

IPv6 Security (IPSEC)

Advanced Networking



Maks Miketa N0945100

Contents

[IPv6 and IPSEC Overview 3](#_Toc102483337)

[What is IPv6? 3](#_Toc102483338)

[What is IPsec? 3](#_Toc102483339)

[Comparison with IPv4 3](#_Toc102483340)

[Differences 3](#_Toc102483341)

[IPv6 and IPSEC Security Features 5](#_Toc102483342)

[Native Security 5](#_Toc102483343)

[Quality of Service (QoS) 5](#_Toc102483344)

[Auto-Configuration 5](#_Toc102483345)

[New Extension Headers 5](#_Toc102483346)

[Security Associations 6](#_Toc102483347)

[IKE Phase 1 6](#_Toc102483348)

[IKE Phase 2 6](#_Toc102483349)

[IPsec Transport and Tunnel Modes 7](#_Toc102483350)

[Authentication Header 7](#_Toc102483351)

[Encapsulating Security Payload Header 7](#_Toc102483352)

[Transport Mode 7](#_Toc102483353)

[Tunnel Mode 8](#_Toc102483354)

[References 8](#_Toc102483355)

# IPv6 and IPSEC Overview

## What is IPv6?

IPv6 is the most recent Internet Protocol version (IP). It is intended to provide IP addressing and improved security to support the anticipated growth of linked devices in IoT, manufacturing, and new fields such as autonomous driving. IPv6 uses hexadecimal addressing structure with each hex digit representing 4 bits. IPv6 addressing helps to reduce routing table size by allowing ISPs to aggregate customers' prefixes into a single prefix and present only that one prefix out to the IPv6 internet. (What Is IPv6?, 2022).

## What is IPsec?

IPsec (Internet Protocol Security) is a set of protocols and algorithms used to secure data sent over the internet or any public network. In the mid-1990s, the Internet Engineering Task Force, or IETF, created the IPsec protocols to provide security at the IP layer through authentication and encryption of IP network packets (Loshin, 2021). IPSEC is mainly applied to virtual private networks (VPNs). IPsec can be implemented on routers which only requires minimal changes between the routers and end host implementation to provide more flexibility and security but there is more work required compared to implementing IPsec on routers.

# Comparison with IPv4

IPv4 is an abbreviation for the internet Protocol version 4. It is the fundamental technology that makes it possible to connect devices to the internet. When a device connects to the internet, it is provided with a unique IP address. To transport data from one computer to another via the internet, a data packet containing both devices IP addresses must be exchanged across the network (IPv4 vs. IPv6, 2022). The original IPv4 IP address scheme has ran out of addresses as announced by the RIPE NCC in November 2019 (The IPv4 run-out – one year on, 2021). IPv4’s address pool is 32-bits (232) in size and contains 4,294,967,296 addresses that are all assigned.

### Differences

There are many differences between IPv4 and IPv6. They are very similar by using IP addresses to identify machines however, they are different in how they work.

#### Size of IP Address/Addressing Method

IPv4 has a 32-bit numeric IP address, and its binary bits are separated by a dot. It can generate 4.29×109 address space that offers five different classes of IP address that are class A to E whilst IPv6 has a 128-bit alphanumeric IP address with the binary bits separated using a colon and it also contains hexadecimals. IPv6 can produce 3.4×1038 address space and allows an unlimited number of IP addresses stored.

#### Header Fields

There is a difference in the headers as IPv4 contains a checksum field within the header to detect corruption within the header of the packets unlike in IPv6 however, it is not included as the upper layer protocols such as UDP and TCP have their own checksum fields as well as the ethernet layer including CRC validation making it unnecessary.

Table

Description automatically generated

Figure - IPv4 and IPv6 Header Comparison (IPv4 vs IPv6 - Understanding the differences, n.d.)

IPv6 supports 8 fields in the header for improved efficiency. It contains 3 fields that remain the same that are the version to identify the IP protocol in use, source address to identify the sender of the packet and destination address to identify the network layer in the packet. It also contains 4 fields that have the same functionality but are renamed. The Type of Service and Traffic Class are used for traffic classification and marking, Total Length and Payload Length indicate the length of the IP packet with IPv6 including the extension header but not including the main IP header. Time to Live and Hop Limit ensure that packets do not loop around the network and Protocol and Next Header that indicate the protocol being transported in the payload portion. IPv6 does not include the Internet Header Length as it has a fixed header length, Identification, Flags, Fragment Offset which is used by the Fragmentation extension header, Options also used by extension header and Padding as IPv6 is fixed sized do padding is unnecessary. Only the Flow Label does not exist in IPv4 that is used for identifying if a packet is part of a sequence and must be handled the same way as the entire traffic flow (IPv4 vs IPv6 - Understanding the differences, n.d.).

#### Additional Differences

Unlike IPv4, IPSEC is mandatory within the IPv6 protocol specification which allows IPv6 packet authentication and/or payload encryption via Extension Headers. However, IPSEC is not automatically implemented therefore, it must be configured and utilised with a security key exchange. (IPv6 Packet Security | IPv6 Now, 2007).

IPv4 must be configured before communicating with other systems, it supports VLSM, RIP, SNMP, DHSC, ARP to map to a MAC address and the network requires manual or DHCP configuration of the network. IPv6 does not require any of these protocols (Williams, 2022). IPv6 does not have a broadcast address as its multicast address serves the same purpose.

# IPv6 and IPSEC Security Features

### Native Security

Since IPSEC is mandatory in IPV6, it provides end-to-end security whilst data is getting sent through routers, internet etc. from the originating host to the destination host.

### Quality of Service (QoS)

QoS ensures that high priority is given to the packets that need to arrive to their destination at a timely manner. It improves streaming videos and voice over IP by making sure the packets arrive close together to avoid lagging voice or video.

### Auto-Configuration

It is easier to configure network as devices are given a permanent address and do not require manual configuration due to stateful and stateless auto-configuration of IP Addresses. The stateful auto-configuration utilises DHCP in which static tables are maintained to determine the IP address to be given to a node without the use of DHCP.

### New Extension Headers

IPv6 includes several extension headers with possible new additional headers in the future. Extension headers, which are put between the fixed header and the upper-layer protocol header, carry optional internet layer information.

Hop-by-Hop Options Header - A set of options required by routers to conduct specific administration or debugging functions.

Routing Header – Similar to IPv4's source routing options. It is used to define a specific routing.

Destination Options Header - This header contains a collection of options that will only be processed by the last destination node. A Destination Options Header is an example of one.

Fragmentation Header - The Fragmentation Header is identical to the IPv4 fragmentation options.

Authentication Header (AH) - A security header that facilitates for authentication and integrity.

ESP Header - An encapsulating security payload (ESP) header that provides authentication and encryption.

# Security Associations

Security Association (SA) is a fundamental concept in IPsec. SA is uniquely identified by the Security Parameters Index which is a field in the AH and ESP header, the destination IP address and security protocol. The selection of SA can include pre shared keys, but Internet Key Exchange (IKE) can be used to generate shared security keys to establish the SA. SAs are needed for the encryption and decryption processes to negotiate a security level between two entities. A special router or firewall that sits between two networks usually handles the SA negotiation process. To establish an IPsec tunnel, the IKE protocol is used. IKE has two phases that are the IKE Phase 1 and IKE Phase 2.

IKE Phase 1 establishes an ISAKMP session between two peers to negotiate the encryption, authentication, hashing and other protocols that are required or want to be used (SA’s). IKE Phase 1 is only used for management traffic therefore, the tunnel is used as a secure method to establish the IKE phase 2 tunnel which is used to protect user data. IKE builds the tunnels but does not authenticate or encrypt user data as the AH And ESP protocols do this instead.

### IKE Phase 1

In IKE phase 1, there are three steps to establish a secure tunnel that are the negotiation, DH Key Exchange and authentication. In step 1, the peer containing traffic will initiate the negotiation stage. Two peers negotiate: hashing which is used to verify integrity, authentication through pre-shared keys or digital certificates, DH (Diffie Hellman) group that determines the strength of the key used within the key exchange process (higher group numbers are more secure but take longer to process), lifetime of the IKE phase 1 and encryption. After successful negotiation, the DH group that was negotiated is used to exchange the key material resulting in both the peers’ sharing keys. Lastly, both peers authenticate each other using the authentication method agreed upon negotiation. The main or aggressive mode can be used to complete authentication. The main mode uses 6 messages whilst aggressive mode uses 3 messages to establish the SA. Main mode is considered more secure as identification is encrypted as aggressive mode does this in clear text. After authentication, IKE phase 1 is completed resulting in a bidirectional IKE Phase 1 tunnel.

### IKE Phase 2

The IKE Phase 2 tunnel is built through quick mode which negotiates like negotiations in IKE phase 1. The IPsec protocol is decided (AH and/or ESP), encapsulation mode (transport/tunnel mode), encryption algorithm, authentication algorithm, lifetime and optionally DH exchange used for Perfect Forward Secrecy.

IKE consists of two versions that are IKEv1 and IKEv2. The first version was released around 1998 and its successor is IKEv2 released in 2005 with many more advantages such as requiring less bandwidth, supporting EAP authentication and built in keepalive mechanism for tunnels etc. IKEv2 does not have a main or aggressive mode for phase 1 and there’s no quick mode in phase 2. It still has two phases though, phase 1 is called the IKE\_SA\_INIT and the second phase is called IKE\_AUTH. Only four messages are required for the entire exchange.

# IPsec Transport and Tunnel Modes

IPsec operates in two different modes that are the transport mode (host-to-host) and tunnel mode (gateway-to-gateway or gateway-to-host). It is a common choice for VPN implementations.

### Authentication Header

The Authentication Header (AH) ensures data integrity and data authentication throughout the IPv6 packet. The AH also offers anti-replay protection. Packets are authenticated with an Integrity Check Value (ICV) calculated over the payload, the header, and unchanging fields of the IPv6 header and options. AH does not provide privacy and confidentiality of packet contents.

Data Authentication means that if a computer receives an IP packet with a given source address in the IP header, it can be assured that the IP packet arrived from that IP address and data integrity means that if a computer receives an IP packet, it can be assured that it was not modified, changed or manipulated along the path from the source to the destination. Anti-replay protection means that if a computer already received a packet, another packet containing modified data would not be accepted as valid data.

ICV is contained in the variable length Authentication Data which provides the authentication and integrity by an authentication algorithm specified by the SA. ICV is calculated over the IP header fields that are unchanged during delivery. The Hop Limit, Traffic Class, and Flow Label fields are changed during delivery. The ICV value is recalculated by the receiver of the IP packet with an AH header using the authentication algorithm and key identified in the SA. If the ICV is the same, the receiver knows that the data has been authenticated and has not been altered.

### Encapsulating Security Payload Header

The Encapsulating Security Payload (ESP) header provides confidentiality, authentication, data integrity and anti-replay protection to the encapsulated payload. The authentication algorithm is only applied to the data being encrypted during authentication in the ESP Header. As a result, unless the IP header fields are enclosed in "tunnel mode," the authentication technique does not protect them. Confidentiality refers to a computer receiving an IP packet that can be assured that no one else has seen the contents of the IP packet unless it is the router requiring necessary information. Both the confidentiality and authentication services are optional but, at least one of the services must be selected.

### Transport Mode

In transport mode, the IP addresses in the outer header are used to determine the IPsec policy that will be applied to the packet. IPsec protects what is delivered from the transport layer to the network layer thus, the payload to be encapsulated is protected in the network layer. Transport mode does not protect the IP header and the whole IP packet as it only protects the packet from the transport layer (IP-layer payload). Transport mode is less complex than tunnel mode as a new IP header is not created. Transport mode works by creating and inserting a new AH or ESP header after the original IP header. In ESP transport mode, both the ESP trailer and ESP authentication trailer are created and added after the original package and the original packet payload is signed by authentication (not including its IP header) and encrypted if required. In AH transport mode, the entire packet is signed for integrity and authentication.

Transport mode is best used when fast and secure end-to-end communications are required.

### Tunnel Mode

The entire original IP packet is encapsulated in tunnel mode to become the payload of a new IP packet. A new header is added to the to the top of the original IP packet. These IPsec gateways, in turn, can securely connect two distinct networks. Tunnel mode is beneficial for securing traffic between separate networks since a new packet is produced using the original information. Another advantage of using this mode is that it makes it very simple to create a "tunnel" between two secure IPsec gateways. Using secure IPsec proxies can be particularly beneficial for connecting two remote branches via an encrypted connection.

The original packet is encapsulated in a new IP packet including its IP header and its payload. If it is an AH tunnel mode, the AH header and a new IP header are added, and the entire packet is signed for integrity and authentication. If it is the ESP tunnel mode, the ESP header new IP header, ESP trailer and ESP authentication trailer are added. The ESP header and ESP trailer is signed for integrity and authentication and the new packet can be encrypted for increased security.

Tunnel mode is best used for configurations requiring a secure connection between two different networks that is separated by an intermediate untrusted network such as the internet.

Both ESP And AH can be used together at the same time in both modes to maximise security.

# References

Cisco. 2022. What Is IPv6?. [online] Available at: <https://www.cisco.com/c/en/us/solutions/ipv6/overview.html> [Accessed 15 April 2022].

DataCenterDynamics. 2021. The IPv4 run-out – one year on. [online] Available at: <https://www.datacenterdynamics.com/en/opinions/the-ipv4-run-out-one-year-on/#:~:text=Back%20in%20November%202019%2C%20the,its%20pool%20of%20IPv4%20addresses.> [Accessed 16 April 2022].

Hermann-Seton, P., 2005. Security Features in IPv6. [online] Giac.org. Available at: <https://www.giac.org/paper/gsec/2158/security-features-ipv6/103684#:~:text=IPv6%20supports%20many%20new%20features,for%20the%20entire%20IPv6%20packet.> [Accessed 29 April 2022].

Ipv6now.com.au. 2007. IPv6 Packet Security | IPv6 Now. [online] Available at: <http://www.ipv6now.com.au/primers/IPv6PacketSecurity.php#:~:text=Unlike%20IPv4%2C%20IPsec%20security%20is,with%20a%20security%20key%20exchange.> [Accessed 15 April 2022].

Loshin, P., 2021. What is IPsec (Internet Protocol Security)?. [online] SearchSecurity. Available at: <https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security> [Accessed 15 April 2022].

NetworkAcademy.io. n.d. IPv4 vs IPv6 - Understanding the differences. [online] Available at: <https://www.networkacademy.io/ccna/ipv6/ipv4-vs-ipv6> [Accessed 22 April 2022].

NetworkLessons.com. n.d. IPsec (Internet Protocol Security). [online] Available at: <https://networklessons.com/cisco/ccie-routing-switching/ipsec-internet-protocol-security> [Accessed 29 April 2022].

Sanoja, D., 2021. IPsec Tunnel Mode vs. Transport Mode. [online] Twingate.com. Available at: <https://www.twingate.com/blog/ipsec-tunnel-mode/> [Accessed 29 April 2022].

ThousandEyes. 2022. IPv4 vs. IPv6. [online] Available at: <https://www.thousandeyes.com/learning/techtorials/ipv4-vs-ipv6> [Accessed 16 April 2022].

Williams, L., 2022. IPv4 vs IPv6: What is the Difference Between IPv4 and IPv6?. [online] Guru99. Available at: <https://www.guru99.com/difference-ipv4-vs-ipv6.html> [Accessed 22 April 2022].