

Cisco IPv6 Certification Testing

Background: IPv6 Mandate from the U.S. Department of Defense and Office of Management and Budget

As U.S. Government agencies continue their migration to incorporate IPv6 into their Enterprise Architecture it is critical that there is a baseline set of standards that are mandated to promote interoperable architectures. The US Government issued a mandate that states that government networks must be IPv6-capable and any future procurements must consist of “IPv6 Capable” networking equipment. In response to this mandate, the government has worked closely with industry vendors to ensure that any equipment purchased will meet the IPv6-capable requirement.

These requirements are defined by a set of documents produced by both the U.S. Department of Defense for DoD networks and the National Institute of Standards and Technologies (NIST) for government civilian networks. Additionally, the DoD has defined the process by which a network device can achieve IPv6 certification. NIST is currently finalizing their own parallel IPv6 certification process..

Cisco has actively participated in the DoD IPv6 certification process, and has become one of the leading vendors on the certification Approved Product List. Cisco has successfully certified edge, aggregation, and core routers, the first IPv6 certified Firewall (Cisco IOS[®] Firewall), and is currently the only vendor with certified Layer 3 switches.

For more information on the IPv6 Government mandate, please see:

<http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf>

Defining Products as IPv6-Capable

Successful completion of IPv6 certification testing requires that the IPv6 capability criteria be clearly defined. In the case of IPv6, the IPv6 mandate identifies that government networks must be IPv6-capable. Both DoD and NIST have taken steps to clearly define what IPv6-capable means.

The DoD has published several iterations of the “DoD IPv6 Standard Profiles For IPv6 Capable Products”. IPv6 Capable as defined by this document is:

“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.”

This document, commonly referred to as the IPv6 Product Profiles, attempts to categorize network devices into subsets based on functionality or place in the network, as well as, the requirements that each profile must meet to ensure IPv6 capability. The requirements are generated using IETF RFC descriptions to ensure a standards-based approach.

Collectively, the DoD IPv6 Product Profiles provide the baseline definition of IPv6-capable for network equipment vendors. For more information on the DoD IPv6 Product Profiles, see:

http://jitc.fhu.disa.mil/apl/ipv6/pdf/distr_ipv6_product_profile_v2.pdf

NIST has also published a separate document titled “A Profile for IPv6 in the U.S. Government” that provides its own definition of network equipment profiles, as well as the specific RFC requirements that must be met by within each profile.

The NIST document provides a definition of IPv6-capable with respect to civilian networks. For more information on the NIST profiles, see: <http://www.antd.nist.gov/usgv6/usgv6-v1-draft2.pdf>

DoD–JITC and NIST IPv6 Certifications

JITC Certification Process

1. A vendor must first provide a “Letter of Compliance” verifying that the product meets appropriate IETF RFC conformance (see IPv6 Product Profile).
2. To schedule the product for testing, find the appropriate Point of Contact (POCs) at: <http://jitc.fhu.disa.mil/apl/ipv6.html>
3. Once the test is scheduled, the vendor must ship at least two devices (must be identical in OS and hardware) to the Joint Interoperability Test Command (JITC) POCs
4. The vendor must provide at least one engineer to be onsite for the testing
5. The vendor must provide funding and equipment to JITC POCs at least two weeks ahead of the scheduled test
6. JITC will test the device in the prescribed time
7. One to two weeks after successful completion of the testing, the device will be added to the online Approved Products List (APL) pending finalized report
8. One to two months after the test, JITC will provide the vendor with the test report, and IPv6 Capable Certification letter
9. If all IPv6 Capable requirements are met, the device will be added to the DoD IPv6 APL

NIST Certification Process

NIST is currently developing a parallel process to the JITC which is similar to test for compliance with IPv6 requirements. The current proposal is still in draft status and is available at:

<http://www.antd.nist.gov/usgv6/usgv6-v1-draft2.pdf>

Global IPv6 Certifications (IPv6 Ready)

Most commercial, enterprise customers and other countries use the IPv6 Ready Logo to help determine if network equipment meets minimum standards for IPv6. The IPv6 Ready Logo has three distinct phases and is defined as follows:

- Phase 1:
In a first stage, the Logo indicates that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations.
- Phase 2:
The "IPv6 ready" step implies a proper care, technical consensus, and clear technical references. The IPv6 Ready Logo indicates that a product has successfully satisfied stringent requirements stated by the IPv6 Logo Committee (v6LC).
To avoid confusion, the logo "IPv6 Ready" will be generic. The v6LC will define the test profiles with associated requirements for specific functionalities.
- Phase 3:

Same as Phase 2 with IPsec mandated.

Cisco has participated in the IPv6 Ready Logo, and certified many products and subsequent product releases through this process. With the introduction of the more stringent US Government IPv6 Certification process, Cisco has focused efforts on certifying its products against the approved product profiles and has even seen other governments take a reciprocal stand – meaning products that have successfully completed the DoD IPv6 Certification process, they would only require testing for those features that may be unique to their government.

More information on the IPv6 Ready Logo is available at: <http://www.ipv6ready.org/frames.html>

Value of IPv6 Certifications

Global government and Public Sector agencies rely on standardization and certifications to ensure people, processes, and missions are uniformly focused in on their goals. This level of assurance is equally paramount in the deployed communication systems throughout and between agencies. To deliver products that comply with rigorous security and assurance standards, networking and communications equipment vendors must rely on government certification guidelines and processes.

IPv6 certifications provide government agencies a level of assurance that equipment purchases will be protected when a government agency needs to enable IPv6 on its network. Regardless of whether an agency plans to deploy IPv6 immediately or after June 30, 2008 mandate, the agency can rest assured that purchasing IPv6 capable equipment that has successfully passed the IPv6 certification process, will meet the IPv6 capabilities required by the certifying authority.

IPv6 certifications are part of a larger overall certification strategy that Cisco has participated in for many years and is one of the leading vendors in this process. An example of key certifications that Cisco has achieved across a wide range of product families and platforms are NIAP Common Criteria and NIST FIPS. For a broader discussion of certifications that Cisco participates in, see <http://www.cisco.com/go/securitycert>.

Table 1. Cisco DoD IPv6 Certification Status

Products	Places in the Network								
	Campus			Branch				WAN	
	Access	Distribution	Core	Edge	Distribution	Access	Firewall	Aggregation Edge	Core
Cisco® Integrated Services Routers (IOS 12.4T)									
Cisco 2821 ISR				X					
Cisco 2851 ISR				X					
Cisco 3825 ISR				X					
Cisco 3845 ISR				X					
Cisco 7200 Series Router (IOS 12.4T)									
Cisco 7201				X				X	
Cisco 7204 VXR				X				X	
Cisco 7206 VXR				X				X	
Cisco 7600 Series Routers (IOS 12.2SR)									
Cisco 7603-S		X	X					X	X
Cisco 7604		X	X					X	X
Cisco 7606		X	X					X	X
Cisco 7606-S		X	X					X	X

Cisco 7609		X	X					X	X
Cisco 7609-S		X	X					X	X
Cisco 7613		X	X					X	X
Cisco Catalyst® 3560E Series Switches* (IOS 12.2SE)									
Catalyst 3560E-24TD	X						X		
Catalyst 3560E-48TD	X						X		
Catalyst 3560E-24PD	X						X		
Catalyst 3560E-48PD	X						X		
Catalyst 3560E-48D (full power)	X						X		
Cisco Catalyst 3750E Series Switches* (IOS 12.2SE)									
Catalyst 3750E-24TD	X				X	X			
Catalyst 3750E-48TD	X				X	X			
Catalyst 3750E-24PD	X				X	X			
Catalyst 3750E-48PD	X				X	X			
Catalyst 3750E-48D (full power)	X				X	X			
Cisco Catalyst 4500 Series Switches (IOS 12.2SG)									
Catalyst 4503 with Supervisor Engine 6-E	X	X	X		X	X			
Catalyst 4503-E with Supervisor Engine 6-E	X	X	X		X	X			
Catalyst 4506 with Supervisor Engine 6-E	X	X	X		X	X			
Catalyst 4506-E with Supervisor Engine 6-E	X	X	X		X	X			
Catalyst 4507R with Supervisor Engine 6-E	X	X	X		X	X			
Catalyst 4507R-E with Supervisor Engine 6-E	X	X	X		X	X			
Catalyst 4510R with Supervisor Engine 6-E	X	X	X		X	X			
Catalyst 4510R-E with Supervisor Engine 6-E	X	X	X		X	X			
Cisco Catalyst 6500 Series Switches (IOS 12.2SX)									
Catalyst 6503-E with Supervisor Engine 720, 32, and 32-PISA	X	X	X						
Catalyst 6504-E with Supervisor Engine 720, 32, and 32-PISA	X	X	X						

Catalyst 6506-E with Supervisor Engine 720, 32, and 32-PISA	X	X	X						
Catalyst 6509-E with Supervisor Engine 720, 32, and 32-PISA	X	X	X						
Catalyst 6509-NEB-A with Supervisor Engine 720, 32, and 32-PISA	X	X	X						
Catalyst 6513 with Supervisor Engine 720, 32, and 32-PISA	X	X	X						
Cisco ME 6524 Ethernet Switches									
Cisco IOS Firewalls for Cisco Integrated Services Routers (ISRs) (IOS 12.4T)									
Cisco IOS Firewall for the Cisco 2811 ISR							X		
Cisco IOS Firewall for the Cisco 2821 ISR							X		
Cisco IOS Firewall for the Cisco 2851 ISR							X		
Cisco IOS Firewall for the Cisco 3825 ISR							X		
Cisco IOS Firewall for the Cisco 3845 ISR							X		

* In-progress of IPv6 certification

Conclusion

Cisco continues to be an industry leader in delivering a wide range of products that incorporate critical IPv6 features and functionality. For a complete list of Cisco products that have successfully completed the IPv6 certification process through the DoD/JITC process, currently the most stringent certification process defined, please see <http://jitc.fhu.disa.mil/apl/ipv6.html>.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)