Global Information Assurance Certification Paper

IPv6 Enhancements and Endangerments

By Scott Sexton

March 28th, 2004

GIAC Certification GSEC Practical (Option 1) Version 1.4b

Table of Contents

ABSTRACT

This practical assignment briefly discusses the origins of IPv6, the next generation Internet protocol, describes some of the enhancements over the IPv4 protocol, educates on new transition mechanisms used in a dual protocol infrastructure and finally, suggest a defense in depth security strategy to protect against intrusion.

The HoneyNet Project has already documented a hacking event on their network using an IPv6 transition mechanism. Now is the time for security engineers and system administrators to implement a security policy that includes a defense in depth and diversity in defense that encompasses the IPv6, next generation Internet protocol.

INTRODUCTION

Law enforcement and security engineering share many points of commonality. Under current law and ethical conduct practices, both must be reactive, not proactive to the dangers that await them. Take for example a police officer working undercover, assigned a mugger detail, walking in public areas with a history of armed and strong-armed robbery (Internet). The officer knows his best bet at completing his shift in a safe manner is to pre-plan all scenarios (security policy) and have his defenses in place (defense in depth). He places himself in position as a decoy, postures himself to be the perfect victim, (honeypot) and waits for the inevitable bad guy to make his move. The officer accomplishes this by staying in line of site of his backup officers at all times (IDS), he is wearing a bullet proof vest, front and back panels (firewall filters, both sides), has his radio and hand signals for real time communication and emergencies, (alerts/logging) and is of course armed with pistol(s) and hand defense weapons (anti-virus/ /bugtraq). He uses his training, experience and gut instincts (security training, experience, bulletins, analysis) in choosing the best option to deploy at the moment he comes in contact with a bad guy. Bad guys come in two forms, the professional muggers (always was, is and will be a mugger) and the newbies (low on experience but high on enthusiasm). The professionals, (known hacker techniques) of course know the rules of the game, "everyone lives to play the game again". The real danger lies in interaction with the newbies (new hacker techniques). The newbies with their unconventional attack techniques, new tools, attacking unconventional/new targets, are a very serious threat. My paper provides a brief description, method of operation and suggestions for configuration against a potentially active "newbie", goes by the name of "IPv6", a.k.a. "IPng".

Origins

In December of 1993, RFC 1550 was published soliciting white papers on the subjects of suggested requirements and selection criteria for a new IP protocol,

referenced at that time as “IPng” or IP Next Generation. In December of 1995, RFC 1883 was released labeling the new version of the Internet protocol “IPv6.” The document specified the basic IPv6 header and initially defined IPv6 extension headers and options, packet size issues, the semantics of flow labels and priority, and the effects of IPv6 on upper-layer protocols.[1]

The IPV6 protocol deployment has begun in earnest in Europe, Asia and parts of South America and coincides directly with the deployment of new digital technology in those areas. IPv6 deployment is moving more slowly in North America due directly to the cost of replacing existing analog infrastructure with the digital enhancement. Infrastructure costs of upgrading the Internet’s backbone and supporting systems, few ISPs are currently utilizing IPV6.

> “It's certainly taking a long time," Margaret Wasserman, chairperson of the IPv6 working group of the Internet Engineering Task Force (IETF), told NewsFactor. "We thought we would run out of address space fairly soon. The use of NATs has slowed down the use of IP addresses. In the U.S. we see little or no pressure to move to IPv6**.”**[2]

However, major IPV6 deployment project are under way in North America and the U.S. Department of Defense (DoD) is planning to move from IPv4 to IPv6 by the year 2008. AT&T, Sprint, NTT, the University of New Hampshire - Interoperability Laboratory, the North American IPv6 Task Force (NAv6TF) and the Joint Interoperability Testing Command with other DoD agencies, are sponsoring a nationwide test of IPv6 called the Moonv6 Project. Approximately thirty organizations are participating in the project, donating their time, labor, and services. According to Jim Bound, Chairman of the U.S. North American IPv6 Task Force and an HP Fellow. By February (2004), five ISPs will have an IPv6 service for Moonv6 and two more ISPs will join the project [3]

The Moonv6 Project is open to any company who wants to test IPv6 however participations fees are required. Phase One of the project is complete and organizations are invited to participate in Phase Two.

Enhanced Features

The steadily increasing growth of the Internet has exposed the number one limitation of IPv4, the limit of unique address spaces available, maxxing out at 4.3 billion. The current size of the Earth’s population exceeds IPv4s ability to provide each person a unique IP address. Future demand for IP addresses will only increase due to the proliferation of personal devices such as PDAs, as well as

[1] RFC 1883, p.3.
[2] Ryan. p 1.
[3] Marsan. p. 2.

VOIP, RFID, wireless/mobile devices and online home appliances requiring access to the Internet. The use of CIDR, NAT, DHCP and aggregation has proven useful methodologies however the steady growth rate of demand on the routing infrastructure will soon result in total utilization of the available addresses.

Expanded Address Field

Address Field was expanded from 32 bits to 128 bits written in a sequence of eight sets of four hex digits and separated by colons. Rules that apply are leading zeroes in a group can be omitted, all zero groups can be replaced by "**::**" and only one such group can be replaced. The 128 bit IP address field is broken down into the following parts:

Public Topology

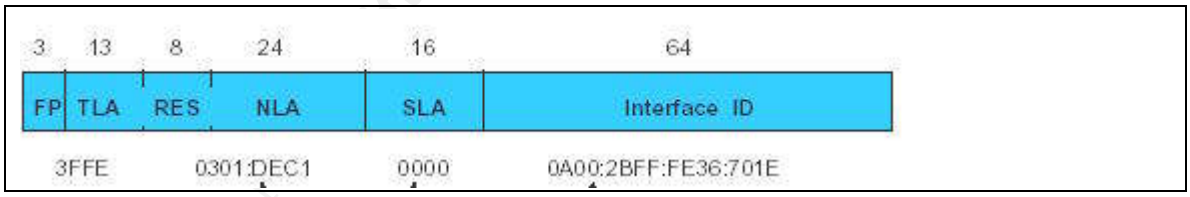
- Format prefix (3 bits)
- Top-level aggregation (13 bits), allocated by The Regional Internet Registries (RIRs) to providers
- Next-level aggregation (24 bits) used by ISP for subnetting to customers
- Reserved for future use (8 bits)

Site Topology

- Site-level aggregation (16 bits)

Interface ID

- Interface (64 bits) usually provided by the local LAN (unique on subnet).



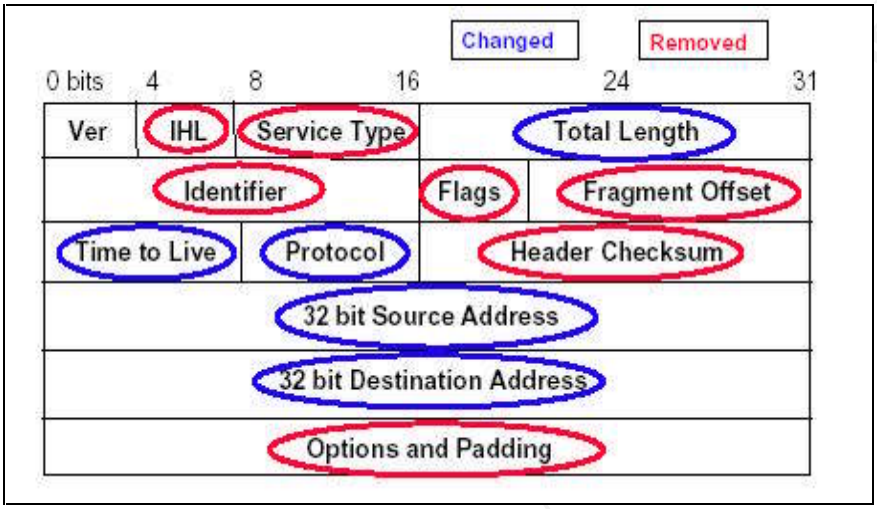
[4]

Routing No Longer Classless

IPv6 no longer uses address classes but instead assigns predefined address prefixes for unicast, multicast, LAN or local site address, and a method to include an IPv4 address into an IPv6 address.

[4] Muggeridge, p. 21.

IPv6 has removed several of the header fields that were not being used in IPv4 with all optional header information placed into extension headers. Multiple extension headers may be employed and are identified through the Next Header value in the previous packet. List of mandatory header fields include: traffic class at 8 bits, flow label at 20 bits, payload length at 16 bits or 0 (zero)for large payloads called a Jumbogram which requires additional info in the extended header, next header - 8bits, hop limit –set in hops, not seconds which replaces the Time To Live field. The field is lessened by one for each node that forwards the packet.



[5]

Checksums

The use of redundant checksums in IPv4 was eliminated in IPv6. If a checksum function is required, you may create an encrypted checksum using AH, ESP or AH/ESP with in an extension header.

Flow Labels and Priority Setting

A flow describes a sequence of packets sent from a set source to a set destination with a request for special handling such as real-time service by the routers. Packets that do not belong to a sequence of packets (flow) have a flow value of zero. A source address and a value other than zero identify the packet as part of a flow. A flow must contain the same source address, destination address and the same flow value.

The IPv6 header contains a 4-bit priority field that allows the source node the ability to prioritize packets sent from the same source address. The priority field has two ranges, 0-7 range specifies the priority of packets not in real time and the 8-15 range specifies the priority of real time packets

[5] Muggeridge, p. 33.

Authentication and Encryption

Another welcome enhancement in IPv6 is native support for IPSec. The IPSec Protocol Suite provides for the secure and reliable transmission of data by providing both authentication and encryption. IPSec support was added over time to the IPV4 protocol, out of necessity but with IPv6 it was a built in security feature from the inception. The security features are added in extension headers and if not required, may be turned off to reduce network overhead.

The Authentication Header (AH) can be used for integrity and data origin authentication. The sender places a generated digital signature into the header and the receiver validates the signature in the received field. The HMAC secret key algorithm provides the structure for inserting the hashing algorithms such as MD5 or SHA-1. No packets will be received without the digital signature providing authentication. IPv6 also supports Encapsulating Security Payload (ESP), which provides for authentication and encryption. The ESP field is inserted as a header into the payload, which selects the encryption parameters and scheme. ESP encrypts part of the ESP header field and the payload. ESP may be used alone or in conjunction with AH with both supporting extension headers. AH and ESP both require Security Associations to collaborate security parameters and algorithms (SPI in header) and are used extensively today to form secure VPN tunnel connectivity.

Dynamic Address Auto-Configuration

Address space limitation is remediated through transition mechanisms and auto-configuration methods. IPv6's auto-configuration methods are stateless using address auto-configuration (LAN), dynamic renumbering, multiple addresses and transition periods. Stateful connections are achieved using dynamic host configuration methods (DHCPv6).

Neighbor Discovery (ND) replaces the functionality of ARP, ICMP router discovery and ICMP redirect messages. Routers and hosts use the ND protocol to determine link-layer address. Hosts employ router discovery, prefix discovery and parameter discovery to determine current/new addresses and Internet parameters. Routers are configured to send neighbor address solicitations and to respond to neighbor address broadcasts. Current addresses have an assigned "time to live" and routers, hosts, and systems must be configured to discover active neighbor addresses and release addresses that are no longer active. Aggregating smaller networks into pools and aggregation IDs enhances network growth. Handling of the header is streamlined as the router only reads one address.

Resistance to Scanning

Increasing the address size to 128 bits improves security by making it more time intensive and difficult to scan all possible addresses.

> A typical IPv6 subnet will have 64 bits reserved for host addressing. In such a case, a remote attacker needs to probe 2^64 addresses to determine if a particular open service is running on a host in that subnet. At one probe per second, such a scan may take some 5 billion years to complete. [6]

Jumbograms

The jumbogram payload feature of IPv6 allows for a header extension payload option for packets longer than 65,535 octets. The payload length field in the IPv6 header must be set to zero in every packet that transports the Jumbogram payload. The Jumbogram payload option is not to be used in a packet that transports a fragment header. Jumbograms are applicable to IPv6 nodes attached to links with a MTU greater than 65,575 octets. On links running IPv6 and IPv4 with configurable MTU, the MTU must be set at a maximum of 65,575 octets to avoid delivery to IPv4 nodes. Nodes receiving errors report back to the source node by sending an ICMP Parameter Problem message [ICMPv6]. UDP Jumbogram packets are created by setting the UDP header length field to zero which forces the receiving node to deduct the correct UDP packet length from the IPv6 payload length.

Fragmentation Supported In the Extended Header Only

Only the source node performs fragmentation. Fragmentation is no longer supported in the base IP header but is made available in the extension header. The fragment size is determined by the host, “discovering” the link or path MTU.

CREATES PROBLEMS FOR IPv4 NETWORKS

Most IPv6 migration plans will involve handling IPv6 traffic over the current, production IPv4 network. Simple Internet Transition (SIT) is the standard set of protocol tools implemented in hosts and routers that provide a transition mechanism to facilitate the upgrade to the new Internet protocol. Tunneling encapsulates the IPv6 packet into an IPv4 packet (using IP Protocol 41), which allows the IPv6 packet to transport across an IPv4 Internet. SIT tunnels are the best tools for this

[6] Chown, p. 3.

task while running both IP protocols in a parallel phase. Tunneling classifications are determined by the method the sending node, encapsulating the IPv6 packet, determines the destination address at the end of the tunnel. If a router is sending to a router or if a host is sending to a router, the traffic will be tunneled to a router. If the router is sending to a host or a host sending to a host, the traffic will be tunneled to the host. Hosts and routers must be configured with a dual stack having both IPv4 and IPv6 protocols configured and running on the same infrastructure. The tunneling mechanism must map DNS host name and IP address for both IP protocols to allow for proper addressing. The dual stack transition mechanism should be configured to resolve DNS queries using the IPv6 address first and if not applicable, the IPv4 address.

Three types of tunnel methodologies are available and listed in order of complexity: automatic, 6to4 and configured. Automatic tunnels use the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), which connects IPv6 hosts over IPv4 networks. The transition mechanism configures the IPv4 network as a link-layer for IPv6 and the other hosts on the network as IPv6 hosts. [7] Once the router configuration is completed the only thing left is to configure the clients to the router. The client will discover and receive an IPv6 prefix address to use from the ISATAP router.

Configured tunnels manually configure an IPv6 address on the tunnel interface and an IPv4 address at the source or end point. Configured tunnels provide a high degree of security but can depreciate network resources.

Tunneling and Security

6to4 tunneling should prove to be the most common mechanism of transferring the encapsulated IPv6 packet across an IPv4 Internet. 6to4 utilizes a custom IPv6 prefix: 2002::/16, followed by the 32 bit IPv4 address that creates a uniquely global endpoint for the tunnel. Tunneling may be enhanced by utilizing the services of 6to4 tunnel brokers. Registering with a tunnel broker is a simple verification process. The process is so simple, it can even be done anonymously.

> Freenet6 is a quick and easy way to get an IPv6 address and establish a tunnel. What makes it so easy is its Tunnel Setup Protocol (TSP) client. The program, available here, automatically gets your IPv6 address and establishes a tunnel with the Freenet6 servers. The program can be run without registering, but registration lets you get a /48 prefix (anonymous connections are given /64 addresses), and it lets you keep the same address, regardless of IPv4 address changes. [8]

[7] Templin, Gleeson, Thalwar and Thanler, p. 1.
[8] Soup4you2, p. 1.

Those on the offense however never rest in their relentless attacks as the professionals and the newbies have proven themselves quite knowledgeable about the new weapons of IVp6. Hackers are already actively taking advantage of new IPv6 services and turning this lack of understanding about IPv6 to their own advantage. IPv6 and IPv6 transitional mechanisms introduce new, not widely understood, tools and techniques that intruders can use to secure unauthorized activity from detection. [9]

Software tools used for scanning, sniffing, infecting, flooding, modifying, and stealing data are readily available and user friendly. Now is the time system administrators and security professionals to be proactive in their efforts in preventing unauthorized IPv6 traffic on their networks from the IPv6 intrusion tools available on the Internet. Even if IPv6 is not supported on the network, the tools for tunneling are readily available.

> Underground sites now offer IPv6-enabled and IPv6-specific tools such as relay6, 6tunnel, nt6tunnel, asybo, and 6to4DDoS. Relay6, 6tunnel, nt6tunnel, and asybo are protocol bouncers which accept connections on IPv4 or IPv6 and redirect those connections to IPv6 or IPv4. This ability allows IPv4-only applications to connect to IPv6 services and vice versa. While these tools are legitimate, they are easily abused by the underground to create tunnels and redirects for backdoors and Trojans. [10]

Most system administrators have a very limited knowledge of the new Internet protocol . Most have taken zero to minimal proactive actions in configuring their defense in depth strategies (SANS mantra) to prevent an intrusion via the IPv6 protocol. The old adage, “to be forewarned is to be fore-armed” is applicable as any network not deploying an adequate defense in depth and defense in diversity against this methodology and readily available tools used by this protocol is a network ripe for an IPv6 intrusion.

IPv6 SECURITY AWARENESS

Begin the process of IPv6 awareness by defining the new protocol for detection and intrusion in your company’s security policy. If no security policy exists, or your security policy is out of date, security templates are available online through several reputable security centric organizations. A recommended site is the SANS website at http://www.sans.org/resources/policies/, which provides downloadable policies written with the collaboration of thousands of security professionals. Determine if any new tools are required to detect IPv6 intrusion and plan how to successfully implement the security policy. Conduct regular parameter audits of system to enforce policy.

[9] Warfield, p. 16.
[10] Warfield, p. 6.

Security Audit the Network Parameter

Audit the firewall making sure the vendor software is up to date on all patches. Check your configuration for optimization and ensure proper logging. Verify firewall performance by conducting a differential firewall analysis. Comparing traffic from both sides of the firewall will confirm the firewall is enforcing all configured rules…or that the firewall is functioning at all. Security policies will be more difficult to enforce when IPv6 encrypts the port and IP address. Firewall inspection of the packet content will not be possible when ESP is configured. Host verification is recommended on AH rather than using the IP address however; decryption responsibility by the host will require more demand on the processor and may increase chances of DoS attacks. Host to host addressing will restrict the firewall's ability to limit the internal host's access to excluded Internet sites. Be vigilante that packet sniffing will still be available to internal hosts. Limit access to legacy systems or known susceptible systems. If IPv6 or SIT is not yet supported on your network, block IP protocol 41.

Router

Audit the router making sure the vendor software is up to date on all patches. Check your configuration for optimization and ensure proper logging. Firewall and router filters should not mirror each other as they provide separate layers of defense. IPv6 ACL's are named, not numbered and cannot share the same name as an IPv4 ACL. The Neighbor Discovery protocol will create additional problems such as unauthorized routers making secure (IPSec) connections. Changes in router or router prefixes should not be common. Monitor for unauthorized router advertisement such as duplicate prefixes, prefix changes outside the normal transition periods, or any new prefixes. If hackers are able to access the security keys shared by the routers, they could assume a role of an authorized router. If IPv6 is supported, routers should handle the SIT tunnels.

DNS

Proper DNS configuration will be critical due to the length of the address field and the dynamic addressing nature of IPv6. In the Windows world today, how often do we connect to a network device via an IP address instead of a device name? Long IP address fields will change this habit quickly. It is recommended to hide the internal network from spoofed DNS entries (or spoofed DNS servers) by dividing DNS into zones: a public DNS zone and a private DNS zone. Gateway servers, public web servers and mail exchange servers could be placed in the public DNS zone (DMZ), while internal servers are kept in the private DNS zone. DNS name registry must be secured from unauthorized resources. Changes to existing DNS entries must be made from authorized resources. Be aware of instances of DNS cache poisoning, completed by spoofing the DNS query reply.

If the attacker spoofs the address of the authorized DNS server and uses the predicted Query ID to send the reply, the DNS server stores this value into cache precluding further replies for the address of the hostname. [11]

HONEYPOTS

Honeypots are an Internet-attached server that acts as a decoy, luring in potential hackers in order to study their activities and monitor how they are able to break into a system. (http://honeypots.sourceforge.net/). Honeypots provide no legitimate service on the network and any system activity on the PC should be analyzed for unauthorized activity. Honeypots can be used in preventing attacks, detecting attacks, researching attacks and gathering information and forensics on attacks. They require minimal hardware resources, and because they only capture unauthorized traffic, can provide concise details and accurate alerts. Honeypots can be broken down into two types, low-interaction and high interaction. Low integration honeypots work by emulating operating systems and services while high integration honeypots employ actual operating systems and real services. Most IDS products on the market are not configured to detect IPv6 activities. IPv6 attacks are occurring now and honeypots may be considered your best, (and early) warning system against the new protocol. The professionals and newbies know about IPv6 hacking methods as confirmed by Lance Spitzner,co-founder of the HoneyNet Project who advised one of the projects honeypots was attached by Italian (hackers) using an IPv6 tunnel into IPv4. [12]

IDS

Audit the IDS for latest software patches and check your configuration for optimization, proper logging and alerts. Monitor all subnets, not just the perimeter. Use IDS to validate performance by monitoring both sides of the firewall. Use a vulnerability scanner to check payload detection. Use tcpdump or windump to check the results of your vulnerability scan. If IPv6 or SIT is not supported on your network, any traffic of this nature should be subject to inspection. If IPv6 is supported, monitor traffic for unauthorized router advertisment or any new external routers advertising new prefixes. Teredo tunnels, (a.k.a. Shipworm) transport IPv6 traffic over UDP, sidestepping the firewall. Stay abreast of IPv6 detection features as they become available in new version of commercial NIDS products. These products need to increase their ability to examine the contents of encapsulated IPv6 packets as well as UDP. Never forget that bad guys on the inside have as much or more potential for doing damage than the bad guys on the outside.

[11] Sangi,Prof. Dheerj, p. 6
[12] Tee, p. 1.

REFERENCES

(1), Deering, S., Hinden, R., RFC 1883 Internet Protocol, Version 6 (IPv6) Specification, Internet RFC/STD/FYI/BCP Archives, December 1995, p. 3.

(2), Ryan, Vincent, "Time for a New Internet Protocol." NewsFactor Network, March 4, 2003, p. 1.
URL: http://enterprise-security-today.newsfactor.com/story.xhtml?story_id=20902

(3), Marsan, Carolyn Duffy, "North American ISPs Trial IPv6." Network World Fusion, p. 2.
URL:http://www.nwfusion.com/newsletters/isp/2003/1201isp1.html

(4), Muggeridge, Matt, "IPv6 Networking For the 21St Century." IPv6: IP next generation Technology Update, Compaq Computer Corporation, Session ES 147, DECUS, Fall 1999, p. 21.
URL:http://www.decus.gr.jp/decus99/sessioncd/NOTES/ES147.PDF

(5) Muggeridge, Matt, "IPv6 Networking For the 21St Century." IPv6: IP next generation Technology Update, Compaq Computer Corporation, Session ES 147, DECUS, Fall 1999, p. 33.
URL:http://www.decus.gr.jp/decus99/sessioncd/NOTES/ES147.PDF

(6), Chown, T., "IPv6 Operations, Internet-Draft." IPv6 Implications for TCP/UDP Port Scanning draft-chown-v6ops-port-scanning-implications-00, University of Southamton, March 31, 2004, p. 3
URL: http://www.6net.org/publications/standards/draft-chown-v6ops-port-scanning-implications-00.txt

(7), Templin, F., Gleeson, T., Talwar, M., Thaler, D., "Network Working Group, Internet-Draft." Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) draft-ietf-ngtrans-isatap-20.txt. Feburary 16, 2004, p. 1.
URL: http://www.join.uni-muenster.de/Dokumente/drafts/draft-ietf-ngtrans-isatap-20.txt

(8), Soup4you2, "Configuring An IPv6 Router And Client." October 25, 2003. p. 1.
URL: http://bsdhound.com/newsread.php?newsid=28

(9), Warfield, Michael H., "Security Implications of IPv6." Internet Secruity Systems, date unknown, p. 16.
URL: http://documents.iss.net/whitepapers/IPv6.pdf

(10), Warfield, Michael H., “Security Implications of IPv6.” Internet Secruity Systems, date unknown, p. 6.
URL: http://documents.iss.net/whitepapers/IPv6.pdf

(11), Sanghi, Prof. Dheeraj, “Security in the wake of IPv6.” A Term Paper Report for Advanced Computer Networks (CS625), date unknown, p. 6.
URL: http://www.cse.iitk.ac.in/~dheeraj/reports/network-security.pdf

(12), Tee, Edmund, “Enter the Honeypot.” Nework Computing Asia, July 1, 2003, p. 1. URL: http://www.ncasia.com/ViewArt.cfm?Magid=3&Artid=20259&Catid=5&subcat=50