SANDIA REPORT
SAND2007-4476
Unlimited Release
Printed July 2007

Supersedes SAND2006-3635
dated June 2006

A REPORT ON IPv6 DEPLOYMENT ACTIVITIES AND ISSUES AT SANDIA NATIONAL LABORATORIES: FY2007

John M. Eldridge, Tan C. Hu, Joseph H. Maestas, Lawrence F. Tolendino

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2007-4476
Unlimited Release
Printed July 2007

Supersedes SAND2006-3635
dated June 2006

A Report on IPv6 Deployment Activities and Issues at Sandia National Laboratories: FY2007

John M. Eldridge and Joseph Maestas
Advanced Networking Integration Department

Tan C. Hu, System Analysis and Trouble Resolution Department

Lawrence F. Tolendino
Network System Design and Implementation Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS0806

Abstract

Internet Protocol version 4 (IPv4) has been a mainstay of the both the Internet and corporate networks for delivering network packets to the desired destination. However, rapid proliferation of network appliances, evolution of corporate networks, and the expanding Internet has begun to stress the limitations of the protocol. Internet Protocol version 6 (IPv6) is the replacement protocol that overcomes the constraints of IPv4. As the emerging Internet network protocol, SNL needs to prepare for its eventual deployment in international, national, customer, and local networks. Additionally, the United States Office of Management and Budget has mandated that IPv6 deployment in government network backbones occurs by 2008. This paper explores the readiness of the Sandia National Laboratories' network backbone to support IPv6, the issues that must be addressed before a deployment begins, and recommends the next steps to take to comply with government mandates. The paper describes a joint work effort of the Sandia National Laboratories ASC WAN project team and members of the System Analysis & Trouble Resolution, the Communication & Network Systems, and Network System Design & Implementation Departments.

ACKNOWLEDGEMENTS

Many people contributed to the discussions, testing, and deployment planning that the authors document in this report. In particular, the following Sandia employees comprised the IPv6 project team.

Sandia IPv6 Project Team Members

Casey T. Deccio,	Department 8949
John M. Eldridge,	Department 9336
Richard D. Gay,	Department 8949
Michael J. Hamill,	Department 9334
Tan C. Hu,	Department 9338
Joseph H. Maestas,	Department 9336
Michael A. Rios,	Department 6432 (formerly 9334)
Lawrence F. Tolendino,	Department 9334
Vicki K. Williams,	Department 9334

Thomas Archuleta, Cisco Systems, Inc representative to Sandia provided the Cisco ScoreCard® software for the device surveys and support for installing and using the software.

Contents

Acknowledgements 4
Introduction 7
Background 7
OMB directive 9
NIST Guidelines 10
IPv6 Addressing Schema and Support Issues 11
SNL IPv6 Network Address and Subnet Configuration Decisions 12
Selected Method for Router Addressing 15
Selected Method for Host Addressing 15
Small Scale System Testing 15
Testbed 15
Configuration 15
Router Configuration Testing 17
DHCP Testing 17
DNS Testing 18
NTP – IPV6 Time of Day Service 19
Scope 20
Description of Setup and Test Results 21
Application Testing 26
IPv6 in the ASC WAN 27
Status of ASC WAN IPv6 Readiness 27
ASC WAN IPv6 Implementation Plan Based on NIST Draft requirements 29
ASC WAN IPv6 Addressing 29
ASC WAN IPv6 Routing 29
Risks 30
Schedule 30
Verifying ASC WAN IPv6 Implementation 30
Implementing Ipv6 in the SNL Enterprise 31
SNL Environments 31
Network Hardware Costs Estimates to Support IPv6 31
ConclusionS and Recommendations 32
Recommended Actions 33
Issues to Resolve 33
References 35
Bibliography 36
Appendix A: Network Device Survey Results 39
SRN Core and Distribution Router Status 39
SNL/NM SRN, IPv6 Capability Scorecard Results 40
Internet Protocol version 6 (IPv6) 42
Appendix B: Cisco Router – IOS Features and Releases 49

Figures

Figure 1: IPv6 Address Structure 12
Figure 2: SNL IPv6 Test Bed Configuration. 16
Figure 3: Network Time Service Components. 20
Figure 4: Linux Timeservice Configuration Commands. 22
Figure 5: Windows Vista IPv6 Based NTP Service Access. 24
Figure 6: Ubuntu Linux Log Showing IPv6 NTP Update 24
Figure 7: Vista IPv6 Based DNS Query and Response 25
Figure 8: ASC WAN Design in 2007. 27

Tables

Table 1: Comparison of Host Addressing Methods. 13
Table 2: Comparison of Router Addressing Methods. 14
Table 3: IPv6 Network Services Testing Status. 25
Table 4: Router Compliance with NIST Requirements. 30
Table 5: Survey of SRN Core and Distribution Router Readiness. 39
Table 6: IPv6 Upgrade Path for Switches 42
Table 7: IPv6 Upgrade Path for Routers 43

INTRODUCTION

The Internet Protocol suite is the network protocol of choice for Sandia National Laboratories (SNL) corporate computer networks. This protocol suite and its foundation protocol IP version 4 (IPv4) emerged from early government funded research networks. The growth of the Internet has led to the need to modify and evolve IPv4. The intent of the paper is twofold. The first is to highlight the emergence of Internet Protocol version 6 (IPv6) in the network environment, and the second is to point out the issues that SNL needs to resolve to successfully deploy IPv6.

SNL's expanding networking requirements as well as outside forces require that SNL prepare to deploy IPv6 in the corporate networks. In particular, the United States Government Office of Management and Budget (OMB) has mandated that all government agencies and government contractors deploy IPv6 by June 2008. That means that SNL's corporate networking environments and the WAN and LAN that makeup the ASC computing environment should be IPv6 capable by June 2008. To verify that the networks are indeed IPv6 capable, the IPv6 project team deployed some subset of network hosts and services to demonstrate an installed IPv6 network and operational capability.

In anticipation of an eventual IPv6 deployment, Sandia National Laboratories obtained an IPv6 prefix from ESnet, our Internet Service Provider on November 13, 2003. The team used this prefix (2001:400:4410::/48), which is 48 bits long, in the work that this paper describes.

In this paper, the authors provide information regarding the IPv6 readiness of SNL's network infrastructure and highlight decisions that SNL needs to make to support IPv6 in the corporate infrastructure. Further, we recommend the next steps to provide IPv6 capability at the enterprise level with the hope that the information that this paper provides allows SNL to formulate a measured response to this mandate. This response needs to be one that is appropriate to the current state of IPv6 technology, fulfills the spirit of the mandate, and provides real benefit to the enterprise. The router resource requirements identified in this paper pertain to SNL/NM only. Resources required for SNL/CA are different.

BACKGROUND

Internet protocol version 4 (IPv4) has served the networking community well for over 20 years delivering network packets to the desired destination. However, the limitations of IPv4 have become apparent as both the Internet and enterprise networking have grown explosively (see "The Evolution of the Internet and IPv6", Geoff Huston). The rapid growth of the Internet is quickly depleting the available IPv4 address pool. To obtain more addresses requires more address bits in the protocol, which means a longer IP address, which means a new architecture, which means changes to all of the routing software. In essence, this means a revision in the underlying elements of the network. After examining a number of proposals, the Internet Engineering Task Force (IETF) settled on IPv6, as recommended in January 1995 in RFC 1752. Over time, equipment manufacturers and application developers have slowly been adding IPv6 functionality to their equipment and software.

The need for more IP addresses has been the compelling reason for the adoption of IPv6. In the public sector, the Internet has spawned the development and adoption of numerous applications and devices, such as telephony appliances, personal digital assistants, and monitoring systems to

name a few, that require network connectivity. The utility and value of the Internet has also prompted many more people to connect computers to it.

While there may be alternative technical solutions, such as Network Address Translation (NAT), to the address space problem, they do not work easily to allow this growth of new, enhanced applications, services, and innovation. Furthermore, these alternative solutions make the Internet, the applications, and the devices more complex to configure and operate; thus, they cause higher costs. IPv6 can, in the medium to long time frame, make every IP device cheaper and more functional.

The primary design goal of IPv6 was to increase the address space. However, the protocol designers also took the version development as an opportunity to make other improvements to the protocol. The design of IPv6 incorporates new benefits that include:

- Expanded addressing capabilities. IPv6 has 128 bits of addresses space versus 32 bits of address space for IPv4.
- Server-less auto-configuration ("plug-n-play") and reconfiguration. Reference stateless IPv6 addressing below
- More efficient and robust mobility mechanisms.
- End-to-end security, with built-in, strong IP-layer encryption and authentication. IPv6 includes support for security, such as information encryption and the authentication of the source of this information in its specifications.
- Streamlined header format and flow identification.
- Inclusion of flow labels in the specification for better real time traffic support. Real time applications might include video conferencing and IP telephony. By means of flow labeling, routers can recognize the end-to-end flow to which transmitted packets belong and provide them a different level of service.
- Enhanced support for multicast and QoS.
- Extensibility: Improved support for options and extensions.

From the literature, it appears that there are technical and economic advantages in moving from IPv4 to IPv6. However, there is also a concern about the cost impacts and timing for the transition from IPv4 to IPv6. The generally accepted view is that a quick and forced move to IPv6 will be much more costly and disruptive than a more gradual evolutionary change. During the normal operation of a communication network, operations staffs constantly upgrade, grow, and replace equipment and software. The designers of IPv6 considered this requirement when developing the protocol. IPv6 and IPv4 can easily coexist within the same network.

The Internet Protocol is at the core of the Internet, SNL's networks, and collaboration networks. Over time, customers of these networks will require that the networks support the evolving protocol standards. The deployment of a new network protocol will affect many systems at SNL, and it will affect the processes that SNL uses to operate the networks. SNL needs to begin efforts to deploy IPv6 now because of the lead-time required to prepare for implementation.

Government mandates compel Sandia National Laboratories to prepare to use IPv6 in its networks. However, this is not the only reason to use IPv6. IPv6 provides some technical benefits that may provide SNL with programmatic benefits and opportunities to operate more efficiently. As IPv6 becomes more embedded in the operation of the Internet and customer Intranets, SNL will have to react to maintain long term inter-operability with these networks. Over time, SNL's network organizations will begin to receive customer requests for IPv6 capability. Customers will also introduce IPv6 components into the network knowingly and in some cases unknowingly. New versions of operating systems will increasingly include IPv6 as the default network stack running concurrently with an IPv4 stack. If SNL does not prepare for these network changes, these changes may introduce operational and security weaknesses into the network.

OMB directive

In response to The President's *"National Strategy to Secure Cyberspace*" (National Strategy) the U.S. Department of Commerce created a task force to examine the IPv6 technology. The President charged the task force with considering a variety of IPv6-related issues, "including the appropriate role of government, international interoperability, security in transition, and costs and benefits." The task force produced a report [COM] that describes IPv6 and its benefits and costs. A large section of the report deals with the role of the government in promoting IPv6 as a driver of business investment. It appears that the results of this task force contributed to the formation of an Office of Management and Budget directive that the government use IPv6 in its computer networks.

In the second half of 2005, the OMB issued a directive that government agencies must begin preparing for and supporting IPv6. The OMB directive outlines steps that agencies must take to comply. In response to this directive, the DOE has begun to take steps to implement the directive. In particular, the DOE has issued an Acquisition Regulation [DOE] letter that outlines requirements for information technology purchases to be IPv6 compliant. Part of this letter is language for a model contract that needs to be included in procurement contracts. Following the guidance in this OMB memorandum [Ev], agencies must take the following actions by:

> ***November 15, 2005***
> *• Assign an official to lead and coordinate agency planning,*
> *• Complete an inventory of existing routers, switches, and hardware firewalls,*
> *• Begin an inventory of all other existing IP compliant devices and technologies not captured in the first inventory; and*
> *• Begin impact analysis to determine fiscal and operational impacts and risks of migrating to IPv6.*
>
> ***February 2006***
> *• Using the guidance issued by Chief Information Officers Council Architecture and Infrastructure Committee, address your agency's IPv6 transition plan and provide the*
> *completed IPv6 transition plan as part of the agency's Enterprise Architecture (EA) submission to OMB.*
> *• Provide a progress report on the inventory and impact analysis, as part of the*

agency's Enterprise Architecture (EA) submission to OMB.

June 30, 2006
• Complete inventory of existing IP compliant devices and technologies not captured in first inventory, and
• Complete impact analysis of fiscal and operational impacts and risks.

June 30, 2008
• All agency infrastructures (network backbones) must be using IPv6[1] and agency networks must interface with this infrastructure. Agencies will include progress reports on meeting this target date as part of their EA transition strategy.

NIST Guidelines

The National Institute of Standards has prepared a set of guidelines [Ni] that seeks to assist Federal Agencies and non-governmental organizations in formulating plans for the acquisition and operational deployment of IPv6 technologies. The guidelines identify standardized IPv6 deployment and operations profiles. The standard profile is meant to:

- define a simple taxonomy of common network devices;
- define their minimal mandatory IPv6 capabilities and identify significant options so as to assist agencies in the development of more specific acquisition and deployment plans; and,
- provide the basis to define further the technical meaning of specific policies.

The document presents information in a format that is independent of specific vendor platforms, operating systems, or applications. Throughout, it goes back to references of the pertinent Internet standards. The recommendations and profiles in the document are conservative by nature, so that they should apply to a very wide range of systems. This approach provides the highest likelihood of functional interoperability.

The document provides profiles meant to be a landmark to guide the acquisition and deployment of significant new IPv6 capabilities in operational systems. The profiles do not attempt to grandfather existing early implementations, or to cover potential non-production uses of the technology in test-beds, pilots, etc. Further, it is meant as a strategic planning guide for future acquisitions and deployments in operational networks. The document profiles cover guidelines for several aspects of an IPv6 deployment. The document defines profiles for hosts, routers, network protection devices, and network management. There are three device types: Hosts, Routers and Network Protection Devices, defined as:

1. **Host:** any Node that is not a Router.
2. **Router:** a Node that forwards IPv6 packets not explicitly addressed to itself.
3. **Network Protection Devices:** Including Firewalls and Intrusion Detection / Prevention devices that examine and selectively block or modify network traffic.

[1] Meaning the network backbone is either operating a dual stack network core or it is operating in a pure IPv6 mode, i.e., IPv6-compliant and configured to carry operational IPv6 traffic.

The document does not address specific applications at this stage of IPv6 deployment. Rather it outlines infrastructure services that the network should provide to customer applications. To the extent that Domain Name resolution is a requirement for all systems, the provisions of RFC 3596 *DNS Extensions for IPv6* [45] apply to both hosts and routers. Quad-A resource records, as defined by the RFC, are in particular mandated for both, along with Extension mechanisms for DNS queries and responses. In some relation to this is the specification of URIs. The Host part of a URI may be specified as a registered domain name (e.g. nist.gov), or an address. IPv4 addresses take the form '192.168.0.1', while IPv6 addresses have a more complex syntax including such styles as '2001:db8::7'. The provisions of RFC 3986 *Uniform Resource Identifier: Generic Syntax [46]*, are mandatory for Hosts, to cover these formats. There is a set of RFCs (3493, 3542, 4584 [47]-[49]) relating to Socket API extensions for IPv6, and these SHOULD be implemented in hosts that provide such interfaces to applications.

This NIST profiles address capabilities for production level, large-scale deployment of IPv6 devices. Towards this goal, the document specifies general requirements for network management. In particular, the profiles call for all nodes to support a basic Simple Network Management Protocol (SNMP) capability and provide the basic IPv6 Management Information Base (MIB) specified in RFC4293 [66]. Routers, in addition, must support the Forwarding Table and Tunnel MIBs. Future versions of this profile are expected to require full support of IPv6 MIBs at the Network and Transport layers.

The NIST document [Ni] is a technical specification for IPv6 devices, and it is intended to benefit agencies in their procurement and use of IPv6 devices. The specification focuses on the capabilities necessary to establish a core IPv6 network infrastructure, with basic data-plane services, and secure its use. Future versions of the profiles are expected to enhance these basic network services (e.g., in the areas of security, quality of service, mobility) and define specific application uses of IPv6.

IPV6 ADDRESSING SCHEMA AND SUPPORT ISSUES

SNL currently has five provider independent class B address blocks (132.175.0.0/16, 134.252.0.0/16, 134.253.0.0/16, 134.218.0.0/16, and 146.246.0.0/16) and several contiguous blocks of class C's (192.73.207.0/24, 196.208.220-223.0/24, and 205.137.80-95.0/24, etc). In the early 1990s, Sandia National Laboratories (SNL) started to manage these address spaces and the IPv4 environment. The current support infrastructure assumes a default standard class C addresses assignment (24-bit netmask) drawn from the legacy class B blocks (16-bit netmask). The current allocation practice permits only 256 subnets per class B block.

An IPv6 address is four times as large compared to IPv4 address, i.e. 128 bits versus 32 bits. Addresses are written using 32 hexadecimal digits arranged into eight groups of four digits that are separated by colons. Therefore, the written form of IPv6 address could look like this at SNL:

2001:400:4410:0016:020d:56ff:fe77:52a3.

Because of its length, an IPv6 address is much more difficult to remember and deal with than an IPv4 address. The actual address is composed of at least two parts; a prefix provided by the

enterprise Internet Service Provider (ISP) and a suffix generated in a variety of ways by the enterprise. For instance, the suffix may actually contain two parts. The format of an IPv6 address is illustrated in Figure 1.

Figure 1: IPv6 Address Structure

In this case, the parts are the global prefix assigned by the ISP, a subnet ID assigned by the enterprise, and an interface ID. Depending on host configuration, the host may self assign the interface ID as the interface MAC address with a prefix of fffe.

By design, the address structure is hierarchical so that routes can be summarized. To take advantage of IPv6, the SNL subnet assignment practice must be enhanced to provide address assignment capabilities as follows:

1. Using 128 bit addresses in nibble format.
2. Contain network prefix and netmask.
3. Track subnet address assignment out of the given address space to permit proper sizing to match actual machine count.
4. Support EUI-64 subnet assignment scheme.
5. Support 65535 subnet assignments as a minimum (assuming a 16 bit Subnet ID).
6. Return a network matching the desired client numbers for efficient use of addresses.

The differences between IPv6 and IPv4 are in five major areas: addressing and routing, security, network address translation, administrative workload, and support for mobile devices. Wikipedia, the online encyclopedia at URL http://en.wikipedia.org/wiki/IPv6, provides a list of new features introduced by IPv6. As IPv6 becomes more prevalent, the support staff will have to understand the differences as compared to IPv4 and adjust SNL practices accordingly.

Another IPv6 address management issue to be aware of is some IPv6 address prefixes are "owned" by the Internet Service Providers (ISP). This means that both multi-homing and changing ISP are issues to consider. In the case of multi-homing, the end site is limited to using the same ISP since a different ISP would have to use a different IPv6 prefix assignment for the same site. In the second case, sites that change ISPs would require renumbering all host IPv6 prefixes to that assigned by the new ISP. However, the Internet naming organizations have recently provided the means for organizations to request ISP independent addresses. This change makes it easier for entities to changes ISPs.

SNL IPv6 Network Address and Subnet Configuration Decisions

To arrive at a decision for addressing methodology, the project team considered addressing for both network routers and for computer hosts. Each device performs a different role, and there are different considerations for choosing the addressing methodology for each. The project team considered three addressing methods for each type of device. These methods included manual,

stateless, and statefull (DHCPv6) addressing. Table 1 and Table 2 provide comparisons of the trade-off for each addressing method.

As an example of the management decisions that must occur before the introduction of IPv6 into the SNL environment, one must consider the method of IPv6 address assignment. Address assignment can be either automatic or manual. There are two accepted methods for performing automatic address assignment for hosts systems. Most of the world considers Stateless automatic EUI-64 address assignment to be one of the most significant new IPv6 capabilities because it replaces manual or DHCP address assignment processes.

Even if SNL uses EUI-64 automatic, or stateless address assignment, client systems and network services must exchange additional information. This information includes domain membership and associated information such as DNS name server addresses. There is also a reverse information flow from the client to register/update DNS. Unfortunately, the methods for disseminating such information are still under debate, which makes IPv6 deployment more difficult.

Table 1: Comparison of Host Addressing Methods.

Host Addressing Methods	Pros	Cons
Stateless (RFC 2462, Router Based, RFC 3041 Privacy Extensions for Stateless Address Auto-configuration in IPv6, RFC 4193 Unique Local IPv6 Unicast Addresses).	• Simplicity. Address assignment without management intervention. • Multiple concurrent assigned addresses with different lifetimes to facilitate re-location of hosts • Generation of default gateway. • Separate Global and link local addresses.	• Automated tracking of an IP address to a node is not available. (Security related). • In case of network outages, neighbor discovery may not function correctly resulting in duplicate addresses. (Theoretical) • The host can control the process for address assignment and reassignment. (Do you trust the host node to perform this task?) • Limited to EUI-64 addressing scheme which could lead to inefficient use of assigned address space • Dynamic update of DNS is required. • Manual configuration of host domain name server is still necessary.
Statefull (RFC 3315, DHCPv6)	• Consistent with existing network configuration and operation. • Security posture with DHCP is known and accepted. • Single centralized resource for the assignment, distribution, and tracking of network addresses. • Easier management as compared to stateless assignment. • Presentation to host for IPv6 address and other relevant information. • Routers could act as DHCPv6 servers (IETF-draft) to reduce additional	• Availability of DHCP server software is limited. • DHCPv6 does not completely define DNS server (or domain) for the host. (Manual configuration is still required.) • Increased complexity on the host. Must support DHCPv6 client. • Additional router configuration to support a centralized DHCPv6 server. (The case when the DHCP server is not on the same local link as the host).

	hardware.	• Automated tracking of an IP address to a node is not available on client side. (Security related). • The host can control the process for address assignment and reassignment. (RFC 3041 Privacy Extensions for Stateless Address Auto-configuration in IPv6)
Manual	• Simple with minimal auxiliary support services. • Only current method to perform DNS configuration. • Fix address for widely used services and data access. (Web, mail, etc.)	• Tedious and error prone. • Hands on changes at each node. • Not scalable and adaptable to changing network • Does not prevent RFC 3041. So automated tracking of an IP address to a node is not available on client side. (Security related).

Table 2: Comparison of Router Addressing Methods.

Router Addressing Methods	**Pros**	**Cons**
Link Local (RFC 4193 Unique Local IPv6 Unicast Address, RFC 2462)	• Automatic network addressing. • Minimal network router configuration. • Address is already present and method does not consume any other resources. • Service provider reassignment with minimal router changes.	• Reduced flexibility for in-band interface connectivity. • Possible maintenance and trouble shooting complexity. • Lack ability to monitor interfaces via the interface's address. (SNMP, Netflow, etc.) • Network configuration is dynamic and may present different or unknown topologies over time. • Possible longer recovery time in case of outages for the network to reassign addresses and to propagate routes. • Static route entries become difficult or impossible. (At a minimum, they are different.)
Statefull (DHCPv6)	• Allow DNS updates with reduced security risk	• Inefficient use of router resources
Manual	• Simple with minimal auxiliary support services. • Consistent with existing IPv4 network.	• Tedious and error prone. • Hands on changes at each node. • Requires assignment of subnets for routing purposes where the subnets are particularly small. • Higher operational cost and not scalable.

Selected Method for Router Addressing

For router addresses, SNL will use manual address assignments. Subnet ordering for router addresses will begin at the high end of the subnet address range and progress downward. While the use of manually assigned addresses will add additional configuration effort, it will allow us to maintain better control over the configuration.

Selected Method for Host Addressing

For host addresses, SNL will use DHCPv6, or statefull automatic addressing, for most hosts. SNL will use fixed, or manual, addresses for servers. This method will allow SNL to maintain a higher measure of commonality with the current IPv4 network. Stateless address assignment is only possible when using EUI-64 based identifiers. To maintain the ability to use stateless address assignment, SNL will use /64 subnet masks. Subnet assignment for hosts will begin at the lower end of the prefix range and progress upwards.

SMALL SCALE SYSTEM TESTING

Testing the IPv6 readiness of the enterprise network environment involves testing network elements, network services, and host systems. The project team used the current corporate IPv4 network as a guide. The small-scale testing focused on network routers, DHCP network services, domain name services, network time-of-day services, and a small set of host applications. All of the testing reported in this document occurred in our development laboratory with a very limited number of network elements and hosts. The following sections of this document cover these tests in more detail.

TESTBED

Configuration

An IPv6 test bed was created in the Advanced Networking Integration Department laboratory using many of the existing resources. The test bed consists of two routers and four switches as shown in Figure 2.

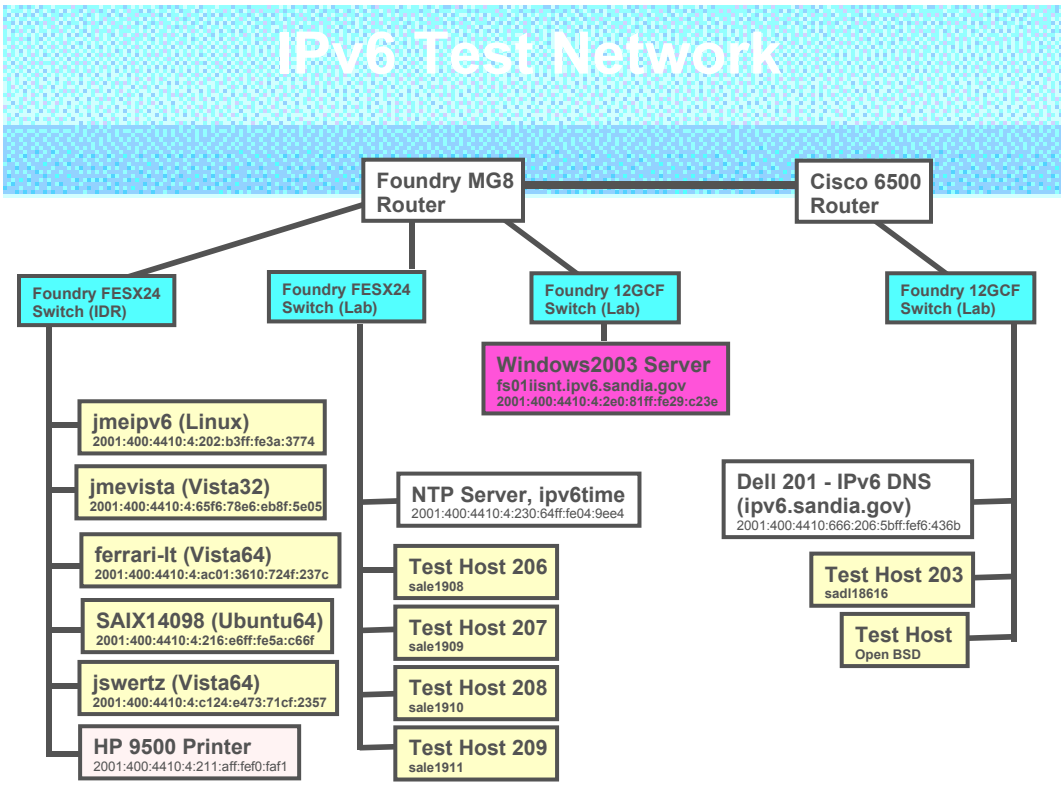

Figure 2: SNL IPv6 Test Bed Configuration.

All the test bed elements are running both IPv6 and IPv4 in a dual stack configuration that represents the most likely SNL network production environment. Several other existing resources were added to the test bed to provide network services against which to test IPv6 network client systems.

1. One Foundry router and one Cisco router are at the heart of the test bed and represent the typical SNL routers in operation today. Each router was configured as it would be in an operational SNL IPv6 network.
2. Both Cisco and Foundry switches were also configured into the test bed since both are used in the SNL production networks.
3. An existing HP9500, a network attached printer, was upgraded to support IPv6 and configured for standalone IPv6 printing.
4. A Microsoft Windows 2003 server was configured to support IPv6 and used to test IPv6 remote mounted disk volumes.
5. A new NTP timeserver appliance was purchased and added to the test bed to verify the viability of NTP updating via IPv6 packets. The NTP server uses IPv4 to synchronize with an existing IPv4 based timeserver.
6. One of the Dell servers (201) was used as a DNS server for the domain ipv6.sandia.gov and the IPv6 enabled network servers were added to the proper quad-A based tables.
7. A representative set of desktop clients were configured with IPv6 and used in day-to-day operations to exercise the network services.

Several operating systems are IPv6 enabled in the test bed as shown in the diagram; however, one may note that Windows XP is not represented. XP cannot function in a pure IPv6

environment and depends on IPv4 packets to interact with certain network services such as DNS. Therefore, Windows XP cannot serve to test IPv6 based network services.

Router Configuration Testing

Configuring network routers to support IPv6 is the most obvious requirement to provide IPv6 capability in network backbones. To become familiar with IPv6, the team enabled it on two routers in the network development laboratory. Sandia currently deploys network equipment from two major vendors – Cisco and Foundry - in the unclassified and classified environments. The initial test involved Foundry MG8s populated with V6 blades. This configuration is typical of current generation, network routers from major vendors. Using these routers, the project team tested both EUI-64 and non-EUI-64 addressing schemes. The routers were capable of implementing both address assignment and advertisement functions. The Linux client however would log error messages when it received a non-EUI-64 advertisement. It is uncertain if Microsoft clients behave similarly. OSPF version three is required for IPv6. It is active on both test routers, but we have not thoroughly exercised it. The project team added a Cisco 6500 with IOS 12.2.(18)SXD7 loaded on a Supervisor 720 management module to the mix. For rudimentary connectivity testing, the project team enabled a loopback interface with an EUI-64 address and OSPFv3. ICMP6 was successful between an IPv6 system, that was two hops away, and the loopback interface. IPv6 routing exchange was also successful with OSPFv3.

Examination of Cisco's documentation on the company's website[2] indicates that Cisco's full feature IPv6 release is contained in the 12.4 IOS. Earlier versions of the IOS train, starting with 12.0.S, support IPv6; however, they do not support the complete feature set as in IOS 12.4. It is not clear that the Supervisor 2/MSFC2 management blades are capable of supporting IOS 12.4. Supervisor 2/MSFC2 does support limited IPv6 with IOS version 12.2(18)SXD7 and later. For full IPv6 functionality, the routers need to operate at IOS version 12.4. A survey of the SON and SRN network environments determined router readiness. The survey results, see Appendix A, indicate that there are 119 and 437 Cisco devices respectively in the SON and SRN. Out of those numbers, approximately 50 devices in the SRN function as routers. The other devices function as switches, and as such, they will support the transport of IPv6.

A move towards activating IPv6 can follow three paths. The first would be upgrading all Cisco routers in the SON and SRN to IOS 12.4. This upgrade would consist of software; a combination of additional memory, flash, supervisor modules, fan trays, power supplies; and additional replacement blades to address incompatibilities. The second path would be to implement the minimum IPv6 support by locating the appropriate IOS images from 12.0S, 12.xT, 12.2S.12.2SB, 12.3, and 12.4 to match the existing equipment. Additional hardware upgrades may still be necessary. The last path is to replace the equipment with IPv6 capable systems as time and budget permits. It would be the lowest cost path; however, it runs into the probability of not meeting the June 2008 mandate.

DHCP Testing

DHCP is a network service that is a critical component for the current IPv4 infrastructure as it automatically provides IPv4 addresses to requesting hosts while also providing configuration

[2] URL: http://www.cisco.com/ipv6 , reviewed June 29, 2007.

information, such as the addresses of DNS servers and domain names. We entered the study of the IPv6 protocol with the expectation that DHCP would provide the same critical functions in this new environment. Indeed, there is an IETF document RFC 3315 that defines the DHCPv6 services. However, we have learned that one of the perceived strengths of the IPv6 protocol installation is the ability to assign addresses without coordinated server involvement, or stateless auto-configuration, see RFC 2462. That is, there are two mainstream methodologies for providing hosts with dynamic IPv6 addresses, a stateless model and a stateful model. DHCPv6 represents the stateful model of assigning addresses while auto-configuration represents the stateless model.

Stateless configuration is seen as simplifying the network administration task. From reading the literature and searching for DHCPv6 server software[3], it became obvious to us that there is a worldwide desire to minimize the need for DHCP type services. Therefore, the project team is examining both stateful and stateless configuration strategies for an IPv6 network in our IPv6 testing. Our literature search and testing reveal that the Dibbler DHCPv6 software is an adequate test vehicle for these studies. Client software has been tested on Linux, Windows Vista, and Windows XP hosts with server software installed on a Linux host. So far, all the hosts have been able to receive an IPv6 address assignment and have successfully obtained an IPv6 DNS address as well as a domain name from the server. Windows XP hosts use IPv4 packets to communicate with the DHCPv6 server. The drawback for Dibbler is that, while Dibbler seems to work well, it is not a commercial product.

Testing a Linux IPv6 client (Fedora Core 4) showed that the Dibbler client software worked correctly using only the IPv6 protocol stack. The Fedora client successfully obtained a new global IPv6 address along with domain name and DNS server address. Similar tests executed on Microsoft Vista systems also showed that the Dibbler client software worked correctly utilizing IPv6 packets.

Although an attempt was made to use other versions of DHCPv6 client and server software, the Dibbler client and server software has proved to be the most useful on both Linux and Windows platforms. However, one should note that the technical community is not spending much time or effort on DHCP service for IPv6. The community seems to be favoring the use of other forms of automatic address assignment. Few system implementers seriously consider widely using manual IPv6 address assignment because of the length of and complexity of IPv6 addressing. If SNL does not use DHCPv6 to assign IPv6 addresses, then it will have to identify how it will dynamically update the DNS servers. The interested reader can follow developments in this area through the IETF drafts.

DNS Testing

Testing the DNS service means ensuring that DNS implements the pertinent standards. These standards include RFC 2136, RFC 3007, RFC 3226, RFC 3364, RFC 3365, and RFC 3596. To provide the IPv6 DNS function, the project team configured a Dell server running the SNL

[3] See reference: DHCPv6 at sourceforge, URL: http://sourceforge.net/search/?type_of_search=soft&words=dhcpv6, reviewed June 29. 2007.

corporate Redhat Enterprise WS 4.0 Linux, and then loaded it with Bind 9.2.4.2 to provide DNS services. DNS records of type AAAA and PTR populated both the forward and reverse lookup zones. The project team tested and checked DNS functionality with Linux IPv6 and Windows Vista clients, and both the forward and reverse address lookup works properly. DNS queries were restricted to IPv6 only; though, bind, when properly configured, could accept both IPv4 and IPv6 packets.

With stateless IPv6 addressing, the very real concern is how to implement a trusted IPv6 dynamic DNS update process. Sandia's current usage of DHCP with IPv4 can be considered stateful, and since the current IPv4 DHCP servers are considered trusted servers, they are allowed to update the DNS servers providing real time, dynamic updates to address information. If dynamic IPv4 addresses are not used on a particular host, then fixed IP addresses are used and entered into NWIS. Therefore, the NWIS database is another authoritative source for SNL DNS.

In the IPv6 world, things will get more complicated and several scenarios will have to be examined if dynamic DNS updates are to be provided. Assuming the IPv6 clients can be configured with DNS name server information using the IPv6 automatic configuration process, dynamic DNS server updates could be done by the host. However, this means that DNS servers would have to accept updates from all IPv6 clients and there would be no single trusted source for dynamic updates. Another solution to this problem might be to populate the NWIS database with host NIC addresses and use that information, along with IPv6 subnet and prefix information, to provide the IPv6 global addresses to the DNS servers. One of the difficulties of implementing this option is that a single IPv6 host WILL BE ASSIGNED multiple IPv6 addresses (see RFC3041, Privacy extension for stateless address auto configuration). Neither of these suggestions seems particularly attractive at this time; so, SNL intends to pursue the option of using stateful IPv6 address assignment based on DHCPv6. This solution will mimic the address assignment process currently implemented for IPv4.

Having an IPv6 capable DNS server running is critical to system level tests. Without it, application testing is almost impossible as illustrated in the next section. SNL's corporate DNS servers currently support IPv6; however, the servers implement neither the forward nor the reverse zones.

NTP – IPV6 TIME OF DAY SERVICE

The IPv6 protocol provides many integrated services that were previously separate and distinct in IPv4. Disciplined network time is not one of the integrated services, despite its importance to maintaining a reliable IT infrastructure in terms of security (authentication, authorization, and accounting) and availability. SNL's existing infrastructure for providing UTC-based synchronization does not support IPv6 nor can SNL upgrade it to provide this feature. Therefore, testing time services served two primary purposes: to evaluate time-keeping systems for SNL's production network and to identify any issues that may impact our ability to reliably synchronize network systems as well as other IPv6-capable information systems.

The Spectracom NETCLOCK/GPS appliance, model 9283, was used to provide the IPv6 testbed with a disciplined Time of Day (ToD) service. This appliance is dual stack, meaning that it supports both IPv4 and IPv6 simultaneously. Since it was not feasible to install an external

antenna to obtain a primary reference from the Global Positioning System (GPS) navigational systems within the lab environment, another method was needed to synchronize this system to Universal Coordinated Time (UTC). To accomplish this, the timeserver was configured to obtain its reference time from one of several production Stratum 1 GPS timeservers available at Sandia using the Network Time Protocol (NTP), via IPv4. Success was declared when the stratum level of the new system equalized to the Stratum 2 level, one level up from its reference.

IPv6 capable systems within the lab environment were subsequently able to use NTP via IPv6 for time synchronization. Figure 3 below summarizes this scenario. The direction of the arrows signifies the reference from which the system derives the time. For example, the IPv6 hosts derive their time from the IPv6 timeserver, the 9283 NetClock. In turn, the IPv6 timeserver derives its time from one of the three IPv4 timeservers.

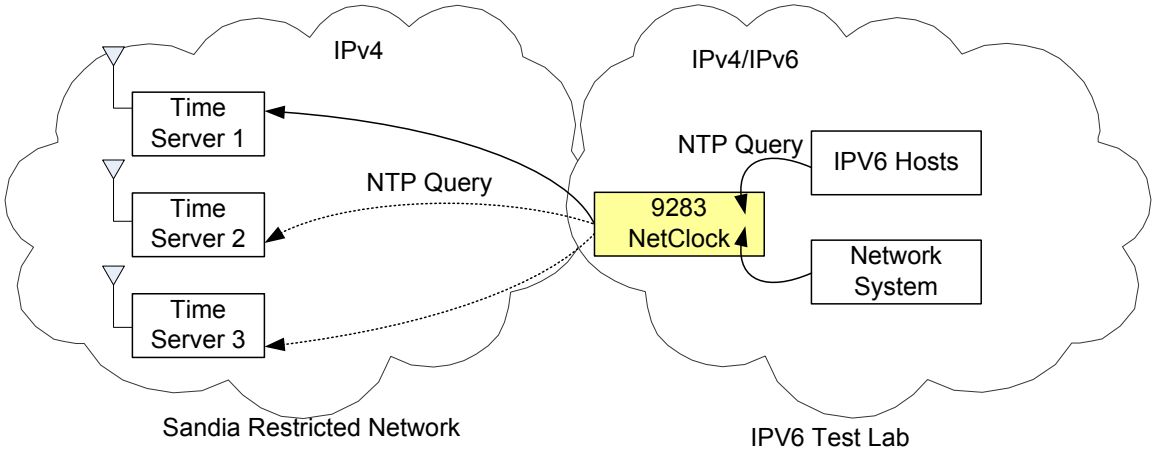

Figure 3: Network Time Service Components.

Scope

The IPv6 timeserver resides on the "4" IPv6 subnet, herein after referred to as v6-4, as well as in the v4-4 subnet. The lab testbed also had a v6-666 subnet. The project team placed hosts in all three subnets to obtain a full range of inter- and intra-subnet, as well as inter- and intra-IP version testing. The project team purposefully limited the NTP test modes and tested only client-server modes while eliminating peer and broadcast modes. One should note that IPv6 does not use broadcast services, but rather replaces the functionality with multicast services. As a learning experience, it would be interesting to test the broadcast modes. Albeit its use would likely be non-existent at SNL since the existing Time-of-Day services and the time-dependent hosts rely on the client-server model. The client-server mode can be described as follows: a host client sends a request for time information to the IPv6 timeserver and expects a reply from that server. During the actual testing, a system achieves success when it, in response to a request for time, successfully receives the reply and subsequently adjusts its clock accordingly.

Description of Setup and Test Results

9283 NetClock

As designed by the manufacturer, the 9283 NetClock appliance was easy to configure. Initial network configuration is accomplished via the setup interface, a serial RS-232 asynchronous port. During initial configuration, the system prompts for various settings and server addresses including DNS servers. Initial system settings cover IPv4 configuration, IPv6 configuration, and finally selecting various services to establish a remote connection to the unit. Via the WEB user interface, additional configuration details are available such as for SNMP configuration, NTP configuration, SSH, Radius, etc. The NTP configuration was also straightforward. Via the WEB user interface, one selects unicast mode while disabling NTP broadcasting. Service filters were turned off by default, allowing service to all IPv4 and IPv6 requests. This particular timeserver is capable of servicing 4,000 time requests per second. When authentication mode is enabled, to allow or deny requests from specific hosts or network segments, the load capacity drops to 340 time requests per second[4]. External, network-based, time references are configured using the NTP reference display. This particular setting enabled us to derive time from the production Stratum 1 servers. When doing so, the selection of "Enable Stratum 0" must be off (local unit cannot become a Stratum 1 reference), otherwise the unit will fail to synchronize to the production servers. When the 9283 is deployed in a production setting and a feed from an external antenna is terminated on the unit, the "Enable Stratum 0" setting can be selected to enable the unit to become a Stratum 1 reference. Obviously, there are other types of configurations than can be performed to enable the full breath of capabilities of this system. However, for the purpose of the IPv6 test lab, additional configuration is unnecessary.

Linux and Ubuntu64

NTP configuration for Linux, regardless of the OS flavor, involved editing the ntp.conf file or the xntp.conf file, depending on the distribution, and then starting the NTP daemon. The two most important configurations in the *.conf file for testing NTP REQUEST/REPLY functionality are the "server hostname" statement and the "restrict" statement. A simplified ntp.conf file used in the lab is listed in the table below. Here, the server statement uses the fully qualified IPv6 domain name (FCDN) assigned to the NetClock unit. Alternatively, the server's global IPv6 address could have been used instead of the name. In reality, multiple server statements should be configured in the event that there are problems with one of the timeservers. The "restrict statement" provides better control and security over what NTP can or cannot do. The "restrict statement" can be problematic to set up correctly the first time. Commenting them out until NTP is verified to be up and running will generally save a lot of time debugging. The project team made no attempt in this phase of the test to control NTP access tightly. For a production system, the "restrict statements" are critical, and the system administrator should thoroughly understand their operation. When NTP is properly working, it adjusts the local system time over a period to match that of its configured time server or reference clock.

[4] Load capacity was taken from the manufacturer's specification.

```
# /etc/ntp.conf
# restrict default nomodify notrap noquery
# restrict 127.0.0.1
# restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
# logfile
logfile /var/log/ntp.log
server ipv6time.ipv6.sandia.gov
```

Figure 4: Linux Timeservice Configuration Commands.

Verification of NTP operation by several methods.

1) **Via the logfile** configured in ntp.conf. Refer to the syslog output file if logging is not explicitly configured in ntp.conf.

   14 Jun 15:09:38 ntpd[30117]: synchronized to 2001:400:4410:4:230:64ff:fe05:9ee4, stratum 2

2) **ntpq -p**

```
# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*2001:400:4410:4 ddd.ddd.ddd.dd   2 u  252 1024  377    0.312   -1.230   0.137
 LOCAL(0)        LOCAL(0)        10 l   51   64  377    0.000    0.000   0.004
```

3) **ntpdate –d FQDN**

```
ntpdate -d FQDN
18 Jun 15:30:10 ntpdate[2995]: ntpdate 4.2.0a@1.1190-r Thu Oct  5 04:11:32 EDT 2006 (1)
Looking for host xxx.ipv6.sandia.gov and service ntp
host found : 2001:400:4410:4:230:64ff:fe05:9ee4
transmit(2001:400:4410:4:230:64ff:fe05:9ee4)
receive(2001:400:4410:4:230:64ff:fe05:9ee4)
transmit(2001:400:4410:4:230:64ff:fe05:9ee4)
receive(2001:400:4410:4:230:64ff:fe05:9ee4)
transmit(2001:400:4410:4:230:64ff:fe05:9ee4)
receive(2001:400:4410:4:230:64ff:fe05:9ee4)
transmit(2001:400:4410:4:230:64ff:fe05:9ee4)
receive(2001:400:4410:4:230:64ff:fe05:9ee4)
transmit(2001:400:4410:4:230:64ff:fe05:9ee4)
server 2001:400:4410:4:230:64ff:fe05:9ee4, port 123
stratum 2, precision -18, leap 00, trust 000
refid [2001:400:4410:4:230:64ff:fe05:9ee4], delay 0.02579, dispersion 0.00000
transmitted 4, in filter 4
reference time:    ca2170ea.9e108c3f  Mon, Jun 18 2007 15:00:26.617
originate timestamp: ca2177e3.057eaa2a  Mon, Jun 18 2007 15:30:11.021
transmit timestamp:  ca2177e3.05cf0307  Mon, Jun 18 2007 15:30:11.022
filter delay:  0.02592  0.02582  0.02579  0.02579
       0.00000  0.00000  0.00000  0.00000
filter offset: -0.00135 -0.00134 -0.00134 -0.00134
       0.000000 0.000000 0.000000 0.000000
delay 0.02579, dispersion 0.00000
offset -0.001348
```

18 Jun 15:30:11 ntpdate[2995]: adjust time server 2001:400:4410:4:230:64ff:fe05:9ee4 offset -0.001348 sec

Windows Vista
The Windows Time Service is on by default in systems running Vista. Default settings rely on a reliable Windows Domain Controller for time; or if the system is a part of a workgroup, the time.windows.com server is used as the trusted time source. For the lab, it was desirable to derive time from the 9283 NetClock via IPv6. For this, the following command was used:

w32tm /config /syncfromflags:manual /manualpeerlist:ipv6time.ipv6.sandia.gov

Verification of NTP operation by several methods.

1) System Event Log: an entry in the event log is made when the Windows Time Service cannot establish contact with the configured time source.
2) Via a Wireshark packet trace.

Network Systems
At the time of publication of this document, the project team has not yet configured the Foundry and Cisco devices in the lab to test time synchronization via IPv6.

Team members installed Wireshark, an IP packet capture and analysis tool, on both Vista and Linux client systems to test the correct functioning of network services. The packet traces were used to verify that network services actually functioned. As shown by Figure 5, Figure 6, and Figure 7 Windows Vista and Ubuntu Linux client systems successfully used IPv6 packets to access both DNS and NTP network services.

Vista NTP Update Request and Response

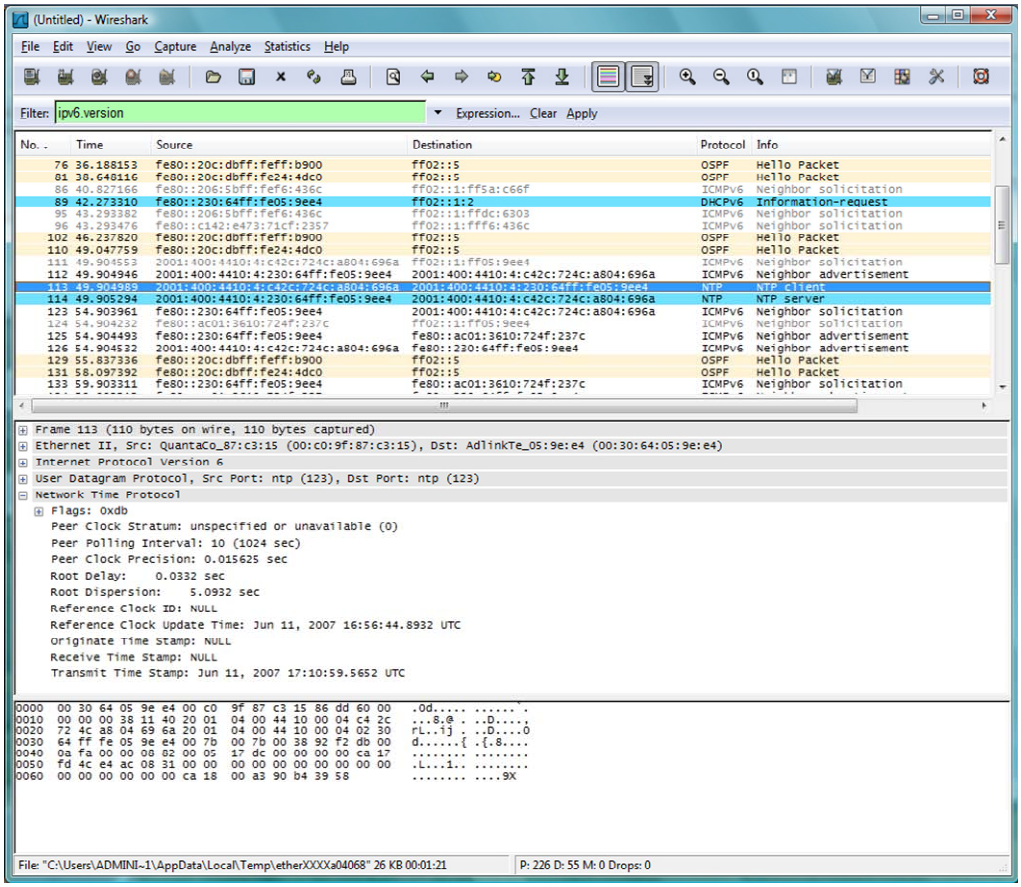

Figure 5: Windows Vista IPv6 Based NTP Service Access.

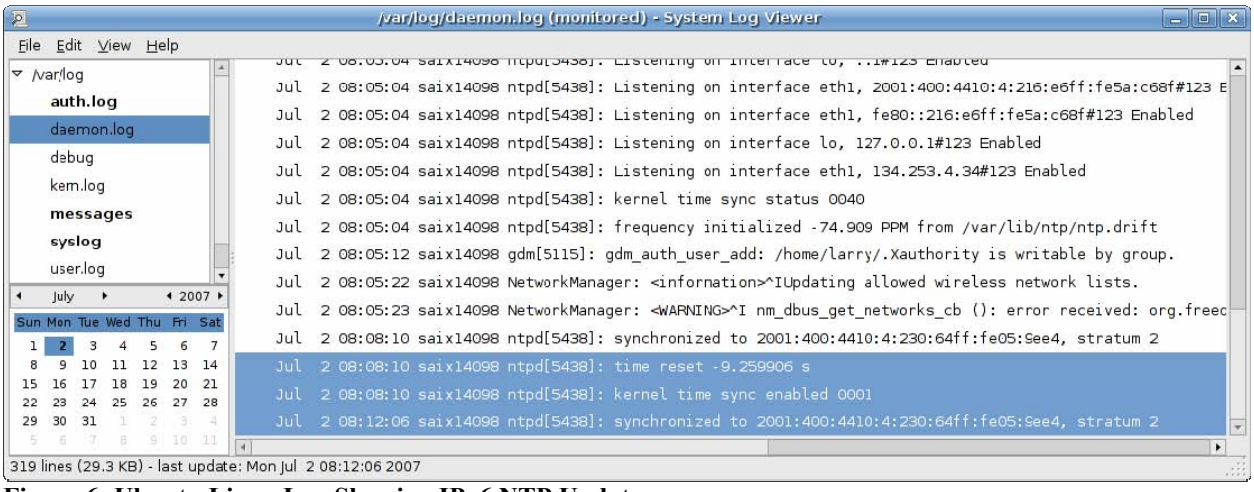

Figure 6: Ubuntu Linux Log Showing IPv6 NTP Update

Vista IPv6 DNS Query and Response

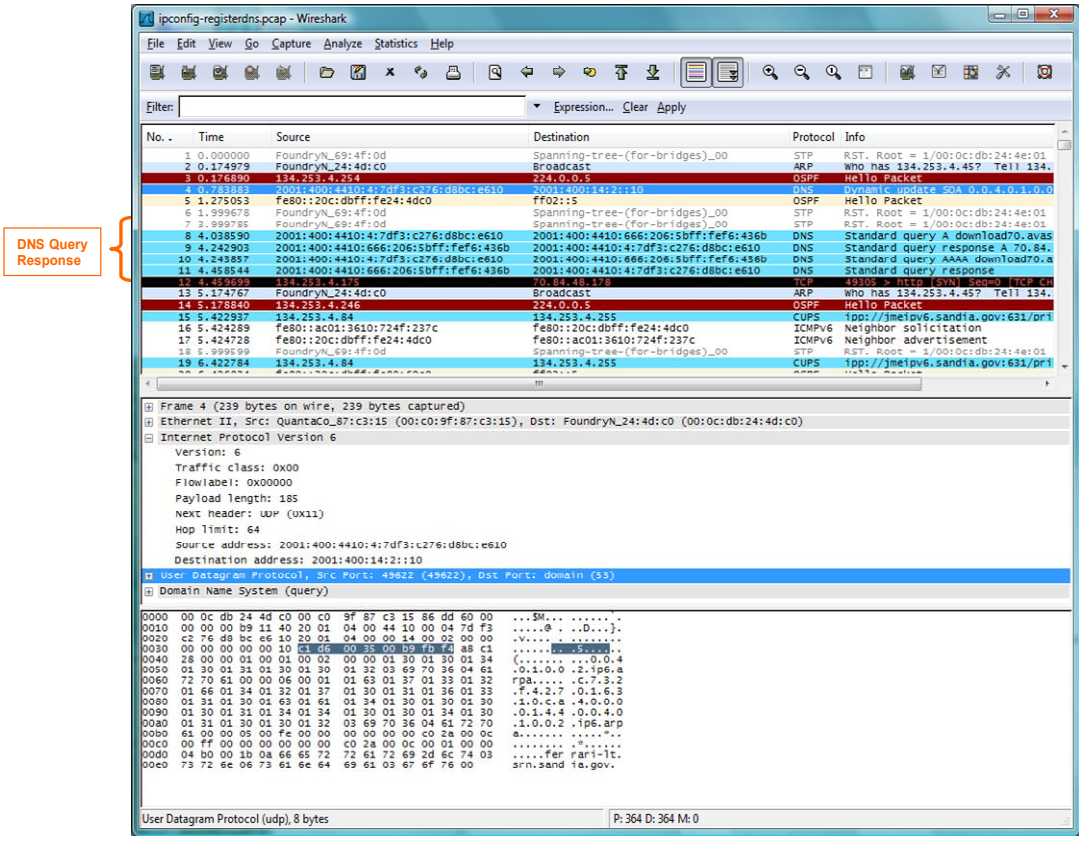

Figure 7: Vista IPv6 Based DNS Query and Response

The following table shows the current state of IPv6 network services testing. It is intended that this table reflects the current state of our client testing, and it will be updated as more testing is completed.

Table 3: IPv6 Network Services Testing Status.

Note: X indicates successful test, -- indicates no test performed.				
Network Service or Function	**Ubuntu Linux**	**Windows Vista**	**Redhat Enterprise Linux**	**FreeBSD**
DNS	X	X	--	--
Network attached printing	X	X	--	--
Windows2003 Server - Disk Mounting	--	X	--	--
NTP Time server	X	X	--	--
DHCP	--	--	--	--

Obviously there is much more work to do as there are no results for Redhat and FreeBSD at this time. However, the initial results allow us to make some observations about the difficulty of configuring clients to use IPv6 network services and validating correct operation.

- First, Windows Vista has the most complete IPv6 implementation tested to date at SNL.

- Second, even with the best implementation, it is difficult to verify correct IPv6 based network services operation.
- Third, given that the servers, clients and network elements all run dual stack configurations, one cannot know how a particular service request is satisfied, IPv4 or IPv6, without careful analysis.
- Fourth, supporting IPv6 packets does not mean that IPv6 network services can be used successfully. In fact, the Linux systems do not execute standard IPv6 DNS queries when executing simple commands such as those needed to mount a remote file system on a network server. Instead they only issue a standard IPv4 DNS query to start the operation. It will be some time before the common desktop and server operating systems use IPv6 and IPv4 equally.

This entire set of observations means that trouble shooting a dual stack network is going to be much more complicated than a pure IPv4 based network.

Literature research reveals that the vast majority of writers have concluded that the dual stack method of introducing IPv6 into the Internet and corporate networks is the best strategy. There is very little mention of implementing IPv6 to IPv4 gateways. There are many reasons given for not investing in any gateway work at all. In fact, the RFCs dealing with a gateway function seem to be relegated to the historical archives. Given that background, the SNL IPv6 test bed does not contain a gateway service, and it is composed completely of dual-stack network elements. More work is necessary to explore IPv6 to IPv4 tunneling as that function may play an important role in IPv6 deployment.

Application Testing

"IPv6 only" host application testing is very difficult to perform since end hosts typically implement both the IPv4 and IPv6 protocol stacks. However, the project team was able to disable IPv4 on some hosts to do some initial tests. A useful reference for examining IPv6 application issues is the website at URL: http://www.ipv6.org/v6-apps.html.

Testing applications against IPv6 reveals that most tested applications work. In particular SSH to a host only accessible via an IPv6 address works from both Windows XP and Linux hosts. SCP also seems to work from Windows XP to the IPv6 test host. However, Linux SCP does not seem to work when given an IPv6 address as the program interprets ":" as a delimiter. The "SCP –6" command option will enable SCP to use IPv6, but there is no way to use the address in place of the hostname. The syntax required is "SCP -6 filename user@host2:filename". Using IPv6 addresses instead of a host name is a burden and will lead to application difficulties. With a functional DNS server, some applications that cannot directly handle IPv6 addresses do work since hosts are referenced by DNS name instead of by address.

The reader is cautioned about reacting to strongly to application compatibility issues because the recommended method of phasing in IPv6 capabilities is through the "dual stack" approach discussed later in this paper. Suffice it to say this approach essentially eliminates all application compatibility issues.

IPV6 IN THE ASC WAN

Distance Computing, the former DisCom project, is a critical infrastructure aspect of the ASC program that makes resource-sharing possible. It allows users to use remote ASC resources as if they were local. The ASC WAN is currently connected as a full ring with links speeds of 10Gbps. As this new WAN will probably last five years, it has to be able to support IPv6. The ASC WAN is a currently envisioned as a private transit network with the Type 1 encryptors functioning as the demarcation point between the WAN and each of the laboratory internal networks. Therefore, there is a very limited set of network components that must be evaluated for IPv6 functionality. In particular, the systems of interest are the gateway routers at each laboratory site and the IP encryptors that form the demarcation point to each site.

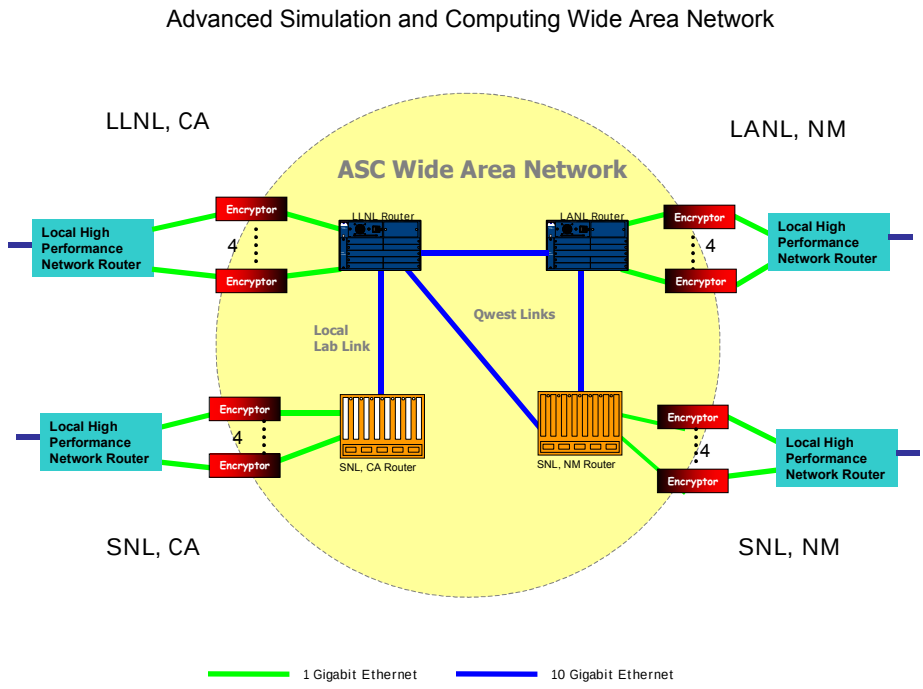

Figure 8: ASC WAN Design in 2007.

Initial evaluations indicate that the most problematic elements will be the encryptors. The routers are either IPv6 capable already or can be upgraded in a straightforward manner. The encryptor manufacturers have scheduled the IP encryptors for upgrade to be IPv6 capable in calendar year 2008.

Status of ASC WAN IPv6 Readiness

The 1Q2007 NIST draft generated an initial, common set of IPv6 requirements. The following bullets summarize the general node requirements from the NIST draft:

1. Network Management - For network management, all nodes must support a basic Simple Network Management Protocol (SNMP) capability and provide the basic IPv6 Management Information Base (MIB) specified in RFC4293. Routers, in addition, must support the Forwarding Table and Tunnel MIBs.

2. Multicast - Routers are required to be capable of discovering Multicast listeners – which may themselves be either Hosts or Routers, so RFC 3810 is mandated. In addition, MLD version 2 has extensions for Source Specific Multicast, encoded in RFC 4604

3. IPsec - Routers MUST implement RFC 3776 *Using IPsec to protect MIP signaling between Mobile Nodes and Home Agents*, if MIPv6 is implemented at all.

4. General – RFC 1981, 2460, 2461, 3315, 3971, 4443.

Since the NIST requirements are only in Draft stage, it is possible and likely that the list of requirements will change.

The project team conducted a review of the vendor's router documentation to determine if the ASC WAN routers meet the proposed NIST requirements. An online search from the Cisco site yielded the following URL:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d65ed.html.

Based on information contained in the URL above, it was discovered that a number of the NIST required RFCs are not currently listed in the Cisco URL. The correct train of images needs to be loaded on to the Cisco routers to provide IPv6 support. An inventory of the currently installed hardware needs to be completed.

For the Ericsson/Marconi BXR-5000, a review of the March 31, 2004, User Guide was conducted. The data sheet for the network processor blade (http://www.marconi.com/Home/customer_center/Products/Metro/Broadband%20Routing%20%26%20Switching/BXR5000) and the user guide listed IPv6 as supported, however, neither had a detail list of the supported RFCs.

The results of the comparison are listed later in this document. It appears that several areas of functionality will be non-compliant if the above RFCs are not implemented by the vendors. The functionality of immediate interest for ASC WAN would be IGP, IPv4 to IPv6 transitioning, IPv6 addressing, and Network Management.

The Type I encryptors are a class of equipment by themselves and the compliance schedule is in the hands of the vendors, General Dynamics and Level 3. Originally, General Dynamics' encryptors were scheduled to have IPv6 support by 4Q2006. The website GD4s.com currently has IPv6 listed as part of the 1Q2008 upgrade. Actual testing of the IPv6 capabilities of the ASC WAN will have to wait until the new encryptor upgrade becomes available.

ASC WAN IPv6 Implementation Plan Based on NIST Draft requirements

The following paragraphs describe a specific plan and timetable for implementing IPv6 in the ASC WAN. Implementing IPv6 in the ASC WAN means that issues must be handled and certain design decisions must be made. These issues and decisions are as follows.

ASC WAN IPv6 Addressing

Currently there is no procedure to obtain a provider independent (PI) IPv6 address block from the American Registry for Internet Numbers (ARIN). As long as the DisCom WAN remains isolated, the IPv6 addresses used can be a private address block. Therefore, RFC 4193 *Unique Local IPv6 Unicast Addresses* could be used for the ASC WAN instead of using an assigned a routable IPv6 prefix. If it becomes infeasible to use unique local addresses for the ASC WAN, the network will be renumbered with the appropriate IPv6.

ASC WAN IPv6 Routing

The ASC WAN currently has OSPFv2 deployed for IPv4. OSPFv3 would be deployed for IPv6. Some limited testing of OSPF3 has been done but it is not complete for all the ASC routers. The ASC WAN currently consists of four routers, two Cisco 6500 routers and two Ericsson BXR routers.

The NIST draft document [Ni] mandates that government IPv6 routers meet the following standards in addition to the general node requirements.

1. IGP - For Interior Routers, RFC 2740 OSPF is the mandatory routing protocol, and *RFC 4552 Authentication for OSPFv3* is strongly recommended.

2. EGP - For Exterior Routers, BGP MUST be supported. RFCs 4271, 1772, 2545 and 2858.

3. QOS - Quality of service support includes RFC 2474 *Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers*.

4. IPv4 to IPv6 transition - RFC 4213 *Basic Transition Mechanisms for IPv6 Hosts and Routers*. These mechanisms include Dual Stack, and Tunneling. The mechanisms mandated for United States Government Routers include Dual Stack IPv4-IPv6 and Configured Tunnels.

5. IPv6 addressing support - RFC 4291 *IP Version 6 Addressing Architecture,* with its scoping rules and its support for Unique Local Unicast addresses defined in RFC4007, and address source address selection rules defined in RFC3484.

Table 4 illustrates the comparison between the vendor documentation and the NIST requirements for a router node.

Table 4: Router Compliance with NIST Requirements.

RFC missing from vendor's compliance documentation		
Group	Cisco	Ericsson
IGP		NA
EGP	RFC 1772	RFC 1772
QOS	RFC 4271	NA
IPv4 to IPv6 transitioning	RFC 4213	NA
IPv6 addressing		NA
Network Management	RFC 4293	NA
Multicast	RFC 4604	NA
IPsec	RFC 3776	NA
General	RFC 3971	NA

NA – No information available from vendor documentation.

Risks

The Type 1 IPv6 support has already been delayed from 2006 to 2008. If its release is delayed past June 2008, it is unlikely that the ASC WAN would be able to meet the OMB mandate.

Ericsson support has been contacted in regards to a detailed list of supported IPv6 RFCs. To provide better IPv6 support, an Engineering version for the BXR-5000 is available. The timetable for the engineering sample to production code is not known at this time. A replacement of the BXR would have to be considered if full support of IPv6 is not part of the BXR-5000 roadmap.

Schedule

The implementation schedule will be driven by the availability of IPv6 for the Type I encryptor and for the Ericsson BXR-5000. This pushes the implementation of IPv6 on the ASC WAN to the first quarter 2008 at the earliest.

It is possible to enable IPv6 on the ASC WAN; however, due to available information for the BXR-5000 and Type 1 encryptors, IPv6 functionality may be limited.

Verifying ASC WAN IPv6 Implementation

IPv6 verification tests for the ASC WAN depend on the assumptions made regarding the architecture and usage of the WAN. If the WAN remains a private transit zone with the IP encryptors forming the functional demarcation points, some simple tests will suffice to prove that the WAN backbone can support IPv6 traffic. Both black side (cipher text) and red side (clear text) tests should be run to validate IPv6 functionality.

First, hosts connected to the cipher text side of routers can be configured to pass IPv6 traffic to each other across the WAN. Black side test hosts are currently installed at each ASC WAN laboratory site and used to verify network performance. In addition, laboratory tests have shown that the Iperf test software, which has been used to test WAN performance, will accept IPv6 addresses and pass packets across an IPv6 infrastructure. Using the same tests as used in the past

allows us to verify that IPv6 data streams are forwarded at the same performance levels as with IPv4 streams. Successfully executing these stream tests will verify the IPv6 capabilities of the ASC WAN network routers.

Once the required IPv6 upgrades are made to the ASC WAN encryptors, SNL can test IPv6 encryptor performance in a laboratory setting. This testing can be performed relatively easily; however, the defining tests must be performed between classified, laboratory networks. These tests will not be as straightforward as the black side or laboratory tests since we do not have access to IPv6 capable resources in the ASC high performance computing environments. Reconfiguring ASC valuable resources is not a viable testing scenario so we may not run full system tests for some time.

IMPLEMENTING IPV6 IN THE SNL ENTERPRISE

SNL Environments

SNL enterprise computing primarily takes place in three separate realms, the open network (SON), the restricted network (SRN), and the classified network (SCN). Each of these environments has an identifiable network core comprised of a set of routers. The SCN is operated under a strict set of rules because of the need to process classified information. That network will not be modified to carry IPv6 until requirements warrant the lengthy process necessary to modify the basic operating practices of the network. OMB dictates are insufficient reason to modify the SCN.

The SON on the other hand represents less than 10% of SNL network connectivity; therefore, a major redesign of the environment is not beneficial to the laboratories. The SRN supports the majority of hosts with approximately 20,000 connected systems. Implementing IPv6 in the SRN SNL/NM core should demonstrate compliance with the OMB directive. Unfortunately, this will be more difficult than the ASC WAN implementation since, to be truly functional, some minimal set of IPv6 network services, for example DNS and DHCPv6, will have to be installed.

Network Hardware Costs Estimates to Support IPv6

To generate a cost estimate to support IPv6, the project team only considered the SRN and the SON in New Mexico. The Foundry routers in the SCN at SNL/NM and the routers in all environments at SNL/CA are already capable of supporting IPv6. Likewise, the network equipment at SNL/CA is also IPv6 ready. The project team collected network equipment information by two methods to evaluate equipment readiness. The first method used the Cisco IPv6 Capability Scorecard ® software product. The second method relied on the DRIFT network mapping software to retrieve equipment information for the SRN core and distribution routers.

After examining the status of the routers currently deployed in the SON and SRN at SNL/NM, one can determine the hardware upgrades necessary to support IPv6. The upgrades fall into two groups; the Cisco 6500 routers which form the nucleus for routing in the two environments and the heterogeneous group of other Cisco routers which support special configurations such as remote links. Largely, the Cisco 6500 systems can be upgraded while the others must be

replaced. For the SNL/NM SON and SRN combined, there are 31 routers in the heterogeneous group and 15 core and distribution routers that SNL must upgrade or replace.

The SNL/NM SON and SRN together have at least 31 small routers that cannot be upgraded to support IPv6; they must be replaced. Replacing those units with a newer Cisco model such as the 3750 would cost an average of about $10,000 each. Therefore the total cost would be about $310,000.

For our Cisco 6500 routers, we must upgrade to IOS 12.4. About two thirds of the Cisco 6500 routers, about 15 (see Table 5 for the SRN) have Supervisor 2 cards. These routers must be upgraded to use the Supervisor 720 cards to support IPv6. To replace the supervisory cards in these routers, we will also need to upgrade fan units, power supplies, and other ancillary equipment at a cost of about $50,000 each for a total of $750,000.

Summary

- Upgrading 31 small routers to Cisco 3750 models at an average cost of $10,000 each would cost about $310,000
- Upgrading the SUP2 based routers to SUP720 based systems means that the fan units, power supplies, and any other incompatible cards would also have to be upgraded. The cost for each system is estimated to average about $50,000 each. Total cost for all 15 $750,000

Estimated Network Hardware Cost ~ $1,060,000.

In addition to the network hardware costs, SNL should also consider the manpower costs to upgrade the network hardware and software, configure and test the new IPv6 capabilities, and install the new IPv6 configurations in the production networks. It is inevitable that the tasks required to upgrade the IT infrastructure to IPv6 will be a burden to the staff and strain limited resources.

Other IPv6 Costs

Other IT groups and activities will incur costs to upgrade the IT infrastructure to IPv6. Those groups and activities include;

- Network services such as DNS and DHCP
- Corporate server platforms
- Network security

  Cost estimates for upgrading the wired network Intrusion Detection System (IDS) is $250K for the sensor hardware and $50K for vulnerability testing.
- Cyber Enterprise Management
- Network analysis and troubleshooting
- NWIS

CONCLUSIONS AND RECOMMENDATIONS

The most straightforward way of incorporating IPv6 into the SNL network environment is the so-called “dual stack approach”. Using the dual stack approach means that each network host,

network service, and network router is configured to support both IPv4 and IPv6 simultaneously. Such a strategy leads to the least negative impact on customers or applications.

Our initial testing and literature search lead to the conclusion that there will be no identifiable migration to IPv6 as one usually thinks of timely changeovers between technologies. Rather, there will be a long, maybe a decade or so, of coexistence where both IPv4 and IPv6 are present in network elements, network services, and host systems. There may be no defining point where IPv6 "takes over" and IPv4 is turned off.

However, to prepare for this time of coexistence, SNL should mandate that all network equipment purchases be certified as IPv6 capable. Our goal should be to position SNL so that there are no additional required equipment costs to provide IPv6 capability in the network backbones.

Recommended Actions

Define What "Support IPv6 in the Network Backbones" Means to SNL

It will be necessary to consider each SNL network environment separately when evaluating the readiness to support IPv6. SNL can use the following suggested definition of support for IPv6 in the backbone as a straw man for discussion purposes.

1. IPv6 backbone support implies that properly formed IPv6 packets are successfully delivered from the sending host to the proper destination host across the enterprise backbone.
2. An IPv6 operational DNS server is available that is capable of functioning using IPv6 packets only.
3. Backbone routers provide the minimal required network services for supporting IPv6. That is they provide prefix advertisement and DNS address advertisement.

Continue the Development Plan to Prepare SNL Network Elements for IPv6

Create a Schedule for IPv6 Implementation on the SNL Corporate Backbones

Issues to Resolve

The following list of IPv6 issues is not claimed to be complete nor are the issues listed in order of importance. Issues to resolve include decisions that must be made but also patterns of thinking that may have to change as SNL implements IPv6 on the corporate backbones.

Multiple Addresses per Host Interface

Refer to IPv6 privacy RFC.

Dynamic IPv6 DNS Updates

Refer to DNS Security or DNSSEC.

IPv6 Compatibility with Corporate Information Systems (NWIS)

NWIS needs additional code to handle IPv6 addressing. The project group submitted a formal request in February, 2007 to the NWIS project lead to modify NWIS to support IPv6; however, the modification is scheduled as part of the 1Q2008 development cycle.

Ipv6 Impact on Network Security Processes and Practices

Availability of IPv6 Capable Network Test Equipment and Trouble Shooting Support

REFERENCES

[COM] *"Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)"*, U.S. Department of Commerce, National Institutes of Standards and Technology, National Telecommunications and Information Administration, January 2006.

[DOE] *"Acquiring Information Technology—Requirement to Comply With Internet Protocol Version 6 (IPv6)"*, United States. Department of Energy Acquisition Letter AL-2006-04, December 14, 2005.

[Ev] Evans, Karen S. (Administrator Office of E-Government and Information Technology), "*MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS, Transition Planning for Internet Protocol Version 6 (IPv6),"* United States. Office of Management and Budget, Memorandum M-05-22, August 2, 2005.

[Ni] Nightingale, Stephen, et al., *"A Profile for IPv6 in the U.S. Government – Version 1.0*", National Institute of Standards and Technology, Special Publication 500-267(Draft), January 31, 2007. (http://www.antd.nist.gov/usgv6-v1-draft.pdf.)

[Ri] Rios, Mike, Archuleta, Thomas, *"SNL/NM SRN IPv6 Capability Scorecard,"* February, 9. 2007.

BIBLIOGRAPHY

For the reader that wants to delve deeper into the world of IPv6 deployment we have included the following bibliography of selected readings.

1. "An IPv6 deployment Guide" editor: Martin Dunmore, http://www.6net.org/
2. "Final IPv4 to IPv6 Transition Cookbook for End Site Networks/Universities", http://www.6net.org/
3. "Understanding IPv6" Joseph Davies, Microsoft Press, 2003,
4. "The Evolution of the Internet and IPv6", Geoff Huston, Australian IPv6 Summit, 31 October 2005, http://www.apnic.net/community/presentations/ipv6.html
5. DNS Extensions to support IP version 6 (RFC 1886).
6. IP Version 6 Addressing Architecture (RFC 1884) made obsolete by RFC 2373
7. An Architecture for IPv6 Unicast Address Allocation (RFC 1887)
8. Internet Protocol, Version 6 (IPv6) Specification (RFC 1883) made obsolete by RFC 2460/ updated by RFC 2147
9. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) (RFC 1885) made obsolete by RFC 2463
10. IPv6 Testing Address Allocation (RFC 1897) made obsolete by RFC 2471
11. Path MTU Discovery for IP version 6 (RFC 1981)
12. OSI NSAPs and IPv6 (RFC 1888)
13. A Method for the Transmission of IPv6 Packets over Ethernet Networks (RFC 1972) made obsolete by RFC 2464
14. Neighbor Discovery for IP Version 6 (IPv6) (RFC 1970) made obsolete by RFC 2461
15. Transmission of IPv6 Packets Over FDDI (RFC 2019) made obsolete by RFC 2467
16. IP Version 6 over PPP (RFC 2023) made obsolete by RFC 2472
17. An IPv6 Provider-Based Unicast Address Format (RFC 2073) made obsolete by RFC 2374
18. Basic Socket Interface Extensions for IPv6 (RFC 2133) made obsolete by RFC 2553
19. TCP and UDP over IPv6 Jumbograms (RFC 2147) made obsolete by RFC 2675/ updates RFC 1883
20. Advanced Sockets API for IPv6 (RFC 2292) made obsolete by RFC 3542
21. IPv6 Multicast Address Assignments (RFC 2375)
22. An IPv6 Aggregatable Global Unicast Address Format (RFC 2374) obsoletes RFC 2073/ made obsolete by RFC 3587
23. IP Version 6 Addressing Architecture (RFC 2373) obsoletes RFC 1884/ made obsolete by RFC 3513
24. Neighbor Discovery for IP Version 6 (IPv6) (RFC 2461) obsoletes RFC 1970/ updated by RFC 4311
25. IPv6 Stateless Address Autoconfiguration (RFC 2462) obsoletes RFC 1971
26. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (RFC 2463) obsoletes RFC 1885
27. Transmission of IPv6 Packets over Ethernet Networks (RFC 2464) obsoletes RFC 1972
28. IPv6 Testing Address Allocation (RFC 2471) obsoletes RFC 1897/ made obsolete by RFC 3701
29. Transmission of IPv6 Packets over Token Ring Networks (RFC 2470)

30. Transmission of IPv6 Packets over FDDI Networks (RFC 2467) obsoletes RFC 2019
31. Proposed TLA and NLA Assignment Rules (RFC 2450)
32. Management Information Base for IP Version 6: ICMPv6 Group (RFC 2466)
33. Management Information Base for IP Version 6: Textual Conventions and General Group (RFC 2465)
34. IP Version 6 Management Information Base for the User Datagram Protocol (RFC 2454) made obsolete by RFC 4113
35. IP Version 6 Management Information Base for the Transmission Control Protocol (RFC 2452) made obsolete by RFC 4022
36. Internet Protocol, Version 6 (IPv6) Specification (RFC 2460) obsoletes RFC 1883
37. IP Version 6 over PPP (RFC 2472) obsoletes RFC 2023
38. Generic Packet Tunneling in IPv6 Specification (RFC 2473)
39. Transmission of IPv6 Packets over ARCnet Networks (RFC 2497)
40. IP Header Compression (RFC 2507)
41. Reserved IPv6 Subnet Anycast Addresses (RFC 2526)
42. Transmission of IPv6 over IPv4 Domains without Explicit Tunnels (RFC 2529)
43. Basic Socket Interface Extensions for IPv6 (RFC 2553) obsoletes RFC 2133/ made obsolete by RFC 3493
44. IPv6 Jumbograms (RFC 2675) obsoletes RFC 2147
45. Multicast Listener Discovery (MLD) for IPv6 (RFC 2710) updated by RFC 3590,RFC 3810
46. IPv6 Router Alert Option (RFC 2711)
47. Format for Literal IPv6 Addresses in URL's (RFC 2732) made obsolete by RFC 3986
48. DNS Extensions to Support IPv6 Address Aggregation and Renumbering (RFC 2874) updated by RFC 3152,RFC 3226,RFC 3363,RFC 3364
49. Router Renumbering for IPv6 (RFC 2894)
50. Initial IPv6 Sub-TLA ID Assignments (RFC 2928)
51. Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (RFC 3041)
52. IP Version 6 Management Information Base for the Multicast Listener Discovery Protocol (RFC 3019)
53. Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification (RFC 3122)
54. IPv6 multihoming support at site exit routers (RFC 3178)
55. Transmission of IPv6 Packets over IEEE 1394 Networks (RFC 3146)
56. Unicast-Prefix-based IPv6 Multicast Addresses (RFC 3306) updated by RFC 3956
57. Recommendations for IPv6 in 3GPP Standards (RFC 3314)
58. Default Address Selection for Internet Protocol version 6 (IPv6) (RFC 3484)
59. Basic Socket Interface Extensions for IPv6 (RFC 3493) obsoletes RFC 2553
60. IP Version 6 Addressing Architecture (RFC 3513) obsoletes RFC 2373/ made obsolete by RFC 4291
61. A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block (RFC 3531)
62. IPv6 for Some Second and Third Generation Cellular Hosts (RFC 3316)
63. Advanced Sockets Application Program Interface (API) for IPv6 (RFC 3542) obsoletes RFC 2292
64. IPv6 Global Unicast Address Format (RFC 3587) obsoletes RFC 2374
65. IPv6 Flow Label Specification (RFC 3697)

66. Requirements for IPv6 prefix delegation (RFC 3769)
67. Deprecating Site Local Addresses (RFC 3879)
68. Management Information Base for the Transmission Control Protocol (TCP) (RFC 4022) obsoletes RFC 2012,RFC 2452
69. IPv6 Scoped Address Architecture (RFC 4007) IP Tunnel MIB (RFC 4087) obsoletes RFC 2667
70. Management Information Base for the User Datagram Protocol (UDP) (RFC 4113) obsoletes RFC 2013,RFC 2454
71. Unique Local IPv6 Unicast Addresses (RFC 4193)
72. Default Router Preferences and More-Specific Routes (RFC 4191) IPv6 Host-to-Router Load Sharing (RFC 4311) updates RFC 2461
73. IP Version 6 Addressing Architecture (RFC 4291) obsoletes RFC 3513
74. NTP References:
    http://support.ntp.org/bin/view/Support/WebHome
    http://lists.ntp.isc.org/pipermail/questions/2003-August/000273.html
    http://tldp.org/LDP/sag/html/ntp-toolkit.html
    http://tldp.org/HOWTO/Linux+IPv6-HOWTO/
    http://technet2.microsoft.com/WindowsVista/en/library/43cda695-3113-4cff-a24a-f2ccca6ca4141033.mspx?mfr=true

APPENDIX A: NETWORK DEVICE SURVEY RESULTS

SRN Core and Distribution Router Status

We were able to use the DRIFT software to query the SRN core and distribution routers for equipment configuration. Based on this query and the Cisco 6500 router reliance on the Supervisor Engine 720 to support IPv6, we were able to identify routers that currently support IPv6. SRN router status is listed in Table 5.

Table 5: Survey of SRN Core and Distribution Router Readiness.

Node Name	Vendor	Node Type	Software Version	Chassis Serial Number	Module Model	Module Description	IPv6 Ready
SACR2197(897/MDR)	Cisco Systems	Cisco C6509	12.1(20)E3	SMG0615A033	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2191(891/MDR)	Cisco Systems	Cisco C6509	12.2(18)SXF7	SCA050703KD	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2190(880/MDC)	Cisco Systems	Cisco C6509	12.2(18)SXF7	SAL082807KX	WS-SUP720-3B	Supervisor Engine 720 (Hot)	YES
SACR2185(880/X53)	Cisco Systems	Cisco C6513	12.2(18)SXF7	TBA05250780	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2180(880/MDC)	Cisco Systems	Cisco C6509	12.2(18)SXF7	SMG1017NGK7	WS-SUP720-3B	Supervisor Engine 720	YES
SACR2166(880SWIDR)	Cisco Systems	Cisco C6509	12.1(20)E3	SCA031300VK	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2160(960/MDR)	Cisco Systems	Cisco C6509	12.1(20)E3	TBA05391021	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2136(836/MDR)	Cisco Systems	Cisco C6509	12.2(18)SXF7	SCA050305YD	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2135(6585/MDR)	Cisco Systems	Cisco C6509	12.1(20)E3	SCA042303DV	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2121(821/MDR)	Cisco Systems	Cisco C6509	12.2(18)SXF7	SCA041201B4	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2107(807/MDR)	Cisco Systems	Cisco C6509	12.1(20)E3	TBA05310367	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2102(802/MDR)	Cisco Systems	Cisco C6509	12.2(18)SXF7	SCA043001JY	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2085(880/X53)	Cisco Systems	Cisco C6513	12.2(18)SXF7	TBA05250119	WS-SUP720-3B	Supervisor Engine 720	YES
SACR2080(880/MDC)	Cisco Systems	Cisco C6509	12.2(18)SXF7	SAL0730H9BP	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2064(6584/MDR)	Cisco Systems	Cisco C6509	12.1(20)E3	SCA045101Z0	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2055(858/MDR)	Cisco Systems	Cisco C6509	12.2(18)SXF	SAL08394HUP	WS-SUP720-3B	Supervisor Engine 720	YES
SACR2038(880/230)	Cisco Systems	Cisco C6513	12.2(18)SXF7	TBM06112328	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO
SACR2001(880/MDC)	Cisco Systems	Cisco C6509	12.2(18)SXF7	TBA05301601	WS-SUP720-3B	Supervisor Engine 720	YES
SACR0006(880/MDC)	Cisco Systems	c6sup2_rp-JK2SV-M	12.1(20)E3	TSC07080027	WS-X6K-S2U-MSFC2	Catalyst 6000 supervisor 2	NO

SNL/NM SRN, IPv6 Capability Scorecard Results

In February/March, 2007, Mike Rios and Thomas Archuleta (Cisco representative) used the Cisco IPv6 Capability Scorecard® to scan the SRN network equipment. The results of that evaluation are given below. The software scanned all SRN devices, both the switches and routers. It identifies a number of devices that are not IPv6 capable. In many cases these devices are network switches that are able to transport IPv6 traffic, but are not necessarily cable of management via IPv6. For the purposes of this study, we consider that the deployed switches are sufficient to meet SNL's IPv6 requirements.

IPv6 Scorecard
Cisco IPv6 scorecards are designed to provide a summary on the network device capability to support IPv6. This combined router and LAN switch IPv6 scorecard identifies and polls selected devices and collects basic data, which then indicates the capability to support IPv6. The scorecard examines Cisco IOS® based routers and Catalyst® Operating System (CatOS) and IOS® based switches, and provides a summary of the devices. If more in-depth device evaluation is required, Cisco Advanced services offer an IPv6 Capability assessment which provides device specific information and recommendations.

The IPv6 scorecard examines hardware running Cisco IOS and CatOS. Results are organized into three major summary categories:

(a) The device is capable of supporting IPv6 features; hardware and/or software upgrades may be required
(b) The device is not capable of supporting IPv6 services
(c) The analysis was unable to determine the device's capability to support IPv6; further analysis is required

The resulting data is correlated and presented in a table format to provide **SNL/NM SRN** an overview at the ability to provide IPv6 services on the **SNL/NM SRN** network.

Note from the Auditors
This IPv6 Scorecard for **SNL/NM SRN** has been performed in one of two ways 1) using the Cisco IPv6 Network Assessor or 2) using a file extracted from CiscoWorks
The primary objective of the scorecard is to gather summary information related to the capabilities of the **SNL/NM SRN** Cisco router and switch network to support IPv6 services. This information will be used as the basis for to provide high level recommendations on issues such as software versions and hardware platforms that will require an upgrade in order to be considered IPv6 compatible. Cisco Advanced Services can provide recommendations regarding best practices that can be implemented to help ensure a smooth transition to IPv6 technology as well as conduct further assessments if necessary.

Overall Scorecard Summary
The Scorecard results have identified several areas that require attention in order for the **SNL/NM SRN** network to provide IPv6 based services across their environment. This section

summarizes the findings.

Of the **437** devices:

Category	Device Count	% of Total Count
1. IPv6 Capable (May Require Upgrades)	**216**	**49.43%**
2. NOT IPv6 Capable	**220**	**50.34%**
3. Further Analysis Required	**1**	**0.23%**
TOTAL	**437**	**100.00%**

Device Summary

Device models marked in **red** on the summary table will not support IPv6. Currently there are **220** devices that will not support IPv6. These currently installed platforms will require replacement with newer hardware in order to support IPv6.

SRN/NM Device Summary

Model	Device Type	Device Count	% of Total Count
[UNKNOWN]		1	0.23%
3550 24 FX SMI	S	13	2.97%
6509 IOS	S	27	6.18%
CATALYST297024	S	2	0.46%
CATALYST356024	S	2	0.46%
CATALYST3560G2	S	5	1.14%
CATALYST3560G2	S	1	0.23%
CATALYST3560G4	S	2	0.46%
CATALYST3560G4	S	2	0.46%
CISCO 2950G 12 EI	S	1	0.23%
CISCO 2950G 48 EI	S	33	7.55%
CISCO 2950T 24	S	31	7.09%
CISCO 3550	S	1	0.23%
CISCO 3550 12G	S	2	0.46%
CISCO 3725	R	8	1.83%
CISCO CATALYST	S	6	1.37%
CISCO3825	R	4	0.92%
CISCO7140	R	1	0.23%
ROUTER 3640	R	1	0.23%
ROUTER 7206VXR	R	3	0.69%
VPNCONCENTRA		1	0.23%
WS-C2912MF-XL	S	2	0.46%
WS-C2948	S	33	7.55%
WS-C2950C-24	S	46	10.53%
WS-C2950G-24	S	14	3.20%
WS-C3508G-XL	S	1	0.23%
WS-C5000	S	6	1.37%
WS-C5500	S	20	4.58%
WS-C5505	S	6	1.37%
WS-C5509	S	7	1.60%
WS-C6006	S	5	1.14%
WS-C6506	S	45	10.30%
WS-C6509	S	64	14.65%
WS-C6513	S	41	9.38%
TOTAL:		437	100.00%

Obsolete Network Devices in the SON and SRN,

Internet Protocol version 6 (IPv6)

Two trends are clear in Telecommunications, IPv6 and VoIP. Each will be covered in greater detail in this release of the document.

IPv6 makes available trillions of new IP addresses, and it enables better address allocation, address aggregation, and features that provide significantly greater end-to-end connectivity and services.

There are three reasons for IPv6. 1) The world is running out of IPv4 addresses. 2) Many devices communicating with different protocols in the past are becoming IP-capable today (e.g. sensors, detectors, monitors, surveillance cameras, etc.). 3) The U.S. Government's Office of Management and Budget has mandated all civilian agencies add IPv6 to their network backbones by June, 2008 (see link in References section).

The obsolete hardware and software does not support IPv6. Not all NOSes on current obsolete hardware support IPv6. All NOS upgrades for core and distribution layer devices are covered under the maintenance contract. All NOS upgrades for access layer devices will need to be purchased because these devices are self-insured. Due to the lack of other protocols and services, the recommended path is replacement. The details for an IPv6 upgrade appear in Tables 13 and 14.

Table 6: IPv6 Upgrade Path for Switches

Model	Upgrade to …			
	Model	Flash	RAM	Min. IOS
Small Switches				
2912MF-XL	C3750-24FS-S	32/16	128	12.2(25)SEE
2948G	C3560G-48PS-S	32/16	128	12.2(25)SEE
2950C-24	C3560G-24TS-S	32/16	128	12.2(25)SEE
	C3560G-24PS-S	32/16	128	12.2(25)SEE
2950T-24	C3560G-24PS-S	32/16	128	12.2(25)SEE
2950G-12				
2950G-24				
2950G-48	C3560G-48PS-S	32/16	128	12.2(25)SEE
2970G-24	C3560G-24PS-S	32/16	128	12.2(25)SEE
3508-GL	C3750G-12S	16/16	128	12.2(25)SEE
3524-PWR	C3560G-24PS-S	32/16	128	12.2(25)SEE
3550-12G	C3750G-12S	16/16	128	12.2(25)SEE
3550-24	C3560G-24PS-S	32/16	128	12.2(25)SEE
3550-24FX	C3750-24FS-S	32/16	128	12.2(25)SEE
3550-24PWR	C3560G-24PS-S	32/16	128	12.2(25)SEE
3550-48PWR	C3560G-48PS-S	32/16	128	12.2(25)SEE
3560G-24TS		32	128	12.2(25)SEE
3560G-48TS		32	128	
3560-24PS		16	128	
Large Switches				

5500 Series				
5009 (Sup I)	WS-C6506-E, WS-C6509-E, Sup32-GE-3B	256/64	512	12.2(18)SXF4
5506 (Sup IIG)				
5509 (Sup II)				
5530 (Sup III)				
6500 Series	Su			
X6K-Sup1A-2GE	X6K-Sup32 X6K-Sup32-MSFC2A	256/64	512	12.2(18)SXF4
X6K-SUP2-2GE				
X6K-S2U-MSFC2	X6K-Sup720-3B			
F6K-MFSC	See X6K-Sup1A-2GE			
F6K-MFC2				
Sup720 w/ MSFC3	WS-CF-UPG=	512/64	512	12.2(18)SXF4
Sup32-10GE-3B		256/64	512	12.2(18)SXF4
Sup32-3B		256/64	512	12.2(18)SXF4

Table 7: IPv6 Upgrade Path for Routers

Model	Upgrade to (min.) …			
	Model	Flash	RAM	IOS
Small Routers				
2500	3825-SEC/K9 ($6831.17)	64	256	12.4(03) (Adv. Sec.)
2507				
3640	3825-SEC/K9 ($6831.17)	64	256	12.4(03) (Adv. Sec.)
3725				
Large Routers				
7000	7204VXR	48	256	12.4(04)XD
7140	7204VXR	48	256	12.4(04)XD
NPE-400 (7204)	7206VXR-NPR-G2	48	256	12.4(04)XD

None of the network devices that have reached end-of-life status will ever support the features listed in Table 12. By replacing the obsolete hardware to support IPv6, all the features in Table 12 will be included in the IOS release for each replacement model. The replacement hardware will support all the features listed in Table 12.

SNL/NM Network Devices Survey (Feb/March 2007)
SNL/NM Network device configuration tables are based on data supplied by Joseph Maestas.

SON SNL/NM Device and Vendor Summary (System Object ID)

Vendor	Chassis	Total	Percentage(%)
Cisco Systems		119	75.3
	Cisco 2501	1	0.6
	Cisco 2507	1	0.6
	Cisco 3550-24-PWR	1	0.6
	Cisco 3725	5	3.1
	Cisco 7507	2	1.2
	Cisco C2950C-24	42	26.5
	Cisco C2950G-12	5	3.1
	Cisco C2950G-24	4	2.5
	Cisco C2950G-48	11	6.9
	Cisco C2950T-24	13	8.2
	Cisco C3524T-PWR-XL	1	0.6
	Cisco C3550-24	2	1.2
	Cisco C3550-24MMF	11	6.9
	Cisco C356024-PS	16	10.1
	Cisco C6509	3	1.8
	Unknown	1	0.6
Cisco Systems		39	24.6
	Cisco WS-C2948G	8	5
	Cisco WS-C5000	10	6.3
	Cisco WS-C5500	1	0.6
	Cisco WS-C5505	6	3.7
	Cisco WS-C5509	1	0.6
	Cisco WS-C6506	2	1.2
	Cisco WS-C6509	10	6.3
	Cisco WS-C6513	1	0.6

Vendor	Node Type	Software Version	Supervisor	DRAM/Flash	Minimum Enterprise IOS	DRAM Need	Flash
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/32	12.2.17d-SXB11 or 12.2.18-	No (256)	Yes (64)
Cisco	Cisco C6509	12.2(17d)SXB10	Supervisor Engine	512/64	12.4, 12.2.17d-SXB11	No (256)	No (64)
Cisco	Cisco 7507	12.1(19)		256/16	REPLACE SYSTEM		
Cisco	Cisco 7507	12.1(19)		256/16	REPLACE SYSTEM		
Cisco	Cisco 3725	12.3(5b)		128/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.3(5b)		128/32	REPLACE SYSTEM		
Cisco	Cisco 2501	11.2(5)		16/8	REPLACE SYSTEM		
Cisco	Cisco 2507	11.2(16)		64/16	REPLACE SYSTEM		
Cisco	Cisco 3725	12.3(5b)		128/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.3(5b)		128/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.3(5b)		128/32	REPLACE SYSTEM		

SRN SNL/NM Device and Vendor Summary (System Object ID)

Vendor	Chassis	Total	Percentage(%)
Cisco Systems		216	46.5
	.1.3.6.1.4.1.9.1.615	1	0.2
	.1.3.6.1.4.1.9.1.617	2	0.4
	Cisco 3640	2	0.4
	Cisco 3725	11	2.3
	Cisco 7140 (2-FE)	2	0.4
	Cisco 7206 VXR	3	0.6
	Cisco 7507	2	0.4
	Cisco C2912MF-XL	2	0.4
	Cisco C2950C-24	45	9.6
	Cisco C2950G-12	4	0.8
	Cisco C2950G-24	14	3
	Cisco C2950G-48	39	8.4
	Cisco C2950T-24	33	7.1
	Cisco C2970-24TS	3	0.6
	Cisco C3508G-XL	1	0.2
	Cisco C3550-12G	2	0.4
	Cisco C3550-24MMF	11	2.3
	Cisco C3550-48	1	0.2
	Cisco C6000 MSFC	1	0.2
	Cisco C6509	21	4.5
	Cisco C6513	5	1
	Cisco C8540MSR	1	0.2
	Cisco LS1010	2	0.4
	Unknown	8	1.7
Cisco Systems		234	50.4
	Cisco WS-C2948G	35	7.5
	Cisco WS-C5000	23	4.9
	Cisco WS-C5500	29	6.2
	Cisco WS-C5505	9	1.9
	Cisco WS-C5509	9	1.9
	Cisco WS-C6006	5	1
	Cisco WS-C6506	23	4.9
	Cisco WS-C6509	56	12
	Cisco WS-C6513	42	9
	Unknown	3	0.6
Cisco		3	0.6
	Cisco-Altiga's VPN	3	0.6
Foundry		11	2.3
	.1.3.6.1.4.1.1991.1.3.32.2	10	2.1
	Foundry BigIron 15000	1	0.2

SRN SNL/NM Router Summary

Vendor	Node Type	Software Version	Supervisor	DRAM/Flash (MB)	Minimum Enterprise IOS version for IPv6	DRAM Need Upgrade	Flash Need Upgrade
Cisco	c6sup2_rp-	12.1(20)E3	Supervisor 2	256/32	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6513	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/32	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/32	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6513	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco	Cisco 7206 VXR	12.3(3b)	Supervisor 2	128/8	REPLACE SYSTEM		
Cisco	Cisco C6509	12.2(18)SXF	Supervisor	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco	Cisco C6509	12.2(18)SXF	Supervisor	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco	Cisco C6513	12.2(18)SXF	Supervisor	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco	Cisco C6509	12.2(18)SXF	Supervisor	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco	Cisco C6509	12.2(18)SXF	Supervisor	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco	Cisco C6513	12.2(18)SXF	Supervisor	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco	Cisco 7507	12.0(9)		256/16			
Cisco	Cisco C6000	12.1(6)E1		128/16	REPLACE SYSTEM		
Cisco	Cisco 7507	12.1(19)		64/16	REPLACE SYSTEM		
Cisco	Cisco 7140 (2-	12.1(9)E		256/8	REPLACE SYSTEM		
Cisco	Cisco 7206 VXR	12.2(15)T8		256/8	REPLACE SYSTEM		
Cisco	RSP-JSV-M	12.1(19)		256/16	REPLACE SYSTEM		
Cisco	Cisco 3640	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.2(15)T8		120/32	REPLACE SYSTEM		
Cisco	Cisco 7206 VXR	12.2(15)T8		256/8	REPLACE SYSTEM		
Cisco	Cisco 3725	12.2(15)T8		256/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.2(15)T8		120/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.3(17a)		252/32	REPLACE SYSTEM		
Cisco	Cisco 7140 (2-	12.2(15)T8		328/8	REPLACE SYSTEM		
Cisco	Cisco 3725	12.2(15)T8		252/32	REPLACE SYSTEM		
Cisco	Cisco 3640	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.2(15)T8		120/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco	C3725-IK9S-M	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco	Cisco 3725	12.2(15)T8		128/32	REPLACE SYSTEM		

SCN Device and Vendor Summary (System Description)

Vendor	Chassis	Total	Percentage(%)
Cisco		29	10.2
	C2950-I6Q4L2-M	3	1
	C3550-I5Q3L2-M	1	0.3
	C3550-I9Q3L2-M	7	2.4
	C5RSM-ISV-M	1	0.3
	c6sup2_rp-JK2SV-M	1	0.3
	c6sup2_rp-JSV-M	13	4.5
	c6sup2_rp-PSV-M	1	0.3
	LS1010-WP-M	1	0.3
	RSP-JSV-M	1	0.3
Cisco		50	17.6
	WS-C2948	9	3.1
	WS-C5500	5	1.7
	WS-C5505	16	5.6
	WS-C5509	4	1.4
	WS-C6506	5	1.7
	WS-C6509	4	1.4
	WS-C6513	7	2.4
Foundry		205	72.1
	Unknown Chassis	205	72.1

APPENDIX B: CISCO ROUTER – IOS FEATURES AND RELEASES

Later versions of code than the identified version below may require more flash and main memory. The table below shows which releases provide support for the indicated features.

Feature	12.0S Release	12.*x*T Release	12.2S Release	12.3 Release	12.4 Release
IPv6	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 address types: Unicast	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6: ICMPv6	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6: IPv6 neighbor discovery	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6: IPv6 stateless autoconfiguration	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6: IPv6 MTU path discovery	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6: ICMPv6 redirect	12.0(22)S	12.2(4)T	12.2(14)S	12.3	12.4
IPv6: neighbor discovery duplicate address detection	12.0(22)S	12.2(4)T	12.2(14)S	12.3	12.4
IPv6: IPv6 static cache entry for neighbor discovery	12.0(22)S	12.2(8)T	12.2(14)S	12.3	12.4
IPv6 address types: Anycast	—	—	12.2(25)S	—	12.4
IPv6: NetFlow for IPv6	—	12.3(7)T	—	—	12.4
IPv6: Mobile IPv6 home agent	—	12.3(14)T	—	—	12.4
IPv6: IPv6 default router preference	—	12.4(2)T	—	—	—
IPv6: IPv6 ACL extensions for Mobile IPv6	—	12.4(2)T	—	—	—
IPv6: IP Receive ACL for IPv6 traffic	12.0(32)S	—	—	—	—
IPv6: HSRP for IPv6	—	12.4(4)T	—	—	—
IPv6: syslog over IPv6	—	12.4(4)T	—	—	—
IPv6 routing: FHRP - GLBP support for IPv6	—	12.4(6)T	—	—	—
IPv6 Switching Services					
IPv6 switching: automatic 6to4 tunnels	12.0(22)S [1]	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 switching: CEF/dCEF support	12.0(22)S	12.2(13)T	12.2(14)S	12.3	12.4
IPv6 switching: CEFv6 switched configured IPv6 over IPv4 tunnels	—	12.2(13)T	12.2(14)S	—	12.4
IPv6 switching: provider edge router over MPLS (6PE)[2 3]	12.0(22)S	12.2(15)T	12.2(14)S	12.3	12.4
IPv6 switching: CEFv6 switched ISATAP tunnels	—	12.3(2)T	12.2(14)S	—	12.4
IPv6 switching: CEFv6 switched automatic IPv4-compatible tunnels	—	12.3(2)T	12.2(14)S	—	12.4
IPv6 Routing					
IPv6 routing: RIP for IPv6 (RIPng)	12.0(22)S	12.2(2)T [4]	12.2(14)S	12.3	12.4
IPv6 routing: static routing	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 routing: route redistribution	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 routing: multiprotocol	12.0(22)S	12.2(2)T [5]	12.2(14)S	12.3	12.4

Feature	12.0S Release	12.*x*T Release	12.2S Release	12.3 Release	12.4 Release
BGP extensions for IPv6					
IPv6 routing: multiprotocol BGP link-local address peering	12.0(22)S	12.2(4)T	12.2(14)S	12.3	12.4
IPv6 routing: IS-IS support for IPv6	12.0(22)S	12.2(8)T	12.2(14)S	12.3	12.4
IPv6 routing: IS-IS multitopology support for IPv6	12.0(26)S	12.2(15)T	12.2(18)S	12.3	12.4
IPv6 routing: OSPF for IPv6 (OSPFv3)	12.0(24)S	12.2(15)T	12.2(18)S	12.3	12.4
IPv6 routing: OSPF for IPv6 authentication support with IPSec	—	12.3(4)T	—	—	12.4
IPv6 routing: IPv6 policy-based routing	—	12.3(7)T	—	—	12.4
IPv6 routing: EIGRP support	—	12.4(6)T	—	—	—
IPv6 Services and Management					
IPv6 services: AAAA DNS lookups over an IPv4 transport	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 services: standard access control lists	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 services: DNS lookups over an IPv6 transport	12.0(22)S	12.2(8)T	12.2(14)S	12.3	12.4
IPv6 services: Secure Shell support over IPv6	12.0(22)S	12.2(8)T	12.2(14)S	12.3	12.4
IPv6 services: Cisco Discovery Protocol—IPv6 address family support for neighbor information	—	12.2(8)T	12.2(14)S	12.3	12.4
IPv6 services: CISCO-IP-MIB support	12.0(22)S	12.2(15)T	12.2(14)S	12.3	12.4
IPv6 services: CISCO-IP-FORWARDING-MIB support	12.0(22)S	12.2(15)T	12.2(14)S	12.3	12.4
IPv6 services: extended access control lists [3]	12.0(23)S	12.2(13)T	12.2(14)S	12.3	12.4
IPv6 services: generic prefix	—	12.3(4)T	—	—	12.4
IPv6 services: SNMP over IPv6 [6]	12.0(27)S	12.3(14)T	—	—	12.4
IPv6 services: IPv6 IOS Firewall	—	12.3(7)T	—	—	12.4
IPv6 services: IPv6 IOS Firewall FTP application support	—	12.3(11)T	—	—	12.4
IPv6 services: IPv6 IPSec VPN	—	12.4(4)T	—	—	—
IPv6 Broadband Access					
IPv6 access services: PPPoA	—	12.2(13)T	—	12.3	12.4
IPv6 access services: PPPoE	—	12.2(13)T	—	12.3	12.4
IPv6 access services: prefix pools	—	12.2(13)T	—	12.3	12.4
IPv6 access services: AAA support for Cisco VSA IPv6 attributes	—	12.2(13)T	—	12.3	12.4

Feature	12.0S Release	12.*x*T Release	12.2S Release	12.3 Release	12.4 Release
IPv6 access services: remote bridged encapsulation	—	12.3(4)T	—	—	12.4
IPv6 access services: AAA support for RFC 3162 IPv6 RADIUS attributes	—	12.3(4)T	—	—	12.4
IPv6 access services: stateless DHCPv6	12.0(32)S [7]	12.3(4)T	—	—	12.4
IPv6 access services: DHCPv6 prefix delegation	12.0(32)S [7]	12.3(4)T	12.2(18)SXE [8]	—	12.4
IPv6 access services: DHCP for IPv6 relay agent	—	12.3(11)T	—	—	12.4
IPv6 access services: DHCPv6 prefix delegation via AAA	—	12.3(14)T	—	—	12.4
IPv6 Multicast	12.0(26)S [9]	12.3(2)T	12.2(18)S	—	12.4
IPv6 multicast: Multicast Listener Discovery (MLD) protocol, versions 1 and 2	12.0(26)S [9]	12.3(2)T	12.2(18)S	—	12.4
IPv6 multicast: PIM sparse mode (PIM-SM)	12.0(26)S [9]	12.3(2)T	12.2(18)S	—	12.4
IPv6 multicast: PIM Source Specific Multicast (PIM-SSM)	12.0(26)S [9]	12.3(2)T	12.2(18)S	—	12.4
IPv6 multicast: scope boundaries	12.0(26)S [9]	12.3(2)T	12.2(18)S	—	12.4
IPv6 multicast: MLD access group	12.0(26)S [9]	12.3(4)T	12.2(25)S	—	12.4
IPv6 multicast: PIM accept register	12.0(26)S [9]	12.3(4)T	12.2(25)S	—	12.4
IPv6 multicast: PIM embedded RP support	12.0(26)S [9]	12.3(4)T	12.2(25)S	—	12.4
IPv6 multicast: RPF flooding of bootstrap router (BSR) packets	12.0(26)S [9]	12.3(4)T	12.2(25)S	—	12.4
IPv6 multicast: routable address hello option	12.0(26)S [9]	12.3(4)T	12.2(25)S	—	12.4
IPv6 multicast: static multicast routing (mroute)	12.0(26)S [9]	12.3(4)T	12.2(25)S	—	12.4
IPv6 multicast: address family support for multiprotocol Border Gateway Protocol (MBGP)	12.0(26)S [9]	12.3(4)T	12.2(25)S	—	12.4
IPv6 multicast: Explicit tracking of receivers	—	12.3(7)T	12.2(25)S	—	12.4
IPv6 multicast: IPv6 bidirectional PIM	—	12.3(7)T	12.2(25)S	—	12.4
IPv6 multicast: MFIB display enhancements	—	12.3(7)T	—	—	12.4
IPv6 multicast: IPv6 BSR	12.0(28)S	12.3(11)T	12.2(25)S	—	12.4
IPv6 multicast: IPv6 BSR bidirectional support	—	12.3(14)T	—	—	12.4
IPv6 multicast: IPv6 BSR scoped-zone support	—	—	12.2(18)SXE [8]	—	—
IPv6 multicast: SSM mapping for MLDv1 SSM	—	12.4(2)T	12.2(18)SXE [8]	—	—
IPv6 multicast: IPv6 BSR—ability to configure RP	—	12.4(2)T	—	—	—

Feature	12.0S Release	12.xT Release	12.2S Release	12.3 Release	12.4 Release
mapping					
IPv6 multicast: MLD group limits	—	12.4(2)T	—	—	—
IPv6 multicast: multicast user authentication and profile support	—	12.4(4)T	—	—	—
NAT Protocol Translation (NAT-PT)	—	12.2(13)T	—	12.3	12.4
NAT-PT: support for DNS ALG	—	12.2(13)T	—	12.3	12.4
NAT-PT: support for overload	—	12.3(2)T	—	—	12.4
NAT-PT: support for FTP ALG	—	12.3(2)T	—	—	12.4
NAT-PT: support for fragmentation	—	12.3(2)T	—	—	12.4
NAT-PT: support for translations in CEF switching	—	12.3(14)T	—	—	12.4
IPv6 Tunnel Services					
IPv6 tunneling: manually configured IPv6 over IPv4 tunnels	12.0(23)S [1]	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 tunneling: automatic 6to4 tunnels	12.0(23)S [1]	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 tunneling: automatic IPv4-compatible tunnels	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 tunneling: IPv6 over IPv4 GRE tunnels	12.0(22)S [10]	12.2(4)T	12.2(14)S	12.3	12.4
IPv6 tunneling: IPv6 over UTI using a tunnel line card [11]	12.0(23)S	—	—	—	—
IPv6 tunneling: ISATAP tunnel support	—	12.2(15)T	12.2(14)S	12.3	12.4
IPv6 tunneling: IPv4 over IPv6 tunnels	—	12.3(7)T	—	—	12.4
IPv6 tunneling: IPv6 over IPv6 tunnels	—	12.3(7)T	—	—	12.4
IPv6 tunneling: IP over IPv6 GRE tunnels	—	12.3(7)T	—	—	12.4
IPv6 tunneling: IPv6 GRE tunnels in CLNS networks	—	12.3(7)T	12.2(25)S	—	12.4
IPv6 QoS (Quality of Service)	12.0(28)S [12]	12.2(13)T	12.2(18)SXE [8]	12.3	12.4
IPv6 QoS: MQC packet classification	—	12.2(13)T	12.2(18)SXE [8]	12.3	12.4
IPv6 QoS: MQC traffic shaping	12.0(28)S [12]	12.2(13)T	12.2(18)SXE [8]	12.3	12.4
IPv6 QoS: MQC traffic policing	12.0(28)S [12]	12.2(13)T	12.2(18)SXE [8]	12.3	12.4
IPv6 QoS: MQC packet marking/re-marking	12.0(28)S [12]	12.2(13)T	12.2(18)SXE [8]	12.3	12.4
IPv6 QoS: queuing	12.0(28)S [12]	12.2(13)T	12.2(18)SXE [8]	12.3	12.4
IPv6 QoS: MQC weighted random early detection (WRED)-based drop	12.0(28)S [12]	12.2(13)T	12.2(18)SXE [8]	12.3	12.4
IPv6 Data Link Layer					

Feature	12.0S Release	12.*x*T Release	12.2S Release	12.3 Release	12.4 Release
IPv6 data link: ATM PVC and ATM LANE	12.0(22)S [13]	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 data link: Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 data link: FDDI	—	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 data link: Frame Relay PVC [14]	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 data link: Cisco High-Level Data Link Control	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 data link: PPP service over packet over SONET, ISDN, and serial (synchronous and asynchronous) interfaces	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 data link: VLANs using IEEE 802.1Q encapsulation	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 data link: VLANs using Cisco Inter-Switch Link (ISL)	12.0(22)S	12.2(2)T	12.2(14)S	12.3	12.4
IPv6 data link: dynamic packet transport (DPT)	12.0(23)S	—	—	—	—

Notes:

[1] In Cisco IOS Release 12.0(23)S, the Cisco 12000 series Internet router provides enhanced performance for IPv6 manually configured tunnels by processing traffic on the line card.

[2] The Cisco 10720 Internet router is supported in Cisco IOS Release 12.0(26)S.

[3] IPv6 extended access control lists and IPv6 provider edge routers over MPLS are implemented with IPv6 hardware acceleration on the Cisco 12000 series Internet router IP service engine (ISE) line cards in Cisco IOS routers in Cisco IOS Release 12.0(25)S and later releases.

[4] The RIP for IPv6 feature was updated in Cisco IOS Release 12.2(13)T.

[5] Enhancements were made to several multiprotocol BGP commands.

[6] SNMP versions 1, 2, and 3 are supported over an IPv6 transport.

[7] In Cisco IOS Release 12.0(32)S, the Dynamic Host Configuration Protocol (DHCP) for IPv6 prefix delegation is supported on shared port adaptors (SPAs) in the 10G Engine 5 SPA Interface Processor (SIP) on the Cisco 12000 series Internet router only for stateless address assignment.

[8] Cisco IOS Release 12.2(18)SXE provides support for this feature. Cisco IOS Release 12.2(18)SXE is specific to Cisco Catalyst 6500 and Cisco 7600 series routers.

[9] Feature is supported on Cisco 12000 series Internet routers in Cisco IOS Release 12.0(26)S.

[10] IPv6 over IPv4 GRE tunnels are not supported on the Cisco 12000 series Internet router.

[11] Feature is supported on the Cisco 12000 series Internet router only.

[12] Feature is supported on Cisco 12000 series Internet routers in Cisco IOS Release 12.0(28)S.

[13] Only ATM PVCs are supported in the Cisco IOS 12.0S software release train; ATM LANE is not supported.

[14] Frame Relay PVCs are not supported by distributed CEF switching for IPv6 in the 12.0S Cisco IOS software train. In the Cisco 12000 series Internet routers, Frame Relay encapsulated IPv6 packets are process switched on the Route Processor.
As the requirements for IPv6 features in the network grow, visit the following link to see what IOS version features map to:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d65ed.html

Distribution

1	MS 0630	A.L. Hale, 9600
1	MS 0630	N.A. Marsh, 6601
4	MS 0662	T. Klitsner, 9330
1	MS 0672	B.P. Van Leeuwen, 5615
1	MS 0781	E.L. Witzke, 6432
1	MS 0788	M.A. Rios, 6432
1	MS 0788	J.H. Maestas, 9336
4	MS 0788	P.A. Manke, 9338
1	MS 0788	M.J. Hamill, 9334
1	MS 0788	V.K. Williams, 9334
1	MS 0795	P.C. Jones, 9317
1	MS 0801	R.W. Leland, 9300
1	MS 0801	D.S. Rarick, 9310
1	MS 0801	D.R. White, 9340
1	MS 0823	J.D. Zepper, 9320
4	MS 0806	Len Stans, 9336
1	MS 0806	J.L. Akins, 9336
1	MS 0806	J.P. Brenkosh, 9336
6	MS 0806	J.M. Eldridge, 9336
1	MS 0806	A. Ganti, 9336
1	MS 0806	S.A. Gossage, 9336
6	MS 0806	T.C. Hu, 9338
1	MS 0806	B.R. Kellogg, 9336
1	MS 0806	J.H. Maestas, 9336
1	MS 0806	J.H. Naegle, 9336
1	MS 0806	T.J. Pratt, 9338
6	MS 0806	L.F. Tolendino, 9334
1	MS 0806	J.S. Wertz, 9336
1	MS 0813	G.K. Rogers, 9329
1	MS 0813	R.M. Cahoon, 9311
1	MS 0823	J.D. Zepper, 9320
1	MS 0832	J. H. Dexter, 9335
1	MS 1206	T.D. Tarman, 5622
1	MS 9012	B.A. Maxwell, 8949
1	MS 9012	C.T. Deccio, 8949
1	MS 9012	R.D. Gay, 8949
1	MS 9151	C.T. Oien, 8940
1	MS 9158	H.Y. Chen, 8961
2	MS 9018	Central Technical Files, 8944
2	MS 0899	Technical Library, 9536