AUSPEX TECHNOLOGIES

DISCOVER THE TRUE VALUE OF TECHNOLOGY

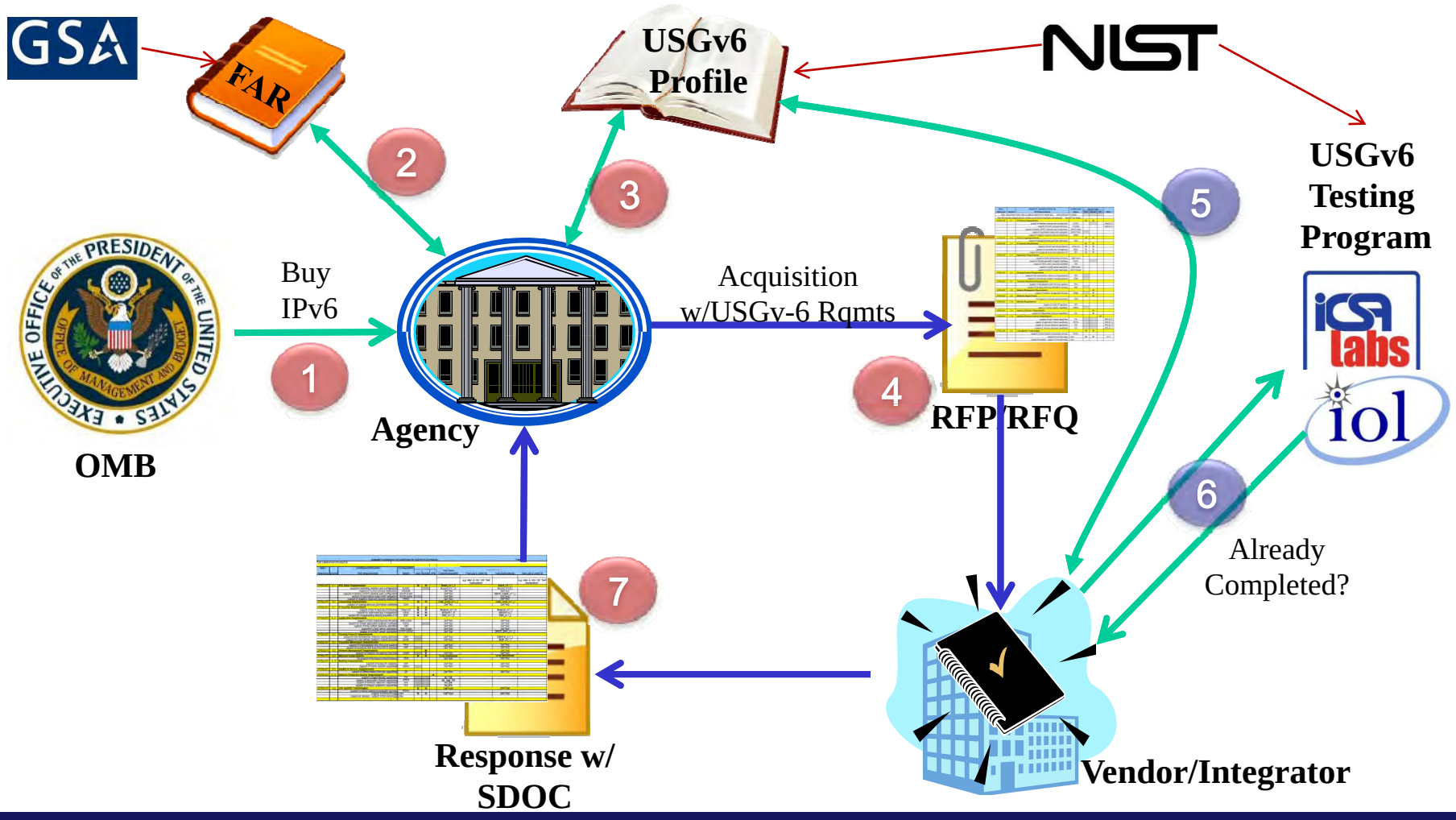
Understanding the USGv6 Profile

NIST Special Publication 500-267 A Profile for IPv6 in the U.S. Government – Version 1.0

02/02/2011

Dale Geesey
Chief Operating Officer
Auspex Technologies, LLC
Phone: 703.319.1925
Fax: 866.873.1277
E-mail: dgeesey@auspextech.com
Web: www.auspextech.com

USGv6 – A Concept in Agency IPv6 Acquisitions



DISCOVER THE TRUE VALUE OF TECHNOLOGY

IPv6 Addition to the FAR

- 11.002(g)

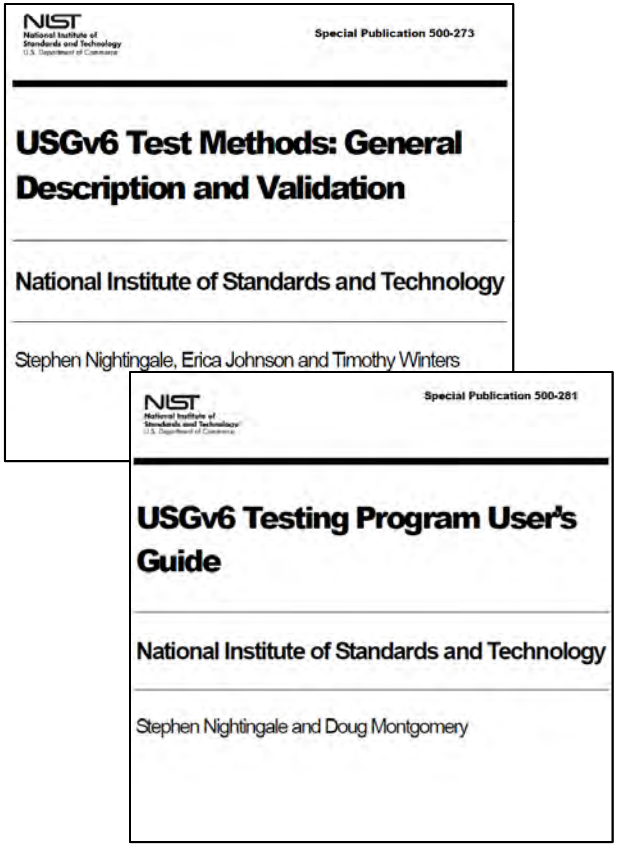
Unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet Protocol, the requirements documents must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. The applicability of IPv6 to agency networks, infrastructure, and applications specific to individual acquisitions will be in accordance with the agency's Enterprise Architecture (see OMB Memorandum M-05-22 dated August 2, 2005).

NIST SP 500-267 A Profile for IPv6 in the U.S. Government – Version 1.0

- Acquisition Focused (not deployment, operational, etc.)
- Purpose
  - *Define a simple taxonomy of common network devices;*
  - *Define their minimal mandatory IPv6 capabilities and identify significant configuration options so as to assist agencies in the development of more specific acquisition and deployment plans; and,*
  - *Provide the technical basis upon which future USG polices can be defined.*
- Why
  - OMB Directed (05-22)
  - USG-wide benefit from a common definition of IPv6 capabilities
  - Promote confidence and protect IPv6 investments
  - "Raise the bar" of IPv6 security and network protection technologies
  - Existing profiling and testing efforts are insufficient for USG requirements
  - Support IPv6 progression to meeting future USG IPv6 requirements and protect investments

Federal IPv6 Product Testing Program

- Tied to Federal IPv6 Product Profile
- Utilizes Suppliers Declaration of Conformity process
- Leveraged by changes to FAR
- Types of Testing
  - Conformance
  - Interoperability
  - Network Protection Device
- 1st/2nd/3rd Party Testing



DISCOVER THE TRUE VALUE OF TECHNOLOGY

USGv6 Acquisition Process in a Nutshell

- Provides the ability for an agency to specify what they mean when they say “I want to buy an IPv6 capable/enabled/etc product”
- Pulls from IETF RFCs (and other sources)
- Provides agency with tested products (to some degree)
  - Conformance
  - Interoperability
  - Security

DISCOVER THE TRUE VALUE OF TECHNOLOGY

Tools - Agency Sends out an IPv6 Profile (Part of RFP/RFQ)

Spec / Reference	Section	USGv6-V1 Node Requirements Title / Definition	Status	Year	Condition / Context	Host	Router	NPD	Effective Date
		IPv6 Basic Requirements							
RFC2460		**IPv6 Specification**	DS	1998		M	M		2010/07
	2	IPv6 Packets: send, receive				M	M		2010/07
	2	IPv6 packet forwarding					M		2010/07
	4	Extension headers: processing				M	M		2010/07
	4.3	Hop-by-Hop & unrecognized options				M	M		2010/07
	4.5	Fragment headers: send, receive, process				M	M		2010/07
	4.6	Destination Options extensions				M	M		2010/07
RFC5095		**Deprecation of Type 0 Routing Headers**	PS	2007		M	M		2010/07
RFC2711		**IPv6 Router Alert Option**	PS	1999			M		2010/07
RFC4443		**ICMPv6**	DS	2006		M	M		2010/07
RFC4884		**Extended ICMP for Multi-Part Messages**	PS	2007		S+	S+		
RFC1981		**Path MTU Discovery for IPv6**	DS	1996		M	M		2010/07
	4	Discovery Protocol Requirements				M	S+		2010/07
RFC2675		**IPv6 Jumbograms**	PS	1999		O	O		
RFC4861		**Neighbor Discovery for IPv6**	DS	2006		M	M		2010/07
	4.1, 4.2	Router Discovery				M	M		2010/07
	4.6.2	Prefix Discovery				M	M		2010/07
	7.2	Address Resolution				M	M		2010/07
	7.2.5	NA and NS processing				M	M		2010/07
(RFC4862)	7.2.3	Duplicate Address Detection				M	M		2010/07
	7.3	Neighbor Unreachability Detection				M	M		2010/07
	8	Redirect functionality				S	M		2010/07
RFC5175		**IPv6 Router Advertisement Flags Option**	PS	2008		S	S		
RFC4191		**Default Router Preference**	PS	2005		S+	S+		
RFC3971		**Secure Neighbor Discovery**	PS	2005	SEND	c(M)	c(M)		2010/07

Tools - Agency Gets an SDOC

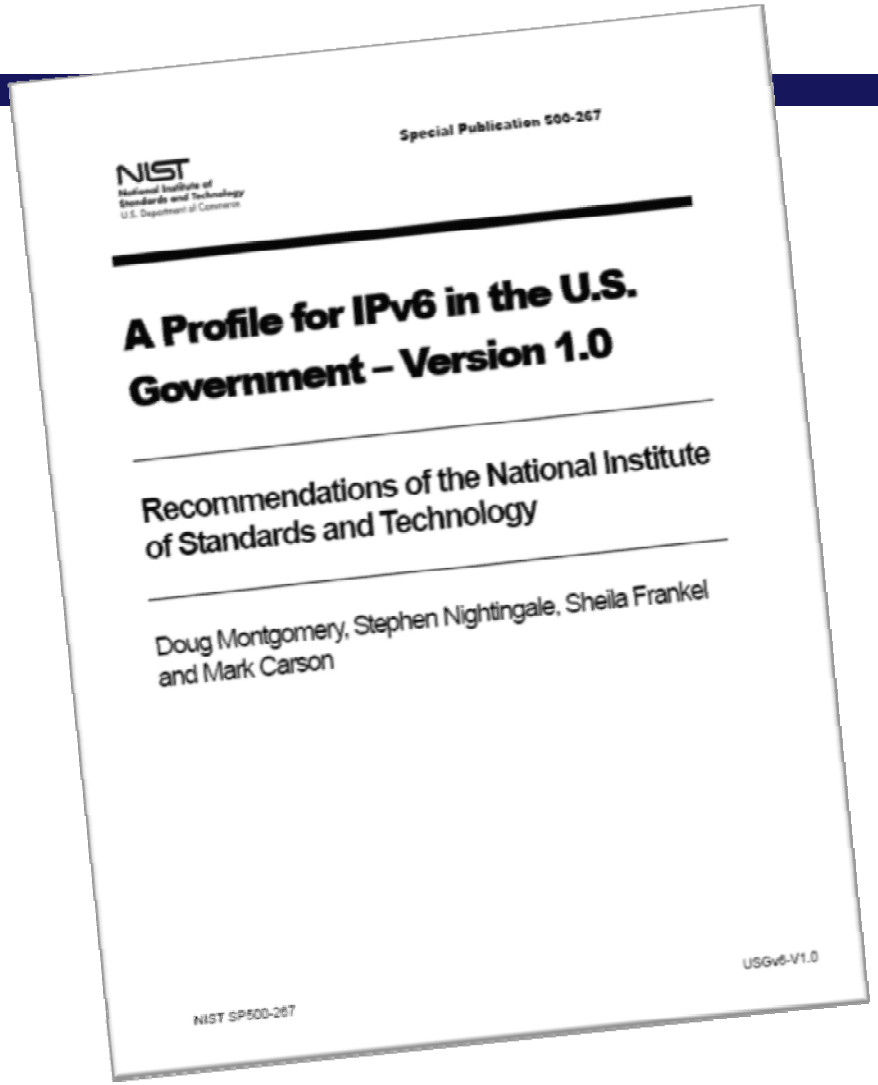
DISCOVER THE TRUE VALUE OF TECHNOLOGY

Supplier's Declaration of Conformity for USGv6-v1.0 Products										Page 3
Product Id										
Spec / Reference	Section	Additional Information IPv6 Requirements	Configuration Option	Host	Router	NPD	Test Suite Conformance/NPD	Test Lab & Result ID	Test Suite Interop	Test Lab & Result ID
								e.g <lab> & <ID> OR "Self Declaration"		e.g <lab> & <ID> OR "Self Declaration"
SP500-267	6.1	**IPv6 Basic Requirements**		M	M		Basic_v1.*_C		Basic_V1.*_I	
		support of stateless address auto-configuration	SLAAC				SLAAC-V1.*_C		SLAAC-V1.0_I	
		support of SLAAC privacy extensions	PRIVADDR				*Self Test*		*Self Test*	
		support of stateful (DHCP) address auto-configuration	DHCP-Client				*Self Test*		DHCP_Client_v1.*_I	
		support of automated router prefix delegation	DHCP-Prefix				*Self Test*		*Self Test*	
		support of neighbor discovery security extensions	SEND				*Self Test*		*Self Test*	
SP500-267	6.6	**Addressing Requirements**		M	M		Addr_Arch_v1.*_C		Addr_Arch_v1.*_I	
		support of cryptographically generated addresses	CGA				*Self Test*		*Self Test*	
SP500-267	6.7	**IP Security Requirements**		M	M					
		support of the IP security architecture	IPsec-V3	M	M		IPsecv3_v1.*_C		IPsecv3_v1.*_I	
		support for automated key management	IKEv2	M	M		IKEv2v1.*_C		IKEv2v1.0_I	
		support for encapsulating security payloads in IP	ESP	M	M		ESP_v1.*_C		ESP_v1.*_I	
SP500-267	6.11	**Application Requirements**								
		support of DNS client/resolver functions	DNS-Client				*Self Test*		*Self Test*	
		support of Socket application program interfaces	SOCK				*Self Test*		*Self Test*	
		support of IPv6 uniform resource identifiers	URI				*Self Test*		*Self Test*	
		support of a DNS server application	DNS-Server				*Self Test*		*Self Test*	
		support of a DHCP server application	DHCP-Server				*Self Test*		DHCP_Serv_v1.*_I	
SP500-267	6.2	**Routing Protocol Requirements**								
		support of the intra-domain (interior) routing protocols	IGW				*Self Test*		OSPFv3_v1.*_I	
		support for inter-domain (exterior) routing protocols	EGW				*Self Test*		BGP_v1.*_I	
SP500-267	6.4	**Transition Mechanism Requirements**								
		support of interoperation with IPv4-only systems	IPv4				*Self Test*		*Self Test*	
		support of tunneling IPv6 over IPv4 MPLS services	6PE				*Self Test*		*Self Test*	
SP500-267	6.8	**Network Management Requirements**			M				Self Test	
		support of network management services	SNMP		M		*Self Test*		*Self Test*	
SP500-267	6.9	**Multicast Requirements**		M	M					
		full support of multicast communications	SSM				*Self Test*		*Self Test*	
SP500-267	6.10	**Mobility Requirements**								
		support of mobile IP capability	MIP				*Self Test*		*Self Test*	
		support of mobile network capabilities	NEMO				*Self Test*		*Self Test*	
SP500-267	6.3	**Quality of Service Requirements**								
		support of Differentiated Services capabilities	DS				*Self Test*		*Self Test*	
SP500-267	6.12	**Network Protection Device Requirements**				M				
		support of basic firewall capabilities	FW				N1_FW			
		support of application firewall capabilities	APFW				N2_App_FW			
		support of intrusion detection capabilities	IDS				N3_IDS			
		support of intrusion protection capabilities	IPS				N4_IPS			
SP500-267	6.5	**Link Specific Technologies**		M	M		Self Test		Self Test	
		support of robust packet compression services	ROHC							
		support of link technology	Link=	M	M		Self Test		Self Test	
		(repeat as needed) support of link technology	Link=							

AUSPEX TECHNOLOGIES

DISCOVER THE TRUE VALUE OF TECHNOLOGY

USGV6 – BUILDING PROFILES



AUSPEX TECHNOLOGIES

DISCOVER THE TRUE VALUE OF TECHNOLOGY

Device Types

Host

- Any Node that is not a Router. A Host's primary purpose is to support application protocols that are the source and/or destination of IP layer communication.

Router

- A Node that interconnects sub-networks by packet forwarding. A Router's primary purpose is to support the control protocols necessary to enable interconnection of distinct IP sub-networks by IP layer packet forwarding.

Network Protection Device

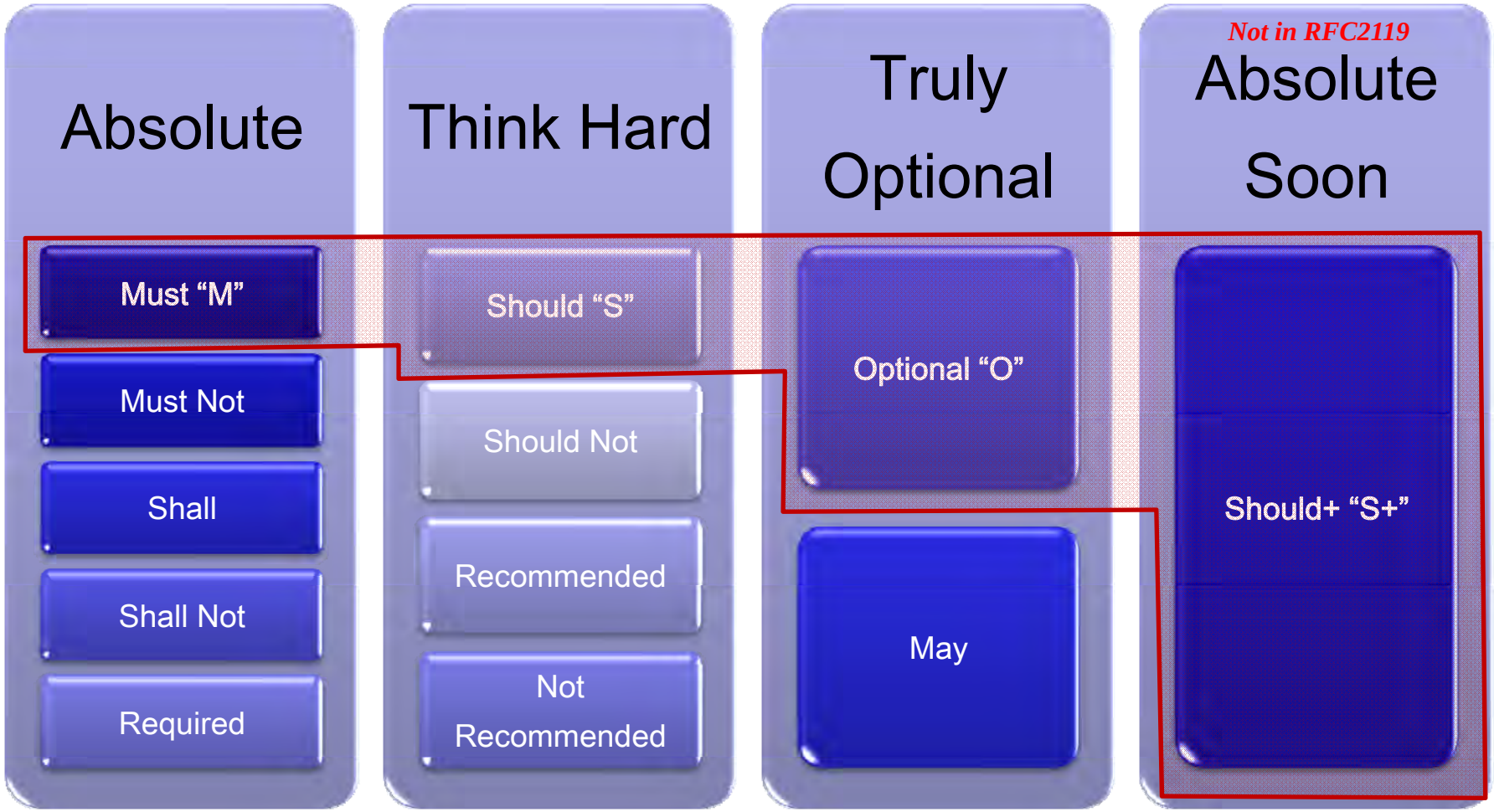
- Firewalls or Intrusion Detection / Prevention devices that examine and selectively block or modify network traffic.

Functional Categories

IPv6 Basic Capabilities	Routing Protocols	Quality of Service	Transition Mechanisms
Link Specific Capabilities	Addressing	IP Security	Network Management
Multicast	Mobility	Application Requirements	Network Protection Device Requirements

DISCOVER THE TRUE VALUE OF TECHNOLOGY

Profile Utilizes IETF RCF2119 Terminology



USGv6 Profile Specific Terminology

- Specific Line Items
  - "**M**" = Mandatory "**O**" = Optional "**S**" = Should "**S+**" = Should+ (mandatory in future)
  - **c(X,Y)** = Configuration Option, if selected then the requirement is "X", otherwise "Y"
    - Example "c(M,S)" if true then it is "M", otherwise it is "S"
  - **c(X)** = Shorthand notation for above, "Y" in this case is considered "O" Optional.

  Requirements Table

  - "**O:n**" = Optional, but must choose "n" options from the set
    - Example "O:1" choose 1 option, "O:3" choose 3 options
  - "**Y/N**" = Optional and a simple yes or no selection
  - Entire Functional Categories
    - "M" (mandatory): Contains unconditional MUSTs and may have Options
    - "O" (optional): Does not contain unconditional MUSTs

  Template
- "USGv6-V1-Capable" = set of requirements that are unconditionally mandatory
- "USGv6-V1-Compliant" = "USGv6-V1-Capable" + requirements that are mandatory under each of the selected configuration options

DISCOVER THE TRUE VALUE OF TECHNOLOGY

Reading the Node Requirements Table

Spec / Reference	Section	USGv6-V1 Node Requirements Title / Definition	Status	Year	Condition / Context	Host	Router	NPD	Effective Date
		IPv6 Basic Requirements							
RFC2460		**IPv6 Specification**	DS	1998		M	M		2010/07
		IPv6 Packets: send, receive				M	M		2010/07
		IPv6 packet forwarding					M		2010/07
		Extension headers: processing				M	M		2010/07
		Hop-by-Hop & unrecognized options				M	M		2010/07
		gment headers: send, receive, process				M	M		2010/07
		Destination Options extensions				M	M		2010/07
RFC5095		precation of Type 0 Routing Headers				M	M		2010/07
RFC2711		**IPv6 Router Alert Option**					M		2010/07
RFC4443		**ICMPv6**				M	M		2010/07
RFC4884		**Extended ICMP for Multi-Part Messages**	PS	2007		S+	S+		
RFC1981		**Path MTU Discovery for IPv6**	DS	1996		M	M		2010/07
	4	Discovery Protocol Requirements				M	S+		2010/07
RFC2675		**IPv6 Jumbograms**	PS	1999		O	O		
RFC4861		**Neighbor Discovery for IPv6**	DS	2006		M	M		2010/07
	4.1, 4.2	Router Discovery				M	M		2010/07
	4.6.2	Prefix Discovery				M	M		2010/07
	7.2	Address Resolution				M	M		2010/07
	7.2.5	NA and NS processing				M	M		2010/07
(RFC4862)	7.2.3	Duplicate Address Detection				M	M		2010/07
	7.3	Neighbor Unreachability Detection				M	M		2010/07
	8	Redirect functionality				S	M		2010/07
RFC5175		**IPv6 Router Advertisement Flags Option**	PS	2008		S	S		
RFC4191		**Default Router Preference**	PS	2005		S+	S+		
RFC3971		**Secure Neighbor Discovery**	PS	2005	SEND	c(M)	c(M)		2010/07

Specific Profile Item

Device Type

Functional Category

RFC Reference

Requirement Level

Creating a Product Specific Profile

- Agency Specific Product Profile
  - Decide the device type
  - Start with unconditional “M” mandatory set (USGv6-V1-Capable)
  - Add sets of requirements that are “C” conditional (USGv6-V1-Compliant)
  - Add “S” should and “S+” requirements for inclusion (Close)
  - Add “O” optional (USGv6-V1-Agency-Product-Compliant)
  - ** Modify any “M”s*
  - ** Add others*
- How many choices are there?

	M	S	S+	C	O	Choices
Host	54	10	15	69	18	112
Router	67	12	22	58	18	92
NPD	9	0	0	14	0	14

Is There An Easier Way?

- Yes - use the templates provided in the Profile
  - Host (20 Choices)
  - Router (22 Choices)
  - NPD (4 Choices)
- Common selections
- Shorthand Notation Available, examples:
  - USGv6-V1-Capable+DHCP-client+Sock+DNS-Client+Link=Ethernet
  - USGv6-V1-Capable+SLAAC+Sock+DNS-Client+MIP+Link=PPP+Link=Ethernet
- Is this the best approach?
  - Maybe/Maybe Not
  - Do you need more options?

USGv6-V1 Host Requirements Template:

- [M] – IPv6 Basic Requirements – see section 6.1.
  - [O:1] – SLAAC – require support of stateless address auto-configuration.
  - [O:1] – DHCP-Client – require support of stateful (DHCP) address auto-configuration.
  - [Y/N] – PrivAddr – require support of SLAAC privacy extensions.
  - [Y/N] – SEND – require support of neighbor discovery security extensions.
- [M] – Addressing Requirements – see section 6.6.
  - [Y/N] – CGA – require support of cryptographically generated addresses.
- [O] – Application Requirements – see section 6.11.
  - [Y/N] – DNS-Client – require support of DNS client/resolver functions.
  - [Y/N] – SOCK – require support of Socket application program interfaces.
  - [Y/N] – URI – require support of IPv6 uniform resource identifiers.
  - [Y/N] – DNS-Server – require support of a DNS server application.
  - [Y/N] – DHCP-Server – require support of a DHCP server application.
- [M] – IP Security Requirements – see section 6.7.
  - [M] – IPsec-V3 – require support of the IP security architecture.
  - [M] – IKEv2 – require support for automated key management.
  - [M] – ESP – require support for encapsulating security payloads in IP.
- [O] – Transition Mechanism Requirements – see section 6.4.
  - [Y/N] – IPv4 – require support to enable interoperation with IPv4-only systems.
- [O] – Network Management Requirements – see section 6.8.
  - [Y/N] – SNMP – require support of network management services.
- [M] – Multicast Requirements – see section 6.9.
  - [Y/N] – SSM – require full support of multicast communications.
- [O] – Mobility Requirements – see section 6.10.
  - [Y/N] – MIP – require support of capability for this host to be a mobile node.
- [O] – Quality of Service Requirements – see section 6.3.
  - [Y/N] – DS – require support of Differentiated Services capabilities.
- [M] – Link Specific Technologies – see section 6.5.
  - [O:1] – Link – require support of 1 or more link technologies.
  - [Y/N] – ROHC – require support of robust packet compression services.

DISCOVER THE TRUE VALUE OF TECHNOLOGY

How to Select Which S, S+, C and O's to Include

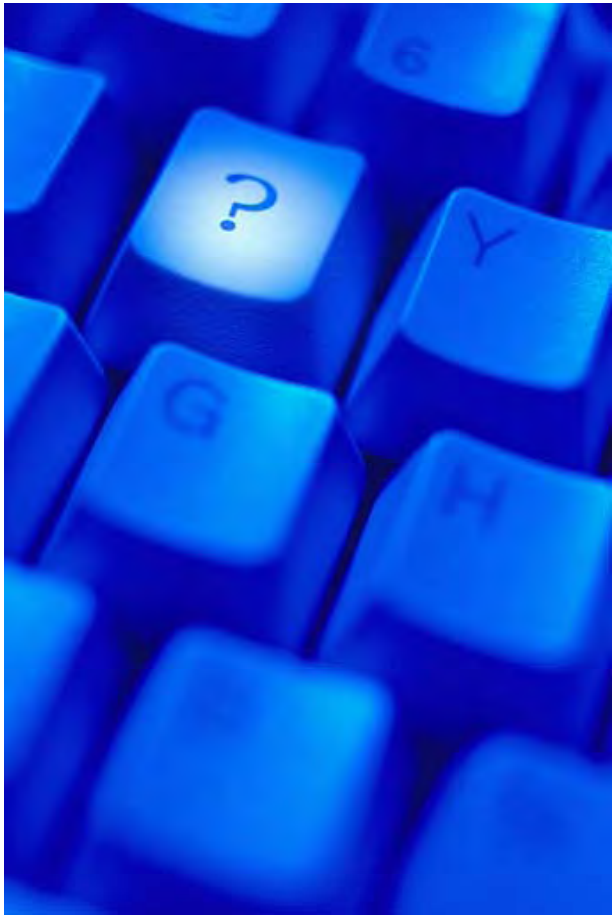
- This is the big question
  - Not really a one size fits all
  - Some profiles will be common across agencies
  - Many will not and may vary based on how much IPv6 you plan to use
- Sources to help select
  - Mission/Agency Requirements
  - Policies
  - Future Planning
  - Testing
  - Engineer Support (Internal/External)
  - NIST
  - Vendors
  - IETF
- Considerations
  - Will it do what I want it to do?
  - Will it do what I do not want it to do?
  - How much will it cost?
  - Security

USGv6 Profile Interesting Notes

- Expected that agencies will augment and/or modify specifications
  - Meet their own requirements
  - Configuration options
  - Agencies may modify profile conformance requirements
    - Must ensure interoperability with conforming systems
    - No easy way to do this
- Scope of devices and mandatory capabilities
  - Partially Conservative: Lowest common denominator of capabilities common to the USG as a whole
  - Partially Aggressive: Areas for current and future security
  - Options: To make up the difference
- Only addresses IPv6 requirements
  - Cannot stand in isolation
  - IPv4 capabilities, Hardware, Performance, Reliability, Support, etc.

Questions

Dale Geesey
Chief Operating Officer
Auspex Technologies, LLC
Phone: 703.319.1925
Fax: 866.873.1277
E-Mail:
dgeesey@auspextech.com
Web: www.auspextech.com
(IPv6 Enabled)



DISCOVER THE TRUE VALUE OF TECHNOLOGY