Implementing Internet Protocol Version 6 (IPv6) on an Army Installation

By: Trace Gunsch, Emerging Technology Critical Skill Expert (CSE) U.S. Army Information Systems Engineering Command (USAISEC), Technology Integration Center (TIC); trace.gunsch@us.army.mil, with special thanks to Delle Lambert and Patsy Platt, also at the TIC.

Abstract

With Department of Defense (DOD) and Office of Management and Budget (OMB) mandating a migration to IPv6, Army installation Directors of Information Management (DOIMs) are beginning to feel pressured to implement IPv6 on their post networks. Unfortunately, little practical guidance exists to inform the DOIMs the procedures necessary to prepare their networks for IPv6. More is needed than simply enabling IPv6 on local area network (LAN) routers and switches. Many infrastructure components must be upgraded as well, including Domain Name Service (DNS), directory services, security, and network management. Besides the physical hardware and software components, local policies need to be defined for network security and IPv6 addressing, and steps need to be taken to provide training for administrators and registration of IPv6 pilots.

This paper attempts to summarize the steps necessary to enable an IPv6 pilot on an Army post. It attempts to address the question, "What is necessary to do today to prepare for an IPv6 application on the post network tomorrow." It will cover the procedures necessary to implement IPv6 on an Army base, including covering current status of commercial product support and Government testing of IPv6 capabilities.

INTRODUCTION

When DOD first began implementing communications networks using Transmission Control Protocol/Internet Protocol (TCP/IP), network protocols were fairly immature. Configuration of devices was manual, security and prioritization were absent, network management was immature, and communications speeds were incredibly slow by today's standards. Over time, our IP networks have become more robust, more user-friendly, and equivalently more relied upon by users and managers. Our users now expect a high level of performance from our IPv4 networks. We have in-depth security systems, highly robust network management, auto-configuration, prioritization, converged voice and video, multicast, mobility, and high-speed performance capabilities on our IPv4 networks.

The challenge of implementing IPv6 into an Army network comes from two conditions placed upon the DOD by the U.S. Congress: Do No Harm and IPv4 Parity. The first is easily understood and met–we do not want to diminish our current communications capability in order to develop a future capability. The second is the real challenge; that the IPv6 network will perform equivalent to or better than the current IPv4 network.

The upside of IPv6 implementation is that most IPv4 vendors are now moving to support IPv6 in the same devices that currently run our IPv4 networks. The downside of IPv6 implementation is that the equivalent features and capabilities of IPv6 tend to lag several years behind IPv4.

This paper investigates the network service areas of a typical Army post and shows what can be achieved now with IPv6 and what lags behind in achieving IPv4 parity. It describes the current state of industry and the pieces which need to become mature before we can implement IPv6 on our networks with IPv4 parity.

BACKGROUND

In June 2003, DOD Chief Information Officer (CIO) published a memorandum [ref a] requiring a migration of DOD networks to IPv6. This memo, and a September 30 follow-on [ref b], defined that the IPv6 transition would be accomplished through technical refresh cycles, and that all future purchases should be of IPv6-capable products, with a loose definition of what IPv6-capable means. The hope was that by 2008, all network devices would be IPv6-capable and enabling IPv6 would be relatively simple and cost-effective.

The fallacy of this approach is that the products available for purchase in 2003 were not really IPv6-capable, and continuing progress has not generated IPv6-capable products. It was well known in 2003, that several Asian countries were building IPv6 networks, but the commercial products available at that time did not have the capabilities of IPv4. For example, Gigabit-Ethernet (GbE) switches, which pass IPv4 packets at rates of 1 billion bits per second could only pass IPv6 packets at less then 1 percent of that rate. This may not have been an issue for China, which had little to no IPv4 infrastructure–to them, any IPv6 capability is an improvement–but it stymied DOD deployments. Even now, 4 years later, many capabilities regularly found in IPv4 products are not available

in IPv6 implementations, and vendors are more motivated to build new IPv4 capabilities than to improve IPv6.

IPV6 PILOTS

As stated previously, one of the DOD goals is transition through technical refresh. Communications hardware often gets replaced every 3 to 5 years. Replacing the hardware with IPv6-capable products, if they existed, could be accomplished with little additional cost. The technical refresh approach, however, does not solve all the needs of a transition to IPv6. At best, it can cover much of the hardware and software cost of the migration; but it fails to address many other issues such as Testing, Modeling & Simulation; Developing Policies; Changing Security Architecture; Increased Operations and Maintenance; and Training.

The DOD's solution to these gaps in the implementation is through the extensive use of pilot programs. A pilot is considered to be an intermediate step between test and implementation. The DOD hopes to eliminate much of the costs of testing and training through the use of service pilots and has been pressuring the services to identify pilot candidate programs and to begin testing IPv6 in constrained implementations.

DOD Milestone objectives

In addition to the two DOD memoranda mentioned previously, numerous different mandates and memos from DOD, OMB, and Assistant Secretary of Defense (Networks and Information Integration) [ASD(NII)] provide guidance for implementing IPv6 on Government and DOD networks. A listing and short description of all these documents are covered in Appendix A of this paper. References j and l established the following milestone objectives for conducting an IPv6 pilot.

a. Milestone Objective 1 (MO1) states that services and agencies are authorized to operate IPv6 systems within an enclave. The MO1 allows the use, familiarization, and testing of IPv6 protocol and applications for operational pilots in order to ascertain issues and derive migration strategies. Pilots are authorized to operate at MO1, effective 1 October 2005.

b. Milestone Objective 2 (MO2) provides the ability to evaluate the scalability and further evaluate the IPv6 Information Assurance (IA) implications using tunneling and native IPv6 routing, as available. The MO2 permits applications to test IPv6 specific end-to-end capabilities and routing schema efficiencies. Pilots are authorized to operate at MO2, effective 1 December 2006.

c. Milestone Objective 3 (MO3) will be authorized when all policy, planning, and technical transition guidance has been provided to allow tunneled and native IPv6 traffic to exist on DOD operational networks. The MO3 will permit applications and data owners to complete operational transition to IPv6 with at least the same functionality as currently found in IPv4. Target date for MO3 is Fiscal Year (FY) 2008.

ENABLING IPV6 FOR AN ARMY PILOT

The Army is considering leveraging the Installation Information Infrastructure Modernization Program (I3MP) to conduct a pilot for IPv6 on an installation. The Army's I3MP provides for the engineering, acquisition, implementation and management of the Army's installation level telecommunications infrastructure. While I3MP is primarily responsible for Ethernet switches which compose the network backbone, a pilot cannot simply be enabling IPv6 on a couple of switches or routers. An effective pilot requires an IPv6 application running across the post infrastructure, demonstrating the operation of IPv6 end to end.

At the I3MP program manager's request, engineers at USAISEC conducted an analysis to determine how to enable an IPv6 pilot on an Army post. Our approach to this analysis was to answer the question, "What do we need to do on the post today to be ready for IPv6 application tomorrow?" We scoped the problem with a couple of assumptions:

a. Every affected device in the system will be dual-stack, supporting IPv4 and IPv6. This includes the application server, client and network backbone. There will not be any IPv6-only devices and no tunneling.

b. The application will reside entirely on-post. The client and server machines will all be on the same post and no IPv6 traffic will leave the post. This meets the MO1 guidance.

REQUIREMENTS

Figure B-1 shows the typical architecture of an Army installation network. This architecture was designed for the I3MP and has been adopted by most Army post DOIMs. The diagram shows several zones delineating network capabilities and areas of responsibility. Zones 1, 2, and 3 define a GbE backbone in a star configuration, put in place by the I3MP. This backbone provides connectivity for the central server farm or local processing center (LPC) (Zone 5), network management stations (Zone 6), and client machines (Zone 4). The Army post connection to the NIPRNet is protected by a Top-Level Architecture (TLA) security suite (Zone 7), through which all external traffic must traverse.

Post-wide Requirements

Several issues must be addressed that will affect all aspects of the IPv6 implementation. These are policy, addressing, and training. For policy, current DOD directives state that IPv6 traffic is not allowed on any operational DOD Network, except under a pilot project. The DOD IPv6 Transition Office (DITO) has established that any DOD pilot must adhere to the MO1 and MO2 guidance and must be registered with the DITO. Another policy issue relates to security. A pilot implementation must define appropriate security policies of what IPv6 traffic will be allowed on the network and where that traffic will be allowed to go. This will be discussed more in the section on Zone 7, TLA.

An address plan is necessary before establishing IPv6 traffic. Most IPv6 experts suggest that a post IPv6 address plan should closely reflect the current IPv4 addressing plan, to ease network management, but opportunity exists to improve the addressing scheme in IPv6. Addresses should be given out in a manner that will facilitate hierarchical routing, where prudent, and should follow Army and DOD addressing policies. Unfortunately, Army and DOD addressing policies are not complete at this time, and so a post cannot at present obtain permanent IPv6 address space.

The final global requirement is equipping the network administration team, who will be responsible for troubleshooting network problems and enabling IPv6 on the

network. Network administrators require training on the IPv6 protocols and require tools that can analyze both IPv4 and IPv6 traffic. The availability of such tools is discussed in Zone 6.

Zones 1-3: Backbone Zones

Zones 1-3 make up what is referred to as the I3MP or post backbone. The Core of the network, Zone 1, is typically two to three high-power Layer 3 (L3) switches, defined as Main Core Nodes (MCNs). The distribution layer, Zone 2, consists of more L3 switches, called Area Distribution Nodes (ADNs). These ADNs are not as powerful as the MCNs, but support connections to the end-user buildings (EUBs) in the Access Layer. Zone 3, the Access Layer, usually consists of Layer 2 (L2) Ethernet switches. The L2 switches do not deal with traffic at the IP layer, so do not have to support IPv4 or IPv6, other than remote network management access (see the following).

Current I3MP requirements [ref c] dictate that L3 switches must meet full performance parity of IPv6 and IPv4. This means that those switches must be able to transmit the full 1 or 10 Gigabits per second on each GbE or 10-GbE port. In addition, they must have support for Open Shortest Path First (OSPF) version 3 (the IPv6 equivalent of OSPF version 2), and must support IPv6 Access Control Lists (ACLs) and security logging. Often an ADN switch will be dual-homed to both MCNs, so if one link fails, the other will automatically take over. This should be a requirement for IPv6 traffic as well as IPv4. Lastly, all IPv6 devices must support Internet Protocol Security (IPSec), according to the DOD Information Technology Standards Registry (DISR) Product Profile [ref d], so these switches must do this as well.

Of these requirements, several L3 switches exist which meet the performance, OSPFv3, and ACL/security logging requirements; but none tested at the TIC have met the IPSec requirements to date. We have not tested dual-homing capabilities for IPv6 to date, so that capability is unknown. Additional I3MP requirements go into effect on 1 Jan 2008 [refs e and f], requiring L3 switches to fully support IPv6 network management and IPv6 security, equivalent to current IPv4 standards.

Several other features of Zone 1-3 devices are optional. This means that an IPv6 pilot can operate without these features, and they are typically considered "nice to have." These optional features include Differentiated Services (DiffServ) for traffic prioritization, tunneling IPv6 over IPv4, multicast, virtual LAN (VLAN), 802.1X, and auto-configuration support. Of these features, DiffServ, auto-configuration, and tunneling are common to commercial I3MP switches, but secure network management, multicast, and 802.1X support are not. Support for IPv6 VLANs is widely varying among current switch vendors.

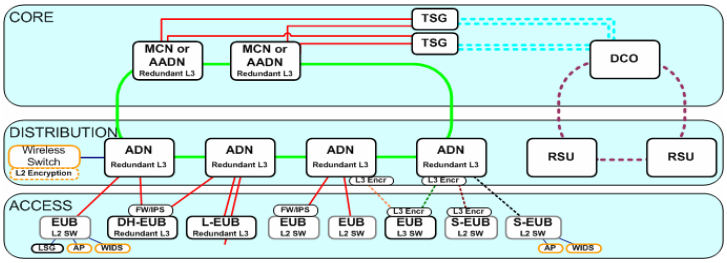

Figure 1. Zones 1-3 : Core/Distribution/Access Requirements A (Backbone) Zones

Zone 4: Client Edge:

A typical IPv6 application will communicate between a client and a server across the network. For the assumed scenario, some number of client computers will need to be IPv6-enabled. This will require a computer operating system (OS) that can run in dual-stack mode. Most commercial OSs can do this; LINUX, Solaris, MAC, and Windows Vista all support IPv6 fairly well. Windows XP lacks many IPv6 capabilities, so it should not be used for a pilot.

In addition to a dual-stack OS, the client system needs some sort of auto-configuration support from the network. Dynamic Host Configuration Protocol (DHCP) is not mature in IPv6, so switch-based auto-configuration is the preferred method, and it is supported in most L3 switches.

Those are the minimum requirements; however, several features that users expect from their client devices are not mature for IPv6. Public Key Infrastructure (PKI) and common access card (CAC) support, for example, are not developed yet for IPv6. Active Directory and thin client support for Microsoft OSs are not established yet for IPv6, either, though Microsoft promises these features in their next server OS, Longhorn, due in late 2007. Dynamic Domain Name Service (DDNS) is also not mature for IPv6. The DDNS is highly valuable for network managers, who otherwise have to manually enter every IP address into static DNS tables. Manual entry is very time-consuming and error-prone with IPv4; much more so with IPv6. This also is promised in Longhorn. Support for DDNS in other OSs is unknown.

Finally, the issue of user applications is critical to IPv6 deployment. At present, few commercial applications exist that fully support IPv6 and it is incredibly rare to find one that uses features of IPv6 that IPv4 cannot support. This is a major issue in the push for IPv6 deployment: without applications that use IPv6 features, the motivation to migrate to IPv6 is very low, and the momentum to improve IPv6 capabilities is very small.

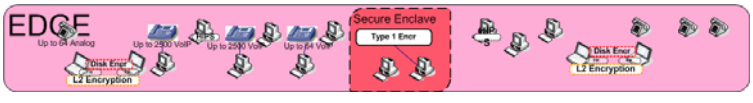

Figure 2. Zone 4: Client Edge

Zone 5: Server Farm

The server farm, now called the LPC under the Server Consolidation Program, is where the domain controllers, mail, file, and other application servers reside. It is typically a centralized location where the network administrators can conveniently maintain hardware components, monitor security patches, and conduct system backups. For an IPv6 implementation, the required components are an IPv6-capable

DNS system and a dual-stack OS on the server that will host the IPv6 application. Other server farm components, such as DDNS, Active Directory, and back-up tools, are not required to run on IPv6.

Commercial DNS products have supported IPv6 for several years; in fact, DNS is one of the first aspects to fully support IPv6. Dual-stack OSs are coming along. Most UNIX platforms support most IPv6 features, but Windows 2003 does not. Microsoft's Longhorn, due out in late 2007, promises built-in IPv6 support, including Active Directory and DDNS support over IPv6. Longhorn will require a 64-bit server bus, which means many DOIMs will have to upgrade their server hardware to implement it. Once released, users should expect several months before Network Enterprise Technology Command (NETCOM) policy allows Longhorn's implementation on Army networks.

Standard office applications do not typically make use of IPv6 features and often do not support it. Microsoft's Exchange 2007, for example, just released this year, will not support IPv6 until Service Pack 1, due out in late 2007. Other applications are at various stages of IPv6 implementation. Many UNIX-based thin client systems support IPv6, but Microsoft's thin client support for IPv6 is unknown. Voice over IP products presently do not support IPv6, so providing an IPv6 call processor system will be very difficult. Even more challenging will be the thousands of Army-specific applications that will need to be upgraded to IPv6 support at some time. Most of these applications do not require IPv6 support for a pilot project, but these are issues Army users need to start considering.

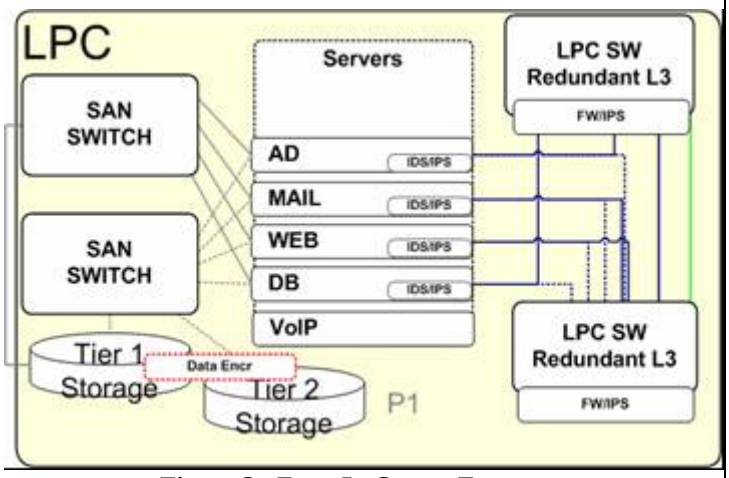

Figure 3. Zone 5: Server Farm

Zone 6: Network Management Zone

Network management over IPv6 will often be one of the last areas enabled for an IPv6 implementation. Devices that use IPv6 traffic in a dual-stack mode can be managed using IPv4, without any impact to the IPv6 traffic. Network management is also the least mature of the IPv6 technologies in the commercial realm. It will eventually become a requirement when the Army moves to IPv6-only deployments, and with that goal in mind, I3MP is requiring IPv6 network management in L3 switches starting in January 2008, but few vendors presently show much capability in this area.

Element manager tools, like Hewlett-Packard (HP) OpenView and Spectrum, use secure Simple Network Management Protocol (SNMP) over IPv4 to manage network devices, but presently do not support secure SNMP over IPv6. Patch management tools, like Storage Management System (SMS) and anti-virus updates currently cannot be accomplished over IPv6. Again, these tools do not need to run over IPv6 for a network to support IPv6, but we will eventually need this capability when we leave our dual-stack environments for IPv6-native deployments.

Network management includes the ability to scan networks for hostile IPv6 traffic, IPv6 viruses, and vulnerabilities to IPv6 attacks. It also includes the ability to analyze traffic patterns and tools for troubleshooting and optimizing networks. These tools are things DOIMs use frequently in their day-to-day operations and are vital for deploying and maintaining an operational or a pilot network. Some network sniffers, such as Ethereal, support IPv6, but the status of vendor development for other scanning tools varies, and DOIMs will need to determine if the tools they presently use can support IPv6.

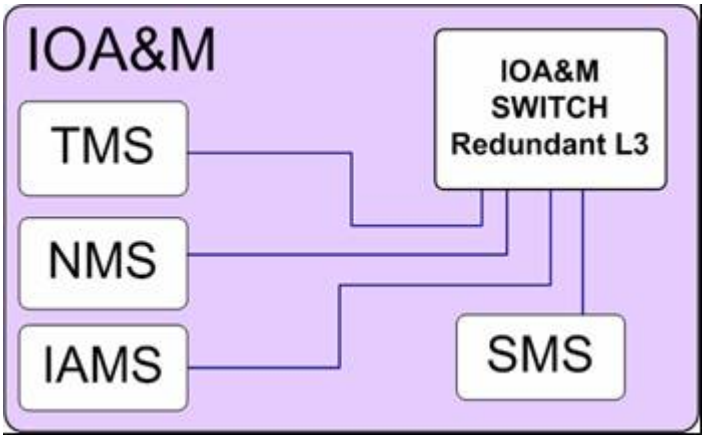

Figure 4. Zone 6: Network Management Zone

Zone 7: Top Level Architecture (TLA)

The TLA is the security architecture that protects the network from external intrusions and attacks. It is typically installed and managed by NETCOM, instead of the local DOIM. Figure 5 shows a typical security implementation, from NIPRNet connection to the network core. The Army Processing Center (APC) represents a regional server farm, where a global application might be hosted.

Our initial conditions for this paper stated that an IPv6 application would not leave the local post. This means that the TLA really is not involved in passing IPv6 traffic. The only thing necessary in the TLA stack is to block IPv6 traffic from crossing either direction. Current firewalls do this by default, so no action is necessary at the TLA for a local pilot implementation.

However, the Army is moving toward regional server consolidation, so remote applications are desirable. If an IPv6 application were to be hosted at an APC, several new requirements emerge. First of all, some sort of tunneling mechanism will be required between the APC and either the LPC, the client machine or perhaps the Army DISN (Defense Information Systems Network) Router Program (ADRP) router. The tunnel mechanism must encapsulate the IPv6 data into IPv4 packets to ship across the NIPRNet. Tunnel mechanisms exist, but they create a new requirement for security devices, firewalls, and intrusion detection systems (IDSs). In a tunnel, IPv6 packets are encapsulated within IPv4 and usually encrypted. This makes deep packet inspection,

required by current Defense-in-Depth policies, extremely difficult. Security as an industry is far behind in the deployment of IPv6, and finding IPv6-inspecting firewalls and IDSs is challenging.

An alternative solution to tunneling is to use IPv6-capable virtual private networks (VPNs) to encrypt IPv6 traffic between the local post and the APC. This removes the requirement for a tunneling device and bypasses the issue of packet inspection on firewalls and IDSs because encrypted traffic cannot be inspected. This approach is counter to the current security policies, however, and much collaboration is needed between DOD and Army security architects and IPv6 implementers to work through these security issues.

Eventually, we will need to open up the entire network to IPv6 traffic, so that IPv6 applications can communicate between any military posts and to the Internet. When that time comes, we will need full IPv6 support on firewalls, IDSs, VPNs, and proxy servers. The Army Secure Router (ASR) and ADRP devices will need to be dual-stack at that time. Current ASR and ADRP routers may require hardware upgrades to support dual-stack, and industry will have to start building IPv6 capability into these security devices, which at present have very little IPv6 support.

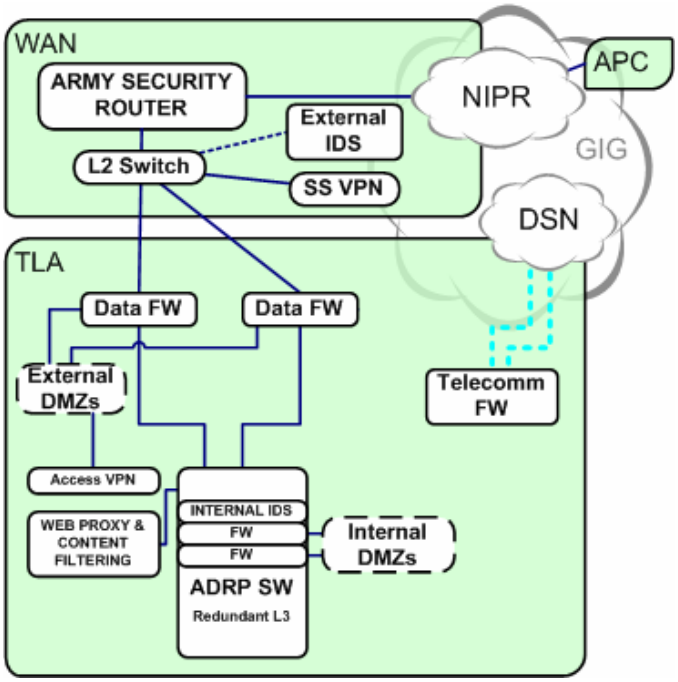

Figure 5. Zone 7: TLA

WHEN WILL WE GET THERE?

A lot of the delays to DOD's IPv6 implementation occur because commercial vendors do not see the pressing need to migrate to IPv6. Twenty years ago, DOD was a dominant customer in the communications industry and DOD directives were taken very seriously by industry. Today, DOD represents a relatively small market segment for most commercial vendors. To make matters worse, DOD as a whole is not investing money into IPv6 development and is only half-heartedly promoting IPv6 implementation on its networks. It is a classic Catch-22; DOD agencies do not want to invest a lot of money into IPv6 until industry starts making better products, but industry does not want to spend a lot of money developing IPv6 products until customers start buying them.

Some glimmers of hope do exist, though. The DOD has established a number of testbeds where IPv6 capabilities are being evaluated and products are being recommended for implementations. For example, the Army's TIC has established an IPv6 System Integration Facility for validating IPv6 capabilities for hardware, software, and systems. Under the sponsorship of I3MP, this lab is testing Ethernet switches, routers, OSs, and security devices. They also are testing commercial applications and are able to test Army-specific applications in a replicated Army post environment.

The DOD has also established an Approved Products List (APL) of commercial products that have demonstrated conformance to DOD standards, interoperability with DOD equipment, and a certain level of performance in IPv6. As the APL gets populated, the DOD intends to mandate that only products on the APL can be purchased and used on DOD networks.

ISSUES/CONCERNS

Several concerns are prevalent in any implementation of IPv6; Internet Protocol Security (IPSec) is one of the most controversial. Current guidance states that all IPv6 devices must support IPSec. Current NSA Guidance appears to indicate any IPSec device is an IA device and therefore must undergo Federal Information Processing Standard (FIPS) certification and National Information Assurance Partnership (NIAP) Common Criteria evaluation. The majority of IPv6 devices available at present do not support IPSec. Both the development of IPSec capabilities and the FIPS/NIAP processes are very expensive for vendors and time-consuming, meaning extensive delays in getting secure products for DOD implementations.

Another issue, touched on in the Zone 5 discussion, is that upgrades are required for most servers to support the 64-bit bus speed required for Longhorn. The NETCOM has proactively mandated that future server purchases must be 64-bit, but the bulk of current servers are only 32-bit.

Finally, the issue of addressing policies is not yet defined for DOD and Army. A pilot implementation could proceed with temporary IPv6 addresses, but unless an addressing plan is defined, implementers risk wasting a great deal of time and effort in renumbering and restructuring a pilot implementation when the addressing plans are finalized.

CONCLUSIONS AND RECOMMENDATIONS

Implementing IPv6 on an Army Post requires many more components than just IPv6-enabling core elements. Besides the switches, implementers need to be concerned with server and client OSs, network scanning and vulnerability analysis tools, addressing plans, policies, and training. Commercial products for these aspects are lacking in IPv6 development, so conducting pilots at this time is very difficult.

The DOD needs to continue to encourage industry to develop IPv6 products. The DITO should publish a mandate now requiring APL usage at some future date and encouraging vendors to submit their products for APL testing. Army program managers need to pressure vendors to develop IPv6 capabilities now in their products and applications and pursue

testing, at places like the TIC, to confirm that they will work in the Army secure dual-stack environment.

REFERENCES

a. DOD CIO Memorandum, *Internet Protocol Version 6 (IPv6)*, 9 June 2003

b. DOD Chief Information Officer (CIO) Memorandum, *Internet Protocol version 6 (IPv6) Interim Transition Guidance*, September 29, 2003.

c. Program Executive Office, Enterprise Information Systems (PEO EIS) Memorandum, *Approved Product Performance Specification for Internet Protocol Version 6 (IPv6)*, 7 June 2006.

d. DOD CIO, Department of Defense Information Technology Standards Registry Baseline Release 05-2.0 (DISR), September 6, 2005.

e. PEO EIS Memorandum, Recommended Product Management Specification for Internet Protocol Version 6 (IPv6), October 2006.

f. PEI EIS Memorandum, Recommended Product Security Specification for Internet Protocol Version 6 (IPv6), October 2006.

g. DOD CIO Memorandum, Internet Protocol Version 6 (IPv6) Transition Plan Coordination and Interim Tasking, 28 November 2003.

h. OMB Memorandum, M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6), 5 August 2005.

i. DOD CIO Memorandum, Department of Defense (DOD) Internet Protocol Version 6 (IPv6) Master Test Plan, 16 August 2005.

j. DOD CIO Memorandum, DOD Internet Protocol Version 6 (IPv6) Pilot Nominations, 16 August 2005.

k. DOD CIO Memorandum, Department of Defense (DOD) Internet Protocol Version 6 (IPv6) Implementation Schedules for Major Networks and Programs, 18 July 2006.

l. Assistant Secretary of Defense, Networks and Information Integration [ASD(NII)] Memorandum, Internet Protocol Version 6 (IPv6) Policy Update, 16 August 2005.

BIOGRAPHICAL SKETCH

Mr. Gunsch is the Emerging Technologies CSE at the USAISEC-TIC, Fort Huachuca, Arizona. He holds a Bachelor of Science Degree in Engineering Physics from North Dakota State University and a Master of Science Degree in Electrical and Computer Engineering from the University of Arizona.

APPENDIX A. LIST OF MANDATES

a. DOD CIO Memorandum, *Internet Protocol Version 6 (IPv6)* (also known as the *Stenbit Memo*), 9 June 2003.

- Directed that as 1 October 2003, all Global Information Grid (GIG) assets being developed, procured, or acquired shall be IPv6 capable (in addition to maintaining interoperability with IPv4 systems/capabilities)

b. DOD CIO Memorandum – 29 September 2003, Internet Protocol version 6 (IPv6) Interim Transition Guidance

- Established policy that products and systems procured or acquired after 1 October 2003 must be capable of operating in IPv6 networks.
- Defined IPv6-Capable.
- Identified the Joint Technical Architecture (JTA) IPv4/IPv6 IT standards Profile as a reference.
- Established provisional process and requirement for Component CIO waiver when IPv6-capable criteria cannot be met.

c. DOD CIO Memorandum – 28 November 2003

- Required DOD Components to develop **Transition Plans** no later than (NLT) April 2004, and include resource requirements in program objective memorandum (POM) and budget submissions.
- Required National Security Agency (NSA) to develop security guidelines and solutions, and take actions to ensure availability of IA-certified products to support fielding.
- Required NSA to develop IA and Network Connection Guidelines for IPv6 Pilots.

d. OMB Memorandum – 5 August 2005

- Set June 2008 by which all agencies' infrastructure (**network backbones**) must be using IPv6.

e. ASD(NII) Memorandum – 16 August 2005

- Defined **Milestone Objectives** for enterprise-wide deployment of IPv6.
- Established Components' authority to determine their waiver policy.

f. DOD CIO Memorandum – 16 August 2005

- Established DOD Chief Information Officer-Executive Board (CIO-EB) and **Information Technology Standards Guidance (ITSG)** for oversight of planning.
- Required Components to nominate O-6/GS-15 ITSG representatives.

g. DOD CIO Memorandum – 16 August 2005

- Established requirements for nomination, planning and implementation of **pilots**.
- Requested Components to nominate pilots.
- Authorized pilots to commence on 1 October 2005, subject to meeting required conditions.

h. DOD CIO Memorandum – 18 July 2006

- Required Components to submit **IPv6 Implementation Schedules** for major networks and programs.
- Requires Components to submit quarterly updates to DOD CIO-EB on transition progress.

This page intentionally left blank.

APPENDIX B. I3MP ARCHITECTURE

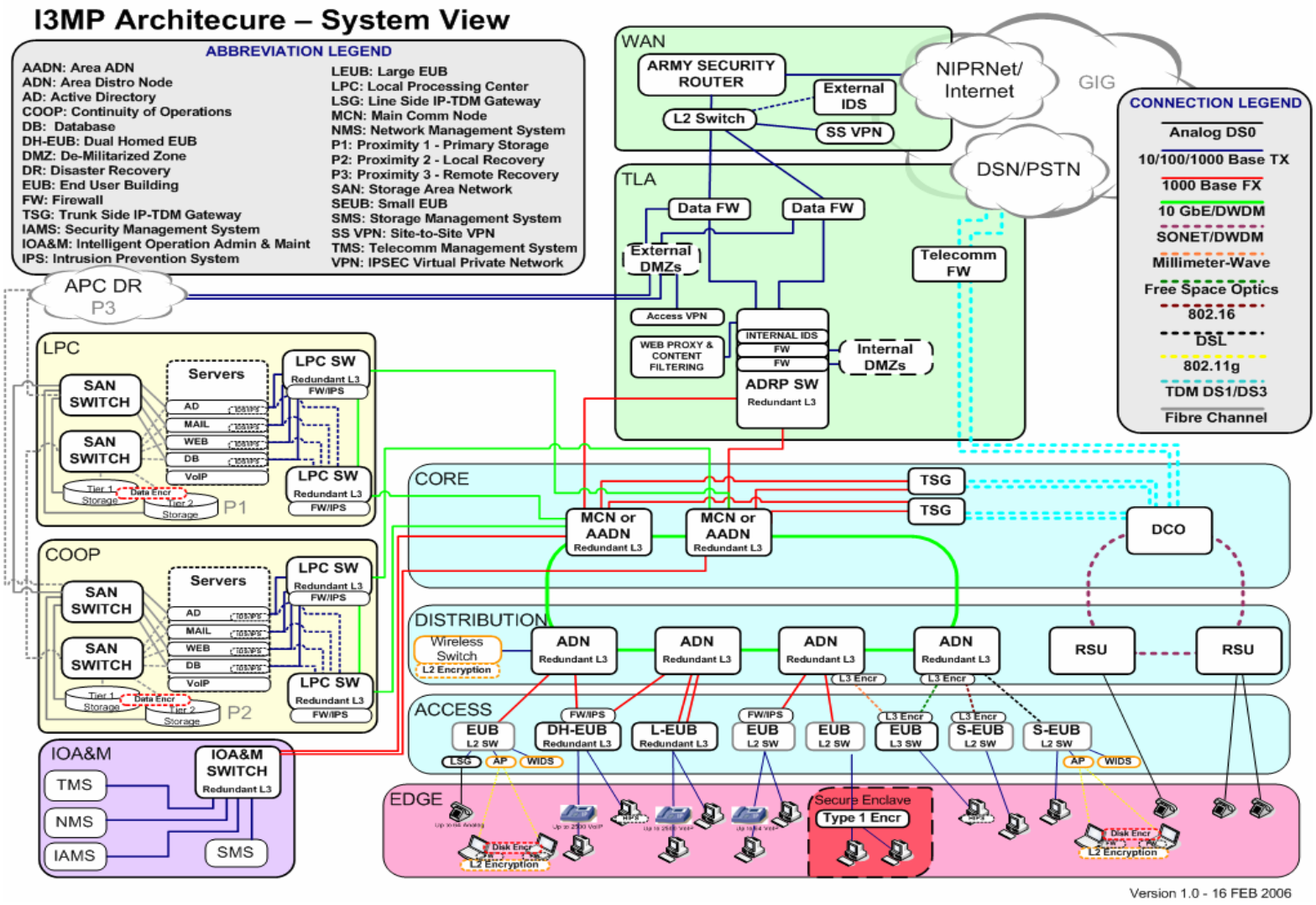

Figure B-1. I3MP Architecture – System View

This page intentionally left blank

GLOSSARY. ACRONYMS AND ABBREVIATIONS

ACL	Access Control List
ADRP	Army DISN (Defense Information Systems Network) Router Program
APC	Army Processing Center
APL	Approved Products List
ASD(NII)	Assistant Secretary of Defense (Networks and Information Integration)
ASR	Army Secure Router
CAC	common access card
CIO	Chief Information Officer
CIO-EB	Chief Information Officer-Executive Board
CSE	Critical Skill Expert
DDNS	Dynamic Domain Name Service
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DISN	Defense Information Systems Network
DISR	DOD (Department of Defense) IT (Information Technology) Standards Registry
DITO	DOD (Department of Defense) IPv6 (Internet Protocol version 6) Transition Office
DNS	Domain Name Service
DOD	Department of Defense
DOIM	Director of Information Management
DSN	Defense Switched Network
EUB	end-user building
FIPS	Federal Information Processing Standard
FY	Fiscal Year
GIG	Global Information Grid
HP	Hewlett-Packard
I3MP	Installation Information Infrastructure Modernization Program
IA	Information Assurance
IDS	intrusion detection system
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

ITSG	Information Technology Standards Guidance
JTA	Joint Technical Architecture (superseded by the DISR)
L2	Layer 2
L3	Layer 3
LAN	local area network
LPC	local processing center
MCN	Main Core Node
NETCOM	Network Enterprise Technology Command
NIAP	National Information Assurance Partnership
NIPRNet	Non-classified Internet Protocol Router Network
NLT	no later than
NSA	National Security Agency
OMB	Office of Management and Budget
OS	operating system
OSPF	Open Shortest Path First
PKI	Public Key Infrastructure
POM	program objective memorandum
SMS	Storage Management System
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TIC	Technology Integration Center
TLA	Top-Level Architecture
U.S.	United States
USAISEC	U.S. Army Information Systems Engineering Command
VLAN	virtual local area network
VPN	virtual private network