A STUDY ON THE NETWORK SECURITY ASPECTS IN IPv6

(A CAPSTONE PROJECT REPORT)

Submitted by

RAGHAVENDRA JAYARAMAN

A report submitted to the

Department of Computing Science

In partial fulfilment of the requirement for the degree

Of

Master of Science

in

Internetworking

University of Alberta

(2009-2011)

Acknowledgement

I wish to express my thanks to my Project Supervisor Dr.M.H.MacGregor, Professor and Chair in Department of Computing Science, University of Alberta for so readily granting permission to undergo this study and for his valuable suggestions at every stage and kind encouragement for this work.

I would also like to thank my family and friends those who motivated and cooperated for completing this project successfully.

Abstract

These days, technology has advanced and facilitates networking. With data demand rising exponentially over the networks, security is a rising concern. The data over a network is highly vulnerable to risks of both intentional attacks and unintentional events. IPv6 was designed with security in mind and it brings significant improvements in mechanisms for assuring a higher level of security and confidentiality of the transmitted information in modern IP networks. This project will evaluate the fundamental security deployment aspects for IPv6-enabled networks and will detail the deployment considerations for effective design and architecture of secure IPv6 networks. First it focuses on IPv6 solutions for IPv4 security issues, pursued by end-to-end security, transition mechanism security considerations, function of firewalls and IDS along with the IPv6 specific security issues. Finally, some possible solutions to avoid a number of security threats in IPv6 networks have been specified. This project does not intend to provide a definitive security policy for any particular environment but rather, it is an attempt to enumerate all of the considerations to be accounted for when creating an appropriate security policy and architecting the IPv6 network to incorporate security measures. Consequently additional security measures are essential and more capable security management equipments are required in IPv6 networks in order to attain a security posture at parity with that of the ideal networks.

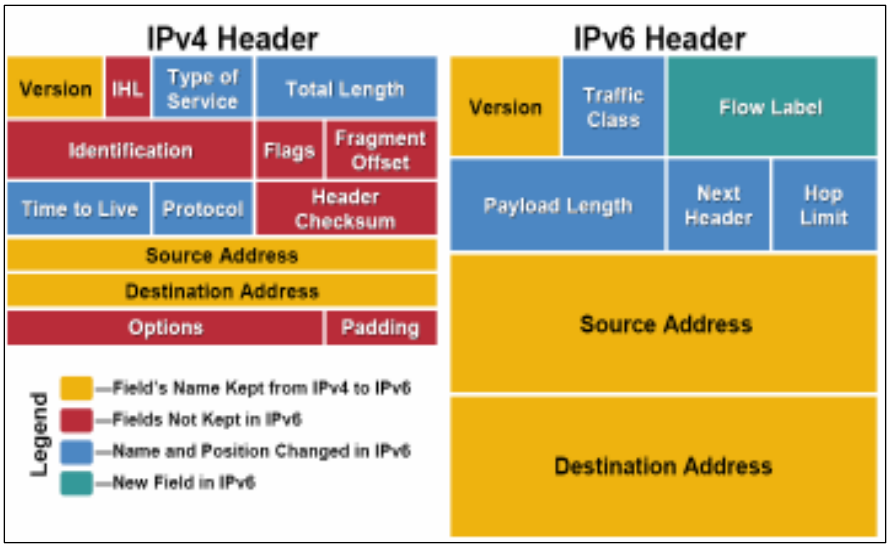
CONTENTS

Introduction

IPv6 protocol, which should replace the IPv4 protocol, brings many new improvements and possibilities considering simplicity, quality of service, routing speed and security. In comparison to IPv4, IPv6 improves mechanisms for assuring a secure and confidential transfer of information. Despite these improvements, network security remains an extremely significant issue since IPv6 is more resistant to some threats than IPv4 but there are various new threats specific to IPv6. Considering security, particularly problematic is the transition period of coexistence of both IPv4 and IPv6 protocols. It brings new challenges to present security system along with its security mechanism and results in huge impact on formerly significant security tools.

Overview of IPv4 and IPv6 Comparison

a. Simplified Header:



IPv6 has a simplified and more streamlined header format which is exactly 40 bytes with 8 fields in it. It is designed to keep the header overhead for routers to a minimum resulting in less hardware complexity and faster packet processing. The checksum field is dropped and IPv6 checksum computations must be carried out by upper-layer protocols like TCP and UDP.

The Traffic Class field together with new Flow Label provides prioritized traffic and Quality of Service (QoS). The time to live, Protocol and Options present in IPv4 header has been replaced with the Hop Limit, Next Header Type and optional IPv6 Extension Headers respectively. The elimination of the options field in the IPv6 header provides more proficient processing at intermediate routers.

IPv4 and IPv6 headers are not interoperable. A router or host must use an implementation of both IPv4 and IPv6 in order to recognize and process both header formats.

b. Address Space and Address Types:

IPv6 has 128 bits (16 bytes) in length address bits hierarchically assigned with address scoping (e.g., local link versus global) to improve scalability as compared to 32 bits (4 bytes) in length in IPv4. This results in a very large increase in the number of IP addresses available and has a number of advantages. Address-conservation techniques, such as the deployment of Network Address Translation (*NAT*) are no longer necessary.

NAT breaks end to end connectivity and does not work well with peer to peer applications like VOIP. IPv6 eliminates the need for NAT and can offer end to end connectivity to all hosts, thus providing a simplified network configuration and reduced hardware and software complexity.

Also, certain higher layer protocols like FTP have a similar issue with NAT and require specialized software to work through NAT. Such issues are resolved using IPv6. The increasing deployment of wireless and mobile devices will also not be cramped by IP address scarcity issues.

IPv6 addresses are written as eight groups of hexadecimal 16 bit words separated by colons as shown below:

9CD2:567:1044:305:8888:9999:1111:CA27

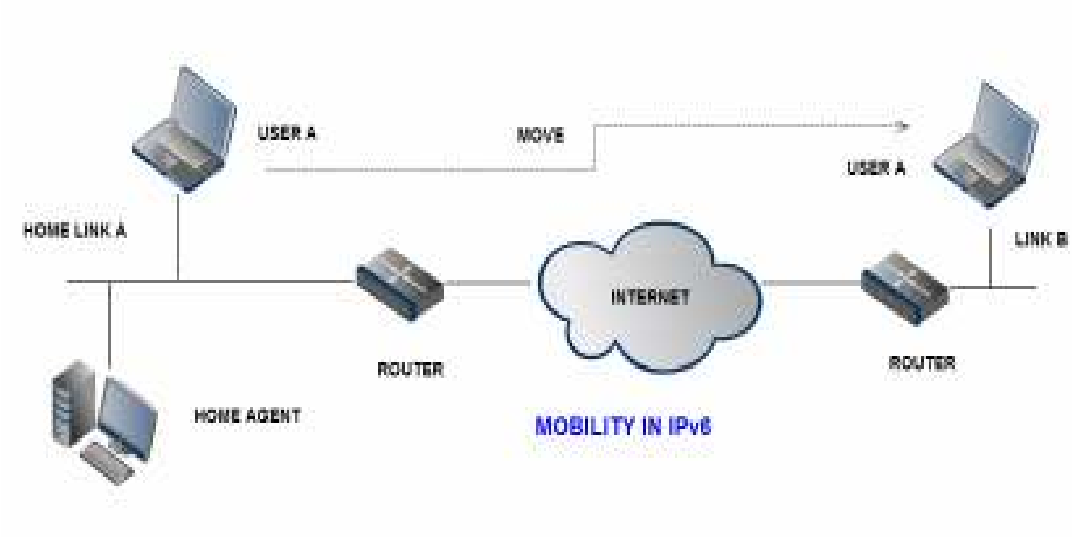
Three types of IPv6 addresses have been defined-*Unicast, Anycast and Multicast*.

Unicast is the IP address of a single interface and packets sent to a Unicast destination address are delivered to that unique interface alone.

Anycast address is assigned to a set of interfaces belonging to different nodes thus providing Redundant services using nonunique addresses.

Broadcast addresses are eliminated in IPv6. Broadcast addresses are replaced with a link-local scope all-nodes multicast address. This increases the efficient use of one-to-many communications.

c. Mobility



IPv6 offers improved mobility support than IPv4 using Mobile IPv6 (*MIPv6*). It provides separate protocol based on the use of IPv6 extension headers and has better authentication, traffic handling, faster handover, routing and hierarchical mobility capabilities than MIPv4.

It uses the same IP address regardless of the network and equipment it is connected to. It also provides mechanisms that allow mobile nodes to change their addresses and location without loosing the existing connections through which those nodes are communicating. This service is supported at the Internet level and thus fully transparent to upper-layer protocols.

d. Auto-configuration

IPv6 offers *Stateless and Stateful* address self-configuration for IP devices.

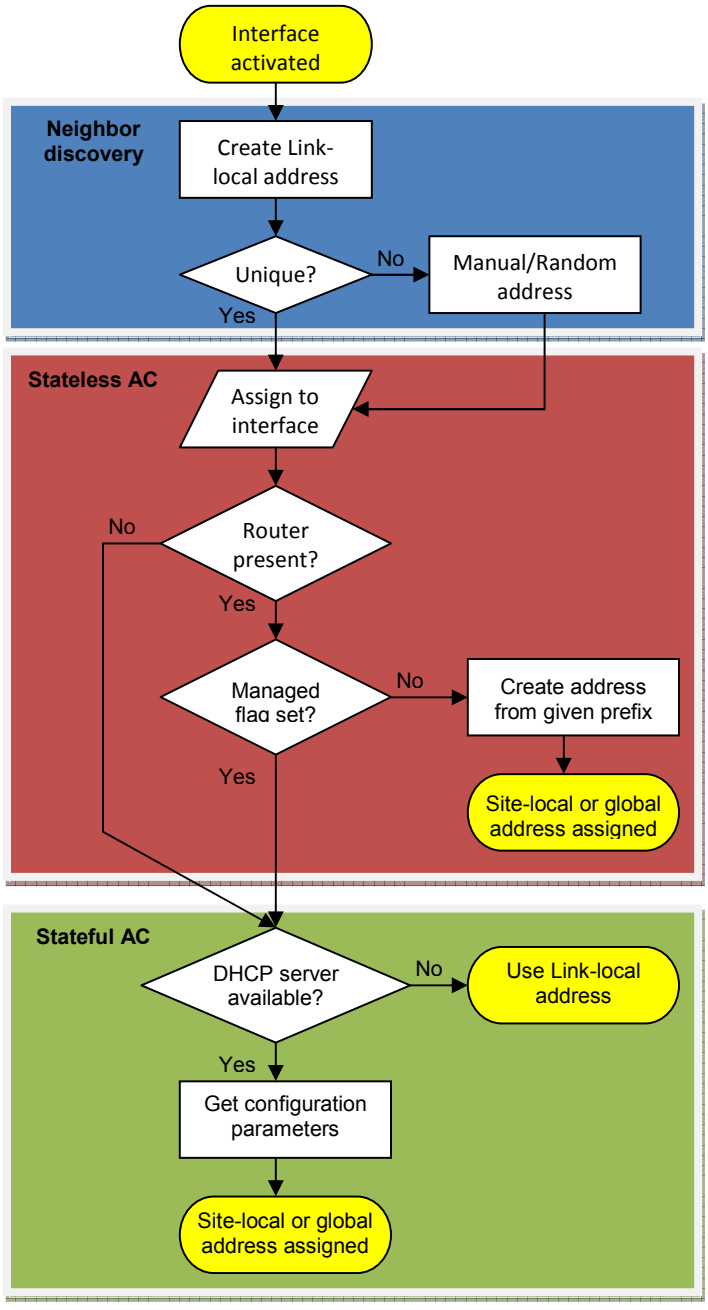
State-Less Address Auto Configuration *(SLAAC)* automatically configures IP addresses on new nodes allowing the appliance to behave in a *plug and play* fashion reducing the administrative burden of manually configuring them. This greatly improves scalability and manageability of networks. The Neighbor Discovery (*ND*) protocols are used for this purpose (same as *ARP* in IPv4). But the trust model used by Auto discovery is too trusting to be secure. For that reason new protocols called the Secure Neighbor Discovery (*SEND*) were defined to avoid spoofing related and other attacks. Even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration.

Stateful **configuration** in IPv6 is controlled through DHCPv6. Address configuration is performed in the presence of a DHCP server. IPv4 is limited to stateful protocols such as DHCP, which require a server to store a requesting host's configuration information.

Combination of Stateless and Stateful entails an IP device auto-configuring an IPv6 address using the stateless method and then utilizing DHCPv6 to obtain additional parameters or options such as which *NTP* servers to query for time resolution on the given network.

The use of Internet Control Message Protocol (ICMP) is now required, versus its optional use in IPv4. Use of ICMPv4 was not required for the basic IPv4 functions; network administrators often could block all ICMPv4 messages to secure the networks. The similar blockage is however not possible for IPv6 networks because IPv6 operations like Auto-configuration and Path MTU discovery do not work without the use of ICMPv6 messages.

*The **auto-configuration** process is visualized in a flowchart describing the steps involved from activation of the interface to the final address assignment:*

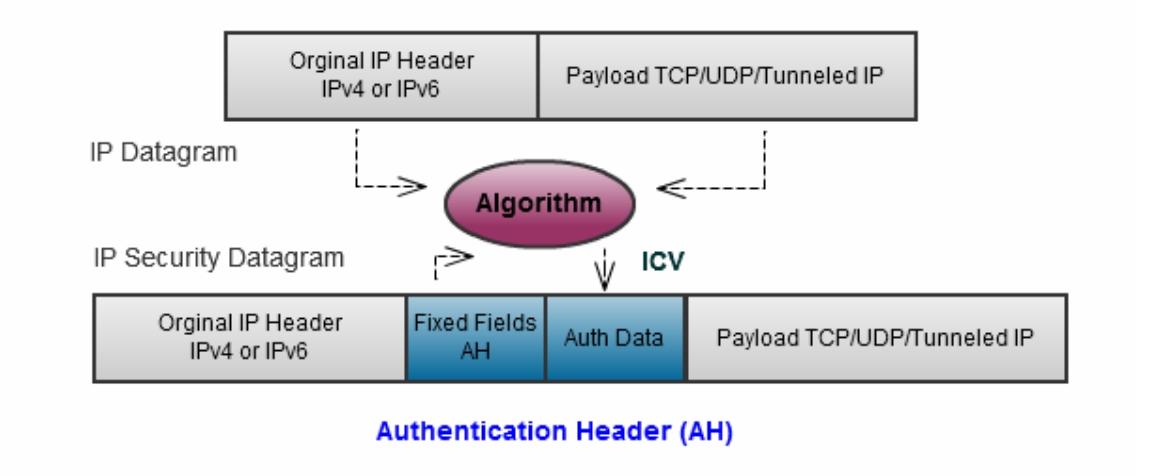


e. Authentication & Encrypted Security

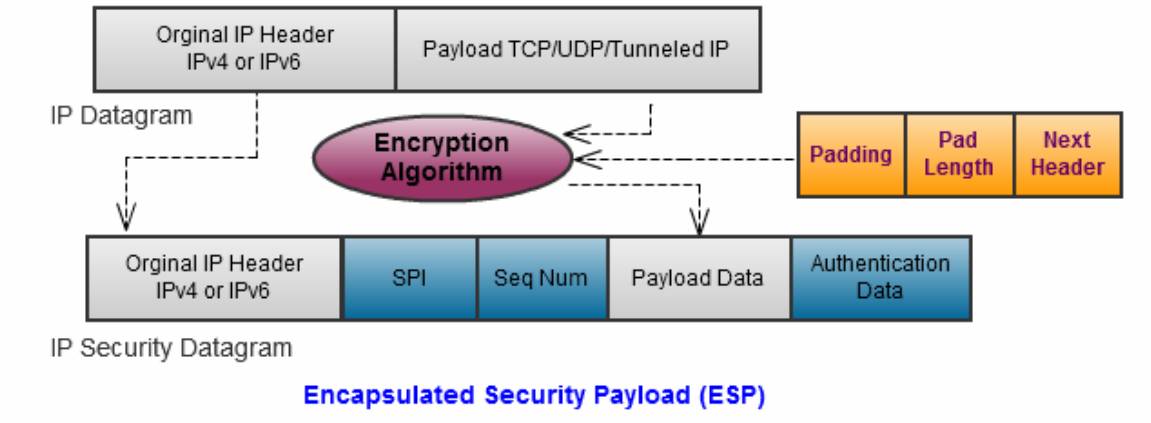
IPv6 implements built-in Network-layer Authentication and Encryption via IP security which is not an option but a requirement.

IP security (*IP sec*), a set of protocols that provide data integrity, confidentiality, and authentication was introduced while security became a concern for IP-based networks.

IPsec is also available for IPv4 implementations; it is not mandated but optional. Deploying IPsec in IPv4 networks causes problems with *NAT* and security problems with *UDP* traffic.



Authentication Header (AH)



Encapsulated Security Payload (ESP)

The two headers *Authentication header* (*AH*) and *Encapsulating Security Payload* (*ESP*) are the components of IP security (*IPsec*). This support was somewhat weakened when, the IPv6 security architecture

downgraded the requirement for the support of AH from *MUST* to *MAY*. This condition provides a standards-based solution for network security requirements and promotes interoperability between different IPv6 implementations.

By means of *Internet key exchange version2* (*IKEv2*) procedures, two entities using IPsec can exchange the essential parameter information to establish secure communications between them. As IPsec support is mandatory in IPv6, an entire IPv6 network operation should provide improved security than its IPv4 counterpart.

In addition, majority of the security breaches occur at the application level, even the successful deployment of IPsec with IPv6 does not guarantee any further security for those attacks beyond the valuable capability to determine the source of the attack.

f. Fragmentation

In IPv4, Fragmentation is supported at both routers and the sending host. But in IPv6 Fragmentation is not allowed at routers. It is only supported at the sending host.

The fragment fields which appear in the IPv4 header that dealt with the packet fragments namely fragment offset, (fragment) flags, and (fragment) identification were dropped from the main IPv6 header. Fragment information was relegated to an extension header. In IPv6, only the original sender of a packet is permitted to break the packet into fragments. This has significant implications for network security because *Internet Control Message Protocol* (*ICMP*) control packets that support path *Maximum Transmission Unit* (*MTU*) discovery must be permitted through all IPv6 networks which were optional in IPv4 networks.

This enhances the router performance and also eliminates fragmentation related attacks on the routers. However, the

fragmentation related attacks are still possible against the receiving hosts, as well as the security devices (firewalls, IDS/IPS) which still must perform packet reassembly for deep packet inspection.

IPv4 cannot allow packets bigger than 64 Kilobytes (*KB*) but IPv6 supports *Jumbograms* and allows payloads that are longer than 64 Kilobytes.

g. Quality of Service (QoS)

The IPv4 Type of service (ToS)/DS header field is replaced by the "***Traffic Class***" field in IPv6 that facilitate the support for QoS for both differentiated and integrated services. It indicates the type or priority of traffic in order to request routing treatment.

Advanced applications such as IP telephony, video/audio, interactive games or ecommerce will require a higher level of QoS. One of the main issues QoS deals with is data loss. The Traffic class field reduces or eliminates data loss part of the QoS enhancement.

To provide better support for real-time traffic (e.g. VOIP), IPv6 includes "***Flow Label***" in its specification. This mechanism is used to indicate that some packets require special handling by the IPv6 routers in the network such as low delay or high bandwidth and it allows routers to recognize the end-to-end flow to which transmitted packets belong. Resource allocation can be provided using *Resource Reservation Protocol (RSVP)*.

Flow label enables efficient and consistent routing treatment for packets within a given communication session, such as those within a real-time communication *versus* a best-effort data transmission.

The traffic is identified in the IPv6 header; thus support for QoS can be achieved even when the packet payload is encrypted through IPsec. No identification of payload for QoS is present within the IPv4 header.

IPv6 has Built-in support in the framework for specifying the various QoS requirement and related negotiation (IPv4 has only the ToS field which is ignored by majority of commercial IP Routers).

h. Efficient Routing Infrastructure

IPv6 provides significant improvements such as better handling of packet fragmentation and provisions for header chaining that reduce routing table size and processing time. It offers strong hierarchical routing infrastructure, supporting route aggregation based on the common occurrence of multiple levels of Internet service providers. Also, hierarchical addressing in IPv6 allows proper address space allocation resulting in smaller routing tables and more efficient routing in the overall network.

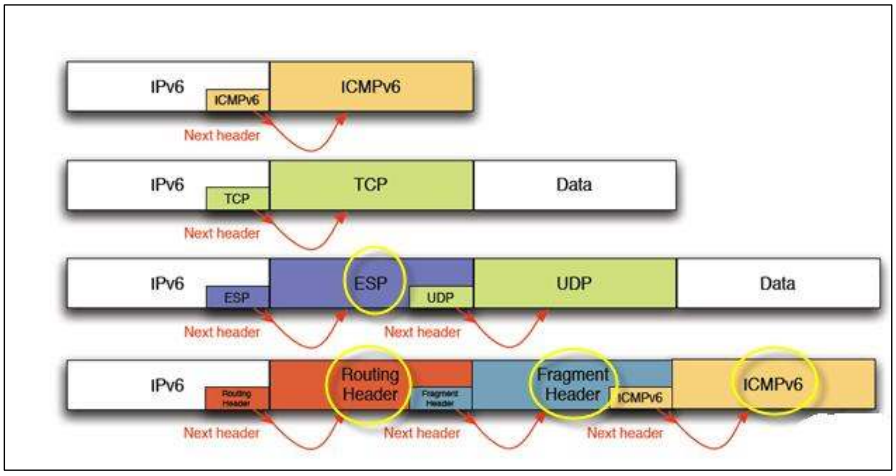
As IPv6 addressing specification restricts the amount of backbone routing entries by performing route aggregation we can view only 8192 routes on the default-free zone. Thus IPv6 Internet, backbone routers have much efficient routing tables, corresponding to the routing infrastructure of Top-Level Aggregators.

It is observed that cost of running IPv6 networks is less as compared to that of IPv4 networks; however the throughput analysis shows that routing performance of IPv4 is better. Different load balancing approaches can be used to enhance the performance of IPv6 networks.

i. Extensibility (Extension Headers)

IPv6 can be simply extended for new features by adding extension headers following the IPv6 header. IPv4 Header includes “options” which can support only 40 bytes of options whereas in IPv6 all optional data are moved to “extension headers”. There is no limit for the number of headers that can be chained together.

As the next header field is an 8-bit number, there can be 255 different types of header. Only 6 different header types are defined at present: *Hop-by-hop options Header, Routing Header, Destination Options Header, Fragment Header, Authentication Header (AH),* and *Encapsulating Security Payload (ESP) header.*



This feature does not only provide for better extensibility but also provides more efficient routing; only the information that is needed by a router is processed; thus increasing the network overall performance.

In a Nutshell, these changes provide powerful capabilities to an IPv6 network infrastructure. However, they also give rise to new security vulnerabilities.

Current security threats in IPv4

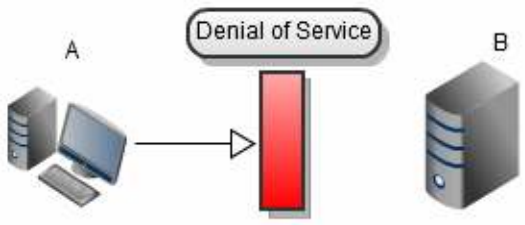
a. Reconnaissance attacks

The first category of security attack is usually a reconnaissance attack. An intruder attempts to learn as much as essential data about the victim network that can be misused later in further attacks.

Reconnaissance is carried out by ***Ping sweeps and Port scans***. In IPv4 network it would only take little more than 4 minutes to find any host address through *NMAP* as it has only a 2^{32} subnet addresses.

First, an attacker uses ***ping probes*** in order to determine which IP addresses are in use in the victim network. After having found an accessible system, an attacker performs ***port scan*** procedure. Open ports can be used to exploit the specific hosts further. Because of the small address space, reconnaissance attack is easy in IPv4 architecture.

b. Denial of Service Attack



The A can not get the service of B

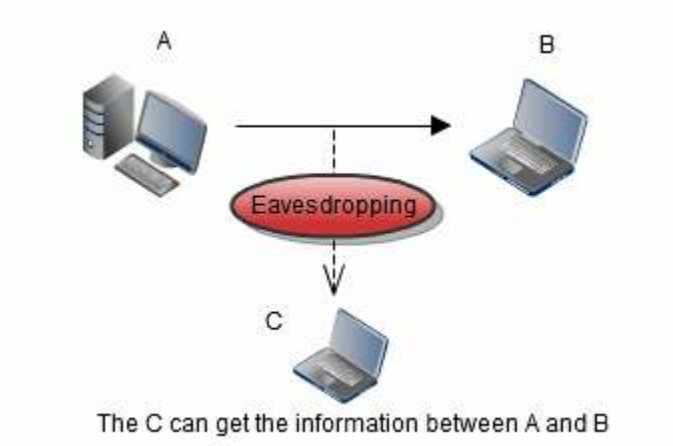
In this kind of attack a user or organization is deprived of service of a resource they would normally expected to have or else it may result in a degradation of ***Quality of Service (QoS)***, which is hard to detect. Normal activities will be disrupted by delay of communication on purpose.

In the worst cases, a website can be forced to cease operating. Attacker may use one or some of the following methods: flooding packets until a computer or the entire network cease operating; preventing valid network traffic, which will cause lost of network resource to its intended users. In the cases of web corpse, results were paralysis of services provided or degradation of QoS.

An example of DoS attack that results from an architectural vulnerability of IPv4 is the broadcast ***flooding attack*** *or* ***Smurf attack***.

A ***Distributed DOS (DDoS) attack*** is a *DoS attack* that uses many nodes against one or more targets. These nodes may be acting knowingly or unknowingly. The attack is usually launched by software agents installed within the conspiring nodes.

c. Eavesdropping



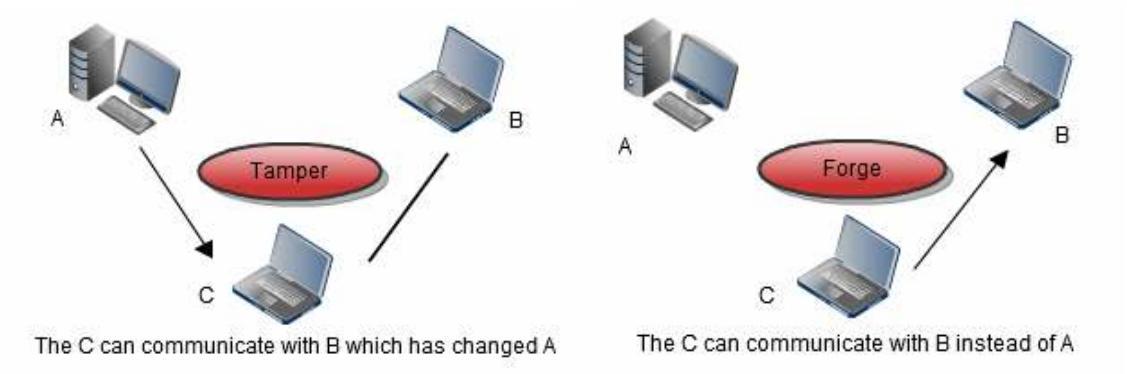
The C can get the information between A and B

In Ipv4, network communication is sometimes performed without encryption, this provides chances for attacker who have acquired data route to tail and read communication. In case that confidential information is transmitted in a plaintext protocol, they can easily be compromised by an attacker running sniffing attack. A ***sniffing attack***

is a passive attack aiming to eavesdrop information travelling along a network.

Sniffing attacks can be avoided by a proper use of the *IPsec security architecture*, which is used in IPv4 as an option.

d. Tamper & Forge Attack



Computer's validity is set by the operating system or network through the rules IP protocols. In some case, IP address is forged by attacker namely forged ID. Attacker may use special program to manufacture IP packet, make the packet seemingly from valid address inside the web.

The IP ***Spoofing attack*** involves forging ones source address. After acquiring access authorization by valid IP address, attacker can modify, reroute, and delete data.

Other forms of spoofing, such as ***DNS spoofing***, occur when an attacker has accomplished a DNS server and explicitly alter the host-name-IP address tables.

e. Fragmentation and Reassembly Vulnerabilities

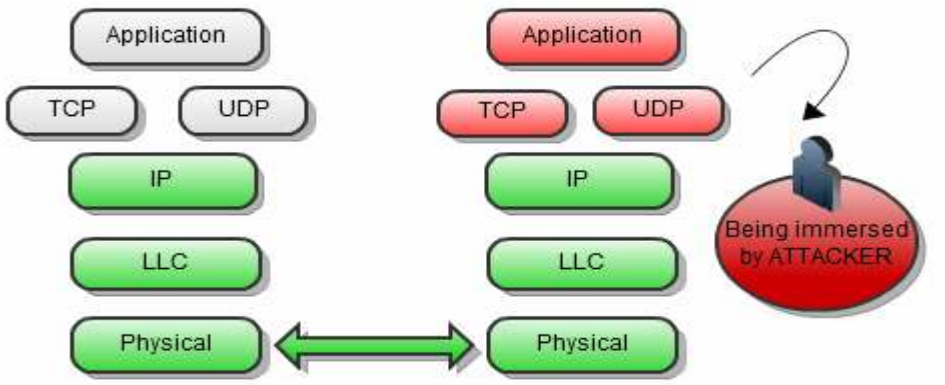
Fragmentation and reassembly of packets is required for IPv4 routers. The vulnerabilities due to this requirement on the routers are therefore unique to IPv4.

This type of attacks exploits the way certain operating systems handle large IPv4 packets. An example is the "***ping of death attack***". In a ping of death attack the target system is flooded with fragmented ICMP ping packets. With each fragment, the size of the reassembled ping packet exceeds beyond the packet size limit (size of an IP datagram) of IPv4 therefore, causing the target system to crash, hang or even reboot.

The fragmentation related ***DoS attacks*** are possible against the IPv4 routers which are required to perform all packet fragmentation and reassembly. An example of the DoS attack in IPv4 is by sending a large number of fragmented packets to a router or end host exclusive of including a terminating last fragment packet.

Such *DoS attacks* are also possible against IPv4 security devices, e.g. *firewalls, IDS/IPS*. These devices need to reassemble the fragmented packets in order to carry out deep packet inspection to apply packet filtering security policy and to perform signature analysis.

f. Application layer attacks



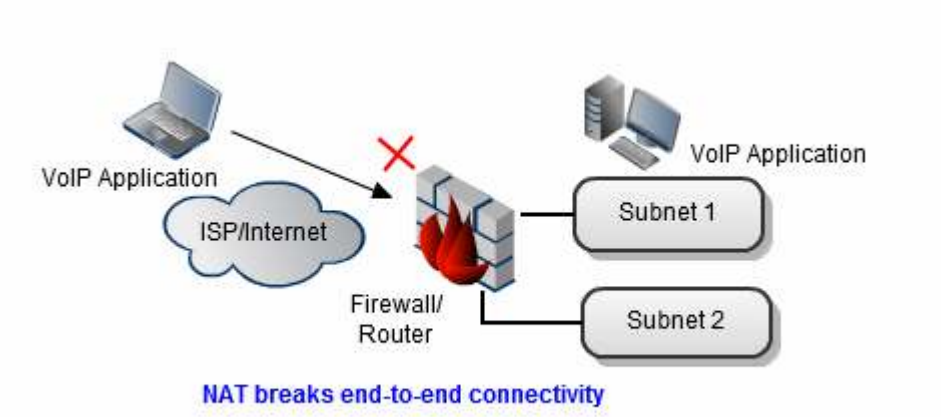
Application Layer Attack

Application layer attacks are the most common attacks today. Attacks such as buffer overflow attacks, web application attacks (e.g. CGI attacks), different types of viruses and worms which are distributed through malicious code/programs can propagate themselves from one infected or compromised hosts to infect remote systems.

These types of attacks are performed at the application layer of the ISO/OSI network model (layer 7). Since IPv4 is a protocol of the network layer it does not have influence on these types of attacks.

Using IP sec which is optional in IPv4 will neither prevent computer systems and networks from these attacks nor alleviate their consequences. Moreover, IPv4's small address space can facilitate malicious code distribution.

g. Lack of end-to-end connectivity



NAT breaks end-to-end connectivity

The use of NATs breaks the end-to-end connectivity and addressability. This causes problems in deploying IPsec in IPv4 networks with NAT, and security problems with UDP traffic. Because of the lack of address space in IPv4, NAT schemes are deployed.

Another security restriction of NATs is in the application of enterprise wide security policies. These policies can not be pushed to the nodes

that are behind a NAT by a centrally controlled policy server positioned outside the NAT. This is because in common, only that traffic can reach a node behind NAT that was originated by the node.

The NAT mechanisms provide "***security through obscurity***" as a side benefit to its main purpose.

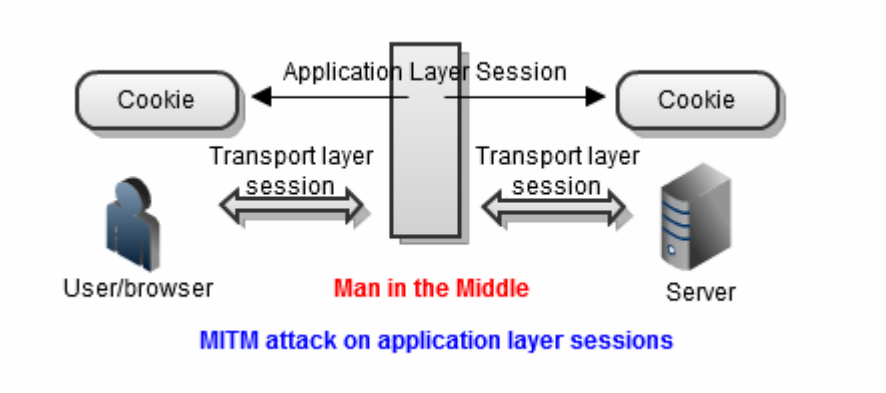
h. ARP poisoning and ICMP redirect

IPv4 networks use *Address Resolution Protocol* (*ARP*) for mapping a host's IP address with its physical or MAC address. This selective information is stored by each host in a special memory location known as the ARP table.

Each time a connection with an unknown host is needed, an ARP request is sent out on the network. Then, either the unknown host responds broadcasting its own IP address or a router does it with the appropriate information. ARP poisoning occurs when forged ARP responses are broadcasted with incorrect mapping information that could force packets to be sent to the wrong destination. A similar approach is used by ICMP redirect attacks.

Nevertheless, many techniques have been developed to overcome some of the IPv4 security limitations. For instance, although Network Address Translation (NAT) and Network Address Port Translation (NAPT) were introduced to facilitate the re-use and preservation of a rapidly depleting IPv4 address space, these techniques can provide also for certain level of protection against some of the aforementioned threats. Also, IPsec facilitate the use of encryption communication, but its implementation is optional.

i. Man-in-the-middle attacks (MITM): Attacks



IPv4's lack of proper authentication mechanisms may facilitate men-in-the-middle attacks.

When a *node A* requires the layer 2 address *(MAC address)* of another *node B*, it sends out a neighbor solicitation *(NS)* message to the all-nodes multicast address. An attacker on the same link can view the NS message and reply to it with the corresponding neighbor advertisement *(NA)* message, thereby taking over the intended traffic flow between A and B. Now the attacker is able to ***view, insert*** and ***alter*** messages between two hosts without either hosts knowing that their communication has been compromised.

Because the IPv4 headers have no security mechanisms themselves, each protocol relies on the IPsec protocol suite for security which is not mandatory. Tools that can attack an *Internet key exchange (IKE)* aggressive mode negotiation and derive a preshared key are documented.

j. Rogue devices

Rogue devices are unauthorized devices connected to a network. While this could most easily be a simple unauthorized laptop, more interesting for an adversary would be a rogue wireless access point, DNS or DHCP server, router, or switch.

These attacks are reasonably common in IPv4 networks. If IPsec (optional) were ever used in a more comprehensive manner in the IPv4 protocol (including device bootstrap), authentication for devices could mitigate this attack reasonably.

The 802.1x standard also has the potential to assist here, though an undetected rogue device could funnel 802.1x authentication sequences to a compromised node acting as an AAA server while capturing valid credentials.

IPv6 Solutions for IPv4 Security issues

IPv4 Issue - No mechanism for Resistance to Scanning
IPv6 Solution- Resistance to Scanning possible only in IPv6

It is impracticable to brute-force scan an IPv6 network for live nodes, as the IPv6 address space is so large. There are 2^{64} subnet addresses in IPv6. So, it is very difficult to scan every address from this large space of addresses.

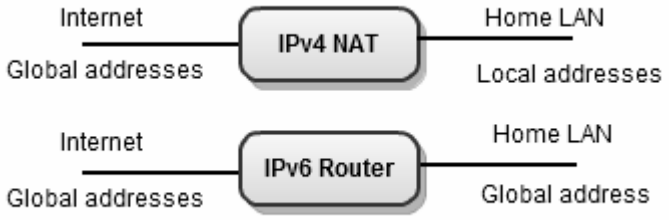
Though if we scan million packets per second it will take lot of years to find one host address in the network while in IPv4, it would only take 4 minute to find any host address through *Network Mapper* (Nmap) as it has a 2^{32} subnet addresses. And IPv6 does not support Nmap. So, attacker cannot scan the addresses and catch its target.

The flip side to this advantage of IPv6 is that the administrators can also not do a brute force scan for topology mapping. We cannot catch the attacker who is doing spoofing in the network.

This advantage is only possible if the IPv6 interface IDs and subnet IDs are randomized. This advantage is lost if an administrator chooses interface IDs in a non randomized deterministic manner, for example using 02 interface ID values for routers.

The most common compromised systems are hosts. So when a host is compromised, brute-force scanning becomes trivial. Therefore reliance on the IPv6 address space as a main security measure against device scanning is not recommended.

IPv4 Issue - NAT breaks end-to-end network security
IPv6 Solution- Huge address range: No need of NAT

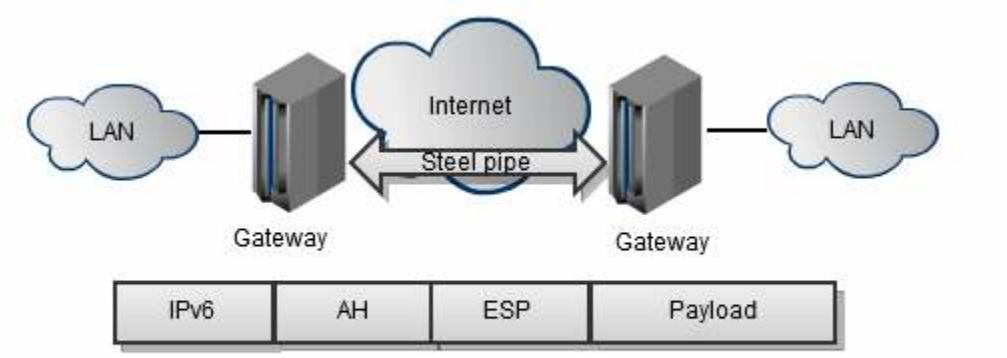


To prevent the IPv4 address space from being exhausted, or at least doing it at a more moderate rate, temporary solutions like Network Address Translation (NAT) is being used. NAT lets a local network connected to the Internet use its own local address space, completely different from the global address space. This is done by placing the NAT machine between the Internet and the local network and then applying the appropriate mapping between the internal local addresses into global addresses.

There are, however, disadvantages when using a NAT. It could easily become a performance bottleneck since it has to replace the address fields inside every IP packet. Also, certain protocols that embed the source and destination address inside the packet will not work without especially configured NAT machines. NAT also breaks end-to-end connectivity; VOIP application between two private addresses cannot take place.

IPv6 with this large 128 bit address space IPv6 can offer end-to-end (E2E) connectivity to all hosts. When IPv6 is fully deployed, the need for NAT will be eliminated. All home networks will be able to use global addresses such as the aggregatable-unicast addresses. However, with E2E connectivity, security and the onus of security will lie with the hosts. All hosts may not have the required computing resources for providing security.

IPv4 Issue - IPsec is Optional
IPv6 Solution – IPsec is Mandatory



Secure connection using IPsec

As IPv6 became more and more developed, improvements were "*back ported*" to IPv4. *For example*, a highly touted feature of IPv6 is security provided by IPsec. But even by the first documents on IPsec, this improvement was added (backwards in) to IPv4 but was made OPTIONAL.

Integrated IPsec makes IPv6 secure and provides a unified security strategy for the entire network. Administrators rely on the IPsec protocol suite for network layer security.

IPsec uses ***Authentication Header (AH)*** and ***Encapsulation Security Payload (ESP)*** protocols to provide data security. It offers several security services such as:

- Access control
- Connectionless data integrity
- Data origin authentication
- Confidentiality (encryption)
- Limited traffic flow confidentiality

IPv4 Issue - External Firewalls introduce performance bottlenecks
IPv6 Solution - Confidentiality and data integrity without need for additional firewalls

The *Authentication Header (AH)* provides the ***data integrity*** and authentication for IP packets either in the transport mode or tunnel mode. Transport mode is implemented between two remote systems and tunnel mode is implemented in the intermediate systems.

AH prevents the *IP address spoofing attacks* and *replay attack*. In Replay attack the attacker gets the copy of the authenticate packet and later sends it to the intended destination. AH prevents this type of attack by tracking sequence numbers. When system sends a packet it establishes the new *Security Association (SA)* and increments the sequence number by 1 and so on.

	AH	ESP	ESP (encryption + authentication)
Access control	☑	☑	☑
Connectionless integrity	☑		☑
Data orgin authentication	☑		☑
Rejection of replayed attacks	☑	☑	☑
Confidentiality		☑	☑
Limited traffic flow confidentiality		☑	☑

Services offered by AH and ESP

The *Encapsulation Security Payload (ESP)* provides the data integrity, ***confidentiality*** and some traffic flow confidentiality. It encrypts the IP payload and IPv6 extension headers. It gives the authentication service also as AH does.

Security Association (SA) is a one way relationship between sender and receiver which gives the security to flow of traffic. It can give service to either *AH* or *ESP* and they must keep the database of SAs.

IPv4 Issue - Security issues related to ICMPv4
IPv6 Solution - ICMPv6 uses IPsec authentication and encryption

ICMPv4 use in IPv4 networks is optional and not mandatory for normal network operations. Therefore it is possible to block most of ICMP messages without a direct influence to the proper network functionality. Thus to avoid network security issues related to ICMPv4, blocking of ICMP messages was a common practice.

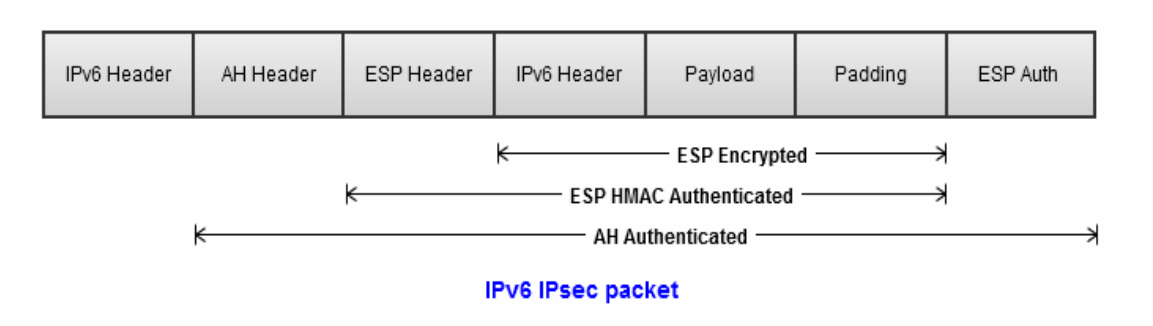
On the other hand, complete *ICMPv6* blocking is not possible in IPv6 networks as ICMPv6 is responsible and is required for few network operations as follows:

- The discovery of ***Path Maximum Transmission Unit*** *(PMTU)* requires a "*Packet Too Big*" response in an ICMPv6 message. This helps the sender to either send smaller packets or to fragment them.

- An invalid option in the ***hop-by-hop options header*** requires the routers to send a "*Parameter Problem*" response to the sender in an ICMPv6 message.

- ***SLAAC*** requires ICMPv6 *solicitation* and *advertisement* messages for its operation.

- ***Secure Neighbor Discovery*** *(SEND)* requires ICMPv6 for *solicitation* and *advertisement* messages as well as for *authentication* and *certification* path messages.



The ***AH*** and ***ESP*** in IPsec provides ***authentication*** and ***encryption*** respectively for ICMPv6 messages. Because of the essential role of ICMPv6 in IPv6 networks a blanket filtering of ICMPv6 messages is no longer possible in IPv6. But we can allow trusted sources and deny everything else.

IPv4 Issue – Routers suffer from Fragmentation attacks
IPv6 Solution – Routers do not perform Fragmentation & Reassembly

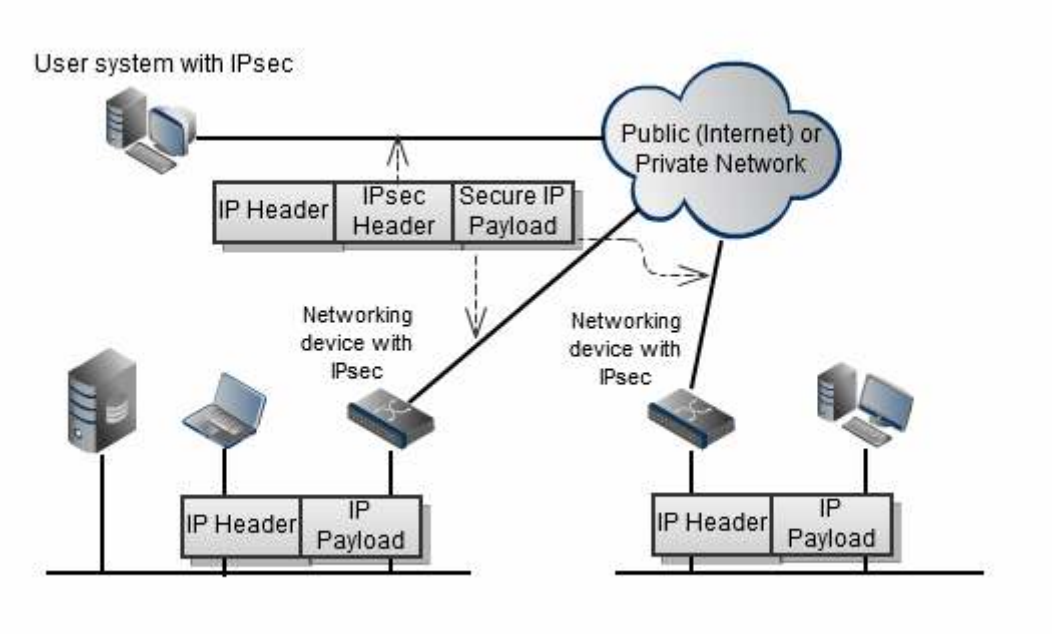
Routers in IPv4 network are required to perform Fragmentation and reassembly. Due to this requirement IPv4 routers are suffer from fragmentation attack.

On the other hand, IPv6 routers do not perform this function. It eliminates fragmentation related attacks on *routers*. Only the sender and receiver hosts perform packet fragmentation and reassembly respectively.

In IPv6 networks, the usage of path MTU discovery method is an obligation which is supported by ICMPv6 messages. The minimal MTU size for IPv6 networks is 1280 octets. For security reasons it is recommended to discard all fragments less than 1280 octets unless the packet is last in the flow. Also at the receiving end it is a recommended security practice to limit the *total number of fragments* and their allowed *arrival rate*.

IPsec in IPv6

IPv6 was designed with security in mind. It brings security enhancement into modern IP networks. IPv6 headers have no security mechanisms themselves, just as in IPv4. Administrators rely on IPsec protocol suite for security. IPsec is a compilation of mechanisms to protect IP traffic from eavesdropping, modification in transit, and more. As IPsec support is mandatory in IPv6, a fully compliant IPv6 network deployment should provide better security than its IPv4 counterpart.

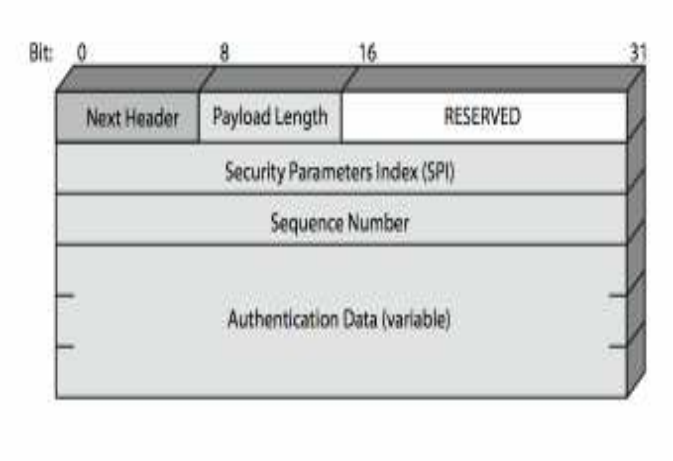


At present, IPsec is widely deployed in IPv4 as a method to connect multiple remote sites for creating a single *Virtual Private Network (VPN)* over the Internet. As IPsec-related protocols are a mandatory requirement for any IPv6 node, all IPv6 nodes have IPsec enabled by default. This requirement will increase the deployment of IPsec not only for creating VPNs but also to promote secure communications among IPv6 nodes.

There are two IPsec headers:

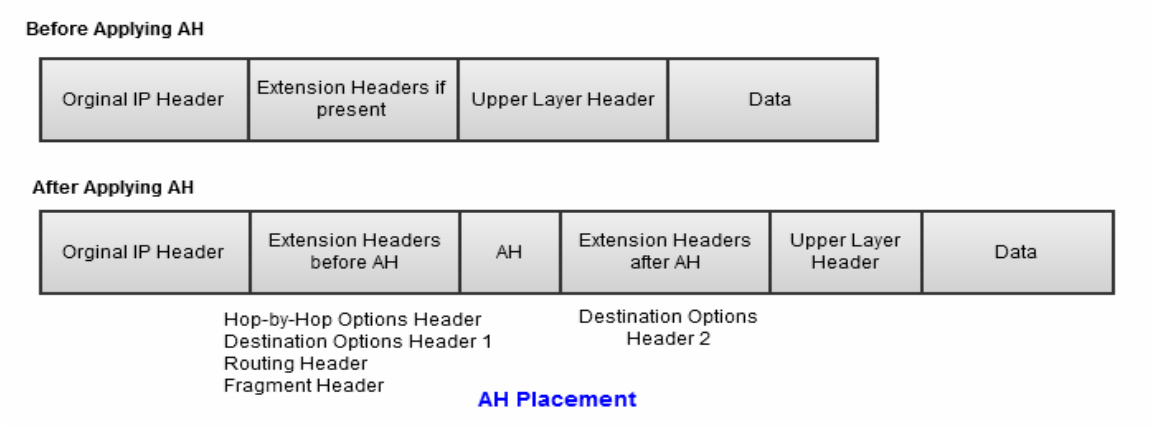
- IP Authentication Header (AH) as defined in *[RFC2402]*
- IP Encapsulating Security Payload (ESP) as defined in *[RFC2406]*

AH offers connectionless data origin authentication and data integrity for IP packets with optional protection against packet replays. The authentication header covers the IPv6 header, the extension headers and upper layer protocol data.



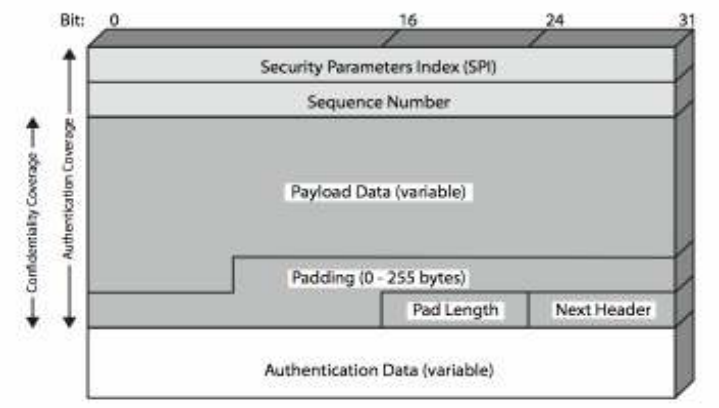
The Authentication header contains a Next Header field, a Header Length field, a Security Parameters Index (SPI) field that identifies a specific IP Security (IPSec) security association (SA), a Sequence Number field that provides anti-replay protection, and an Authentication Data field that contains an integrity check value (ICV). The ICV provides data authentication and integrity.

Packet fragmentation occurs after the AH processing of the packet, so Fragment Header is not included in the AH computation.



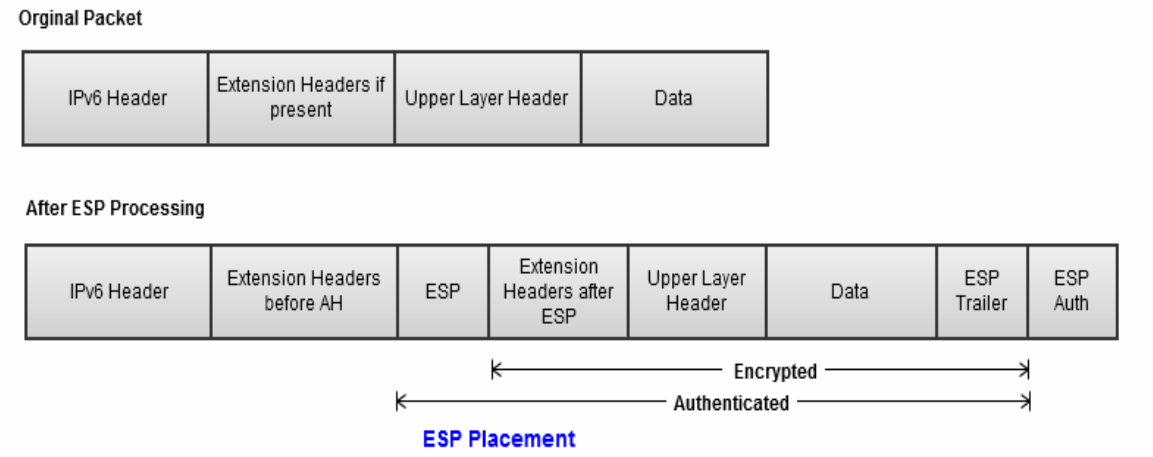
The AH is inserted after the Hop-by-Hop Options Header, the Routing Header, and the Fragment Header but before the ESP and upper layer protocol headers. The Destination Options Header may appear before or after the AH.

ESP provides all of the security services offered by AH. In addition, ESP offers data confidentiality by means of encryption and limited traffic flow confidentiality. The header coverage is the primary difference between the authentication service provided by AH and that provided by ESP. ESP does not cover the IPv6 header and the extension headers unless these are encapsulated in the tunnel.



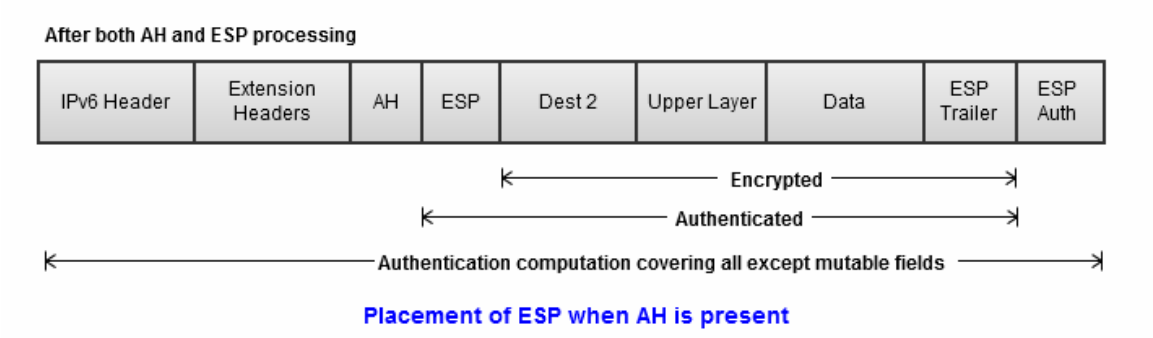
The ESP header contains a Security Parameters Index (SPI) field that identifies the IPSec SA and a Sequence Number field that provides anti-replay protection. The ESP trailer contains the Padding, Padding

Length, Next Header, and Authentication Data fields. The Authentication Data field contains the integrity check value (ICV).



ESP is placed after the IPv6 header but before the second Destination Options header, and before any upper layer protocol headers.

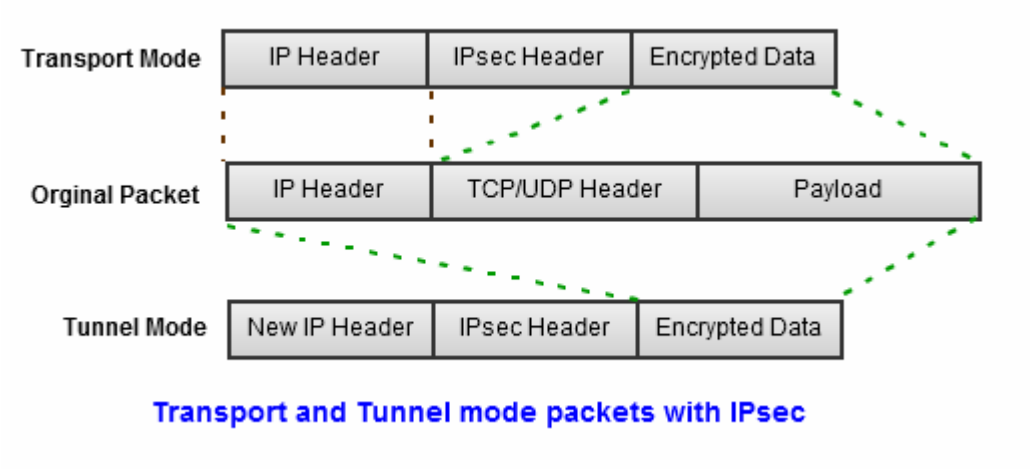
ESP is placed just after AH if AH is applied in addition to ESP. The *figure* below shows the placement of ESP when AH is present



Both AH and ESP is applied in one of two modes: *Transport mode or Tunnel mode*.

In ***transport mode***, the AH or ESP header is inserted between the IP header and transport protocol headers. In transport mode, a secure path is established between the communicating end nodes.

In transport mode, the source and destination hosts do the IPsec processing. Some people consider transport mode more secure because (with ESP encryption) the original source and destination addresses are hidden, but this isn't necessarily a huge security advantage.



Transport and Tunnel mode packets with IPsec

In ***tunnel mode***, the AH or ESP header precedes the original IP header, and a new IP header is put in front of the AH or ESP header. In tunnel mode, a secure channel is established between two security gateways (SG), which are usually placed at the site borders.

The downside of tunnel mode implemented in security gateways is that the packet is carried in clear text over part of the network. This part is supposed to be trusted, but that mostly means that it's an attractive target for attackers. There may also be MTU issues, because if a host sends a 1280 byte packet, after encapsulation by the security gateway, the packet will be larger, requiring path MTU discovering, even though the host limited its packets to 1280 bytes.

Both *authentication and encryption* can be provided by a host of different algorithms.

Authentication algorithms include HMAC-MD5-96, a 96-bit Hash-based Message Authentication Code (HMAC) based on the MD5 one-way hash function, and HMAC-SHA-1-96 based on the SHA-1 one-way hash function.

Encryption algorithm choices include DES (no longer considered safe), 3DES, and AES. Both the HMAC authentication and the encryption algorithms require secret keys, which should change regularly for optimum security.

Exchanging Keys, SA, SPD and SAD:

The *Internet Key Exchange (IKE)* protocol makes it possible to negotiate most of the settings between two hosts that implement IPsec. IKE itself contains several parts, including the *Internet Security Association and Key Management Protocol (ISAKMP)* and parts of the *Oakley Key Determination Protocol*.

IKE works in two phases: During phase 1, IKE checks the identity of the correspondent and negotiates a secure channel so that further IKE communication can be encrypted. Then during phase 2, the protocol negotiates *Security Associations (SAs)* that are used to protect packets from other applications.

A ***Security Association (SA)*** represents a specification of the security services offered to traffic carried through a unidirectional channel from one node to another. A separate SA is necessary to offer secure traffic in the reverse direction between the same pair of nodes. In other words, there are two SAs associated with bi-directional traffic between a pair of communicating peers. An SA can offer either the AH or the ESP service, but not both. Two security associations are necessary to provide both types of services simultaneously. A total of four SAs are required for bi-directional traffic using both AH and ESP.

The actual IPsec encryption and authentication is generally implemented in the kernel with the aid of two databases: the ***Security Policy Database (SPD)*** and the ***Security Association Database (SAD)***.

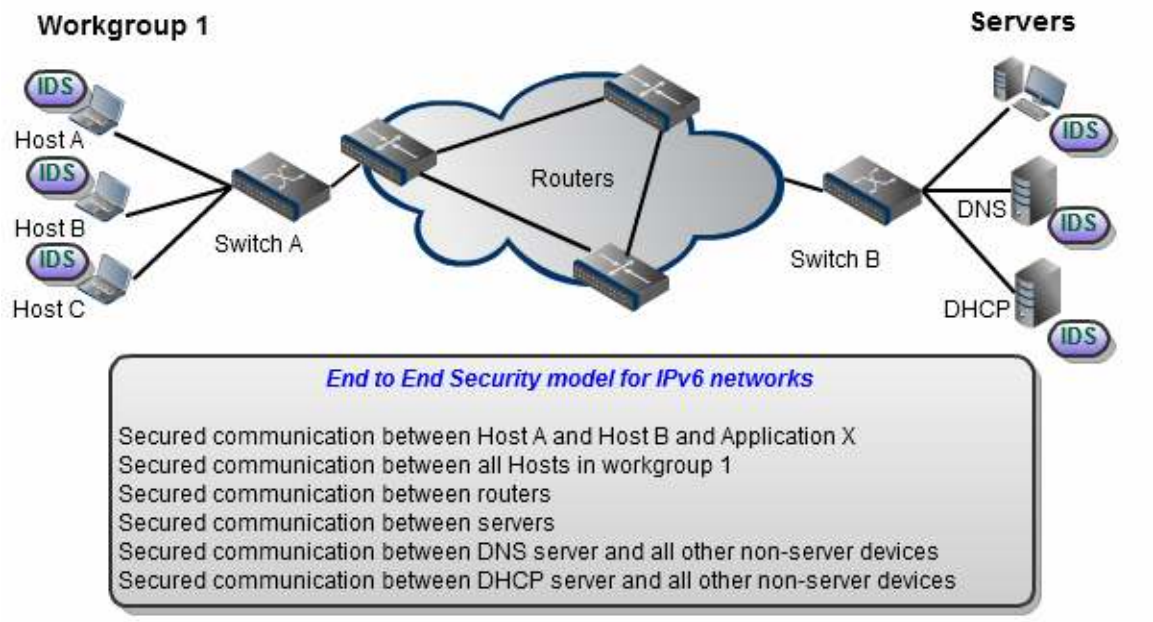
The ***Security Policy Database*** *(SPD)* contains a set of rules that determines whether a packet is subject to IPsec processing and governs the processing details. Each entry in the SPD represents a policy that defines how the set of traffic covered under the policy will be processed.

The ***Security Association Database*** *(SAD)* is a central repository containing all of the active SAs for both inbound and outbound traffic, with each entry defining the parameters for a specific SA.

The SPD is a lot like an IP filter: packets are matched based on source and destination addresses or prefixes, protocol, and port numbers. Matching packets are allowed through, blocked, or piped through AH or ESP in transport mode or tunnel mode. When packets match an AH/ESP entry in the *SPD*, the *SAD* is consulted to determine the exact authentication and encryption parameters. If there are no SAD entries, the IKE daemon is triggered, which then negotiates a Security Association with its counterpart on the remote system.

End-to-End security for IPv6 Networks

IPv6 network architectures can simply adjust to an end-to-end security structure where the end hosts have the task of providing the security services required to protect any data traffic between them. This result in better flexibility for creating policy-based trust domains that are based on altering parameters including node address and application, as shown in the figure below. Every device or end-host can be a member of multiple trust domains, each subject to varying security policies.



When a couple of end devices requests to communicate securely, they can initiate an authenticated and confidential exchange. These end devices can be end-hosts, servers or routers as the end points in an end-to-end model illustrate the device that is either initiating or receiving the data. Generally workstation or server based security implementations increase or improve local security measures to enforce data integrity, impede exploitation of the system, and ensure system availability.

An end-to-end security structure does not signify that there won't be any security services within the network infrastructure. In contrast, security services have to be deployed in both areas to augment the security in depth. There exist a number of mixed scenarios that merge end-to-end and network centric security architectures when deploying IPv6. For many transition networks these hybrid solutions can offer a gradual shift to native IPv6 networks while still maintaining a secure network which mitigates most of the recognized vulnerabilities. The exchange is often a decision based on performance against management.

Transition mechanism security considerations

IPv6 networks will operate in parallel with IPv4 based networks in many environments, possibly for a longtime. Thus the effective approach is to migrate from IPv4 to IPv6 or to support their coexistence. This requires transition specific protocols that bring into networks their own security vulnerabilities.

Currently available transition approaches include:

- **Dual Stack**: Support of both IPv4 and IPv6 on network devices.
- **Tunneling**: Encapsulation of an IPv6 packet within an IPv4 packet for transmission over an IPv4 network or vice versa.
- **Translation**: IP header, address, and/or port translation such as that performed by gateway or NAT devices.

The two basic transition mechanisms that are widely adopted are the ***Dual-stack mechanism*** and the ***Tunneling mechanism***.

Security for dual-stack configuration:

In dual-stack approach the network node has two separated protocol stacks for IPv4 and IPv6 respectively. Both IPv4 and IPv6 traffic will be running on the device and the application will decide which transport layer to use. The IPv4 or IPv6 datagram's arriving at the network interface is analyzed and forwarded to the IPv4 stack or IPv6 stack correspondingly for further processing.

Managing the security configurations of both IPv4 and IPv6 infrastructures will be a main concern. Applications can be targeted by both IPv4 and IPv6 attacks. Thus firewalls, IDS/IPS on such hosts must support both IPv4 and IPv6 protocols and must have proper filtering and detection rules for both protocols.

However configuring packet filter rules and access lists to provide the same level of protection for both protocols will be complex. It is recommended to have mechanisms to correlate logs and auditing tools for both IPv4 and IPv6 traffic to recognize any potential attacks.

Security for tunneling mechanism:

Tunnels are either configured or automatic. *Configured tunnels* are pre-defined by administrators in advance of communications. Tunnel endpoints are preconfigured and the IPv6 packets are tunneled based on the destination with other tunnel configuration parameters required for tunnel implementation. *Automatic tunnel* does not need tunnel pre-configuration but enabling the tunnel configuration may be required. Automatic tunnels are created based on the IPv6 packet information such as source or destination IP address. Some of the automatic tunneling techniques are given below:

- **6to4:** Automatic router-to-router tunneling based on a particular global address prefix and embedded IPv4 address.
- **ISATAP:** Automatic host-to-router, router-to-host, or host-to-host tunnelling based on a particular IPv6 address format with inclusion of an embedded IPv4 address.
- **Teredo:** Automatic tunneling through NAT firewalls over IPv4 networks.
- **Tunnel Brokers:** Automatic tunnel setup by a server acting as a tunnel broker in assigning tunnel gateway resources on behalf of hosts requiring tunneling.
- **Dual-stack transition mechanism:** Enables automatic tunneling of IPv4 packets over IPv6 networks.

Any tunneling mechanism mentioned above is related to a number of security issues which include exploiting the tunnel interface and bypassing ingress filtering checks since it is usual to create a hole in the firewall to allow tunnelled traffic to pass through.

While carrying IPv6 traffic over an IPv4 tunnel, the firewall rules will let IPv4 traffic through without examining the encapsulated IPv6 traffic which might contain malicious packets. Network addresses within the IPv6 & IPv4 headers may be spoofed which gives way to DoS attacks.

Therefore proper IPv6 ingress filtering must be performed before accepting the IPv6 packet and deploying IPsec between endpoints can provide additional protection. Traffic monitoring and detection of abnormal behaviour is critical.

Since tunneling mechanism have more security issues it is recommended to use dual-stack configurations rather than tunneling. If tunneling is in use, it is more secure to use manual tunnels rather than automatic tunnels as it offers more control, but the administrative overhead to configure the manual tunnels are not always operationally optimal.

Various Security threats in IPv6

a. Security threats related to IPv6 routing headers

IPv6 packet structure allows routing headers, which list the addresses of one or more intermediate nodes that the packets will go through. An attacker can generate specific packets with routing headers to reach hosts that normally would not accept the attacker's traffic. Further, if an end point accepts these headers and follows their routing instructions, trusted nodes could forward malicious packets or the flow of packets could lead to resource exhaustion at the routers, resulting in a DoS attack.

Routing Header Type-0 (RH0) does not have any important applications; it only generates security issues. Routing header is an extension of the IPv6 header. So in the network every router or node has to process routing header which made the dream come true for DoS attackers. To defense from this issue, just disable RH0 feature in your network.

Unfortunately, *Mobile IPv6* requires routing headers. Networks with MIPv6 functionality should therefore incorporate mechanisms to securely handle packets with these headers; otherwise, they should not allow these packets.

b. Fragmentation related attacks

In IPv6 networks, fragmentation is done by the end hosts only, intermediate router or host cannot fragment the packets. So, end host have to do MTU discovery along the way and then fragment the packets. Sometimes receiver side, firewall drops the packets due to this fragmentation feature.

The minimum recommended *MTU size* for IPv6 is 1280 octets. For security purpose it is recommended to drop all fragments with less than 1280 octets unless the packet is the last in the flow. By using fragmentation an intruder can attain that port numbers are not found in the first fragment and in that way bypass security monitoring devices (which do not reassemble fragments) expecting to find transport layer protocol data in the first fragment.

An attacker sends a large number of small fragments causing an overload of reconstruction buffers on the target system potentially implying a system to crash, a type of a DoS attack. This type of attack can be avoided by *limiting the total number of fragments and their arrival rate.*

c. Security threats related to ICMPv6 and multicast

In IPv4 networks it was possible to block most of ICMP messages without a direct influence to the proper network functionality.

Alternatively, in IPv6 networks some important functions such as neighbor discovery and path maximum transmission unit discovery mechanisms are dependent on some types of ICMPv6 messages. Therefore, some ICMPv6 messages must be allowed for proper network operation (e.g. a '*parameter problem*' message is required if an unrecognized option occurs in the IPv6 packet header or a '*packet too big*' message is necessary for the procedure of path maximum transmission unit discovery).

But if an attacker generates a flood of ICMPv6 messages, a victim node or network segment will suffer decreased performance.

IPv6 has standard multicast address for important devices such as the "*all routers*" and "*all DHCP servers*" groups. An attacker can modify messages directed to these addresses on a network and receive

information that helps to identify key systems on which to target attacks.

ICMPv6 pattern allows an error notification response to be sent to multicast addresses (if a packet was targeted to a multicast address). That fact can be misused by an attacker. By sending an appropriate packet to a multicast address an attacker can cause multiple responses targeted at the victim (the spoofed source of the multicast packet).

Smurf-type attacks are still possible on multicast traffic. *Filtering out unnecessary traffic* is the recommended best practice.

d. Reconnaissance attacks in IPv6 networks

Scanning for valid host addresses and services is extensively more difficult in IPv6 networks than IPv4 networks.

Host probing and *port scanning* are usually the initial activities an attacker engages in to discover vulnerabilities in a network. In host probing, the attacker tries to identify the hosts connected to a network. Once the hosts are found, the attacker uses port scanning to look for exploitable vulnerabilities. The potentially huge size of IPv6 subnets makes reconnaissance attacks more difficult, but there are other ways to identify target systems.

The attacker might find that a network administrator uses a *sequential numbering* scheme to assign IP addresses to hosts; thus, finding hosts to scan becomes trivial.

IPv6's multicast address structure lets an attacker identify groups of key network components, such as all the *"routers"* or all *"DHCP servers"* for a given network, thereby providing an opportunity to scan these devices' vulnerabilities. Also querying the router neighbor discovery cache in poorly secured routers can cause issues.

Administrators can use *IPsec* security services to reduce packet sniffing, looking at a packet's content and port scanning activities. The difficulty in scanning posed by IPv6 addressing also makes it hard for an administrator to identify hosts that are either malicious or possible targets for attackers.

Other types of attacks known in IPv4 networks such as ***Sniffing attacks, Application layer attacks, Flooding attacks, Rogue devices*** and ***Man-in-the-middle attacks*** did not fundamentally change appearance in IPv6 protocol. They take affect both in IPv4 and IPv6 networks.

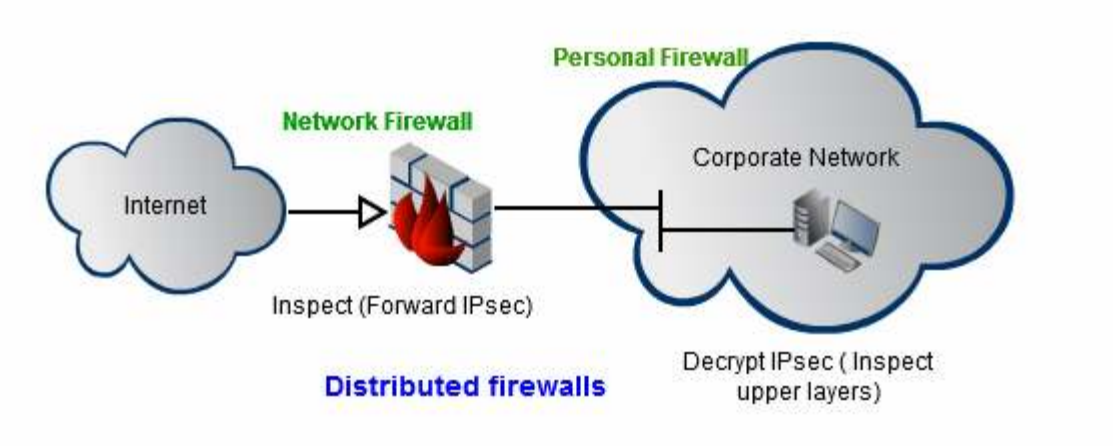
Firewalls in IPv6 Networks

Currently, many open-source and commercial firewalls supporting IPv6 are available. They act as network traffic filters filtering all traffic that enters or leaves the local network. Firewalls are usually positioned between a Local area network (LAN) and the internet which is considered to be insecure (or any other insecure network). Each and every packet is being analysed and the results are compared with a predefined set of rules. Based on the predefined rules, the packet can be accepted, discarded or sent to an additional check.

Many freeware and commercial firewalls are present for IPv4 networks with user-friendly graphical interfaces which enable user to define filtering rules easily. Many of them already have a predefined set of filtering rules for frequently used applications such as e-mail clients, web browsers etc. The users are allowed to modify existing rules and add new ones.

IPv4 and IPv6 traffic must be defined with separate filtering rules. IPv6 networks must have support for IPv6 protocol, as IPv6 has new packet header format which must be properly recognized and processed by IPv6 firewall. ICMPv6 protocol must be supported by IPv6 firewall. In IPv4 networks, ICMP messages can be filtered by firewall, whereas in IPv6 networks some ICMPv6 messages must be allowed since they are essential for proper network functioning.

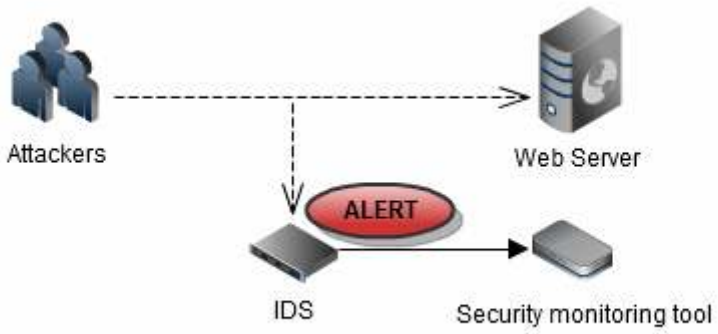
Linux platform has an "ip6tables" tool for configuring IPv6 firewall for writing filtering rules for IPv6 traffic. "ip6tables" is very similar to the IPv4 firewall "iptables" tool. Microsoft Windows platform uses a "Windows Firewall" which supports IPv6 protocol.



One of the most common hybrid security models will incorporate the concept of ***"Distributed firewalls"***. It consists of supervised host-based firewalls in addition to the conventional perimeter firewall model. The addition of managed host-based firewall security increases "defence in depth" to an enterprise's security architecture and reduces trust on a single "*chokepoint*" perimeter security network design.

Present firewall systems typically perform all security screening through a common checkpoint. The performance of a single checkpoint approach is increasingly degraded as broadband traffic increases over time, new network protocols are added, and as end to end networking and encrypted tunnelling become more widespread.

IDS in IPv6 Networks



Intrusion Detection System (IDS) is a software or hardware system for supervision and analysis of different events occurring in a particular host or on the network. The purpose of the IDS system is to discover potential security problems and to detect an unauthorized intrusion and misuse of network resources. They also detect distributed denial of service (DDoS) attacks, worms, and virus outbreaks.

It logs files (***host-based intrusion detection systems***, HIDS) or monitors traffic (***network-based intrusion detection systems***, NIDS) and issues alerts when a suspected attack is detected. *Knowledge-based intrusion detection* depends on databases of known attack patterns. The challenge here is to keep the database up-to-date and facilitating fast search. *Anomaly-based intrusion detection* is based on the principle that intrusions are apparent differences from normal behaviour.

The NIDS system captures and analyzes network traffic on a complete local network or a network segment protecting many hosts simultaneously. The HIDS system protects a single host. For achieving maximum level of protection it is recommended to install the HIDS system at every host in LAN. The NIDS system should be implemented on every segment (subnet) of LAN or at least between LAN and the Internet. Such placement of HIDS and NIDS systems enables detection

of outside attacks such as unauthorized activities of local users.

For IPv4 networks exists some open source IDS systems. By using software IDS systems in IPv4 networks, procedure of intrusion detection can be automated. In that case intrusion attempt will be recognized and logged by IDS system and user will be warned.

There are several commercial IDS systems with IPv6 support. But the situation considering IPv6 support by non-commercial IDS systems is not so good.

IPv6 supporting the IDS system must consider some new things typical of the IPv6 protocol. IPv6 defines a new header format that the IDS system must properly recognize. In order to simplify the main header, IPv6 introduces extension headers (such as Hop-by-hop, Routing, Fragment, Destination Options, Authentication, and Encapsulation Security Payload). The Next Header type also permits new types of IPv6 extension headers to be defined and implemented. The IDS system must implement support for these types of headers. A proper header order is also defined, thus it is desirable for IDS to check the order of extension headers. It is recommended for IDS to discard a packet with an undefined "Next Header" value and to record this as incident.

A Hop-by-hop options header is the only header examined at each hop along the path from the source to the destination node. Since it may have multiple or repeated options an IDS system should be capable of detecting irregular or duplicate options. A Destination options header should also be checked by IDS due to a possibility of irregular or duplicate options. A Bad hop-by-hop option or a destination option can be established intentionally by an attacker. If the node is set to send an ICMP error message in case of bad options, it can be misused for a smurf-like attack.

IDS with IPv6 support should also be able to recognize and analyze IPv6 traffic tunnelled in IPv4. That implies support for both automatic and manual tunnels. Proper deployment of IDS is also very important. If a node or a network has separate connections for IPv4 and IPv6, it is necessary to deploy proper IDS for every connection. For a dual-stack node with a single connection deployed IDS must recognize and support both protocols. If IPv6 traffic is tunnelled, a tunnel should be terminated outside the IPv6 firewall and IDS deployed at the ingress point of a network, behind firewall.

Positioning of IDS and Firewalls:

The highest possible security level (considering *firewalls and IDS systems*) connotes usage of properly configured firewalls and IDS systems positioned on appropriate locations inside the network.

The first step toward this goal is positioning firewall at the ingress point of the local network (i.e. between the local network and the Internet). It is recommended to deploy an IDS system in front and behind of that firewall. IDS system located in front of that firewall (i.e. between firewall and the Internet) will record all intrusion attempts, and IDS system positioned behind will record intrusions that successfully passed through firewall.

Deployment of *firewall and IDS* system on every segment of local network is also commendable. It is even possible to install firewall and Host-Based IDS system on every single host in local network. Possibility of intrusion detection is very important in networks that require a high level of security and protection.

IPv6 Security Considerations

Several security procedures must be followed to ensure a secure IPv6 communication network. The considerations are significant in order to increase the defense-in-depth. Several factors such as costs, network size, required quality of service, the transition mechanism used and the level of protection needed during the transition play a vital role. It is impractical to create a uniform security policy for all IPv6 environments. The main consideration is to maintain the integrity, confidentiality, accountability and availability of the data and the required devices.

A risk assessment must be performed to determine how the security policy should be applied while migrating to IPv6. Some of the vital considerations to be followed are given below:

- Effective filtering and auditing of IPv6 addresses is necessary as most devices have multiple IPv6 addresses per interface.

- Firewall filtering policies should to be modified to adapt IPv6 scenarios.

- IPsec provides secure peer-to-peer communication and it can also be used for secure end-to- end communication between IPv6 nodes for authentication and integrity. Thus it will not only secure IPv6 clients and servers but also the dual-stack routers and tunnel broker devices.

- Transition mechanism such as tunneling solution will create more security concerns due to the ease at which tunnel end points can be spoofed. Thus, where to tunnel and whether to use static or dynamic tunnels will have to be determined.

- If the filtering and auditing can be executed at the host level rather than within the network infrastructure then end-to-end confidentiality using IPSec can become a viable security policy mandate.

- Mandatory use of Fully Qualified Domain Names (FQDN) and DNS to locate users is necessary as IPv6 depends heavily on DNS. This requires DHCPv6 (server & client) and dynamic updates to DNS.

End-Host Security:

End-Host Security relates to any client & server that is IPv6 capable. The main concerns are to ensure that:

- Spoofing is avoided by performing address reassignment in a reliable manner.
- Protection against deletion, modification or spoofing of traffic sourced from or destined to an end-host.
- Detection and subversion of malicious behavior.

All devices themselves need to be hardened similar to any IPv4 environment. The exception is that since IPSec is available, it is recommended to use IPSec ESP with NULL encryption to provide integrity and authentication services between all endpoint communications. In addition, the following guidelines should be applied:

- Individuals must be authenticated and authorized using client or server.
- Monitor and audit access to the client and server.
- Unused services on the end node should be turned off.
- Traffic that gets processed by upper layer protocols can be controlled using capabilities in host firewall.

- Virus scanners can be used to detect malicious activity.

Network Infrastructure Security:

It relates to the components that make up the network infrastructure which includes the routers, switches, firewalls, IDS/IPS as well as network services such as AAA, Syslog, DNS, DHCP, SNMP and NTP. All these components should be secured using the following guidelines:

- IPv6 access for telnet and ssh should be restricted.
- Individuals must be authenticated and authorized using certain device.
- Monitor and audit access to the device frequently.
- Unused services on the device should be turned off.
- Use virus scanners to detect any malicious activity (mostly applicable to DNS, DHCP servers).
- Provide integrity and authentication services between communicating peers by using IPSec ESP with NULL encryption.

IPv6 Security and Hacking tools

Many security monitoring and auditing tools lack IPv6 support and the tools that exist are limited in their capabilities. Some open source security tools and hacking tools that support IPv6 are given below:

- **THC-IPv6:** a tool suite for attacking IPv6-based networks.
- **Multi-Generator (MGEN), Scapy6 and Ipv6PacketGen:** tools for generating IPv6 packets/traffic.
- **NDPWatch:** keeps a database of Ethernet versus IPv6 address pairings and reports any changes to the pairings.
- **Neighbor Discovery Protocol Monitor (NDPmon):** monitors the local network and reports any suspicious ND messages.
- **Detect DAD Denial of Service (ddaddos):** monitors a network to detect any DAD-based attack.
- **Nmap:** network vulnerability scanner.
- **Wireshark/Ethereal:** network protocol analyzer.
- **Netcat6:** utility to read and write data across IPv6 network connections.
- **Snort:** open source network intrusion prevention and detection system (IDS/IPS).
- **6tunneldos, 4to6DDOS, Imps6-tools:** tools for generating Dos and DDoS attack.
- **SendIP, Packit, Spak6:** used for Packet forging.
- **Slapper:** family of worms that use an OpenSSL buffer overflow exploit to run a shell on a remote computer.

Conclusion

For every secure network, the aim is to protect every device that is participating in the network communication and all information that is either stored on a device or is in transit between communicating devices. While IPv6 offers better security (use of encrypted communication and larger address space), the protocol also raises new security challenges. As most vulnerabilities are found in the upper layer, no layer-3 protocol will help an broken browser, unsecured DNS or broken database application. Even when it comes to Layer3 issues that are previously-known, IPv6 is not that different from IPv4. Security and Transition were the two major goals of IPv6. But now secure transition became the major goal of IPv6. Thus it is not more secure or less secure than IPv4. The controversy of whether network based security is better than host based security should be resolved with the understanding that a layered security approach is necessary. A combination of host, network and application based security is required to secure networks. Successful solving of the security issues will certainly contribute to wider acceptance and usage of IPv6 protocol. Therefore it is necessary to make furthermore study and accumulate experiences.

Glossary

AAA: Authentication, Authorization and Accounting.
AC: Auto Configuration
AES: Advanced Encryption Standard
AH: Authentication Header
ARP: Address Resolution Protocol
Ddaddos: Detect DAD Denial of Service
DDoS: Distributed Denial of Service
DES: Data Encryption Standard
DHCPv6: Dynamic Host Configuration Protocol
DNS: Domain Name System
DoS: Denial of Service
ESP: Encapsulating Security Payload
E2E: End to End
FTP: File Transfer Protocol
FQDN: Fully Qualified Domain Names
HIDS: Host-based Intrusion Detection Systems
HMAC: Hash-based Message Authentication Code
ICV: Integrity Check Value
ICMPv6: Internet Control Message Protocol
IDS: Intrusion Detection System
IKEv2: Internet Key Exchange version 2
IPS: Intrusion Prevention System
IPsec: Internet Protocol Security
IPv4: Internet Protocol version 4
IPv6: Internet Protocol version 6
ISAKMP: Internet Security Association and Key Management Protocol
ISATAP: Intra-Site Automatic Tunnel Addressing Protocol
LAN: Local Area Network
MAC: Media Access Control

MGEN: Multi-Generator
MIPv6: Mobile Internet Protocol version 6
MITM: Man In The Middle Attack
MTU: Maximum Transmission Unit
NA: Neighbor Advertisement
NAT: Network Address Translation
ND: Neighbor Discovery
NDPmon: Neighbor Discovery Protocol Monitor
NIDS: Network-based Intrusion Detection Systems
Nmap: Network Mapper
NS: Neighbor Solicitation
NTP: Network Time Protocol
PING: Packet Internet Groper
QoS: Quality of Service
RH: Routing Header
RSVP: Resource Reservation Protocol
SA: Security Association
SAD: Security Association Database
SEND: Secure Neighbor Discovery
SLAAC: Stateless Address Auto Configuration
SG: Security Gateways
SNMP: Simple Network Management Protocol
SPI: Security Parameters Index
SPD: Security Policy Database
SSH: Secure Shell
SSL: Secure Sockets Layer
TCP: Transport Control Protocol
ToS: Type of Service
TLS: Transport Layer Security
UDP: User Datagram Protocol
VoIP: Voice over Internet Protocol
VPN: Virtual Private Network
WAN: Wide Area Network

References (A-Z)

Abdur Rahim Choudhary, Scientist, Serco North America - *In-depth Analysis of IPv6 Security Posture, 2009.*

Abdur Rahim Choudhary, Alan Sekelsky - *Securing IPv6 Network Infrastructure:A New Security Model, IEEE, 2010.*

Carol Kavalla, Global Knowledge Instructor - *Why Install IPv6 Instead Of IPv4, 2009.*

Carlos E. Caicedo and James B.D. Joshi, University of Pittsburgh and Summit R. Tuladhar, Ericsson - *IPv6 Security Challenges, 2009.*

Christer Engman, Stockholm, Sweden – *IPv6@home, A study on using IPv6 in home networks, 1999.*

Dequan Yang, Xu Song, Qiao Guo - *Security on IPv6, IEEE, 2010.*

Dieter Gollmann - John Wiley & Sons, Inc, *Computer security*, *2010.*

Drago Zagar, Faculty of Electrical Engineering, University of Osijek, Croatia - *IPv6 Security threats and possible solutions, 2006.*

Drago Zagar, Kresimir Grgic´, Snjezana Rimac-Drlje - *Security aspects in IPv6 networks - implementation and testing, 2007.*

Emre Durdagi, Ali Buldu - IPV4/IPV6 security and threat comparisons, 2010.

Edward Lewis, NeuStar, Inc., Sterling, VA - *Moving from IPv4 to IPv6.*

Fernando Gont, Sao Paulo, Brazil - *Results of a Security Assessment of the Internet Protocol version 6 (IPv6), 2010.*

Georgios Koutepas, National Technical University of Athens, Greece - *IPv6 Transition Mechanisms and their Security and Management, 2006.*

IPv6 (2nd Edition), Pete Loshin, *Chapter 15 - (IPv6 Deployment and IPv6 Coexistence) and Chapter 2 (Internet Protocol version 6).*

Iljitsch van Beijnum – Running IPv6, *Chapter 9 (Security)*.

Jalan Gadong, *Information Technology Protective Security Services - IPv6-to-IPv4 Transition and Security Issues, 2008.*

Jason Detchevery, Lawrie Brown - *IP and Web Security*, *2009.*

Joe Davies, Principal Technical Writer Windows Server User Assistance Microsoft Corporation - *Understanding IPv6 Transition Technologies, 2009.*

Muhammad Rizwan Sabir, University of Engineering and Technology, Lahore, Pakistan - *An Overview of IPv4 to IPv6 Transition and Security Issues, 2009.*

Omar Santos, Senior network security engineer, Cisco - *End-to-End Network Security Defense-in-Depth, 2008.*

Pedro J. Muñoz Merino, Alberto García-Martínez, Mario Muñoz Organero, and Carlos Delgado Kloos - *Enabling Practical IPsec Authentication for the Internet, 2006*.

Philip Hunter - *IPv6: Security Issues, 2009.*

Piush Sinha, TCS, India - IPv6 Network Security, 2008.

Procurve Networking (HP Innovation): *IPv6 – The Next Generation of Networking, 2006.*
Qing Li, Tatuya Jinmei, Keiichi Shima, IPv6 Advanced Protocols Implementation, *Chapter 6 (Pages 903-952) — IPv6 and IP Security, 2007.*

Rahul Banerjee, Birla Institute of Technology & Science (BITS), Pilani (India) - *The Internet Protocol (IPv6): Challenges and Issues for the Next Generation Internetworking, 2002.*

Ron Broersma, Internet2 Members Meeting Arlington, VA - *Securing an IPv6 Network, 2005*.

R Radhakrishnan, Majid Jamil, Shabana Mehfuz, Moinuddin - *Security issues in IPv6, IEEE, 2007.*

Sajjad Tabib, Sanjose University, Computer Engineering Department - *Network Security Team Research Paper on: Analysis of IPv6 Security, 2008.*

Samuel Sotillo, East Carolina University - *IPv6 Security Issues, 2006.*

Surekha Shinde – *Project IPv6 Security Aspects (PowerPoint presentation).*

Tushar M. Raste, D.B. Kulkarni - *Design and implementation scheme for deploying IPv4 over IPv6 tunnel, 2006.*

Troy A. Buchanan – *IPv6: IP Addressing Solution for the next 25 years, 2008.*

YI Xiushuang, Network Center, North-eastern University, China - *Sniffing threat and practices in ipv6, 2006*.