

# **SANDIA REPORT**

SAND2006-3635  
Unlimited Release  
Printed June 2006

## **A Report On FY06 IPV6 Deployment Activities And Issues At Sandia National Laboratories**

John M. Eldridge, Tan C. Hu and 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](mailto: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](mailto:orders@ntis.fedworld.gov)  
Online order: <http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online>



SAND2006-3635  
Unlimited Release  
Printed June 2006

# **A Report on FY06 IPv6 Deployment Activities and Issues at Sandia National Laboratories**

John M. Eldridge, 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. IPv6 deployment in government network backbones has been mandated to occur 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 and Network System Design & Implementation Departments.



**Table of Contents**

*Introduction*..... 7  
*Background*..... 7  
**OMB directive**..... 9  
*IPv6 Addressing Schema and Support Issues* ..... 11  
*IPv6 Small Scale System Testing* ..... 13  
    **Router Configuration Testing**..... 13  
    **DHCP Testing**..... 14  
    **DNS Testing**..... 15  
    **Application Testing**..... 16  
*IPv6 in the ASC WAN* ..... 17  
    **Status of ASC WAN IPv6 Readiness**..... 18  
    **Verifying ASC WAN IPv6 Capability**..... 18  
*Implementing Ipv6 in the SNL Enterprise*..... 19  
    **SNL Environments**..... 19  
    **Estimated Network Hardware Costs to Support IPv6 SNL/NM**..... 19  
*Conclusion and Recommendations* ..... 21  
    **Next Steps to Take** ..... 21  
    Issues to Resolve..... 22  
*Bibliography* ..... 23  
Appendices..... 27  
    *IPv6 Test Host Configurations*..... 27  
    *IPv6 Test Node Configurations*..... 28  
    *Initial Test Results*..... 30  
    SNL/NM Network Devices Survey (March 23, 2006) ..... 37

**Table of Figures**

Figure 1: IPv6 Address Structure..... 11  
Figure 2: Draft ASC WAN Design January 2006 ..... 17



## ***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 we need to resolve to successfully deploy IPv6 at SNL.

SNL's expanding networking requirements as well as outside forces require that we evaluate and prepared 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 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, we deployed some subset of network hosts and services to demonstrate an installed 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.

We provide in this paper information regarding the IPv6 readiness of the 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. We hope that the information provided in this paper allows SNL to determine 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 resource requirements identified in this paper pertain to SNL/NM only. Resources required for SNL/CA will have to be determined independently

## ***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 in the 1990's is quickly depleting the available IPv4 address pool. To obtain more addresses, you need more bits, 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, recommended in January 1995 in RFC 1752. Over time, industry and 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 of numerous applications and devices, such as telephony appliances, PDA, 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 to it.

While there may be alternative technical solutions, such as NAT (Network Address Translation), to the address space problem, they don't work easily to allow this grow of new enhanced applications and services, and innovation. Furthermore, these alternative techniques make the Internet, the applications and the devices more complex resulting in higher costs. IPv6 can in the medium to long-term 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 included new benefits such as:

- 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.
- To provide better real time traffic support, IPv6 includes flow labels in its specifications.  
Real time applications might include video conferencing and IP telephony. Enhanced support for multicast and QoS.  
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.
- 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, 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 design of IPv6 took this consideration into account. IPv6 and IPv4 can easily coexist within the network.

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 system will increasingly include IPv6 as the default network stack running concurrently with an IPv4 stack. If SNL does not prepare for these network changes, the changes may introduce operational and security weaknesses to 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<sup>1</sup> 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 using 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 a procurement, Acquisition Regulation<sup>2</sup> 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<sup>3</sup>, 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

---

<sup>1</sup> U.S. Department of Commerce, National Institutes of Standards and Technology, National Telecommunications and Information Administration, "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6), January 2006.

<sup>2</sup> DOE Acquisition Letter AL-2006-04; Dated December 14, 2005; Subject: Acquiring Information Technology—Requirement to Comply With Internet Protocol Version 6 (IPv6).

<sup>3</sup> OMB Memorandum M-05-22; Dated: August 2, 2005; Titled: MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS; FROM: Karen S. Evans Administrator Office of E-Government and Information Technology; SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6).

- 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. Additional guidance on your agency's EA submission will be forthcoming.

### **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<sup>4</sup> 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.

---

<sup>4</sup> 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.

## IPv6 Addressing Schema and Support Issues

SNL currently has five portable 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). The Sandia National Laboratories (SNL) management of this IPv4 environment was an effort that was initiated in the early 1990s. The current support infrastructure assumes a default standard class C addresses assignment (24bit netmask) drawn from the legacy class B blocks (16bit 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. 128bits versus 32 bits and addresses are written using 32 hexadecimal digits arranged into 8 groups of four separated by colons. So 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 for the human mind to 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 it may actually contain three parts as illustrated.



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, two special bytes (fffe), and interface ID (6 bytes) which is the interface MAC assigned by the manufacturer.

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 E64 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. The following URL <http://en.wikipedia.org/wiki/IPv6> provides a list of differences and new features introduced by IPv6. As IPv6 becomes more prevalent, the support staff will have to understand the differences and adjust SNL practices accordingly.

As an example of the management decisions that will have to be made before IPv6 is introduced into the SNL environment, we must consider automatic E64 address assignment for host systems. Most of the world considers automatic E64 address assignment to be one of the most significant new IPv6 capabilities because it replaces manual or DHCP address assignment processes. SNL will have to make a decision whether to use the automatic host E64 address generation or continue with address assignment using DHCP. If the E64 automatic addressing capability is used it will reduce the address configuration effort; however, it may make the tracking of network activity more difficult. Further details of the impact on DNS and DHCP operations are discussed below.

Even if SNL uses E64 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.

Other IPv6 address management issue to be aware of is that the current policy for IPv6 address assignment does not permit portable or provider independent IPv6 address space to end sites. The 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, site that change ISP’s would require renumbering all host IPv6 prefix to that assigned by the new ISP.

## **IPv6 Small Scale System Testing**

Testing the IPv6 readiness of the enterprise network environment involves testing network elements, network services, and host systems. Using the current corporate IPv4 implementation as a guide, the small scale testing focused on network routers, DHCP network services, DNS, plus a small set of host applications. All of the testing reported in this document has taken place in our development laboratory with a very limited number of network elements and hosts.

## **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, we enabled it on two routers in the network development laboratory. Sandia currently deploys network equipment from two major vendors – Cisco and Foundry - in the open and restricted 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, we tested both E64 and non-E64 addressing schemes. We found the routers capable of implementing both address assignment and advertisement functions. The Linux client however would log error messages when it received a non-E64 advertisement. It is uncertain if Microsoft clients behave similarly. OSPF version three is required for IPv6 and it is active on both test routers, but we have not thoroughly exercise it. We added a Cisco 6500 with IOS 12.2.(18)SXD7 loaded on top of a Supervisor 2 management module to the mix. For rudimentary connectivity testing, we 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 at <http://www.cisco.com/ipv6> indicates that Cisco's full feature IPv6 release is contained in the 12.4 IOS. Earlier versions of IOS train starting with 12.0.S supports IPv6, but not 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. We performed a survey of the Open and Restricted network environments to determine router readiness. The survey indicates that there are 158 and 450 Cisco devices on the open and restricted environments (see "SNL/NM Network Devices Survey" in the Appendices). Out of those numbers, approximately eleven on the Open side and 44 on the Restricted side are designated as routers.

A move towards activating IPv6 would constitute three scenarios.

The first would be migrating to IOS 12.4, meaning potentially upgrading approximately 55 routers. An upgrade which could consist of software, a combination of additional memory + flash, supervisor+fan tray+ power supply, and additional replacement blades to address incompatibilities.

The second 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. Although this option may cost less in terms of hardware purchases it still involves replacing 31 routers (7507, 3725, 2501, 2507, 7140, 7206, 3640) and upgrading the flash on 16 Catalyst 6500 (reference spreadsheet in Appendices).

The last scenario is to replace the equipment with IPv6 capable systems as time and budget permits. It would be the lowest cost scenario; however, it runs into the probability of not meeting the June 2008 mandate.

We describe the full cost for scenarios one and two in detail later in this document.

## ***DHCP Testing***

DHCP is a network service that is a critical component for the current IPv4 infrastructure as it provides IPv4 addresses to requesting hosts automatically while providing configuration 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 (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<sup>5</sup>.

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

Testing a Linux IPv6 client (Fedora core4 Linux) showed that the Dnsmasq client software worked correctly using only the IPv6 protocol stack. The client (Fedora Linux) successfully obtained a new global IPv6 address along with domain name and DNS server address. Similar tests executed on Windows XP and Vista systems also showed that the Dnsmasq client software worked correctly utilizing IPv6 packets.

---

<sup>5</sup> See reference: DHCPv6 at sourceforge.

Even though we attempted to use other versions of DHCP client and server software, the Dibbler client and server software have proved to be the most useful on both Linux and Windows platforms. However, it should be noted 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 DHCP 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. We configured a Dell server running the SNL corporate Redhat Enterprise WS 4.0 Linux, and then we loaded it with Bind 9.2.4.2 to provide DNS services. Both the forward and reverse lookup zones were populated with AAAA records. DNS functionality has been checked with a Linux IPv6 client and both the forward and reverse address lookup works properly. DNS queries were restricted to IPv6 only although bind could be configured to accept both IPv4 and IPv6 packets. However, none of the Windows test platforms have been successfully configured to use the DNS server via IPv6. As a matter of fact even Windows Vista (beta2) would not accept an IPv6 addresses for a DNS server.

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 and the NWIS database is used as 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, this complex issue will require more thought and broader exposure before we can identify a corporate solution.

However, having an IPv6 capable DNS server running is absolutely 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.

## ***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, we were able to disable IPv4 on some hosts to do some initial tests. A useful reference for examining IPv6 application issues is <http://www.ipv6.org/v6-apps.html>.

Testing applications against IPv6 reveals that most, tested to this point, 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 let SCP use IPv6 but there is no way to use the address in place of the hostname; the syntax required appears to be “SCP -6 filename user@host2:filename”. So in this case it was not possible to test SCPv6 without a functioning IPv6 capable DNS. Using IPv6 addresses instead of a host name is a burden and will lead to application difficulties. If we have a functional DNS server installed, some applications that cannot handle IPv6 addresses might work since hosts are referenced by name instead of address.

The reader is cautioned about reacting too 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 and allows users to utilize remote ASC resources as if they were local. The ASC WAN is currently in a transition phase moving from a point-to-point OC48 to a full ring at 10Gbps. As this new WAN will probably last five years, it has to be able to support IPv6. The ASC WAN is 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.

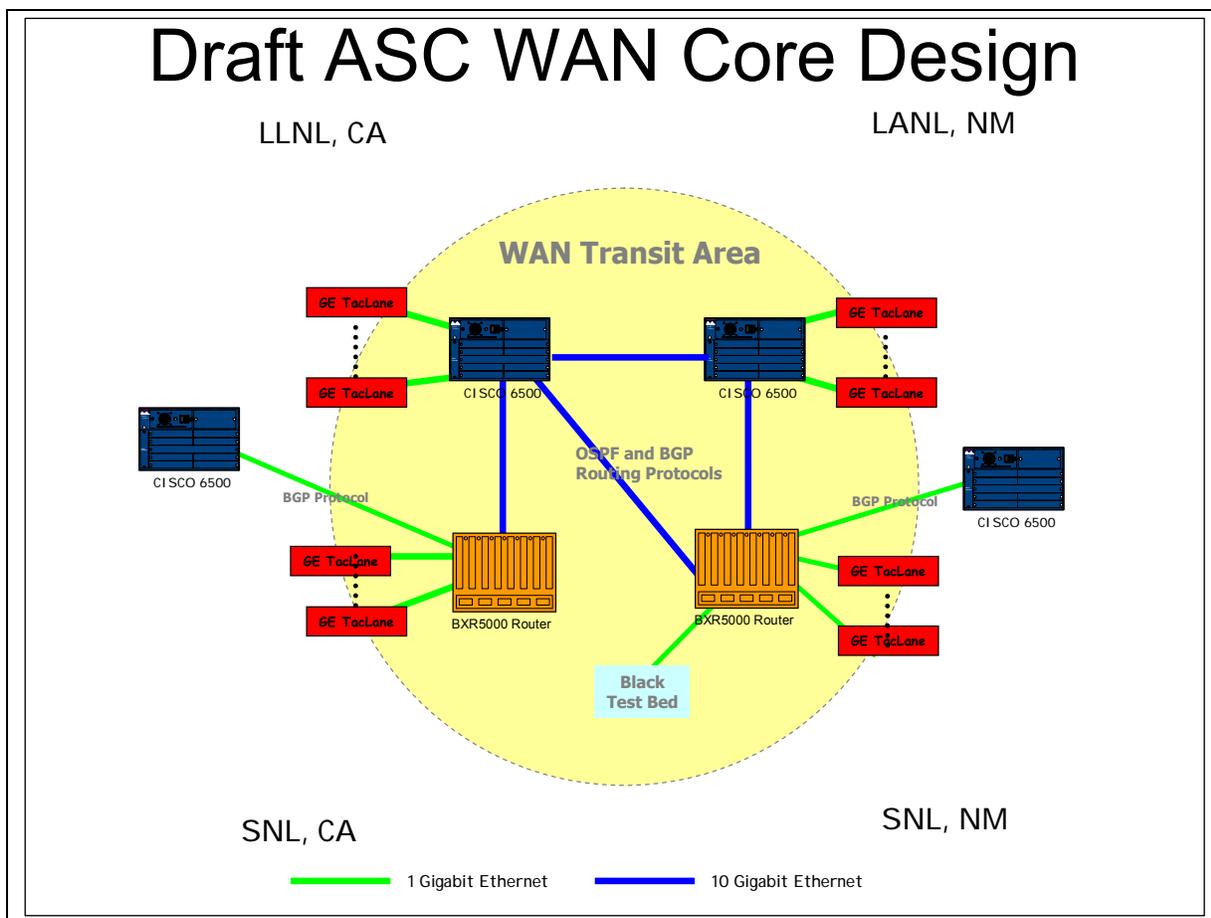


Figure 2: Draft ASC WAN Design January 2006

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 IP encryptors are scheduled to be upgraded to IPv6 capable within the year.

## ***Status of ASC WAN IPv6 Readiness***

After reviewing the available information for the network routers, we find that the Cisco and Marconi routers are capable of supporting IPv6 routing and addressing. However, the encryptors do not support IPv6 at the present. General Dynamics, the manufacturer of the IP encryptors being installed, expects to have IPv6 support as of 4Q2006. Actual testing of the IPv6 capabilities of the routers will have to wait until the new ASC WAN is completed and normal operations over this new network have become routine. Beginning a development effort to determine IPv6 capabilities while we are putting this new network into production would not be prudent.

Future events may make our initial evaluation inadequate. First, the initial evaluation of the ASC WAN assumed a simple configuration. The discussion as to whether the ASC WAN will remain a private transit zone is still underway. In addition, it is not clear where IPv6 addresses for this private network would be obtained. 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.

Secondly, it is possible that the ASC WAN will be used for additional interconnections between the tri-lab sites, such as restricted environment interconnection. In this case our simple transit zone model is inadequate as routing information will have to be transferred between sites. This will make the IPv6 address and routing configurations much more complicated.

Unfortunately, these scenarios cannot be examined at this time. We do not have adequate equipment in the tri-lab development environments to perform the required tests and the production environment is inappropriate for this type of work.

## ***Verifying ASC WAN IPv6 Capability***

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 we have used in the past will allow us to verify that IPv6 data streams are forwarded at the same performance levels as 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 IP encryptors, we can test IPv6 encryptor performance in a test laboratory setting. This testing can be done relatively easily, but the defining tests must be run from one laboratory classified network to another. These tests will not be as straight forward 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 needed to change the network's basic operating practices. OMB dictates are insufficient reason to modify the SCN.

The SON SNL/NM on the other hand represents less than 10% of SNL network connectivity and a major redesign of the environment is not really beneficial to the laboratories. The SRN SNL/NM is where the SNL action is 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 (DNS, DHCP?) will have to be installed.

### ***Estimated Network Hardware Costs to Support IPv6 SNL/NM***

In generating a cost estimate for supporting IPv6 only the SRN SNL/NM and the SON SNL/NM were considered as the Foundry routers in the SCN SNL/NM are already capable of supporting IPv6.

After examining the status of the routers currently deployed in the SNL/NM SON and SRN we 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. By and large the 6500 systems can be upgraded while the others must be replaced. There are 31 routers in the heterogeneous group and 16 Cisco 6500 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, 16 are populated with SUP2 cards, and must be upgraded to support IPv6. There are two possibilities to consider with these units. First we could retain the SUP2 cards and simply upgrade memory which would allow us to claim that we support IPv6 albeit at a lower level of functionality than desired. Of course we would also be upgrading obsolete hardware. The cost of upgrading the memory is about \$3,000 each for a total of \$48,000.

The second alternative for the Cisco model 6500 routers would be to upgrade the routers to SUP720 cards. This would entail upgrading fan units, power supplies, and other ancillary equipment at a cost of about \$50,000 each for a total of \$800,000.

The following two scenarios allow us to calculate the likely network costs involved.

#### **Scenario 1**

- Upgrading 31 small routers to Cisco 3750 models at an average cost of \$10,000 each would cost about \$310,000
- Upgrading the memory on the 17 SUP2 based Cisco 6500 routers might cost about \$3,000 each for a total cost of \$48,000. Of course we would be upgrading obsolete hardware which would soon be retired.

Estimated Network Cost ~ \$358,000

#### **Scenario 2**

- 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 16 \$800,000

Estimated Network Cost ~ \$1,110,000

These two scenarios bound the network hardware costs for the SNL/NM SON and SRN to support IPv6 to between \$358,000 and \$1,110,000.

In addition to the network hardware costs we 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 also 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
- Cyber Enterprise Management
- Network analysis and troubleshooting
- NWIS

### **Conclusion and Recommendations**

The most straight forward 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 and network services as well as 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.

### **Next Steps to Take**

#### **Define What “Support IPv6 in the Network Backbones” Means to SNL**

It will be necessary to consider each SNL network environment separately when we evaluate the readiness to support IPv6. We 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; prefix advertisement, DNS address advertisement.

Create a Plan to Prepare SNL Network Elements for IPv6

Create a Schedule for IPv6 Implementation on the SNL Corporate Backbones

Create a Schedule and Plan to Implement IPv6 in the ASC WAN

1. Document and test BXR5000 IPv6 capabilities

### **Create a Formal IPv6 Development Lab and Assign Responsibility for Implementation Planning**

Include required IPv6 services and network elements in the development lab.

#### *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.

#### **Address Assignment Methodology**

To DHCPv6 or not!

E64 addressing or not!

Support Provider Dependent or Provider Independent address prefix (See ARIN IPv6 addressing policy)

#### **Multiple Addresses per Host Interface**

See IPv6 privacy RFC.

#### **Dynamic IPv6 DNS Updates**

See DNSSEC.

#### **IPv6 Compatibility with Corporate Information Systems (NWIS)**

NWIS needs additional code to handle IPv6 addressing.

#### **IPv6 Impact on Network Security Processes and Practices**

#### **Availability of IPv6 Capable Network Test Equipment/Trouble Shooting Support**

## **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 \(RFC 1884\)](#) obsoleted by RFC 2373
7. [An Architecture for IPv6 Unicast Address Allocation \(RFC 1887\)](#)
8. [Internet Protocol, Version 6 \(IPv6\) Specification \(RFC 1883\)](#) obsoleted by RFC 2460/ updated by RFC 2147
9. [Internet Control Message Protocol \(ICMPv6\) for the Internet Protocol Version 6 \(IPv6\) \(RFC 1885\)](#) obsoleted by RFC 2463
10. [IPv6 Testing Address Allocation \(RFC 1897\)](#) obsoleted 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 \(RFC 1972\)](#) obsoleted by RFC 2464
14. [Neighbor Discovery for IP Version 6 \(IPv6\) \(RFC 1970\)](#) obsoleted by RFC 2461
15. [Transmission of IPv6 Packets Over FDDI \(RFC 2019\)](#) obsoleted by RFC 2467
16. [IP Version 6 over PPP \(RFC 2023\)](#) obsoleted by RFC 2472
17. [An IPv6 Provider-Based Unicast Address Format \(RFC 2073\)](#) obsoleted by RFC 2374
18. [Basic Socket Interface Extensions for IPv6 \(RFC 2133\)](#) obsoleted by RFC 2553
19. [TCP and UDP over IPv6 Jumbograms \(RFC 2147\)](#) obsoleted by RFC 2675/ updates RFC 1883
20. [Advanced Sockets API for IPv6 \(RFC 2292\)](#) obsoleted by RFC 3542
21. [IPv6 Multicast Address Assignments \(RFC 2375\)](#)
22. [An IPv6 Aggregatable Global Unicast Address Format \(RFC 2374\)](#) obsoletes RFC 2073/ obsoleted by RFC 3587
23. [IP Version 6 Addressing Architecture \(RFC 2373\)](#) obsoletes RFC 1884/ obsoleted 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/ obsoleted 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 \(RFC 2454\)](#) obsolete by RFC 4113
35. [IP Version 6 Management Information Base for the Transmission Control Protocol \(RFC 2452\)](#) 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/ 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 \(RFC 2732\)](#) 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/ 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



## APPENDICES

For those interested in the technical testing details, configurations used for IPv6 testing, or current router configurations, we offer the following appendix.

### *IPv6 Test Host Configurations*

System Identity	IP Address	Current OS	Future/Function	Notes
Dell-2650	Fixed	Red Hat Enterprise 4	DHCPv6 (Dibbler), DNSv6	Standard password
Dell-2650	Fixed	Red Hat Enterprise 4	IPv6 only data server	Standard password
Dell-2650	Fixed	Mepis Linux		Non Standard password
Newisys	Fixed	Open BSD		Non Standard password
Verrari	Fixed	Fedora Core4 x64	Test Data Client	Standard password
Verrari	Fixed	Fedora Core4 x64	Test Data Client	Standard password
Verrari	Fixed	Fedora Core4 x64	Test Data Client	Standard password
Verrari	Fixed	Fedora Core4 x64	Test Data Client	Standard password
Dell-2650	Fixed		Foundry Ironview	
Newisys	Fixed	Fedora Core 5	Test Host	
Saix14098	DHCP	XP, Linux FC4, Vista	Test Host	
Ferrari-It	DHCP	XP, Linux FC\$	Laptop	
Dell-2650	Fixed		ASC WAN Test Host	
Dell-2650	Fixed		ASC WAN Test Host	

Host	IPv6 Address	Scope
ferrari-It	2001:400:4410:4:2c0:9fff:fe87:c315	global
saix14098	2001:400:4410:4:20c:6eff:feb3:3e98	global
Dell203	2001:400:4410:4:206:5bff:fef6:4312	global
Dell201	2001:400:4410:4:206:5bff:fef6:436c	global

### **Dibbler Linux File Locations**

Dibbler is the best implementation of the DHCPv6 specs currently available. It is written by a graduate student in Poland.

- Accessed or used conf files /etc/dibbler
- Template conf and pid files /var/lib/dibbler
- Dibbler-server, dibbler-client /usr/sbin

## IPv6 Test Node Configurations

November 15, 2005

### Windows Vista Automatically Generated IP Parameters

When a Windows Vista system is set to auto-configure and use IPv4 DHCP on the NIC, the system automatically generates IPv6 addresses and parameters based on the NIC address and the IPv4 address assigned to the host.

```
D:\Users\Administrator\Desktop>ipconfig /all
```

```
Windows IP Configuration
```

```
Host Name . . . . . : saix14098
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : srn.sandia.gov
System Quarantine State . . . . . : Not Restricted
```

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . : srn.sandia.gov
Description . . . . . : Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet
Controller
Physical Address. . . . . : 00-0C-6E-B3-3E-98
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:400:4410:4:20c:6eff:feb3:3e98
Temporary IPv6 Address. . . . . : 2001:400:4410:4:e916:72ec:a14e:8882
Link-local IPv6 Address . . . . . : fe80::20c:6eff:feb3:3e98%8
IPv4 Address. . . . . : AAA.AAA.AAA.177
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, November 15, 2005 8:59:07 AM
Lease Expires . . . . . : Saturday, November 19, 2005 8:59:07 AM
Default Gateway . . . . . : fe80::20c:dbff:fe80:60e0%8
                             fe80::20c:dbff:fe80:79e0%8
                             AAA.AAA.AAA.254
DHCP Server . . . . . : AAA.AAA.BBB.24
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                             fec0:0:0:ffff::2%1
                             fec0:0:0:ffff::3%1
                             AAA.AAA.CCC.25
                             AAA.AAA.DDD.5
Primary WINS Server . . . . . : AAA.AAA.CCC.100
Secondary WINS Server . . . . . : AAA.AAA.BBB.42
NetBIOS over Tcpi . . . . . : Enabled
```

```
Tunnel adapter Local Area Connection* 8:
```

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : isatap.srn.sandia.gov
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

The configuration includes various addresses and tunnel setups to operate in a mixed IPv4 and IPv6 realm.

November 16, 2005

## Ferrari Windows XP SP2 IPv6 and IPv4 Parameters

```
C:\Documents and Settings\Administrator>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : Ferrari-LT
Primary Dns Suffix . . . . . : srn.sandia.gov
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : srn.sandia.gov
                                   srn.sandia.gov
                                   sandia.gov
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . : srn.sandia.gov
Description . . . . . : Broadcom NetLink (TM) Gigabit Ethernet
Physical Address. . . . . : 00-C0-9F-87-C3-15
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : AAA.AAA.AAA.175
Subnet Mask . . . . . : 255.255.255.0
IP Address. . . . . : 2001:400:4410:4:b057:fa4b:c552:a5e9
IP Address. . . . . : 2001:400:4410:4:2c0:9fff:fe87:c315
IP Address. . . . . : fe80::2c0:9fff:fe87:c315%4
Default Gateway . . . . . : AAA.AAA.AAA.254
                                   fe80::20c:dbff:fe80:60e0%4
                                   fe80::20c:dbff:fe80:79e0%4

DHCP Server . . . . . : AAA.AAA.BBB.24
DNS Servers . . . . . : AAA.AAA.CCC.25
                                   AAA.AAA.DDD.5
                                   fec0:0:0:ffff::1%4
                                   fec0:0:0:ffff::2%4
                                   fec0:0:0:ffff::3%4

Primary WINS Server . . . . . : AAA.AAA.CCC.100
Secondary WINS Server . . . . . : AAA.AAA.BBB.42
NetBIOS over Tcpip. . . . . : Disabled
Lease Obtained. . . . . : Tuesday, November 15, 2005 7:34:27 AM
Lease Expires . . . . . : Saturday, November 19, 2005 7:34:27 AM
```

Tunnel adapter Teredo Tunneling Pseudo-Interface:

```
Connection-specific DNS Suffix . :
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : FF-FF-FF-FF-FF-FF-FF-FF
Dhcp Enabled. . . . . : No
IP Address. . . . . : fe80::5445:5245:444f%5
Default Gateway . . . . . :
NetBIOS over Tcpip. . . . . : Disabled
```

Tunnel adapter 6to4 Tunneling Pseudo-Interface:

```
Connection-specific DNS Suffix . : srn.sandia.gov
Description . . . . . : 6to4 Tunneling Pseudo-Interface
Physical Address. . . . . : 86-FD-04-AF
Dhcp Enabled. . . . . : No
Default Gateway . . . . . :
DNS Servers . . . . . : fec0:0:0:ffff::1%4
                                   fec0:0:0:ffff::2%4
                                   fec0:0:0:ffff::3%4
```

```
NetBIOS over Tcpi. . . . . : Disabled
Tunnel adapter Automatic Tunneling Pseudo-Interface:
    Connection-specific DNS Suffix . : srn.sandia.gov
    Description . . . . . : Automatic Tunneling Pseudo-Interface
    Physical Address. . . . . : 86-FD-04-AF
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : fe80::5efe:AAA.AAA.AAA.175%2
    Default Gateway . . . . . :
    DNS Servers . . . . . : fec0:0:0:ffff::1%4
                           fec0:0:0:ffff::2%4
                           fec0:0:0:ffff::3%4
NetBIOS over Tcpi. . . . . : Disabled
```

## ***Initial Test Results***

Testing of IPv6 capabilities has one subtle aspect that must be addressed when evaluating test results. Most all network elements and hosts will be running both the IPv4 and IPv6 protocol stacks at once, a dual stack configuration. Therefore when running tests of services such as DNS and DHCP or other applications one cannot be assured that the information is actually being transmitted using IPv6 packets. One must always check to insure that IPv6 packets are being used.

As far as Vista is concerned there is just one ping utility and it accepts either IPv4 or IPv6 addresses.

Ping works in both IPv4 and IPv6 mode; however, there are difficulties when using Windump to capture traffic. First, the Windows systems use the temporary IPv6 address by default for Ping. This address seems to change at every reboot of the system. Second, one must count on using the hardware based addresses to get some continuity between tests BUT one never knows the replying address when doing a test.

November 17, 2005

Subsequent Ping tests have shown the power of the link-local address and the ability of IPv6 to resolve host names to addresses without the use of DNS as long as the nodes are in a local (non-routed) network. For Example look at the following two Ping tests.

```
D:\Users\Administrator\Desktop>ping fe80::2c0:9fff:fe87:c315

Pinging fe80::2c0:9fff:fe87:c315 from fe80::20c:6eff:feb3:3e98%8 with 32
bytes of data:

Reply from fe80::2c0:9fff:fe87:c315: time<1ms
Reply from fe80::2c0:9fff:fe87:c315: time<1ms
Reply from fe80::2c0:9fff:fe87:c315: time<1ms
Reply from fe80::2c0:9fff:fe87:c315: time<1ms

Ping statistics for fe80::2c0:9fff:fe87:c315:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms

```
D:\Users\Administrator\Desktop>ping ferrari-lt
```

```
Pinging ferrari-lt [2001:400:4410:4:2c0:9fff:fe87:c315] from  
2001:400:4410:4:bcc0:db01:b616:4046 with 32 bytes of data:
```

```
Reply from 2001:400:4410:4:2c0:9fff:fe87:c315: time<1ms  
Reply from 2001:400:4410:4:2c0:9fff:fe87:c315: time<1ms  
Reply from 2001:400:4410:4:2c0:9fff:fe87:c315: time<1ms  
Reply from 2001:400:4410:4:2c0:9fff:fe87:c315: time<1ms
```

```
Ping statistics for 2001:400:4410:4:2c0:9fff:fe87:c315:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Using the name ferrari-lt successfully indicates that the sending node could resolve the name to an IPv6 addresses without the use of DNS since we did not have a DNS IPv6 server running.

## November 18, 2005 - IPv6 Testing Standalone Testing on Local Switch

### Ferrari Windows XP SP2 IPv6 and IPv4 Parameters

```
C:\Documents and Settings\Administrator>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : Ferrari-LT  
Primary Dns Suffix . . . . . : srn.sandia.gov  
Node Type . . . . . : Hybrid  
IP Routing Enabled. . . . . : No  
WINS Proxy Enabled. . . . . : No  
DNS Suffix Search List. . . . . : srn.sandia.gov  
                                srn.sandia.gov  
                                sandia.gov
```

Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . : srn.sandia.gov  
Description . . . . . : Broadcom NetLink (TM) Gigabit  
Ethernet  
Physical Address. . . . . : 00-C0-9F-87-C3-15  
Dhcp Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . : Yes  
IP Address. . . . . : AAA.AAA.AAA.175  
Subnet Mask . . . . . : 255.255.255.0  
IP Address. . . . . :  
2001:400:4410:4:b057:fa4b:c552:a5e9  
IP Address. . . . . :  
2001:400:4410:4:2c0:9fff:fe87:c315  
IP Address. . . . . : fe80::2c0:9fff:fe87:c315%4
```

A Report on FY06 IPv6 Deployment Activities and Issues at Sandia National Laboratories

```
Default Gateway . . . . . : AAA.AAA.AAA.254
                             fe80::20c:dbff:fe80:60e0%4
                             fe80::20c:dbff:fe80:79e0%4
DHCP Server . . . . . : AAA.AAA.BBB.24
DNS Servers . . . . . : AAA.AAA.CCC.25
                             AAA.AAA.DDD.5
                             fec0:0:0:ffff::1%4
                             fec0:0:0:ffff::2%4
                             fec0:0:0:ffff::3%4
Primary WINS Server . . . . . : AAA.AAA.CCC.100
Secondary WINS Server . . . . . : AAA.AAA.BBB.42
NetBIOS over Tcpi. . . . . : Disabled
Lease Obtained. . . . . : Tuesday, November 15, 2005
7:34:27 AM
Lease Expires . . . . . : Saturday, November 19, 2005
7:34:27 AM
```

Tunnel adapter Teredo Tunneling Pseudo-Interface:

```
Connection-specific DNS Suffix . :
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : FF-FF-FF-FF-FF-FF-FF-FF
Dhcp Enabled. . . . . : No
IP Address. . . . . : fe80::5445:5245:444f%5
Default Gateway . . . . . :
NetBIOS over Tcpi. . . . . : Disabled
```

Tunnel adapter 6to4 Tunneling Pseudo-Interface:

```
Connection-specific DNS Suffix . : srn.sandia.gov
Description . . . . . : 6to4 Tunneling Pseudo-Interface
Physical Address. . . . . : 86-FD-04-AF
Dhcp Enabled. . . . . : No
Default Gateway . . . . . :
DNS Servers . . . . . : fec0:0:0:ffff::1%4
                             fec0:0:0:ffff::2%4
                             fec0:0:0:ffff::3%4
NetBIOS over Tcpi. . . . . : Disabled
```

Tunnel adapter Automatic Tunneling Pseudo-Interface:

```
Connection-specific DNS Suffix . : srn.sandia.gov
Description . . . . . : Automatic Tunneling Pseudo-
Interface
Physical Address. . . . . : 86-FD-04-AF
Dhcp Enabled. . . . . : No
IP Address. . . . . : fe80::5efe:AAA.AAA.AAA.175%2
Default Gateway . . . . . :
DNS Servers . . . . . : fec0:0:0:ffff::1%4
                             fec0:0:0:ffff::2%4
                             fec0:0:0:ffff::3%4
NetBIOS over Tcpi. . . . . : Disabled
```

C:\Documents and Settings\Administrator>ping6 fe80::20c:6eff:feb3:3e98

Pinging fe80::20c:6eff:feb3:3e98 with 32 bytes of data:

No route to destination.

Specify correct scope-id or use -s to specify source address.

No route to destination.

Specify correct scope-id or use -s to specify source address.

No route to destination.

Specify correct scope-id or use -s to specify source address.

No route to destination.

Specify correct scope-id or use -s to specify source address.

Ping statistics for fe80::20c:6eff:feb3:3e98:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>ping6 -s fe80::2c0:9fff:fe87:c315  
fe80::20c:6eff:feb3:3e98

Pinging fe80::20c:6eff:feb3:3e98

from fe80::2c0:9fff:fe87:c315 with 32 bytes of data:

Invalid source route specified.

Problem with source address or scope-id.

Invalid source route specified.

Problem with source address or scope-id.

Invalid source route specified.

Problem with source address or scope-id.

Invalid source route specified.

Problem with source address or scope-id.

Ping statistics for fe80::20c:6eff:feb3:3e98:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>ping6 -s fe80::2c0:9fff:fe87:c315  
fe80::20c:6eff:feb3:3e98

Pinging fe80::20c:6eff:feb3:3e98

from fe80::2c0:9fff:fe87:c315 with 32 bytes of data:

Invalid source route specified.

Problem with source address or scope-id.

Invalid source route specified.

Problem with source address or scope-id.

Invalid source route specified.

Problem with source address or scope-id.

Invalid source route specified.

Problem with source address or scope-id.

Ping statistics for fe80::20c:6eff:feb3:3e98:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

But, from the Vistal node, ping works fine on the stand alone switch as captured by Ethereal on the Ferrari node.

## A Report on FY06 IPv6 Deployment Activities and Issues at Sandia National Laboratories

---

No.	Time	Source	Destination	Protocol Info
1	0.000000	fe80::20c:6eff:feb3:3e98	fe80::2c0:9fff:fe87:c315	ICMPv6

Echo request

Frame 1 (94 bytes on wire, 94 bytes captured)  
Ethernet II, Src: AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98), Dst:  
QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
2	0.000044	fe80::2c0:9fff:fe87:c315	fe80::20c:6eff:feb3:3e98	ICMPv6

Echo reply

Frame 2 (94 bytes on wire, 94 bytes captured)  
Ethernet II, Src: QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15), Dst:  
AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
3	1.004022	fe80::20c:6eff:feb3:3e98	fe80::2c0:9fff:fe87:c315	ICMPv6

Echo request

Frame 3 (94 bytes on wire, 94 bytes captured)  
Ethernet II, Src: AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98), Dst:  
QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
4	1.004064	fe80::2c0:9fff:fe87:c315	fe80::20c:6eff:feb3:3e98	ICMPv6

Echo reply

Frame 4 (94 bytes on wire, 94 bytes captured)  
Ethernet II, Src: QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15), Dst:  
AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
5	2.007907	fe80::20c:6eff:feb3:3e98	fe80::2c0:9fff:fe87:c315	ICMPv6

Echo request

Frame 5 (94 bytes on wire, 94 bytes captured)  
Ethernet II, Src: AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98), Dst:  
QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
6	2.007951	fe80::2c0:9fff:fe87:c315	fe80::20c:6eff:feb3:3e98	ICMPv6

Echo reply

Frame 6 (94 bytes on wire, 94 bytes captured)

## A Report on FY06 IPv6 Deployment Activities and Issues at Sandia National Laboratories

---

Ethernet II, Src: QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15), Dst:  
AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
7	3.011796	fe80::20c:6eff:feb3:3e98	fe80::2c0:9fff:fe87:c315	ICMPv6 Echo request

Frame 7 (94 bytes on wire, 94 bytes captured)  
Ethernet II, Src: AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98), Dst:  
QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
8	3.011839	fe80::2c0:9fff:fe87:c315	fe80::20c:6eff:feb3:3e98	ICMPv6 Echo reply

Frame 8 (94 bytes on wire, 94 bytes captured)  
Ethernet II, Src: QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15), Dst:  
AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
9	4.830013	fe80::20c:6eff:feb3:3e98	fe80::2c0:9fff:fe87:c315	ICMPv6 Neighbor solicitation

Frame 9 (86 bytes on wire, 86 bytes captured)  
Ethernet II, Src: AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98), Dst:  
QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
10	4.830053	fe80::2c0:9fff:fe87:c315	fe80::20c:6eff:feb3:3e98	ICMPv6 Neighbor advertisement

Frame 10 (86 bytes on wire, 86 bytes captured)  
Ethernet II, Src: QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15), Dst:  
AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
11	4.975149	fe80::2c0:9fff:fe87:c315	fe80::20c:6eff:feb3:3e98	ICMPv6 Neighbor solicitation

Frame 11 (86 bytes on wire, 86 bytes captured)  
Ethernet II, Src: QuantaCo\_87:c3:15 (00:c0:9f:87:c3:15), Dst:  
AsustekC\_b3:3e:98 (00:0c:6e:b3:3e:98)  
Internet Protocol Version 6  
Internet Control Message Protocol v6

No.	Time	Source	Destination	Protocol Info
-----	------	--------	-------------	---------------

```
12 4.975271    fe80::20c:6eff:feb3:3e98 fe80::2c0:9fff:fe87:c315 ICMPv6  
Neighbor advertisement
```

```
Frame 12 (86 bytes on wire, 86 bytes captured)  
Ethernet II, Src: AsustekC_b3:3e:98 (00:0c:6e:b3:3e:98), Dst:  
QuantaCo_87:c3:15 (00:c0:9f:87:c3:15)  
Internet Protocol Version 6  
Internet Control Message Protocol v6
```

**From these tests it looks like the Windows XP system cannot utilize the link-local addresses to run IPv6 apps such as ping.**

Ipconfig /renew executed on both systems gets the usual set of global-scope IPv6 addresses. However, the Windows XP system cannot use the link-local addresses as a source but can still respond on that address. The reason that Windows XP does not work quite right is that the system never seems to send a neighbor solicitation message asking for neighbor information. Apparently my installation of Fedora Core 4 also does not send any solicitation messages. The only ones I see in Ethereal are from the Vista system.

According to documentation Windows Server 2003 has the IPv6 protocol well integrated and should work properly. It would be good to have such a system in the IPv6 test bed to compliment the Vista system.

## SNL/NM Network Devices Survey (March 23, 2006)

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

## SON SNL/NM Router Summary

Vendor	Node Type	Software Version	Supervisor	DRAM/ Flash (MB)	Minimum Enterprise IOS version for IPv6 (or replace system)	DRAM Need Upgrade	Flash Need Upgrade
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/32	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.2(17d)SXB10	Supervisor Engine 720	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco Systems	Cisco 7507	12.1(19)		256/16	REPLACE SYSTEM		
Cisco Systems	Cisco 7507	12.1(19)		256/16	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.3(5b)		128/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.3(5b)		128/32	REPLACE SYSTEM		
Cisco Systems	Cisco 2501	11.2(5)		16/8	REPLACE SYSTEM		
Cisco Systems	Cisco 2507	11.2(16)		64/16	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.3(5b)		128/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.3(5b)		128/32	REPLACE SYSTEM		
Cisco Systems	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		<u>216</u>	46.5
	.1.3.6.1.4.1.9.1.615	<u>1</u>	0.2
	.1.3.6.1.4.1.9.1.617	<u>2</u>	0.4
	Cisco 3640	<u>2</u>	0.4
	Cisco 3725	<u>11</u>	2.3
	Cisco 7140 (2-FE)	<u>2</u>	0.4
	Cisco 7206 VXR	<u>3</u>	0.6
	Cisco 7507	<u>2</u>	0.4
	Cisco C2912MF-XL	<u>2</u>	0.4
	Cisco C2950C-24	<u>45</u>	9.6
	Cisco C2950G-12	<u>4</u>	0.8
	Cisco C2950G-24	<u>14</u>	3
	Cisco C2950G-48	<u>39</u>	8.4
	Cisco C2950T-24	<u>33</u>	7.1
	Cisco C2970-24TS	<u>3</u>	0.6
	Cisco C3508G-XL	<u>1</u>	0.2
	Cisco C3550-12G	<u>2</u>	0.4
	Cisco C3550-24MMF	<u>11</u>	2.3
	Cisco C3550-48	<u>1</u>	0.2
	Cisco C6000 MSFC	<u>1</u>	0.2
	Cisco C6509	<u>21</u>	4.5
	Cisco C6513	<u>5</u>	1
	Cisco C8540MSR	<u>1</u>	0.2
	Cisco LS1010	<u>2</u>	0.4
	Unknown	<u>8</u>	1.7
Cisco Systems (Catalyst)		<u>234</u>	50.4
	Cisco WS-C2948G	<u>35</u>	7.5
	Cisco WS-C5000	<u>23</u>	4.9
	Cisco WS-C5500	<u>29</u>	6.2
	Cisco WS-C5505	<u>9</u>	1.9
	Cisco WS-C5509	<u>9</u>	1.9
	Cisco WS-C6006	<u>5</u>	1
	Cisco WS-C6506	<u>23</u>	4.9
	Cisco WS-C6509	<u>56</u>	12
	Cisco WS-C6513	<u>42</u>	9
	Unknown	<u>3</u>	0.6
Cisco Systems/Altiga networks VPN concentrator		<u>3</u>	0.6

A Report on FY06 IPv6 Deployment Activities and Issues at Sandia National Laboratories

---

	Cisco-Altiga's VPN Concentrator hardware	<u>3</u>	0.6
Foundry Networks		<u>11</u>	2.3
	.1.3.6.1.4.1.1991.1.3.32.2	<u>10</u>	2.1
	Foundry BigIron 15000 Router	<u>1</u>	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 Systems	c6sup2_rp-JK2SV-M	12.1(20)E3	Supervisor 2	256/32	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6513	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/32	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/32	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/32	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)

A Report on FY06 IPv6 Deployment Activities and Issues at Sandia National Laboratories

Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6513	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco C6509	12.1(20)E3	Supervisor 2	256/16	12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	Yes (64)
Cisco Systems	Cisco 7206 VXR	12.3(3b)	Supervisor 2	128/8	REPLACE SYSTEM		
Cisco Systems	Cisco C6509	12.2(18)SXF	Supervisor Engine 720	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco Systems	Cisco C6509	12.2(18)SXF	Supervisor Engine 720	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco Systems	Cisco C6513	12.2(18)SXF	Supervisor Engine 720	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco Systems	Cisco C6509	12.2(18)SXF	Supervisor Engine 720	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco Systems	Cisco C6509	12.2(18)SXF	Supervisor Engine 720	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco Systems	Cisco C6513	12.2(18)SXF	Supervisor Engine 720	512/64	12.4, 12.2.17d-SXB11 or 12.2.18-SXD7	No (256)	No (64)
Cisco Systems	Cisco 7507	12.0(9)		256/16			
Cisco Systems	Cisco C6000 MSFC	12.1(6)E1		128/16	REPLACE SYSTEM		
Cisco Systems	Cisco 7507	12.1(19)		64/16	REPLACE SYSTEM		

A Report on FY06 IPv6 Deployment Activities and Issues at Sandia National Laboratories

---

Cisco Systems	Cisco 7140 (2-FE)	12.1(9)E		256/8	REPLACE SYSTEM		
Cisco Systems	Cisco 7206 VXR	12.2(15)T8		256/8	REPLACE SYSTEM		
Cisco Systems	RSP-JSV-M	12.1(19)		256/16	REPLACE SYSTEM		
Cisco Systems	Cisco 3640	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.2(15)T8		120/32	REPLACE SYSTEM		
Cisco Systems	Cisco 7206 VXR	12.2(15)T8		256/8	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.2(15)T8		256/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.2(15)T8		120/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.3(17a)		252/32	REPLACE SYSTEM		
Cisco Systems	Cisco 7140 (2-FE)	12.2(15)T8		328/8	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.2(15)T8		252/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3640	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.2(15)T8		120/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco Systems	C3725-IK9S-M	12.2(15)T8		128/32	REPLACE SYSTEM		

A Report on FY06 IPv6 Deployment Activities and Issues at Sandia National Laboratories

---

Cisco Systems	Cisco 3725	12.2(15)T8		128/32	REPLACE SYSTEM		
Cisco Systems	Cisco 3725	12.2(15)T8		128/32	REPLACE SYSTEM		

## SCN Device and Vendor Summary (System Description)

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

## Distribution

1	MS 0136	G.E. Connor, 4333
1	MS 0630	K.E. Washington, 4600
1	MS 0630	N.A. Marsh, 4601
4	MS 0788	M.J. Benson, 4334
1	MS 0788	J.H. Maestas, 4334
4	MS 0788	P.A. Manke, 4338
1	MS 0788	V.K. Williams, 4334
1	MS 0788	M.A. Rios, 4334
1	MS 0795	P.C. Jones, 4317
1	MS 0801	R.W. Leland, 4300
1	MS 0801	D.S. Rarick, 4310
1	MS 0801	D.R. White, 4340
1	MS 0823	J.D. Zepper, 4320
1	MS 0805	W.D. Swartz, 4329
4	MS 0806	Len Stans, 4336
3	MS 0806	J.M. Eldridge, 4436
1	MS 0806	S.A. Gossage, 4336
6	MS 0806	T.C. Hu, 4338
1	MS 0806	C.M. Keliiaa, 4336
1	MS 0806	B.R. Kellogg, 4336
1	MS 0806	J.H. Naegle, 4336
1	MS 0806	T.J. Pratt, 4338
6	MS 0806	L.F. Tolendino, 4334
1	MS 0806	J.S. Wertz, 4336
1	MS 0813	G.K. Rogers, 4312
1	MS 0813	R.M. Cahoon, 4311
1	MS 1393	J.A. Larson, 12120
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, 4536