Security in an IPv6 Environment

Daniel Minoli • Jake Kouns

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Security in an IPv6 Environment

OTHER TELECOMMUNICATIONS BOOKS FROM AUERBACH

Active and Programmable Networks for Adaptive Architectures and Services
Syed Asad Hussain
ISBN: 0-8493-8214-9

Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications
Subir Kumar Sarkar, T.G. Basavaraju,
and C. Puttamadappa
ISBN: 1-4200-6221-2

Comprehensive Glossary of Telecom Abbreviations and Acronyms
Ali Akbar Arabi
ISBN: 1-4200-5866-5

Contemporary Coding Techniques and Applications for Mobile Communications
Onur Osman and Osman Nuri Ucan
ISBN: 1-4200-5461-9

Context-Aware Pervasive Systems: Architectures for a New Breed of Applications
Seng Loke
ISBN: 0-8493-7255-0

Data-driven Block Ciphers for Fast Telecommunication Systems
Nikolai Moldovyan and Alexander A. Moldovyan
ISBN: 1-4200-5411-2

Distributed Antenna Systems: Open Architecture for Future Wireless Communications
Honglin Hu, Yan Zhang, and Jijun Luo
ISBN: 1-4200-4288-2

Encyclopedia of Wireless and Mobile Communications
Borko Furht
ISBN: 1-4200-4326-9

Handbook of Mobile Broadcasting: DVB-H, DMB, ISDB-T, AND MEDIAFLO
Borko Furht and Syed A. Ahson
ISBN: 1-4200-5386-8

The Handbook of Mobile Middleware
Paolo Bellavista and Antonio Corradi
ISBN: 0-8493-3833-6

The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems
Lu Yan, Yan Zhang, Laurence T. Yang,
and Huansheng Ning
ISBN: 1-4200-5281-0

Introduction to Mobile Communications: Technology, Services, Markets
Tony Wakefield, Dave McNally, David Bowler,
and Alan Mayne
ISBN: 1-4200-4653-5

Millimeter Wave Technology in Wireless PAN, LAN, and MAN
Shao-Qiu Xiao, Ming-Tuo Zhou, and Yan Zhang
ISBN: 0-8493-8227-0

Mobile WiMAX: Toward Broadband Wireless Metropolitan Area Networks
Yan Zhang and Hsiao-Hwa Chen
ISBN: 0-8493-2624-9

Optical Wireless Communications: IR for Wireless Connectivity
Roberto Ramirez-Iniguez, Sevia M. Idrus,
and Ziran Sun
ISBN: 0-8493-7209-7

Performance Optimization of Digital Communications Systems
Vladimir Mitlin
ISBN: 0-8493-6896-0

Physical Principles of Wireless Communications
Victor L. Granatstein
ISBN: 0-8493-3259-1

Principles of Mobile Computing and Communications
Mazliza Othman
ISBN: 1-4200-6158-5

Resource, Mobility, and Security Management in Wireless Networks and Mobile Communications
Yan Zhang, Honglin Hu, and Masayuki Fujise
ISBN: 0-8493-8036-7

Security in Wireless Mesh Networks
Yan Zhang, Jun Zheng, and Honglin Hu
ISBN: 0-8493-8250-5

Wireless Ad Hoc Networking: Personal-Area, Local-Area, and the Sensory-Area Networks
Shih-Lin Wu and Yu-Chee Tseng
ISBN: 0-8493-9254-3

Wireless Mesh Networking: Architectures, Protocols and Standards
Yan Zhang, Jijun Luo, and Honglin Hu
ISBN: 0-8493-7399-9

AUERBACH PUBLICATIONS
www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

Security in an IPv6 Environment

Daniel Minoli • Jake Kouns

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-4200-9229-5 (Hardcover)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Minoli, Daniel, 1952-
Security in an IPv6 environment / authors, Daniel Minoli, Jake Kouns.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-4200-9229-5 (alk. paper)
1. Computer networks--Security measures. 2. Wireless communication systems--Security measures. 3. TCP/IP (Computer network protocol) I. Kouns, Jake. II. Title.

TK5105.59.M56 2009
005.8--dc22 2008044401

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the Auerbach Web site at
http://www.auerbach-publications.com

Dedication

For Anna (Dan)
and
For Jill, Elora, and my family (Jake)

Contents

Chapter 3

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Preface

Internet Protocol Version 6 (IPv6) is a technology now being deployed in various parts of the world that will allow truly explicit end-to-end device addressability. As the number of intelligent systems that need direct access expands to the multiple billions (e.g., including cell phones, PDAs, appliances, sensors/actuators/Smart Dust, and even body-worn bio-metric devices), IPv6 becomes an institutional imperative in the final analysis. The expectation is that by 2010 and beyond there will be increased use of IPv6. IPv6 is already gaining momentum globally, with major interest and activity in Europe and Asia, and there also is some traction in the United States. For example, in 2005 the U.S. Government Accountability Office (GAO) recommended that all agencies become proactive in planning a coherent transition to IPv6. Specifically, OMB Memorandum M-05-22 directed that agencies must transition from IPv4 Agency infrastructures to IPv6 Agency infrastructures (network backbones) by June 2008. Where specific agency task orders required connectivity and compliance with IPv6 networks, service providers needed to ensure that services delivered support federal agencies as required to comply with OMB IPv6 directives. All agency infrastructures had to be using IPv6 by June 30, 2008 (meaning that the network backbone was either operating a dual stack network core or it was operating in a pure IPv6 mode, i.e., IPv6-compliant and configured to carry operational IPv6 traffic) and agency networks must have interface with this infrastructure. This goal was actually met, implying that broader deployment is now likely.

Corporations and institutions need to start planning at this time how to kick off the transition planning process and determining how best coexistence can be maintained during the 3- to 6-year window that will likely be required to achieve the global worldwide transition, and this book addresses the migration and macro-level scalability requirements for this transition.

Security considerations continue to be critically important. With the increased number of mission-critical commercial and military operations being supported via distributed, mobile, always-connected, hybrid public–private networks, and with the increased number of attackers or inimical agents, it is mandatory that high-assurance security mechanisms be in place in all computing environments and in various layered modes.

Key questions are being asked about the security aspects and subtending apparatuses of IPv6. While there is a reasonably extensive open literature on the topic, there is currently no book that covers the topic in a systematic manner. This text pulls together and organizes this pool of knowledge in a logically organized manner. The basic material is based on or drawn from industry sources and RFCs. Some of the pragmatic considerations are based on the authors' own security experience. This text is *not* intended to be an exhaustive treatment of all topics related to IPv6 or IPv6 security, but a point of departure for a treatment of the topic. This text can be used by corporate and government professionals, developers, security stakeholders, and college instructors.

Even network/security administrators who operate in a pure IPv4 environment need to be aware of IPv6-related security issues, because there could be a compromise of security in these traditional networks if the administrators do not at least have a rudimentary understanding of IPv6 security principles, as we discuss in the text.

Consistent with the goal of providing a systematic treatment, this book covers the field in a terse and pragmatic manner. After an overview and introduction in Chapter 1, Chapters 2 and 3 provide a primer on IPv6. Chapter 4 discusses general security mechanisms and approaches. Chapter 5 discusses other IPv6 security features. Chapter 6 covers the fundamental topic of IPsec and its use in IPv6 environments. Chapter 7 looks at firewall use in IPv6 environments. Finally, Chapter 8 addresses security considerations for migration environments that may consist of mixed IPv4-IPv6 networks.

About the Authors

Daniel Minoli has many years of technical hands-on and managerial experience in networking, telecom, wireless, video, Enterprise Architecture, and security for global Best-In-Class carriers and financial companies. He has done extensive work in IPv6, including leading-edge topics such as Voice-over-IPv6 (work documented in the first text on the topic of *Voice Over IPv6—Architecting the Next-Generation VoIP,* Elsevier, 2006), satellite communications in an IPv6 environment (work documented in the first text on the topic of *Satellite Systems Engineering in an IPv6 Environment,* Auerbach Publications, Taylor & Francis Group, 2009), IPv4 to IPv6 migration of commercial and institutional networks (work documented in the *Handbook of IPv4 to IPv6 Transition Methodologies for Institutional & Corporate Networks,* Taylor & Francis, 2008) (coauthored)), and, security in general (work documented in the *Minoli–Cordovana Authoritative Computer and Network Security Dictionary,* Wiley, 2006 (coauthored)).

Mr. Minoli has worked at financial firms such as AIG, Prudential Securities, Capital One Financial, and service provider firms such as Network Analysis Corporation, Bell Telephone Laboratories, ITT, Bell Communications Research (now Telcordia), AT&T, Leading Edge Networks, Inc., and SES Americom, where he is director of Terrestrial Systems Engineering. SES is the largest satellite company in the world. He also played a founding role in the launching of two companies through the high-tech incubator Leading Edge Networks, Inc., which he ran in the early 2000s: Global Wireless Services, a provider of secure broadband hotspot mobile Internet and hotspot VoIP services; and InfoPort Communications Group, an optical and Gigabit Ethernet metropolitan carrier supporting Data Center/SAN/channel extension and Grid Computing network access services. For several years he has been Session-, Tutorial-, and now overall technical program chair for the IEEE ENTNET (Enterprise Networking) conference. ENTNET focuses on enterprise networking requirements for large financial firms and other corporate institutions.

Mr. Minoli has also written columns for *ComputerWorld, NetworkWorld*, and *Network Computing* (1985–2006). He has taught at New York University (Information Technology Institute), Rutgers University, and Stevens Institute of Technology (1984–2006). Also, he was a technology analyst at large for

Gartner/DataPro (1985–2001); based on extensive hands-on work at financial firms and carriers, he tracked technologies and wrote CTO/CIO-level technical scans in the area of telephony and data systems, including topics on security, disaster recovery, network management, LANs, WANs (ATM and MPLS), wireless (LAN and public hotspot), VoIP, network design/economics, carrier networks (such as metro Ethernet and CWDM/DWDM), and e-commerce. Over the years he has advised venture capitals for investments of $150M in a dozen high-tech companies. He has acted as expert witness in a (won) $11B lawsuit regarding a VoIP-based wireless air-to-ground communication system, and has been involved as a technical expert in a number of patent infringement proceedings.

Jake Kouns is a business-focused technology and information security executive with an extensive knowledge base and international experience. He focuses on the application of security concepts across a broad range on information technology areas including data communications, network design, operations, database structures, operating systems, application development, and disaster recovery. He holds numerous certifications including ISC2's CISSP, and ISACA's CISM and CISA.

Mr. Kouns is currently the director of Information Security and Network Services for Markel Corporation, a specialty insurance company. He has created and implemented a repeatable information security program from the ground up to ensure that risks are properly managed as part of normal business operations. Prior to his current role he was senior network security manager for Capital One Financial, a Fortune 200 financial institution where he provided technical management, consulting, architecture and design implementation for a wide array of security mitigating strategies. He was responsible for the day-to-day global security management of a large complex firewall environment, intrusion detection, risk assessment, and resolving incidents in a timely manner.

Mr. Kouns has twice presented for Check Point Software Technologies as an expert in global firewall management and intrusion detection. In recent years, Mr. Kouns' main focus has been spent redefining the information security vulnerability industry, and he has presented on the topic at many well-known security conferences including CanSecWest and SyScan. He has also been interviewed as an expert in the security industry by *Information Week, eWeek, Processor.com, Federal Computer Week, Government Computer News* and *SC Magazine.*

Mr. Kouns is co-founder and president of the Open Security Foundation (OSF), a 501(c)3 nonprofit organization that oversees the operations of the Open Source Vulnerability Database (OSVDB.org). OSVDB is an independent and open source database created by and for the community. The goal of the OSVDB project is to provide accurate, detailed, current, and unbiased technical information on security vulnerabilities. The project manages a master collection of computer security vulnerabilities, available for free use by the world's information security community.

Chapter 1

Introduction, Overview, and Motivations

1.1 Introduction and Motivations

IP Version 6 (IPv6), defined in the mid-1990s in Request for Comments (RFC) 2460 "Internet Protocol, Version 6 (IPv6) Specification" and a host of other more recent RFCs, is an "improved, streamlined, successor version" of IP version 4 (IPv4).* Because of market pull from the Office of Management and Budget's mandate that 24 major federal agencies in the U.S. Government (USG) be IPv6-ready by June 30, 2008, a goal that was met, and because of market pull from European and Asian institutions, IPv6 is expected to see gradual deployment from this point forward and in the coming decade. IPv6 is already gaining momentum globally, with major interest and activity in Europe and Asia and also some traction in the U.S; the expectation is that in the next few years a (slow) transition to this new protocol will occur worldwide. An IP-based infrastructure has now become the ubiquitous underlying architecture for commercial, institutional, and USG/Other (non-U.S.) Government (OG) communications and services functions. IPv6 is expected to be the next step in the industry evolution of the past 50 years from analog to digital to packet to broadband.

IPv6 offers the potential of achieving increased scalability, reachability, end-to-end interworking, Quality of Service (QoS), and commercial-grade robustness for data communication, mobile connectivity, and for Voice Over IP (VoIP)/triple-play networks. The current version of the Internet Protocol, IPv4, has been in use

* IPv6 was originally defined in [RFC 1883], [RFC 1884], and [RFC 1885], December 1995. [RFC 2460] obsoletes [RFC 1883].

successfully for almost 30 years and exhibits some challenges in supporting emerging demands for address space cardinality, high-density mobility, multimedia, and strong security. This is particularly true in developing domestic and defense department applications utilizing peer-to-peer networking. IPv6 is an improved version of IP that is designed to coexist with IPv4 while providing better internetworking capabilities than IPv4.

When the current version of the Internet Protocol (IPv4) was conceived in the mid-1970s and defined soon thereafter (1981), it provided just over 4 billion addresses. That is not enough to provide each person on the planet with one address without even considering the myriad of other devices and device modules needing addressability (such as, but not limited to, over 3 billion cell phones.) Additionally, 74% of IPv4 addresses have been assigned to North American organizations. The goal of developers is to be able to assign IP addresses to a new class of Internet-capable devices: mobile phones, car navigation systems, home appliances, industrial equipment, and other devices (such as sensors and Body-Area-Network medical devices). All of these devices can then be linked together, constantly communicating, even wirelessly. Projections show that the current generation of the Internet will "run out of space" in the near future (2010/2011) if IPv6 is not adopted around the world. IPv6 is an essential technology for ambient intelligence and will be a key driver for a multitude of new, innovative mobile/wireless applications and services [DIR200801].

IPv6 was initially developed in the early 1990s because of the anticipated need for more end system addresses based on anticipated Internet growth, encompassing mobile phone deployment, smart home appliances, and billions of new users in developing countries (e.g., in China and India). New technologies and applications such as VoIP, "always-on access" (e.g., Digital Subscriber Line and cable), Ethernet-to-the-home, converged networks, and evolving ubiquitous computing applications will continue to drive this need even more in the next few years [IPV200501].

IPv6 features, in comparison with IPv4, include the following [RFC0791]:

- Expanded Addressing Capabilities. IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels in the addressing hierarchy, a much greater number of addressable nodes, and simpler autoconfiguration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. A new type of address called an "anycast address" is also defined to be used to send a packet to any one of a group of nodes.
- Header Format Simplification. Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header.
- Authentication and Privacy Capabilities. In IPv6, security is built in as part of the protocol suite: extensions to support authentication, data integrity (encryption), and (optional) data confidentiality are specified for IPv6. The

security features of IPv6 are described in the Security Architecture for the Internet Protocol RFC 2401 [RFC2401], along with RFC 2402 [RFC2402] and RFC 2406 [RFC2406]; Internet Protocol Security (IPsec), defined in these RFCs, is required (mandatory). IPsec is a set of protocols and related mechanisms that supports confidentiality and integrity. (IPsec was originally developed as part of the IPv6 specification, but due to the need for security in the IPv4 environment, it has also been adapted for IPv4.)

- Flow Labeling Capability. A new feature is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service. Services such as VoIP and IP-based entertainment video delivery (known as IPTV) is becoming broadly deployed, and flow labeling, especially in the network core, can be very beneficial.
- Improved Support for Extensions and Options. Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

Figure 1.1 depicts the positioning of IPv6 in the overall protocol stack of typical end systems. End systems (such as PCs and servers), Network Elements (customer-owned or carrier-owned) and (perhaps) applications need to be IPv6-aware to communicate in the IPv6 environment. IPv6 has been enabled on many computing platforms. At this juncture, many operating systems come with IPv6 enabled by default; IPv6-ready Operating Systems (OS) include but are not limited to: Mac OS X, OpenBSD, NetBSD, FreeBSD, Linux, Windows Vista, Windows XP (Service Pack 2), Windows 2003 Server, and Windows 2008 Server. Java began supporting IPv6 with J2SE 1.4 (in 2002) on Solaris and Linux. Support for IPv6 on Windows was added with J2SE 1.5. Other languages, such as C and C++ also support IPv6.

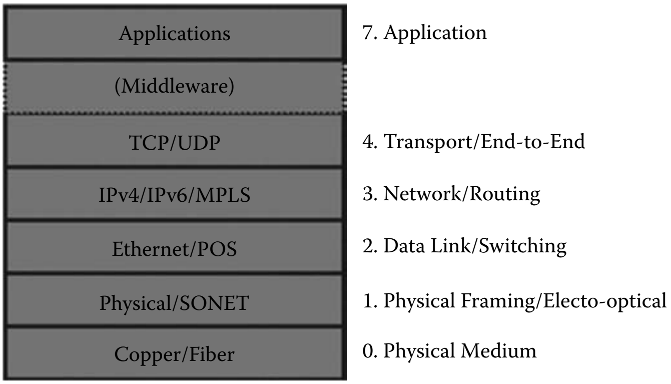


Figure 1.1 Typical communications stack.

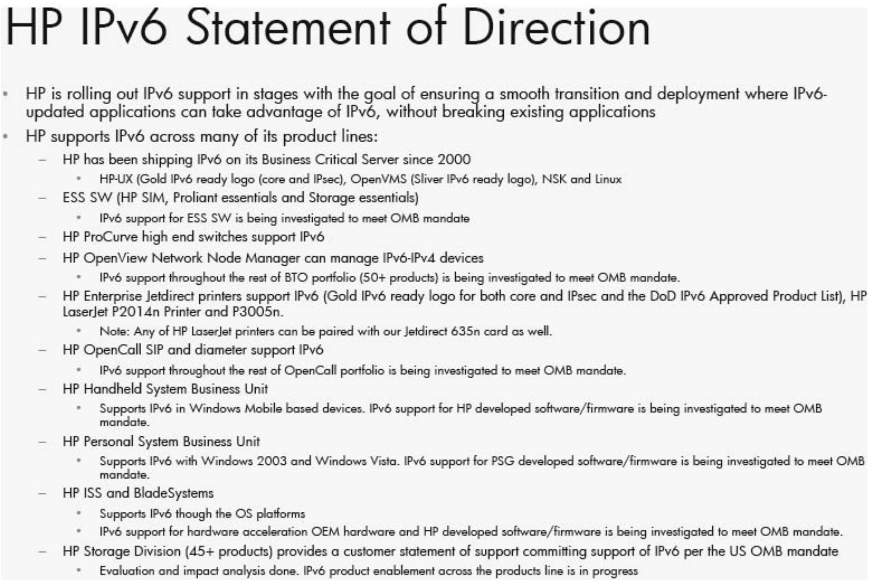
At this time, the number of applications with native IPv6 support is significant given that most important networking applications provide native IPv6 support. Hardware vendors including Apple Computer, Cisco Systems, HP, Hitachi, IBM, Microsoft, Nortel Networks, and Sun Microsystems support IPv6. Figure 1.2 depicts an example of a vendor's roadmap, to illustrate progress being made over the years in IPv6 support. One should note that IPv6 was designed with security in mind, but at the current time its implementation and deployment are (much) less mature than is the case for IPv4. When IPv4 was developed in the early 1980s, security was not a consideration; now a number of mechanisms have been added to address security considerations to IP. When IPv6 was developed in the early-to-mid 1990s, security was a consideration; hence a number of mechanisms have been built into the protocol from the get-go to furnish security capabilities to IP.*

Security considerations continue to be critically important in the networking and computing space. With the increased number of mission-critical commercial and military operations being supported via distributed, mobile, always-connected,

* Some purists will argue (perhaps as an exercise in semantics), that since IPsec is *available* also to IPv4, that IPv6 and IPv4 have the same level of security. We take the approach in this text that since the use of IPsec is mandated as required in IPv6 while it is optional in IPv4, that at *the practical, actual level*, "IPv6 is more secure." We know firsthand, for example, of credit card companies with extranets reaching numerous foreign locations that are supposed to be using encryption (IPsec) in their wide area IPv4 links when they do transborder transmission of sensitive personal credit card information, and in fact do not, on the excuse that their WAN routers are out of "bandwidth points" (well, just get new routers that can support such bandwidth points and protect sensitive personal credit card information). IPv6 mandates the use of IPv6, so if IPsec were used in this case, the encryption would be there by design or default.

Purists would argue philosophical points forever, but we approach the matter pragmatically: If State A mandated the use of helmets for motorcycle riders and State B does not, we believe statistics would show that riders are "safer" in State A by actual number of injuries and deaths; well, riders in State B always have the *option* of using helmets, but the question is "what do the actual accidents stats show?" If State A mandated the use of seatbelts for car riders and State B does not, we believe statistics would show that riders are "safer" in State A by actual number of injuries and deaths; well, riders in State B always have the *option* of using seatbelts, but the question is "what do the actual accidents stats show?" If State A mandated the use hardhats in construction sites and State B does not, we believe statistics would show that workers are "safer" in State A by actual number of injuries and deaths; well, workers in State B always have the *option* of using hardhats, but the question is "what do the actual accidents stats show?"

We believe that enough "ink on paper" has been spent here on this semantics issue and proceed by taking the position that, when everything else is equal, in a narrow abstract sense IPv6 is pragmatically more secure than IPv4. Naturally IPv6 is vulnerable to a multitude of attacks, infractions, compromises, and penetrations. That is precisely why these authors have written this book: because there is a need to lay out a plan, an approach, a strategy, a policy, and a set of tools to protect an IPv6-based infrastructure. The challenge is to make "everything else equal," equal firewall support, equal Intrusion Detection System (IDS) support, and so forth. Read on …



HP IPv6 Statement of Direction

- HP is rolling out IPv6 support in stages with the goal of ensuring a smooth transition and deployment where IPv6-updated applications can take advantage of IPv6, without breaking existing applications
- HP supports IPv6 across many of its product lines:
    - HP has been shipping IPv6 on its Business Critical Server since 2000
        - HP-UX (Gold IPv6 ready logo (core and IPsec), OpenVMS (Sliver IPv6 ready logo), NSK and Linux
    - ESS SW (HP SIM, Proliant essentials and Storage essentials)
        - IPv6 support for ESS SW is being investigated to meet OMB mandate
    - HP ProCurve high end switches support IPv6
    - HP OpenView Network Node Manager can manage IPv6-IPv4 devices
        - IPv6 support throughout the rest of BTO portfolio (50+ products) is being investigated to meet OMB mandate.
    - HP Enterprise Jetdirect printers support IPv6 (Gold IPv6 ready logo for both core and IPsec and the DoD IPv6 Approved Product List), HP LaserJet P2014n Printer and P3005n.
        - Note: Any of HP LaserJet printers can be paired with our Jetdirect 635n card as well.
    - HP OpenCall SIP and diameter support IPv6
        - IPv6 support throughout the rest of OpenCall portfolio is being investigated to meet OMB mandate.
    - HP Handheld System Business Unit
        - Supports IPv6 in Windows Mobile based devices. IPv6 support for HP developed software/firmware is being investigated to meet OMB mandate.
    - HP Personal System Business Unit
        - Supports IPv6 with Windows 2003 and Windows Vista. IPv6 support for PSG developed software/firmware is being investigated to meet OMB mandate.
    - HP ISS and BladeSystems
        - Supports IPv6 though the OS platforms
        - IPv6 support for hardware acceleration OEM hardware and HP developed software/firmware is being investigated to meet OMB mandate.
    - HP Storage Division (45+ products) provides a customer statement of support committing support of IPv6 per the US OMB mandate
        - Evaluation and impact analysis done. IPv6 product enablement across the products line is in progress

Figure 1.2 Illustrative roadmap.

hybrid public-private networks, and with the increased number of attackers or inimical agents, it is mandatory that high-assurance security mechanisms be in place in all computing environments and in various layered models. Given the avalanche of daily security threats being identified and directed at all sorts of corporate IT assets, ranging from PCs, midrange servers, mainframes, networks, storage systems, telecommunications and VoIP systems, and cell phones, to list just a few, the case for the effective proactive management of these IT and networking security risks does not require much motivation these days. Issues of concern include but are not limited to: interception, interruption, modification, and fabrication of corporate/institutional information. In general, infractions may entail inadvertent acts, deliberate nefarious acts, so-called Acts of God, technical failure, and management malfeasance/failure. Many agencies in USG/Department of Defense (DoD) are moving toward the introduction of next-generation systems to support collaborative architectures, geospatial application, net-centric warfare, mobility, and continuity of operations (COOP), as well as numerous other applications to better suit their mission; IPv6 security is critical to these stakeholders [JUN200801]. Attackers have already developed IPv6 Denial of Service (DoS) attacks and are exploiting weaknesses in IPv6/IPv4 tunneled networks. Tunneling is a key technique for transitioning between an IPv4 and an IPv6 environment. IPsec tunnels transit through normal firewalls or Network Address Translation (NAT) devices. It follows that tunneled IPsec traffic may contain malware, and so, new, appropriate security techniques are needed in IPv6 environments.

This recent quote is very revealing, if not alarming:

> Network administrators managing IPv4 networks often overlook or ignore IPv6. They typically do not recognize its presence or its availability, and they frequently lack the skills or expertise to manage it. So they assume it is not present on their networks. Unfortunately, this assumption is erroneous: IPv6 is available nearly anywhere IPv4 is available, because of transitional mechanisms defined by IETF [Internet Engineering Task Force]. Due to ignorance, lack of experience, and inertia, the security and administrative personnel tasked with defending IPv4 networks have not kept pace with the growth of IPv6. The underground community of black hats knows IPv6, and has developed the expertise to take advantage of it—especially given the relative lack of expertise on the part of the average network administrator. This expertise reflects a similar regional divide to the deployment of IPv6, with better IPv6 skills developing in parts of the world that are less rich in IPv4 technology [WAR200401].

Only a handful of organizations have developed principle-based security architecture frameworks intended to define the necessary elements of security. Most companies still take a fragmented, piecemeal view of security management, often even in the case of large Fortune 1000 firms. What is needed is a comprehensive framework for the uniform and organized treatment of all aspects of security facing an organization. This can be accomplished through a well-thought-out Security Architecture plan. An architecture is a blueprint for the optimal and target-conformant placement of resources in the Information Technologies (IT) environment for the ultimate support of the business function. A Security Architecture is an architecture plan that describes (a) the security services that a system is required to provide to meet the needs of its users, (b) the elements required to implement the services, and, (c) the behaviors of the elements (including the performance goals) to deal with the threat environment. Specifically, a Security Architecture includes administrative security, telecom and network security, computer security, emanations (radiation) security, personnel security, and physical security.

As part of an overall Security Architecture, organizations need security mechanisms to guard against network infractions, or breaches into a network to then use it as a vector to further compromise other IT assets. The industry has had about 20 years to develop layered approaches to network security in an IPv4 environment (the first firewall was developed in 1988). Key questions are now being posed about the security aspects and subtending apparatuses of IPv6. As the industry begins to migrate to IPv6, basic questions arise as to:

- What vulnerabilities do IPv6 networks have?
- What security mechanisms exist for IPv6?
- What differences exist between securing an IPv6 versus an IPv4 network?

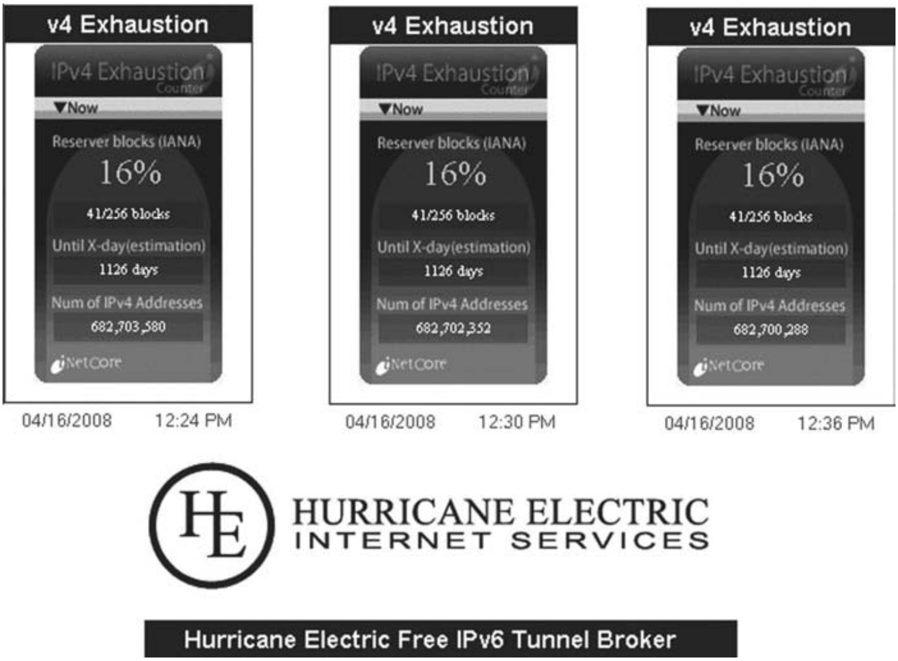
One challenge that institutions and USG agencies must face while transitioning to IPv6 is the context of security. "Security" has been presented by proponents as a motivating factor for transitioning to IPv6. In fact, security mechanisms and tools exist but the IETF is still working on and refining IPv6 security for Internet Control Message Protocol (ICMPv6), IPv6 firewalls, mobility, transition, and so on. In the final analysis, security approaches and issues in IPv6 are similar to security approaches and issues in IPv4. IPv6 faces many of the same risks associated with IPv4; in addition, IPv6 offers a number of new capabilities that could potentially result in additional vulnerabilities and threats to users. However, if properly implemented, IPv6 has the potential to provide a foundation for creating a secure infrastructure for an agency's enterprise as well as the Internet as a whole [JUN200801]. Prima facia security strengths of IPv6 are based on the *requirement* for IPv6 to implement IPsec [RFC2401], [RFC2402], [RFC2406], although, to date IPsec implementations are more readily available commercially in IPv4 routers and firewalls than in IPv6 devices. There are, however, some features of the protocol that reduce some specific threats (for example, fragmentation). By itself IPv6 is not a panacea for IP-level/network-level security concerns; nonetheless, IPv6 planners need to become aware of the issues, advantages, limitations, and the potential pitfalls. Corporations and institutions need to start planning the migration process and how coexistence of IPv4 and IPv6 networks can be maintained securely during the 2- to 5-year window that will likely be required to achieve the global worldwide transition.

It is critical that network and security engineers at large become IPv6-knowledgeable. There are some anecdotal indications that organizations may not be able to achieve the same security baseline for IPv6 networks as they are currently able to achieve for IPv4 networks [ICA200701]. Therefore, it is important that IPv6 planners begin to develop a baseline understanding of this space and the issues, opportunities, and challenges.

A presentation delivered during an open session at the July 2007 Internet Corporation for Assigned Names and Numbers (ICANN) Public Meeting in San Juan, Puerto Rico, made note of the accelerated depletion rate of IPv4 addresses and the growing difficulties the Regional Internet Registries (RIRs) are experiencing in allocating contiguous address blocks of sufficient size to service providers. Furthermore, the fragmentation in the IPv4 address space is taxing and stressing the global routing fabric, and the near-term expectation is that the RIRs will impose more restrictive IPv4 allocation policies and promote a rapid adoption of IPv6 addresses [ICA200701]. As of April 16, 2008, there were nominally 1,126 days before the IPv4 address space is depleted (IPv4 address space is expected to run out by 2012*). See Figure 1.3.

While there is a reasonably extensive open literature in the topic of IPv6 security, there is currently no book that covers the topic in a systematic manner. To this end, this book covers the field in a terse and pragmatic manner. After an

* There has been talk about reclaiming unused IPv4 space, saying that it would be a huge undertaking. A reclaiming of some portion of the IPv4 space will not help with the goal of providing an addressable IP address to appliances, cell phones, sensors (such as Smart Dust), surveillance cameras, Body Area Network devices, Unmanned Aerial Vehicle, and so forth.



v4 Exhaustion

IPv4 Exhaustion Counter

▼Now

Reserver blocks (IANA)

16%

41/256 blocks

Until X-day(estimation)

1126 days

Num of IPv4 Addresses

682,703,580

iNetCore

04/16/2008 12:24 PM

v4 Exhaustion

IPv4 Exhaustion Counter

▼Now

Reserver blocks (IANA)

16%

41/256 blocks

Until X-day(estimation)

1126 days

Num of IPv4 Addresses

682,702,352

iNetCore

04/16/2008 12:30 PM

v4 Exhaustion

IPv4 Exhaustion Counter

▼Now

Reserver blocks (IANA)

16%

41/256 blocks

Until X-day(estimation)

1126 days

Num of IPv4 Addresses

682,700,288

iNetCore

04/16/2008 12:36 PM

Figure 1.3 "...We have just three years until IPv4 addresses are depleted".

overview and introduction in Chapter 1, Chapters 2 and 3 provide a primer on IPv6. Chapter 4 discusses general network security mechanisms and approaches. Chapter 5 covers the fundamental topic of IPsec and its use in IPv6 environments. Chapter 6 discusses other IPv6 security features. Chapter 7 looks at firewall use in IPv6 environments. Finally, Chapter 8 addresses security considerations for migration environments that may consist of mixed IPv4-IPv6 networks.

1.2 IPv6 Overview

While the basic function of the Internet Protocol is to move information across networks, IPv6 has more capabilities built into its foundation than IPv4. A key capability is the significant increase in address space. For example, all devices could have a public IP address, so that they can be uniquely tracked.* Today inventory management of dispersed assets in a very large distributed organization such as the UAG DoD cannot be achieved with IPv4 mechanisms; during the inventory cycle someone has to manually verify the location of each desktop computer. With IPv6 one

* Note that this has some potential negative security issues as attackers could be able to own a machine and then exactly know how to go back to that same machine again. Therefore, reliable security mechanisms need to be understood and put in place in IPv6 environments.

can use the network to verify that such equipment is there; even non-IT equipment in the field can also be tracked by having an IP address permanently assigned. IPv6 also has extensive automatic configuration (autoconfiguration) mechanisms and reduces the IT burden by making configuration essentially plug-and-play (autoconfiguration implies that a Dynamic Host Configuration Protocol (DHCP) server is not needed or does not have to be configured). (Because IPv4 manual configuration is already a challenge in itself, one can understand that manually manipulating IPv6 addresses that are four times longer can be much more problematic). Corporations and government agencies will be able to achieve a number of improvements with IPv6. IPv6 can improve a firm's intranet, with benefits such as, but not limited to:

- Expanded addressing capabilities
- Serverless autoconfiguration (what some call plug-n-play) and reconfiguration
- Streamlined header format and flow identification
- End-to-end security, with built-in, strong IP-layer encryption and authentication (embedded security support with mandatory IPsec implementation)
- In IPv6, creating a VPN is easier and more standard than in IPv4, because of the (Authentication Header (AH) and Encapsulating Security Protocol (ESP)) Extension headers. The performance penalty is lower for the VPN implemented in IPv6 compared to those built in IPv4 [LIO199801]
- Enhanced support for multicast and QoS (more refined support for Flow Control and QoS for the near real-time delivery of data)
- More efficient and robust mobility mechanisms (enhanced support for Mobile IP and Mobile Computing Devices)
- Extensibility: improved support for feature options/extensions
- IPv6 makes it easy for nodes to have multiple IPv6 addresses on the same network interface. This can create the opportunity for users to establish overlay or Communities of Interest (COI) networks on top of other physical IPv6 networks. Department, groups, or other users and resources can belong to one or more COIs, where each can have its own specific security policy [JUN200801]
- Merging two IPv4 networks with overlapping addresses (say, if two organizations merge) is complex; it will be much easier to merge networks with IPv6
- IPv6 network architectures can easily adapt to an end-to-end security model where the end hosts have the responsibility of providing the security services necessary to protect any data traffic between them; this results in greater flexibility for creating policy-based trust domains that are based on varying parameters including node address and application [KAE200601]

IPv6 basic capabilities include the following:

- Addressing
- Anycast

- Flow labels
- ICMPv6
- Neighbor Discovery

Table 1.1 shows the core protocols that compose IPv6.

IP was designed in the 1970s for the purpose of connecting computers that were in separate geographic locations. Computers in a campus were connected by means of local networks, but these local networks were separated into essentially standalone islands. "Internet," as a name to designate the protocol and more recently the worldwide information network, simply means "inter network," that is, a connection between multiple networks. In the beginning, the protocol initially had only military use in mind, but computers from universities and enterprises were quickly added. The Internet as a worldwide information network is the result of the practical application of the Internet Protocol, that is, the interconnection of a large set of information networks [IPV200501]. Starting in the early 1990s, developers realized that the communication needs of the 21st century required a protocol with

Table 1.1 Key IPv6 Protocols

Protocol	*Description*
Internet Protocol version 6 (IPv6): RFC 2460	IPv6 is a connectionless datagram protocol used for routing packets between hosts.
Internet Control Message Protocol for IPv6 (ICMPv6): RFC 2463	A mechanism that enables hosts and routers that use IPv6 communication to report errors and send status messages.
Multicast Listener Discovery (MLD): RFC 2710, RFC 3590, RFC 3810	A mechanism that enables one to manage subnet multicast membership for IPv6. MLD uses a series of three ICMPv6 messages. MLD replaces the Internet Group Management Protocol (IGMP) v3 that is employed for IPv4.
Neighbor Discovery (ND): RFC 2461	A mechanism that is used to manage node-to-node communication on a link. ND uses a series of five ICMPv6 messages. ND replaces Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and the ICMPv4 Redirect message. ND is implemented using the Neighbor Discovery Protocol (NDP).

some new features and capabilities, while at the same time retaining the useful features of the existing protocol.

While link-level communication does not generally require a node identifier (address) since the device is intrinsically identified with the link-level address, communication over a group of links (a network) does require unique node identifiers (addresses). The IP address is an identifier that is applied to each device connected to an IP network. In this setup, different elements taking part in the network (servers, routers, desktop computers, etc.) communicate among each other using their IP address as an entity identifier. In version 4 of the Internet Protocol, addresses consist of four octets. For ease of human conversation, IP addresses are represented as separated by periods, for example, 166.74.110.83, where the decimal numbers are a shorthand for (and correspond to) the binary code described by the byte in question (an 8-bit number takes a value in the 0–255 range). Since the IPv4 address has 32 bits, there are nominally 2^{32} different IP addresses (approximately 4 billion nodes if all combinations are used). (The Domain Name System (DNS) also helped the human conversation in the context of IPv4; DNS is going to be even more critical in IPv6 and will have substantial impact on security administrators that use IP addresses to define security policies (e.g., firewalls)).

IPv4 has proven, by means of its long life, to be a flexible and powerful networking mechanism. However, IPv4 is starting to exhibit limitations, not only with respect to the need for an increase of the IP address space, driven, for example, by new populations of users in countries such as China and India, and by new technologies with "always connected devices" (DSL [Digital Subscription Lines], cable, networked PDAs, 2.5G/3G mobile telephones, etc.), but also in reference to a potential global rollout of VoIP. IPv6 creates a new IP address format, so that the number of IP addresses will not exhaust for several decades or longer even though an entire new crop of devices are expected to connect to the Internet.

IPv6 also adds improvements in areas such as routing and network autoconfiguration. Specifically, new devices that connect to the Internet will be plug-and-play devices. With IPv6, one is not required to configure dynamic non-published local IP addresses, the gateway address, the subnetwork mask, or any other parameters. The equipment, when plugged into the network, automatically obtains all requisite configuration data [IPV200501].

The advantages of IPv6 can be summarized as follows:

- Scalability: IPv6 has 128-bit addresses versus 32-bit IPv4 addresses. With IPv4, the theoretical number of available IP addresses is $2^{32} \sim 10^{10}$. IPv6 offers a 2^{128} space. Hence, the number of available unique node addressees is $2^{128} \sim 10^{39}$.
- Security: IPv6 includes security features in its specifications such as payload encryption and authentication of the source of the communication.
- Real-time applications: To provide better support for real-time traffic (e.g., VoIP), IPv6 includes "labeled flows" in its specifications. By means of this

mechanism, routers can recognize the end-to-end flow to which transmitted packets belong. This is similar to the service offered by MultiProtocol Label Switching (MPLS), but it is intrinsic with the IP mechanism rather than an add-on. Also, it preceded this MPLS feature by a number of years.

- Plug-and-play: IPv6 includes a plug-and-play mechanism that facilitates the connection of equipment to the network. The requisite configuration is automatic.
- Mobility: IPv6 includes more efficient and enhanced mobility mechanisms, which are important for mobile networks.*
- Optimized protocol: IPv6 embodies IPv4 best practices but removes unused or obsolete IPv4 characteristics. This results in a better-optimized Internet Protocol.
- Addressing and routing: IPv6 improves the addressing and routing hierarchy.
- Extensibility: IPv6 has been designed to be extensible and offers support for new options and extensions.

With IPv4, the 32-bit address can be represented as AdrClass|netID|hostID. The network portion can contain either a network ID or a network ID and a subnet. Every network and every host or device has a unique address, by definition. Basic NATing is a method by which IP addresses (specifically IPv4 addresses) are transparently mapped from one group to another. Specifically, private "non-registered" addresses are mapped to a small set (as small as 1) of public registered addresses; this impacts the general addressability, accessibility, and "individuality" of the device. Network Address Port Translation (NAPT), also referred to as Port Address Translation (PAT), is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. Together, these two methods, referred to as traditional NAT, provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses [RFC3022]. NAT is a short-term solution for the anticipated Internet growth phenomenon, and a better solution is needed for address exhaustion. There is a clear recognition that NAT techniques make the Internet, the

* Some of the benefits of IPv6 in the context of mobility include [YAI200001]: (i) Larger Addresses, which allow for new techniques to be used in order for the Mobile Node (MN) to obtain a care-of address; here, MNs can always get a collocated care-of address, a fact that removes the need for a Foreign Agent (FA). (ii) New Routing Header, which allows for proper use of source routing. This was not possible with IPv4. (iii) Authentication Header, which allows for the authentication of the binding messages. (iv) *Destination Options* Header, which allows for the use of options without significant performance degradation; performance degradation may have occurred in IPv4 because every router along the path had to examine the options even when they were only destined for the receiver of the packet.