UC products" and "NAs" are shortened to "system." As shown in Figure 5.3.2-1, 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 ASLAN or the non-ASLAN. The primary interfaces associated with the IPv6 requirements are the signaling, AS-SIP, and bearer, SRTP interfaces.

LAN Switches can be either Layer 3 switches (with IP routing functions) or Layer 2 switches (without IP routing functions) within the ASLAN. In Section 5.3.5.3, Interim UC IPv6 Rules of Engagement, only Layer 3 LS must be IPv6 capable.

Finally, whenever a reference to a specific RFC appears in a UCR requirement, the specific language of the UCR requirement and its subtended requirements should be understood within the context of the RFC. The acronyms used for designating the appliances that a requirement pertains to are shown in Table 5.3.5-1, IPv6 Requirements for Products and/or Function.

Table 5.3.5-1. IPv6 Requirements for Products and/or Function

UC PRODUCT OR FUNCTION	DOD IPv6 PROFILE CATEGORY	UCR IPv6 REQUIREMENTS (1, 2, 3)
Multifunction Softswitch (MFSS)	Network Appliance or Simple Server (NA/SS)	The MFSS/Call Control Agent (CCA) application in conjunction with the Voice and Video over IP (VVoIP) End Instrument (EI) and Media Gateway (MG)(4) must be IPv6-capable. Other applications within this APL product have a conditional requirement to be IPv6-capable if the IP packets remain internal to the product.
Local Session Controller (LSC)	NA/SS	The LSC/CCA application in conjunction with the VVoIP EI and MG(4) must be IPv6-capable. Other applications in the APL product have a conditional requirement to be IPv6-capable.
Video Telephony Unit (VTU)	NA/SS	If the VTU has an IP interface, the VTU must be IPv6-capable.
Multipoint Control Unit (MCU)	NA/SS	If the MCU has an IP interface, the MCU must be IPv6-capable.

UC PRODUCT OR FUNCTION	DOD IPv6 PROFILE CATEGORY	UCR IPv6 REQUIREMENTS (1, 2, 3)
End Instrument (EI)	NA/SS	The EI in conjunction with the CCA application must be IPv6-capable. This requirement is applicable for EIs manufactured after January 2009. Softphones and soft videophones have a conditional requirement for IPv6.
Customer Premise Equipment (CPE)	NA/SS	With exception of EIs, the CPE have a conditional requirement for IPv6 capability.
Network Element (NE)	NA/SS	Conditional requirement for IPv6.
Echo Canceller (EC)	NA/SS	Conditional requirement for IPv6.
Integrated Access Switch (IAS)	NA/SS	Conditional requirement for IPv6.
Conference Bridge (external) (CB)	NA/SS	Conditional requirement for IPv6.
H.323/H.320 Gateway (GW)	NA/SS	Conditional requirement for IPv6.
Edge Boundary Controller (EBC)	Information Assurance Device	Must be IPv6-capable.
Intrusion Protection Systems (IPS) and Intrusion Detection Systems (IDS)	Information Assurance Device	Must be capable of inspecting both IPv4 and IPv6 packets.
Firewalls (FW)	Information Assurance Device	Must be IPv6-capable.
VPN Concentrator (VPN)	Information Assurance Device	Must be IPv6-capable.
LAN Switch (LS)	Layer 3 Switch	Must be IPv6-capable.
Router (R)	Router	Must be IPv6-capable.

Notes:
1. The terms “Conditional requirement for IPv6” and “Other applications within the APL product have a conditional requirement to be IPv6-capable” effectively mean that the IPv6-capable features for the indicated UCR IPv6 application is optional and not required for listing on the UC APL.
2. While there is a requirement to manage IPv6 networks, the NM may be done using IPv4. Thus, NM is not included in this list.
3. Components within the UC products for which the IP packets remain internal to the SUT are not required to be IPv6-capable at this time, such as voice mail systems. In these cases, the resulting product can only be fielded within a B/P/C/S boundary. End instruments are required to be IPv6-capable regardless of placement within the SUT as indicated in this table. The UC APL certification shall reflect conditions under which the product was certified. The product is to be fielded within B/P/C/S boundaries.
4. The MG is only required to be IPv6-capable if it has an external IP interface to the SUT. In these cases, the resulting product can only be fielded within a B/P/C/S boundary. The UC APL certification shall reflect conditions under which the product was certified.

5.3.5.3 Interim UC IPv6 Rules of Engagement

The purpose of this section is to provide interim policy and guidance/ROE to be used by the Government and industry to achieve UC APL status for IPv6-capable products. This set of IPv6 ROE applies to all industry vendors seeking to place products on the DoD UC APL. The UCCO and DISA JITC shall enforce this guidance in test and certification of vendor products that have IP capabilities. This guidance is effective immediately and supersedes any previous ROE Versions that have been issued.

5.3.5.3.1 Definitions

These definitions are derived from DoD Deputy CIO Memorandum "DoD IPv6 Definitions."

1. IPv6 Capable Products. Products (whether developed by commercial vendor or the government) that can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/IPv6 environments.

2. System Under Test (SUT). The inclusive components required to test a UC product for APL certification. Examples of a SUT include VoIP system components (e.g., LSC and gateway), LAN components (e.g., routers and Ethernet switches), and EIs.

3. IPv6-Capable Networks. Networks that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks and systems, where those networks and systems may be operating with only IPv4, only IPv6, or both IPv4 and IPv6. An IPv6-capable network shall be ready to have IPv6 enabled for operational use, when mission need or business case dictates. Specifically, an IPv6-capable network must:

    a. Use IPv6-capable products.

    b. Accommodate IPv6 in network infrastructures, services, and management tools and applications.

    c. Conform to DoD and NSA-developed IPv6 network security implementation guidance.

    d. Manage, administer, and resolve IPv6 addresses in compliance with the DoD IPv6 Address Plan when enabled.

4. IPv6-Enabled Network. An IP network that is supporting operational IPv6 traffic through the network, E2E.

5.3.5.3.2 IPv6 Rules of Engagement

1. IPv6 Requirements. Detailed IPv6 requirements for UC products and/or functions are provided in this section of the UCR. Table 5.3.5-1, IPv6 Requirements for Products and/or Function, provides a high-level listing of UC products or functions, DoD IPv6 Profile categories, and UCR IPv6 requirements to be considered IPv6-capable.

2. UC APL Listing.

   a. The DoD no longer supports standalone IPv6 product certification testing. For products identified in the UCR, IPv6 requirements will be validated in conjunction with the larger Interoperability certification and Information Assurance testing that is conducted on the product for listing on the UC APL.

   b. Products that have been placed on the DoD UC APL as a result of vendor commitments, via an LOC, to be IPv6 capable (or other IPv6-related commitments) will be removed from the APL, and may be subject to other actions, if the vendor does not deliver on the commitment within 12 months of the LOC.

5.3.5.4 Product Requirements

1. **[Required: NA/SS, R, EBC] [Conditional: EI]** The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213.

   [Conditional: LS] If the LS also supports a routing function, the product shall support RFC 4213.

   NOTE: The tunnel requirements are only associated 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.

   1.1 **[Required: EI, NA/SS, R, LS, EBC]** Dual stack end points or Call Control Agents shall be configured to choose IPv4 over IPv6.

   NOTE: Most commercial vendors can configure their equipment to choose IPv4 or IPv6. JITC testing preference, for IPv6 features, is to test the equipment configured for IPv6 to insure that it can dynamically negotiate with IPv4 only end points.

   1.2 **[Required: EI, NA/SS, R, LS, EBC]** All nodes that are “IPv6-capable” shall be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a risk management strategy. This includes the stateless auto configuration of link-local addresses.

[Conditional: EI CY 2008-2012] The EIs are allowed to use alternative mechanisms (e.g., translation and tunneling) between CY 2008 and CY 2012 as long as performance, Interoperability, and Information Assurance requirements are met.

NOTE: Translation based on RFC 2766, Network Address Translation – Protocol Translation (NAT-PT) is no longer supported in the IETF community and has been rendered *Historic* by the publication of RFC 4966 primarily for security concerns.

1.3 **[Conditional: R, LS]** If the product supports routing functions, the product shall support the manual tunnel requirements as described in RFC 4213.

2. **[Required: EI, NA/SS, R, EBC]** 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, the product shall support RFC 2460 and updated by RFC 5095.

3. **[Required: EI, NA/SS, R, LS, EBC]** 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.

5.3.5.4.1 Maximum Transmission Unit

4. **[Required: EI (Softphone Only), R, EBC]** The product shall support Path Maximum Transmission Unit (MTU) Discovery (RFC 1981). **[Conditional: LS]** If the LS supports a routing function, the product shall support RFC 1981.

5. **[Required: EI, NA/SS, R, LS, EBC]** The product shall support a minimum MTU of 1280 bytes (RFC 2460 and updated by RFC 5095).

   NOTE: Guidance on MTU requirements and settings can be found in Section 5.3.3.10.1.2, Layer 2 Data Link Layer.

6. **[Conditional: EI, NA/SS, R, LS, EBC]** 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, the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet.

   NOTE: This is to mitigate an attack where the path MTU is adequate, but the “Packet Too Big” messages are used to make the packet so small it is inefficient.

5.3.5.4.2 Flow Label

7. **[Required: EI, NA/SS, EBC]** The product shall not use the Flow Label field as described in RFC 2460.

   7.1 **[Required: EI, NA/SS, EBC]** The product shall be capable of setting the Flow Label field to zero when originating a packet.

   7.2 **[Required: NA/SS, EBC]** The product shall not modify the Flow Label field when forwarding packets.

   7.3 **[Required: EI, NA/SS, EBC]** The product shall be capable of ignoring the Flow Label field when receiving packets.

5.3.5.4.3 Address

8. **[Required: EI, NA/SS, R, LS, EBC]** The product shall support the IPv6 Addressing Architecture as described in RFC 4291.

   NOTE: According to "DoD IPv6 Standard Profiles For IPv6-capable Products-Supplemental Guidance" version 3.0, the use of "IPv4-mapped" addresses "on-the-wire" is discouraged due to security risks raised by inherent ambiguities.

   NOTE: As noted in NIST SP500-267 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) [RFC4193] mechanism has been designed to fulfill a similar requirement. While Private Addresses are widely used in IPv4 networks, the generalized use and support of ULAs in IPv6 is 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.

   8.1 An end site is defined as an end-user (subscriber) edge network domain that requires multiple subnets/64 as defined in Section 5.1, End-Site Definition of DoD IPv6 Address Plan. Therefore, vendors will not be required to support anything greater than /64, such as /116 or /126 subnet.

9. **[Required: EI, NA/SS, R, LS, EBC]** The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.

   9.1 **[Conditional: EI, NA/ SS, R, LS, EBC]** If a scoped address (RFC 4007) is used, the product shall use a scope index value of zero when the default zone is intended.

9.2 Reserved.

5.3.5.4.4 DHCP

10. **[Required: IE] [Conditional: NA/SS, R]** If DHCP is supported within an IPv6 environment, it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315.

[Conditional: LS] If the LS also supports a routing function, the product shall support RFC 3315.

NOTE: Section 5.4, Information Assurance, requires that the voice or video DHCP servers are not to be located on the same physical appliance as the voice or video LAN switches and routers in accordance with the STIGs. Also, the VoIP STIG requires (in VoIP 0082) separate DHCP servers for (1) the telephone system in the phone VLAN(s) and (2) the data devices (PCs) in the data VLAN(s).

NOTE: There is no requirement that separate DHCP servers be used for IPv4 and for IPv6.

10.1 **[Conditional: EI, NA/SS]** If the product is a DHCPv6 client, 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).

10.2 **[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.

10.2.1 **[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, the client shall continue with a client-initiated message exchange by sending a Request message.

10.2.2 **[Required: EI – Conditional: NA/SS]** If the product is a DHCPv6 client and the DHCPv6 solicitation message exchange fails, 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.

10.2.3 **[Required: EI – Conditional: NA/SS]** If the product is a DHCPv6 client and it sends an Information-Request message, it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server.

10.2.4 **[Required: EI – Conditional: NA/SS]** If the product is a DHCPv6 client, it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server before transmitting packets using that address for itself.

10.2.5 **[Required: EI – Conditional: NA/SS]** If the product is a DHCPv6 client, 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).

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

NOTE: This requirement assumes authentication is used as described in RFC 3118 (and extended in RFC 3315) but does not require authentication.

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

5.3.5.4.5 Neighbor Discovery

11. **[Required: EI, NA/SS, R, EBC]** The product shall support Neighbor Discovery for IPv6 as described in RFC 2461 and RFC 4861 (UCR 2010).

[Conditional: LS] If the LS also supports a routing function, the product shall support RFC 2461 and RFC 4861 (UCR 2010).

NOTE: For ICMPv6 Neighbor Discovery functions specified by RFC 2461 (Router Advertisement/Solicitation, Neighbor Advertisement/Solicitation, and Redirect) the preferred DSCP for ICMPv6 neighbor discovery related packets is DSCP 0, which is defined in Section 5.3.3, Network Infrastructure End-to-End Performance Requirements for Granular Service Class of Best Effort.

11.1 **[Required: NA/SS, R, LS, EBC]** The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements.

11.2 Reserved.

11.3 **[Required: EI, NA/SS, R, LS, EBC]** 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.

11.4 **[Required: EI, NA/SS, R, LS, EBC]** 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.

11.5 **[Required: EI, NA/SS, R, LS, EBC]** When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache.

5.3.5.4.5.1 Redirect Messages

11.6 **[Required: EI, NA/SS, EBC]** The product shall support the ability to configure the product to ignore Redirect messages.

11.7 **[Required: EI, NA/SS, EBC]** 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.

11.7.1 **[Conditional: EI, NA/SS, EBC]** If "Redirect" messages are allowed, the product shall update its destination cache in accordance with the validated Redirect message.

11.7.2 **[Conditional: EI, NA/SS, EBC]** If the valid "Redirect" message is allowed and no entry exists in the destination cache, the product shall create an entry.

5.3.5.4.5.2 Router Advertisements

11.8 **[Required: R] [Conditional: LS]** If the product supports routing functions, 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).

11.8.1 **[Required: EI, NA/SS, EBC]** The product shall prefer routers that are reachable over routers whose reachability is suspect or unknown.

11.8.2 Reserved.

11.9 **[Required: R] [Conditional: LS]** If the product supports routing functions, the product shall include the MTU value in the router advertisement message for all links in accordance with RFC 2461 and RFC 4861 (UCR 2010).

5.3.5.4.6 Stateless Address Autoconfiguration and Manual Address Assignment

12. **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports stateless IP address autoconfiguration including those provided for the commercial market, the product shall support IPv6 Stateless Address Autoconfiguration (SLAAC) for interfaces supporting UC functions in accordance with RFC 2462 and RFC 4862 (UCR 2010).

NOTE: "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: 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.

NOTE: 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.

12.1 **[Conditional: SS, NA, EBC, EI]** If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the function to be enabled and disabled.

NOTE: The objective of this requirement is to prevent a product from using stateless auto configuration.

NOTE: An alternative to the configurable parameter, the IPv6 SLAAC functions may be removed from the operating system of the IPv6 node.

12.1.1 **[Conditional: EI, NA/ SS, R, LS, EBC]** If the product supports IPv6 SLAAC, the product shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless autoconfiguration.

NOTE: The objective of this requirement is to prevent a product from using stateless auto configuration.

12.2 [**Conditional: EI, NS/NA, R, LS, EBC]** If the product supports stateless IP address autoconfiguration including those provided for the commercial market, the DAD shall be disabled in accordance with RFC 2462 and RFC 4862 (UCR 2010).

12.3 **[Required: EI, NA/SS, R, LS, EBC]** The product shall support manual assignment of IPv6 addresses.

12.4 **[Required: EI]** The product shall support stateful autoconfiguration (i.e., ManagedFlag=TRUE).

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

12.4.1 **[Required: R] [Conditional: LS]** If the product provides routing functions, 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.

12.5 **[Conditional: EI]** If the product supports a subtended appliance behind it, 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.

12.6. **[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, IPSec-capable products shall support privacy extensions for stateless address autoconfiguration as defined in RFC 3041 and RFC 4941 (UCR 2010).

13. Reserved.

5.3.5.4.7 Internet Control Message Protocol

14 **[Required: EI, NA/SS, R, EBC]** The product shall support the ICMPv6 as described in RFC 4443. **[Conditional: LS]** If the LS supports a routing function, the product shall support RFC 4443.

14.1 **[Required: NA/SS, R, EBC]** The product shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages.

[Conditional: LS] If the LS supports a routing function, subtended requirement 14.1 applies.

14.2 **[Required: NA/SS, R, EBC]** 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.

[Conditional: LS] If the LS supports a routing function, subtended Requirement 14.2 applies.

14.3 **[Required: EI, NA/SS, R, EBC]** 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.

[Conditional: LS] If the LS supports a routing function, subtended Requirement 14.3 applies.

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

14.4 **[Required: EI, NA/SS, R, EBC]** 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.

[Conditional: LS] If the LS supports a routing function, subtended Requirement 14.4 applies.

5.3.5.4.8 Routing Functions

15. **[Required: R] [Conditional: LS]** If the product supports routing functions, the product shall support the OSPF for IPv6 as described in RFC 2740.

    15.1 **[Required: R] [Conditional: LS]** If the product supports routing functions, the product shall support securing OSPF with IPSec as described for other IPSec instances in Section 5.4, Information Assurance.

    15.2. **[Required: R] [Conditional: LS]** If the product supports routing functions, the product shall support router-to-router integrity using the IP Authentication Header with HMAC-SHA1-96 within ESP and 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 IETF is encouraging the standardization of HMAC-SHA-256 to ensure an orderly transition to a more secure MAC.

    15.3 **[Required: R] [Conditional: LS]** If the product supports interior routing functions of OSPFv3, the product shall support RFC 4552.

15a. **[Required: R] [Conditional: LS]** If the product supports the Intermediate System to Intermediate System (IS-IS) routing protocol used in DoD backbone networks, the product shall support the IS-IS for IPv6 as described in RFC 5308 (UCR 2010).

    15a.1 **[Required: R] [Conditional: LS]** If the product supports IS-IS routing architecture (for IPv6-only or dual-stack operation) the product shall support RFC 5304 (UCR 2010) and RFC 5310 (UCR 2010).

    NOTE: IS-IS implementers should monitor further specification of ancillary features in the IETF ISIS Working Group, including http://tools.ietf.org/html/draft-ietf-isis-ipv6-te-06 on traffic engineering.

16. **[Conditional: R, LS]** If the product acts as a CE Router, the product shall support the use of BGP as described in RFC 1772 and RFC 4271.

    16.1. **[Conditional: R, LS]** If the product acts as a CE Router, the product shall support the use of BGP4 multiprotocol extensions for IPv6 inter-domain routing (RFC 2545).

    NOTE: The requirement to support BGP4 is in Section 5.3.3, Wide Area Network General System Requirements.

17. [**Conditional: R, LS]** If the product acts as a CE Router, the product shall support multiprotocol extensions for BGP4 in RFC 2858 and RFC 4760 (UCR 2010).

    NOTE: The requirement to support BGP4 is in Section 5.3.3, Wide Area Network General System Requirements.

18. [**Conditional: R]** If the product acts as a CE Router, the product shall support the Generic Routing Encapsulation (GRE) as described in RFC 2784.

19. [**Conditional: R]** If the product acts as a CE Router, the product shall support the Generic Packet Tunneling in IPv6 Specification as described in RFC 2473.

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

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

    NOTE: The CY 2008 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.

    20.1 **[Required: EI (Softphone Only), R] [Conditional: LS]** If the product supports MLD process as described in RFC 2710 and extended in RFC 3810, the product shall support 2711.

21. **[Required: EI, NA/SS, EBC]** 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.

5.3.5.4.9 IP Security

22. **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If the product uses IPSec, the product shall support the Security Architecture for the IP RFC 2401 and RFC 4301 (UCR 2010).

    NOTE: In CY 2009, RFC 2401 (and its related RFCs) is the Threshold requirement as described in Section 5.4, Information Assurance. In addition, the interfaces required to use IPSec are defined in Section 5.4, Information Assurance.

22.1 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support binding of a security association (SA) with a particular context.

22.2 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, 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.

22.3 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall not support the mixing of IPv4 and IPv6 in a security association.

22.4 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, 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, describes a scenario where this could occur.

22.5 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall be capable of correlating the DSCP for a VVoIP stream to the security association in accordance with Section 5.3.2, Assured Services Requirements and Section 5.3.3, Network Infrastructure E2E Performance Requirements, plain text DSCP plan.

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

22.7 **[Required: EI (Softphone Only, R)] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, 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.

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

22.8 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC**] If RFC 4301 is supported, the product shall be capable of enabling or disabling the propagation of the Explicit Congestion Notification (ECN) bits.

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

22.10 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** 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, 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).

22.11 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product should include a management control to allow an administrator to enable or disable the ability of the product to send an Internet Key Exchange (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).

22.12 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the Encapsulating Security Payload (ESP) Protocol in accordance with RFC 4303.

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

22.12.2 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4303 is supported, 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.

22.13. **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the cryptographic algorithms as defined in RFC 4308 for Suite Virtual Private Network (VPN)-B.

22.13.1. **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the use of AES-CBC with 128-bits keys for encryption.

22.13.2. **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the use of HMAC-SHA1-96 for (Threshold) and AES-XCBC-MAC-96 (UCR 2010).

22.14. **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support IKE version 1 (IKEv1) (Threshold) as defined in RFC 2409, and IKE version 2 (IKEv2) (UCR 2010) as defined in RFC 4306 (UCR 2010).

NOTE: The IKEv1 requirements are found in Section 5.4, Information Assurance.

22.14.1. **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, it shall be capable of configuring the maximum User Datagram Protocol (UDP) message size.

22.14.2 Reserved.

22.14.3 **[Conditional: EI, NA/SS, R, LS, EBC]** To prevent a 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.

22.14.4 Reserved.

22.14.5 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall reject initial IKE messages unless they contain a Notify Payload of type COOKIE.

22.14.6 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall close an SA instead of rekeying when its lifetime expires if there has been no traffic since the last rekey.

22.14.7 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall not use the Extensible Authentication Protocol (EAP) method for IKE authentication.

22.14.8 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall limit the frequency to which it responds to messages on UDP port 500 or 4500 when outside the context of a security association known to it.

22.14.9 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall not support temporary IP addresses or respond to such requests.

22.14.10 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall support the IKEv2 cryptographic algorithms defined in RFC 4307.

22.14.11 **[Conditional: EI, NA/SS, R, LS, EBC]** If the product supports IKEv2, the product shall support the VPN-B Suite as defined in RFC 4308 and RFC 4869 (UCR 2010).

- Encryption – AES with 128-bit keys in CBC Mode
- Pseudo-random function – AES-XCBC-PRF-128
- Integrity – AES-XCBC-MAC-96
- Diffie-Hellman Group – 2048-bit MODP
- Rekeying of Phase 2 or the CREATE_CHILD_SA shall be supported by both parties. The initiator of the exchange may include a Diffie-Hellman key; if included, it shall be a type 2048 – bit MODP. If the initiator of the exchange includes a Diffie-Hellman key, the responder shall include a Diffie-Hellman key and it shall also be a type 2048-bit MODP.

NOTE: RFC 4869 Suite B Cryptographic Suites for IPSec identifies four new cryptographic user interface suites based on implementations of the U.S. NSA's Suite B algorithms.

22.15 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, 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.

22.16 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the ISAKMP as defined in RFC 2408.

22.17 **[Required: R] [Conditional: EI, NA/SS, LS, EBC]** If the product supports the IPSec Authentication Header Mode, the product shall support the IP Authentication Header (AH) as defined in RFC 4302.

22.18 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support manual keying of IPSec.

22.19 **[Required: EI (Softphone Only), R] [Conditional: EI, NA/SS, LS, EBC]** If RFC 4301 is supported, the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined in RFC 4305 and RFC 4835 (UCR 2010).

22.20 Reserved.

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

5.3.5.4.10 Network Management

23. **[Conditional: R, LS]** If IPv6-compatible nodes are managed via SNMP, 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 5.3.2.17.3.1.5, SNMP Version 2 and Version 3 Format Alarm messages, and Section 5.4, Information Assurance Requirements.

NOTE: By calendar year (CY) 2011 nodes managed via SNMPv3 are required to do so using IPv6 transport.

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

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

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

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

25. **[Conditional: R, LS]** If IPv6-compatible nodes are managed via SNMP, the product shall support the TCP MIBs as defined in RFC 4022.

26. **[Conditional: R, LS]** If IPv6-compatible nodes are managed via SNMP, the product shall support the UDP MIBs as defined in RFC 4113.

27. **[Conditional: R, LS]** If the product performs routing functions and tunneling functions, the product shall support IP tunnel MIBs as described in RFC 4087.

28. **[Conditional: R, LS]** If the product performs routing functions and is managed by SNMP, the product shall support the IP Forwarding MIB as defined in RFC 4292.

29. **[Conditional: R, LS]** If the product supports mobile users, the product shall support the Mobile IP Management MIBs as described in RFC 4295 (UCR 2010).

30. **[Conditional: R, LS]** If IPv6-capable Nodes are managed via SNMP implementation and support routing functions, the product shall support the textual conventions for IPv6 flow labels as described in RFC 3595.

31. **[Conditional: R, LS]** If the product supports routing functions and if the IPSec policy database is configured through SNMPv3, the product shall support RFC 4807.

32. **[Required: EI (Softphone only)] [Conditional: EI, NA/SS, R, LS, EBC]** If the product uses URIs, the product shall use the URI syntax described in RFC 3986.

NOTE: According to "DoD IPv6 Standard Profiles For IPv6-capable Products-Supplemental Guidance" Version 4.0, RFC 3986 is not a testable requirement for host or server products and has been deleted from the product class requirements of that document.

33. **[Conditional: EI, NA/SS]** If the product uses the DNS resolver, the product shall conform to RFC 3596 for DNS queries.

    NOTE: DNS is primarily used for NM applications.

5.3.5.4.11 Traffic Engineering

34. **[Required: NA/SS, R, LS, EBC]** 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 SRTCP overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.

35. **[Required: R, LS]** The number of VoIP subscribers per link size for IPv6 is the same as for IPv4 and is defined in Section 5.3.1, Assured Services Local Area Network Infrastructure Product Requirements.

36. **[Required: R, LS]** The number of video subscribers per link size for IPv6 is the same as for IPv4 and is defined in Section 5.3.1, Assured Services Local Area Network Infrastructure.

5.3.5.4.12 IP Version Negotiation

37. **[Required: NA/SS, EBC]** 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, the appliance will forward it as an IPv6 packet. If the packet was received as an IPv4 packet, 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. This requirement may be waived from CY 2008 –CY 2012 to support IPv4 or IPv6 only EIs.

38. **[Required: EI, NA/SS]** The product shall use the Alternative Network Address Types (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091 when establishing media streams from dual-stacked appliances for AS-SIP signaled sessions.

38.1 **[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.

38.2 **[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.

38.3 **[Required: EI]** Dual-stacked products shall include the IPv4 and IPv6 addresses within the SDP of the SIP INVITE message when the INVITE contains the SDP.

5.3.5.4.13 AS-SIP IPv6 Unique Requirements

39. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is a unicast address, 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.

40. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP, 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

41. **[Conditional: EI, NA/SS, EBC]** 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), the product shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.

42. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP and the <addrtype> is IPv6, the product shall support the use of RFC 3266 and RFC 4566 [UCR 2010] for IPv6 in SDP as described in Section 5.3.4, AS-SIP Requirements.

43. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is an IPv6 multicast group address, 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.

44. **[Conditional: EI, NA/SS, EBC]** If the product is using AS-SIP, 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.

45. **[Required: EBC]** The product shall be able to provide topology hiding (e.g., NAT) for IPv6 packets as described in Section 5.4, Information Assurance Requirements.

46. **[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.

5.3.5.4.14 Miscellaneous Requirements

47. **[Conditional: R, EBC]** If the product supports Remote Authentication Dial In User Service (RADIUS) authentication, the product shall support RADIUS as defined in RFC 3162.

    [Conditional: LS] If the LS supports a routing function, the product shall support RFC 3162.

    NOTE: RFC 3162 only defines 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: 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.

48. **[Conditional: EI (Softphone Only)]** If the product supports Mobile IP Version 6 (MIPv6), the product shall provide mobility support as defined in RFC 3775 (UCR 2010).

48.1. **[Conditional: R]** If the product acts as a home agent, the product shall provide mobility support as defined in RFC 3775 (UCR 2010).

49. **[Conditional: EI (Softphone Only), R]** If the product supports MIPv6, the product shall provide a secure manner to signal between mobile nodes and home agents as described in RFC 3776 (UCR 2010) and RFC 4877 (UCR 2010).

50. Reserved.

51. **[Conditional: R]** If the product supports network mobility (NEMO), the product shall support the function as defined in RFC 3963 (UCR 2010).

52. **[Required: EI, NA/SS, R, EBC]** The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 5.3.2, Assured Services Requirements, and Section 5.3.3, Network Infrastructure E2E Performance Requirements, plain text DSCP plan.

52.1 **[Conditional: LS]** If the LS supports a routing function, the product shall support RFC 2474.

53. **[Conditional: EI (Softphone Only), R]** If the product acts as an IPv6 tunnel broker, the product shall support the function as defined in RFC 3053.

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

55. **[Conditional: R]** If the product supports the Point-to-Point Protocol (PPP), the product shall support PPP as described in RFC 2472 and RFC 5072 (UCR 2010).

5.3.5.5 Mapping of RFCs to UC Profile Categories

In Section 5.3.5.1, Introduction, the DoD IPv6 Profile, Version 3.0, five exceptions are listed. Tables 5.3.5.2 through 5.3.5.6 identify these exceptions with an asterisk ($*^{(n)}$), where *n* is one of the five exceptions.

Table 5.3.5-2. UC Host/Workstation (EI (Softphone))

RFC NUMBER	RFC TITLE	REQUIRED – R ** CONDITIONAL – C
1981	Path MTU Discovery for IP Version 6	R-8
2401	Security Architecture for the Internet Protocol	R-8; C
2407	The Internet IP Security Domain of Interpretation for ISAKMP	R-8; C

RFC NUMBER	RFC TITLE	REQUIRED – R ** CONDITIONAL – 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
2461	Neighbor Discovery for IP Version 6 (IPv6)	R
2462	IPv6 Stateless Address Autoconfiguration	C
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*(3)-4
2710	Multicast Listener Discovery (MLD) for IPv6	R-8; R
2711	IPv6 Router Alert Option	R*(1)-8
3041	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	C-8
3053	IPv6 Tunnel Broker	C*(3)-8
3266	Support for IPv6 in Session Description Protocol (SDP)	C*(4)
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3484	Default Address Selection for Internet Protocol Version 6 (IPv6)	R*(3)-8
3596	DNS Extensions to Support IPv6	C*(3)
3775	Mobility Support in IPv6	C-8, C-10
3776	Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	C-8, C-10
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R-8
3986	Uniform Resource Identifier (URI): Generic Syntax	R*(2)-8; C*(2)
4007	IPv6 Scoped Address Architecture	R
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R*(4)
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R*(4)
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	R-8; C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	C -1
4291	IP Version 6 Addressing Architecture	R
4301	Security Architecture for the Internet Protocol	R-8, R-10; C-10
4302	IP Authentication Header	C*(3)
4303	IP Encapsulating Security Payload (ESP)	R-8; C
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R-8; C
4306	Internet Key Exchange (IKEv2) Protocol	R-8, R-10; C-10
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C
4308	Cryptographic Suites for IPSec	R*(1)-8, C*(1)

RFC NUMBER	RFC TITLE	REQUIRED – R ** CONDITIONAL – C
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C*(4)-10
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R-8, R-10; C-10
4861	Neighbor Discovery for IP Version 6 (IPv6)	R-10
4862	IPv6 Stateless Address Autoconfiguration	C-10
4869	Suite B Cryptographic Suites for IPSec	C-10
4877	Mobile IPv6 Operation with IKEv2 and the Revised IPSec Architecture	C-8, C-10
4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	C-8, C-10
5095	Deprecation of Type 0 Routing Headers in IPv6	R*(1)

NOTES:
C/R-1: Only meets the dual-stack requirements of this RFC.
R-2: Only meets IPv6 formatting requirements of this RFC.
R-3: Only meets framing format aspects of RFC.
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements
C-5: Condition is that product acts as a router.
C-6: Only applies to MGs.
C-7: Requirements only apply if the product acts as an edge router.
C/R-8: EI (softphones only).
C/R-10: Conditional/Objective Requirement for UCR 2010.
*(n): Deviation from DoD IPv6 Profile, Version 3.0, Appendix C. Key to "n" values is described in Section 5.3.5.1, Introduction.
** 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 5.3.5-3. UC Simple Server (LSC, MFSS)/ UC Network Appliance (MG)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
2401	Security Architecture for the Internet Protocol	C*(3)
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C*(3)
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C*(3)
2409	The Internet Key Exchange (IKE)	C*(3)
2460	Internet Protocol, Version 6 (IPv6) Specification	R-2
2461	Neighbor Discovery for IP Version 6 (IPv6)	R
2462	IPv6 Stateless Address Autoconfiguration	C
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*(3)-4
2710	Multicast Listener Discovery (MLD) for IPv6	R
3266	Support for IPv6 in Session Description Protocol (SDP)	C*(4)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C
3596	DNS Extensions to Support IPv6	C*(3)
3986	Uniform Resource Identifier (URI): Generic Syntax	C*(2)
4007	IPv6 Scoped Address Architecture	R
4091	The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework	R*(4)
4092	Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)	R*(4)
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C*(3)
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*(3)-10
4302	IP Authentication Header	C*(3)
4303	IP Encapsulating Security Payload (ESP)	C*(3)
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C*(3)
4306	Internet Key Exchange (IKEv2) Protocol	C*(3)-10
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C*(3)
4308	Cryptographic Suites for IPSec	C*(1, 3)
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C*(4)-10
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C*(3)-10
4861	Neighbor Discovery for IP Version 6 (IPv6)	R-10
4862	IPv6 Stateless Address Autoconfiguration	C-10
4869	Suite B Cryptographic Suites for IPSec	C*(3)-10
5095	Deprecation of Type 0 Routing Headers in IPv6	R*(1)

NOTES:
R-1: Only meets the dual-stack requirements of this RFC.
R-2: Only meets IPv6 formatting requirements of this RFC.
R-3: Only meets framing format aspects of RFC.
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.
C-5: Condition is that product acts as a router.
C-6: Only applies to MGs.
C-7: Requirements only apply if the product acts as an edge router.
C/R-8: EI (softphones only).
C/R-10: Conditional/Objective Requirement for UCR 2010.
*(n): Deviation from DoD IPv6 Profile, version 3.0, Appendix C. Key to "n" values is described in Section 5.3.5.1, Introduction.

Table 5.3.5-4. 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
2401	Security Architecture for the Internet Protocol	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
2461	Neighbor Discovery for IP Version 6 (IPv6)	R
2462	IPv6 Stateless Address Autoconfiguration	C
2464	Transmission of IPv6 Packets over Ethernet Networks	R-3
2472	IP Version 6 over PPP	C
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
2710	Multicast Listener Discovery (MLD) for IPv6	R
2711	IPv6 Router Alert Option	R*(1)
2740	OSPF for IPv6	R
2784	Generic Router Encapsulation (GRE)	C-7
2858	Multiprotocol Extensions for BGP-4	C-7
3053	IPv6 Tunnel Broker	C
3162	RADIUS and IPv6	C*(3)
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
3595	Textual Conventions for IPv6 Flow Label	C
3775	Mobility Support in IPv6	C*(3)-10
3776	Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	C-10
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	R
3963	Network Mobility (NEMO) Basic Support Protocol	C-10
3986	Uniform Resource Identifier (URI): Generic Syntax	C*(2)
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	C
4087	IP Tunnel MIB	C*(3)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – 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*(3)
4291	IP Version 6 Addressing Architecture	R
4292	IP Forwarding MIB	C
4293	Management Information Base for the Internet Protocol (IP)	C
4295	Mobile IP Management MIB	C-10
4301	Security Architecture for the Internet Protocol	R-10
4302	IP Authentication Header	R
4303	IP Encapsulating Security Payload (ESP)	R
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R
4306	Internet Key Exchange (IKEv2) Protocol	R-10
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C
4308	Cryptographic Suites for IPSec	R*(1)
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-10
4807	IPSec Security Policy Database Configuration MIB	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	R-10
4861	Neighbor Discovery for IP Version 6 (IPv6)	R-10
4862	IPv6 Stateless Address Autoconfiguration	C-10
4869	Suite B Cryptographic Suites for IPSec	C-10
4877	MIPv6 Operation with IKE2 and the Revised IPSec Architecture	C-10
5072	IP Version 6 over PPP	C-10
5095	Deprecation of Type 0 Routing Headers in IPv6	R*(1)
5304	IS-IS Cryptographic Authentication	R-10
5308	Routing IPv6 with ISIS	R-10
5310	IS-IS Generic Cryptographic Authentication	R-10

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C

NOTES:
R-1: Only meets the dual-stack requirements of this RFC.
R-2: Only meets IPv6 formatting requirements of this RFC.
R-3: Only meets framing format aspects of RFC.
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.
C-5: Condition is that product acts as a router.
C-6: Only applies to MGs.
C-7: Requirements only apply if the product acts as an edge router.
C/R-8: EI (softphones only).
C/R-10: Conditional/Objective Requirement for UCR 2010.
*(n): Deviation from DoD IPv6 Profile, version 3.0, Appendix C. Key to "n" values is described in Section 5.3.5.1, Introduction.

Table 5.3.5-5. LAN Switch (LS)

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	C-5
2401	Security Architecture for the Internet Protocol	C*(3)
2404	The Use of HMAC-SHA-1-96 within ESP and AH	C-5
2407	The Internet IP Security Domain of Interpretation for ISAKMP	C*(3)
2408	Internet Security Association and Key Management Protocol (ISAKMP)	C*(3)
2409	The Internet Key Exchange (IKE)	C*(3)
2460	Internet Protocol, Version 6 (v6) Specification	C-2, C-5
2461	Neighbor Discovery for IP Version 6 (IPv6)	C-5
2462	IPv6 Stateless Address Autoconfiguration	C
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	C*(3)-4, C-5
2545	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	C-7
2710	Multicast Listener Discovery (MLD) for IPv6	C-5
2711	IPv6 Router Alert Option	C*(1)-5
2740	OSPF for IPv6	C-5
2858	Multiprotocol Extensions for BGP-4	C-5, C-7
3162	RADIUS and IPv6	C*(3)-5
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	C-5
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	C-5
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	C-5
3413	Simple Network Management Protocol (SNMP) Applications	C-5
3595	Textual Conventions for IPv6 Flow Label	C

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
3810	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	C*(3)-5
3986	Uniform Resource Identifier (URI): Generic Syntax	C*(2)
4007	IPv6 Scoped Address Architecture	R
4022	Management Information Base for the Transmission Control Protocol (TCP)	C
4087	IP Tunnel MIB	C*(3)
4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	C*(3)
4113	Management Information Base for the User Datagram Protocol (UDP)	C
4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	C-1, C-5
4271	A Border Gateway Protocol 4 (BGP-4)	C-7
4291	IP Version 6 Addressing Architecture	R
4292	IP Forwarding MIB	C
4293	Management Information Base for the Internet Protocol (IP)	C
4295	Mobile IP Management MIB	C-10
4301	Security Architecture for the Internet Protocol	C*(3)-10
4302	IP Authentication Header	C*(3)
4303	IP Encapsulating Security Payload (ESP)	C*(3)
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C*(3)
4306	Internet Key Exchange (IKEv2) Protocol	C*(3)-10
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C*(3)
4308	Cryptographic Suites for IPSec	C*(1, 3)
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	C-5
4552	Authentication Confidentiality for OSPFv3	C-5
4760	Multiprotocol Extensions for BGP-4	C-5,C-7, C-10
4807	IPSec Security Policy Database Configuration MIB	C
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C*(3)-10
4861	Neighbor Discovery for IP Version 6 (IPv6)	C-5, C-10
4862	IPv6 Stateless Address Autoconfiguration	C-10
4869	Suite B Cryptographic Suites for IPSec	C*(3)`-10
5095	Deprecation of Type 0 Routing Headers in IPv6	C*(1)-5
5304	IS-IS Cryptographic Authentication	C-5, C-10
5308	Routing IPv6 with ISIS	C-5, C-10
5310	IS-IS Generic Cryptographic Authentication	C-5, C-10

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C

NOTES:
R-1: Only meets the dual-stack requirements of this RFC.
C/R-2: Only meets IPv6 formatting requirements of this RFC.
R-3: Only meets framing format aspects of RFC.
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.
C-5: Condition is that product acts as a router.
C-6: Only applies to MGs.
C-7: Requirements only apply if the product acts as an edge router.
C/R-8: EI (softphones only).
C/R-10: Conditional/Objective Requirement for UCR 2010.
*(n): Deviation from DoD IPv6 Profile, version 3.0, Appendix C. Key to "n" values is described in Section 5.3.5.1, Introduction.

Table 5.3.5-6. UC Information Assurance Device (EBC)

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
1981	Path MTU Discovery for IPv6	R
2401	Security Architecture for the Internet Protocol	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 (v6) Specification	R-2
2461	Neighbor Discovery for IP Version 6 (IPv6)	R
2462	IPv6 Stateless Address Autoconfiguration	C
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 *(3)-4
3162	RADIUS and IPv6	C*(3)
3266	Support for IPv6 in Session Description Protocol (SDP)	C*(4)
3986	Uniform Resource Identifier (URI): Generic Syntax	C*(2)
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-10
4302	IP Authentication Header	C*(3)
4303	IP Encapsulating Security Payload (ESP)	C
4305	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C
4306	Internet Key Exchange (IKEv2) Protocol	C-10
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	C

RFC NUMBER	RFC TITLE	REQUIRED – R CONDITIONAL – C
4308	Cryptographic Suites for IPSec	C*(1)
4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	R
4566	SDP: Session Description Protocol	C*(4)-10
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	C-10
4861	Neighbor Discovery for IP version 6 (IPv6)	R-10
4862	IPv6 Stateless Address Autoconfiguration	C-10
4869	Suite B Cryptographic Suites for IPSec	C-10
5095	Deprecation of Type 0 Routing Headers in IPv6	R*(1)

NOTES:
R-1: Only meets the dual-stack requirements of this RFC.
R-2: Only meets IPv6 formatting requirements of this RFC.
R-3: Only meets framing format aspects of RFC.
R-4: Requirement covered in Section 5.3.3, Wide Area Network General System Requirements.
C-5: Condition is that product acts as a router.
C-6: Only applies to MGs.
C-7: Requirements only apply if the product acts as an edge router.
C/R-8: EI (softphones only).
C/R-10: Conditional/Objective Requirement for UCR 2010.
*(n): Deviation from DoD IPv6 Profile, version 3.0, Appendix C. Key to "n" values is described in Section 5.3.5.1, Introduction.

THIS PAGE INTENTIONALLY LEFT BLANK

MEMORANDUM FOR DEPARTMENT OF DEFENSE EXECUTIVE AGENT FOR INFORMATION TECHNOLOGY STANDARDS (ATTN: THE CHAIR, INFORMATION TECHNOLOGY STANDARDS COMMITTEE)

JUL 30 2009

SUBJECT: Department of Defense Information Technology Standards Registry Baseline Release 09-2.0

References: (a) DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), May 5, 2004
(b) Deputy Secretary of Defense Memorandum, "DoD Executive Agent for Information Technology (IT) Standards, May 21, 2007

The DoD Information Technology (IT) Standards Registry (DISR) has been updated from Baseline Release 09-1.0 to DISR Baseline Release 09-2.0 in accordance with Reference (a). The DISR baseline is updated every four months to ensure the DoD capabilities for building and buying IT systems are based on a current and effective set of IT and National Security Systems (NSS) standards.

We as tri-chairs of the Information Technology Standards Oversight Panel (ISOP), acting under the authority of the DoD CIO, approve the changes to the DISR baseline listed in the attached spreadsheets as recommended by the Information Technology Standards Committee (ITSC) at their 24 June 2009 meeting. Please post the approved changes in DISR Baseline 09-2.0 for immediate use in DoD IT and NSS acquisitions and development systems. This DISR Baseline supersedes DISR Baseline 09-1.0 and contains IT and NSS standards needed to support interoperability and a net-centric information-sharing operational environment.

Based on the tri-chairs' approval of DISR Baseline Release 09-2.0 and the applicable standards associated with IPv6, the IPv6 Standard Profiles for IPv6 Capable Products, Version 4.0, July 2009, is approved for distribution via DISRonline..

We extend our thanks once again to the members of the ITSC and the Technical Standards Working Groups for their involvement and contributions to the DoD standards process.

BRIAN G. WILCZYNSKI Director Enterprise Architecture and Standards ASD(NII) DCIO/IMI&T	MICHAEL J. BASLA Brigadier General, USAF Vice Director, Command and Computers Systems, Joint Staff	GORDON M. KRANZ Acting Director Systems and Software Engineering DUSD (AT&L)

Copy to: DoD CIO Executive Board
ITSC Representatives

Attachment: Changes for DISR Baseline 09-2.0

DoD IPv6 Standard Profiles For IPv6 Capable Products Version 4.0

July 2009

Prepared by the DISR IPv6 Standards Technical Working Group
POC: Ralph Liguori, Chair IPv6 Standards TWG
E-mail Address: ralph.liguori@disa.mil

Table of Contents

Executive Summary

This document provides the engineering-level definition of “Internet Protocol (IP) Version 6 (IPv6) Capable” products necessary for interoperable use throughout the U.S. Department of Defense (DoD). This content has been synthesized from multiple sources including DoD policy statements [1] [2] [8], DoD Information Technology Standards Registry (DISR) requirements [3], DoD IPv6 Transition Office (DITO) guidance [4] [5] and Internet Engineering Task Force (IETF) published requirements. The term “IPv6 Capable Product” as used in this document, means any product that meets the minimum set of mandated requirements, appropriate to its Product Class, necessary for it to interoperate with other IPv6 products employed in DoD IPv6 networks. Version 1.0 of this Standard Profiles document was approved by the DoD Information Standards Oversight Panel (ISOP) in 2006 under the authority of the DoD Chief Information Officer (CIO) to “provide guidance to DoD Components and Services responsible for procuring/acquiring IPv6 Capable Global Information Grid (GIG) products” [6] as were the Version 2.0 and 3.0 revisions in 2007 [18] and 2008 [21]. Final review and approval of this revision will be similarly documented.

The document is intended to assist several communities of interest in executing their responsibilities for preparing DoD systems and networks to be IPv6 Capable. The goal of this document is to organize and summarize the requirements included by reference for the convenience of a broad spectrum of readers, including acquisition officers, testing organizations, DoD systems developers and vendors.

This document as a whole defines a set of DoD IPv6 Standard Profiles (Profiles) for IPv6 Capable Products of various classes of equipment or software, and variety of IPv6 network roles. First, Product Classes are defined that will be used in the document to group products according to their role in a network architecture. Then the Base Requirements that apply to all IPv6 Capable Product Classes are defined. Several Functional Requirements blocks are defined for specific functions performed by some products. Finally, Product Class Profiles are defined in terms of the Base Requirements and Functional Requirements.

References, a Glossary and an Appendix with a summary of the requirements in tabular form are provided at the end of the text. Appendix D provides a summary of changes with respect to the previous version of this document.

Dedication

The DoD Standard Profiles for IPv6 Capable Products v4.0 is dedicated in memory of

Jim Bound

Chair of the North American IPv6 Task Force
CTO of the IPv6 Forum
Senior Fellow, Hewlett-Packard

From the earliest discussions of next generation IP, Jim Bound has been a tireless advocate for practical and sensible evolution of an Internet that meets the requirements of end users. In particular, Jim was instrumental in influencing the US Department of Defense to take an early and pro-active role in the development of IPv6, and in encouraging its adoption. With respect to this document, Jim was indispensable in enlisting support from the vendor community via the North American IPv6 Task Force, allowing the editors to draw upon a deep well of subject matter experts for contributions and review starting with Version 2.0. This has helped clarify essential DoD requirements while being realistic about the ability of the commercial marketplace to meet those requirements.

Jim could be counted on to speak his mind courageously and with great integrity. While he could be brutally honest, he was as quick and generous with his support for people and ideas he believed in as he was to critique what he recognized as wrongheaded or counterproductive. We best honor Jim by continuing the fight for integrity, honesty and efficiency in our standards processes, in our products and services, and in how we present ourselves to the world as individuals both professionally and personally.

Recognition

The DoD IPv6 Standard Profiles for IPv6 Capable Products has been recognized with a 2008 Defense Standardization Program (DSP) Achievement award. The award was announced in a memorandum from Mr. Gregory E. Saunders, Director of the Defense Standardization Program Office, dated January 23, 2009. While Mr. Ralph Liguori is specifically named on the award, the editors recognize that this document has earned this recognition due to the contributions and reviews provided by many people, including the original authors of earlier versions, the members of the IPv6 Technical Working Group, other Government staff and contractors, members of the North American IPv6 Task Force, other subject matter experts, industry representatives and those active in the Internet Engineering Task Force standards process. All who collaborated with us in the work should also feel they have a share of this recognition.

1 Introduction

The Internet Protocol (IP) is the network layer for the interconnection of packet-switched networks. The current version of IP in widespread use is IP version 4 (IPv4) first defined and deployed over 25 years ago. IP version 6 (IPv6) is a replacement for IPv4 first proposed in 1995 by publication the Internet Engineering Task Force (IETF) of Request for Comments (RFC) 1883 (obsoleted by 2460) and a series of supporting RFCs. U.S. Department of Defense (DoD) policy mandating use of IPv6 was first documented in the "Internet Protocol Version 6 (IPv6)" memorandum issued 9 June 2003 [2] and updated in September 2003 by "Internet Protocol Version 6 (IPv6) Interim Transition Guidance" [1] both published by the DoD Chief Information Officer (CIO) John Stenbit.

The official released text of this document when approved will be posted at https://disronline.disa.mil. Access to the document on DISRonline requires a CAC card, log on, and selecting the Guidance tab. The document will also be available without access restriction at http://jitc.fhu.disa.mil/apl/.

1.1 IPv6 Definitions

This document provides an elaboration of the technical standards that are required to be considered an "IPv6 Capable Product". A Memorandum issued on 26 June 2008 by the DoD Deputy CIO entitled "Internet Protocol Version 6 (IPv6) Definitions" [20] states the following:

IPv6 Capable Products - Products (whether developed by commercial vendor or the government) [that] can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/IPv6 environments. IPv6 Capable Products shall be able to interoperate with other IPv6 Capable Products on networks supporting only IPv4, only IPv6, or both IPv4 and IPv6, and shall also:

- Conform to the requirements of the DoD IPv6 Standard Profiles for IPv6 Capable Products document contained in the DISR

- Posses a migration path and/or commitment to upgrade from the developer (company Vice President, or equivalent, letter) as the IPv6 standard evolves

- Ensure product developer IPv6 technical support is available

- Conform to National Security Agency (NSA) and /or Unified Cross Domain Management Office requirements for Information Assurance Products

Version 1.0 of this document was approved by the DoD Information Standards Oversight Panel (ISOP) [6] as representing the "IPv6 Profile" cited in the DoD IPv6 Definitions, taking the place of the Generic IPv6 Profile in the DISR. Version 2.0 and 3.0 were similarly approved in turn by the ISOP [18] [21]. Thus, this document in its entirety provides the effective definition of an "IPv6 Capable Product" by enumerating

the requirements that must be met by a particular product. While other terms such as "IPv6 Ready" or "IPv6 Compliant" have been used in other contexts, the term "IPv6 Capable Product" as it is defined in this document should be used in conjunction with a citation of this document to be clear about what is required.

While this document defines IPv6 Capable with respect to individual products, The DoD IPv6 Definitions memorandum also defines an IPv6 Capable Network as one that can receive, process, and forward IPv6 packets from/to devices within the same network and from/to other networks, and systems, where those networks and systems may be operating with only IPv4, only IPv6, or both IPv4 and IPv6. An IPv6 Capable Network shall be ready to have IPv6 enable for operational use, when mission need or business case dictates. Specifically, an IPv6 Capable Network must:

- Use IPv6 Capable Products
- Accommodate IPv6 in network infrastructures, services, and management tools and applications
- Conform to DoD and NSA- developed IPv6 network security implementation guidance
- Manage, administrate, and resolve IPv6 addresses in compliance with the DoD IPv6 Address Plan [14], when enabled

In addition, the DoD IPv6 Definitions memorandum defines an IPv6 Enabled Network as a network that is supporting operational IPv6 traffic, through the network, end-to-end. Note that this does not imply that the network carries only IPv6 traffic; it may still carry IPv4 traffic as well.

1.2 Document Goals and Purpose

This document provides a technical and standards based definition of interoperability requirements for IPv6 Capable Products to be used in DoD networks. This content has been synthesized from multiple sources including DoD policy statements [1] [2] [8], DoD Information Technology Standards Registry (DISR) requirements [3], DoD IPv6 Transition Office (DITO) guidance [4] [5] and Internet Engineering Task Force (IETF) published requirements. Version 2.0 and 3.0 of this document were reviewed and approved by the ISOP as guidance for the acquisition of IPv6 Capable Products [18][21] and when approved, this version will replace Version 3.0.

RFC 4294 "IPv6 Node Requirements" published by the IETF in April 2006 has been an essential guide in the preparation of this document. The following goal statement from that RFC can also serve as the basis for the goals of this document:

> "The goal of this document (RFC 4294) is to define the common functionality required from both IPv6 hosts and routers. Many IPv6 nodes will implement

> optional or additional features, but this document summarizes requirements from other published Standards Track[1] documents in one place.
>
> This document tries to avoid discussion of protocol details, and references RFCs for this purpose. This document is informational in nature and does not update Standards Track RFCs.
>
> Although the document points to different specifications, it should be noted that in most cases, the granularity of requirements are smaller than a single specification, as many specifications define multiple, independent pieces, some of which may not be mandatory."

Likewise, this document does not intend to define or mandate new requirements nor to unduly restrict use of optional requirements, but to summarize the requirements for IPv6 Capable Products. To facilitate interoperability:

1. A device should not rely upon or assume the implementation of optional features in other devices for basic interoperability;

2. A device should, when feasible, implement optional features that may be useful in some deployments;

3. While a device may implement any optional features not specifically forbidden in this document, the implementation should not interfere with another device implementing required and permitted features.

For example, while Mobility is a conditional requirement, and thus optional, products that support Mobility should be interoperable with products that do not support Mobility. Typically, a feature like Mobility must be implemented in a number of cooperating nodes in the network, necessitating selection of products that do implement the option.

1.3 Target Audience

The document is intended to assist several communities of interest in executing their responsibilities for preparing DoD systems and networks to be IPv6 Capable. The topic is rather technical, and requires some background understanding by the reader of the RFCs and other references cited, but the goal of this document is to organize and summarize the requirements included by reference for the convenience of the reader. The authors hope that the document is useful to several categories of users as described in the following paragraphs.

---

[1] Standards Track is an IETF term indicating that an RFC is published with the intention that it will become an Internet Standard when mature and widely implemented. An RFC is usually published as a "Proposed Standard" and is promoted to "Draft Standards" before being considered for Internet Standard status. Further explanation of this process can be found in RFC 2026.

Contracts and Acquisition

Acquisition officers and others writing purchasing and contract language may use this document as a reference when they develop specific product and system requirement text. For their purposes, this document aims to adequately summarize the technical requirements such that it is sufficient (with the citation of RFCs and other specifications referenced by this document) to specify the minimal requirements for products to be IPv6 Capable. The IPv6 Capable Registry and the test reports generated during testing by the Joint Interoperability Test Command (JITC) will provide useful input to the responsible component or program acquisition effort.

Testing and Certification Organizations

DoD components will rely upon testing organizations including the Joint Interoperability Test Command (JITC) to evaluate vendor products and DoD systems as IPv6 Capable. These testing organizations may use this document as an outline and starting point for the development of detailed test plans appropriate to each product class. They will need to go beyond the summary level of this document through reference to the specifications and other technical material cited.

Developers

The engineers and managers responsible for systems development by DoD and vendor organizations may use this document as an additional check on interpretation of the specifications and other technical material cited to develop systems architectures, designs and implementations to assure that their products will be IPv6 Capable. By following the requirements documented herein, they will increase the probability that the systems they build will be interoperable with other DoD IPv6 Capable network elements and will be ready for DoD testing.

1.4 Requirement Sources

The immediate reference for requirements in this document is the Defense Information Systems Registry (DISR). The DISR is a snapshot of the state-of-practice for technical publications being tracked by DISA for inclusion in profiles for products to be acquired by DoD. These technical publications come from a number of sources, primarily external Standards Development Organizations (SDOs) and are reviewed and considered by the DoD IT Standards Committee (ITSC) and a number of DoD IT Standards Technical Working Groups (TWGs). When standards are sufficiently mature, they are added to the DISR database.

In particular, IPv6 specifications and related standards are published by the Internet Engineering Task Force (IETF) as Requests for Comments (RFCs). These documents are reviewed and analyzed by members of the IPv6 Standards TWG, and considered for mandatory or optional use in DoD systems and networks when they are stable and mature and determined to be appropriate requirements for use by DoD. Each of the RFCs cited in the DISR and in this document is included by reference in its entirety,

except where this document notes exceptions or extensions. RFCs can be freely obtained through the RFC Editor by searching on the RFC number or keywords; the IETF Tools page also provides access to an archive of Internet-Drafts and RFCs in HTML format.

The DISR is updated 3 times a year after due consideration of new and replacement RFCs by the IPv6 Standards TWG. This document is coordinated with the content of the DISR database at the time of its publication, and will be updated and republished as necessary to maintain this correspondence.

In February 2007 and again in January 2008, the National Institute of Standards and Technology (NIST) circulated a draft for public comment entitled "A Profile for IPv6 in the U.S. Government" (USGv6) [19]. The final USGv6 Profile for IPv6 Version 1.0 was updated based on a number of comments and published in July 2008 [9]. That document is intended for U.S. Government environments exclusive of the DoD. The editors of this document worked with the editors of the USGv6 to minimize differences between Version 3.0 of this document and Version 1.0 of the USGv6. The two documents will be maintained in parallel efforts for the foreseeable future. Per the cited DoD policy statements [1] [2] [8] DoD acquisition of products for IPv6 deployment should follow this document and all DoD testing and certification is coordinated by the DISA Joint Interoperability Testing Command (JITC). Discussions between NIST and DoD on compatible testing programs continue; however, there are no significant differences in functional requirements as of the currently circulating drafts meaning that products approved under one program are highly likely to be interoperable with products approved under the other. There are minor differences in the effective dates of some requirements that will naturally converge over time.

1.5 Terminology Used in This Document

The DISR database and IETF RFCs use different terminology to describe requirements. RFCs and other technical publications referenced in the DISR as standards are assigned to one of 3 statuses:

EMERGING: An EMERGING standard is a new or evolving standard that is likely to eventually become a MANDATED standard.

MANDATED: A MANDATED standard is a stable and mature standard that can be cited as a requirement in acquisition. One of the considerations for determining maturity of a standard is the existence of vendor implementations.

RETIRED: A standard that has been replaced by a newer standard or otherwise determined to be no longer appropriate for use in DoD systems is a RETIRED standard.

Additionally, RFCs or other publications can be referenced in the DISR as **INFORMATIONAL/GUIDANCE** meaning that they provide useful information that is not a standard.

IETF terminology for use in RFCs is defined in RFC 2119 including the terms MUST, SHOULD, and MAY. To provide a common lexicon, the following six terms used in this document are to be interpreted as follows:

MUST: This term indicates an imperative; the requirement is essential to IPv6 capability and interoperability. This level of requirement is indicated in the DISR by MANDATED. Synonyms used in other contexts include Threshold, SHALL or REQUIRED.

MUST NOT: This term indicates an absolute prohibition of a behavior. A synonym is SHALL NOT.

SHOULD: This term indicates a desirable or expected course of action or policy that is to be followed unless inappropriate or cost-prohibitive for a particular circumstance. This corresponds to the EMERGING[2] level in the DISR. In other contexts, the term Objective is used.

SHOULD NOT: This term is used to indicate that the particular behavior is discouraged though not prohibited. There may be valid reasons in particular circumstances when the behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing.

MAY: This term denotes the permissive or that an item is truly optional. An implementation which does not include a particular option MUST interoperate with another implementation which does include the option. In the same vein, an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (in both cases without the feature the option provides). Normally standards that a product MAY follow would be listed in the DISR as INFORMATIONAL.

SHOULD+: This term indicates a near-term goal for technology insertion that is strongly expected to be elevated to a MUST or MANDATED in the near future (see paragraph 1.5.1). SHOULD+ means a strongly recommended and expected course of action or policy that is to be followed unless inappropriate for a particular circumstance. This term is normally associated with an EMERGING specification in the DISR.

1.5.1 Effective Dates for Mandate of New and Revised RFCs

IPv6 is defined by an active and evolving set of RFCs. In addition to new emerging standards, existing standards are occasionally updated by RFCs that extend or elaborate the standards, and on occasion standards may be rendered obsolete by revised RFCs. In IETF practice, once published, an RFC is never modified; the technical material it defines can only be changed by publication of another RFC. The

[2] A standard that is listed in DISR as MANDATED could also be used in SHOULD, SHOULD+ and MAY clauses.

RFC Editor web page tracks all RFCs, and relates them to other RFCs that update or obsolete them.

The obsolescence and replacement of RFCs by new RFCs complicates a simple and clear definition of the mandatory requirements in this Standard Profiles document. There will be a period of time during which commercially available products may support either or both of the versions of the standard. In some cases the requirement is to support the *function*, preferably complying with the emerging replacement RFC but at least according to the previously published RFC. In these situations, the old and new standards will be discussed together in this document with exceptions or conditions noted, to provide clear guidance to vendors for implementation and testing.

Prior to Version 3.0, this specification did not provide for "in effect" dates for new or strengthened requirements, implying that they were always "effective immediately" when stated as a MUST. Recognizing realistic product cycles, the following policy was established in Version 3.0:

1. An emerging requirement will typically be stated as a SHOULD+ when it is first cited in a revision of this specification, indicating that it is likely to be strengthened to a MUST in the next revision nominally 12 months later; in exceptional circumstances the first citation of a requirement may be a MUST;

2. A "grace" period of 12-24 months will be allowed between the statement of a new or strengthened MUST requirement in a revision of this specification and enforcement of the mandate;

    a. Nominally, a replacement RFC will have an effective date 12 months following its first citation as a MUST; In some cases, the *function* specified in a set of revised and obsolete RFCs MUST be supported, preferably according to the revised RFC, but minimally at the prior RFC;

    b. Nominally, a new functional requirement will have an effective date 24 months following the first citation as a MUST; this recognizes the more significant development effort for a new feature rather than an update based on a revised specification for an existing capability;

3. Exceptions for specific requirements will be noted in the text, where a longer or shorter allowance is appropriate; in all cases, the Effective Date column in the Appendix C Requirements Summary will provide an unambiguous indication of the effective date;

4. Requests for dispensations beyond the stated policy will be evaluated on a case-by-case basis by DISA Standards Engineering and JITC. The ultimate authority for waiver of any requirement for IPv6 Capable products will be defined by the component making the purchase and deployment decision.

The Requirements Summary Table in Appendix C includes a column to indicate the effective date for each requirement in the text.

1.5.2 Distinction Between Capability and Deployment

Throughout this document the terms “support” and “implement” as well as other forms of the words such as “supported”, “implementation”, etc. are used to indicate that a requirement or function is available in a product. In other words, the compliant product is capable of providing the function. For example, if a product class MUST support MLDv2 as defined in RFC 3810, a compliant product of that class meets the requirements in that RFC to provide MLDv2 function. This does not imply that the available function will be actively used. The terms “deployment” and “use” as well as other forms of those words indicate active operation of an available capability or function.

1.5.3 Conditional Requirements

Note also that some requirements clauses or paragraphs of this specification may be applied conditionally. The language in these instances is intended to be self-explanatory, and stated as simply as possible to capture the technical nuances, for example as used in Section 3.1.1:

> “An IPv6 Capable Host/Workstation…Conditionally, MUST implement MIPv6 Capable Node Functional Requirements (Section 2.5.1) IF intended to be deployed as a Mobile Node.”

This should be read to mean that the requirement to support the sections of the RFCs for MIPv6 Mobile Node functionality would not be mandatory for all IPv6 Capable Host/Workstation Products, but is mandatory for products that are intended to operate as a Mobile Node in a MIPv6 deployment. Submission and test results for a product will note whether or not the product includes any of the conditional requirements. For example, “Product X meets the requirements for an IPv6 Capable Host/Workstation with Mobility” indicates that Product X complies with all the basic requirements for Host/Workstation and also meets the requirements for a MIPv6 Capable mobile node. On the other hand “Product Y meets the requirements for an IPv6 Capable Network Appliance” indicates that Product Y only meets the basic requirements for a Network Appliance but does not necessarily meet any Conditional requirements such as MIPv6 Capable.

1.6 IPv6 Capable Product Classes

Before examining detailed requirements it would be useful to frame the discussion by defining the classes of IPv6 Capable Products. The terminology used in the IPv6 base specification [RFC 2460] defines two general subclasses of IPv6 nodes; an IPv6 router is an IPv6 node that forwards IPv6 packets not explicitly addressed to it and an IPv6 host is any node that is not a router. Describing the requirements for a specific IPv6 Capable product using those broad classes would require complex exceptions and

explanations to distinguish among different products. This Standard Profiles document groups IPv6 Capable Products into a small number of Product Classes convenient for defining common requirements. IPv6 Capable Products are classified according to their architectural and functional role in an IPv6 network**:**

- **End Node:** A node processing IPv6 packets addressed to the node itself or originating IPv6 packets with a source address of the node itself. End Nodes include the following Product Classes:

  - **Host/Workstation:** a personal computer (PC) or other end-user computer or workstation running a general purpose Operating System (OS) such as UNIX®[3], Linux®[4],Windows®[5], or a proprietary operating system that is capable of supporting multiple applications. A Host/Workstation typically has a single user, with a local (console) login, and is generally managed by the end-user (or the end-user organization support team, rather than the Internet Service Provider (ISP) or other third party).

    Note that a Host/Workstation can be viewed as a hardware platform combined with its OS; however, the implementation of the IPv6 Capability in one embodiment is that the operating system (OS) implements IPv6 and it is independent of the hardware platform. In fact the particular hardware platform running the OS is usually irrelevant; for example, Microsoft Windows Vista running on any PC has the same IPv6 capabilities. The PC running Windows Vista in this case, whether HP, Dell or custom-built has no IPv6 capability of its own independent of the OS. The implementation of the IPv6 Capability in a second embodiment consists of the OS that works with a hardware implementation of the IP stack (usually a network interface card). Thus an OS and a network interface card with an IPv6 hardware implementation may entirely implement IPv6 capability and thus run on any particular hardware platform. Overall, this note may apply to products in any of the Product Classes.

  - **Network Appliance or Simple Server[6]:** Simple end nodes such as cameras, sensors, automation controllers, networked phones or adapters

---

[3] *UNIX® is a registered trademark of The Open Group*

[4] *Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.*

[5] *Windows® is a registered trademark of Microsoft Corporation in the United States and other countries.*

[6] The distinction between Simple Server and Network Appliance results in no real difference in requirements or testing. Simple Server product class could be eliminated completely, but is retained for consistency with previous revisions and test results.

such as Circuit-to-Packet (CTP) devices, typically with an embedded operating system and specialized software for limited applications. A **Network Appliance** is typically managed by an end-user, but may support more than one concurrent user remotely via a Web browser interface. A **Simple Server** supports a small number of concurrent clients via a web browser interface or other protocol with a client application. Examples of simple servers are stand-alone network print servers, storage servers, Session Initiation Protocol (SIP)[7] servers, a "web camera" appliance that serves pictures via an embedded web server, and a network time server appliance that solely functions to serve NTP requests. A device with a trivial or no role at the IP layer, for example a modem or layer 2 switch, may have a user or management interface with an IPv6 address. These devices should also be evaluated as a Network Appliance/Simple Server.

- **Advanced Server:** End Nodes with one or more server-side applications (for example Dynamic Host Configuration Protocol (DHCPv6), Domain Name Server (DNS), Network Time Protocol (NTP), E-mail, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), web server, storage server or database) to support clients in the network. Servers are usually managed by network administrators or operated by a third party such as an ISP or other vendor. An **Advanced Server** typically runs a general purpose operating system such as UNIX, Linux, Windows, or a proprietary operating system and is capable of serving any number of applications to many concurrent clients.

- **Intermediate Node:** A node that forwards IPv6 packets not explicitly addressed to the node itself.[8]

  - **Router:** An Intermediate Node that forwards packets based on paths discovered using routing protocols. A router typically has a small number of ports to interconnect several networks, in particular to connect a Local Area Network (LAN) to a Wide Area Network (WAN). A Router implements complex control plane functions, including routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) which are typically implemented in software run on a general purpose CPU.

  - **Layer-3 Switch:** An Intermediate Node that forwards IPv6 packets at switching speeds usually through the use of special purpose dedicated

[7] See RFC 3261 Session Initiation Protocol for more information on SIP

[8] Please note that an Intermediate Node may also act as an End Node for Network Management and other protocols, and must conform to Simple Server functionality for IPv6 packets addressed to an IPv6 address of the node itself.

hardware. A Layer-3 Switch typically has a higher port density than a Router and is intended to interconnect end-nodes in a LAN environment. A Layer-3 Switch may have some limited layer-3 control plane (management or routing) functions but is primarily a data plane device. A Layer 2 switch is transparent at the IP layer, and as such plays no active role as an IPv6 Capable product. However, the device may be managed over an IPv6 interface and should be evaluated as a Simple Server.

- **Information Assurance Device:** An Intermediate Node that performs a security function as its primary purpose by filtering or encrypting network traffic, and which may block traffic when security policy dictates. For example a Firewall, Intrusion Detection System, Authentication Server, Security Gateway, High Assurance IP Encryptor (HAIPE) or Virtual Private Network (VPN) is an Information Assurance Device. A Router or Layer 3 (L3) Switch may incorporate an IA function in addition to its primary role, but is not an IA Device but rather an "IA Enabled" product. .

- **IPv6 Capable Software:** a product that implements functions available via an IPv6 interface to end-users, network nodes or other software, when installed on an appropriate hardware platform. Section 4 of this document introduces some concepts for the evaluation of pure software IPv6 Capable products (operating systems or applications) but a full definition of IPv6 Capable Software Product Classes is deferred to a future revision of this document.

Some of the terms used in this document for defining Product Classes have been used with different definitions in the networking industry, but throughout this document and in references to this document, the terms are intended to be used as defined above. In particular the term Network Appliance has been used for a variety of End Node and Intermediate Node products, and is the name of a storage solutions company.

We have attempted to make the distinctions between Product Classes as objective as possible, but some of the differences are subject to interpretation, in particular the classification of a Server product as "Simple" or "Advanced". It is essential that a vendor come to agreement with the testing organization (JITC for example) on proper classification of their product before testing. The testing organization and the Chairman of the DISR IPv6 Standards TWG can be of assistance in classifying products that don't obviously fit one of the Product Classes. Many products include other interfaces in addition to the IPv6 interface, such as a Voice-over-IP (VOIP) device or Circuit-to-Packet (CTP) device. Such a device can be evaluated as a "black box" from its IPv6 interface, without regard to other internal or external non-IPv6 interfaces.

The following table summarizes the Product Class definitions and characteristics to help with the classification of specific products. For example, if the product is an End Node, managed by the End-User organization, accessed by a single user through a local interface rather than remotely via a Web interface, it is best identified as a Host/Workstation.

<table>
<tr><th></th><th>Host/ Workstation</th><th>Network Appliance or Simple Server</th><th>Advanced Server</th><th>Router</th><th>Layer 3 Switch</th><th>Information Assurance Device</th></tr>
<tr><td>End Node</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Optional</td><td>Optional</td><td>Optional</td></tr>
<tr><td>Intermediate Node</td><td>No</td><td>No</td><td>No</td><td>Yes</td><td>Yes</td><td>Yes</td></tr>
<tr><td>End-User Managed</td><td>Yes</td><td>Yes</td><td>No</td><td>No</td><td>No</td><td>No</td></tr>
<tr><td>Web Access</td><td>No</td><td>Optional</td><td>Optional</td><td>Optional</td><td>Optional</td><td>Optional</td></tr>
<tr><td>Local login or console</td><td>Yes</td><td>Optional</td><td>Optional</td><td>Optional</td><td>Optional</td><td>Optional</td></tr>
<tr><td>Loadable or Embedded</td><td>Loadable[9]</td><td>Embedded</td><td>Optional</td><td>Optional</td><td>Optional</td><td>Optional</td></tr>
<tr><td>Number of Applications</td><td>Many</td><td>Few</td><td>1 to Many</td><td colspan="3" rowspan="2">unspecified</td></tr>
<tr><td>Number of Users</td><td>1</td><td>1 to Few</td><td>Many</td></tr>
<tr><td>Network Interconnection</td><td colspan="3" rowspan="4">Not applicable</td><td>Yes</td><td>No</td><td rowspan="3">Not Applicable</td></tr>
<tr><td>Port Density</td><td>Low</td><td>High</td></tr>
<tr><td>Complex Control Plane</td><td>Yes</td><td>No</td></tr>
<tr><td>IA Function</td><td>Optional</td><td>Optional</td><td>Yes</td></tr>
</table>

Table 1-1: Product Class Summary

2 IPv6 Capable Product Requirements

This section identifies the specifications that will be used to define the requirements for the Product Classes outlined above. These specifications are organized into several functional categories. First, the Base Requirements are defined, comprising the standards that will (with minor exceptions) apply equally to all Product Classes. Then, a

[9] A Host/Workstation is typically “loadable” although in practice, some systems may be preloaded by an administrator with the end user restricted from loading additional software.

set of Functional Requirements categories are defined, which will be used as "building blocks" to construct the detailed Product Class Profiles in Section 3.

Specific requirements in the RFCs cited in the Base or Functional Requirements may in some cases apply in the same manner to IPv6 End Nodes and IPv6 Intermediate Nodes or may apply differently to each class; the language in this document is intended to make these distinctions clear. The reader may read the cited RFCs for a more detailed understanding of the specific requirements. Extensions, restrictions and exceptions with respect to the Product Classes defined in this document can be found in Section 3.

While this document is intended to cover the preponderance of products to be used in DoD networks and applications, the authors recognize that programs may have circumstances that justify the extension, modification or exception to requirements in this document by means of program-specific documentation. For example, the Real-Time Services (RTS) program defines some unique appliances and products for use in the Defense Switched Network (DSN) and the Defense Red Switch Network (DRSN). RTS/DSN/DRSN components such as the Local Session Controller (LSC), IP Enabled End Office (EO) and Edge Boundary Controller (EBC) will be IPv6 capable as specified in this document with exceptions and design/implementation guidelines noted in latest version of the DoD Unified Capabilities Requirements (UCR) document. As of this publication, UCR 2008 has been published, and its IPv6 requirements were based on v2.0 of this publication, but substantially consistent with v3.0 of the profiles. UCR 2008-Change 1 is soon to be published which will be fully aligned with v3.0 and largely in line with this v4.0 publication.

2.1 Base Requirements

These Base Requirements are the core of interoperability requirements for IPv6 Nodes.

- All IPv6 Nodes MUST conform to RFC 2460, Internet Protocol v6 (IPv6) Specification, as updated by RFC 5095 – Deprecation of Type 0 Routing Headers in IPv6; this is the fundamental definition of IPv6.
- All IPv6 Nodes MUST implement RFC 4443, Internet Control Message Protocol (ICMPv6) and SHOULD be interoperable with nodes implementing the extensions defined in RFC 4884, Extended ICMP to support Multipart Messages[10].
- All IPv6 Nodes MUST implement RFC 4861 – superseding RFC 2461, Neighbor Discovery (ND) for IPv6, as appropriate to their role as an IPv6 End Node or IPv6 Intermediate Node. Informational RFC 4943 provides additional background on implementation of ND. Also note that ND implies that nodes MUST support Multicast Listener Discovery (see below).

[10] RFC 4884 indicates that most implementations of ICMP have no problem interoperating with these extensions; we are not requiring implementation of the extensions, but recommending permissive interoperability as implementations appear.

- All IPv6 Nodes MUST operate with the default minimum Path MTU (PMTU) size of 1280 octets as defined in RFC 2460. All IPv6 Nodes SHOULD support a minimum PMTU of 1500 to allow for encapsulation. All IPv6 Nodes except Network Appliance/Simple Server MUST implement RFC 1981, Path MTU Discovery for IPv6. Note that RFC 1981 does not impose additional requirements for Router behavior with respect to PMTU discovery beyond what is already required in RFC 4443 (ICMPv6); however, a Router is required to perform PMTU discovery like a Host on its own interface(s).
- All IPv6 Nodes MUST provide manual or static configuration of its IPv6 interface address(es).
- End Node addresses are generally based on a /64 network prefix with a 64-bit Interface Identifier. Nodes are not required to support longer prefixes. End sites may require multiple /64 prefixes to support multiple subnets. [14]
- An IPv6 Node which supports an autonomous method for discovering its own unique IPv6 interface addresses (see section 2.9) MUST have the means to disable the autonomous method to force manual or static configuration of addresses, e.g. the user can disable the "Creation of Global Addresses" as described in Section 5.5 of RFC 4862 (replaces RFC 2462 as of Version 3.0 of this document) on an IPv6 Node that supports Stateless Address Autoconfiguration (SLAAC).
- While nodes are not required to autoconfigure their addresses using SLAAC, all IPv6 Nodes MUST support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862; DAD MUST NOT be disabled.
- All IPv6 Nodes MUST support the IPv6 Addressing Architecture as defined in:
    - RFC 4291, IPv6 Addressing Architecture[11]
    - RFC 4007, Scoped Address Architecture (All IPv6 addressing plans MUST use this standard definition for scoped addressing architectures; however, support for zone indexes is optional)
    - RFC 5375, IPv6 Unicast Address Assignment Considerations covers aspects of the design of IPv6 address schemes
    - Additional guidance may be found in RFC 5156 – Special Use IPv6 Addresses which documents addresses with special purposes in various protocols, including some that should not appear on the public Internet
    - RFC 2526, 3306 and 3307 will also be useful in understanding and planning IPv6 addressing
    - Network designers SHOULD consider RFC 4192 - Procedures for Renumbering an IPv6 Network without a Flag Day and RFC 2894 – Router Renumbering for IPv6.
- An IPv6 Node MAY support RFC 4193, Unique Local IPv6 Unicast Addresses (ULA), which replaces the site-local address with a new type of address that is

[11] Also see the current Internet-Draft http://tools.ietf.org/html/draft-ietf-v6ops-addcon-07 and the DoD Addressing Plan [14]

private to an organization, yet unique across all of the sites[12] of the organization. Nodes are not required to support ULA at this time. Nodes implementing ULA MUST follow RFC 4193.

- All IPv6 Nodes MUST implement Multicast Listener Discovery (MLD)
  - Neighbor Discovery (ND) [RFC 4861] is a core feature of IPv6, analogous to ARP in IPv4, and is therefore a fundamental requirement for IPv4 parity. ND relies upon link-layer Multicast for some of its services; therefore ALL IPv6 Capable products will be using Multicast. In addition, switches may include the "MLD Snooping" feature that will block multicast addresses that are not registered with MLD. This implies that all IPv6 Nodes MUST implement MLD to support ND, and that products lacking MLD support cannot guarantee that ND will work in all deployments.
  - At a minimum all nodes MUST follow RFC 2710, Multicast Listener Discovery for IPv6 and SHOULD+ support the extended MLDv2 as in RFC 3810, Multicast Listener Discovery Version 2 (MLDv2) for IPv6.
  - MLD requires the use of the Router Alert option in a hop-by-hop[13] header as specified in RFC 2711
  - All IPv6 Nodes SHOULD+ follow the source address selection rules in RFC 3590 – Source Address Selection for the Multicast Listener when MLD is used, per RFC 4294 section 4.6.

2.1.1 Connection Technologies

All IPv6 Nodes conditionally MUST support a connection technology (link layer) that can carry IPv6 packets, consistent with its intended deployment. When using a connection technology with a published “IPv6 over” standard, the device MUST follow the corresponding standard for interoperability across that connection technology. Most IPv6 Capable products will implement one or more of the following standards:

- RFC 2464, Transmission of IPv6 Packets over Ethernet Networks;
- RFC 2492, IPv6 over ATM Networks;
- RFC 5072 (replaces RFC 2472), IP Version 6 over PPP;
- RFC 3572, IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH).

---

[12] RFC 3879 “Deprecating Site Local Addresses”

[13] The hop-by-hop extension header can potentially be exploited by an attacker initiating a storm of packets including the HBH header. This may trigger high CPU-utilization in a vulnerable implementation. While this is unlikely and there is no legitimate reason to expect significant volume of IPv6 HBH packets on a network, a recent Internet Draft http://tools.ietf.org/id/draft-krishnan-ipv6-hopbyhop-02.txt proposes some approaches to the issue. Options such as blocking, rate limiting or forwarding without processing of HBH should be considered when implementing HBH header processing.

- RFC 2467, Transmission of IPv6 Packets over FDDI Networks;
- RFC 2491, IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks;
- RFC 2497, Transmission of IPv6 Packets over ARCnet Networks;
- RFC 2590, Transmission of IPv6 Packets over Frame Relay Networks Specification;
- RFC 3146, Transmission of IPv6 over IEEE 1394 Networks;
- RFC 4338, Transmission of IPv6, IPv4 and Address Resolution Protocol (ARP) Packets over Fibre Channel;
- RFC 4944, Transmission of IPv6 Packets Over IEEE 802.15.4 Networks (Low Power Networks)

2.2 IP Layer Security (IPsec) Functional Requirements

Security is a complex topic and the role of IP Layer Security (IPsec) within the overall DoD approach to security is still evolving. The DoD transition to IPv6 requires IPsec as part of the toolkit to build secure networks, but this does not preclude the use of other security methods. Secure Socket Layer (SSL), HTTP over SSL (HTTPS), Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) will continue to be appropriate for some deployments.

There are several dimensions to the treatment of IPsec in this set of profiles:

1. For IPsec to be useful as a security tool it must be generally available and devices in the network cannot interfere with its use[14]; IPsec has long been considered a core part of IPv6 Capable products as recognized in RFC 4294 – IPv6 Node Requirements;

2. A node's responsibilities with respect to IPsec must be considered in the architectural context; a Router or Switch does not perform IPsec as part of normal traffic forwarding; however, it may implement IPsec when it is acting as an End Node in some deployments for network management and in routing protocols; if an Intermediate Node integrates IPsec capability to protect traffic it forwards, that Node becomes a special-purpose IA Enabled device functioning as a Security Gateway; alternatively, this function might be provided by an outboard cryptographic device;

3. Products are required to support IPsec so that it is available for use; however, this document does not require its activation or use; activation of IPsec or waiver of IPsec requirements is a deployment decision; effective use of IPsec in a particular deployment may also be dependent on integration with other elements, including IPsec-aware applications;

[14] A firewall or other IA Device might be configured to block IPsec but would not inherently "interfere" with the deployment of IPsec otherwise.

4. NSA opinion that any device implementing encryption with IPsec is an Information Assurance (IA) device subject to Federal Information Processing Standards (FIPS) and National Information Assurance Partnership (NIAP) certification may be an impediment to wide vendor support but this is beyond the scope of this document. NIST publication [7] on this subject implies that a vendor may rely on previously approved and available cryptographic modules (hardware or software) integrated with their product to avoid certification of their product set as a new IA Device.

After due consideration of the above points, the IPv6 Standards TWG consensus was to maintain the strong requirement for IPsec at the current published standards as was stated in Version 1.0 and reiterated in subsequent versions. The intention is to prevent the proliferation of IPsec deficient products that may interfere with DoD ability to fully utilize IPsec. The Product Class Profiles in Section 3 identify which Product Classes MUST be IPsec Capable; however, all IPv6 Capable products SHOULD+ be IPsec Capable. IPsec Capable requirements are:

1. IPsec Capable products MUST support the current RFC 4301 Architecture as defined in Section 2.2.1.

2. IPsec Capable products MUST support Manual Keying and MUST support Internet Key Exchange Version 2 (IKEv2), as defined in Section 2.2.2.

3. IPsec Capable products SHOULD support RFC 3971, Secure Neighbor Discovery (SEND) and RFC 3972 Cryptographically Generated Addresses (CGAs)[15].

4. Conditionally, where security requirements prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, IPsec Capable products MUST support RFC 4941 (replaces RFC 3041), Privacy Extensions for Stateless Address Auto configuration in IPv6.

Further guidance for network security can be found in RFC 4942 – IPv6 Transition/Co-existence Security Considerations and RFC 5157 – IPv6 Implications for Network Scanning. Deployments requiring the network topology hiding that IPv4 NAT provided as a side-effect should consider RFC 4864 – Local Network Protection.

A waiver process outside the scope of this document may be available (as determined by DoD component) to allow use of a product that does not at this time support the IPsec requirements as defined in this document for its Product Class Profile. However, we recognize that implementation of IPsec Version 3 and IKEv2 is not prevalent at this

[15] There are some intellectual property rights concerns with CGA and use of CGA in SEND; although the rights are offered on a "Royalty-Free, Reasonable and Non-Discriminatory License to All Implementers", the fact that a license is required may hinder adoption by some vendors.

time. Products that do not meet these standards MUST at least meet the fallback requirements defined in paragraph 2.2.3.

Multi-Protocol Label Switching (MPLS) will also be used by the IPv6 network along with routing protocols like BGP and OSPF. IPsec connection between the two ends over the network acts as the Virtual Private Network (VPN) because the IPsec connection between the two unknown end points cannot be set up arbitrarily. It is also recommended that BGP/MPLS IPv6 VPN using IPsec SHOULD be used as stated in RFCs 4364, 4577, and 4684.

2.2.1 RFC 4301 Architecture

A set of RFCs defining the Security Architecture for IP and supporting protocols was published in November 1998, and became the de facto standard for security in IPv6 products (RFC 2401 et al, referred to as IPsec Version 2 or the RFC 2401 Architecture). This set of standards was rendered obsolete (for the most part) by a set of revised standards in December 2005 (RFC 4301 et al, referred to as IPsec Version 3 the RFC 4301 Architecture).

All IPv6 Nodes implementing IPsec RFC 4301 Architecture MUST support the Security Architecture for the Internet Protocol as defined in RFC 4301 and as well:

- MUST support the Encapsulating Security Payload (ESP) defined in RFC 4303;
- SHOULD support RFC 4302, IP Authentication Header (AH);
- MUST implement ESP and AH cryptography as defined in RFC 4835 (replaces RFC 4305), Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).

IPv6 Nodes implementing IPsec RFC 4301 Architecture MUST support suites of cryptographic algorithms for IPsec and IKE including:

- Suite VPN-B in RFC 4308 – Cryptographic Suites for IPsec
    - While VPN-B specifies AES-XCBC-MAC-96 as the algorithm for ESP integrity, this algorithm is not currently FIPS approved [27]; it is unclear at this time whether that algorithm will be approved for use or an acceptable replacement for the suite will be specified in an update to the RFC
    - The Effective Date for compliance is July 2010, subject to review during the v5.0 revision cycle pending solution to the issue.
- RFC 4869
    - Suite-B-GCM-128 (for encryption plus authentication) in RFC 4869 – Suite B Cryptographic Suites for IPsec; this suite requires Diffie-Helman 256-bit random ECP (RFC 4753) and ECDSA 256 Authentication (RFC 4754)

both of which present Intellectual Property Rights (IPR) concerns to vendors[16]; this has limited the availability of this suite in products

- Suite-B-GMAC-128 (for authentication only) in RFC 4869 – Suite B Cryptographic Suites for IPsec

- In the light of the IPR concern the effective date for requiring these suites has been extended to July 2010 subject to review during the v5.0 revision cycle. Commercial availability (several vendor commitments to implementation) is a prerequisite for mandating conformance with this RFC

Conformance with these cryptographic suites will ensure that all IPsec implementations for DoD approved products support an interoperable set of options. These RFCs do not introduce new algorithms, but detail a subset of other referenced RFCs. RFC 4869 MUST be used as guidance in the interpretation of the RFCs that it references. Nodes MAY support additional cryptographic suites and options where appropriate to the deployment and application but MUST NOT depend on other nodes support. While the published USGv6 [19] does not at this time require support for RFC 4869, the basic IPsec RFCs define a sufficient set of compatible mandatory algorithms to insure interoperability with devices compliant to this profile.

NIST publications provide guidance on the use of cryptographic algorithms and key management, including FIPS 197 [26] FIPS 140-2 [27] and NIST SP 800-57 [25]. Additional guidance can be found in RFC 4308 and NSA publications on Suite B including the Fact Sheet available at http://www.nsa.gov/ia/industry/crypto_suite_b.cfm. Nothing in this Profiles document should be interpreted as extending or abrogating any prior published policy defined in the NSA and NIST publications.

IPv6 End Nodes in wireless LAN deployments requiring strong Advanced Encryption Standard (AES) security across wireless links Conditionally SHOULD support AES Counter with Cipher-block Chaining Message Authentication Code (CCM) Mode as specified in IEEE 802.11-2007 amendment 802.11i wireless security standard. [16] [17]

The requirement for RFC 4301 Architecture for IPsec is effective with publication of Version 3.0, which is 24 months from specification of MUST for this requirement in

---

[16] The following statement can be found on the NSA Suite B website: "A key aspect of Suite B is its use of elliptic curve technology instead of classic public key technology. In order to facilitate adoption of Suite B by industry, NSA has licensed the rights to 26 patents held by Certicom Inc. covering a variety of elliptic curve technology. Under the license, NSA has a right to grant a sublicense to vendors building certain types of products or components that can be used for protecting national security information." While this covers the use of the patents in USG and DoD it does not guarantee commercial availability of implementations. http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

Version 1.0 of this document. It is strongly recommended that all products meet this requirement before submission for IPv6 Capable testing. While a product may be on the IPv6 Capable Registry with an exception, DoD components may have specific deployment requirements that prevent them from buying products that do not meet the IPsec requirements.

2.2.2 IKE Version 2 Support

In conjunction with the IPsec Architecture, some method for key management is required. All IPv6 Nodes implementing IPsec need to be interoperable with Product Classes that only support Manual Keying (especially Network Appliances and Simple Servers). Therefore all IPv6 Nodes MUST support Manual Keying for IPsec.

Internet Key Exchange (IKE) was defined in RFC 2409 but has been rendered obsolete by IKE Version 2 (IKEv2). IKEv2 is simpler to deploy, has clearer documentation, is more efficient, has fewer options and fixes some of the shortcomings in IKEv1. IKEv2 is integral to the RFC 4301 Architecture and some of its advanced features depend on IKEv2 and are not available with the original IKE.

IKE Version 2 (IKEv2) is defined in the following referenced RFCs. An IPv6 Node implementing IKEv2 MUST support:

- RFC 4306, Internet Key Exchange (IKEv2) Protocol
- RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

In addition, RFC 4718 provides guidance and clarification for IKEv2 implementations.

IKEv2 by design is not interoperable with IKEv1 implementations. Products implementing IKEv2 MAY implement an operational fall-back to IKEv1 to provide interoperability.

The requirement for IKEv2 has an effective date of July 2010, which is 12 months from the publication of Version 4.0 of this document, reiterating the MUST first stated in Version 2.0. It is still strongly recommended that all products meet this requirement before submission for IPv6 Capable testing, and if not the vendor Letter of Conformance (LoC) MUST include a statement of the vendor intention regarding future support. While a product may be on the IPv6 Capable Registry with an exception, DoD components may have specific deployment requirements that prevent them from buying products that do not meet the IKEv2 requirements.

2.2.3 IPsec and IKE Fall-back Requirements

A product in a product class that MUST support IPsec which does not implement IKEv2 may be approved with an exception, but in such a case the product MUST at least

support the legacy automatic Internet Key Exchange (IKE) original version by supporting the following RFCs

- RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408, Internet Security Association and Key Management Protocol
- RFC 2409, The Internet Key Exchange (IKE)
- RFC 4109, Algorithms for Internet Key Exchange Version 1 (IKEv1)
- SHOULD support RFC 4304, Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP).

A product in a product class that MUST support IPsec RFC 4301 architecture may be approved with an exception, but in such a case the product must support the following fallback requirements for RFC 2401 architecture:

- All nodes MUST support the Security Architecture for the Internet Protocol as defined in RFC 2401
- All nodes MUST support the IPsec Encapsulating Security Payload (ESP) as defined in RFC 2406
- All nodes MUST support the IPsec Authentication Header (AH) as defined in RFC 2402,

Although this version of IPsec is RETIRED, this definition is included to help evaluate legacy products that will not meet the RFC 4301 architecture.

2.3 Transition Mechanism (TM) Functional Requirements

The long-established strategy for IPv6 transition depends on achievement of “IPv6-dominance” before the exhaustion of IPv4 address space. In an IPv6-dominant network the preponderance of end-nodes would be IPv6 Capable, all routers would be Dual Stack, and the majority of traffic would be IPv6. IPv6 Capable end-nodes would be Dual Stack to support communication with the residual IPv4 legacy nodes. Unfortunately, the day of reckoning (shortage or exhaustion of IPv4 address space) will arrive before the achievement of IPv6-dominance. The provision of significant routable IPv4 address space to support large numbers of Dual Stack end-nodes is difficult already, and will become impossible as registries restrict allocation and eventually run out. Dual Stack will not be feasible for some network operators (e.g. broadband access networks that would require a large pool of IPv4 addresses for new Dual Stack subscribers) and significant new effort is in progress in the IETF IPv6 Operations (v6ops) working group to define viable alternatives to transition that will not require IPv4 address space. While such developments will be of interest to DoD, the exhaustion of IPv4 address space will not significantly impede the deployment of Dual Stack hosts within DoD networks due to the large pool of IPv4 addresses already allocated.

Recognizing that IPv6 Nodes will coexist with legacy IPv4-only Nodes for some time, Transition Mechanisms (TMs) will be needed to support interoperability. There is some disagreement on the proper terminology to use but the term “transition” in the context of this document refers to the co-existence of IPv4 and IPv6 nodes in an operational network regardless of the time span. The editors are continuing to use the terms Transition and Transition Mechanism for consistency with previous versions and with other policy statements [8]. Several IETF working groups including Behave, Softwires, 6man and v6ops as well as a combined interim meeting have focused on the coexistence problem. The editors of this document are closely following and participating in these discussions. This work is likely to result in additional useful tools to support coexistence and transition.

Like IPsec, TM requirements are dependent on application, deployment and architectural factors. Deployment of IPv6 must accommodate the IPv4 base, as there will be no capability for IPv4 networks or nodes to interoperate with IPv6. It is difficult to define transition requirements for a particular product – the network architecture must support the long-term interoperability of IPv6-only end-nodes with IPv4-only peers, and among the residual IPv4 networks and nodes. All new nodes being acquired for connection to the DoD Global Information Grid (GIG) must support certain transition mechanisms as described in this section, and may support others.

These mechanisms include dual stack operation, configured and automatic tunneling and translation. RFC 4213, Transition Mechanisms for IPv6 Hosts and Routers, describes several general transition strategies. Each has strengths and weaknesses and would be appropriate to particular architectural situations. To provide maximum interoperability between IPv6 Capable Nodes/Networks and IPv4 nodes/networks the following principles apply:

The core network (Routers, Switches, Information Assurance Devices and any other intermediate nodes) MUST permit transit of both IPv6 and IPv4 packets. This condition can be met through Dual Stack operation across the network (dual protocol routing) OR tunneling at the edge Router. RFC 2185 “Router Aspects of IPv6 Transition” provides some additional considerations for routers deployed in dual-stack environments.

All IPv6 nodes SHOULD support Dual Stack to ensure interoperation with the IPv4 base at all phases of the transition. Conditionally, IF an IPv6 End Node is required to interoperate with an IPv4-Only End Node, it MUST accept and transmit IPv4 packets. This condition can be met with Dual Stack operation on the platform and dual stack support in the Application or via translation. The translation method can be internal to the platform (bump-in-the-stack), or provided in an external translation device. While Dual Stack in all nodes (including Dual Stack aware applications) is a preferred solution, some products (Network Appliance or Simple Server) may be IPv6-Only, and for some time IPv4-Only legacy devices will remain.

Security is a particular concern in transition mechanisms. RFC 4942 – IPv6 Transition/Coexistence Security Consideration should be consulted for guidance on the use of transition mechanisms. For example “IPv4 Mapped” addresses SHOULD NOT

be used "on-the-wire" due to security risks raised by their inherent ambiguities[17]. The Teredo method [RFC 4380] which allows IPv6 traffic to punch through simple Network Address Translators (NATs) raises a number of security issues that have been documented [11]. Therefore the use of IPv4 firewalls and Local Network Protection for IPv6 (RFC 4864) is strongly recommended in DoD networks. Teredo is not an acceptable transition mechanism in DoD networks and is explicitly prohibited by DoD policy in some DoD networks as documented in the Network Infrastructure STIG [23] and MO2 Guidance [12].

Translation based on RFC 2766, Network Address Translation – Protocol Translation (NAT-PT) is no longer supported in the IETF community and has been rendered *Historic* by the publication of RFC 4966 primarily for security concerns. NAT-PT as defined in RFC 2766 SHOULD NOT be used in operational DoD networks.[18] Mechanisms based on similar designs are being discussed within IETF and it appears that one or more of the proposals may progress to standards track. The current IETF efforts proceed with the requirement to mitigate the security risks and other problems inherent to NAT-PT.

Programs MAY use translation as a temporary coexistence tool, to continue use of legacy IPv4 components for the remainder of their life cycle. This approach SHOULD NOT be used for new acquisitions or development of systems which according to previously cited policy documents MUST be IPv6 Capable. An external translation box MAY be used for isolated IPv4-legacy devices or networks at the edge. With the deprecation of NAT-PT, there are no "standards based" translation solutions, although there are commercial products based on Stateless IP/ICMP Translation (SIIT) [RFC 2765] and as of this publication, two of these products have been tested and certified by DoD as IPv6 Capable.

If a translation solution is internal to a product, this MAY be irrelevant to the IPv6 Capable determination because the IPv4-only component and behavior has no external visibility, and thus should not impact IPv6 capability in the network. For example, a translation box combined with an IPv4-Only legacy device could be evaluated as an IPv6 Host/Workstation, Network Appliance or Server depending on its network deployment. Similarly, a complex product composed of several components may have an internal IPv4 network to connect those components, which is not visible if the "system under test" is considered to be the total complex. Only the externally visible IPv6 interface behavior is relevant to the determination of IPv6 Capability; the internal IPv4 interfaces and the IPv4 legacy devices will not be evaluated, analogous to the

---

[17] See http://tools.ietf.org/html/draft-itojun-v6ops-v4mapped-harmful-02 an expired but widely cited Internet Draft

[18] While there are security considerations, there are limited situations where NAT-PT could be used securely, and there were comments at IETF from some who intend to use it in their networks. This specification does not absolutely forbid NAT-PT, but any use requires a thorough understanding of the security concerns

internal functions (bus, memory, etc.) of any device or set of devices being evaluated as a unit under test for IPv6 Capability.

Systems MAY use other approaches to transition defined in RFCs or Internet-Drafts, as long as they do not conflict or interfere with other requirements for IPv6 Capable Nodes. RFC 4852 – IPv6 Enterprise Network Analysis provides analysis of managed network scenarios that are relevant to DoD network transition. Conditionally, where IPv6-in-IPv4 tunneling from a Dual Stack host is needed RFC 3053, IPv6 Tunnel Broker MUST be followed. Dual Stack Routers may use automatic tunneling per RFC 4852. All Routers and L3 Switches serving as Provider Edge Router SHOULD support IPv6 over MPLS following RFC 4798, Connecting IPv6 islands over IPv4 MPLS using IPv6 Provider Edge (6PE) routers.

Additional mechanisms built on top of these existing mechanisms MAY be supported. An example of this is turning a communications gateway server, such as an e-mail server, into a Dual Stacked Application-Level Gateway (ALG) that can intermediate between IPv4-only mail clients and IPv6-only mail clients.

2.3.1 NAT and Transition Mechanisms

Coexistence and Dual-Stack operations introduce some issues that network designers should be aware of and mitigate as much as possible:

IPv4 networks use Network Address Translation (NAT) to extend the lifetime of IPv4 address space, but this has the side effect of hiding the hosts from public access, and this has become accepted as a “security feature”. IPv6 obviates the need for NAT for address space multiplication, but there is some movement to retain the topology hiding feature. There are other approaches available in IPv6, in particular RFC 4864 – Local Network Protection.

IPv4 NATs present other security issues. Encryption (IPsec ESP) does not work over NATs and Authentication (IPsec AH), while possible, is complicated. The Voice-over-IP (VoIP) media payload traffic that uses user datagram protocol (UDP) cannot flow though NATs. If NATs are kept open by any proprietary or other schemes for transferring of UDP-based traffic continuously, the security vulnerabilities become enormous. These vulnerabilities extend to IPv6 coexistence.

In addition, if IPv6 networks need to use private addressing domains for IPv6 deployments, these mechanisms can be provided using IPv6 standards. This decision will need to be based on priorities and strategies of the tactical networks. However, consequences of using private IPv6 addresses in conjunction with the public addresses should be examined.

In the light of the above, the dual-stack IPv4-IPv6 router SHOULD be used in the edge of the IPv6 network while the core of the IPv6 network SHOULD be using IPv6-only routers as far as practicable. Moreover, IPv4 network will be using OSPFv2 as its interior routing protocol while the IPv6 network will use OSPFv3. This will make sure

that IPv4-based VPN and IPv6-based VPN remain logically separated ensuring interoperability without any security vulnerabilities.

2.4 Quality of Service (QoS) Functional Requirements

As IPv6 Quality of Services (QoS) extensions and usage guidance matures, this profile will be expanded. The following are current IPv6 protocols related to QoS signaling:

- RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
  - Routers MUST process Differentiated Service (DiffServ) headers and offer differentiation of traffic service classes
- RFC 3168, The Addition of Explicit Congestion Notification (ECN) to IP
  - Routers SHOULD process the ECN field in the IP header
- Routers to be deployed in an Integrated Services (IntServe) architecture SHOULD+ support RSVP based QoS as defined in the following RFCs:
  - RFC 2205, Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification
  - RFC 2207, RSVP Extensions for IPSEC Data Flows
  - RFC 2210, The Use of RSVP with IETF Integrated Services
  - RFC 2750, RSVP Extensions for Policy Control
- Optionally, Routers may also support RFC 3175, Aggregation of RSVP for IPv4 and IPv6 Reservations
- The following RFCs MAY be supported in some deployments:
  - RFC 3181, Signaled Preemption Priority Policy Object
  - RFC 2961, RSVP Refresh Overhead Reduction Extension
  - RFC 4495, A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow
  - RFC 2998, A Framework for Integrated Services Operation over DiffServ Networks
  - RFC 2996, Format of the RSVP DCLASS Object
  - RFC 2746, RSVP Operation Over IP Tunnels
  - RFC 3182, Identity Representation for RSVP
  - RFC 2872, Application and Sub Application Identity Policy Element for Use with RSVP
  - RFC 2747, RSVP Cryptographic Authentication

2.5 Mobility (MOB) Functional Requirements

Mobile IPv6 (MIPv6) and NEtwork MObility (NEMO) are emerging IPv6-based network mobility services that SHOULD be implemented on new IPv6 systems. MIPv6 is not mature enough to be generally mandated, and work continues in several important related areas to fill holes in the Mobility architecture. The profile for Mobility presented here is not a complete analysis of all Mobility specifications, but attempts to cover some of the basic requirements for MIPv6-capable Hosts and Routers. An organization considering a Mobility deployment will have to evaluate applicability of the RFCs cited

here, as well as more recently published RFCs and current work in the IETF. Mobile IP provides some very powerful and flexible options for deployment and should be considered in long-term planning and evaluated through experimentation and pilot programs.

At this time MIPv6 is not mandatory for any particular product class; application and deployment conditions will dictate whether these optional features are required in products selected for particular configurations. These requirements as a whole are conditional: IF MIPv6 is included, the product MUST implement it as defined in the RFCs cited in this section. MIPv6 is defined in RFC 3775, Mobility Support in IPv6 and security for MIPv6 is defined in RFC 3776, Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents as updated by RFC 4877, Mobile IPv6 Operations With IKEv2 and the Revised IPsec Architecture. NEMO is defined in RFC 3963, Network Mobility (NEMO) Basic Support Protocol.

RFC 4877 recently extended the previous definition of MIPv6 security, RFC 3776. RFC 3776 specified IKEv1 for MIPv6 security while RFC 4877 provides compatibility with the RFC 4301 IPsec architecture by specifying the use of IKEv2 with MIPv6. While the requirement on RFC 4877 is new in Version 3.0 of this specification, with an effective date 24 months following publication, we recommend that MIPv6 Capable Nodes and Home Agent Routers support IKEv2 for MIPv6 security as soon as practical.

There are three primary roles in a MIPv6 deployment:

1. Mobile Node (MN) – a Mobile Node implements the host requirements for MIPv6

2. Home Agent (HA) – a Home Agent is an enhanced router on the home network of a MN which maintains bindings of the MN home address to its current care of address, and arranges for forwarding (via tunnel) of packets which appear on the home link addressed to the MN home address

3. Correspondent Node (CN) – any other node exchanging packets with a MN; any unmodified IPv6-capable node is a CN, without the advantage of Route Optimization (RO)

Route Optimization provides a means for an enhanced CN to discover the care of address for a MN, and to avoid triangular routing via the HA after the initial exchange of packets.

2.5.1 MIPv6 Capable Node

An End Node which can operate as a Mobile IPv6 node is “MIPv6 Capable”. If a product will be deployed as a MIPv6 Capable Node it MUST support the Mobile Node requirements in RFC 3775, MUST support RFC 3776 and MUST support RFC 4877. A MIPv6 Capable Node SHOULD+ support RFC 4282, The Network Access Identifier and SHOULD+ support RFC 4283, Mobile Node Identifier Option for MIPv6. While it appears there may be some incentive to support MIPv6 in portable devices, it is more

difficult to see a use case for desktop systems. However, the distinction between "desktop" and "portable" has been shrinking with trend towards a single laptop for desktop and travel use. MIPv6 may be a useful feature for OS vendors to consider for all versions, not just those targeted to hand-held and palm-top devices.

2.5.2 Home Agent Router

A Router that will be deployed as a Home Agent MUST support the Home Agent requirements in RFC 3775, MUST support RFC 3776, MUST support RFC 4877 and SHOULD+ implement RFC 4282 and RFC 4283.

2.5.3 NEMO Capable Router

Network Mobility (NEMO) extends Mobile Node capability to an entire sub-network. A Router which meets the requirements for Network Mobility is a "NEMO Capable Router." A NEMO Capable Router MUST implement RFC 3963.

2.5.4 Route Optimization

Any IPv6 Capable Node can interoperate with a MIPv6 Mobile Node as a Correspondent Node as stated in Section 8.1 of RFC 3775 (no additional functionality is required). MIPv6 includes a feature called "Route Optimization" which increases the efficiency of packet routing between a Mobile Node and Correspondent Node. An IPv6 Capable Node to be deployed where MIPv6 is prevalent SHOULD support Route Optimization as defined in RFC 3775.

Route Optimization presents some unique challenges. There is a misalignment of incentive – for RO to be effective it must be widely implemented by the Correspondent Nodes including general purpose servers for which it provides no benefit. RO certainly would provide performance enhancement for a geographically dispersed enterprise, where it would eliminate triangular routing of packets to a home network when the MN was visiting a location where the enterprise maintained corporate servers. While it would be helpful for general servers to support RO, due to current lack of MIPv6 deployments and the small benefit it does not make sense to require RO for servers at this time.

RO raises some security concerns, especially in deployments where it would be undesirable to reveal the location of a travelling MIPv6 MN. At least an approximate location can be derived from IPv6 prefix of the network where the MN is operating. In those cases, it would be better to disable RO in the MN and rely on the Home Agent to conceal the current location of the MN.

2.6 Bandwidth Limited Networks Functional Requirements

IPv6 support for RF wireless systems and other bandwidth limited deployments will benefit from optimizations including header compression. The requirements in this section are conditional; where header compression is needed, the listed RFCs MUST

be followed. Please note that header compression by its nature may not be compatible with IPsec in some configurations.

2.6.1 Robust Header Compression (RoHC)

Robust Header Compression (RoHC) is designed to provide a significant improvement in transmission efficiency for bandwidth limited networks. It will likely be used in cellular networks (2.5G and 3G) and other wireless links. It is an emerging technology, and currently optional. Where it is used the following RFCs are relevant:

- RFC 3095, RObust Header Compression (ROHC) – Supports reliable IP header compression over wireless links. When header compression over wireless links is required ROHC MUST be used.
- RFC 4815, Corrections and Clarifications to RFC 3095.
- RFC 4995, RoHC Framework – this RFC is an unmodified extract of the framework definition from RFC 3095.
- RFC 4996, RoHC: A profile for TCP/IP – this RFC provides a specific profile for compression of TCP/IP headers based on the framework defined in RFC 4995.
- For compression over various PPP and low-speed links – RFC 3241, RObust Header Compression (ROHC) over PPP.
- RFC 3843, RObust Header Compression (ROHC): A Compression Profile for IP– Additional guidance for extending RFC 3095 for any arbitrary IP header chain. Supports reliable IP header compression over wireless links. When header compression over wireless links is required ROHC MUST be used.
- RFC 4362, RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP - Additional guidance for optimizing RFC 3095 for various link-layers. Supports reliable IP header compression over wireless links.

2.6.2 IP Header Compression

IP Header Compression is an earlier alternative to RoHC. IP Header Compression is optional; where it is used the following RFCs are relevant.

- RFC 2507, IP Header Compression, February 1999 (For low-speed wired links requiring compression)
- RFC 2508, Compressing IP/UDP/RTP Headers for Low-Speed Serial Links (For low-speed serial links requiring compression)
  RFC 3173, IP Payload Compression

2.7 Network Management (NM) Functional Requirements

Networking infrastructures at scales larger than today's networks require that both Hosts and Routers have scalable mechanisms to configure, to monitor and to manage their behavior. The Simple Network Management Protocol (SNMP) provides a means for automated remote management of IPv6 Nodes based upon Management Information Bases (MIBs) for IPv6 protocols. While support in Routers is common, SNMP management has rarely been used in the industry for the management of Hosts.

While the requirements for Network Management are still evolving, SNMP Version 3 (SNMPv3) as defined in Standard 62/RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks is the preferred method of remote management, although alternative management tools are also permitted. Prior to SNMPv3 SNMP included only rudimentary security. Conditionally, IF IPv6 Capable Nodes are managed via SNMP the management MUST support SNMPv3 as defined in IETF Standard 62:

- RFC 3411, An Architecture for Describing Simple Network Management Protocol Version 3 (SNMPv3)
- RFC 3412, Message Processing and Dispatching for the SNMP
- RFC 3413, SNMP Applications

While configuration via SNMP is not mandated for all deployments, availability in products is recommended to enable the use of SNMP for monitoring and configuring network elements when desirable.

SNMP implementation is built around a Management Information Base (MIB) defined by several general MIB and protocol RFCs as well as MIB RFCs specific to a node type or specific features. Conditionally, IF IPv6 Capable Nodes are managed via SNMP implementations MUST support the following general MIB specifications:

- RFC 3595, Textual Conventions for IPv6 Flow Label
- RFC 4293, Management Information Base (MIB) for IP, obsoletes RFC 2465 and 2466 and MUST be supported to provide SNMPv3 management of IPv6 features; these two RFCs have been combined with IPv4 MIBs and updated in RFC 4293 to cover all IP management

In general, if a feature/function/protocol is configured or managed via SNMP, support for the corresponding MIB RFC is conditionally required.

Hosts and Servers managed by SNMPv3 Conditionally SHOULD+ also support the following MIBs:

- RFC 4022, Management Information Base for the Transmission Control Protocol
- RFC 4113, Management Information Base for the User Datagram Protocol

Routers managed by SNMPv3 MUST also support the following MIBs:

- RFC 4292, Forwarding
- Conditionally, If the IPsec Security Policy Database is configured through SNMP, RFC 4807
- Conditionally, if the Differentiated Services Architecture is configured through SNMP, RFC 3289
- Conditionally, if the router supports tunneling RFC 4087
- Conditionally, if the router supports MIPv6 RFC 4295

Other MIBs that MAY be appropriate to specific products or features include:

- RFC 4807, IPsec Security Policy Database Configuration MIB SHOULD be supported when the IPsec Security Policy Database is used
- RFC 4292, IP Forwarding Table MIB SHOULD be supported

IPv6 Capable Nodes managed via SNMP MUST support SNMP over an IPv6 interface.

2.8 Routing Protocol Requirements

A Router may be deployed as an Exterior Router (at the network edge) or an Interior Router (in the network core). Router products MAY include both capabilities.

2.8.1 Interior Router Requirements

An Interior Router MUST support OSPF for IPv6 (OSPFv3) as specified in RFC 5340[19]. Conditionally, an Interior Router implementing OSPFv3 MUST support RFC 4552, Authentication/Confidentiality for OSPFv3[20].

The Intermediate System to Intermediate System (IS-IS) routing protocol is used in DoD backbone networks. IS-IS was developed roughly in parallel with OSPF, originally for OSI stack networks and later adapted to TCP/IP networks.

Conditionally, an IPv6-Capable Interior Router deployed in an IS-IS routing architecture (for IPv6-only or dual-stack operation) MUST implement IS-IS for IPv6 as specified in:

- RFC 5308 – Routing IPv6 with IS-IS
- RFC 5304 – IS-IS Cryptographic Authentication
- RFC 5310 – IS-IS Generic Cryptographic Authentication

IS-IS implementers should monitor further specification of ancillary features in the IETF ISIS Working Group, including http://tools.ietf.org/html/draft-ietf-isis-ipv6-te-06 on traffic engineering.

An Interior Router MAY support other routing protocols as appropriate to the deployed routing architecture.

2.8.2 Exterior Router Requirements

An Exterior Router (BGP gateway) between routing systems MUST support:

- RFC 4271, A Border Gateway Protocol 4 (BGP-4)

---

[19]RFC 5340 recently replaced RFC 2740. An Interior Router not supporting 5340 at this time MUST at least support 2740.

[20] 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.

- RFC 1772, Application of the Border Gateway Protocol in the Internet
- RFC 2545, Use of BGP-4 Multi-protocol Extensions for IPv6 Inter-Domain Routing
- RFC 4760[21], Multi-protocol Extensions for BGP-4
- Conditionally, an edge router MUST support RFC 2784, Generic Router Encapsulation (GRE): IPv6-in-IPv4 tunnels when transiting IPv4 core network; Routers implementing GRE SHOULD also support RFC 2890 – Key and Sequence Number Extensions to GRE.
- Conditionally, an edge router MUST support RFC 2473, Generic Packet Tunneling in IPv6 Specification to provide IPv4-in-IPv6 tunnels;

2.9 Automatic Configuration

IPv6 includes two methods by which a node can automatically discover and configure its own unique global IPv6 interface address(es) along with other network configuration parameters. Stateless Address Autoconfiguration (SLAAC) and Dynamic Host Configuration Protocol for IPv6 (DHCPv6) are complementary methods, but not mutually exclusive. A product may include an implementation of either or both.

SLAAC is appropriate in deployments where Host/Workstation and Network Appliance nodes are permitted to obtain their interface address(es) dynamically from the currently available on-link router. DHCPv6 provides for a stateful equivalent to SLAAC in deployments where more central control is necessary, through administration of DHCP servers. Due to the nature of many deployments, configuration management requirements may imply a preference for DHCPv6 for automatic configuration. For example, DoDI 8520.2 – PKI and Public Key Enabling will depend on DHCPv6 and Dynamic DNS to support Fully Qualified Domain Names (FQDN) which are not supported in SLAAC.

There will be deployments where static IP addresses are always assigned so all nodes implementing either or both autoconfiguration methods MUST have a configuration option to disable the autoconfiguration. Autoconfiguration is generally inappropriate for Intermediate Nodes (Routers, L3 Switches and IA Devices) and Servers but MAY be implemented for configuring the global addresses for administrative interface on any node. However, all nodes MUST generate link-local addresses as specified in RFC 4862 (replaces RFC 2462 as of version 3.0 of this document).

Network designers SHOULD consider RFC 4192 “Procedures for Renumbering an IPv6 Network without a Flag Day” when planning network address architecture and whether and how to implement autoconfiguration. RFC 4192 indicates that SLAAC and DHCPv6 both provide advantages that help mitigate the impact of renumbering on hosts.

---

[21] Recently obsoleted RFC 2858

2.9.1 Stateless Address Autoconfiguration (SLAAC)

An IPv6 Node using SLAAC to configure its unique IPv6 interface addresses MUST implement the host requirements specified by RFC 4862 (replaces RFC 2462 as of version 3.0 of this document) and SHOULD+ implement RFC 5175[22] extensions to Router Advertisement flags.

2.9.2 Dynamic Host Configuration Protocol – Version 6 (DHCPv6) Client

An IPv6 Node using DHCPv6 to configure its unique IPv6 interface address(es) MUST implement the client requirements specified by RFC 3315, DHCPv6.

2.9.3 DHCPv6 Server

An IPv6 Node that is deployed as a DHCPv6 Server MUST implement the server requirements specified by RFC 3315, DHCPv6 and SHOULD implement IPv6 Prefix Delegation as specified by RFC 3633. RFC 3769 provides additional background on the design of Prefix Delegation.

2.9.4 DHCPv6 Relay Agent

An IPv6 Node that is deployed as a DHCPv6 Relay Agent MUST implement the relay agent requirements specified by RFC 3315, DHCPv6.

2.10 Virtual Private Network (VPN)

It is common for managed network environments to offer Virtual Private Network (VPN) to allow secure remote access. VPN is a Conditional requirement because not every installation will use it. In addition, not all VPN devices will be placed in a position where they need to support full routing tables as required by BGP or OSPF. In deployments that require VPN with WAN interfaces and Interior or Exterior routing, the device Conditionally MUST conform to:

- RFC 4364 – BGP/MPLS IPv6 VPNs
- RFC 4577 – OSPF Edge Protocol for BGP/MPLS IPv6 VPNs
- RFC 4684 – Constrained Route Distribution for BGP/MPLS IPv6 VPNs

2.11 Additional UCR IA and Interoperability Recommendations

The publication of the 2008 version Unified Capabilities Requirements (UCR2008) included a restatement of the IPv6 requirements as specified in Version 2.0 of this document, with some changes corresponding to Version 3.0. UCR2008 included a number of additional Information Assurance (IA) and interoperability statements that

[22] RFC 5175 obsoleted RFC 5075 which was cited in draft 2.1 of this document

clarified or extended a particular RFC that have been identified as divergence from this Profiles document.

While it would be optimal to have a single definition of IPv6 requirements for all DoD purposes, editorial constraints on the publication of UCR2008 maintains a parallel restatement of the requirements. The differences between the two documents have been minimized through cooperative efforts of both editorial teams, and mainly a remnant of the derivation of the UCR2008 document from a specific statement of Real-Time Services (RTS) requirements. UCR2008 (Change 1) update is expected to be published around the time that Version 4.0 of this document is published, and will be a further step towards eliminating differences and avoiding parallel restatement. The two documents are intended to be companions, with UCR defining the overarching DoD architecture and requirements for all vertical services (voice, video and data) over IP networks and the IPv6 Profiles providing specific detailed definition of IPv6-Capable product requirements for network interoperability.

The following recommendations[23] should be considered in the specification, design, implementation and deployment of IPv6-Capable products. These recommendations are included in this (draft) version of the Profiles to elicit further analysis and comment from potential implementers. After further analysis each of these recommendations will either:

1. Be referred to IETF as a general deficiency requiring an update RFC;
2. Become a baseline requirement in a future version of this document;
3. Remain a specific modification in the UCR document;
4. Be deemed inappropriate or redundant with respect to other DoD policy statements, or otherwise unnecessary.

2.11.1 Operation of Internet Control Message Protocol (ICMPv6)

Internet Control Message Protocol for IPv6 (ICMPv6) extends ICMP to work with IPv6 and to provide additional support for IPv6 features. ICMP is used to provide some signaling and feedback (error messages) to enable features such as Path MTU Discovery. There are situations where these capabilities should be limited to moderate the risk of Denial of Service attack or exploit of a covert channel.

1. RFC 4443 Section 3.1 states: *A Destination Unreachable message SHOULD be generated by a router, or by the IPv6 layer in the originating node, in response to a packet that cannot be delivered to its destination address for reasons other than congestion.*

[23] Portions of this section are a result of analysis contributed by the Unified Capabilities Requirements (UCR) program.

The following statement should be appended to this section: *A system MUST have a configuration option to enable or disable generation of a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.* This is recommended because there are situations where it is appropriate to drop packets without an indication of why they are being dropped.

2. RFC 4443 Section 4.2 states: *An Echo Reply SHOULD be sent in response to an Echo Request message sent to an IPv6 multicast or anycast address.*

   The following statement should be appended: *The system shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address. NOTE: The number of responses may be traffic conditioned to limit the effect of a denial of service attack.*

3. RFC 4443 Section 5.2.6 states: *It is recommended that the upper layers perform some form of validation of ICMP messages (using the information contained in the payload of the ICMP message) before acting upon them.*

   This recommendation should be strengthened: *The system MUST validate ICMPv6 messages, using the information contained in the payload, prior to acting on them.* While it is not possible to eliminate all exploits of the ICMPv6 protocol, systems should be designed with reasonable safeguards.

4. RFC 1981 Section 4 states: *A node may receive a Packet Too Big message reporting a next-hop MTU that is less than the IPv6 minimum link MTU. In that case, the node is not required to reduce the size of subsequent packets sent on the path to less than the IPv6 minimum link MTU, but rather must include a Fragment header in those packets [RFC 2460].*

   This statement should be clarified or strengthened to read*: If Path MTU Discovery is used and a Packet Too Big message is received requesting a next-hop MTU that is less then the IPv6 minimum link MTU, the system MUST ignore the request for the smaller MTU and MUST include a fragment header in the packet. NOTE: This is to mitigate an attack where the path MTU is adequate, but the Packet Too Big messages are used to make the packet so small it is inefficient.*

2.11.2 Address Configuration

The flexibility of automatic configuration of addresses comes with some new attack surfaces that should be carefully considered in some deployments.

1. RFC 4861 (similarly RFC 2461) Section 4.4 states: *It [the override flag bit] SHOULD NOT be set in solicited advertisements for anycast addresses and in*

solicited proxy advertisements.

This statement should be strengthened to say: *The system MUST NOT set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements.*

2. RFC 2461 Section 7.2.5 states: I*f the target's Neighbor Cache entry is in the INCOMPLETE state when the advertisement is received, one of two things happens. If the link layer has addresses and no Target Link-Layer address option is included, the receiving node SHOULD silently discard the received advertisement. Otherwise…*

   For safety, the statement should be strengthened to say *If a valid neighbor advertisement is received by the system and the system 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 system MUST silently discard the received advertisement. Otherwise…*

3. RFC 2461 Section 6.2.7 states*: Detected inconsistencies indicate that one or more routers might be misconfigured and SHOULD be logged to system or network management.*

   An additional clause should be added, covering the audit requirement for such events: *If the system supports routing functions, the system MUST inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link and MUST log any inconsistent router advertisements.*

4. RFC 2461 Section 6.3.6 1states: *Routers that are reachable or probably reachable state SHOULD be preferred over routers whose reachability is unknown or suspect.*

   This statement should be strengthened to say: *The system MUST prefer routers that are reachable over routers whose reachability is suspect or unknown.*

2.11.3 Dynamic Host Configuration Protocol (DHCPv6)

DHCPv6 provides an alternative and complementary method in conjunction with Neighbor Discovery and Stateless Address Configuration (SLAAC) for configuring nodes in IPv6. Section 3.2.3 of this document cites the requirements for DHCPv6 as specified in RFC 3315; there are several features and options that merit additional analysis to ensure security.

1. RFC 3315 Section 17.1.2 has the following statement: *If the first RT elapses and the client has received an Advertise message, the client SHOULD continue with a client-initiated message exchange by sending a Request message.*

This statement should be clarified and strengthened to: *If 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, the client MUST continue with a client-initiated message exchange by sending a Request message*

2. RFC 3315 Section 17.1.2 has the following statement: *After the DHCP client stops trying to configure the interface, it SHOULD restart the reconfiguration process after some external event, such as user input, system restart or when the client is attached to a new link*.

   For clarity and to ensure that the configuration process eventually succeeds, the statement above should be amended to the following: *If the system is a DHCPv6 client and the DHCPv6 message exchange fails, it MUST restart the reconfiguration process on triggering events to include: 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.*

3. RFC 3315 Section 18.1.5 states: *The client SHOULD include a Client Identifier option to identify itself to the server. If the client does not include a Client Identifier option, the server will not be able to return any client-specific options to the client, or the server may choose not to respond to the message at all. The client MUST include a Client Identifier option if the Information-Request message will be authenticated.*

   These three statements should be strengthened and simplified to read: *The client MUST include a Client Identifier option to identify it to the server, enabling the server to authenticate the Information-Request message and return client-specific options.*

4. RFC 3315 Section 18.1.8 has the following statement: *The client SHOULD perform duplicate address detection on each of the addresses in any IAs it receives in the Reply message before using that address for traffic.*

   This should be strengthened to read: *The client MUST perform duplicate address detection upon receipt of an address from the DHCPv6 server prior to transmitting packets using that address for itself.* Note that while Section 2.1 of this document (Base Requirements) states that all nodes MUST perform DAD as part of SLAAC this statement would make the requirement explicit for address configuration using DHCPv6. Further note that the requirement for DAD is subject to further analysis due to security concerns with Neighbor Discovery and DAD itself.

5. RFC 3315 Section 19.4 states: *Since the results of a reconfiguration event may affect application layer programs, the client SHOULD log these events, and MAY*

notify these programs of the change through an implementation-specific interface.

This statement should be strengthened to read: *Since the results of a reconfiguration event may affect application layer programs, the client MUST log these events; conditionally, IF an implementation-specific API is available for notification, the client MUST notify the application layer programs of the change.*

6. RFC 3315 Section 21.4.4.2 states: *If a client does accept an unauthenticated message, the client SHOULD inform any local users and SHOULD log the event.*

   The above statement should be strengthened to: *If the system supports DHCPv6 authentication, it MUST discard unauthenticated DHCPv6 messages and log the event; otherwise, if a client does accept an unauthenticated message, the client SHOULD inform any local users and SHOULD log the event*

2.11.4 IPsec Configuration

The definition of IPsec in RFC 4301 leaves several key features open as options or recommendations rather than MUSTs. Systems that implement IPsec [RFC 4301] should consider strengthening these clauses as described here.

1. RFC 4301 Section 4.4 describes a potential implementation of IPsec security gateway, where multiple contexts are maintained for several subscribers. The paragraph suggests that *IPsec Security Associations (SAs) MAY be conveyed from initiator to responder in the signaling messages, with the result that IPsec SAs are created with a binding to a particular context.*

   An additional statement should follow the above, conditioned on the implementation being a security gateway: *IF a system maintains multiple contexts for independent subscriber sessions (acting as a security gateway) it MUST bind the SA for each session to the particular context.*

2. RFC 4301 Section 4.4.1 defines three Processing Choices on an entry in the Security Policy Database (SPD): DISCARD, BYPASS or PROTECT using IPsec. This allows a system administrator to determine whether some or all traffic will be protected with IPsec versus allowed to bypass this protection.

   For IA reasons, in some situations the following statement should be added: *The system MUST have an option to disallow the BYPASS IPsec Processing Choice.*

3. RFC 4301 Section 4.4.2 has a statement: *In particular, simply storing the (remote tunnel header IP address, remote SPI) pair in the SPD cache is not sufficient, since the pair does not always uniquely identify a single SAD entry.*

   Since a single SAD entry may be associated with multiple Security Associations,

add a statement: *The SAD cache MUST have a method to uniquely identify a SAD entry.*

4. RFC 4301 Section 5.2 has the statement: *Every SPD SHOULD have a nominal, final entry that catches anything that is otherwise unmatched, and discards it.*

   For completeness and safety, this statement should be strengthened to say: *An implementation of the SPD MUST default to DISCARD for any traffic that does not match any entries, using a nominal, final entry that discards anything that is otherwise unmatched.*

5. RFC 4301 Section 5.2 states: *The audit log entry for this event SHOULD include the current date/time, SPI, source and destination of the packet, IPsec protocol, and any other selector values of the packet that are available.*

   Auditability is an important consideration, thus this statement should be strengthened to read: *The system MUST log an event when it receives a packet that does not match any SPD cache entries and the system determines it should be discarded; the event log MUST include the date/time and any selector values that are available, including the Security Parameter Index (SPI), IPSec protocol, source and destination of the packet, and any other selector values of the packet.* Logging is mandatory and should be as complete as possible; however, not every event will have all the fields mentioned.

6. RFC 4301 Section 5.2 states that in addition to logging an event for INVALID_SELECTORS that *the system SHOULD also be capable of generating and sending an IKE notification of INVALID_SELECTORS to the sender (IPsec peer), indicating that the received packet was discarded because of failure to pass selector checks.*

   In some situations it would be inappropriate to send such a message to the sender, and thus an additional clause should inserted: *the system should include a management control to allow an administrator to enable or disable the ability of the system to send an Internet Key Exchange (IKE) notification of an INVALID_SELECTORS.*

7. RFC 4303 Section 3.4.3 states; *This SHOULD be the first ESP check applied to a packet after it has been matched to an SA, to speed rejection of duplicate packets.*

   For completeness and certainty this statement should be strengthened to read: *immediately after a packet has been matched to its SA the system MUST check that 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.*

2.11.5 Key Exchange

The protections afforded by IPsec rely upon a key exchange protocol, IKEv2, for the configuration of many of the cryptographic algorithms available for use. While configuring keys manually may be appropriate in some situations, this method is not scalable to large pools of end devices, and may not be workable in tactical deployments. The following modifications to IKEv2 specifications should be considered when planning a deployment utilizing IKEv2.

1. RFC 4306 Section 2.4 has the statement: *To prevent this, the initiator MAY be willing to 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 should be ignored whether or not they are cryptographically valid.*

   This last statement should be strengthened. *Once a cryptographically valid response is received, all subsequent responses MUST be ignored whether or not they are cryptographically valid.*

2. RFC 4306 [Section 2.6] has the statement regarding protection against flooding from forged IP addresses: *To accomplish this, a responder SHOULD when it detects a large number of half-open IKE SAs reject initial IKE messages unless they contain a Notify payload of type COOKIE.* This should be strengthened to MUST.

3. RFC 4306 Section 3.4.3 states: *If an SA bundle has been inactive for a long time and if an endpoint would not initiate the SA in the absence of traffic, the endpoint MAY choose to close the SA instead of rekeying it when its lifetime expires. It SHOULD do so if there has been no traffic since the last time the SA was rekeyed.* The last clause should be strengthened to MUST.

4. RFC 4306 Section 3.21 discusses error handling and in particular cautions about responding to errors that occur before establishment of a cryptographically protected IKE_SA. One clause states *If the message is marked as a request, the node MAY audit the suspicious event and MAY send a response*.

   For completeness, after this clause insert *the system MUST limit the frequency at which it responds to messages on UDP port 500 or 4500 when they are outside the context of a security association known to it; excess messages MUST be logged as a suspicious event, and the system MUST NOT respond*.

5. RFC 4306 Section 4 lists a number of optional features that can be ignored without harming interoperability with minimal implementations including *Ability to request (and respond to a request for) a temporary IP address on the remote end of the tunnel.*

IA considerations suggest that *The system MUST NOT request a temporary IP address on the remote end of a tunnel, and MUST NOT respond to such a request for a temporary IP address.*

2.11.6 Other IA Considerations

1. RFC 2460 Section 4 states: Hosts or routers that do not support the functions of the Flow Label field are required to set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet. The Flow Label field can be exploited as a covert channel to pass information outside the payload protected by IPsec. The statement above should be modified to state: The system MUST NOT use the Flow Label field as described in RFC 2460. The system MUST set the Flow Label field to zero when originating a packet, MUST NOT modify the Flow Label field when forwarding packets, and MUST ignore the Flow Label field when receiving packets.

2. RFC 4443 Section 2.4 (f) states: *ICMPv6 rate-limiting parameters SHOULD be configurable*."

   It would be better to state that *the system MUST have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages.* This is recommended for interoperability and reducing risk of some modes of denial-of-service attack.

2.11.7 Interoperability Considerations

1. RFC 4007 Section 6 states in reference to default zone in a scope: *And, when supported, the index value zero at each scope SHOULD be reserved to mean "use the default zone".*

   This statement should be strengthened and clarified to read: *The system MUST use a scope index value of zero (0) to represent "use the default zone."*

2. RFC 4861 (similarly 2461) Section 7.2.5 states: *When a valid Neighbor Advertisement is received (either solicited or unsolicited), the Neighbor Cache is searched for the target's entry. If no entry exists, the advertisement SHOULD be silently discarded.*

   This statement should be strengthened to read: *If a valid neighbor advertisement is received by the system and the system neighbor cache does not contain the target's entry, the advertisement shall be silently discarded.*

3. RFC 4861 (similarly 2461) Section 7.3.3 states with respect to resolving out of INCOMPLETE state: *If address resolution fails, the entry SHOULD be deleted, so that subsequent traffic to that neighbor invokes the next-hop determination procedure again.*

To ensure that next-hop determination is invoked again this statement should be strengthened to MUST.

3 Product Class Profiles

The Product Class Profiles for each of the Product Classes defined in section 1.6 can now be specified in terms of the Functional Requirements defined in Section 2. For a specific product presented for evaluation as IPv6 Capable, the information in Section 1.6 should be used to determine the appropriate Product Class for the product and the corresponding Product Class Profile in the following sections.

Additional Product Classes may be added in the future as new products are developed and presented for evaluation, or these Product Classes may be modified to cover additional products. The following paragraphs provide detailed Profiles for each Product Class.

3.1 IPv6 End Nodes

3.1.1 Host/Workstation Product Class Profile

IPv6 Capable Host/Workstation Products:

- MUST implement the Base Requirements (Section 2.1);
- MUST implement RFC 3810, MLDv2 and RFC 2711, Router Alert Option;
- MUST implement at least one method of autoconfiguration, ether SLAAC as specified in section 2.9.1 or DHCPv6 autoconfiguration as specified in section 2.9.2;
- MUST be IPsec Capable, implementing the IPsec Functional Requirements (Section 2.2);
  - And SHOULD+ support RFC 4941 (replaces RFC 3041), Privacy Extensions for Stateless Address Autoconfiguration;
  - Conditionally, Hosts/Workstations that will operate on networks requiring privacy address extensions or otherwise need to maintain anonymity MUST follow RFC 4941 (replaces RFC 3041) when generating interface identifiers;
- Conditionally, MUST support Transition Mechanism (Section 2.3) requirements for Dual Stack capability IF intended deployment requires interoperation with IPv4-only legacy nodes;

- MAY support QoS Functional Requirements (Section 2.4);
- Conditionally, MUST implement Correspondent Node (CN) with Route Optimization (Section 2.5.4) IF intended deployment requires interoperation with MIPv6 Capable Nodes; note that Route Optimization is an efficiency concern with priority related to the prevalence of and interaction with MIPv6 Mobile Nodes;
- Conditionally, MUST implement MIPv6 Capable Node Functional Requirements (Section 2.5.1) IF intended to be deployed as a Mobile Node;
- MUST be capable of using IPv6 DNS Resolver function per RFC 3596, DNS Extensions to Support IPv6;
- MUST implement RFC 3484, Default Address Selection for IPv6. It is expected that IPv6 nodes will need to deal with multiple addresses. Section 2.1 of RFC 3484 requires a default "policy table" and encourages implementations to allow manual configuration. Host/Workstation nodes SHOULD+ provide a user configurable policy table to enable override of Default Address Selection (i.e. to force use of specific address in certain situations).[24]

3.1.2 Network Appliance Product Class Profile

IPv6 Capable Network Appliances:

- MUST implement the Base Requirements (Section 2.1);
- SHOULD+ be IPsec Capable by supporting the IPsec Functional Requirements (Section 2.2);
- SHOULD support the complete Host/Workstation profile if possible.

While it is preferable that all IPv6 Capable Products interoperate with IPv4-Only legacy nodes and networks, a Network Appliance MAY be IPv6-Only and therefore rely upon external methods (tunneling or translation) to interoperate with IPv4.

3.1.3 Server Product Class Profiles

3.1.3.1 Advanced Server Profile

IPv6 Capable Advanced Servers:

- MUST implement the Base Requirements (Section 2.1);
  - And MUST implement RFC 3810, MLDv2 and RFC 2711, Router Alert Option;
- MUST be IPsec Capable, implementing the IPsec Functional Requirements (Section 2.2);

[24] This recommendation is under consideration for upgrade to a MUST. Implementations with configurable policy tables are strongly recommended, and where possible, choose to use operating systems that support a configurable policy table.

- Conditionally, IF an Advanced Server is acting as a client AND needs to maintain anonymity, it MUST support RFC 4941 (replaces RFC 3041), Privacy Extensions for Stateless Address Autoconfiguration when generating interface identifiers; note that a server's primary address will likely be registered in DNS or well-known, so privacy addressing normally would not apply.
- Conditionally, MUST support Transition Mechanism (Section 2.3) requirements for Dual Stack capability IF intended deployment requires interoperation with IPv4-only legacy nodes;
- MAY support QoS Functional Requirements (Section 2.4);
- If the server is to be deployed to support MIPv6 mobile clients, it Conditionally MUST implement Correspondent Node (CN) with Route Optimization (Section 2.5.4). Although any server MAY interoperate with MIPv6 Capable Nodes Route Optimization is not unconditionally required for general purpose servers at this time - note that Route Optimization is an efficiency concern with priority related to the prevalence of and interaction with MIPv6 Mobile Nodes;
- SHOULD support the Network Management requirements (Section 2.7)
- MUST be capable of using IPv6 DNS Resolver function per RFC 3596, DNS Extensions to Support IPv6;
- MUST implement RFC 3484, Default Address Selection for IPv6. It is expected that IPv6 nodes will need to deal with multiple addresses. Section 2.1 of RFC 3484 requires a default "policy table" and encourages implementations to allow manual configuration. Advanced Server nodes SHOULD+ provide a user configurable policy table to enable override of Default Address Selection (i.e. to force use of specific address in certain situations).[25]

A Server will add services according to the manufacturer's service profile and the deployment requirements for the Server. The full service profile of applications offered by an advanced server is beyond the scope of this document, but should be available from the operating system manufacturer or by referencing industry standard profiles such as the UNIX 03 Standard[26] Linux Base Standard (LSB)[27] or others. Whatever service profile is specified, the IPv6 Advanced Server is expected to offer an IPv6 equivalent of any IPv4 service that the Server is hosting, as well as any IPv6-only services specified in its service profile.

There are many network application services possible, a partial list of services that MAY be provided by a Server include:

---

[25] This recommendation is under consideration for upgrade to a MUST. Implementations with configurable policy tables are strongly recommended, and where possible, choose to use operating systems that support a configurable policy table.

[26] http://www.opengroup.org/openbrand/register/xy.htm
[27] http://www.opengroup.org/lsb/cert/register.html

- RFC 4330, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI[28]
- RFC 3596, DNS Extensions to Support IPv6
- RFC 3226, DNS Security and IPv6 Aware Server/Resolver Message Size Requirements
- RFC 3261, Session Initiation Protocol (SIP)
- RFC 3315 Section 2.9.3 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Server
- RFC 3315 Section 2.9.4 DHCPv6 Relay Agent
- RFC 3053, IPv6 Tunnel Broker
- RFC 3162, RADIUS (Remote Authentication Dial In User Service) and IPv6
- RFC 2911, Internet Printing Protocol (IPP)
- RFC 2821, Simple Mail Transfer Protocol (SMTP)
- RFC 2428, FTP Extensions for IPv6 and NATs; Server must be capable of transferring files with IPv6 and support Extended Data Port (EPRT) and Extended Passive (EPSV) commands
- Standard 9/RFC 959, File Transfer Protocol (FTP)

3.1.3.2 Simple Server Profile

Requirements for IPv6 Capable Simple Servers are identical to Network Appliance, with the addition that a Simple Server:

- SHOULD meet the Advanced Server Profile if possible (section 3.1.3.1);
- SHOULD provide at least one network service as discussed in Section 3.1.3.1.

3.2 IPv6 Intermediate Nodes

3.2.1 Router Product Profile

IPv6 Capable Routers:

- MUST implement the Base Requirements (Section 2.1)
  - And MUST implement RFC 3810, MLDv2 and RFC 2711, Router Alert Option;
- MUST implement the router requirements defined in RFC 4862 (replaces RFC 2462 as of Version 3.0 of this document) including configuration of link-local addresses;
- SHOULD implement RFC 2894 – Router Renumbering for IPv6
- MUST be IPsec capable, implementing the IPsec Functional Requirements (Section 2.2)
  - And SHOULD+ support RFC 4941 (replaces RFC 3041), Privacy Extensions;

[28] A protocol specification draft for NTPv4 is on track for publication in the NTP working group. See http://tools.ietf.org/html/draft-ietf-ntp-ntpv4-proto-09

  - And Conditionally, IF the Open Shortest Path First (OSPF) routing protocol is used the router MUST support RFC 4302 (AH) to secure OSPF;[29]
- MUST, at a minimum, support transport of both IPv4 and IPv6 traffic via Dual Stack OR manual tunneling Transition Mechanisms (Section 2.3)
- MUST support the QoS Functional Requirements (Section 2.4)
- Conditionally, A Router MUST implement Home Agent capability as defined in Section 2.5.2 IF it will be deployed as a Home Agent Router;
- Conditionally, A Router MUST implement MIPv6 Network Mobility (NEMO) capability as defined in Section 2.5.3 IF it will be deployed as a NEMO Capable Router.
- MUST support the Network Management Functional Requirements (Section 2.7)
- Conditionally, IF the router functions as an Interior Router (network core) it MUST support the Interior Router Requirements (Section 2.8.1)
- Conditionally, IF the router functions as an Exterior Router (BGP gateway) between routing systems, it MUST support the Exterior Router Requirements (Section 2.8.2)
- Conditionally, IF the Router functions as a DHCPv6 Server it MUST implement Section 2.9.3.
- Conditionally, IF the Router functions as a DHCPv6 Relay Agent it MUST implement Section 2.9.4.

A Router product MAY implement one or more Information Assurance functions as defined in section 3.2.3. As such, the router would be an “IA Enabled Product”.

Note on multicast routing protocols: Multicast routing protocols have recently emerged from the IETF Protocol Independent Multicast (PIM) Working Group as Proposed Standards. RFC 4601, Protocol Independent Multicast – Sparse Mode (PIM-SM) and RFC 3973, Protocol Independent Multicast – Dense Mode (PIM-DM) conditionally **SHOULD+** be implemented IF deployment requires multicast routing protocols.

3.2.2 Layer-3 (L3) Switch Product Profile

IPv6 Capable L3 Switches:

- MUST implement the Base Requirements (Section 2.1)
- SHOULD+ be IPsec Capable, implementing the IPsec Functional Requirements (Section 2.2)

[29] This is to be consistent with the DISA FSO Backbone Transport Services (BTS) Security Technical Implementation Guide (STIG) [13] which states the following: "(BTS-RTR-010: CAT II) The router administrator will ensure neighbor authentication with MD5 or *IPv6 AH is implemented for all routing protocols* with all peering routers within the same autonomous system as well as between autonomous systems." Implementing IPsec to secure routing protocols would make a router an “IA Enabled Device” rather than an “IA Device”.

- Conditionally, IF the L3 Switch is used as an Exterior Router it
  - MUST support the Exterior Router Requirements (Section 2.8.2) IF the product will be used as an exterior system node and must support routing functions to interface with routers at edge of a switching network
  - MUST, at a minimum, support transport of both IPv4 and IPv6 traffic via Dual Stack OR manual tunneling Transition Mechanisms (Section 2.3)
- Conditionally, IF the L3 Switch is used as an Interior Router it MUST support the Interior Routing Requirements (Section 2.8.1)
- Conditionally, MUST support the Network Management Functional Requirements (Section 2.7) IF the product is a managed switch
- Conditionally, SHOULD support RFC 4541, Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches IF MLD Snooping is required in the deployment;
- MUST implement the “multicast router” requirements and the “multicast address listener” part of RFC 2710 and conditionally, IF RFC 3810 is supported, MUST implement the “multicast router” requirements and the “multicast address listener” part of RFC 3810.

A L3 Switch product MAY implement one or more Information Assurance functions as defined in section 3.2.3. As such, the router would be an “IA Enabled Product”.

3.2.3 Information Assurance (IA) Device Product Profile

An IPv6 Capable Information Assurance (IA) Device provides one or more Information Assurance functions:

- Intrusion Detection
- Intrusion Protection
- Firewall
- Security Proxy
- In-line Network Encryptor (INE)
- Virtual Private Network (VPN) server
- VPN remote access client software
- Authentication, Authorization and Accounting (AAA) server

This specification only addresses the requirements for an IPv6 Capable IA Device to interoperate in an IPv6 environment; the specific IA function is beyond the scope of these requirements, and beyond the scope of testing based on this specification. Previously established policies and requirements already cover the evaluation and approval of several types of IA devices. The IPv6 Capable evaluation process does not affect or change the requirements defined by the National Information Assurance Partnership (NIAP) or FIPS 140-2 [27] or any other mandated requirements on Information Assurance Devices. Specific guidance on IA can be found in the memorandum Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Information Assurance (IA) Guidance for Milestone Objective 2

(MO2) Version 1.1 [12] and MO3[30] to follow. See also the NSA published "Internet Protocol Version Six Information Assurance Test Plan" [28] that includes additional information.

In addition to its IA functions, An IPv6 Capable IA Device is a "middlebox" and may be viewed as an IPv6 Capable Intermediate Node, forwarding (or blocking) packets depending on the security policy it is implementing. The IA Device will present one or more IPv6 interfaces to the network, and therefore can be evaluated for IPv6 interoperability on those interfaces. The device may behave like an end-node on the network side while appearing to be a router on the LAN side. An IA Device may not participate in all IPv6 support protocols, by the nature of the architectural role it plays. Some IA Devices (for example an Intrusion Detection System) may need to maintain transparency to protocols such as Neighbor Discovery, ICMPv6, IPsec, etc. to perform their mission. Therefore it is not straightforward to specify how such a device can be IPv6 Capable, and it is challenging to verify compliance through testing.

Regardless of how the device is evaluated on its data path, an IA Device may also operate as an IPv6 Capable end-node to be managed via its User Interface or SNMP.

IPv6 Capable IA Devices:

- MUST implement the Base Requirements (Section 2.1)
- Conditionally, MUST be IPsec Capable, implement the IPsec Functional Requirements, IF the device is an IPsec based in-line network encryptor (INE), VPN server, or if it must exchange information with other devices across IPsec secured connections. Some instances of intrusion detection devices, simple firewalls, and other security devices may simply monitor traffic flows and not actually send/receive data across the network and may not require IPsec.
- These devices SHOULD+ support the complete IPsec Functional Requirements but MAY support the following minimal subset of the IPsec requirements:
    - RFC 4301, Security Architecture for the Internet Protocol
    - RFC 4303, IP Encapsulating Security Payload (ESP)
    - Manual Keying
- If a security device must distribute IP Security Policy information to other devices, it SHOULD+ implement:
    - RFC 3585, IPsec Configuration Policy Information Model
    - RFC 3586, IP Security Policy Requirements
    - Note: New Security device standards are emerging for managing IPsec policy information, managing distributed firewalls, etc., which will fit in this category. There is no official DoD IPv6 IPsec policy available at this time.

[30] MO3 draft is currently under internal DoD review, and scheduled for wider review and publication later in 2009.

- Devices MUST also support IPv6 requirements defined for any special security function of the device. Example:
  - Conditionally, Remote Authentication Dial In User Service (RADIUS) authentication servers MUST support RFC 3162, Remote Authentication Dial In User Service (RADIUS) and IPv6, when used to support IPv6 networks.

An IA Device MAY integrate some router or switch functions, and some MAY function as DHCP servers or relays. If an IA Device incorporates a DHCP server function, it MUST follow the relevant sections of RFC 3315. If an IA device incorporates a DHCP relay function, it MUST follow the relevant sections of RFC 3315.

Conditionally, an IA Device MUST process Differentiated Services (RFC 2474 - DiffServ) field where policy forbids their use or requires enforced setting to zeros to prevent exploit as a covert channel.

3.2.3.1 Integrated Security Device (ISD) Additional Requirements

An Integrated Security Device (ISD) is a device that performs stateful packet inspection of both the IPv4 and IPv6 protocols and performs Intrusion Prevention and Intrusion Detection functions (IPS/IDS) within the same device on both IPv4 and IPv6 protocol stacks. An IPv6 Capable ISD MUST support the Information Assurance Device Profile requirements.

3.2.3.2 IPv6 Security Proxy Additional Requirements

An IPv6 Security Proxy is a device or appliance that is designed to terminate a session and initiate a session on the behalf of an IPv6 host. An IPv6 Security Proxy also serves as a network segregator for services and applications. A Security Proxy Appliance has scalable proxy platform architecture to secure Web communications and accelerate delivery of business applications.

- An IPv6 Security Proxy MUST support the Information Assurance Device Profile Requirements.
- An IPv6 Security Proxy is limited to Tunnel Mode IPsec, and MUST NOT provide Transport Mode IPsec.

3.2.3.3 HAIPE Devices

The High Assurance IP Encryption device (HAIPE) is a special case of IA Device. The HAIPE is designed for pair-wise deployment, providing peer-to-peer implementation of encryption using IPsec (in particular, ESPv3 transport mode and IKEv2) to protect classified traffic over an open network. The HAIPE is a “bump-in-the-wire” device; on one side, the plaintext or PT interface connects to host/workstation device or LAN; on

the other side, the cypertext or CT interface connects to an IPv6 backbone network. The HAIPE presents a unique problem to testing:

a. As a cryptographic device, the HAIPE has its own set of specifications and requirements [15] and test plans and must be certified by a designated test facility at the Space and Naval Warfare Systems Command (SPAWAR);
b. As an IPv6 Capable device, the CT side SHOULD+ meet the requirements of this specification for a Host/Workstation, and the PT side SHOULD+ meet the requirements for a Router;
c. Where requirements are inconsistent or in conflict, the HAIPE specifications and test plans take precedence over this specification; the authors are not aware of any conflicts that would interfere with the interoperability of approved HAIPE devices with other IPv6 Capable products that comply with this specification.

3.2.3.4 IPv6 Firewalls

Like HAIPE, firewalls are covered by established policies for test and evaluation. By their nature, firewalls intentionally interfere with standard protocols by blocking the transit of packets that are permitted by the specification but are forbidden by other security requirements. A good example is the IPv6 Routing extension header type 0 (RH0) which allows a sender (or an attacker) to dictate intermediate nodes in the routing of the packet and any response. As with IPv4 source routing, a firewall may be configured to block IPv6 packets with RH0 to prevent the attack scenario. Although RH0 has been deprecated by RFC 5095, there may still be products that generate or respond to RH0 and a firewall configured to block RH0 would ensure that this vector cannot be used.

The National Security Agency (NSA) has a publication “Firewall Design Considerations for IPv6” [29] which explains the role of a firewall in an IPv6 network. This document includes analysis of the IPv6 implications of IPsec, tunneling, higher layer protocols and other topics on firewall design and operation. Current requirements and testing procedures defined under Common Criteria do not address IPv6, but we anticipate that NSA will develop and publish procedures for IPv6 firewalls. NSA public information can be found at http://www.nsa.gov/ as well as the Common Criteria site http://www.niap-ccevs.org/cc-scheme/.

4 IPv6 Capable Software

We anticipate that software products will be presented for evaluation as IPv6 Capable, but the specific requirements for IPv6 Capable software are limited. Further analysis is needed to develop Product Class definitions for software products, but this section is included to document the current state of the discussion on requirements for Software products.

Software products can be divided into Operating System products, Middleware and Application products, with the following definitions:

Operating System (OS): The foundational software on a Host/Workstation or Server that provides an environment for running applications. The OS includes the communications software (drivers) that provide the IPv6 capabilities and an Application Programming Interface (API) that allows IPv6 Capable Applications to use these features.

Middleware: Middleware is software that provides a layer of functionality between the OS and application software, or between the hardware platform and the OS. An example of the former would be a relational database management system (RDBMS) that can be used to build various applications, while an example of the latter would be a virtualization product that enables running multiple instances of one or more operating systems on the same platform.

Application: Software expressing specific functional requirements, particular to its use. The evaluation of an Application software product as IPv6 Capable is based on its use of IPv6 addresses and other IPv6-specific features available through the API.

Application Vendors can be expected to scan and test their code for IPv6 compliance and provide a letter of compliance indicating to what degree they comply. End users of Applications will be looking to DISA to verify that the Application will interoperate with other IPv6 components based on the DISR profiles. Third party or packaged Applications may be considered COTS if they have already been submitted by the vendor, tested and on the IPv6 Capable Registry. Embedded or custom applications as well as unevaluated vendor Applications (i.e. not on the Registry) will be subject to testing.

General purpose Operating Systems can be considered COTS components, if previously submitted by the vendor, tested, and on the APL. This will limit the scope of testing to verifying IPv6 compliance of IPv6-specific requirements upon the application itself in these cases. In cases where the Application under test includes a proprietary or customized Operating System, the test plan may also address the IPv6 functional requirements on the operating system.

An Application or Operating System cannot be tested in isolation; some level of integration testing will be achieved when exercising the two components. Novel combinations of previously approved COTS Applications and Operating Systems may be subjected to Integration Testing, but in general that would be an end-user responsibility.

4.1 Application Programming Interface (API) Characteristics

All applications on Hosts/Workstations, Advanced Servers, Simple Servers or Network Appliances that require IP network protocol service MUST use IPv6 Capable versions of those network protocols. These include the basic and extended specifications of the

Socket API as appropriate to the application architecture[31]. Applications will require evaluation and testing for approval as IPv6 capable as components of a system under test (embedded software) or as a stand-alone product.

Currently, generic requirements are not defined for an IPv6 Capable application beyond the following:

- IEEE Standard 1003.1-2001 [22] based on The Open Group's Networking Services (XNS) specification, issue 6;
- RFC 3542, Advanced Sockets Application Program Interface (API) for IPv6
- RFC 4038, Application Aspects of IPv6 Transition
- On MIPv6 Capable Nodes, for some Mobile applications, RFC 4584, Extension to Sockets API for Mobile IPv6
- RFC 5014, IPv6 Socket API for Source Address Selection is an emerging specification
- RFC 3678, Socket Interface Extensions for Multicast Source Filtering

In addition, specific requirements may be needed for various classes of applications including:

1. File Transfer Protocol (FTP) client
2. Web Browser
3. E-mail client
4. IM client

It is also suggested that applications comply with RFC 3986 Uniform Resource Identifiers: Generic Syntax, for the representation of IPv6 addresses in user interfaces.

4.2 Software Requirements

An IPv6 Capable Application software product will be evaluated on its ability to send and receive IPv6 packets with an IPv6 client, and its use of IPv6 addresses and features available through the API.

IPv6 Capable Operating Systems Conditionally MUST support Dual Stack and MUST support both IPv4 and IPv6 applications in the Application Program Interface (APIs) when deployed with IPv4 legacy peers.

[31] The Socket API extensions are defined in Informational RFCs, as they would not apply to all applications, i.e. those that use other operating system methods for networking.

Appendix A: References

The primary source for requirements cited in this document is the body of Internet Engineering Task Force (IETF) specifications known as "Request For Comment" (RFC) which are referenced throughout the document. These references can be found through http://www.ietf.org/ by using the RFC Search feature on the RFC Editor page. The Requirements Summary Table (Appendix C) can be used as a cross-reference for the RFCs cited as requirements in this document.

The following additional sources were used in generating requirements for this document:

[1] "Internet Protocol Version 6 (IPv6) Interim Transition Guidance" John Stenbit, CIO U.S. Department of Defense; September 23, 2003

[2] "Internet Protocol Version 6 (IPv6)" DoD CIO Memorandum; June 9, 2003

[3] DoD Information Technology Standards Registry (DISR); a repository of cited standards to be followed by DoD projects and deployments. This database can be accessed by authorized users via the web at https://disronline.disa.mil/

[4] "Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Draft IPv6 Capable Functional Specification v1.0" November 22 2005

[5] "Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Information Assurance (IA) Solutions Version 1.0" September 8, 2005

[6] Memorandum for Department of Defense Executive Agent for Information Technology Standards regarding DISR Baseline Release 06-02; June 27, 2006. This Memorandum linked Version 1.0 of the Standard Profiles document to the DISR baseline, and stated that the Standard Profiles document was approved as guidance in the procuring/acquisition of IPv6 Capable Products

[7] NIST Communications Security Establishment document "FAQ for the Cryptographic Module Validation Program" updated December 8, 2006 http://csrc.nist.gov/cryptval/140-1/CMVPFAQ.pdf

[8] Memorandum for Secretaries of the Military Departments, et al "Internet Protocol Version 6 (IPv6) Policy Update" issued by Assistant Secretary of Defense – Networks and Information Integration, August 16, 2005

[9] NIST Special Publication 500-267 "A Profile for IPv6 in the U.S. Government – Version 1.0" Recommendations of the National Institute of Standards and Technology, July 2008 http://www.antd.nist.gov/usgv6/usgv6-v1.pdf

[10] Internet Draft "Deprecation of Type 0 Routing Headers in IPv6" J. Abley et al, May 16, 2007; subsequently published by IETF as RFC 5095 and is an update to RFC 2460.

[11] "The Teredo Protocol: Tunneling Past Network Security and Other Security Implications" Dr. James Hoagland, Symantec Report http://www.symantec.com/avcenter/reference/Teredo_Security.pdf

[12] Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Information Assurance (IA) Guidance for Milestone Objective 2 (MO2) Version 1.1; MO3 draft is currently circulating within DoD for internal review and should be published later in 2009.

[13] DISA FSO Backbone Transport Services (BTS) Security Technical Implementation Guide (STIG) http://iase.disa.mil/stigs/index.html

[14] The Department of Defense Internet Protocol Version 6 Address Plan – version 1.0; Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer; March 2008

[15] High Assurance Internet Protocol Encryptor Interoperability Specification Guide: HAIPE IS version 3.1.2; National Security Agency; 29 February 2008

[16] IEEE 802.11-2007 Standard for Information Technology Part 11 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE 3 Park Ave, NYC NY 12June 2007 http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[17] IEEE 802.11i Standard for Information Technology Part 11 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6 MAC Security Enhancements, IEEE 3 Park Ave, NYC NY 12June 2007 http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[18] Memorandum for Department of Defense Executive Agent for Information Technology Standards regarding DISR Baseline Release 07-03; 6 November 2007. This Memorandum linked Version 2.0 of the Standard Profiles document to the DISR baseline, and stated that the Standard Profiles document was approved as guidance in the procuring/acquisition of IPv6 Capable Products, obsolescing and superseding Version 1.0 of the Standard Profiles.

[19] NIST Special Publication 500-267 "A Profile for IPv6 in the U.S. Government – Version 1.0 Draft 2" draft for public comment, 23 January 2008

[20] Memorandum for the Secretaries of the Military Departments et al, "DoD Internet Protocol Version 6 (IPv6) Definitions", issued by David M. Wennergren, Deputy CIO, 26 June 2008

[21] Memorandum for Department of Defense Executive Agent for Information Technology Standards regarding DISR Baseline Release 08-02; 14 July 2008. This Memorandum linked Version 2.0 of the Standard Profiles document to the DISR baseline, and stated that the Standard Profiles document was approved as guidance in the procuring/acquisition of IPv6 Capable Products, obsolescing and superseding Version 2.0 of the Standard Profiles.

[22] IEEE 1003.1-2001, Issue 6 Standard for Information Technology – Portable Operating System Interface (POSIX) http://www.opengroup.org/onlinepubs/000095399/toc.htm

[23] DISA Network Infrastructure Security Technical Implementation Guide (STIG) http://iase.disa.mil/stigs/index.html

[24] Department of Defense Unified Capabilities Requirements 2008 (UCR2008) published by the Office of the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer (ASD-NII/CIO), 22 January 2008. https://www.us.army.mil/suite/folder/14829537 Note: The UCR is marked For Official Use Only, and requires a DKO account for access. Contact a DoD sponsor for access.

[25] NIST Special Publication 800-57 "Recommendations for Key Management-Part 3: Application-specific Key Management" Draft guidance for the use of cryptographic key management from the National Institute of Standards and Technology, August 2008 http://csrc.nist.gov/publications/drafts/800-57-part3/Draft_SP800-57-Part3_Recommendationforkeymanagement.pdf

Sections 1 and 2 are available at http://csrc.nist.gov/publications/PubsSPs.html#800-57

[26] Federal Information Processing Standards (FIPS) Publication 197 – Advanced Encryption Standard (AES), November 26, 2001 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[27] Federal Information Processing Standards (FIPS) Publication 140 – Security Requirements for Cryptographic Modules, May 25, 2001 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[28] Internet Protocol Version Six Information Assurance Test Plan, National Security Agency, January 2009

[29] Firewall Design Considerations for IPv6; Report #I733-041R-2007 National Security Agency; 03 October 2007 http://www.nsa.gov/ia/_files/ipv6/I733-041R-2007.pdf

Appendix B: Glossary

This glossary is provided for the convenience of the reader, and is intended to include terminology and acronym definitions specific to this document, plus other terms in general use.

Information Assurance Device: An Intermediate Node that performs a security function as its primary purpose by filtering or encrypting network traffic, and which may block traffic when security policy dictates. For example a Firewall, Intrusion Detection System, Authentication Server, Security Gateway, HAIPE or VPN are Information Assurance Devices.

Information Assurance Enabled: An IPv6 Capable Node may incorporate an IA function in addition to its primary role, for example implementing cryptographic algorithms as part of IPsec protocols. This is not the core role of the device so it should not be considered an IA Device but rather is an "IA Enabled" product.

IP: Internet Protocol; the glue that holds the Internet together, that is the network layer protocol for the interconnection of packet-switched networks. The first widely deployed version of IP was IP version 4, defined and implemented over 25 years ago.

IPv6: The Internet Protocol Version 6; a replacement for the widely deployed Internet Protocol Version 4. IPv6 and related protocols are defined by IETF in RFCs which can be found at http://www.ietf.org/. Basic information on IPv6 can be found at http://en.wikipedia.org/wiki/IPv6 or through the North American IPv6 Task Force.

IETF: The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC 3935. More information can be found at http://www.ietf.org/.

RFC: Request for Comment; for historical reasons, publications of the IETF are called Requests for Comment, but everyone just calls them RFCs. When an Internet-Draft is accepted for publication, the RFC Editor assigns a number which permanently identifies the publication. Thus any RFC cited can be found by number through the RFC Editor.

IPv6 Capable: According to the DoD IPv6 Definitions Memorandum [20] "IPv6 Capable" Products – are products (whether developed by commercial vendor or the government) [that] can create or receive, process, and send or forward (as appropriate) IPv6 packets in mixed IPv4/IPv6 environments. IPv6 Capable Products shall be able to interoperate with other IPv6 Capable Products on networks supporting only IPv4, only IPv6, or both IPv4 and IPv6, and shall also:

- Conform to the requirements of the DoD IPv6 Standard Profiles for IPv6 Capable Products document contained in the DISR

- Posses a migration path and/or commitment to upgrade from the developer (company Vice President, or equivalent, letter) as the IPv6 standard evolves

- Ensure product developer IPv6 technical support is available

- Conform to National Security Agency (NSA) and /or Unified Cross Domain Management Office requirements for Information Assurance Products

The term “IPv6 Capable Product” as used in this document, is any product that meets the minimum set of mandated requirements, appropriate to its Product Class, necessary for it to interoperate with other IPv6 products employed in DoD IPv6 networks. Thus an IPv6 Capable Product is one that meets the IPv6 Capable requirements specific to the Product Profile for the Product Class appropriate for the product.

Network Appliance: As used in this document, a class of simple end node devices typically with an embedded operating system and specialized supporting software for limited applications.

Product Class: as used in this document a Product Class is one of a set of definitions used in this document to group products with common characteristics and requirements.

SLAAC: Stateless Address Autoconfiguration; one of the methods of configuring end-node interface addresses for IPv6, relying on Neighbor Discovery Protocol (NDP) and Duplicate Address Detection (DAD) to construct globally unique addresses using network prefixes assigned and advertised by a router.

Appendix C: Requirements Summary Table

The Requirements Summary Table list RFC numbers and notes on their applicability to each Product Class.

RFC Status: Info – Informational; PS – Proposed Standard; DS – Draft Standard; STD – Approved Standard; BCP – Best Current Practice; OBS – Obsolete; HIST – Historic; EXP – Experimental

Applicability: M – MUST; S+ – SHOULD+; S – SHOULD; O – Optional (MAY); C – Conditional (followed by another code, for example C M indicates Conditional MUST); I – Informational; SN – SHOULD NOT; MN – MUST NOT

In-effect Date: Date at which the requirement will be in effect for products; “current” indicates requirements already in effect as of this publication

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
2.1	Base Requirements	2460	Internet Protocol, Version 6 (IPv6) Protocol Specification	DS	M	M	M	M	M	M	Current
		5095	Deprecation of Type 0 Routing Headers in IPv6	PS	M	M	M	M	M	M	Current
		4443	Internet Control Message Protocol (ICMPv6)	DS	M	M	M	M	M	M	Current
		4884 [compatibility only]	Extensions to ICMP to Support Multipart Messages	PS	S	S	S	S	S	S	7/2010
		4861 [replaced 2461]	Neighbor Discovery for IPv6	DS	M	M	M	M	M	M	Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4862 [replaced 2462]	IPv6 Stateless Address Autoconfiguration [only link-local addresses and Duplicate Address Detection]	DS	M	M	M	M	M	M	Current
		1981	Path MTU Discovery for IPv6	DS	M	S	M	M	M	M	Current
	[address architecture]	4291	IPv6 Addressing Architecture	DS	M	M	M	M	M	M	Current
		4007	Scoped Address Architecture	PS	M	M	M	M	M	M	Current
		4193	Unique Local IPv6 Unicast Addresses	PS	O	O	O	O	O	O	Current
		2526	Reserved IPv6 Subnet Anycast Addresses	PS							Current
		3306	Unicast-prefix-based IPv6 Multicast Addresses	PS							Current
		3307	Allocation Guidelines for IPv6 Multicast Addresses	PS							Current
		5156	Special-Use IPv6 Addresses	INFO							Current
		5375	IPv6 Unicast Address Assignment Considerations	INFO							Current
	[Multicast listener	2710	Multicast Listener Discovery for IPv6	PS	M	M	M	M	M	M	Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
	discovery]	3810	MLDv2 for IPv6	PS	M	S+	M	M	S+[32]	S+	Current
		2711	IPv6 Router Alert Option	PS	M	S+	M	M	S+	S+	Current
		3590	Source Address Selection for MLD Protocol	PS	S+	S+	S+	S+	S+	S+	Current
	[connection technology]	2464	IPv6 over Ethernet	PS	C M	C M	C M	C M	C M	C M	Current
		2492	IPv6 over ATM	PS	C M	C M	C M	C M	C M	C M	Current
		5072 [replaced 2472]	IPv6 over PPP	PS	C M	C M	C M	C M	C M	C M	Current
		3572	IPv6 over MAPOS	PS	C M	C M	C M	C M	C M	C M	Current
		2467	IPv6 over FDDI	PS	C M	C M	C M	C M	C M	C M	Current
		2491	IPv6 over NBMA	PS	C M	C M	C M	C M	C M	C M	Current
		2497	IPv6 over ARCnet	PS	C M	C M	C M	C M	C M	C M	Current
		2590	IPv6 over Frame Relay	PS	C M	C M	C M	C M	C M	C M	Current
		3146	IPv6 over IEEE 1394 Networks	PS	C M	C M	C M	C M	C M	C M	Current

[32] Note that an L3 Switch MUST also implement the “multicast router part” and “multicast address listener part” of RFC 3810 IF supporting RFC 3810.

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4338	IPv6, IPv4 and ARP Packets over Fibre Channel	PS	C M	C M	C M	C M	C M	C M	Current
		4944	Transmission of IPv6 Packets Over IEEE 802.15.4 Networks	PS	C M	C M	C M	C M	C M	C M	Current
2.2	IPsec	4301	Security Architecture for the Internet Protocol	PS	M	S+	M	M	S+	C M	Current
		4302	IP Authentication Header	PS	S	S	S	C M	S	C S	Current
		4303	IP Encapsulating Security Payload	PS	M	S+	M	M	S+	C M	Current
		4308 [VPN-B]	Cryptographic Suites for IPsec	PS	M	S+	M	M	S+	C M	07/2010
		4835 [replaced 4305]	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	PS	M	S+	M	M	S+	C M	07/2010
		4869	Suite B Cryptographic Suites for IPsec	Info	M	S+	M	M	S+	C M	07/2010

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		IEEE 802.11-2007i	Standard for Information Technology Part 11 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6 MAC Security Enhancements	PS	C[33] S	C S					Current
	IPsec Fallback[34]	2401	Security Architecture for the Internet Protocol	OBS	C M	C S+	C M	C M	C S+	C M	Current
		2406	IPsec Encapsulating Security Payload (ESP)	OBS	C M	C S+	C M	C M	C S+	C M	Current
		2402	IPsec Authenticating Header (AH)	OBS	C M	C S+	C M	C M	C S+	C M	Current
	[SeND]	3971	Secure Neighbor Discovery	PS	S	S	S	S	S	S	Current
	[CGA]	3972	Cryptographically Generated Addresses	PS	S	S	S	S	S	S	Current
	[SLAAC Privacy Extension]	4941 [replaced 3041]	Privacy Extensions for Stateless Address Auto configuration in IPv6	PS	S+ C M	S	C M	S+	S	S	7/2010
2.2.2	IKEv2	4306	Internet Key Exchange Version 2 (IKEv2) Protocol	PS	M	S+	M	M	S+	C M	7/2010

[33] Applies to end-nodes with wireless LAN interface

[34] IPsec Fallback requirements only apply to a product that MUST support IPsec that does not currently support IPsec RFC 4301 requirements

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4307	Cryptographic Algorithms for Internet Key Exchange Version 2 (IKEv2)	PS	M	S+	M	M	S+	C M	7/2010
	IKEv1[35]	2407	The Internet IP Security Domain of Interpretation for ISAKMP	OBS	C M	C S+	C M	C M	C S+	C M	Current
		2408	Internet Security Association and Key Management Protocol (ISAKMP)	OBS	C M	C S+	C M	C M	C S+	C M	Current
		2409	The Internet Key Exchange (IKE)	OBS	C M	C S+	C M	C M	C S+	C M	Current
		4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	PS	C M	C S+	C M	C M	C S+	C M	Current
		4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	PS	C S	C S	C S	C S	C S	C S	Current

[35] Products with IKEv2 implementation MAY also include a fall-back to IKEv1; products without IKEv2 MUST at least meet the IKEv1 requirements

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
2.3	Transition Mechanisms	4213	Transition Mechanisms for IPv6 Hosts and Routers [Dual Stack]	PS	C M[36]	S	C M[36]	M[36]	C M[36]	S	Current
		4213	Transition Mechanisms for IPv6 Hosts and Routers [manual tunnels]	PS							Current
		4213	Transition Mechanisms for IPv6 Hosts and Routers [Translation and other methods]	PS	O	O	O	O	O	O	Current
		2766	Network Address Translation – Protocol Translation (NAT-PT)	PS (HIST)	SN	SN	SN	SN	SN	SN	Current
		3053	IPv6 Tunnel Broker	INFO	C M	C S	C M	C M	C M		Current
	[provider edge]	4798	Connecting IPv6 islands over IPv4 MPLS using IPv6 Provider Edge (6PE) routers	PS				C S	C S		Current
2.4	QoS	2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	PS	O	O	O	M	O	C M	Current 7/2010
		3168	The Addition of Explicit Congestion Notification (ECN) to IP	PS	O	O	O	S	O		Current

[36] MUST implement Dual Stack OR Tunneling to meet the requirement to carry both IPv4 and IPv6 traffic

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		2205	Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification	PS	O	O	O	S+	O		Current
		2207	RSVP Extensions for IPSEC Data Flows	PS	O	O	O	S+	O		Current
		2210	The Use of RSVP with IETF Integrated Services	PS	O	O	O	S+	O		Current
		2750	RSVP Extensions for Policy Control	PS	O	O	O	S+	O		Current
		3175	Aggregation of RSVP for IPv4 and IPv6 Reservations	PS	O	O	O	O	O		Current
		3181	Signaled Preemption Priority Policy Object	PS	O	O	O	O	O		Current
		2961	RSVP Refresh Overhead Reduction Extension	PS	O	O	O	O	O		Current
		4495	A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow	PS	O	O	O	O	O		Current
		2998	A Framework for Integrated Services Operation over DiffServ Networks	I	O	O	O	O	O		Current
		2996	Format of the RSVP DCLASS Object,	PS	O	O	O	O	O		Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		2746	RSVP Operation Over IP Tunnels	PS	O	O	O	O	O		Current
		3182	Identity Representation for RSVP	PS	O	O	O	O	O		Current
		2872	Application and Sub Application Identity Policy Element for Use with RSVP	PS	O	O	O	O	O		Current
		2747	RSVP Cryptographic Authentication	PS	O	O	O	O	O		Current
2.5.1	MIPv6 Capable	3775 [Mobile Node]	Mobility Support in IPv6	PS	C M	C S					Current
		3776	Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents	PS	C M	C S					Current
		4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture	PS	C M	C S					7/2010
		4282	The Network Access Identifier	PS	C S+	C S					Current
		4283	Mobile Node Identifier for Option for IPv6	PS	C S+	C S					Current
2.5.2	Home Agent Router	3775 [Home Agent]	Mobility Support in IPv6	PS				C M			Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		3776	Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents	PS				C M			Current
		4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture	PS				C M			7/2010
		4282	The Network Access Identifier	PS				C S+			Current
		4283	Mobile Node Identifier for Option for IPv6	PS				C S+			Current
2.5.3	NEMO Capable	3963	Network Mobility (NEMO) Basic Support Protocol	PS				C M			Current
2.5.4	Route Optimization	3775 (sect 9)	Mobility Support in IPv6	PS	C M	C S					Current
							C M				7/2010
2.6.1	RoHC	3095	Robust Header Compression (RoHC)	PS	O	O	O	O	O		Current
		4815	Corrections and Clarifications to RFC 3095	PS	O	O	O	O	O		Current
		4995	RoHC Framework	PS	O	O	O	O	O		Current
		4996	RoHC: A profile for TCP/IP	PS	O	O	O	O	O		Current
		3241	RoHC over PPP	PS	O	O	O	O	O		Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		3843	RoHC: A Compression Profile for IP	PS	O	O	O	O	O		Current
		4362	RoHC: A Link-Layer Assisted Profile for IP/UDP/RTP	PS	O	O	O	O	O		Current
2.6.2	IP Header Compression	2507	IP Header Compression	PS	O	O	O	O	O		Current
		2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links	PS	O	O	O	O	O		Current
		3173	IP Payload Compression	PS	O	O	O	O	O		Current
2.7	Network Management	3411	An Architecture for Describing Simple Protocol Version 3 (SNMPv3)	STD 62			S	M	C M		Current
		3412	Message Processing and Dispatching for the SNMP	STD 62			S	M	C M		Current
		3413	SNMP Applications	STD 62			S	M	C M		Current
			SNMP over IPv6[37]				S	M	C M		7/2011

[37] Nodes managed via SNMPv3 are required to do so using IPv6 transport.

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
	[MIBs]	3595	Textual Conventions for IPv6 Flow Label	PS	C S+			C M	C M		Current
		4022	Management Information Base for the Transmission Control Protocol	PS	C S+			C M	C M		Current
		4113	Management Information Base for the User Datagram Protocol	PS	C S+			C M	C M		Current
		4087	IP Tunnel MIB	PS				C S	C S		Current
		4293	Management Information Base (MIB) for IP	PS				C M	C M		Current
		4295	Mobile IP Management MIB	PS				C M	C M		Current
		4807	IPsec Security Policy Database Configuration	PS				C M	C M		Current
		3298	MIB For the Differentiated Services Architecture	PS				C M	C M		Current
		4292	IP Forwarding Table MIB	PS				C M	C M		Current
	[Multicast]	4601	Protocol Independent Multicast – Sparse Mode (PIM-SM)	PS				C S+			Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		3973	Protocol Independent Multicast – Dense Mode	PS				C S+			Current
2.8.1	Interior Router	2740[38]	OSPF for IPv6 (OSPFv3)	PS				C M	C M		Current
		5340	OSPF for IPv6 (OSPFv3)	PS				C M	C M		7/2010
		4552	Authentication/Confidentiality for OSPFv3	PS				C M	C M		Current
	Interior Router in IPv6/IS-IS deployment	5308	Routing IPv6 with ISIS	PS				C M	C M		7/2010
		5304	IS-IS Cryptographic Authentication	PS				C M	C M		7/2010
		5310	IS-IS Generic Cryptographic Authentication	PS				C M	C M		7/2010
2.8.2	Exterior Router	4271	A Border Gate Protocol (BGP-4)	DS				C M	C M		Current
		1772	Application of the Border Gateway Protocol in the Internet	DS				C M	C M		Current
		2545	Use of BGP-4 Multi-Protocol Extensions for IPv6 Inter-Domain Routing	PS				C M	C M		Current

[38] RFC 2740 was recently obsoleted by RFC 5340. Support for 5340 is preferred but 2740 is acceptable at this time

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4760 [replaced 2858]	Multi-Protocol Extensions for BGP-4	PS				C M	C M		Current
		2784	Generic Router Encapsulation (GRE):	PS				C M			Current
		2890	Key and Sequence Number Extensions to GRE	PS				C M			7/2010
		2473	Generic Packet Tunneling in IPv6	PS				C M			Current
2.9	Automatic Configuration	4862 [replaced 2462]	IPv6 Stateless Address Auto-configuration (SLAAC)	DS	M[39]	M[33]		M[33]			Current
		3315	DHCPv6 [client]	PS							Current
		3315	DHCPv6 [server]	PS		C M	C M	C M		C M	current
		3315	DHCPv6 [Relay Agent]	PS				C M	C M	C M	current

[39] Host and Net Appliance Product Classes MUST support a method of autonomous configuration, either SLAAC or DHCPv6 client; Routers MUST support Router requirements for SLAAC.

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		3769	Requirements for IPv6 Prefix Delegation	Info		I	I	I			current
		3633	IPv6 Prefix Options for DHCPv6	PS		C S	C S	C S			current
		n/a	[disable autoconfiguration]		M	M	M	M	M	M	Current
		5175	Extensions to Router Advertisement Flags	PS	C S+	C S+	C S+	C S+	C S+	C S+	current
		4192	Procedures for Renumbering an IPv6 Network without a Flag Day	INFO	S	S	S	S	S	S	Current
2.10	VPN	4364	BGP/MPLS IP Virtual Private Networks	PS	C M		C M	C M	C M	C M	7/2010
		4577	OSPF as the provider/customer edge protocol for BGP/MPLS IP VPNs	PS	C M		C M	C M	C M	C M	7/2010
		4684	Constrained route distribution for BGP/MPLS IP VPN	PS	C M		C M	C M	C M	C M	7/2010
3.1.3.1	Server [Services]	959	File Transfer Protocol	STD 9		O	O				Current
		2428	FTP Extensions for IPv6 and NAT	PS		O	O				Current
		2821	Simple Mail Transfer Protocol (SMTP)	PS		O	O				Current
		2911	Internet Printing Protocol	PS		O	O				Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		3162	RADIUS (Remote Authentication Dial-In User Service) and IPv6	PS		O	O			C M	Current
		4330	Simple Network Time Protocol (SNTP)	INFO		O	O				Current
		3226	DNS Security and IPv6 A6 Aware Server/Resolver Message Size Requirements	PS		O	O				Current
		3261	Session Initiation Protocol (SIP)	PS		O	O				Current
		3596	DNS Extensions to Support IPv6	DS		O	O				Current
		3053	IPv6 Tunnel Broker	INFO		O	O				Current
3.1.1	Host	3484 [Sec 2.1]	Default Address Selection for IPv6 [Policy Table]	PS	S+	S	S+				Current
		3484 [rest of RFC]	Default Address Selection for IPv6	PS	M	S	M				Current
		3596 [resolver]	DNS Extensions to Support IPv6	DS	M	S	M				Current
3.2.2	L3 Switch	4541	Considerations for IGMP and MLD Snooping Switches	Info					C S		Current
3.2.3	IA Device	3585	IPsec Configuration Policy Information Model	PS						C S+	Current
		3586	IP Security Policy Requirements	PS						C S+	Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
4.1	API	IEEE 1003.1-2001	Open Group Base Standards, Issue 6	INFO							
		3542	Advanced Sockets Application Program Interface for IPv6	INFO							
		4038	Application Aspects of IPv6 Transition	INFO							
		4584	Extension to Sockets API for Mobile IPv6	INFO							
		5014	IPv6 Socket API for Source Address Selection	INFO							
		3986	Uniform Resource Identifiers: Generic Syntax	STD 66							
		3768	Socket Interface Extensions for Multicast Source Filters	INFO							

Appendix D: Summary of Revisions

Changes from Version 3.0 to Version 4.0

This Final v4.0 specification includes revisions based on comments received since the publication of Version 3.0, dated 13 June 2008 and officially promulgated on 14 July 2008. Many of the comments were minor editorial and clarification points which have been addressed in the text; however, a number of substantive additions and revisions have been received and addressed in this version. The following tables highlight substantial changes as an aid to the reader in comparing Version 3.0 and Version 4.0.

Paragraph	Type of Edit	Change from v3.0 to v4.0
1.0	Addition	Reference to original 2003 Stenbit memo in intro
1.1	Update	Definition of IPv6 Capable, etc. consistent with revisions in 26 June 08 Wennergren memo
1.5.3	Clarification	More detail in the Conditional requirement counter-example
1.6	Update	Merge Network Appliance and Simple Server columns in table 1-1
2.0	Addition	Further explanation of relationship with UCR 2008
2.1	Addition	Compatibility with RFC 4884 implementations
2.1	Addition	Explanatory comment on /64 prefix length
2.1	Addition	Footnote regarding a hop-by-hop header vulnerability and citation of an Internet Draft on solutions.
2.1	Addition	Add citation of RFC 2711 along with RFC 3810
2.1	Addition	Addressing Architecture: add informational citation of RFC 2526, 3306, 3307 and 5375
2.1	Editorial	Correct reference to RFC 4862 section 5.5, title changed from RFC 2462 reflecting deprecation of site-local addresses
2.1	Clarification	Added clarifying text stating that RFC 1981 does not impose any new Router requirements beyond RFC 4443
2.1, 2.9	Addition	Cite RFC 4192 – Renumbering without a Flag Day

Paragraph	Type of Edit	Change from v3.0 to v4.0
2.2.1	Correction	IEEE 802.11.-2007 amendment (i) only applies to End Nodes with wireless LAN interface requiring strong authentication. Corresponding change in App C
2.2.1, App C	Update	Relax effective date for RFC 4308, with explanatory notes
2.2.1, References	Addition	Clarify guidance and cite FIPS 140-2, FIPS 197 and NIST SP 800-57
2.2.1, App C	Update	Due to IPR issues relax effective date for RFC 4869 (Suite B); explanatory footnote.
2.2.1	Clarification	Add comment regarding RFC 4869 and compatibility with USGv6 Profiles. Remove extraneous comment from section 1.4.
2.3	Clarification	Add language to the discussion of translation to emphasize its temporary nature.
2.3	Typo	Fix citation of RFC 2185
2.5	Addition	Introductory text about the status of MIPv6 and clarifying the conditional nature of the requirements; at the end of the section, explanatory text on the roles of nodes in MIPv6
2.5.1	Addition	Text on applicability of Mobile Node requirements
2.5.4	Addition	Caveats on Route Optimization
2.7	Clarification	Clarify that RFC 4807 and RFC 3289 are conditional requirements for managing IPsec SPD and DiffServ.
2.7 and App C	Update	Restate SNMPv3 transport over IPv6 as a MUST; effective date 7/2011
2.8.1	Addition	Conditional requirement for IS-IS Interior Routing Protocol
2.8.1	Update	RFC 5340 replaces RFC 2740 (OSPFv3)
2.8.1	Clarification	Footnote recognizing exemption from 4552 in tactical deployments
2.8.2	Addition	GRE Routers SHOULD support RFC 2890

Paragraph	Type of Edit	Change from v3.0 to v4.0
2.9.3 and App C	Correction	RFC 3769 is Informational not a standard, cite only as background
2.10	Addition	Clarifying text on the conditional requirement for VPN
2.11	Addition	New section documenting additional IA and interoperability considerations originating in UCR2008. These are characterized as “recommendations” at this time.
3.1.1, 3.1.31 and App C	Correction	RFC 3986 (Uniform Resource Identifier) is not a testable requirement for Host or Server products and has been deleted from the product class requirements
3.1.3.1 and App C	Update	Added SHOULD for SNMPv3 for Advanced Server
3.1.3.1 and App C	Update	Strengthen Route Optimization for advanced server to MUST – effective date 7/2010; UPDATE – the change was intended to be relaxed to a Conditional MUST, but the circulated draft v3.3 did not include this change
3.2.3 and References	Addition	Cite NSA IPv6 Information Assurance Test Plan as informational reference for IA device requirements
App C	Update	Delay effective date for RFC 4941 (replaces 3041) Privacy Extension for SLAAC. RFC 4941 remains an Emerging RFC.
App C	Correction	Requirements level on RFC 2711 should have matched RFC 3810
App C	Addition	Under MLD, add row for RFC 2711 and RFC 3590
App C	Correction	RFC 3289 was left out of the table
App C	Update	Delete SNMPv3 requirement on Host/Workstation; probably added in error in previous draft
App C	Update	RFCs cited as “effective date 7/2009 now Current: 4760, 4862, 3315, 3769, 3633, 5175, 5095, 4861, 5072, 4944, 4304

Paragraph	Type of Edit	Change from v3.0 to v4.0
App C	Addition	Add rows under Addressing Architecture for RFC 2526, 3306, 3307, 5156 and 5375
App C	Editorial	Table entry incorrect for RFC 3769 and 3633; change to C S (conditional Should) consistent with the text in paragraph 2.9.3
App C	Correction	Effective date for RFC 4552 (new MUST) should have been 1 year from publication; 7/2009 (now current)
Throughout	Update	References updated to current: 26 June 08 Wennergren NIST Profile Change shorthand reference to the USG Profiles for IPv6 to “USGv6” rather than “NIST”
Various	Editorial	Spelling, punctuation and grammar

Changes since Version 2.0

This Final v3.0 specification includes revisions based on comments received since the publication of Version 2.0, dated August 2007 and officially promulgated on 6 November 2007. Many of the comments were minor editorial and clarification points which have been addressed in the text; however, a number of substantive additions and revisions have been received and addressed in this version. The following tables highlight substantial changes as an aid to the reader in comparing Version 2.0 and Version 3.0.

Paragraph	Type of Edit	Change from v2.0 to v3.0
1.5.1	Addition	Based on several comments and requests, Version 3.0 defines a general policy for the timing of mandate for new or revised standards, and specific schedule notes for several requirements throughout the document
1.5.1, App C	Update	Allow 12-24 months (after this publication) for Effective Date window depending on requirement, rather than blanket 18 month as stated in v2.1; corresponding date changes in App C to 7/2009 or 7/2010
1.5.3	Addition	New text suggesting that test results indicate whether a particular product includes conditional requirements
1.6, 3.1	Update	Collapse Network Appliance and Simple Server to a single product class; but continue to use the two names and maintain section 3.1.3.2 for comparability to earlier version.
1.6	Clarification	Clarify that an operating system using a hardware implementation of the IPv6 stack embodies “IPv6 Capable” independent of the hardware platform, same as an OS that included the stack in software.
2.0	Addition	Per request of RTS program, added text explaining that programs may extend or modify requirements for specific circumstances in their own requirements documents.
2.1	Update	RFC 4861 replaces RFC 2461 as a mandatory standard as of Version 3.0 of this document and is preferred; products implementing RFC 2461 will be considered compliant until 31-December-2009

Paragraph	Type of Edit	Change from v2.0 to v3.0
2.1	Update	RFC 4862 replaces RFC 2462 as a mandatory standard as of Version 3.0 of this document and is preferred; products implementing RFC 2462 will be considered compliant until 31-December-2009
2.1	Addition	SHOULD+ RFC 3590 Source Address Selection for Multicast Listener
2.1	Deletion	Address Autoconfiguration is removed from Base Requirements; the requirement for Autoconfiguration no longer applies to all product classes
2.1	Clarification	Reword the statement on Autoconfiguration to clarify that portions of RFC 4862 apply to all nodes, specifically the MUST statements on Duplicate Address Detection and the automatic configuration of link-local addresses. Corresponding change in App C Base Requirements
2.2	Addition	Added clarifying language about the architectural role of nodes in IPsec and the use of other security tools
2.2	Update	RFC 4941 replaces RFC 3041 for Privacy Addressing, and the requirement is strengthened to a Conditional MUST; updated other references to 3041 throughout text and in Appendix C
2.2.1	Update	RFC 4869 strengthened to MUST
2.2.1	Update	Specify minimal requirement for interoperability as Suite-B-GCM-128 and Suite-B-GMAC-128
2.2.1	Update	Effective date for IPsec RFC 4301 architecture is stated as Current due to it being a MUST since version 1 publication
2.2.1	Update	Restore requirement for RFC 4308 removed in error in v2.0; clarify explanation of 4308 and 4869 and inclusion of the suites
2.2.2	Update	Relaxed statement on support for IKEv1 fall-back for interoperability; IKEv2 implementations MAY (but are not required to) implement IKEv1 as well.

Paragraph	Type of Edit	Change from v2.0 to v3.0
2.2.2	Update	Effective date for IKEv2 is July 2010, also implementations must include support for IKEv1 for interoperability; MUST on IKEv1 fall-back for IKEv2 implementations reduced to MAY
2.2.3	Addition	New section describing the fallback requirements for products that do not at this time meet the MUST requirements for IPsec RFC 4301 and IKEv2; at a minimum products Conditionally MUST support IPsec RFC 2401 and IKEv1. Corresponding changes inserted in App C.
2.3	Clarification	Clarify deprecation of Teredo, and reword the requirements
2.3	Correction	Text incorrectly cited RFC 3053 as MAY, should be Conditional MUST consistent with Appendix C
2.4	Addition	Cited several additional optional RFCs for QoS
2.5, 2.5.1, 2.5.2	Update	RFC 4877 updates 3776 for MIPv6 security
2.6.1	Addition	Add citation of RFCs 4815, 4995 and 4996
2.6.1, 2.6.2	Clarification	RoHC and IP Header compression are restated as “optional” to be consistent with Appendix C in v2.0
2.6.2	Addition	Add citation of RFC 3173
2.7	Addition	SNMP SHOULD+ be over IPv6; effective date +24 months
2.8.2	Update	RFC 4760 replaces RFC 2858
2.9	Addition	New section clarifying and elaborating on Autoconfiguration requirements
2.9.1	Addition	RFC 5075 extensions to Router Advertisement flags
2.9.1	Update	RFC 5175 obsoletes RFC 5075
3.1.1	Clarification	Reference to new section 2.9, clarifying applicability of autoconfiguration requirements to Host/Workstation

Paragraph	Type of Edit	Change from v2.0 to v3.0
3.1.3.1	Update	Privacy addressing for Advanced Server made conditional, only applies when the Server is acting as a client AND requires anonymity
3.2.1	Clarification	Specific citation of limited router requirements for SLAAC (RFC 4862)
3.2.1	Addition	Conditional requirements for Router deployed as DHCPv6 Server or Relay Agent
3.2.1	Update	Reduce tunneling requirements to Conditional MUST
3.2.2	Addition	Conditional requirement for L3 Switch deployed with interior router capability
3.2.3	Addition	Introductory paragraphs
3.2.3.3	Addition	Added section on HAIPE
App C	Updates	Added a column for “effective date” for new/revised RFCs; made table changes consistent with updates in the text
App C	Correction	Missing row for RFC 3633 which is tied to RFC 3769 as stated in paragraph 2.9.3
App C	Correction	Replace table reference to RFC 4309 with a reference to IEEE 802.11-2007i consistent with an earlier change in the text
App D	Editorial	Merge change logs of interim versions v2.1 and v2.2 to reflect all changes from v2.0 baseline to v3.0; resort and eliminate redundant or reversed entries
Various	Editorial	Clarification of language, punctuation, etc. as pointed out by reviewers and discovered in final check

Appendix E: IPsec and IKE RFC References

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Header	Function	Algorithm	RFC	RFC 4835	RFC 4308 VPN-B	RFC 4869 Suite-B-GCM-128	RFC 4869 Suite-B-GMAC-128	RFC 4307	DoD IPv6 v1.0	DoD IPv6 v2.0	DoD IPv6 v3.0	NIST IPv6 v1 draft 2
2	ESP	encryption	NULL	2410	MUST				MAY	MUST	MUST	MUST	MUST
3	ESP	encryption	AES-CBC-128	3602	MUST	MUST				MUST	MUST	MUST	MUST
4	ESP	integrity	HMAC-SHA1-96	2404	MUST					MUST	MUST	MUST	MUST
5	AH	integrity	HMAC-SHA1-96	2404	MUST					MUST	MUST	MUST	MUST
6	IKEv2	integrity	HMAC-SHA1-96	2404					MUST	SHOULD+	MUST	MUST	MUST
7	ESP	integrity	AES-XCBC-MAC-96	3566	SHOULD+					SHOULD+	SHOULD+	SHOULD+	SHOULD+
8	AH	integrity	AES-XCBC-MAC-96	3566	SHOULD+					SHOULD+	SHOULD+	SHOULD+	SHOULD+
9	IKEv2	encryption	AES-CBC-128	3602		MUST	MUST	MUST	SHOULD+	SHOULD+	SHOULD+	MUST	MUST
10	IKEv2	pseudo random	AES-XCBC-PRF-128	4434		MUST			SHOULD+	SHOULD+	SHOULD+	SHOULD+	SHOULD+
11	IKEv2	integrity	AES-XCBC-MAC-96	3566		MUST			SHOULD+	SHOULD+	SHOULD+	SHOULD+	SHOULD+
12	IKEv2	diffie-hellman	2048-bit MODP	3526		MUST			SHOULD+	SHOULD+	SHOULD+	SHOULD+	SHOULD+
13	ESP	encryption/integrity	AES-CBC-128 16-octet ICV GCM	4106			MUST	MUST			SHOULD+	MUST	
14	ESP	integrity	NULL	4303	MAY		MUST	MUST		MUST	SHOULD+	MUST	Discouraged
15	IKEv2	pseudo random	HMAC-SHA-256	4868			MUST	MUST			SHOULD+	MUST	SHOULD+
16	IKEv2	integrity	HMAC-SHA-256-128	4868			MUST	MUST			SHOULD+	MUST	SHOULD+
17	IKEv2	diffie-hellman	256-bit random ECP	4753			MUST	MUST			SHOULD+	MUST	
18	IKEv2	authentication	ECDSA-256	4754			MUST	MUST			SHOULD+	MUST	
19	IKEv2	pseudo random	PRF-HMAC-SHA1	2401					MUST	SHOULD+	MUST	MUST	MUST
20	ESP	encryption	3DES-CBC	2451	MUST				MUST	MUST	MUST	MUST	MUST
21	IKEv2	encryption	3DES-CBC	2451					MUST				MUST
22	SEND			3971						SHOULD+	SHOULD	SHOULD	
23	CGA			3972						SHOULD+	SHOULD	SHOULD	
24	SLAAC		privacy extensions	3041						SHOULD	SHOULD	OBS	
25	SLAAC		privacy extensions	4941								SHOULD	
26	IPsec	key mgmt	manual key management	4301						MUST	MUST	MUST	
27	IKEv2	key mgmt	IPsec Certificate Management Profile	4809									SHOULD+
28	IKEv2	key mgmt	IPsec PKI Profile	4945									SHOULD+
29	ESP	encryption	AES-CTR-128	3686	SHOULD				SHOULD				SHOULD
30	ESP	integrity	HMAC-SHA-256-128	4868									SHOULD+
31	AH	integrity	HMAC-SHA-256-128	4868									SHOULD+