This chapter covers the following subjects:

- **Reintroduction to IPv6:** Brief overview of IPv6
- **IPv6 Update:** Describes the current state of IPv6 adoption
- **IPv6 Vulnerabilities:** Describes the weaknesses in IPv6 that are key areas of focus
- **Hacker Experience:** Covers the current state of attack tools and skills
- **IPv6 Security Mitigation Techniques:** Introduces the high-level methods of securing IPv6

# 1

# Introduction to IPv6 Security

The Internet Protocol (IP) is the most widely used communications protocol. Because it is the most pervasive communication technology, it is the focus of hundreds of thousands of IT professionals like you. Because so many people rely on the protocol, the safety of communications is top of mind. The security research that is performed on IP is conducted by both benevolent and malevolent people. All the security research has caused many patches and adjustments to IP, as it has been deployed internationally. In hindsight, it would have been better if deeper consideration were given to the security of the protocol before it was extensively deployed.

This book provides you with insight into the security ramifications of a new version of IP and provides guidance to avoid issues prior to deployment. This chapter provides a brief background on this next version of IP, IPv6. You learn why it is important to consider the security for IPv6 before its wide-scale deployment. A review of the current risks and industry knowledge of the vulnerabilities is provided, as well as the common ways that IPv6 can be secured.

## Reintroduction to IPv6

The Internet Engineering Task Force (IETF) is the organization that is responsible for defining the Internet Protocol standards. When the IETF developed IPv4, the global expansion of the Internet and the current Internet security issues were not anticipated. In IPv4's original design, network security was only given minor consideration. In the 1980s, when IPv4 was developing, the "Internet" was constructed by a set of cooperative organizations. As IPv4 was developed and the Internet explosion took place in the 1990s, Internet threats became prolific. If the current environment of Internet threats could have been predicted when IPv4 was

being developed, the protocol would have had more security measures incorporated into its design.

In the early 1990s, the IETF realized that a new version of IP would be needed, and the Task Force started by drafting the new protocol's requirements. IP Next Generation (IPng) was created, which then became IPv6 (RFC 1883). IPv6 is the second network layer standard protocol that follows IPv4 for computer communications across the Internet and other computer networks. IPv6 offers several compelling functions and is really the next step in the evolution of the Internet Protocol. These improvements came in the form of increased address size, a streamlined header format, extensible headers, and the ability to preserve the confidentiality and integrity of communications. The IPv6 protocol was then fully standardized at the end of 1998 in RFC 2460, which defines the header structure. IPv6 is now ready to overcome many of the deficiencies in the current IPv4 protocol and to create new ways of communicating that IPv4 cannot support.

IPv6 provides several improvements over its predecessor. The advantages of IPv6 are detailed in many other books on IPv6. However, the following list summarizes the characteristics of IPv6 and the improvements it can deliver:

- **Larger address space:** Increased address size from 32 bits to 128 bits
- **Streamlined protocol header:** Improves packet-forwarding efficiency
- **Stateless autoconfiguration:** The ability for nodes to determine their own address
- **Multicast:** Increased use of efficient one-to-many communications
- **Jumbograms:** The ability to have very large packet payloads for greater efficiency
- **Network layer security:** Encryption and authentication of communications
- **Quality of service (QoS) capabilities:** QoS markings of packets and flow labels that help identify priority traffic
- **Anycast:** Redundant services using nonunique addresses
- **Mobility:** Simpler handling of mobile or roaming nodes

---

**NOTE** Remember the following IPv6 terminology:

- A *node* is any system (computer, router, and so on) that communicates IPv6.

- A *router* is any Layer 3 device capable of routing and forwarding IPv6 packets.
- A *host* is a node that is a computer or any other access device that is not a router.
- A *packet* is the Layer 3 message sourced from an IPv6 node destined for an IPv6 address.

During the development of IPv6, one of the requirements was that this new protocol must have flexible transition mechanisms. It should be easy to transition to this new protocol gradually, over many years. Because it was evident that IPv6 would become very popular, the transition would need to be slow and methodical.

Running both IPv4 and IPv6 at the same time, called *dual stack*, is one of the primary transition strategies. This concept describes the scenario in which a router supports two or more different routed protocols and forwards each type of traffic, independent of the behavior of the other routed protocol. Seasoned network engineers will recall the concept of "ships-in-the-night routing." This term refers to the fact that packets from either protocol can pass by each other without affecting each other or having anything to do with each other. Because "dual stacking" can be a dominant migration strategy, running a network with both protocols can open that network to attacks on both protocols. Attacks can also evolve that leverage a combination of vulnerabilities in IPv4 and IPv6.

In addition to dual stack, the transition to IPv6 involves various types of tunneling approaches where IPv6 is carried over IPv4 networks that have yet to migrate to IPv6. There will likely be attacks on the transition mechanisms themselves to gain access to either the IPv4 or IPv6 portions of a network. The security of IPv6 systems must be assessed before IPv6 is permitted to be enabled on current and future networks and systems.

Because IPv6 and IPv4 are both network layer protocols, many of the network layer vulnerabilities are therefore similar. However, because the protocol layers above and below the IP layer remain the same for either IP version, many of those attacks will not change. Because the two protocols are related, the similarities between the protocols can create similar attack patterns. IPv6 could improve security in some areas, but in other areas, it could also open new threats. Chapter 2, "IPv6 Protocol Security Vulnerabilities," focuses on the attacks against the IPv6 protocol itself and describes ways to protect against them.

IPv6 has continued to evolve since December 1998, when the IETF published RFC 2460. As the number of available IPv4 public addresses has reduced, IPv6 has become more attractive. In fact, IPv6 is the only viable solution to this IP address depletion problem. Many of the problems in current IPv4 networks relate to address conservation. For example, perpetuating the use of Network Address

Translation (NAT) and double-NAT is not a realistic long-term strategy for Internet expansion.

Today, the identity of users on the Internet is often unknown, and this has created an environment where attackers can easily operate. The use of anonymizer tools such as Tor and open proxies and the use of NAT allow users to hide their source IP addresses and allow hackers to operate without their targets knowing much about the source of the messages. NAT is often misunderstood as a security protection measure because it hides the internal addresses and thus obfuscates the internal network topology. Many network administrators feel a false sense of security and put too much faith in NAT. NAT breaks the use of the full end-to-end communication model that IP Security (IPsec) needs to be fully effective. The firewalls that perform the NAT function have difficulty maintaining the NAT state during failover. Troubleshooting application traffic that flows through a NAT is often difficult. When using IPv6, the use of NAT is not necessary because of the large amount of addresses available. Each node has its own unique address, and it can use that address for internal and external communications.

After the core, distribution, and access layers are dual-stack enabled, the computer systems themselves can be IPv6 enabled. After this takes place, the system administrators can start to enable IPsec tunnels between IPv6-enabled nodes to provide confidentiality and the integrity of the communications between systems. This provides a greater level of security over current unencrypted IPv4 implementations. IPsec deployments utilizing both authentication and encryption are rarely used today for computer-to-computer communication. Today the common method of using IPsec only encrypts the payload in tunnel mode because the NATs that are in place prevent authenticating the header. However, communications between critical systems can optionally be secured with IPv6 IPsec, using both authentication and encryption. Chapter 8, “IPsec and SSL Virtual Private Networks,” provides further details on how to secure IPv6 communications. IPv6 can uniquely provide this clear end-to-end secure communication because NAT is not needed when IPv6 can provide every node with a globally unique IP address.

# IPv6 Update

IPv6 is becoming a reality. The many years of early protocol research have paid dividends with products that easily interoperate. Several early IPv6 research groups have disbanded because the protocol is starting to move into the transition phase. The 6BONE (phased out with RFC 3701) and the KAME (http://www.kame.net) IPv6 research and development projects have wound down

and given way to more IPv6 products from a wide variety of vendors. Deployment of IPv6 is not a question of if but when. IPv6 is an eventuality.

The transition to IPv6 continues to take place around the world. The protocol is gaining popularity and is being integrated into more products. There are many IPv6-capable operating systems on the market today. Linux, BSD, Solaris, Microsoft Vista, and Microsoft Server 2008 operating systems all have their IPv6 stacks enabled by default, and IPv6 operates as the preferred protocol stack. Of course, Cisco equipment fully supports dual-stack configuration, and the number of IPv6 features within IOS devices continues to grow. However, the production use of IPv6 is still in the domain of the early adopters.

The rate of IPv6 adoption is growing but is also unpredictable. The timeline for the deployment of IPv6 is long and difficult to measure. Generally speaking, the transition to IPv6 has thus far been based on geography and politics. The Asian and European regions that did not have as many allocated IPv4 addresses have felt the pressure to transition to IPv6. While organizations in North America have more IPv4 addresses, the address-depletion effects are making the migration to IPv6 more urgent. The market segments that are focused on IPv6 are few and far between. There are few IPv6-specific applications that appeal to enterprises, service providers, and consumers that make them want to transition sooner. Some vertical markets such as government and defense, public sector, education, video distribution, and high tech are starting to see the benefits of IPv6 and are working on their transition plans.

There are still many areas of IPv6 where issues remain to be resolved. One of the remaining challenges for IPv6 is that few IPv6 service providers exist. Currently, Internet IPv6 traffic is still light compared to IPv4, but it continues to grow. This can be attributed to the lack of last-mile IPv6 access and customer premises equipment (CPE) that does not support IPv6. Multihoming, which is the concept of connecting to multiple service providers for redundancy, is an issue that will take some time to resolve, but it is doubtful that it is significantly holding back organizations from deploying IPv6. Hardware acceleration for IPv6 is not universal, and many applications lack IPv6 support. Just like the deployment of other networking technologies, network management and security are left to the end. The goal of this book is to raise awareness of the security issues related to IPv6 and to provide methods to secure the protocol before deployment.

# IPv6 Vulnerabilities

IPv6 will eventually be just as popular as IPv4, if not more so. Over the next decade as IPv6 is deployed, the number of systems it is deployed on will surpass those on IPv4. While early adopters can help flesh out the bugs, there are still

many issues to resolve. IPv6 implementations are relatively new to the market, and the software that has created these systems has not been field tested as thoroughly as their IPv4 counterparts. There is likely to be a period of time where defects will be found, and vendors will need to respond quickly to patching their bugs. Many groups are performing extensive testing of IPv6, so they hopefully can find many of the issues before it is time to deploy IPv6. However, all the major vendors of IT equipment and software have published vulnerabilities in their IPv6 implementations. Microsoft, Juniper, Linux, Sun, BSD, and even Cisco all have published vulnerabilities in their software. As IPv6 has been adopted, it is evident that these major vendors have drawn the attention of the hackers.

The early adopters of IPv6 technology are encouraged to tread lightly and make sure that security is part of their transition plans. There are distinct threats of running IPv6 on a network without any security protection measures. Some operating systems can run both protocols at the same time without the user's intervention. These operating systems might also try to connect to the IPv6 Internet without explicit configuration by the user. If users are not aware of this fact and there is no security policy or IPv6 security protections implemented, they are running the risk of attack. IPv6 can be used as a "backdoor protocol" because many security systems only secure IPv4 and ignore IPv6 packets. For these reasons, it is important to secure IPv6 before it is widely deployed.

When you consider the ways that an IPv4 or IPv6 network can be compromised, there are many similarities. Attacks against networks typically fall within one of the following common attack vectors:

- Internet (DMZ, fragmentation, web pages, pop-ups)
- IP spoofing, protocol fuzzing, header manipulation, session hijacking, man-in-the-middle, sniffing
- Buffer overflows, SQL injection, cross-site scripting
- Email (attachments, phishing, hoaxes)
- Worms, viruses, distributed denial of service (DDoS)
- Macros, Trojan horses, spyware, malware, key loggers
- VPN, business-to-business (B2B)
- Chat, peer-to-peer (P2P)
- Malicious insider, physical security, rogue devices, dumpster diving

In 2007, the Computer Security Institute (CSI — http://www.gocsi.com) 12th Annual Computer Crime and Security Survey stated that 59 percent of all survey

respondents suffered from insider abuse of network access. This percentage historically has been lower in the mid- to late 1990s and has risen steadily each year. So the percentage of internal attack sources is likely to be even higher today. Those internal sources of attacks could either be a legitimate hacker or an unknowing end user. The key issue is that most organizations do not spend 50 percent of their security budget on mitigating inside threats. Therefore, external as well as internal devices must be hardened equally well but not necessarily against the same types of attacks.

One disadvantage of both IP versions is the fact that the signaling of network reachability information takes place in the same medium as the user traffic. Routing protocols perform their communication in-band, and that increases the risks to infrastructure destabilization attacks. The threat mentioned here is that user traffic can affect the protocol-signaling information to destabilize the network. Protections against these types of attacks involve securing the signaling communications between network devices. IPv6 routing protocols can use encryption and authentication to secure the signaling information, even if it is transported inside the data path. Domain Name System (DNS) is another key infrastructure component that provides important signaling functions for IPv4 and IPv6. As seen over the past ten years, there is an increase in the number of attacks that target the infrastructure and DNS of the Internet and private networks. The attacks aim to create a denial of service (DoS), which affects the usability of the entire network.

Attacks against network elements typically come from the Internet for perimeter-based devices, while attacks on intranet devices originate from malicious insiders. Most internal routers have simple protection mechanisms like simple passwords and Simple Network Management Protocol (SNMP) community strings. Ease of management typically outweighs security in most enterprise networks. Internet routers do not enjoy this friendly environment, and they are constantly susceptible to many different forms of attack.

Routers are not usually capable of running traditional server software or other applications that can have vulnerabilities. However, they can be the target of a buffer overflow, where the attacker attempts to send information to the router to overrun an internal memory buffer. The side effects can be anything from erratic behavior to a software crash or gaining remote access. Any software that the router runs could be vulnerable, and any protocol supported and implemented within that software for communications to other devices is at risk for potential exploitation. Routers communicate over many different protocols, and each of those protocols is a potential target.

## Hacker Experience

As mentioned before, there is a lack of IPv6 deployment experience in the industry. There is also a lack of experience in securing an IPv6 network. That is why it is important to understand the issues with IPv6 and prepare your defenses. This should be done before IPv6 networks become a larger target for hackers. Not many IPv6 attacks exist or are publicly known, and there are few best practices for IPv6 security or reference security architectures for IPv6. However, a select few sophisticated hackers already use IPv6 for Internet Relay Chat (IRC) channels and back doors for their tools. Some DoS attacks are available and one IPv6 worm already exists, but there is little information available on new IPv6 attacks. It is fair to say that the current IPv6 Internet is not a big target for hackers. This is likely to change as the number of IPv6-connected organizations grows.

As IPv6 becomes more popular, it will continue to grow as a target of attacks, just as Microsoft software became more popular it became a larger target. Internet Explorer is a dominant web browser and experiences many attacks. As the Firefox web browser increased in popularity, so did the number of people working to find flaws in it. IPv6 will follow the same course as the number of deployments increases and it becomes a focus of new security research. The process of finding and correcting vulnerabilities will only make IPv6 stronger. However, because IPv6 has had so long to develop prior to mass adoption, the hope is that many of the early vulnerabilities have already been corrected.

The underground hacker community has started exploring IPv6. IPv6 is beginning to be well understood by these groups, and they are constructing tools that leverage weaknesses in the protocol and IPv6 stack implementations. Back doors that utilize IPv6 or IPv6 within IPv4 to obscure attacks and bypass firewalls are part of their repertoire. In fact, IPv6 capabilities have started to be added to several popular hacker tools.

Many of these IPv6 attack tools are already available and relatively easy to install and operate. Tools such as Scapy6 and the Hacker's Choice IPv6 Toolkit come to mind. These two tools are demonstrated in Chapter 2, which describes how these and other tools operate and discusses what risk they pose. This book illustrates the threats against IPv6 networks and describes how you can apply protection measures to neutralize these attacks.

---

**NOTE** Throughout this book, you will see the terms *attacker*, *hacker*, and *miscreant* used interchangeably to refer to malevolent forces that try to take advantage of IPv6 vulnerabilities. Attacks can be initiated by an outsider such as a *malicious user* or some *malicious host* that has been compromised and is being remotely controlled.

However, attacks also can be carried out by unknowing insiders who are not aware that they have just caused a problem.

# IPv6 Security Mitigation Techniques

IPv6 security architectures are not substantially different from those for IPv4. Organizations can still have the same network topologies when they transition to IPv6 as they have today. The network can still support the organization's mission, and the network can still have data centers, remote sites, and Internet connectivity, regardless of what IP version is being used.

With IPv6, the perimeter design has the same relevance as for IPv4, and most organizations can continue to have the "hard, crunchy" exterior and the "soft, squishy" interior networks. The problem is that most organizations put most of their effort into securing the perimeter, and they overlook the internal security of their environments. If these organizations considered the malicious insider threat, they might rethink the perimeter model and move to a model that has an even layer of security spread throughout. Many of these classic security paradigms still apply to IPv6 networks. When it comes to securing IPv6 networks, the following areas of an IT environment need to be protected:

- Perimeter protections from the Internet and external entities
- Secure remote-site connectivity with Virtual Private Network (VPN) technologies
- Infrastructure protection measures to ensure a secure network foundation
- Server security to protect the critical IT assets and data
- Client security measures to mitigate the insider threat

Over time, there will be changes in the way systems communicate with IPv6. Traffic patterns can change from being primarily client/server to being more peer-to-peer in nature. The use of anycast communications can add redundancy to communications but also make them less deterministic. Mobile IPv6 and tunnels can change the perimeter concept because there needs to be trusted nodes outside the perimeter. This can transform the perimeter into a more fuzzy and nebulous concept. Greater use of end-to-end encryption is needed to secure the different communication flows. Therefore, over time, the security architectures for IPv6 networks will transform to keep up with the way people communicate.

Standard IT security principles still apply when thinking about the security of IPv6 networks. Organizations should utilize multiple defensive strategies that support each other. Organizations should also have diversity in their defenses so that different types of protections help protect against multiple types of threats. Your defensive mechanisms are only as strong as the weakest link, so all parts of the protections should be fortified like a castle. A good example of this concept is to have a security architecture that has a perimeter and internal controls to not only mitigate the Internet threats but also the insider threats. Having both defense in depth and diversity of defense is like having "both a belt and suspenders" to prevent you from getting caught with your pants down. If you do not consider both for IPv6, you will have a network that is embarrassingly exposed to the elements.

The Cisco Self Defending Network (SDN) can also be a guide for protecting IPv6 networks. The SDN philosophies apply to IPv4 and IPv6 networks alike. The concepts of integration, collaboration, and adaptability are core capabilities of the self-defending network. Integrated security is the idea that security for networks should be inherent in the design and not added after the fact. This is very much the case with IPv6, where many devices have IPsec built in right from the start.

Collaboration between many diverse security solutions makes the security of the entire system more robust. IPv6 allows this form of collaboration because every node can have its own address and can easily communicate seamlessly across boundaries. Adaptability allows the security systems to respond dynamically to the situation at hand. IPv6 can provide the ability to communicate in new ways that can adapt to the needs of the users while providing security awareness. IPv6 can be the secure network platform that is the fundamental foundation of the Cisco Self Defending Network architecture.

The ways to protect IPv6 networks are much the same as those methods used to protect IPv4 networks. Concepts such as network perimeters, LAN security, remote-site communications and VPNs, infrastructure protection, server farm protection, and host/client security are all areas of focus for IPv6. The building blocks of a Self Defending Network include the following components:

- Endpoint protection
- Admission control
- Infection containment
- Intelligent correlation and incident response
- Inline Intrusion Prevention Systems (IPS) and anomaly detection
- Application security and anti-X defense

While not all of these technologies work seamlessly for IPv4 and IPv6, these are the types of components required for securing either IP version.

Few best practices exist for IPv6 deployment. As the Internet community continues to evolve IPv6 solutions, there will be solutions to the problems discovered through testing and trial deployments. IPv6 mailing lists, collaboration groups, the IETF v6ops working group, and interoperability testing organizations are deeply involved with gathering information on IPv6 deployment experiences. These organizations are experimenting with the early IPv6 solutions and documenting the best ways to implement IPv6. However, there are no current IETF Best Current Practices (BCP) for IPv6 security. As more is known about how IPv6 operates in live networks and more ways are found to secure it, the BCPs will develop.

Security risks can be mitigated through adequate training of the IT staff and the security administrators. Network professionals must understand the risks related to IPv6 and ensure that they are installing the correct protection mechanisms. Security policies need to be drafted or updated with the new security issues that IPv6 brings, and end users need security awareness training to help avoid unknowingly becoming insider threats.

Virtually all organizations rely heavily on their staff and their network security devices to protect their critical computer systems. Most organizations use firewalls, host-based and network-based intrusion prevention systems (IPS), antivirus software, and Security Information Management Systems (SIMS) to help monitor security events in this locked-down environment. Companies have spent a lot of money trying to secure their computer network infrastructure from invasion. This is primarily because there are weaknesses in the protocols and defects in applications used on computer networks that can be subverted by malicious individuals. While malicious individuals exploit weaknesses in protocols, unknowing individuals help propagate the threats by ignoring corporate security policy, guidelines, and standards.

IPv6 security devices need to be purchased when they are available and kept up to date so that when new IPv6 vulnerabilities are discovered, the computer systems are protected. Organizations are going to need IPv6-capable security products ahead of the deployment of IPv6. Firewalls are pervasive in today's networks, and there are several firewall solutions available for IPv6. However, in 2008, many IPSs and VPN concentrators do not support IPv6. The planning for the migration to IPv6 has been taking place for several years, but for now, much of the needed functionality does not exist. It can take a couple of years for there to be feature parity between IPv4 and IPv6 security products. Therefore, organizations should plan to upgrade their current security systems to achieve IPv6 functionality.

Instead of focusing on the theoretical security implications of IPv6, you should aim to implement the practical practices of securing a network based on the information that is available today. No one can yet claim extensive experience deploying all the IPv6 security mitigation techniques. For now, we can only discuss what is known to be true, based on limited deployment experiences. However, there is some certainty that the techniques shown in this book are effective based on the current knowledge of IPv6, testing, and experience securing computer networks.

## Summary

Effective security involves finding that perfect balance between protecting an asset and handling the extra burden security adds to doing business. The implementation of security should match the value of your assets and the acceptable level of risk. You should craft a security strategy that matches your level of risk. When it comes to IPv6, this means adjusting the security measures to fit the changes related to using a new network layer protocol. First you must understand the differences between IPv4 and IPv6 and know how those deltas have security implications. Next you must understand what vulnerabilities in IPv6 you must address. The final step is to implement security mitigation techniques to provide adequate coverage for your environment.

Even though the guidelines in this book are based on sound principles, they are not necessarily considered time-tested best practices. Just as IPv6 is in its early stages, the methods of securing IPv6 are rapidly changing. Because few IPv6 attacks exist, not all the future attacks are fully understood. Therefore, the guidelines in this book need to be customized to meet your organization's needs. Please do not just implement every command listed in this book. Rather, you should read the book, understand the threats, and then embark on using the correct techniques to secure your own IPv6 network.

## Recommended Readings and Resources

Cisco. *Deploying IPv6 in Branch Networks.* http://www.cisco.com/application/pdf/en/us/guest/netsol/ns107/c649/ccmigration_09186a00807753ad.pdf.

Cisco. *Deploying IPv6 in Campus Networks.* http://www.cisco.com/application/pdf/en/us/guest/netsol/ns107/c649/ccmigration_09186a00807753a6.pdf.

Cisco Self Defending Network (SDN) site, http://www.cisco.com/go/sdn.

Convery, Sean, and Darrin Miller. *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation* (v1.0). Cisco Systems Technical Report, March 2004. http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf.

Davies, Joseph. *Understanding IPv6.* Microsoft Press, November 2002.

De Capite, Duane. *Self-Defending Networks: The Next Generation of Network Security*. Cisco Press, August 2006.

Desmeules, Regis. *Cisco Self-Study: Implementing Cisco IPv6 Networks*. Cisco Press, May 2003.

Hagen, Silvia. *IPv6 Essentials*, 2nd Edition. O'Reilly and Associates, May 2006.

Internet Engineering Task Force (IETF) BCP Index, http://www.rfc-editor.org/bcp-index.html.

Internet Engineering Task Force (IETF) IPv6 Operations (v6ops) Working Group. http://www.ietf.org/html.charters/v6ops-charter.html.

Kaeo, Merike, David Green, Jim Bound, and Yanick Pouffary. *IPv6 Security Technology Paper*. North American IPv6 Task Force (NAv6TF) Technology Report, July 2006. http://www.nav6tf.org/documents/nav6tf.security_report.pdf.

Popoviciu, Ciprian P., Eric Levy-Abegnoli, and Patrick Grossetete. *Deploying IPv6 Networks*. Cisco Press, February 2006.

Richard Murphy, Niall, and David Malone. *IPv6 Network Administration.* O'Reilly and Associates, March 2005.

van Beijnum, Iljitsch. *Running IPv6.* Apress, November 2005.

Warfield, Michael H. *Security Implications of IPv6 Whitepaper*. Internet Security Systems, 2003. http://documents.iss.net/whitepapers/IPv6.pdf.