Implementing and Configuring IPv6 in Windows 2003 and XP SP1

Keith H. Irby (Assignment 1.4b, Option 1)

12/22/03

Abstract

This paper will introduce IPv6 from theory and implementation. Expect to receive an introductory to IPv6 and IPsec. When completed with the reading one should have a general understanding of how IPsec and IPv6 interoperate together, and provoke questions requiring further depth of knowledge. The knowledge gained about IPv6 and its security applies to both general theory and the Microsoft implementation.

To fully understand how IPv6 and IPsec is implemented a discussion of Internet Key Exchange (IKE) is needed. The IKE discussion will detail various methods of implementing keying. HIP is introduced and discussed in compare contrast to IPSEC. Details and the importance of automatic re-keying bear importance to an enterprise secure communications environment. The focus of this paper is describing the current implementation of IPv6 in Windows XP SP1 and Windows 2003. Specifically, how is the protocol implemented and deployed in a Windows 2003 infrastructure. To end, IPsec in IPv6 policy implementation and deployment will be discussed and demonstrated. The objective is to examine the current implementation of the Windows 2003 IPSEC implementation and determine its value add to the security infrastructure.

IPv6 Introduction

IP Addressing is the method hosts and routers communicate, using the TCP/IP suite. TCP/IP was first adopted in 1969, as part of ARPA net. It is a layered grouping of multiple protocols. IP, along with UDP, is the protocol that is used to carry traffic destined for a host or multiple hosts. IP is typically referred to as IPv4.

IPv4 has withstood the test of time as a flexible and stable method of communication. Since it originated in the USA and was then adopted by developed nations, most of the large address blocks are owned by early adopters of the Internet, leaving the developing nations little room for growth. Unfortunately, there have been many surprises with the growth and needs of the Internet. Thus, necessitating new standards and features for the future of the Internet IPv6 provides these needs.

IPv6, also referred to as IPng, is the OSI layer 3 emerging protocol. Key features of IPv6 are addressing capabilities, address auto configuration, quality of service (QOS), Neighbor Discovery (ND), and required security. It has the ability to provide many more addresses than IPv4, instead of the 32 bit IPv4 address IPv6 uses a 128 bit length.

Address auto configuration allows a node to generate an IP address without the help of a DHCP Server or manual human configuration. The node accomplished this though communicating with the router on its network. Through communications with the router it determines whether or not it should use address auto configuration. If the router tells it not to use auto configuration, it will then attempt to use a stateful address configuration method. Otherwise, the node will attempt to configure itself by the on-link prefixes.

Allowing nodes to auto-configure themselves make it easy to provide network connectivity to a node when knowledge of networking, on the node owners' part, is absent. However there is one catch, the great benefit of DHCP is the configuration of many other unknown services, i.e. DNS. Many networks will feel the need to use stateful address configuration.

Neighbor Discovery (ND) allows independent nodes to identify themselves to each other. The new feature is key to the new protocol; it represents the first actions a node must do prior to initiating a session between hosts. This protocol resides in ICMPv6 and replaces ARP, ICMPv4 Router Discovery, and ICMP redirect messages. ICMPv6 is encapsulated within an IPv6 header. It is responsible for the initial communication on the network, as well as further communications with routers to determine the default gateway or destination of last resort.

To determine various IPv6 IP addresses ND is used. To understand the process of awakening for each node on an IPv6 network an understanding of ND is essential. First, the host must discover the local routers attached to the node. This is done for several reasons, one being to receive configuration information from the router. This is crucial if the host is determining its address via a stateless configuration method. The router provides for half of the IP Address, while the host determines the other 64 bits.

The process of ND is crucial for information security, as well as the initial flow of information. Several features of ND provide basic protection of attack. First, the Hop Limit field, similar to TTL in IPv4, is set to 255 in a ND packet. This setting informs routers to not pass this packet on to another network, ensuring ND packets from border networks are not able to be used in an attack. Instead, this type of packet would be dropped if it tries to escape the boundary of the local network.

Quality of Service (QOS) is a feature that is an revision of IPv4 Type of Service (TOS). QOS is implemented in different manner than TOS in IPv4, the second and third fields in an IPv6 header are used with QOS. The first field in IPv6 Header states that it is an IPv6 header, immediately followed by the Traffic Class Header. This field allows for the packet to define the content which may be specified for a specific application, thus enabling the application to have priority over other traffic.

The Flow field of the IPv6 Header is experimental at best, but has the most future promise of IPv6 QOS. Flow generally is supposed to allow applications to have priority by providing a peak into the upper layer protocol without revealing what is in the upper layer protocol.

QOS is implemented in IPv6 in such a manner that IPsec can be used. This is changed since IPv4, where the TOS field was not usable while data is encrypted. Thus IPv6 makes the two features usable in tandem, allowing both features to better serve the community instead of just one.

IPng uses a larger address space than IPv4. It is not in the same format that IPv4 is represented; IPv6 uses hexadecimal to represent itself to the end-user. It is a set of 4, 16 bit groups. An example of an IPv6 address is fe80::5445:5245:444f. The back to back colon represents a block of zeros called compressing zeros. This is a simplification method to shorten the readable length, which must be converted back to its binary value to know the true representation of the address. An address of 0:0:0:0:0:0:0:1 represents the loop-back address, commonly used in testing the networking stack on the node. Because the upper prefix of the address is determine by the router on the network, leaving the lower 64 bits to the host, the router manages the netmask.

There are many types of address in IPng and a single node may contain many IP Addresses. Link-local addresses are used for ND, Automatic Address Configuration, and when no routers are present on the local link enabling host to communicate with each other. Site-Local addresses are take the place of IPv4 Private Addresses, RFC 1597, nodes to communicate inside a network and preventing traffic from being leaked to the Internet. On the other hand, a global unicast address is routable on the Internet and used to communicate with any other publicly address able node.

Also, IPv6 is designed with security in mind. IPsec is built into the protocol, not an add-on feature. It has two key specifications built in it, Authentication Header (AH) and Encapsulating Security Payload (ESP), they lay the ground work for a solid secure communications infrastructure. The headers are present and operational in IPv4, however they are a required option in the header of IPv6. Both AH and ESP serve their own purpose in the scope of IPv6 IPsec.

The AH is a quick method of ensuring integrity and authentication, it also protects against replay attacks. Integrity, in this sense of the word, is having confidence that there has been no change in the data during transit. Authentication knows you are who you say you are. Otherwise, you are not someone else attempting to impersonate a third party, in the communication. This will be increasingly important in the event that ubiquitous computing becomes a way of life. If devices within a home or office that do not look, but act like a computing device, otherwise they are addressable via IP, then there must be some method of protection for everyday devices. Today's devices are much not aware of the other devices around them; once a refrigerator and a cell phone are able to communicate there could be a chance for manipulation of the refrigerator from the smart IP based cell phone. Today, however, it is important to start simple and ensure the communication channel between two nodes is trusted.

To verify nothing has changed and the data is authenticated, AH uses a hash signature. A hash signature is nothing more than a digital footprint (a secure hash function). Hash functions convert a message to a hash value for comparison. MD5 and SHA-1 are two publicly available cryptographic hash functions available. MD5 utilizes a 128 bit length versus the 160 bit length of SHA-1. A shorter length of MD5 makes it a faster hash, shorter length equals faster hash.

ESP is more costly than AH, but fills a gap where AH leaves off. ESP provides confidentiality of data by encrypting data in transit. Once the data is encrypted in transit it is very difficult to decrypt the through a means of capturing the data.

The order of placement of the header is dependant upon the mode of ESP; for transport ESP is inserted after the header but prior to the payload data, but for tunnel mode ESP is prior to the IP header. Transport mode is only providing protection for the upper layer protocols. In transport mode ESP is applied after all the other extension headers. On the other hand, tunnel mode provides protection for the entire IP packet. Tunnel mode ESP is much more complicate, but perhaps more secure, it encapsulates the origin IP address and all extension headers. Each mode has its use; tunnel mode is most often used in a VPN, thus securing two endpoints.

The Security Association (SA) defines the type of connection that will take place between two separate connections. SAs are initiated with each one way connection of each host to host or gateway to gateway. If a bi-directional communication is required then two SAs are established, per direction of traffic. A SA is identified by three pieces; the Security Parameter Index (SPI), the destination address, and the security protocol. The SPI is a 32 bit value, assumed to be higher than 255, those below are reserved for future use. The security protocol can be either ESP or AH.

Both of the above protocols, AH and ESP, can function in either transport or tunnel mode. Transport mode provides protection for the upper layer protocols, i.e. TCP, UDP, and ICMP. On the other hand, tunnel mode provides protection at the lower level, encryption applied to IP.

The road to IPv6

The transition to the IPv6 address space will not occur overnight. Perhaps maybe not tomorrow, but the infrastructure may already be available to assist in a migration. Although there are still a few bumps in the road that either have not been implemented across the board in the protocol, or each vendor may be at a slightly different level of implementation. While it is not required, some last mile providers, for example Verio in the United States http://www.verio.com/access/ipv6.cfm, will provide a gateway service to the Internet.

Organizations invest much time and money to implement and maintain a network infrastructure. It may not make sense to many organizations to remove working devices, which are providing a business function, to be replaced by new IPv6 enabled devices. Many of the currently deployed devices cannot or will not communicate via IPv6. However, methods exist to allow IPv4 networks to communicate with IPv6 networks. Also, most of the new IPv6 enabled nodes implement the protocol in dual stack with IPv4, meaning both versions of IP are implemented side-by-side. Thus, allowing a node to communicate with any IP device on the network, without assistance.

For the mid-term future, several types of IP devices will exist. Be that, IPv6 only, IPv4 only (common), dual stack (a near-term goal), or some type of proxy a method will be required to allow devices which are not dual stack to speak to each other. A method of allowing an IPv6 group of node to communicate with a distant IPv4 node is to encapsulate the traffic from IPv6 in a IPv4 packet. Tunneling can be in the form of router to router, crossing an ocean of IPv4 networks to reach another IPv6 network. However, tunneling could be in the forms of host to host, host to router, or also router to host. In the Windows 2003 family of products 6to4 and ISATAP are enabled by default. The above 6over4 must be configured manually in the to work in the W2K3 Family.

To implement an IPv6 infrastructure, one has to understand the changes in DNS. DNS allows for a new resource record called the A6 record, which is comparable to the A record in IPv4. It may be a bit confusing to see the A6 record, because the RFC 1886 originally name the record to be an AAAA record, which has been superseded in RFC 2874. Some implementations of DNS still use AAAA records for IPv6 addresses. To resolve names to IPv6 address's a new reverse lookup zone is created; the new zone is called IP6.ARPA. The new DNS extensions have been implemented to provide simplicity and ease of migration, to make it seamless to the end-user.

IPv6 IPsec and PKI

There are several types of authentication mechanisms. A key exchange is required for IPv6 IPsec and PKI to work. Where RFC 2401 states "…KDC-based systems such as Kerberos and other public-key systems such as SKIP could be employed." [2, 6] The most common method of PKI is implemented in IPsec through IKE.

IKE can use both manual and automatic keying. A manual method is not as secure an option, the greatest margin for error lies in human error of key configuration. While an automatic method of management occurs in larger environment, complexity and costs of implementation and management may drive those who do not see the risk away. There are low cost or free PKI solutions in development. There are numerous options, both commercial and open-source.

To fall within the specification IKE must support DES, MD5 and SHA, Authentication via pre-shared keys and MODP over default group number one. However, it is optional to support signatures and keys via RSA public key encryption. [15, 7] While it is optional, for an IPsec node-to-node communication within an enterprise environment this is highly suggested. It is highly difficult, if not impossible, to manage keys manually for a high number of nodes.

Two types of encryptions are used in the above IKE implementation. Shared secret uses symmetric key algorithms. Symmetric key algorithms use a single key. This key is shared between both of the two nodes communicating. This is very fast, but has the constraint of distributing or communicating the key to the other node in the communication. The obstacle is sharing the key without it being compromised between the two nodes. Once it is shared, this is a fast method and common in VPN implementations.

On the other hand, RSA public key encryption uses Asymmetric key algorithms. Asymmetric key exchange is much slower than symmetric key communications. However, this is due to the implementation of the RSA public key encryption. Another important feature of RSA is its ability to increase its key size. Where DES, and other symmetric key are set lengths asymmetric key pairs can increase their length.

RSA uses 2 key pair in its communications. The key pairs consist of a public and private key. The private key is always kept secret, while the public key is given out for all devices to use to communicate with the owning node. In this manner, the public key identifies the node as part of authentication, but only the private key can decrypt the public key.

The public keys of two different nodes are exchanged, node A trusts that node B's public key is legitimate. RSA signatures use x.509 certificates. The public key can be reference and trusted based upon the Certificate Authority (CA). Node B trusts that node A's public key is legitimate. To verify the key can be trusted, both node A and B can check with the Certificate Authority for authenticity. The CA hierarchy generally uses an external source to verify its authenticity. Implementing PKI can be an overwhelming project in a large organization.

HIP, a new option

Host Identity Protocol is a draft standard that is worth describing. First, one of the reasons for the need of a new addressing structure is the depletion of the IPv4 addresses. This is primarily due to the high number of mobile devices in the near term. HIPs strength is its attempt to solve the three problems of mobility, multi-homing, and security.

To ensure some type of end-to-end tracking of a mobile device HIP is used to follow a mobile device as it moves through the topology. This occurs by keeping the mobile device active as it moves from mobile connector to connector. HIP solves the jump problem from node to node as a mobile device is in transit in the physical world. Packet forwarding is the largest problem solved with HIP. It assists in determining where packets should be sent based upon where the mobile device will be next. This allows a mobile device to travel without having multiple IP addresses and receive traffic bound for it.

HIP introduces a new layer in the TCP/IP family, based on cryptology, which resides between IP and TCP. This layer performs best working with IPSEC. The true benefit to HIP is its ability to allow true host-to-host encryption on the fly. It uses asymmetric cryptography, allowing an exchange of the nodes public keys in real time.

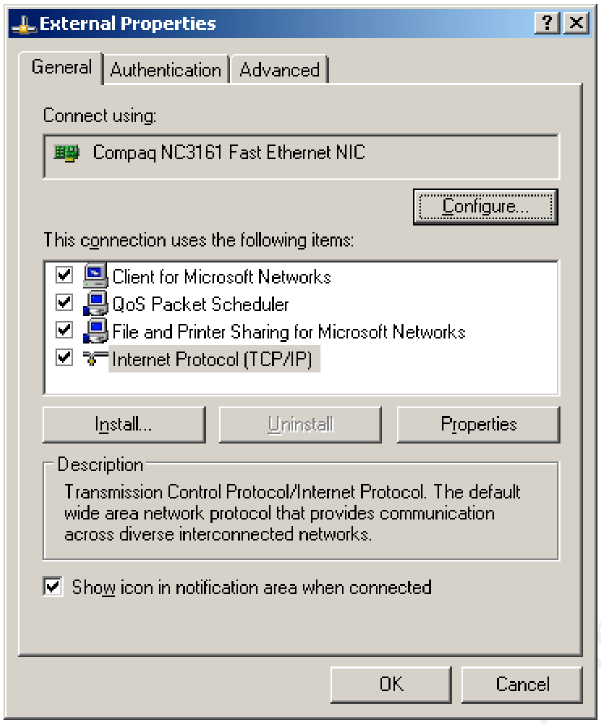
Another benefit of HIP security is its avoidance of PKI. One of the stumbling blocks to many PKI implementations is the vast complexity of the design, and ultimately verifying the data in question with a third party CA. This is not required with HIP, instead it is assumed that no other host could have the private key and while the public key is used for data encryption.

IPv6 Implementation in MS Windows

IPv6 is a not so new protocol, but relatively new in implementation of organizations.

While IPv6 has been fully implemented in routing and UNIX, it has not been implemented in MS Windows until the last year. Windows XP (XP) and Windows 2003 (W2K3) are the only versions of windows that will support IPv6. IPv6 is a native option in W2K3, through several quick installation steps. Windows XP requires a download of SP1 from the below URL.
http://www.microsoft.com/WindowsXP/pro/downloads/servicepacks/sp1/expresso.asp

W2K3 IPv6 installation is quite simple. Go to the networking properties of the NIC; choose properties of Local Area Connection. Below you will see an example of what this sheet might look like.



Connect using:

Compaq NC3161 Fast Ethernet NIC

This connection uses the following items:

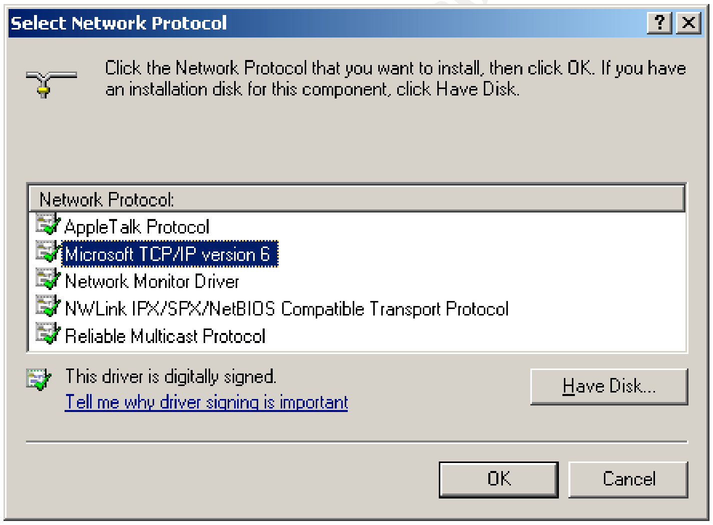
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

Once this display appears, then click the Install button, and choose protocol.



Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

Network Protocol:

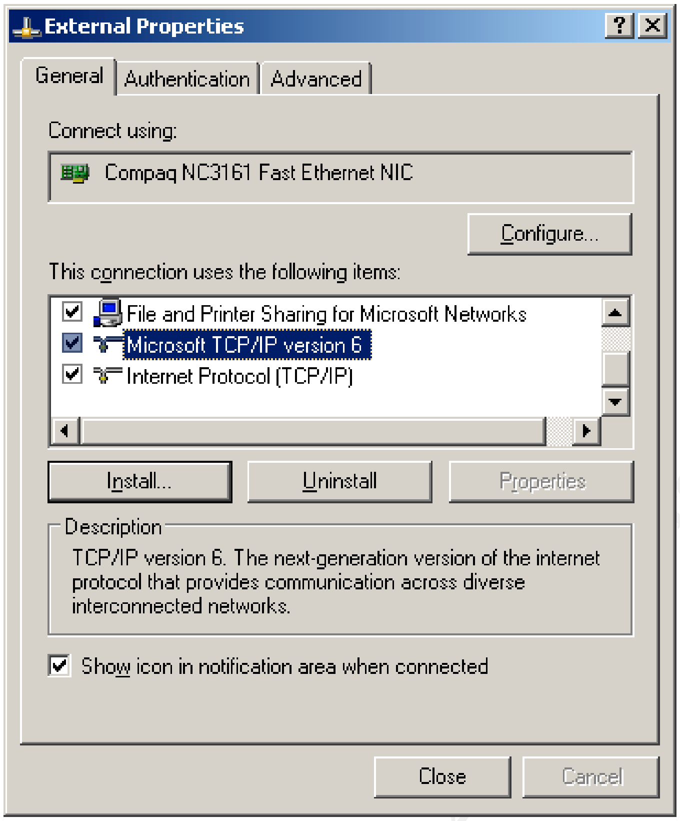
- AppleTalk Protocol
- Microsoft TCP/IP version 6
- Network Monitor Driver
- NWLink IPX/SPX/NetBIOS Compatible Transport Protocol
- Reliable Multicast Protocol

This driver is digitally signed.

Tell me why driver signing is important

Of the choices in the above box choose Microsoft TCP/IP version 6. Notice all of the drivers appearing above are digitally signed. This is new to Windows 2003, ensuring the identity of the software vendor.

By double-clicking on the Microsoft TCP/IP version 6 option the protocol will install. Once the protocol is installed the NIC properties will then show the Microsoft TCP/IP version 6 protocol installed. The screenshot below displays the property sheet of the configured NIC, with IPv6.



Connect using:

Compaq NC3161 Fast Ethernet NIC

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☑ Microsoft TCP/IP version 6
☑ Internet Protocol (TCP/IP)

Description
TCP/IP version 6. The next-generation version of the internet protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

To install IPv6 on an XP system two things must occur within the system configuration. First, follow the instructions for W2K3. Second, you must type ‘install IPv6’ at the command prompt.

Truth be told, there is an easier method to install IPv6 in W2K3 and XP. By going to the command prompt, entering the commands netsh, interface, ipv6, and install the protocol is installed. This is not the traditional method of managing a Microsoft Windows system; however you manually must configure the protocol with the command line interface.

There are specific manual configurations for IPv6. Unless you must configure the IPv6 address manually for advanced configuration or as a router for translation of 4 to 6 and vise versus, there is no need to further configure the system for IPv6. Auto-configuration will ensure the system is able to communicate on the local network.

Once IPv6 is installed, the native ICFv4 will not provide packet filtering for inbound IPv6 traffic; it will continue to provide protection for the configured filter for IPv4. These two products must be configured separately. However, ICFv6 is installed with the installation of the Advanced Networking Pack for Windows XP. ICFv6 is not enabled by default, it is enabled once IPv6 is enabled, then ICFv6 must be configured to protect from unwanted IPv6 traffic. ICFv6 provides a stateful firewall, port allow/deny, and logging. It is deny all for inbound packets, and must be further configured to allow external initiated connections to its external interface. This is not via a GUI interface, which many ZoneAlarm users love, but forces the user to understand what rules they want to implement.

For example, if the local system hosted a web server, external systems would not be able to connect to the system. To allow an external connection to port 80/TCP type the following command ‘netsh firewall>set adapter "Local Area Connection" port 80=enable web, where “Local Area Connection” is the name of the interface that is being configured. External TCP connections to port 80 will then be allowed. All of the configuration can be accomplished via programmatic syntax during the install of an install of a program.

Tracking of connections and denials of connections is done by writing to logs. To enable this feature type ‘netsh firewall>set logging droppedpackets=enabled’, this tells ICFv6 to enable logging of all dropped packets to the default location of c:\windows. Once logging is enabled monitoring of all attempted communications will be logged to a flat text file. It can be reference for auditing and troubleshooting. The complexity of IFCv6 is both its strength and obvious downfall; most end-users will not have the technical skills to configure it. To configure a new rule a user may want to monitor the log and determine if legitimate traffic is being dropped, then create a rule based upon the data in the log.

To perform network diagnostics of a local and distant IPv6 hosts the ping6.exe utility and tracert6.exe are provided for Windows XP. Windows 2003 has its own enhanced command line tools. Ping6 works in a similar fashion to ping.exe. Two new functions are worth mentioning. The –s option instructs the command to specify the source address in the echo request, which is required for link-local destination addresses. To test the return trip or reverse route, use the –r switch.

Both of the new network diagnostic tools tracert6 and ping6 use ICMP6. The ICMP6 protocol provides the framework for Neighbor Discovery (ND) and Multicast Listener Discovery (MLD). MLD is the replacement for Internet Group Management Protocol (IGMP), used to manage multicast messaging. ND manages node to node communication on a link path. ND is the IPv6 replacement for Address Resolution Protocol (ARP); it works to determine communication relationships between different nodes.

Because of the method used to initiate communication with IPv6 ICMPv6, a complete secure end-to-end communication can not be created. Since IPsec requires secure communications from start to finish we are faced with a dilemma. [12, 2] Where does the secure communication from host-to-host begin? Hence, the chicken and the egg scenario, there must be some form of SA negotiation at some point. It is, unfortunately, post ICMPv6 and ND traffic.

By far, the most relevant to security tool is ipsec6.exe. This tool allows the system administrator to configure and analyze current security policies on the local system. This ipsec6.exe is used on both Windows XP SP1 and Windows 2003. By typing '>ipsec6 sp if' the current security policy is displayed.

To manipulate IPsec 6 policies the .sad and .spd files must be configured. SAD (Security Association Database) file contain the configuration information for the SA and SPD (Security Policy Database) file are security policy files. The option SP used along with the designated interface will list the security policies configured for the called interface. If desired the SPD can be quite complex, allowing for exemptions for certain protocols and IPSEC rules for others.

To configure SPD a blank text file must be created. The policy file must list the destination address, IPsec protocol (AH or ESP), IPsec Mode (transport or tunnel), SABundleIndex, Direction, (one or bi-directional), Action, and the InterfaceIndex. Save the changes to the SPD file, and then load the changes with the ipsec6 sp command. Next open the SAD file to begin configuration of it. The SA file must list the SAEntry, SPI, SADestIPAddr, DestIPAddr, SrcIPAddr, Protocol, DestPort, AuthAlg, KeyFile, Direction, and SecPolicyIndex. Once this is completed, save this file and then load the changes with the ipsec6. This process must be completed manually on both nodes to enable IPsec communications between two nodes using IPv6.

Also, by using the SA option with the ipsec6 command the security associations will be listed. The pitfall of Windows XP SP1 and Windows 2003 IPsec6 implementation is the lack of encryption in ESP. It only allows data authentication and integrity. To make matters worse, the Microsoft implementation of IPv6 can not automatically key data, otherwise use IKE. This being a manual process inhibits all but trial use of the tool in most large environments. Most organizations will just not view it as practical to manually configure SPDs on all hosts. This is comparable to deploying hosts files on 1000 systems in an enterprise network, it just becomes too much work to manage for the systems administrators.

Conclusion

IPv6 is ready for large organizational implementation. Implementations must be planned carefully and must enable interoperation with IPv4. Since IPv6 is an industry standard, many different devices can use the protocol to communicate with each other in a secure fashion. IPv6 will be used with mobile and static devices. The IPv6 challenge is implementing IPsec to more than just gateway to gateway. There is a need for host to host, host to gateway, or gateway to host security, beyond today's common gateway to gateway security.

Microsoft has implemented IPv6 in its latest operating systems. Both Windows XP SP1 and Windows 2003 can use IPv6. Installing IPv6 in Windows XP SP1 and Windows 2003 is a straightforward process that does not require user intervention. Often end-users will install a MS Windows Service Pack and not know what the software does; inadvertently IPv6 will be installed without end-user knowledge. While configuration of IPsec with IPv6 may not be easily implemented by an average end-user, it is implemented within the depth of knowledge of a systems administrator. Utilizing IPv6 with IPsec provides a level of security at the lowest level of communication between devices. Because of the limitation within Microsoft's current operating systems IPsec in host-to-host configuration is not recommended for use within a production environment.

Since the majority of networked devices are Microsoft products, IPv6 IPsec will not easily be implemented into the corporate environment until the limitation of manual re-keying is overcome. An alternative for host-to-host authentication, integrity, and encryption is required, until these and other limitations of IPv6 IPsec are overcome, host to host IPv6 IPsec will not be a viable solution. Perhaps HIP will one day be implemented in Microsoft's protocol stack, allowing each host to identify its self to each other, beyond the assumed identity provided via the routing infrastructure. Once Microsoft's devices can utilize an automatic keying procedure, integrating with IKE and encrypt the ESP data, then Microsoft networks in corporate environments will be ready for IPv6 IPsec. While the security infrastructure of IPv6 may not be perfect, IPv6 is ready for prime-time and many organizations will benefit from migration entirely or piecemeal to IPv6.

References:

1. S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Addressing Architecture”, Apr 2003, http://www.faqs.org/ftp/rfc/pdf/rfc3513.txt.pdf

2. S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," Internet Eng. Task Force RFC 2401, Nov. 1998; http://www.ietf.org/rfc/rfc2401.txt

3. S. Kent and R. Atkinson, “IP Authentication Header”, Internet Eng. Task Force RFC 2402, Nov. 1998; http://www.faqs.org/ftp/rfc/pdf/rfc2402.txt.pdf

4. S. Kent and R. Atkinson, “IP Encapsulating Security Payload (ESP)” Internet Eng. Task Force RFC 2406, Nov. 1998; http://www.ietf.org/rfc/rfc2406.txt

5. A. Skarmeta, G. Perez, O. Reverte, and G. Millian, “PKI Services for IPv6”, May/June 2003, http://140.127.47.14/paper/14.pdf

6. C. Metz, “Moving Toward an IPv6 Future”, May/June 2003, http://csdl.computer.org/comp/mags/ic/2003/03/w3025.pdf

7. Microsoft Technet, “Overview of the Advanced Networking Pack for Windows XP”, Sep 2003 http://support.microsoft.com/default.aspx?scid=kb;en-us;817778

8. Microsoft Technet, “Manual Configuration for IPv6”, Sep 2002, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0902.asp

9. Microsoft, “Introduction to IPv6”, Aug 2003, http://www.microsoft.com/windowsserver2003/technologies/ipv6/introipv6.mspx

10. J. Kato, “IPv6 Implementation Status on Windows Platform”, Nov 2000, http://win6.jp/memos/win-ipv6-status.pdf

11. T. Narten and R. Draves, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, Jan 2001, http://www.faqs.org/ftp/rfc/pdf/rfc3041.txt.pdf

12. J. Fleming, “Windows XP, IPv6 and IPv8”, Nov. 2002, http://ipv8.no-ip.com/INFO/Papers/WindowsXP/

13. P. Hermann-Seton, “Security Features in IPv6”, 2002, http://www.sans.org/rr/papers/44/380.pdf

14. J. Arkko and P. Nikander, “Limitations of IPsec Policy Mechinisms” Ericsson Research NomadicLab, written post June 2003, http://www.tml.hut.fi/~pnr/publications/cam2003.pdf

15. D. Harkins and D. Carrel, “The Internet Key Exchange (IKE)” Internet Eng. Task Force RFC 2409, Nov 1998, http://www.faqs.org/ftp/rfc/pdf/rfc2409.txt.pdf

16. S. Deering, “IPv6 Addressing the future” Global IPv6 Summit, Jul 2001, http://www.ipv6.or.kr/ipv6summit/Download/2nd-day/Session-I/s-1-1.ppt

17. P. Nikander, J Ylitalo, J Wall, “Integrating Security, Mobility, and Multi-homing in a HIP Way” Ericsson Research NomadicLab, http://www.tml.hut.fi/~pnr/presentations/HIP-NDSS-slides.pdf