Int. J. of Advanced of Networking and Applications
Volume: 01, Issue: 04, Pages: 258-269 (2010)

IPv6 and IPv4 Security challenge Analysis and Best- Practice Scenario

Viney Sharma
Assistant Professor, Dept. of CSE, Anand Engineering College, Agra-282007
Email: vineyecstacy@rediffmail.com

ABSTRACT

Sharing of information and resources among different devices require networking. As networks are expanding day by day, Internet Protocols are gaining more and more popularity. Different transition mechanisms have been established and yet a lot of research is to be carried out. Internet Protocol version 6 (IPv6) is the next generation Internet Protocol proposed by the Internet Engineering Task Force (IETF) to supersede the current Internet Protocol version 4 (IPv4). To enable the integration of IPv6 into current networks, several transition mechanisms have been proposed by the IETF IPng Transition Working Group. This work examines and empirically evaluates two transition mechanisms, namely 6-over-4, and IPv6 in IPv4 tunneling, as they relate to the performance of IPv6.This paper outlines many of the common known threats against IPv4 and then compares and contrasts how these threats, or similar ones, might affect an IPv6 network. Some new threats specific to IPv6 are also considered. The current capabilities of available products are evaluated, as is how any inherent protocol characteristics of IPv6 affect the nature of the threat. This is prefaced by a brief overview of current best practices around the design of an IPv4 Internet edge network and then followed by a review of how that IPv4 edge network needs to evolve in order to secure the addition of IPv6.

Keywords: IPv4,IPv6,IPsec, Security,Transition mechanism

Date of Submission: December 08, 2009 Accepted: January 17, 2010

1 Introduction

IPv6 security is in many ways the same as IPv4 security. The basic mechanisms for transporting packets across the network stay mostly unchanged, and the upper-layer protocols that transport the actual application data are mostly unaffected. However IPv4 offers IPSec support, but it is optional. Support for IPSec in IPv6 implementations is not an option but a requirement. Because IPv6 mandates the inclusion of IP Security (IPsec), it has often been stated that IPv6 is more secure than IPv4. Although this may be true in an ideal environment with well-coded applications, but in other cases, the same problems that affect IPv4 IPsec deployment will affect IPv6 IPsec deployment. Therefore, IPv6 is usually deployed without cryptographic protections of any kind. Additionally, because most security breaches occur at the application level, even the successful deployment of IPsec with IPv6 does not guarantee any additional security for those attacks beyond the valuable ability to determine the source of the attack. IPSec is an Internet security protocol integrated into Layer 2 that is network layer to secure the network from the unauthorized users through origin Authentication, Data confidentiality and Data Integrity. Some significant differences, however, exist between IPv4 and IPv6 beyond the mandate of IPsec. These differences change the types of attacks IPv6 networks are likely to see. It is also unlikely that the average organization will migrate completely to IPv6 in a short timeframe; rather it will likely maintain IPv4 connectivity throughout the multiyear migration to IPv6. To date, however, there has not been a thorough treatment of the threats such networks will face and the design modifications needed to address these threats. IPv6 security is a large and complex subject. It is also one that has seen little assessment, except by the group who designed the protocol themselves. The paper focuses on the security requirements of medium to large edge networks on the Internet. These networks typically house some element of public services (Domain Name System [DNS], HTTP, Simple Mail Transfer Protocol [SMTP]) and a filtering router or firewall protecting their internal resources.

2. Security challenge Analysis

This section evaluates and compares threats in IP v4 and in IPv6. It is divided into two main sections, the first of which outlines attacks that significantly change as a result of IPv6, and the second summarizes attacks that do not fundamentally change.

2.1 Attacks with New Considerations in IPv6

The following nine attacks have substantial differences when moved to an IPv6 world. In some cases the attacks are easier, in some cases more difficult, and in others only the

method changes.

- Reconnaissance
- Unauthorized access
- Header manipulation and fragmentation
- Layer 3 and Layer 4 spoofing
- Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) attacks
- Broadcast amplification attacks (smurf)
- Routing attacks
- Viruses and worms
- Transition, translation, and tunneling mechanisms

2.1.1 Reconnaissance

In this attack the adversary attempts to learn as much as possible about the victim network. This includes both active network methods such as scanning as well as more passive data mining such as through search engines or public documents. The active network methods have the goal of giving the adversary specific information about the hosts and network devices used in the victim network, their interconnections with one another, and any avenues of attack that can be theorized based on the evaluation of this data.

2.1.1.1 IPv4 Considerations

In IPv4 the adversary has several well-established methods of collecting this information:

- Ping sweeps—By determining the IPv4 addresses in use at an organization , an adversary can systematically sweep a network with ICMP or Layer 4 "ping" messages that solicit a reply, assuming both query and response are not filtered at the network border. Following this scan, the adversary uses the data to formulate some hypothesis regarding the layout of the victim network.
- Port scans—After identifying reachable systems, the adversary can systematically probe these systems on any number of Layer 4 ports to find services both active and reachable. By discovering hosts with active services, the adversary can then move to the next phase.
- Application and vulnerability scans -- The Adversary can then probe these active ports by various means to determine the operating system and the version numbers of applications running on the hosts, and even test for the presence of certain well-known vulnerabilities.

Some tools such as Nmap can perform elements of all these scan types at the same time. Attack mitigation techniques for these reconnaissance techniques are generally limited to filtering certain types of messages used by an adversary to identify the resources of the victim network and trying to detect the reconnaissance activity that must be permitted. Reconnaissance activity cannot be stopped completely because the very act of permitting communications with your devices permits some form of reconnaissance.

2.1.1.2 IPv6 Considerations

This section outlines the differences in the reconnaissance attack when moved to IPv6. Because port and application vulnerability scans are identical after a valid address is identified, this section focuses on identifying valid addresses. The first subsection highlights technology differences independent of currently available technology and the latter outlines current capabilities in this area for the defender.

2.1.1.2.1 Technology and Threat Differences

With regard to technology, IPv6 reconnaissance is different from IPv4 reconnaissance [2] in two major ways. The first is that the ping sweep or port scan, when used to enumerate the hosts on a subnet, are much more difficult to complete in an IPv6 network. The second is that new multicast addresses in IPv6 enable an adversary to find a certain set of key systems (routers, Network Time Protocol [NTP] servers, and so on) more easily. Beyond these two differences, reconnaissance techniques in IPv6 are the same as in IPv4. Additionally, IPv6 networks are even more dependent on ICMPv6 to function properly. Aggressive filtering of ICMPv6 can have negative effects on network functions.

2.1.1.2.1.1 IPv6 Subnet Size Differences

The default subnet size of an IPv6 subnet is 64 bits or 2^{64} as compared to most common subnet size in IPv4 of 8 bits or 2^{8}. This increases the scan size to check each host on a subnet by $2^{64} - 2^{8}$. Additionally 64 bit address is derived based on the EUI-64 version of a host MAC address, or in the case of IPV6 privacy extensions, the number is pseudorandom and changes regularly. So a network that ordinarily required only the sending of 256 probes now requires sending more than 18 quintillion probes to cover an entire subnet. Even if we assume that sound network design principles are discounted and that the same 64-bit subnet now contains 10,000 hosts, that still means only one in every 1.8 quadrillion addresses is actually occupied . And even at a scan rate of 1 million probes per second , it would take more than 28 years of constant scanning to find the first active host, assuming the first success occurs after iterating through 50 percent of the first 1.8 quadrillion addresses. If we assume a more typical subnet with 100 active hosts, that number jumps to more than 28 centuries of constant 1-million-packet-per-second scanning to find that first host on that first subnet of the victim network. Now it should be noted that many variables can make this scanning easier for the adversary. First, public services on the Internet edge need to be reachable with DNS, giving the adversary at least a small number of critical hosts within the victim network to attack. Second, the large nature of IPv6 addresses and the lack of a strict requirement for Network Address Translation (NAT) [3] will cause more networks to adopt dynamic DNS or other mechanisms to ensure that even hosts have a valid DNS name. This means that a compromise of a DNS server within the organization under attack could yield large caches of hosts. Third, administrators may opt for easy-to-remember host addresses for key systems that could be entered into a database used by

the scanning tool. These easy-to-remember names could include simply mapping the decimal v4 last octet to the hex v6 last octet, because dual stack will be the norm for years to come. Fourth, by focusing on popular IEEE OUI designations for NIC vendors, an adversary could significantly reduce the number space of 2^{64}. Finally by exploiting poorly secured routers or other Gateway devices, an adversary could view the IPV6 neighbor – discovery cache data (the functional equivalent of an ARP cache) to find available hosts, or could simply turn on a packet-capture capability such as tcp dump to find addresses available to scan. Also, like in IPv4 networks, the internal hosts should be protected by a firewall that limits or completely prevents uninitiated conversations from reaching these systems. The implications of these larger subnets are significant. Today's network management systems often use ping sweeps as a method of enumerating a network for an administrator. New techniques need to be adopted for this purpose (perhaps neighbor cache checks on routers). Based on initial testing, the neighbor cache is populated on a router only when the device is communicated with by the router (such as sending off-net traffic). Additionally, this has potentially far-reaching implications for the way Internet worms are propagated, whether they are random address-based or use some form of hierarchical address designations. The basic assumption is that worms will have a much more difficult time propagating in the same manner as they have in IPv4.

2.1.1.2.1.2 New Multicast Addresses

IPv6 supports new multicast addresses that can enable an adversary to identify key resources on a network and then attack them. These addresses have a node, link, or site-specific domain of use as defined in RFC 2375 [9]. For example, all routers (FF05::2) and all DHCP servers (FF05::3) have a site-specific address. Although this setup clearly has a legitimate use, it is in effect handing the adversary an official list of systems to further attack with simple flooding attacks or something more sophisticated designed to subvert the device. Therefore, it becomes critical that these internal-use addresses are filtered at the border and not reachable from the outside.

2.1.1.2.2 Current Technology Capabilities

Today there is no known ping sweep tool for IPv6. Nmap, which supports ping sweeping in v4, elected not to support it in IPv6, most likely for the reasons outlined in section 3.1.1.2.1.1. On the detection side, some IDS systems today (host or network) do not support IPv6, making detection of the scanning activity difficult. This will improve as more vendors ship IPv6 inspection capabilities. Current versions of most popular network firewalls do support IPv6, meaning that filtering various messages to complicate the reconnaissance efforts of the adversary is possible. On the network management side, very few—if any—network management tools have been developed to deal with the host identification problem outlined in this section.

2.1.1.3 Candidate Best Practices

Based on the changes in reconnaissance attacks in IPv6, the following candidate best practices are suggested:

- Implement privacy extensions carefully—Although privacy extensions are a benefit from an obscurity standpoint regarding scanning attacks, they can also make it difficult to trace problems and troubleshoot issues on a network. If a network has a misbehaving host and that host's address changes regularly, it could be quite difficult to trace the exact host or to determine if the problems are from one host or many. Better options are to use static addresses for internal communication that are MAC address-based and pseudorandom addresses for traffic destined for the Internet. In addition, this makes current audit capabilities to track worms more challenging because when we track an infection back to a particular subnet, the privacy extensions rotation of the addresses or a machine reboot could make it difficult to identify the infected end host.

- Filter internal-use IPv6 addresses at organization border routers—Administrators can define site- local addresses for their organization, including specific multicast addresses such as the all-routers address FF05::2. These site-local addresses can potentially lead to new avenues of attack, so administrators must Filter these addresses at the organization's border routers.

- Use standard, but no obvious static addresses for critical systems—Instead of standardizing on host addresses such as ::10 or ::20, try something that is more difficult for adversaries to guess, such as ::DEF1 for default gateways. This is certainly a "security through obscurity" technique, but because it involves little additional effort on the administrator's part, its use has no drawbacks. The goal here is to make it difficult for the adversary to guess the global addresses of key systems. Standardizing on a short, fixed pattern for interfaces that should not be directly accessed from the outside allows for a short filter list at the border routers.

- Filter unneeded services at the firewall—Like in IPv4, your public and internal systems should not be reachable on services that they do not need to be reached on. Though some are hoping that tools such as IPsec will eliminate the need for firewalls, they will be around for years to come as Layer 3 and 4 filtering is well understood. Until some nontechnical issues (such as the international politics of who controls any trust roots) are resolved, wide-scale deployment of IPsec will be impractical for both IPv4 and IPv6.

- Selectively filter ICMP—Because neighbor discovery uses ICMP and fragmentation is done only on end stations (which requires path maximum-transmission-unit discovery [PMTUD]), it is imperative that some ICMP messages be permitted in IPv6. That said, nonessential ICMP messages can be filtered at a firewall, as can ICMP echo and echo-reply messages, if that aspect of manageability can be sacrificed. IPv6 requires ICMPv6 neighbor discovery-neighbor solicitation (ND-NS) and neighbor discovery-neighbor advertisement (ND-NA) messages to function (described in section 3.1.2), as well as router-

solicitation (RS)[4] and router-advertisement (RA) messages if auto configuration is used and RA messages are sent from the router for prefix lifetime advertisements. Finally, as in IPv4, packet-too-big messages should be broadly permitted to ensure proper functioning of PMTUD. Section 3.1.2.2.1.3 describes the ICMP messages required in more detail.

- Maintain host and application security—Although timely patching and host lockdown are critical elements in IPv4, they are even more critical during the early stages of IPv6 because many host protections (firewalls, IDSs, and so on) do not yet broadly support IPv6. Additionally, it is highly likely that the initial introduction of IPv6 into networks will result in some hosts not being properly secured. It is necessary to focus on maintaining host security to ensure that hosts that are compromised will not become stepping stones to compromise other end hosts.

2.1.2 Unauthorized Access

Unauthorized access refers to the class of attacks where the adversary is trying to exploit the open transport policy inherent in the IPv4 protocol. Nothing in the IP protocol stack limits the set of hosts that can establish connectivity to another host on an IP network. Attackers rely upon this fact to establish connectivity to upper-layer protocols and applications on internetworking devices and end hosts.

2.1.2.1 IPv4 Considerations

IPv4 networks have concentrated on limiting unauthorized access by deploying access control technologies within the end systems and on gateway devices in between the IPv4 endpoints. These controls can occur at both Layer 3 and Layer 4. The access control methods in IPv4 get more complex as you move up the protocol stack. At the IP layer, the defender uses basic access control lists (ACLs) to allow only approved hosts to send packets to a device. The ACLs are intended to limit access to or through a device based on security policy and by doing so, limit the available avenues of attack to specific services available on the network. In IPv4 networks, these access controls are implemented in networking devices and on end devices themselves (host firewalls). Although firewalls can implement security policy based on information in the IPv4 headers only, they are best used when combined with upper-layer inspection of TCP/UDP and application layer information.

2.1.2.2 IPv6 Considerations

The need for access control technologies is the same in IPv6 as in IPv4, though eventually the requirement for IPsec may enable easier host access control. The defender wants to limit the ability of the adversary to gain avenues of attack against services on an end host. The ability to do access control based in IPv6 changes not only the information that can be filtered in the Layer 3 header, but also the way the addressing and routing systems of IPv6 are architected. The addressing system of IPv6 changes from that for IPv4 because it includes the ability for one adapter in an IPv6-enabled node to have multiple IPv6 addresses. These multiple IPv6 addresses have significance for communicating on the local subnet (link local - FE80::/10), within an organization (site local – FC00::/16 or FD00::/16 pending working group decision), or on the Internet at large (global unicast addresses – aggregates of prefix binary 001). When the use of these address ranges is combined with the routing system, the network designer can limit access to IPv6 end nodes through IPv6 addressing and routing. For instance, with IPv6 the network designer can assign global unicast addresses [5] only to devices that need to communicate with the global Internet while assigning site-local addresses to devices that need to communicate only within the organization. Likewise, if a device needs to communicate only within a particular subnet, only the link-local address is needed. Additionally, the use of IPv6 privacy extensions, as mentioned earlier, can limit the time any single IPv6 address is accessible and exposed to a security threat. Beyond the previously stated differences in IPv6, the following sections outline the differences in the unauthorized access attack avenues when the network moves to IPv6. The first subsection highlights the technology differences in the IPv4 and IPv6 header that are independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

2.1.2.2.1 Technology and Threat Differences

In IPv6 the basic function of mitigating access to other IP devices based on policy is still implemented with firewalling and ACLs on end hosts and internetworking devices. However, numerous significant differences between the IPv6 and IPv4 headers may change how an administrator deploys these technologies. The following paragraphs discuss some of the areas of difference.

2.1.2.2.1.1 IPsec

When implemented with IPv4 or IPv6, IPsec has similar impacts on the administrator's ability to enforce security policy with IP header information. The following discussion points apply to both IPv4 and IPv6. If IPsec encryption is implemented from end to end, current firewalling technology is effective only in applying policy based on Layer 3 information because of the cryptographic protections. If IPv6 uses only the authentication header, it is conceivable that IPv6-capable firewalls could inspect the upper-layer protocols within the authentication-header (AH) encapsulation and permit or deny access to the packet based on that information.

2.1.2.2.1.2 Extension Headers

IP options in IPv4 are replaced with extension headers in IPv6. With this replacement, extension headers may be used in an attempt to circumvent security policy. For example, all IPv6 endpoints are required to accept IPv6 packets with a routing header. It is possible that in addition to accepting IPv6 packets with routing headers, end hosts also process routing headers and forward the packet. With this possibility, routing headers can be used to circumvent security policy implemented on filtering devices such as firewalls [10]. To avoid this possibility, the network manager should designate the specific set of nodes that are to act as MIPv6 home agents (typically the default router

for the subnet). The network designer should also validate that the operating systems within their organization do not forward packets that include the routing header. If operating systems that do forward packets that include the routing header are on the network, then the network designer must configure the network to filter the routing header on access control devices. If MIPv6 is not needed, packets with the routing header can be easily dropped at access control devices without relying on the end host to not forward the packets. Although it is easy to start with a "no MIPv6" policy, the emerging applications on handheld devices with WiFi access will make that stance challenging to maintain. For this reason it is best to make sure the end system policy is correctly implemented as "no-forwarding."

2.1.2.2.1.3 ICMP

ICMPv6 is an integral part of IPv6 operations, even more so than in IPv4. Current best practice for IPv4 firewalling of ICMP is sometimes debated, but it is generally accepted that stringent ICMP filtering is a best practice. In some extreme cases all ICMP messages should be filtered. This blanket prohibitive filtering is simply not possible in IPv6. For the purposes of this document, comparing and contrasting how a generic ICMPv4 policy would translate to ICMPv6 is critical. The following ICMPv4 messages are permitted through the firewall, and all others are denied. The general rules are to permit these inbound ICMP messages from the Internet to a DMZ on a firewall and deny ICMP to the firewall device. These rules may be more or less stringent than a given administrator's ICMP policy, but are included here only for the sake of demonstration.

- ICMPv4 Type 0 - echo reply
- ICMPv4 Type 3 Code 0 - Destination unreachable net unreachable
- ICMPv4 Type 3 Code 4 – Fragmentation needed but don't-fragment (DF) bit set
- ICMPv4 Type 8 - Echo request
- ICMPv4 Type 11 - Time exceeded

In contrast, an ICMPv6 firewall policy needs to support additional messages not only through the device but also to and from the firewall device.

ICMPv6 messages required to support equivalent functions to the firewall policy stated previously are as follows:

- ICMPv6 Type 1 Code 0 – No route to destination
- ICMPv6 Type 3 - Time exceeded
- ICMPv6 Type 128 and Type 129 - Echo request and echo reply

New IPv6 messages potentially required to be supported through the firewall device follow:

- ICMPv6 Type 2 - Packet too big—This is required for PMTUD to function correctly because intermediate nodes on an IPv6 network are not allowed to fragment packets. Though allowing PMTUD to function in IPv4 is useful, in IPv6 intermediary devices cannot fragment, so this message becomes more critical to proper network operations.
- ICMPv6 Type 4 - Parameter problem—This is required as an informational message if an IPv6 node cannot complete the processing of a packet because it has a problem identifying a field in the IPv6 header or in an extension header. Further research into the potential abuse of this message type is needed.

ICMPv6 messages potentially required to be supported to and from the firewall device are as follows:

- ICMPv6 Type 2 – Packet too big—The firewall device must be able to generate these messages for proper MTU discovery to take place, because the firewall device cannot fragment IPv6 packets.
- ICMP Type 130-132 - Multicast listener messages—In IPv4, IGMP would need to be permitted for multicast to function properly. In IPv6 a routing device must accept these messages to participate in multicast routing.
- ICMPv6 Type 133/134 – Router solicitation and router advertisement—These are necessary for a variety of reasons, most notably IPv6 end-node autoconfiguration.[6]
- ICMPv6 Type 135/136 – Neighbor solicitation and neighbor advertisement—These messages are used for duplicate address detection and Layer 2 (Ethernet MAC)-to-IPv6 address resolution.
- ICMPv6 Type 4 – Parameter problem—Refer to the previous explanation; this message may be required, but further research is warranted.

2.1.2.2.1.4 Multicast Inspection

Currently most IPv4 firewalls do minimal multicast inspection and filtering. Local-use multicast is integral to the functioning of IPv6. Firewall devices, at a minimum, need to allow the link-local multicast addresses to the firewall in order to provide neighbor discovery. Firewalls in Layer 3 mode should never forward link-layer multicasts. Devices acting as firewalls should inspect all source IPv6 addresses and filter any packets with a multicast source address.

2.1.2.2.1.5 Anycast Inspection

Additionally, although anycast as per RFC 2373 [11] is restricted to routers at this time, operating systems have started to add anycast support to their kernels. This could make anycast usage for services such as DNS or NTP [12] more prevalent in the short term. If this happens, any stateful device (firewall, network IDS [NIDS], server load balancing [SLB]) needs to make feature enhancements to its code to be able to designate an anycast address for inspection and origin servers that listen and respond to the anycast address. If this is done, then when a server that is serving an anycast service answers with its real address the stateful device can map the return traffic to the inbound-initiated traffic with the anycast address. Finally, as has been noted in [13], using IPsec and Internet Key Exchange (IKE) to secure anycast

communications has limitations. Work within the IETF is ongoing, but this requirement can potentially be addressed with the use of Group Domain of Interpretation (GDOI).

2.1.2.2.1.6 Transparent Firewalls

Several "Layer 2" or "transparent" firewalls on the market act as bridges while enforcing Layer 3 to Layer 7 policy. In current IPv4 networks, these devices have to be specially programmed to deal with a variety of IP and data link layer interactions such as ARP inspection and DHCPv4. In IPv6 these types of firewalls need to enhance their inspection capabilities to inspect the appropriate IPv6 ICMP and multicast messages. As discussed earlier, ICMPv6 is integral to the proper functioning of an IPv6 network, and a transparent firewall must be able to track the ICMPv6 messages that deal with neighbor discovery, duplicate address detections, auto configuration, and multicast management, just to name a few. These capabilities would offer a way to mitigate against attacks that spoof IP-to-MAC address bindings or spoofed DHCP messages. Refer to section 3.1.5 for more discussion on this topic. Additionally, security policy needs to be explicitly defined for the extensive use of multicast addresses in IPv6. For instance, a bridge must forward all FF02:: multicast in IPv6. An IPv6 transparent firewall must be able to define filters to forward the link local all multicast nodes (FF02::1) address that is used in IPv6 functions such as auto configuration.

2.1.2.2.2 Current Technology Capabilities

Though many IPv6-capable firewalls are available, many are implementing partial solutions for IPv6 for time-to-market reasons. For example, some IPv6 firewalls understand only a subset of the extension headers in IPv6, and they drop IPv6 traffic that includes these headers. An example is a firewall that does not have logic to process the routing header. If the firewall receives a packet with the routing header, it discards the packet. This behavior has some security benefit when the firewall is protecting hosts that might unpack and forward a packet with a routing header. However, this behavior precludes the firewall from being utilized in an environment that requires MIPv6.

2.1.2.3 Candidate Best Practices

Based on the differences in the IPv6 header and associated extension headers, the following candidate best practices are suggested:

- Determine what extension headers will be allowed through the access control device—Network designers should match their IPv6 policy to their IPv4 IP options policy. If any IPv4 IP options are denied on the access control device, the IPv6 access control device should implement the same policies. Additionally, administrators should understand the behavior of the end-host operating system when dealing with the extension headers and dictate security policy based on that behavior. For instance, as noted earlier, the administrator should validate that end-host operating systems do not forward packets that contain a routing header.
- Determine which ICMPv6 messages are required—It is recommended that administrators match their policy map closely to the equivalent ICMPv4 policy with the following additions:
  - ICMPv6 Type 2 - Packet too big
  - ICMPv6 Type 4 – Parameter problem
  - ICMPv6 Type 130-132 – Multicast listener
  - ICMPv6 Type 133/134 – Router solicitation and router advertisement
  - ICMPv6 Type 135/136 – Neighbor solicitation and neighbor advertisement

2.1.3 Header Manipulation and Fragmentation

The third category of attack is fragmentation and other header manipulation attacks. This category of attack has been primarily used for one of two purposes. The first purpose is to use fragmentation as a means to evade network security devices, such as NIDS or stateful firewalls. The second purpose of the attack is to use fragmentation or other header manipulation to attack the networking infrastructure directly.

2.1.3.1 IPv4 Considerations

In IPv4 fragmentation is a technique used to fit the IPv4 datagram into the smallest MTU on the path between end hosts. IPv4 fragmentation has been used as a technique to bypass access controls on devices such as routers and firewalls. Fragmentation also has been used to obfuscate attacks in order to bypass network security monitoring products such as NIDS. Most modern firewall and NIDS products go to great lengths to reassemble packets and match the reassembled packets to access control rules or to attack signatures. In general, large amounts of fragmented traffic have been used as an early indicator of an intrusion attempt because most baselines of Internet traffic indicate that the percentage of fragmented traffic is low.

2.1.3.2 IPv6 Considerations

This section outlines the differences in the fragmentation attacks when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

2.1.3.2.1 Technology and Threat Differences

IPv6 fragmentation by intermediary devices is prohibited per RFC 2460 (refer to sections 4.5 and 5). One of the most common fragmentation attacks uses overlapping fragments to obfuscate attacks from IPv4 security devices. In IPv6, overlapping fragments is not a proper way of handling fragmentation based on the rules outlined in RFC 2460; these fragments can possibly be viewed as an attack and dropped. Additionally, if the overlapping packets are allowed to bypass the security device, several end-host operating systems drop overlapping fragments in their IPv6 stack software. However, if the end operating system does accept overlapping fragments, there is nothing to prevent the

adversary from using fragmented packets in an attempt to bypass the IPv6 security device policy for similar purposes as the IPv4 fragmentation attacks. Additionally, an adversary can still use out-of-order fragments to try to bypass string signatures of a network-based IDS. RFC 2460 section 5 says "IPv6 minimum MTU is 1280 octets." For this reason, administrators can allow the security device to drop fragments with less than 1280 octets unless the packet is the last packet in the flow. Administrators can perform this action if the sending operating system fragments the original packet at the MTU supplied by the PMTUD messages and continues to create this size of IPv6 fragments until the last segment of the original packet is delivered. If the host operating system does not behave in this manner, then the security device has to continue to accept and process IPv6 fragments with less than 1280 octets. This behavior would continue to allow obfuscation of attacks by sending large amounts of small fragmented packets. Baselining the fragmentation and reassembly behavior of popular operating systems is necessary to validate the potential of this filtering. Additional fragmentation issues should be considered for devices that are not configured to do fragment reassembly (routers not running firewall), but are trying to enforce security policy based on Layer 3 and Layer 4 information. For example, in IPv4 some routers have the fragment keyword in the access control entry definition. The only packets that match this IPv4 ACL are those packets that have a fragment offset not equal to zero, that is, noninitial fragments. For IPv4 packets, we know the protocol fragments flags and offset values from the IP header, so we can easily calculate if enough of the upper-layer protocol is within the first fragment to determine the Layer 4 port number. So nonfragmented packets and first fragments go through the normal access-list process and can have the appropriate security policy applied. The combination of multiple extension headers and fragmentation in IPv6 creates the potential that the Layer 4 protocol is not included in the first packet of a fragment set, making it difficult to enforce Layer 4 policy on devices that do not do fragment reassembly. An example of this is a router running Cisco IOS Software without the firewall feature set that does fragment reassembly. With IPv6, Cisco IOS Software matches noninitial IPv6 fragments and the first fragment if the protocol cannot be determined. Cisco IOS Software also supports a new keyword "undetermined transport," which matches any IPv6 packet where the upper-layer protocol cannot be determined.

2.1.3.2.2 Current Technology Capabilities

Similar to IPv4, current IPv6 firewalls and IDSs implement fragment reassembly and other fragmentation checks in order to mitigate fragmentation attacks. These fragmentation checks include examining out-of- sequence fragments and switching these packets into order, as well as examining the number of fragments from a single IP given a unique identifier to determine denial-of-service attacks. IPv6 has no known fragmentation attack tools, but that does not eliminate the threat that such tools exist or can be created easily. Firewalls checking for these attacks will want to be matching on source subnets to catch the case where the adversary is using RFC 3041 addressing to generate fragment streams from what would appear to be multiple sources.

2.1.3.3 Candidate Best Practices

Though the handling of IPv6 fragmentation is specified to be much different than in IPv4, the threats in bypassing security devices remain the same. The following candidate best practices should be considered in IPv6 networks to limit the effectiveness of fragmentation attacks:

- Deny IPv6 fragments destined to an internetworking device when possible—This will limit certain attacks against the device. However, this filtering should be tested before deployment to ensure that it does not cause problems in your particular network environment.
- Ensure adequate IPv6 fragmentation filtering capabilities—The combination of multiple extension headers and fragmentation in IPv6 creates the potential that the Layer 4 protocol will not be included in the first packet of a fragment set. Security monitoring devices that expect to find the Layer 4 protocol need to account for this possibility and reassemble fragments.
- Drop all fragments with less than 1280 octets (except the last one)—RFC 2460 section 5 says "IPv6 minimum MTU is 1280 octets." For this reason security devices may be able to drop any IPv6 fragment with less than 1280 octets unless it is the last fragment in the packet. More testing is necessary in this area, as specified in section 3.1.3.2.1. A case that should be noted is for Layer 2 firewalls and IPv4 routers transporting a tunnel. There is no requirement that IPv6 packets be 1280 octets or more between Layer 3 interfaces, just that if the packet is fragmented, the fragments must be reassembled at the receiving interface before forwarding. This is done specifically to allow tunneling over IPv4 networks where the MTU might be less than 1280. In that case, IPv4 is architecturally Layer 2.

2.1.4 Layer 3-Layer 4 Spoofing

A crucial element enabling numerous different types of IP attacks is the ability for an adversary to modify their source IP address and the ports they are communicating on to appear as though traffic initiated from another location or another application. This so-called "spoofing" [15] attack is prevalent despite the presence of best practices to mitigate the usefulness of the attack.

2.1.4.1 IPv4 Considerations

Today in IPv4, spoofing attacks occur every day. They can make DoS, spam, and worm or virus attacks more difficult to track down. Layer 3 spoofing attacks are not generally used in interactive attacks as return traffic routes to the spoofed location, requiring the adversary to "guess" what the return traffic contains (not an easy proposition for TCP-based attacks because TCP has 32-bit sequence numbers). Layer 4

spoofing can be used in interactive attacks in order to make traffic appear to come from a location it did not (such as injecting false Simple Network Management Protocol (SNMP) messages or syslog entries). RFC 2827 [16] specifies methods to implement ingress filtering to prevent spoofed Layer 3 traffic at its origin. Unfortunately such filtering is not broadly implemented, and because it requires widespread usage to have a significant benefit, spoofed traffic is still very common. It is important to note that RFC 2827 ensures that only the network portion of an address is not spoofed, not the host portion. So in the 24-bit subnet 192.0.2.0/24, RFC 2827 filtering ensures that traffic originating from 192.0.3.0 is dropped but does not stop an adversary from spoofing all the hosts within the 192.0.2.0/24 subnet assigned to a broadcast domain. RFC 2827 does allow the administrator to track attacks to a particular organization, and tracking is one of the first steps to accountability. In addition to stopping the spoofing of valid ranges within the IPv4 address space, a large body of addresses have not been allocated [17] in IPv4, and reserved addresses exist that will likely never be allocated. These ranges can be globally blocked, and attacks that attempt to use those spoofed ranges can be identified and stopped at network choke points as implemented with a security policy.

2.1.4.2 IPv6 Considerations

This section outlines the differences in Layer 3 and Layer 4 spoofing attacks when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

2.1.4.2.1 Technology and Threat Differences

One of the most promising benefits of IPv6 from a Layer 3 spoofing perspective is the globally aggregated nature of IPv6 addresses. Unlike IPv4, the IPv6 allocations are set up in such a way as to easily be summarized at different points in the network. This allows RFC 2827-like filtering to be put in place by Internet service providers (ISPs) to ensure that at least their own customers are not spoofing outside their own ranges. Unfortunately this is not required standard behavior, and it requires conscious implementation on the part of operators. Layer 4 spoofing attacks are not changed in any way, because Layer 4 protocols do not change in IPv6 with regard to spoofing. Just be aware that subnets are much larger in IPv6, so even with RFC 2827-like filtering an adversary can spoof an enormous range of addresses. From a transition standpoint, the various tunneling mechanisms offer the ability for an adversary with either IPv4 or IPv6 connectivity to send traffic to the other version of IP while masking the true source. As an example, adversaries can use 6to4 relay routers to inject traffic into an IPv6 network with very little ability to trace back to the true source [19]. It should be noted that this is no worse than the inability to trace IPv4, but simple checks at the relay, such as making sure the outer IPv4 source matches the address embedded in the IPv6 source, enhances traceback from the IPv6 destination.

2.1.4.2.2 Current Technology Capabilities

Currently Layer 3 spoofing can be mitigated using the same techniques as in IPv4 with standard ACLs. Layer 4 spoofing is not changed in any way. Spoofed traffic can be detected using IPv6-capable firewalls or IDSs. Currently no techniques are available to mitigate the spoofing of the 64 bits of host address space available in IPv6. What would be useful in IPv6 networks (and IPv4 Networks as well) is a method to correlate IP, MAC, and Layer 2 port pairings for traffic. This data could be stored by the switch and then polled by or sent to a management station, enabling the operator to quickly determine the physical switch port on which a given IP address is communicating.

2.1.4.3 Candidate Best Practices

Based on the changes in Layer 3 and Layer 4 spoofing attacks in IPv6, the following candidate best practices are suggested:

- Implement RFC 2827-like filtering and encourage your ISP to do the same—At least containing spoofed traffic to the host portion of the IPv6 address provides a large benefit for at least tracing the attack back to the originating network segment.
- Document procedures for last-hop traceback—With the large range of spoofable addresses in a IPv6 subnet, it is critical that when an attack does occur you have mechanisms to determine the true physical source of the traffic. This generally entails some combination of Layer 2 and Layer 3 information gleaned from switches and routers.
- Use cryptographic protections where critical—if an application uses strong cryptographic protections, a successful spoof attack is meaningless without also subverting the cryptographic functions on the device.

2.1.5 ARP and DHCP Attacks

ARP and DHCP attacks attempt to subvert the host initialization process or a device that a host accesses for transit. This generally involves the subversion of host bootstrap conversations through either rogue or compromised devices or spoofed communications. These attacks try to get end hosts to communicate with an unauthorized or compromised device or to be configured with incorrect network information such as default gateway, DNS server IP addresses, and so on.

2.1.5.1 IPv4 Considerations

DHCP uses a broadcast message from the client when it initially boots up, allowing a rogue DHCP server to attempt to respond to the host before the valid DHCP server is able to. This allows the rogue server to set critical connectivity settings, including default gateway and DNS server, thus enabling man-in-the- middle attacks. Additionally, DHCP messages can be spoofed, allowing an adversary to consume all available DHCP messages on the server. ARP attacks center around spoofing ARP information to cause the IP-MAC binding of a particular host to be changed so that the IP address remains valid but the victims communicate with

the adversary's MAC address. This is most often done to spoof the default gateway. Technologies have been developed in IPv4 to address some of these attack types. For example, Cisco has a feature in Ethernet switches called DHCP snooping, which allows certain ports designated as "trusted" to participate in DHCP responses while most of the other ports are configured to allow sending only DHCP client messages. Additionally, a feature called ARP inspection performs similar protections for ARP. Furthermore, some IDS systems can detect certain types of ARP misuse.

2.1.5.2 IPv6 Considerations

This section outlines the differences in ARP and DHCP attacks when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

2.1.5.2.1 Technology and Threat Differences

In IPv6, unfortunately, no inherent security is added on to the IPv6 equivalents of DHCP or ARP. Because stateless auto configuration (a lightweight DHCP-like functionality provided in ICMPv6) can provide a viable alternative to DHCP[16] in many cases, dedicated DHCP servers are not common in IPv6 and are not even broadly available in modern server operating systems. Dedicated DHCPv6 servers may appear in order to offer additional configuration parameters such as DNS servers, time servers, IP telephony servers, and so on, so a level of DHCP protection is still required. Unfortunately, stateless auto configuration messages can be spoofed, and spoofing can be used to deny access to devices. To mitigate this, the trusted port concept should be used in conjunction with router-advertised messages. In IPv6, rather than continue with a unique version of ARP for every media type, ARP is replaced with elements of ICMPv6 called neighbor discovery. Neighbor discovery has the same inherent security as ARP in IPv4. Though the possibility of enabling some sort of more secure neighbor discovery using IPsec exists, this is far from standardized, and it involves unique implementation considerations because of the added security. The Securing Neighbor Discovery (SEND) working group in the IETF is working on a solution to this problem. At present, both router and neighbor-solicitation and -advertisement messages can be spoofed and will overwrite existing neighbor-discovery cache information on a device, resulting in the same issues present in IPv4 ARP. For instance, a spoofed router discovery could inject a bogus router address that hosts listen to and perhaps choose for their default gateway; the bogus router can record traffic and forward it through the proper routers without detection. These ARP spoofing-like attacks have not been implemented in any publicly available test code, so some unique considerations may appear after such code is released and tested. Although DHCPv6 is investigating security options, the protocol is too new to be considered in this paper. At a minimum the approaches used for protecting DHCP in IPv4 networks should be implemented for IPv6.

2.1.5.2.2 Current Technology Capabilities

No security tools are available today to help detect or stop DHCPv6, auto configuration, or neighbor- discovery abuses in IPv6. These messages can be filtered at a router or firewall like any ICMP message, but because most of these attacks are locally significant only, this will have minimal benefit. The neighbor-discovery attacks have not been implemented in any publicly available test code for IPv6, so some unique considerations may appear after such code is released and tested. Getting the equivalent inspection capability that is now present in IPv4 would help mitigate this threat.

2.1.5.3 Candidate Best Practices

Without the ability to detect the misuse of neighbor-discovery messages or to secure their transport, best practices are limited to the following:

- Use static neighbor entries for critical systems—In highly sensitive environments you can specify that a system has a static entry to its default router and avoid many of the typical neighbor-discovery attacks. This is a very administratively burdensome practice and should not be undertaken lightly.

2.1.6 Broadcast Amplification Attacks

Broadcast amplification attacks, commonly referred to as "smurf"[20] attacks, are a DoS attack tool that takes advantage of the ability to send an echo-request message with a destination address of a subnet broadcast and a spoofed source address, using the victim's IP. All end hosts on the subnet respond to the spoofed source address and flood the victim with echo-reply messages.

2.1.6.1 IPv4 Considerations

Documented in the late 1990s, this common attack has a simple mitigation method in IPv4 networks. If IPv4-directed broadcasts are disabled on the router, when an adversary sends an echo-request message to the broadcast address of the IP subnet they end up sending one echo-reply message to the victim, as opposed to replies from all the devices on the network. According to Best Current Practice (BCP) 34 [23], the default behavior for IP routers is to turn IP-directed broadcasts off. The command no ip directed broadcasts is the default for Cisco IOS Software Version 12.0 and later. This specific attack is becoming less common, but can still be used to create an effective DoS attack. A current website still monitors smurf attack-capable subnets.

2.1.6.2 IPv6 Considerations

This section outlines the differences in broadcast amplification attacks when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

2.1.6.2.1 Technology and Threat Differences

In IPv6 the concept of an IP-directed broadcast is removed from the protocol and specific language is added to the protocol designed to mitigate these types of attacks. Specifically with regard to a smurf attack, RFC 2463 [24] states that an ICMPv6 message should not be generated as a response to a packet with an IPv6 multicast destination address, a link-layer multicast address, or a link-layer broadcast address (RFC 2463 section 2.2). If end nodes are compliant to RFC 2463, then smurf and other amplification attacks used against IPv4 are not an issue in IPv6 networks.

2.1.6.2.2 Current Technology Capabilities

Our testing has shown that several popular operating systems comply with the RFC and do not respond to a echo request directed at the link-local all nodes multicast address sourced from a spoofed address. Some ambiguity still exists in the standard about whether end nodes should respond to ICMP messages with global multicast addresses as the source address. If the end nodes do respond to these multicast addresses, then an adversary could make an amplification attack on the multicast infrastructure that may cause a DoS due to resource consumption on the internetworking devices.

2.1.6.3 Candidate Best Practices

- Implement ingress filtering of packets with IPv6 multicast source addresses—There is no valid reason for a multicast source address, so the administrator should drop any packets with a multicast source address at the border of the network.

No other candidate best practices will be available until amplification attacks are discovered in IPv6. Specific testing needs to be performed on a range of operating system end nodes to determine their behavior when responding to an ICMP packet sourced with a global multicast address.

2.1.7 Routing Attacks

Routing attacks focus on disrupting or redirecting traffic flow in a network. This is accomplished in a variety of ways, ranging from flooding attacks, rapid announcement and removal of routes, and bogus announcement of routes. Particulars of the attacks vary, depending on the protocol being used.

2.1.7.1 IPv4 Considerations

In IPv4, routing protocols are commonly protected using cryptographic authentication to secure the routing announcements between peers. The most common implementation is a Message Digest Algorithm 5 (MD5) authentication with a preshared key between routing peers.

2.1.7.2 IPv6 Considerations

This section outlines the differences in several routing protocols underlying security mechanisms when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

2.1.7.2.1 Technology and Threat Differences

Several protocols do not change their security mechanism when transitioning from IPv4 to IPv6. Multiprotocol Border Gateway Protocol (BGP) was extended to carry IPv6 inter domain routing information in RFC 2545 . As such, BGP continues to rely on TCP MD5 for authentication. The Intermediate System-to-Intermediate System (IS-IS) protocol was extended in a draft specification to support IPv6, but the extension does not change the underlying authentication of IS-IS. Originally, IS-IS provided for the authentication of link-state packets (LSPs) through the inclusion of authentication information as part of the LSP. However, the simple password authentication was not encrypted. RFC 3567 adds a cryptographic authentication to IS-IS, and this cryptographic authentication will continue to be used to protect IS-IS for IPv6 traffic. In Open Shortest Path First Version 3 (OSPFv3), the authentication fields of the OSPF header are removed. Routing Information Protocol Next-Generation (RIPng) has also removed the authentication from the protocol specification. OSPF and RIPng rely on IPsec AH and Encapsulating Security Payload (ESP) headers to provide integrity, authentication, confidentiality, and antireplay protection of routing information exchanges. Additional work is being done to secure both IPv4 and IPv6 protocols, such as the “The Generalized TTL Security Mechanism” . This mechanism is also applicable to IPv6-specific protocols if the Hop-Limit field in the IPv6 header is used to protect a protocol stack.

2.1.7.2.2 Current Technology Capabilities

The security mechanisms to secure protocols that have changed with IPv6, OSPFv3, and RIPng are implemented inconsistently across internetworking vendors.

2.1.7.3 Candidate Best Practices

- Use traditional authentication mechanisms on BGP and IS-IS.
- Use IPsec to secure protocols such as OSPFv3 and RIPng—This is dependant on functioning vendor implementations.

Use IPv6 hop limits to protect network devices—Investigate vendor implementations of IPv6 hop limits to protect the protocol stack from attack. For instance, a basic technique is to start the time to live (TTL) of 255 for a valid peer and ensure that the resulting TTL accepted by the router is high enough to prevent acceptance of a spoofed packet that has come from a different part of the infrastructure.

2.1.8 Viruses and Worms

Viruses and worms remain one of the most significant problems in IP networking today, with almost all of the most damaging publicly disclosed attacks in recent years having a virus or worm at its nexus.

2.1.8.1 IPv4 Considerations

In IPv4, viruses and worms not only damage the hosts themselves but also can damage the transport of the network through the increased burden to routers and mail servers around the Internet. SQL slammer, for example, caused massive network flooding due in part to the rate with which it scanned the network (each attack packet was

a single UDP message). Timely patching, host antivirus, and early detection followed by perimeter blocking have been the three techniques used in IPv4. Early detection is most easily performed with anomaly detection systems such as those available from Arbor Networks. Additionally, newer host-based IDS products can intercept certain system calls that would have caused the compromise in the system.

2.1.8.2 IPv6 Considerations

This section outlines the differences in virus and worm attacks when moved to IPv6. The first subsection highlights technology differences independent of currently available technology, and the latter outlines current capabilities in this area for the adversary and the defender.

2.1.8.2.1 Technology and Threat Differences

A traditional virus in no way changes with IPv6. E-mail based viruses or those that infect removable media remain as you would expect. However, worms or viruses and worms that use some form of Internet scanning to find vulnerable hosts may experience significant barriers to propagation in IPv6 due to the issues raised in section 3.1.1. Further research is necessary to identify how significant a change this would be or what techniques the worm writer could employ to improve its propagation efficiency. It would seem that a SQL slammer-type worm would be far less effective in an IPv6 environment because of its inability to find hosts to infect and thus its inability to bring about the flooding result.

2.1.8.2.2 Current Technology Capabilities

The three mitigation techniques currently used in IPv4 are all still available in IPv6. There is not, however, broad IPv6 support in the host IDS products currently available. Additionally, the information provided by routers to aid in anomaly detection is not as extensive in IPv6 at this time.

2.1.8.3 Candidate Best Practices

Beyond establishing techniques to make local attack traceback easier, there are no best practice changes with virus and worm attacks. All the mechanisms from IPv4 (when the products support IPv6) work properly.

2.1.9 Translation, Transition, and Tunneling Mechanisms

Many efforts have been put on evaluating the security implications of the IPv4-to-IPv6 migration techniques. These techniques fall into the following categories:

- Dual stack • Tunneling • Translation

The existence of so many transition technologies creates a situation in which network designers need to understand the security implications of the transition technologies and select the appropriate transition technology for their network. The previous sections of this document assumed that the end hosts and networking infrastructure were dual stacked when discussing IPv6 native access. The following outlines some of the issues when the end hosts are not dual stacked and must rely on tunneling or translation technologies for IPv4 communications.[23]

2.1.9.1 Issues and Observations

- With regard to IPv6 tunneling technologies and firewalls, if the network designer does not consider IPv6 tunneling when defining security policy, unauthorized traffic could possibly traverse the firewall in tunnels. This is similar to the issue with Instant Messaging (IM) and file sharing applications using TCP port 80 out of organizations with IPv4.
- As noted in many of the transition studies done, automatic tunneling mechanisms are susceptible to packet forgery and DoS attacks. These risks are the same as in IPv4, but increase the number of paths of exploitation for adversaries.
- Tunneling overlays are considered nonbroadcast multiaccess (NBMA) networks to IPv6 and require the network designer to consider this fact in the network security design. The network designer must consider this when deploying automatic or static tunneling.
- Relay translation technologies introduce automatic tunneling with third parties and additional DoS vectors. These risks do not change from IPv4, but do provide new avenues for exploitation . These avenues can be limited by restricting the routing advertisements of relays to internal or external customers.
- Static IPv6 in IPv4 tunneling is preferred because explicit allows and disallows are in the policy on the edge devices.
- Translation techniques outlined for IPv6 have been analyzed and shown to suffer from similar spoofing and DoS issues as IPv4-only translation technologies.
- IPv6-to-IPv4 translation and relay techniques can defeat active defense traceback efforts hiding the origin of an attack.

When focusing on host security on a dual-stack device, be aware that applications can be subject to attack on both IPv6 and IPv4. Therefore, any host controls (firewalls, VPN clients, IDSs, and so on) should block traffic from both IP versions when a block is necessary. For example, when split tunneling is disabled on an IPv4 VPN client, that VPN client should block IPv6 split tunneling as well, even if the VPN service does not expressly support IPv6. IPv4 to IPv6 transition attack tools are already available that can spoof, redirect, and launch DoS attacks.

2.1.9.2 Candidate Best Practices

General recommendations for networks when considering IPv6-to-IPv4 transition techniques include the following:

- Use dual stack as your preferred IPv6 migration choice—Use either native IPv4 or IPv6 access to services but not translation because the security issues are better understood and policy implementations can be simplified.
- Use static tunneling rather than dynamic tunneling—This allows the administrator to establish a trust relationship between tunnel endpoints and continue to

implement inbound and outbound security policy.

- Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints—Examples are filtering outbound IP Protocol 41 for 6to4 tunneling and UDP port 3544 for Teredo-based tunneling.

3 Conclusions

IPv6 has both benefits and drawbacks from a security standpoint. The opportunity to ensure secure IPv6 deployments from the outset rather than a slow migration toward security, as occurred with IPv4, should be strongly considered by the Internet community. However, the amount of attention that IPv6 security has so far received is quite low, and new considerations will certainly be uncovered. Without adequate training and attention on the part of network operators to the new considerations with IPv6 security, it will be very difficult to ensure a smooth transition to IPv6. Further research in transition methodologies is required for successful transition to Next Generation Internet Protocol.

References

[1]. Richard L. Williams, GSA and IPv6 White Paper, February 2, 2004

[2]. Hanumanthappa J., Dr. Manjaiah D.H., IP V6 and IP V4 threat reviews with Automated Tunneling and configuration Tunneling Considerations Transitional Model:, IJCSIC, Vol. 3 No. 1 2009

[3]. Dr.Manjaiah.D.H. Hanumanthappa.J,2008, A Study on Comparison and Contrast between IPv4 and IPv6 Feature sets. In Proceedings of ICCNS'08, 2008, Pune,297-302.

[4]. Dr.Manjaiah.D.H. Hanumanthappa.J. 2009,IPv6 over Bluetooth: Security Aspects, Issues and its Challenges, In Proceedings of NCWNT-09,2009, Nitte - 574 110,Karnataka,INDIA –18-22.

[5]. Dr.Manjaiah.D.H.Hanumanthappa.J. 2009, Economical and Technical costs for the Transition of IPv4–to- IPv6 Mechanisms [ETCTIPv4 to ETCTIPv6], In Proceedings of NCWNT-09, 2009.

[6]. D. Waddington and F. Chang, "Realizing the Transition to IPv6," IEEE Communications Magazine, Vol.40, No.6, June 2002, pp.138-147.

[7]. S. Hagen, IPv6 Essentials, O'Reilly, July 2002.

[8]. K. Wang, A.K. Yeo and A.L. Ananda, "DTTS: a Transparent and Scalable Solution for IPv4 to IPv6 Transition," Proceedings of the tenth International Conference on Computer Communications and Networks, 2001, pp.248-253.

[9]. R. Gilligan, Transition Mechanisms for IPv6 Hosts and Routers, RFC2893, August 2000.

[10]. L. Zhou, V. Renesse and M. Marsh, "Implementing IPv6 as a Peer-to-Peer Overlay Network," Proceedings of the 21st IEEE Symposium on Reliable Distributed Systems, 2002, pp.347-351.

[11]. B. Carpenter and C. Jung, Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, RFC2529, March 1999.

[12]. C. Huitema, An Anycast Prefix for 6to4 Relay Routers, RFC3068, June 2001.

[13]. A. Durand, P. Fasano, I. Guardini and D. Lento, IPv6 Tunnel Broker, RFC3053, January 2001.

[14]. E. Nordmark, Stateless IP/ICMP Translation Algorithm (SIIT), RFC2765, February 2000.

[15] K. Tsuchiya, H. Higuchi and Y. Atarashi, Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS), RFC2767, February 2000.

[16] G. Tsirtsis and P. Srisuresh, Network Address Translation- Protocol Translation (NAT-PT), RFC2766, February 2000.

[17] S. Deering and R. Hinden "Internet Protocol, Version 6 Specification" RFC 2460, December 1998.

[18] R. John, et al. "Performance Implications of IPSec Deployment" w3.tmit.bme.hu /ips2004/papers/ips 2004_002.pdf, last accessed May 2004.

[19] S. Ariga, et al. "Performance Evaluation of Data Transmission Using IPSec over IPv6 Networks" http://www.isoc.org/inet2000/cdproceedings/1i/1i_1.ht m, last accessed June 2004.

[20] IPv6 Configurations and Test Lab for Windows XP, Windows XP White Paper, http://mail.cat.or.th/ipv6/ ipv6configs.doc, last accessed June 2004.

[21] IPv6 Transition Technologies, Microsoft Corporation, March 2004.

[22] IPv6 Deployment Strategies–Cisco, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ints olns/ipv6_sol/ipv6dswp.pdf, last accessed June 2004.

[23] C. Bouras et al, "The deployment of IPv6 in an IPv4 world and transition strategies" Internet Research: Electronic Networking Applications and Policy journal, 2003 Volume: 13 Number: 2 Page 86-93.

[24] B. Carpenter and K. Moore "Connection of IPv6 Domains via IPv4 Clouds" RFC 3056, February 2001.

[25] F. Templin et al "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", draft-ietf-ngtrans-isatap-03.txt, January 2002.

[26] Microsoft Windows 2003 Server, Help and Support documentation.

Authors Biography

Viney Sharma, working as Assistant Professor, Dept. of CSE, Anand Engineering College Agra, India for last ten years. I have Bachelor in Engineering in Computer Science from Sant Longowal Institute of Engineering & Technology, Longowal, Punjab and Master in Engineering in Computer Science from Dr. B. R. Ambedkar University, Agra in Hons. My research interest include Computer Networks, Operating Systems.