3.1 Types of threats

What is THREAT? A threat is -

- a statement by someone that they will do something unpleasant.
- an expression of intention to pain, harass, injury, or damage.

Most IPv6 security risks come from bugs in the code, protocol weaknesses and poor implementation by vendors. These risks are the result of the network industry not having as much familiarity with IPv6 as it does with IPv4, which has been around for 30 years.

"You turn on IPv6 and don't realize that your firewall doesn't process IPv6 traffic. It just passes it blindly through. Or you forget to set up filters," Schiller explains. "People have to consciously go in and take all the security infrastructure that's been created in IPv4 and mirror image it in IPv6."

IPv6 Threats

Most common IPv6 threats, that network vendors are hearing about from their enterprise customers:

1. Rogue/ fake IPv6 traffic

Organizations that aren't running IPv6 and don't plan to run it anytime soon, should use their firewalls to block IPv6 traffic from coming in and out of their networks.

- Most experts say this should be a temporary measure because an increasing amount of Internet traffic is IPv6-based, and organizations don't want to limit access to customers or business partners around the world that will be using IPv6.
- "What customers need to do within their intrusion-prevention systems or within their firewalls is to explicitly look for IPv6 traffic and drop it,"

2. IPv6 tunnels

Three types of IPv6 tunnels —Teredo, 6to4 and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) -- allow IPv6 packets to be encapsulated inside IPv4 packets that can be sent through IPv4-enabled firewalls or Network Address Translation(NAT) devices. To a network manager, tunneled IPv6 packets look like normal IPv4 traffic. That's why network managers need deep packet inspections systems that can peer into tunnels to examine what's inside of them.

- We need to have firewalls and intrusion-prevention systems that "support IPv6 but they also need to support full inspection for the tunneling mode."
- Attackers takes "traditional IPv4 attacks" that take advantage of IPv6 tunneling to enter networks where tunneling traffic wasn't being inspected.

3. Rogue IPv6 devices

The auto-configuration capabilities that are built into IPv6 allow an attacker to define a rogue device that assigns IP addresses to all the other devices on the network. Devices introduced into the network that are not authorized. A device may be a single PC, but it could be a switch, router, DNS server, DHCP server or even a wireless access point.

- "Someone could set up a rogue device like a router to assign IPv6 addresses on your network, and you wouldn't even know it,"
- "A hacker can set up a rogue network device that is pretending to be an IPv6 router."
- "All the traffic can be diverted to the rogue router, which can do sniffing of traffic or modify traffic or drop traffic,"

4. Type 0 routing header: DoS

This well-known IPv6 vulnerability creates the opportunity for denial-of-service attacks because it gives a hacker the ability to manipulate how traffic flows over the Internet. This feature of IPv6 allows you to specify in the header what route is used to forward traffic. A hacker could use this feature to saturate a particular part of the network,

- "We haven't seen this yet, this would be a targeted attack."

5. Built-in ICMP and multicast

Unlike IPv4, IPv6 features built-in Internet Control Message Protocol (ICMP) and Multicast. These two types of network traffic are integral to how IPv6 works. With IPv4, network managers can block ICMP and multicast traffic to prevent attacks coming over these channels. But for IPv6, network managers will need to fine-tune the filters on their firewalls or routers to allow some ICMP and multicast traffic through.

- "You have to explicitly configure ICMP6 and multicast with IPv6,"

3.2 Security Techniques

Just as the threats outlined above can be traced back to a few archetypal forms of attack, basic security properties can also be classified into a few fundamental building blocks. These properties can be combined to satisfy more complex security requirements:

- **Data Confidentiality**: Stored or transmitted information cannot be read or altered by an unauthorized party.
- **Data Integrity**: Any alteration of transmitted or stored information can be detected.
- **Authenticity**: The identity of the provider of information (in some cases, the identity of the intended receiver as well) can be proven.
- **Non-Repudiation:** ensure that a party to a contract or a communication cannot deny the authenticity of their signature

- **Access Control:** login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.

For performing of the security services, different security mechanisms have been recommended. Those are:

- **Encipherment mechanisms (encryption mechanisms) :** two secrete keys are used for encryption and decryption process.
- **Digital signature mechanism:** authentication mechanism to know authenticate sender for non-repudiation
- **Access control mechanism:** detecting and preventing unauthorized access and by permitting authorized access
- **Data integrity mechanism:** any alteration should be detected, preventing by using hashing, or message digesting
- **Authentication exchange mechanism:** Key exchange is done **either in-band** or **out-of-band**. In in-band key exchange, keys are exchanged through the same communication channel that will be encrypted. In out-of-band key, keys are exchanged through a channel other than the one that will be encrypted.
- **Routing control mechanism:** techniques to manage and flow control the traffic, routing.
- **Notarization mechanism:** Verified or approved or secure channel for communication

3.3 IPSEC Framework

IPSec, is a framework of open standards (from IETF) that define policies for secure communication in a network. In addition, these standards also describe how to enforce these policies.

Using IPSec, participating peers (computers or machines) can achieve data confidentiality, data integrity, and data authentication at the network layer (i.e. Layer 3 of the Open Systems Interconnection 7-layer networking model). **RFC 2401** specifies the base architecture for IPsec compliant systems. IPv6

This RFC says that "the goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments."

The main purpose of IPSec is to provide interoperable, high quality, cryptographically-based security for IPv4 and IPv6. It offers various security services at the IP layer and therefore, offers protection at this (i.e. IP) and higher layers. These **security services** are, for example, access control, connectionless integrity, data origin authentication, protection against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality.

Goals of IPSec

- ✓ Verify source of IP packets – provide Authentication that is taking in IPv4
- ✓ Protect integrity and/ or confidentiality of packets
- ✓ Prevent replaying of old packets
- ✓ Provide security automatically for upper layer protocols and applications

Technical Details:

IPSec has two different modes: Transport mode (host-to-host) and Tunnel Mode (Gateway-to-Gateway or Gateway-to-host). In transport mode, the payload is encapsulated (header is left intact) and the end-host (to which, the IP packet is addressed) decapsulates the packet. In the tunnel mode, the IP packet is entirely encapsulated (with a new header). The host (or gateway), specified in the new IP header, decapsulates the packet. Note that, in tunnel mode, there is no need for client software to run on the gateway and the communication between client systems and gateways are not protected.

IPSec Features:

- **AH** (Authentication Header) that provides authenticity guarantee for transported packets. This is done by check-summing the packages using a cryptographic algorithm.
- **ESP** (Encapsulating Security Payload) that provides encryption of packets.
- **IPcomp** (IP payload compression) that provides compression before a packet is encrypted.
- **IKE** (Internet Key Exchange) provides the (optional) means to negotiate keys in secrecy.

IPv6 IPSec traditionally implements secure remote access connections using virtual private network (VPN) tunneling protocols such as Layer 2 Tunneling Protocol (L2TP). Note that IPSec is not really a VPN mechanism. In fact, the use of IPSec is changing the last few years, since IPSec is moving from the WAN into the LAN to secure internal network traffic against eavesdropping and modification.

When two computers (peers) want to communicate using IPSec, they mutually authenticate with each other first and then negotiate how to encrypt and digitally sign traffic they exchange. These IPSec communication sessions are called security associations (SAs).

IPSec in IPv6 and why it's important

IPsec is a mandatory component for IPv6, and therefore, the IPsec security model is required to be supported for all IPv6 implementations in near future. In IPv6, IPsec is implemented using the AH authentication header and the ESP extension header. Since at the present moment, IPv4 IPsec is available in nearly all client and server OS platforms, the IPSec IPv6 advanced security can be deployed by IT administrators immediately, without changing applications or networks. The importance of IPsec in IPv6 has grown in recent years as U.S.

Department of Defense and federal government have mandates to buy IPv6-capable systems and to transition to IPv6-capable networks within a few years,

IP Security Overview

- IPSec is not a single protocol.
- Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms to provide security appropriate for the communication.
- Applications of IPSec
  - Secure branch office connectivity over the Internet
  - Secure remote access over the Internet
  - Establisihing extranet and intranet connectivity with partners
  - Enhancing electronic commerce security
- Two protocols are used to provide security:
  - **Authentication Header Protocol (AH):** A protocol that is utilized when data confidentiality is not a concern. It does not perform any form of encryption for the data itself, but rather performs an integrity checksum to ensure that the payload was not modified during transit. AH is a Layer 4 (Transport layer) protocol that can be identified by the IP header's protocol field value of 51.
  - **Encapsulation Security Payload (ESP):** This protocol can actually ensure data confidentiality with encryption, as well as data integrity and authentication. ESP protects the IP data payload by encrypting it and adding (encapsulating) an additional header and trailer. ESP can be used in conjunction with AH to provide authentication and integrity of the data, or ESP can provide this functionality within itself. When ESP authentication is enabled, the data contained between the ESP header and trailer is authenticated. ESP is also a Layer 4 (Transport layer) protocol that can be identified by the IP header's protocol field value of 50.
- IPSec Services: Services provided are:
  - Access control: integrity
  - Data origin authentication
  - Rejection of replayed packets: a form of partial sequence integrity
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality

Benefits of IPSec

- In a firewall/router, provides strong security to all traffic crossing the perimeter
- Is resistant to bypass
- Is below transport layer, hence transparent to applications
- Can be transparent to end users
- Can provide security for individual users if desired
- Additionally, in routing applications:
  - assure that router advertisements come from authorized routers
  - neighbor advertisements come from authorized Neighbors
  - insure redirect messages come from the router to which initial packet was sent
  - insure no forgoing of router update

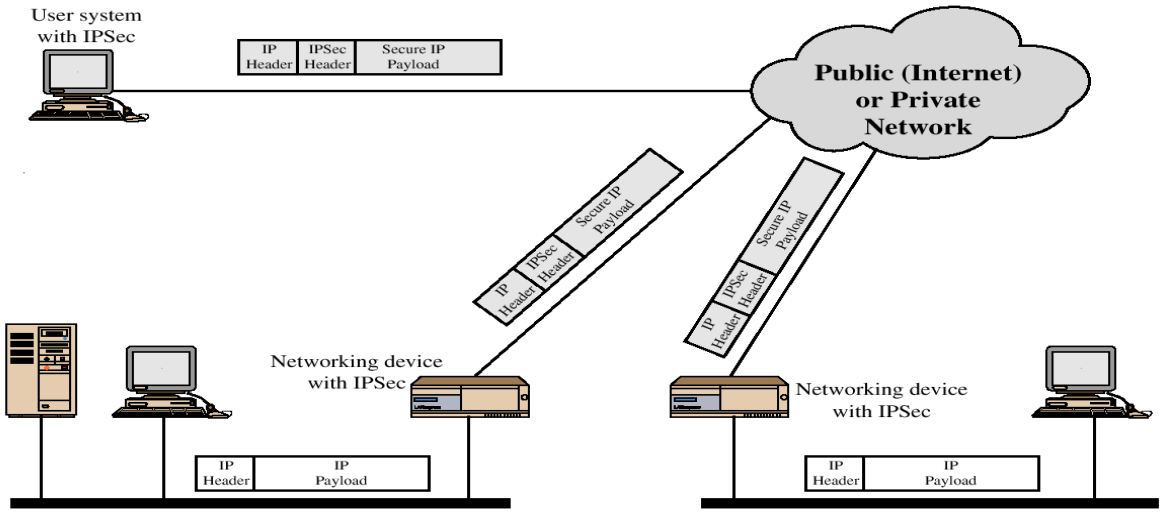


Fig. IP Security Scenario

- general IP Security mechanisms provides
  - authentication
  - Confidentiality
  - Integrity
  - Obligation
  - key management
- applicable to use over LANs, across public & private WANs, & for the Internet

IPSec is a framework of protocols that comprises a combination of standards and technologies. The protocol framework itself is open and flexible in that it does not mandate a specific key length or algorithm. IPSec contains two basic security protocols as part of the IPSec protocol standard:

- **Authentication Header (AH):** A protocol that is utilized when data confidentiality is not a concern. It does not perform any form of encryption for the data itself, but rather performs an integrity checksum to ensure that the payload was not modified during transit.
- **Encapsulating Security Payload (ESP):** This protocol can actually ensure data confidentiality with encryption, as well as data integrity and authentication. ESP protects the IP data payload by encrypting it and adding (encapsulating) an additional header and trailer. ESP can be used in combination with AH to provide authentication and integrity of the data, or ESP can provide this functionality within itself. When ESP authentication is enabled, the data contained between the ESP header and trailer is authenticated.
  - Encryption is applied to packet payload
  - Authentication is applied to data in the IPSec header as well as the payload, after encryption is applied.

Mode / Protocol	Transport	Tunnel
AH	IP AH Data	IP AH IP Data
ESP	IP ESP Data ESP-T	IP ESP IP Data ESP-T

IPSec Modes of Operations : *Transport Mode and Tunnel Mode*

IPsec can be implemented in a host-to-host transport mode, as well as in a network tunneling mode

ESP and AH can operate in either transport mode or tunnel mode. The key difference between the two modes is what portion of the IP datagram is being authenticated and encrypted.

- ***Transport Mode –*** *security protection provided from one end* ***Host to*** *another* ***Host*** i.e. end to end protection, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact, since the IP header is neither modified nor encrypted; however, when the authentication header is used, the IP addresses cannot be modified by network address translation, as this always invalidates the hash value. The transport and application layers are always secured by a hash, so they cannot be modified in any way, for example by translating the port numbers.

A means to encapsulate IPsec messages for NAT traversal has been defined by RFC documents describing the NAT-T mechanism.

- ***Tunnel Mode*** – security protection is provided to traffic from ***Gateway of*** *one network* ***to Gateway*** *of another network e.g. VPN.* In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access) and host-to-host communications (e.g. private chat).

Tunnel mode supports NAT traversal.

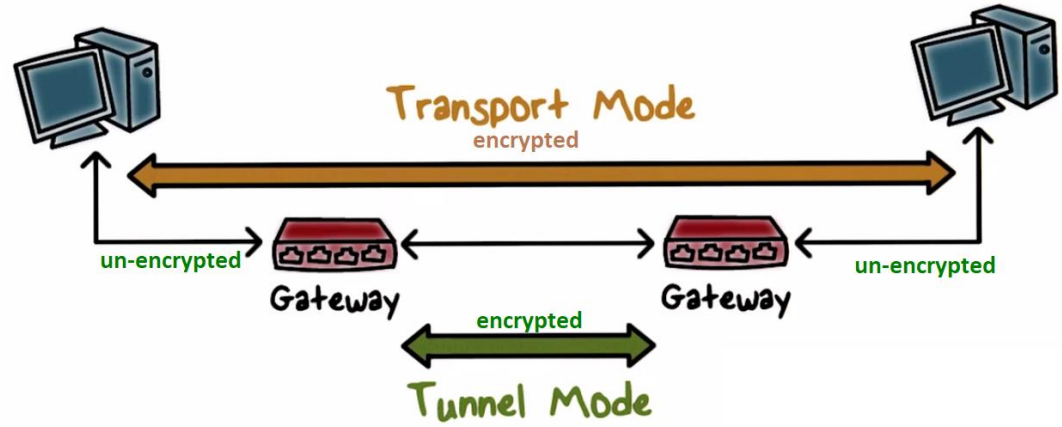


Figure 2.4. ESP in transport and tunnel mode.

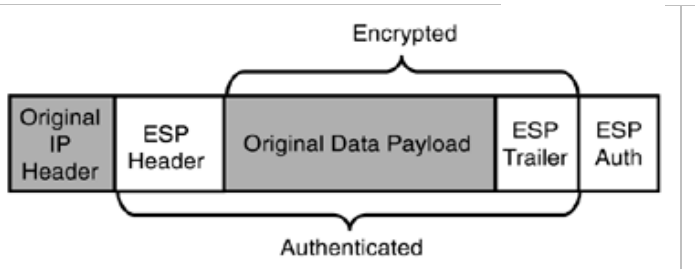


Fig. Transfer Mode

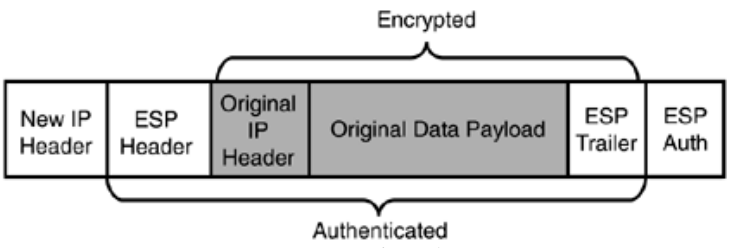
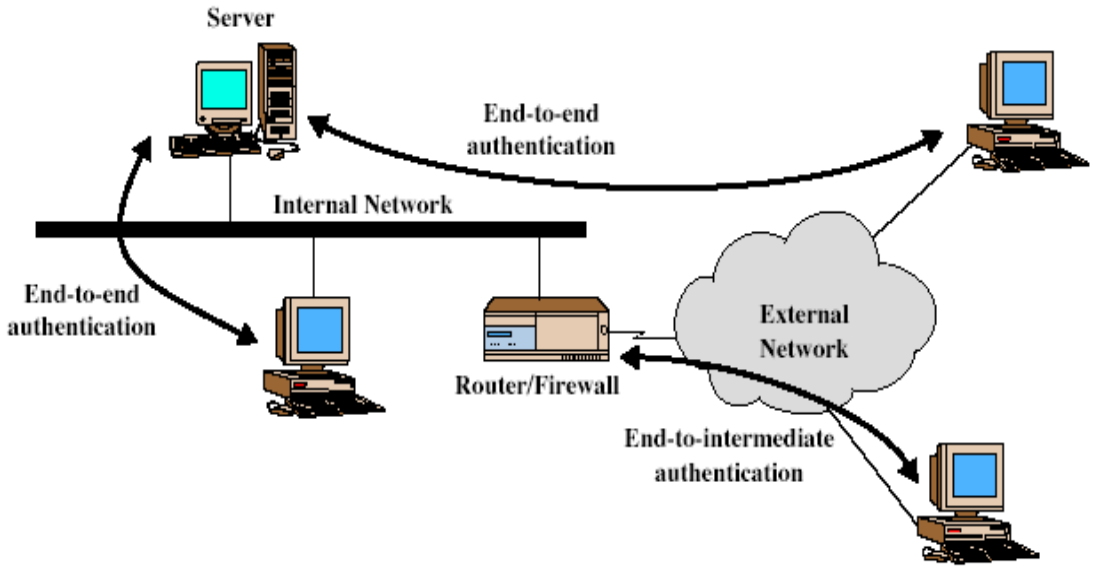
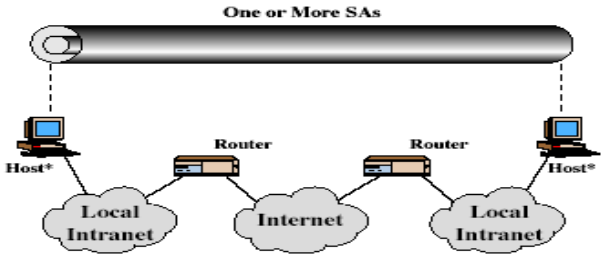


Fig. Tunnel Mode

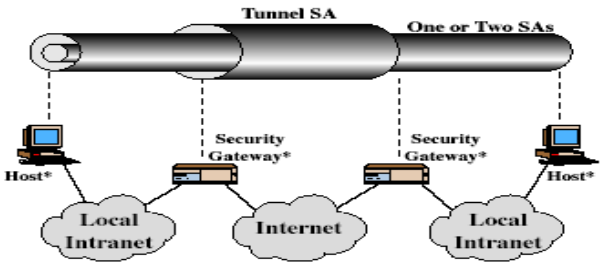


Combining Security Associations (SA)

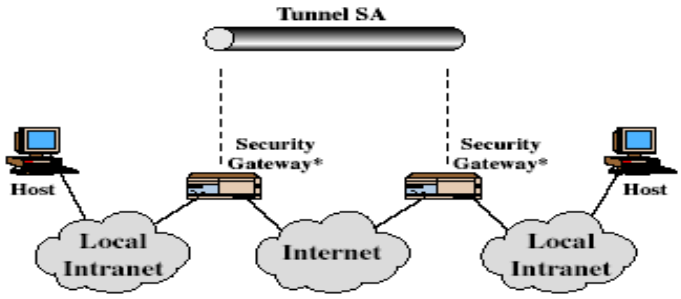
- SA is the establishment of shared security attributes i.e. cryptographic algorithms and mode, encryption key etc. between two network entities to support secure communication.
- A SA is a logical connection involving two devices that transfer data.
- SA's can implement either AH or ESP
- to implement both, need to combine SA's
  - form a security bundle
- have 4 cases
  a) AH in transport mode
  b) ESP in transport mode
  c) AH followed by ESP in transport mode (ESP SA inside an AH SA)
  d) any one a, b, c inside an AH or ESP in tunnel mode



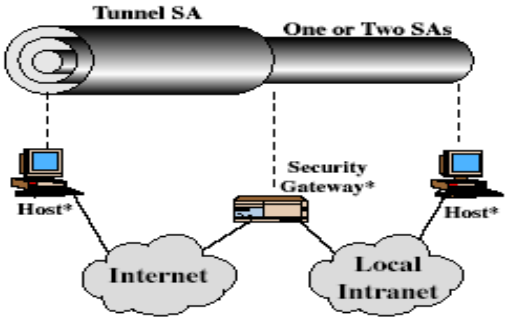
Case (a) AH in transport mode Case



(c) AH followed by ESP in transport mode



Case (b) ESP in transport mode



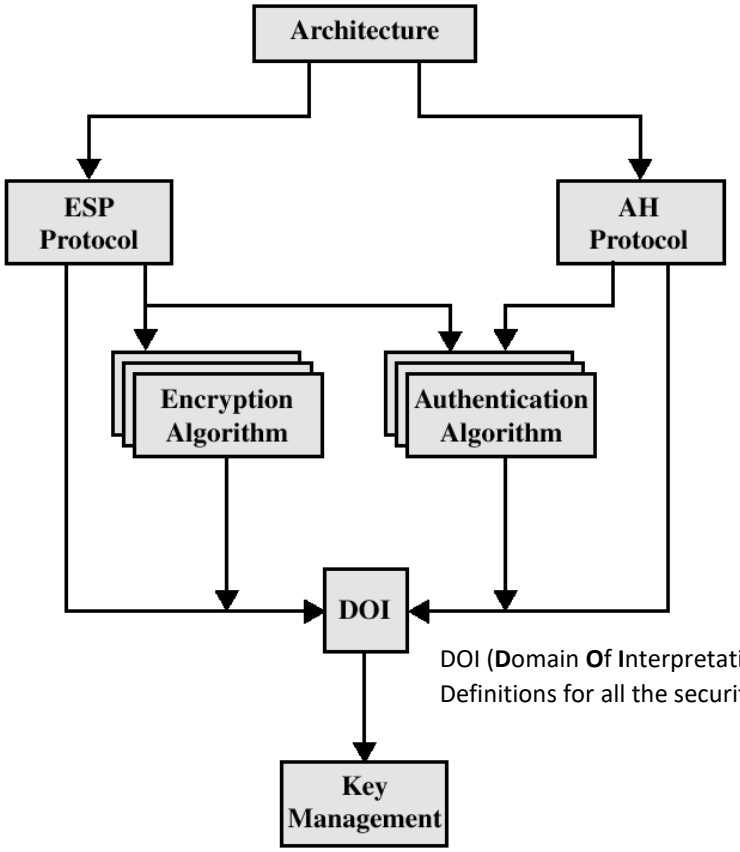
Case (d) any one a, b, c inside an AH or ESP in tunnel mode

	Transport Mode SA	Tunnel Mode SA
AH	**Authenticates** IP payload and selected portions of IP header and IPv6 extension headers	**Authenticates** entire inner IP packet plus selected portions of outer IP header
ESP	**Encrypts** IP payload and any IPv6 extesion header	**Encrypts** inner IP packet
ESP with authentication	**Encrypts** IP payload and any IPv6 extesion header. **Authenticates** IP payload but no IP header	**Encrypts** inner IP packet. **Authenticates** inner IP packet.

IP Security Architecture

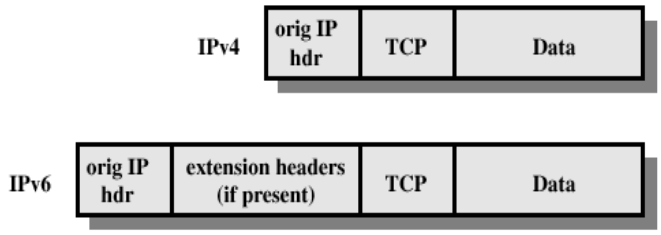
Internet Key Exchange (IKE)

IKE is a hybrid protocol derived from the Internet Security Association and Key Management Protocol (ISAKMP), the Secure Key Exchange Mechanism (SKEME) protocol, and the Oakley protocol. IKE automatically handles the preliminary negotiation and authentication between IPSec peers. This negotiation aspect of IKE entails an agreement between both IPSec peers, in which matching encryption and hash algorithms, as well as peer authentication methods, tunnel modes, and IPSec policy lifetimes, are also determined. As you can discern from the acronym, IKE also negotiates and implements the Diffie-Hellman groups for key exchanges.

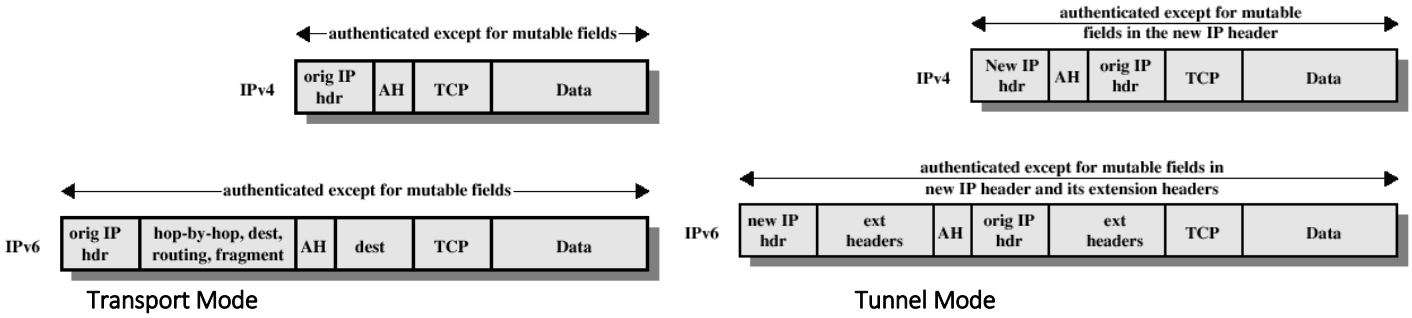


DOI (**D**omain **O**f **I**nterpretation) is a document containing Definitions for all the security parameters required

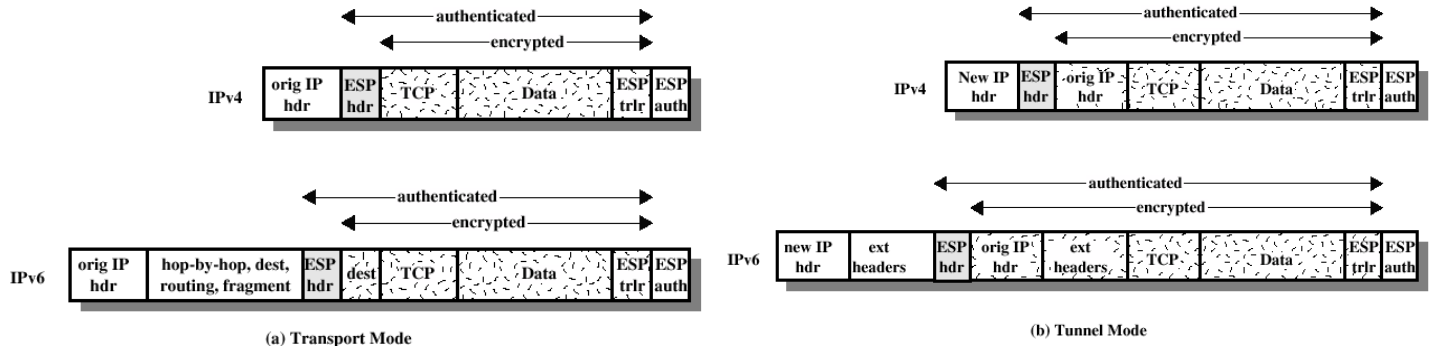
Before applying AH



AH Authentication



ESP Encryption and Authentication



3.4 QoS in IPv6 Protocols

The default IP model treats all packets alike. They are all forwarded with best-effort treatment according to the first-come, first-served principle. Which path a packet takes through the network depends on the available routers, routing tables, and general network load.

• QoS protocols have the task of providing different data streams with priorities and guaranteeing qualities such as bandwidth and delay times.

• Quality of Service (QoS) is a set of technologies for managing network traffic in a cost-effective manner to enhance user experiences for home and enterprise environments. QoS technologies allow you to measure bandwidth, detect changing network conditions (such as congestion or availability of bandwidth), and prioritize or throttle traffic. For example, QoS technologies can be applied to prioritize traffic for latency-sensitive applications (such as voice or video) and to control the impact of latency-insensitive traffic (such as bulk data transfers).

• Integrated Service and Differentiated Service are two architectures of QoS.

QoS Requiremt Elements

• Network quality of service is evaluated by measuring four key parameters: 1. Bandwidth 2. End-to-End delay, 3. Jitter 4. Packet loss.

• **Bandwidth**, typically specified in kilo or mega bits per second (kbps or Mbps), is measured as the average number of bits per second that can travel successfully through the network.

• **End-to-end delay** is the average time it takes for a network packet to traverse the network from one endpoint to the other.

• **Jitter** is the variation in the end-to-end delay of sequential packets.

• **Packet loss** is measured as the percent of transmitted packets that never reach the intended destination.

Models for providing QoS services or Traffic management frameworks in a network:

1) **Integrated Services (*IntServ)***
   - **Hard QoS model**, based on flows, i.e., source and destination IP addresses and ports.
   - Based on reserving resources pers session and limit total demand to the capacity that can be handled by network.
   - The Integrated Services architecture (IntServ) is based on the fact that bandwidth and all related resources per flow are reserved on an end-to-end basis.
   - This presupposes that routers store information about flows and analyze each packet to determine whether it belongs to a specific flow in order to forward the packet according to the criteria for that specific flow.
2) **Differentiated Service (*DiffServ)***
   - **Soft QoS model**, based in service classes and per hop behaviours associated to each class.
   - Helps to classify the traffic into a number or traffic groups and handled based on the traffic group.
   - This approach is not an end-to-end service and is based on the determination of PHB (per hop basis) in each router
   - DS field in IPv4 and IPv6 specifies differentiated service.
   - This is implemented in the ToS field in the IPv4 header and the Traffic Class field in the IPv6 header.
   - The DS field is used by DiffServ routers to determine the QoS forwarding requirements of packets. Communicating nodes can categorize their communication through a so-called Per-Hop Behavior (PHB). Based on the PHB, packets receive specific treatment on DiffServ routers.
   - A DiffServ (DS) domain is a contiguous group of DS routers that work with a common service policy implemented on all routers. A DS domain is defined by DS boundary routers. The boundary routers classify incoming data streams and ensure that all packets traversing the domain are labeled appropriately and use a Per-Hop Behavior from the set available for the domain. Routers within the domain choose the forwarding rules based on the DiffServ values in packets, which they map to the corresponding PHBs.

Fig. the main components of DeffServ network

QoS Service	IntServ	DiffServ
Isolation	Per flow isolation	Per aggregation isolation
Guarantee	Per flow	Per aggregation (Traffic Class)
Service Scope	End-to-end	Per domain
Complexity	Per flow setup	Long term setup
Scalability	Not scalable (each router maintains per flow state)	Scalable (edge routers maintain per aggregate state; core routers per class state)

Suitable for Real Time traffic	Yes, resource reservation.	Yes, LLQ- Low-latency queuing is a feature developed by Cisco to bring strict priority queuing (PQ).
Admission Control	Deterministic based on flows.	Statistic based on Traffic Classes.
Applicability	Small networks and flow aggregation scenarios.	Networks of any size.
Resource Reservation	Per flow on each node in the source-destination path.	Per Traffic Class on every node in the domain.
Complexity	High	Medium

Two fields i.e Traffic Class , Flow label, Hop-Limit field are used to define QoS in IPv6.

1. Traffic Class.

- These 8 bits are divided into two parts.
- The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet i.e. DiffServ. The least significant 2 bits are used for Explicit Congestion Notification (ECN).

2. Flow label

- Flow can be explained as a stream of traffic that is coming from one source and destined for one or more destinations; a flow will contain multiple packets which can each be treated exactly the same way by intermediate routing devices. The Flow Label is used to identify these flows and enables these intermediate routing devices to treat all of the packets within the flow the same, this reduces processing time and delay.
- This field distinguishes packets that require the same treatment in order to facilitate the handling of real-time traffic.
- A sending host can label sequences of packets with a set of options. Routers keep track of flows and can process packets belonging to the same flow more efficiently because they do not have to reprocess each packet's header.
- The flow label and address of the source node uniquely identify the flow. Nodes that do not support the functions of the Flow Label field are required to pass the field unchanged when forwarding a packet and to ignore the field when receiving a packet.
- All packets belonging to the same flow must be sent with the same IP Source address, IP Destination address, identical source and destination ports, and a nonzero flow label.
- The handling of the flow label on routers is efficient, and when IPsec is used, it is always available because the IPv6 header is not encrypted by ESP or authenticated by AH (in transport mode). This implies that the integrity of the information in the DS field cannot be guaranteed by IPsec.
- Routers are free to set up the flow-handling state for any flow. Routers do not need explicit flow establishment information from a control protocol, a hop-by-hop option, or other means
- The violation is reported by a problem message for an ICMP parameter, Code 0.
- Nodes keeping dynamic flow state must not assume packets arriving 120 seconds or more after the previous packet of a flow still belong to the same flow, unless a flow state establishment method in use defines a longer flow state lifetime or the flow state has been explicitly refreshed within the lifetime duration.

3. Hop Limit (8-bits):

This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.

QoS is a feature needed to ensure that high priority is given to certain packets that need to arrive at their destination in a timely manner. *For example, in streaming video or Voice over IP, these packets need to arrive close together since a small delay can make the video or voice choppy. If there is just text being transmitted, a small delay between the packets is really of no consequence.*

QoS in IPv6 Protocols

IPv6 protocols carry a small number of QoS-Specific service elements in the IP based & Extension Header

Flows

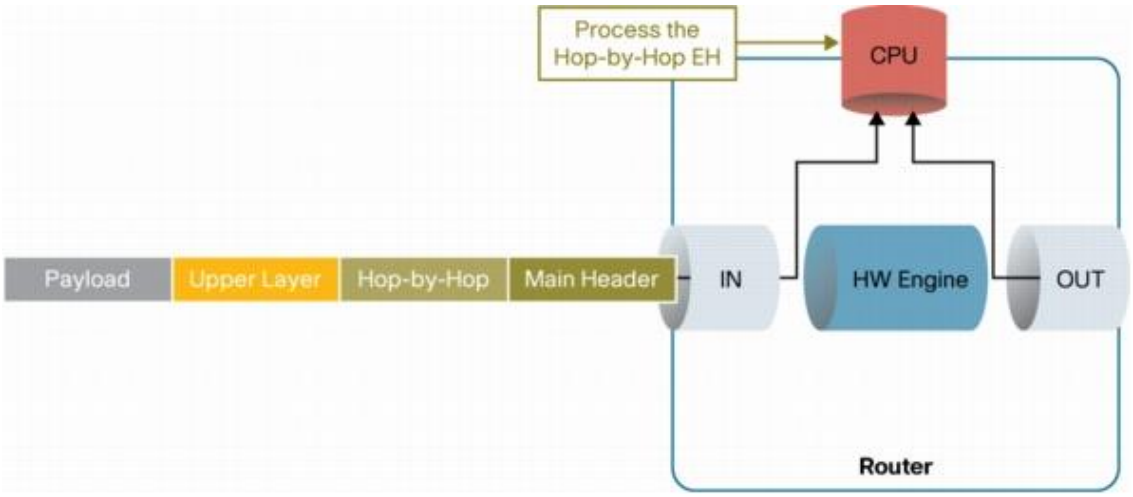
- Sequence of packets sent from a particular source to a particular destination(s) for which the source requires special handling in intermediate routers by control protocols like RSVP (RSVP *(Resource Reservation* Protocol*) is a set of communication rules that allows channels or paths on the Internet to be reserved for the multicast (one source to many receivers) transmission of video and other high-bandwidth messages.)*
- Packets that do not belongs to a flow carry a flow level of all zeros.

- All packets belonging to the same flow must be sent with same IP source address and destination address with non-zero flow label.
- The Flow label field in IPv6 may be used by source to label packets for which it request special handling by the IPv6 routers like real time service.

IPv6 extension Headers

- Two external headers to signal QoS requirements
  - The **Routing extension header** can be used to request a specific route by indicating a sequence of IP address. Defines strict source routing and loose source routing for the packet. (With strict source routing, each intermediate destination device must be a single hop away. With loose source routing, intermediate destination devices can be one or more hops away.)
  - **HOP-by-HOP extension headers** can be used to transport a maximum of one router alert signaling message per IP packet to every router on the path of QoS-sensitive traffic, indicating that each router should specifically process the packets
- The Hop-by-Hop Extension Header is the ONLY EH that MUST be fully processed by all network devices as shown in Figure 5. From this perspective, the Hop-by-Hop EH is similar to the IPv4 options. This explains the reason why this EH MUST be the first in a chain of extension headers.

Figure 5. *Forwarding IPv6 Packets with the Hop-by-Hop Extension Header*



- Because the Hop-by-Hop EH must be fully processed, it is handled by the CPU1 and the IPv6 traffic that contains a Hop-by-Hop EH will go through the slow forwarding path. This rule applies to all vendors. Hardware forwarding is not feasible in this case.

If the HBH Options Extension Header is not too long to process, the forwarding plane hardware scans the header, assigning it to one of the following classes:

00	Skip over this option and continue processing the header.
01	Discard the packet.
10	Discard the packet and send an ICMP parameter problem (type 2 error) to the sender, regardless of whether or not the packet's destination is a multicast address.
11	Discard the packet and send an ICMP parameter problem (type 2 error) to the sender. This error is sent only if the packet's destination is not a multicast address.