Sanjivani Rural Education Society's

Sanjivani College of Engineering, Kopargaon-423603

(An Autonomous Institute Affiliated to Savitribai Phule Pune University, Pune)

NAAC 'A' Grade Accredited, ISO 9001:2015 Certified

Department of Information Technology

(NBA Accredited)

Cryptography and Cyber Security [IT311]

Mrs. Kanchan D. Patil

Assistant Professor

Unit 4: Network Security

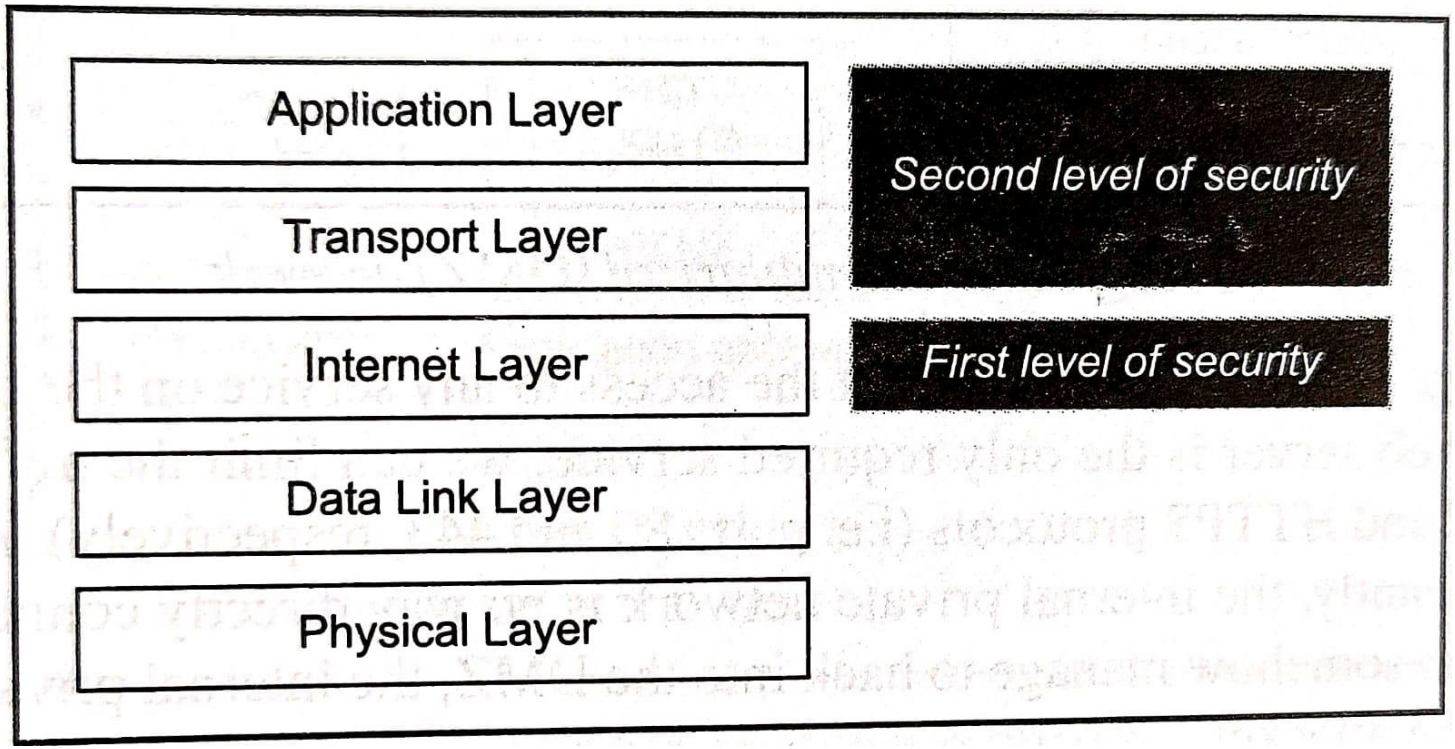
- IPSEC- Introduction, AH and ESP, Tunnel Mode, Transport Mode, Security Associations
- IKE- Internet Key Exchange Protocol
- SSL- Introduction, Handshake Protocol, Record Layer Protocol

IPSec Introduction

- The IP packets contain data in plain text form.
- That is, anyone watching the IP packets pass by a actually access them, read their contents and even change them.
- The higher-level security mechanisms such as SSL, SHTTP, PGP, PEM, S/MIME and SET can be useful to prevent such kinds of attacks
- Although these higher-level protocols enhance the protection mechanisms, there was a general feeling for a long time that why not secure IP packets themselves?
- If we can achieve this, The higher-level security mechanisms can then serve a additional security measures.

IPSec Introduction

- Thus, we will have two levels of security in this scheme:
  - First offer security at the **IP packet level itself**
  - Implementing **higher-level security mechanisms**, depending on the **requirements**



IPSec Introduction

- In 1994, the **Internet Architecture Board** (IAB) prepared a report, called as **Security in the Internet Architecture (RFC 1636)**
- This report stated that the Internet was a very open network, which was unprotected from hostile attacks.
- Therefore, the Internet needs better security measures, in terms of **authentication, integrity and confidentiality.**
- Just in 1997, about 150,000 Web sites were attacked in various ways, proving that the Internet was quite an unsafe place at times.
- Consequently, the IAB decided that authentication, integrity and encryption must be a part of the **next version of the IP protocol, called as IP version 6 (IPv6) or IP new generation (IPng).**
- However, since the new version of IP was to take some years to be released and implemented, the **designers devised ways to incorporate these security measures in the current version of IP, called as IP version 4 (IPv4)** as well.

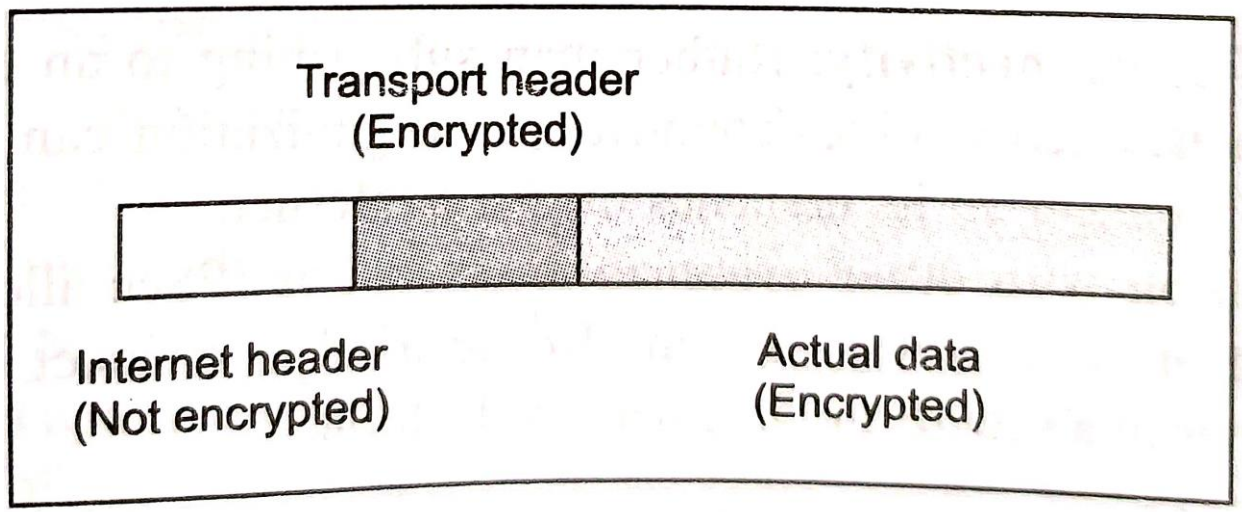
IPSec Introduction

- The outcome of the study and IAB's report is the protocol for providing security at the IP level, called as **IP Security** (IPSec).
- In 1995, the **Internet Engineering Task Force (IETF)** published **five** security-based standards related to IPSec.

RFC Number	Description
1825	An overview of security architecture
1826	Description of a packet authentication extension to IP
1827	Description of a packet encryption extension to IP
1828	A specific authentication mechanism
1829	A specific encryption mechanism

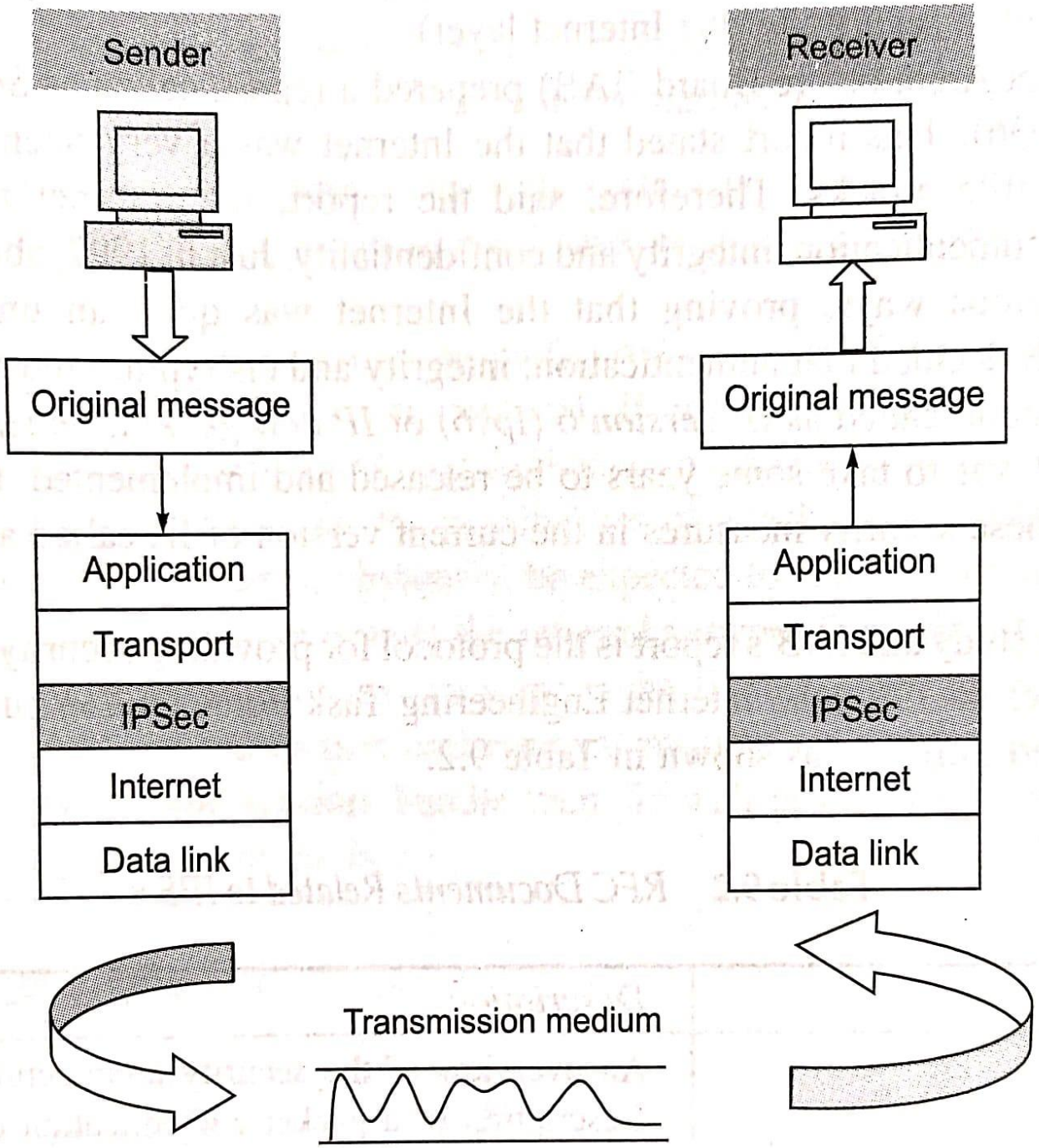
IPSec Introduction

- IPv4 may support these features, but IPv6 must support them.
- The overall idea **of IPSec is to encrypt and seal the transport and application layer data during transmission.**
- It also offers **integrity protection for the Internet layer.**
- However, the **Internet header itself is not encrypted**, because of which the **intermediate routers can deliver encrypted IPSec messages to the intended recipient**.
- The logical format of a **message after IPSec** processing is shown below



IPSec Introduction

- Thus, the sender and the receiver look at IPSec as shown in figure as another layer in the TCP/IP protocol stack.
- This layer sits in-between the transport and the Internet layers of the conventional TCP/ IP protocol stack.



IPSec Applications

- **Secure remote Internet access:**
  - Using IPSec, we can make a local call to our Internet Service Provider (ISP) so as to connect to our organization's network in a secure fashion from our home or hotel.
  - From there, we can access the corporate network facilities or access remote desktop/servers.
- **Secure branch office connectivity**:
  - Rather than subscribing to an expensive leased line for connecting its branches across cities/countries, an organization can set up an IPSec-enabled network to securely connect all its branches over the Internet.
- **Set up communication with other organizations:**
  - Just as IPSec allows connectivity between various branches of an organization, it can also be used to connect the networks of different organizations together in a secure and inexpensive fashion.

IPSec Advantages

- IPSec is transparent to the end users. There is **no need for an user training**, key issuance or revocation
- When IPSec is configured to work with a firewall, it becomes the only **entry-exit point** for all traffic, making it extra secure
- IPSec works at the network layer. Hence, **no change**s are needed to the upper layers (**application and transport**).
- When IPSec is implemented in a firewall or a router, all the outgoing and incoming traffic gets protected. However, the internal traffic does not have to use IPSec. Thus, it **does not add any overheads for the internal traffic**.
- IPSec can allow traveling staff to have secure access to the corporate network.
- IPSec allows interconnectivity between branches/offices in a very inexpensive manner.

IPSec Basic Concepts

- We must learn a few terms and concepts in order to understand the IPSec protocol.
- All these concepts are inter-related.
- However, rather than looking at these individual concepts straightaway, we shall start with the big picture.
- We will first take a look at the basic concepts in IPSec and then elaborate each of the concepts.
  - IPSec Protocols
  - Tunnel mode
  - Transport mode
  - The internet key exchange (IKE) protocol
  - Security Association

IPSec Protocols

- **IP packet consists of two portions:**
  - IP header
  - Actual data
- IPSec **features** are implemented in the **form of additional IP headers**, called as **extension headers** to the standard, default IP headers. These extension IP headers follow the standard IP headers.
- **IPSec offers two main services:**
  - Authentication
  - Confidentiality
- Each of these requires its own extension header.
- To support these two main services**, IPSec defines two IP extension headers:**
  - one for authentication
  - another for confidentiality

IPSec Protocols

- **IPSec actually consists of two main protocols:**
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- These two protocols are required for the following purposes.
- **The Authentication Header (AH) protocol**
  - Provides **authentication (verify identity), integrity (complete, trustworthy, not modified/altered)** and an **optional anti-replay** service.
  - The IPSec AH is a header in an IP packet, which contains a **cryptographic checksum** (similar to a message digest or hash) for the contents of the packet.
  - The AH is simply inserted between the **IP header and any subsequent packet contents.**
  - No changes are required to the data contents of the packet. Thus, security resides completely in the contents of the AH

IPSec Protocols

- **The Encapsulating Security Payload (ESP) protocol**
  - Provides data **confidentiality.**
  - The ESP protocol also defines a **new header** to be inserted into the IP packet.
  - ESP processing also includes the **transformation of the protected data into an unreadable, encrypted format.**
  - Under normal circumstances, the ESP will be inside the AH.
  - That is, **encryption happens first and then authentication**.

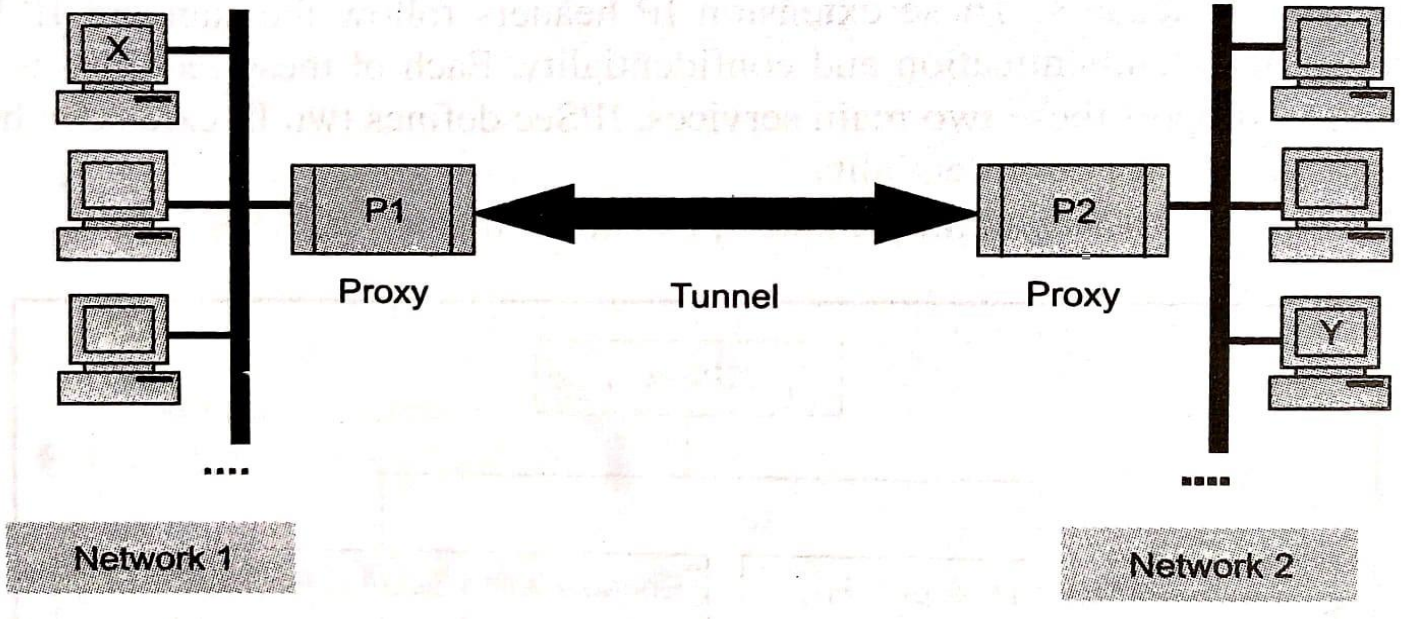
IPSec Protocols

- On receipt of an **IP packet** that was processed by IPSec, the **receiver processes the AH first**, if present.
- The outcome of this tells the receiver if the **contents of the packet are all right or whether they have been tampered with**, while in transit.
- If the receiver finds the **contents acceptable, it extracts the key and algorithms associated with the ESP and decrypt the contents**.

- **Both AH and ESP can be used in one of the two modes:**
  - Tunnel mode
  - Transport mode

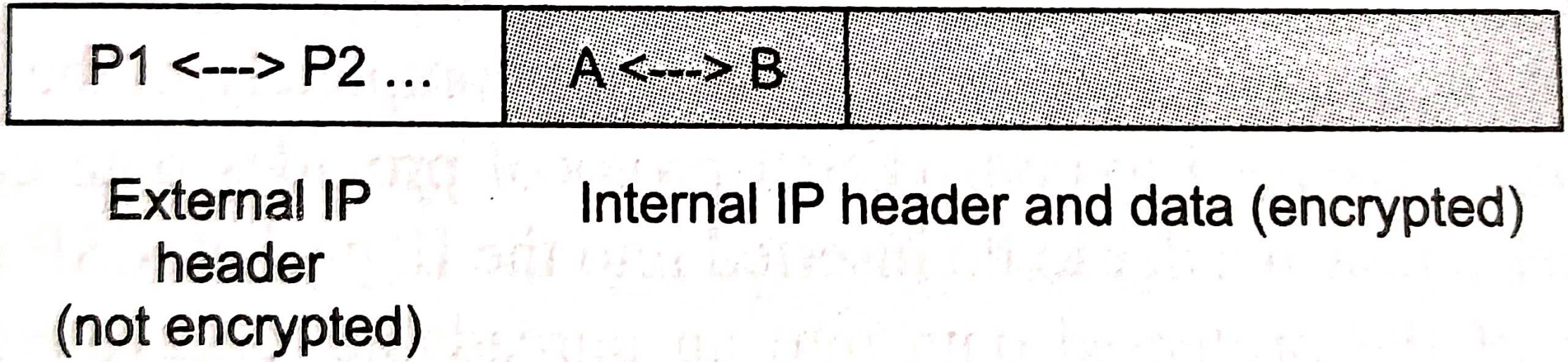
Tunnel Mode

- In the tunnel mode, an encrypted tunnel is established between two hosts.
- Suppose X and Y are two hosts, wanting to communicate with each other using the IPSec tunnel mode.
- What happens here is that they identify their respective proxies, say P1 and P2 and a logical encrypted tunnel is established between P1 and P2.
- X sends its transmission to P1.
- The tunnel carries the transmission to P2. P2 forwards it to Y.



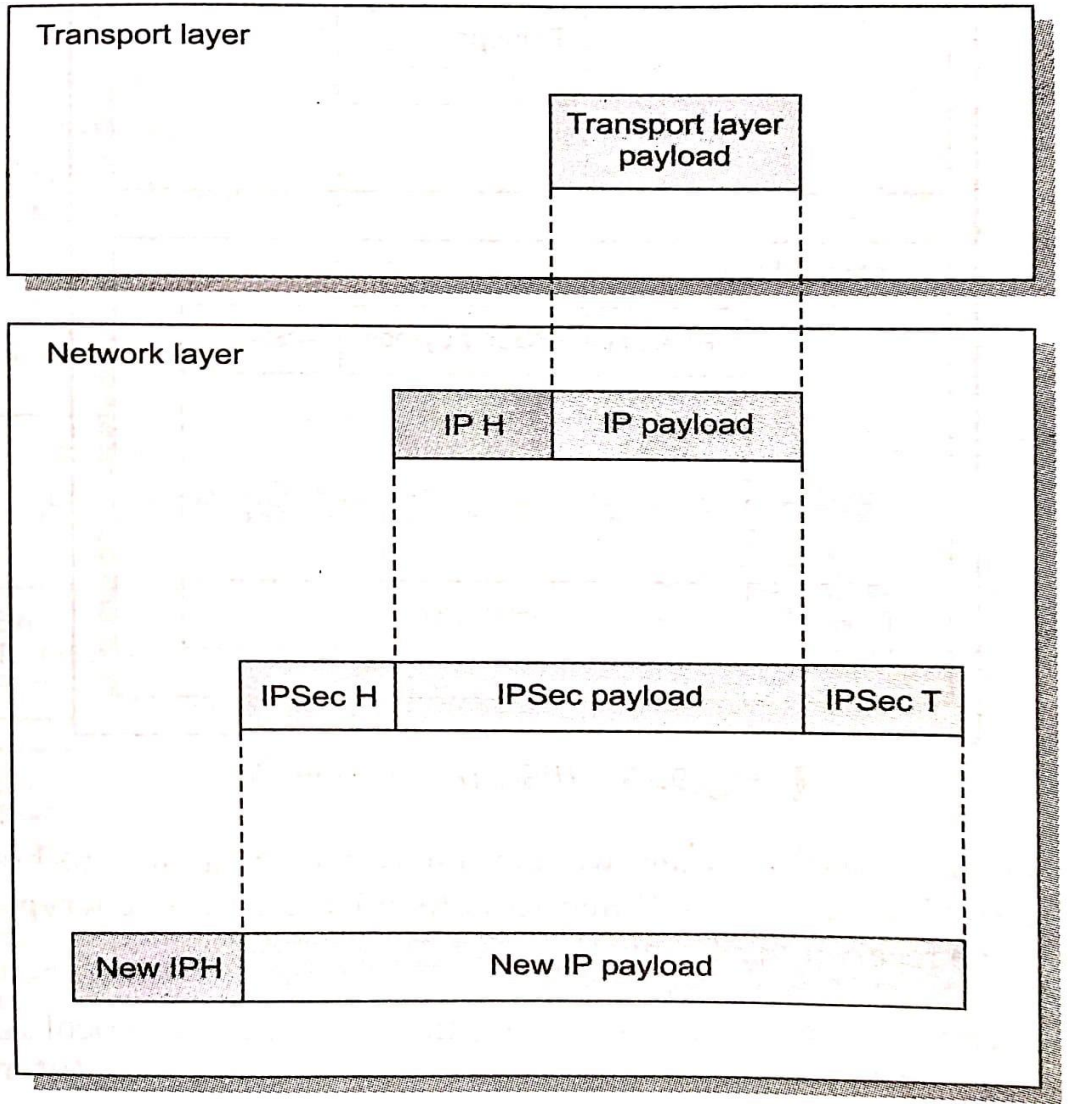
Tunnel Mode Implementation

- We will have **two sets of IP headers: internal and external.**
- The **internal IP header** (which is encrypted) contains the source and destination addresses as X and Y
- The **external IP header** contains the source and destination addresses as P1 and P2.
- That way, X and Y are protected from potential attackers.



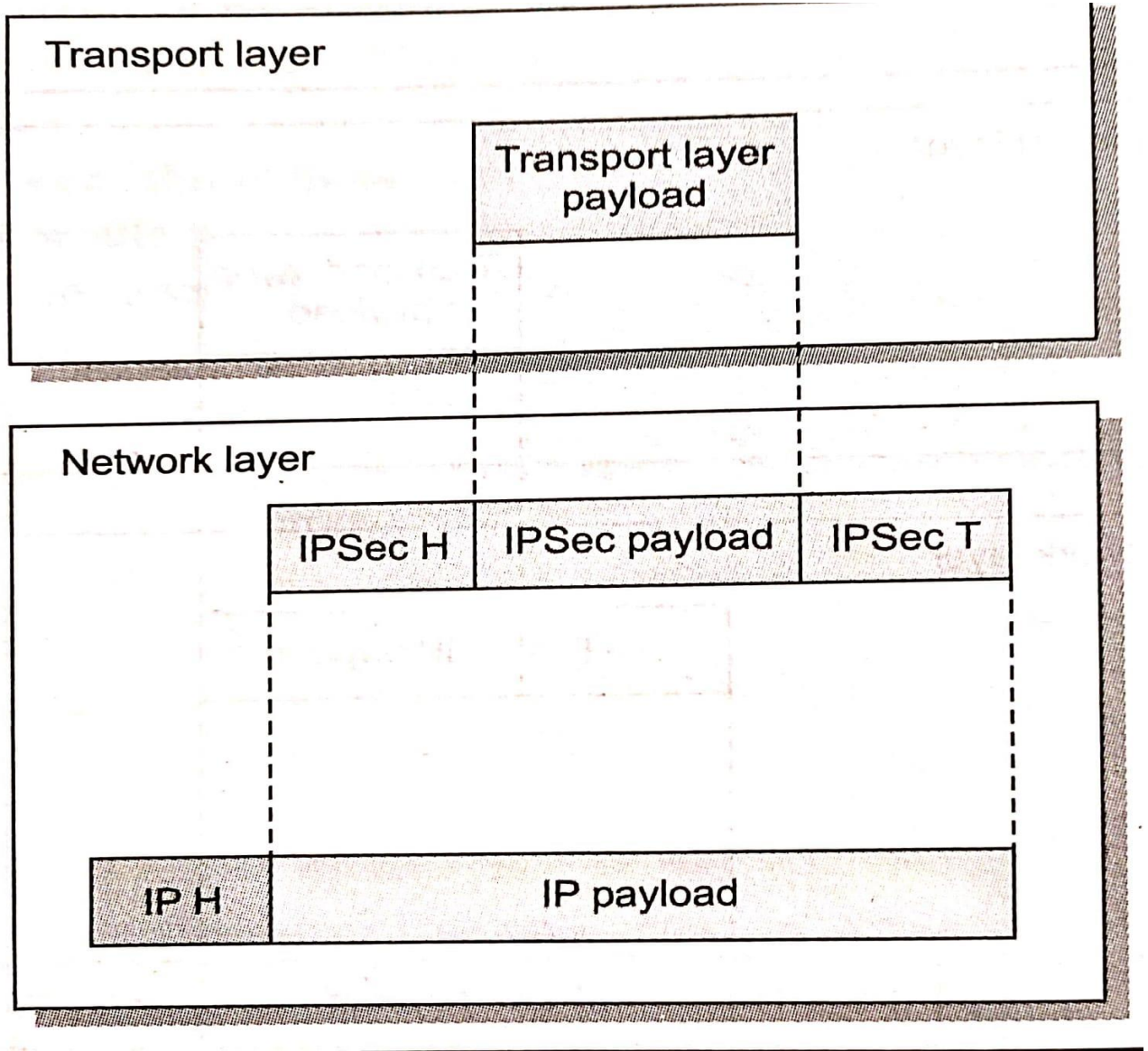
Tunnel Mode Implementation

- In the tunnel mode, IPSec protects the **entire IP datagram (Header and Data)**.
- It takes an IP datagram (including the IP header), adds the IPSec header and trailer and **encrypts the whole thing.**
- It then adds new IP header to this encrypted datagram.



Transport Mode Implementation

- The transport mode **does not hide the actual source and destination addresses.**
- They are visible in plain text, while in transit.
- In the transport mode, IPSec takes the transport layer payload, adds IPSec header and trailer, encrypts the whole thing and then adds the IP header.
- Thus, **the IP header is not encrypted.**

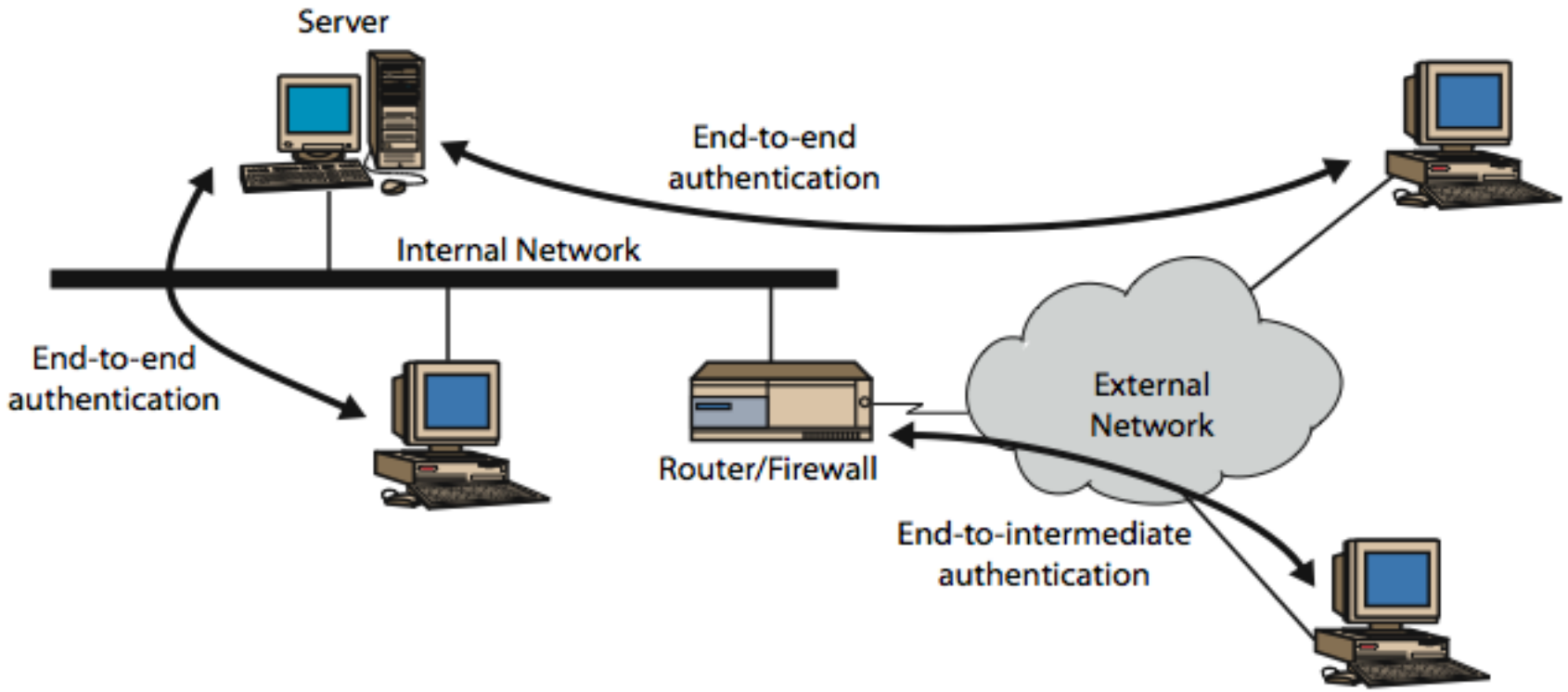


How to decide which mode to use?

- **In the tunnel mode**, the new IP header has information different from that is there in the original IP header.
- The tunnel mode **is normally used between two routers, a host and a router or a router and a host.**
- In other words, it is generally **not used between two hosts**, since the idea is to protect the original packet, including its IP header.
- It is as if the whole packet goes through an imaginary tunnel.
- The **transport mode** is useful when we are interested in a **host-to-host (i.e. end-to-end encryption.**
- The sending host uses IPSec to authenticate and/or encrypt the transport layer payload and only the receiver verifies it.

How to decide which mode to use?

- **In the tunnel mode:** end-to-intermediate authentication
- **In transport mode:** end-to-end authentication



Internet Key Exchange (IKE) Protocol

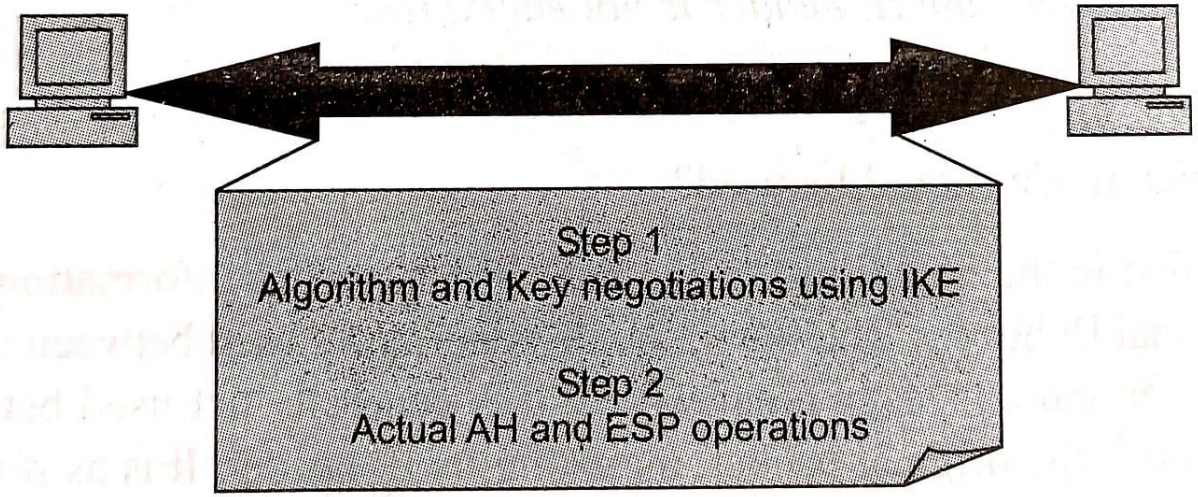
- Another supporting protocol used in IPSec is **Internet Key Exchange (IKE) protocol**
- It is used for the **key management procedures**
- IKE is used to negotiate the cryptographic algorithms to be later used by AH and ESP in the actual cryptographic operations.
- The IPSec protocols are designed to be independent of the actual lower-level cryptographic algorithms.
- Thus, **IKE is the initial phase of IPSec**, where the algorithms and keys are decided.
- After the IKE phase, the AH and ESP protocols take over.

- **Key exchange is done in two ways:**
  - **Manual:** A system administrator manually **configures each system with its own keys** and **with the keys of other communicating systems**. This is practical for small, relatively static environments
  - **Automated:** An automated system **enables the on-demand creation of keys for SAs** and facilitates the use of keys in a large distributed system with an evolving configuration.

Internet Key Exchange (IKE) Protocol

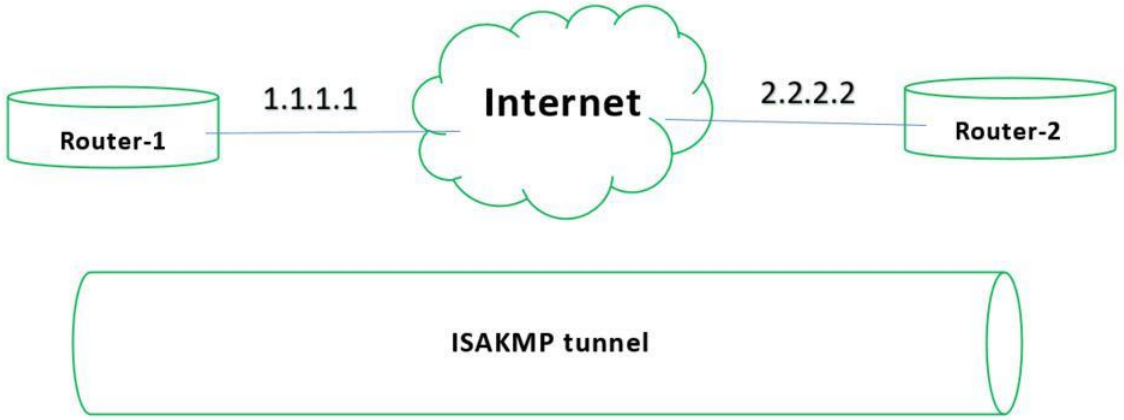
- The default automated key management protocol for IPsec is referred to as ISAKMP/Oakley and consists of the following elements:
  - **Oakley Key Determination Protocol:**
    - Oakley is a key exchange protocol based on the Diffie-Hellman algorithm but providing added security. Oakley is generic in that it does not dictate specific formats.
  - **Internet Security Association and Key Management Protocol (ISAKMP):**
    - ISAKMP provides a **framework for Internet key management** and **provides the specific protocol support, including formats, for negotiation of security attributes**

- **IKE works in two different phases:**
  - Phase 1: Algorithm and key exchange
  - Phase 2: Actual AH and ESP operations



Internet Key Exchange (IKE) Protocol

- **Phase-1:**
- **Step 1 : Negotiation**
- The sender and receiver will **form a security association** which is a collection of parameters that the two devices use.
- Here, the ISAKMP session is established and called the **ISAKMP tunnel or Internet Key Exchange(IKE) Phase-1 tunnel** which is bi-directional.
- When both ends of the tunnel agree to accept a set of security parameters, Phase-1 is done.



Internet Key Exchange (IKE) Protocol

- **Phase-1:**
- **Step 1 : Negotiation**
- Initially, the sender will exchange the **proposals for security services like encryption algorithms. authentication algorithm, hash function, etc.**
- **Hashing:** we use a hashing algorithm to verify the integrity, we use MD5 or SHA for this.
- **Authentication**: each peer has to prove who he is. Two commonly used options are a pre-shared key or digital certificates.
- **DH (Diffie Hellman) group**: the DH group determines the strength of the key that is used in the key exchange process. The higher group numbers are more secure but take longer to compute.
- **Lifetime:** how long does the IKE phase 1 tunnel stand up? the shorter the lifetime, the more secure it is because rebuilding it means we will also use new keying material. Each vendor uses a different lifetime, a common default value is 86400 seconds (1 day).
- **Encryption:** what algorithm do we use for encryption? For example, DES, 3DES or AES.

Internet Key Exchange (IKE) Protocol

- **Phase-1:**
- **Step 2 : Key Exchange**
- Once the negotiation has succeeded, the two peers will know what policy to use. They will now use the DH group that they negotiated to exchange keying material. The end result will be that both peers will have a shared key.

- **Step 3 : Authentication**
- The last step is that the two peers will authenticate each other using the authentication method that they agreed upon on in the negotiation. When the authentication is successful, we have completed IKE phase 1. The end result is a IKE phase 1 tunnel (aka ISAKMP tunnel) which is bidirectional. This means that both peers can send and receive on this tunnel.

Internet Key Exchange (IKE) Protocol

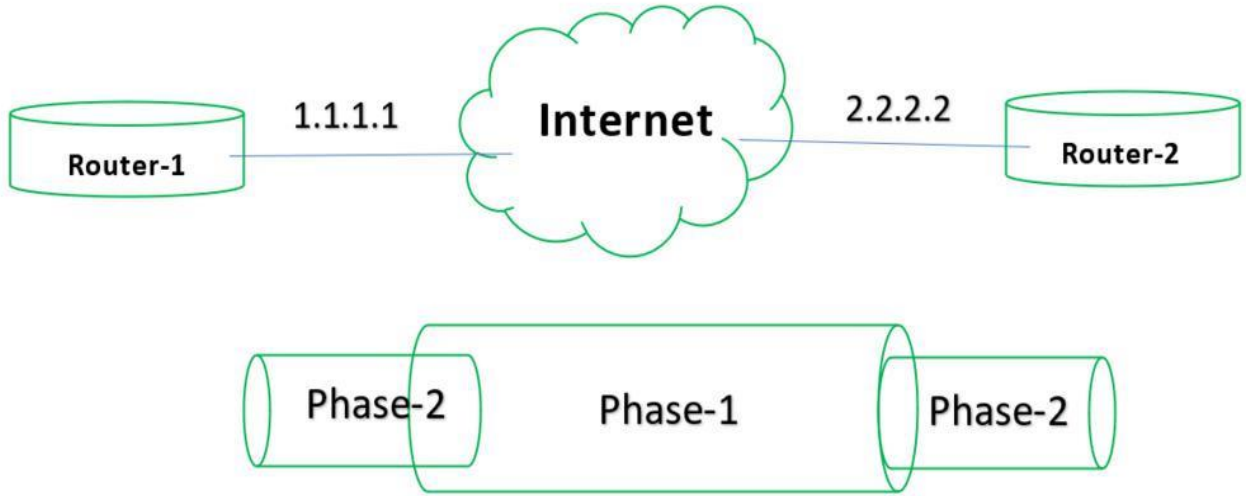
- **Phase-1:** Two modes of Phase-1:
- **Main mode:**
  - The main mode of phase-1 uses **six messages** to secure the key exchange and the Main mode is the more secure.
  - It allows hiding the **end-point identifiers** and the **ability to select the crypto algorithms**.
  - In the six messages:
    - The first two messages **negotiate the policy**
    - The next two messages **depict the Diffie-hellman public values** necessary for key exchange
    - The next two messages are used to **authenticate the Diffie-hellman exchange**.

Internet Key Exchange (IKE) Protocol

- **Phase-1:** Two modes of Phase-1:
- **Aggressive mode:**
  - The Aggressive mode of phase-1 uses three messages and it is less secure than the Main mode. It doesn't allow hiding the endpoints (identity of the parties not hidden)
    - The first message **negotiate the policy**
    - The second message **Key exchange**
    - The third message **authentication**
    - It's quicker than main mode since it adds all the information required for the DH exchange in the first two messages.

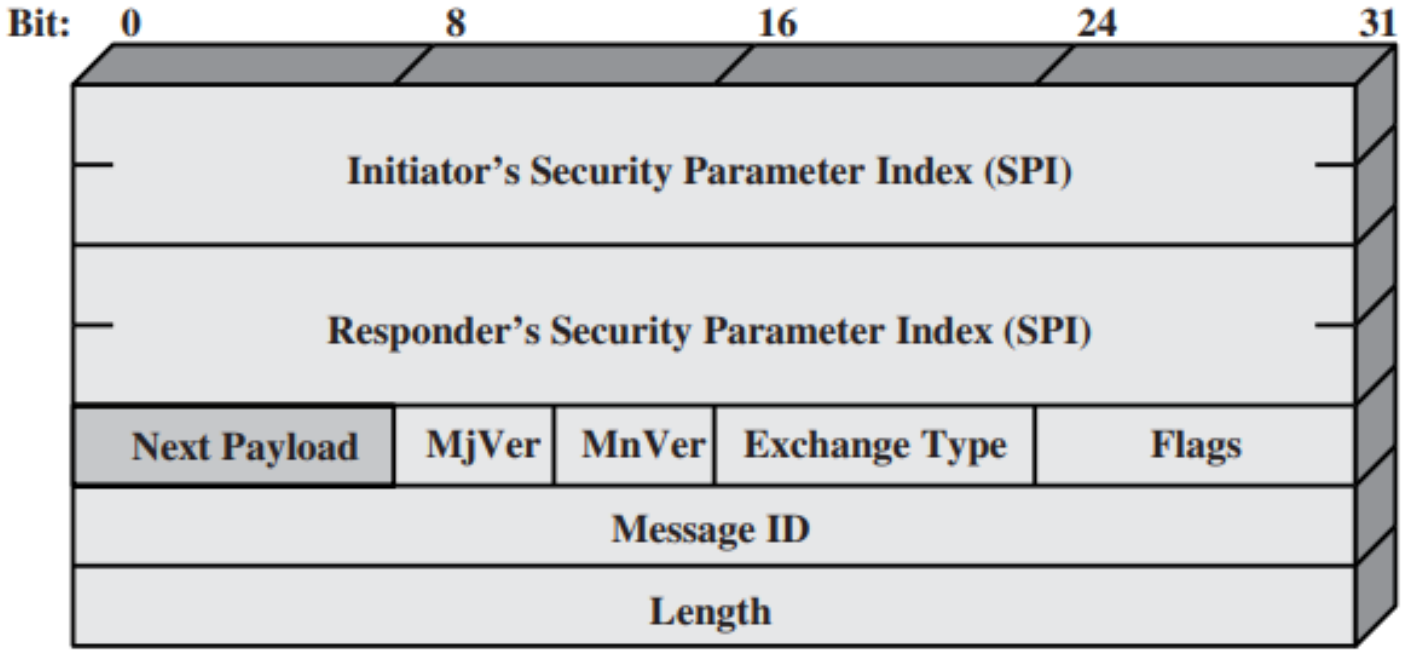
Internet Key Exchange (IKE) Protocol

- **Phase-2:**
  - **Also called as Quick mode**
  - There will be two devices i.e. sender and receiver.
  - Once the sender and receiver established the ISAKMP tunnel in phase-1 they move to phase-2.
  - Here the security associations and services between the two devices are negotiated.
  - The devices will choose **which protocol (Authentication Header or Encapsulation Security Protocol) and which algorithm to use.**

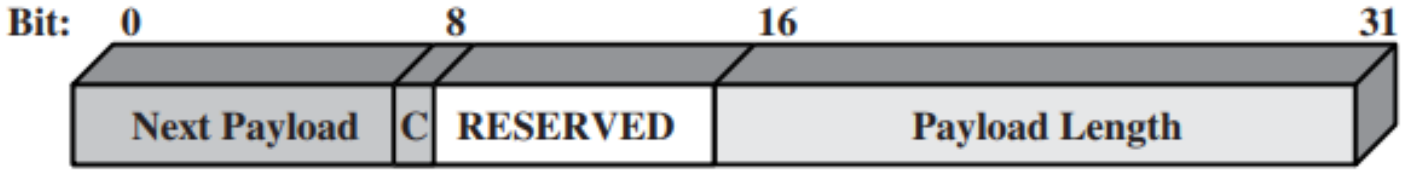


Internet Key Exchange (IKE) Protocol

- **IKE Header Format:**



(a) IKE header



(b) Generic Payload header

Internet Key Exchange (IKE) Protocol

- **IKE Header Format:**

- Initiator SPI (64 bits): A value chosen by the initiator to identify a unique IKE security association (SA).
- Responder SPI (64 bits): A value chosen by the responder to identify a unique IKE SA.
- Next Payload (8 bits): Indicates the type of the first payload in the message.
- Major Version (4 bits): Indicates major version of IKE in use.
- Minor Version (4 bits): Indicates minor version in use.
- Exchange Type (8 bits): Indicates the type of exchange.

Internet Key Exchange (IKE) Protocol

- **IKE Header Format:**

- Flags (8 bits): Indicates specific options set for this IKE exchange. The **initiator bit** indicates whether this packet is sent by the SA initiator. The **version bit** indicates whether the transmitter is capable of using a higher major version number than the one currently indicated. The **response bit** indicates whether this is a response to a message containing the same message ID.
- Message ID (32 bits): Used to control retransmission of lost packets and matching of requests and responses.
- Length (32 bits): Length of total message (header plus all payloads) in octets.

Security Association (SA)

- The **output of the IKE phase** is a Security Association (SA).
- SA is an agreement between the communicating parties about factors such as **the IPSec protocol version in use, mode of operation (transport mode or tunnel mode), cryptographic algorithms, cryptographic keys, lifetime of keys,** etc.
- The principal objective of the IKE protocol is to establish an SA between the communicating parties.
- Once this is done, both major protocols of IPSec (ie. AH and ESP) make use of SA for their actual operation.
- Note that if both AH and ESP are used, each communicating party requires **two sets of SA:** one for AH and one for ESP.

Security Association (SA)

- **SA is simplex, i.e. unidirectional.**
- Therefore, at a second level, we need two sets of SA per communicating party:
  - one for incoming transmission
  - Another for outgoing transmission
- Thus, if the two communicating parties use both AH and ESP, each of them would require **four sets of SA**

SA	: 1
Traffic direction	: Incoming
Protocol	: AH

SA	: 1
Traffic direction	: Incoming
Protocol	: AH

SA	: 2
Traffic direction	: Outgoing
Protocol	: AH

SA	: 2
Traffic direction	: Outgoing
Protocol	: AH

SA	: 3
Traffic direction	: Incoming
Protocol	: ESP

SA	: 3
Traffic direction	: Incoming
Protocol	: ESP

SA	: 4
Traffic direction	: Outgoing
Protocol	: ESP

SA	: 4
Traffic direction	: Outgoing
Protocol	: ESP

Security Association (SA) Database

- Both the communicating parties must allocate some storage area for storing the SA information at their end.
- For this purpose, a standard storage area called as **Security Association Database (SAD)** is pre-defined and used by IPSec.
- Thus, each communicating party requires maintaining its own SAD.
- The SAD contains active SA entries.

- Contents of SAD fields are as follows
- **Sequence Number Counter:**
  - This 32-bit field is used to generate the sequence number field, which is used in the AH or ESP headers.

Security Association (SA) Database

- **Sequence Counter Overflow:**
  - This flag indicates whether the overflow of the sequence number counter should generate an audible event and prevent further
- **Anti-replay window:**
  - A 32-bit counter field and a bit map, which are used to detect if an incoming AH or ESP packet is a replay.
- **AH authentication:**
  - AH authentication cryptographic algorithm and the required key.
- **ESP authentication:**
  - ESP authentication cryptographic algorithm and the required key

Security Association (SA) Database

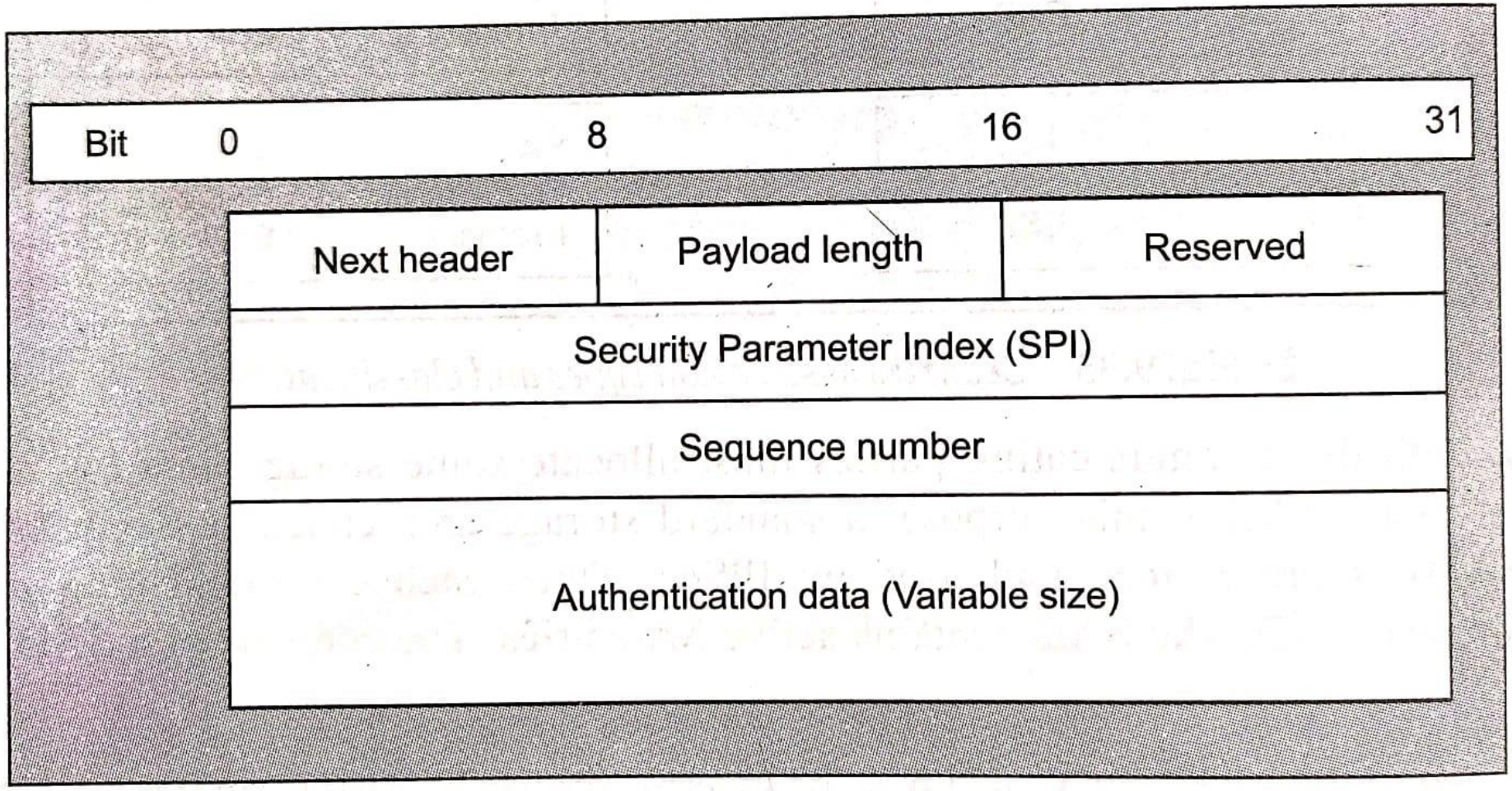
- **ESP encryption:**
  - ESP encryption algorithm, key, Initial Vector (IV).
- **IPSec Protocol mode:**
  - Indicates which IPSec protocol mode (eg, transport or tunnel) should be applied to the AH and ESP traffic.
- **Path Maximum Transfer Unit:**
  - The maximum size of an IP datagram that will be allowed to pass through a given network path without fragmentation.
- **Lifetime:**
  - Specifies the life of the SA. After this time interval, the SA must be replaced with a new one.

Authentication Header (AH)

- The Authentication Header (AH) provides support for **data integrity and authentication of IP packets**.
- The data integrity service ensures that data inside IP packets is not altered during the transit.
- The authentication service enables an end user or a computer system to authenticate the user or the application at the other end and decide to accept or reject packets, accordingly.
- This also prevents the IP spoofing attacks.
- Internally, AH is based on the MAC protocol, which means that the two communicating parties must share a secret key in order to use AH.

Authentication Header (AH)

- AH Structure



Authentication Header (AH)

- **Next header**
  - This 8-bit field identifies the type of header that immediately follows the AH.
  - For example, if an ESP header follows the AH, this field contains a value 50, whereas if another AH follows this AH, this field contains a value 51.
- **Payload length**
  - This 8-bit field contains the length of the AH in 32-bit words minus 2
  - Suppose that the length of the authentication data field is 96 bits (or three 32-bit words).
  - With a three-word fixed header, we have a total of 6 words in the header. Therefore, this field will contain a value of 4.
- **Reserved**
  - This 16-bit field is reserved for future use.

Authentication Header (AH)

- **Security Parameter Index (SPI)**
  - This 32-bit field is used in combination with the source and destination addresses as well as the IPSec protocol used (AH or ESP) to uniquely identify the Security Association (SA) for the traffic to which a datagram belongs.
- **Sequence number**
  - This 32-bit field is used to prevent replay attacks
- **Authentication data**
  - This variable-length field contains the authentication data, called as the **Integrity Check Value (ICV)** for the datagram.
  - This value is the MAC, used for authentication and integrity purposes.
  - For IPv4 datagrams, the value of this field must be an integral multiple of 32.
  - For IPv6 datagrams, the value of this field must be an integral multiple of 64.
  - For this, additional padding bits may be required.
  - The ICV is calculated generating a MAC using the HMAC digest algorithm.

How AH Deals with Replay attacks?

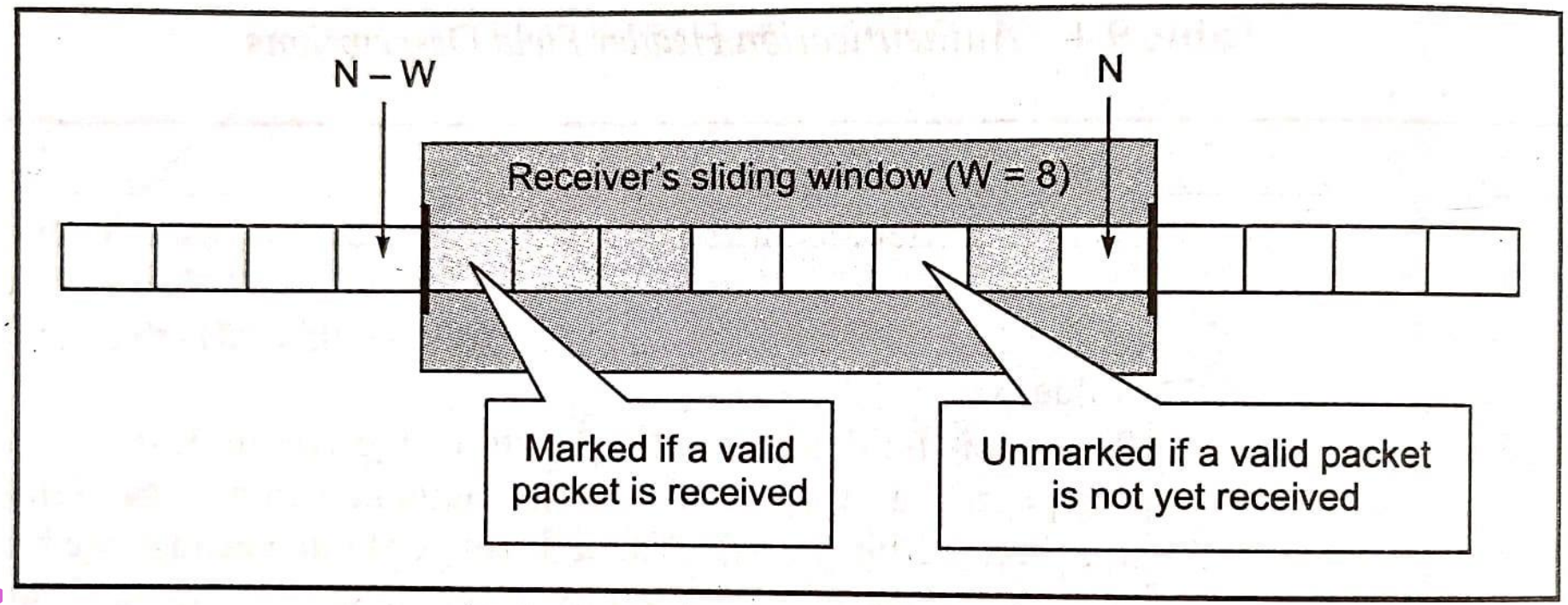
- In a replay attack, the attacker obtains a **copy of an authenticated packet** and later sends it to the intended destination.
- Since the same **packet is received twice**, the destination could face some problems because of this.
- To prevent this, we use a field called as **sequence number**.
- Initially, the value of this field is set to 0.
- Every time the sender sends a packet to the same sender over the same SA, it increments the value of this field by 1.
- The sender must not allow this value to circle back from 2^32 - 1 to 0.
- If the number of packets over the same increases this number, the sender must establish a new SA with the recipient.

How AH Deals with Replay attacks?

- On the receiver's side, there is some more processing involved.
- The receiver maintains a sliding window of size W, with the default value of W = 64.
- The right edge of the window represents the highest sequence number N received so far, for a valid packet.
- For simplicity, let us depict a sliding window with W = 8
- Following values are used:
  - W: Specifies the size of the window. In our example, it is 8
  - N: Specifies the maximum highest sequence number so far received for a valid packet. N is always at the right edge of the window.

How AH Deals with Replay attacks?

- For any packet with a sequence number in the range from (N-W+1) to N that has been correctly received (i.e. successfully authenticated), the corresponding slot in the window is marked.
- On the other hand, any packet in this range, which is not correctly received (i.e. not successfully authenticated), the slot is unmarked



How AH Deals with Replay attacks?

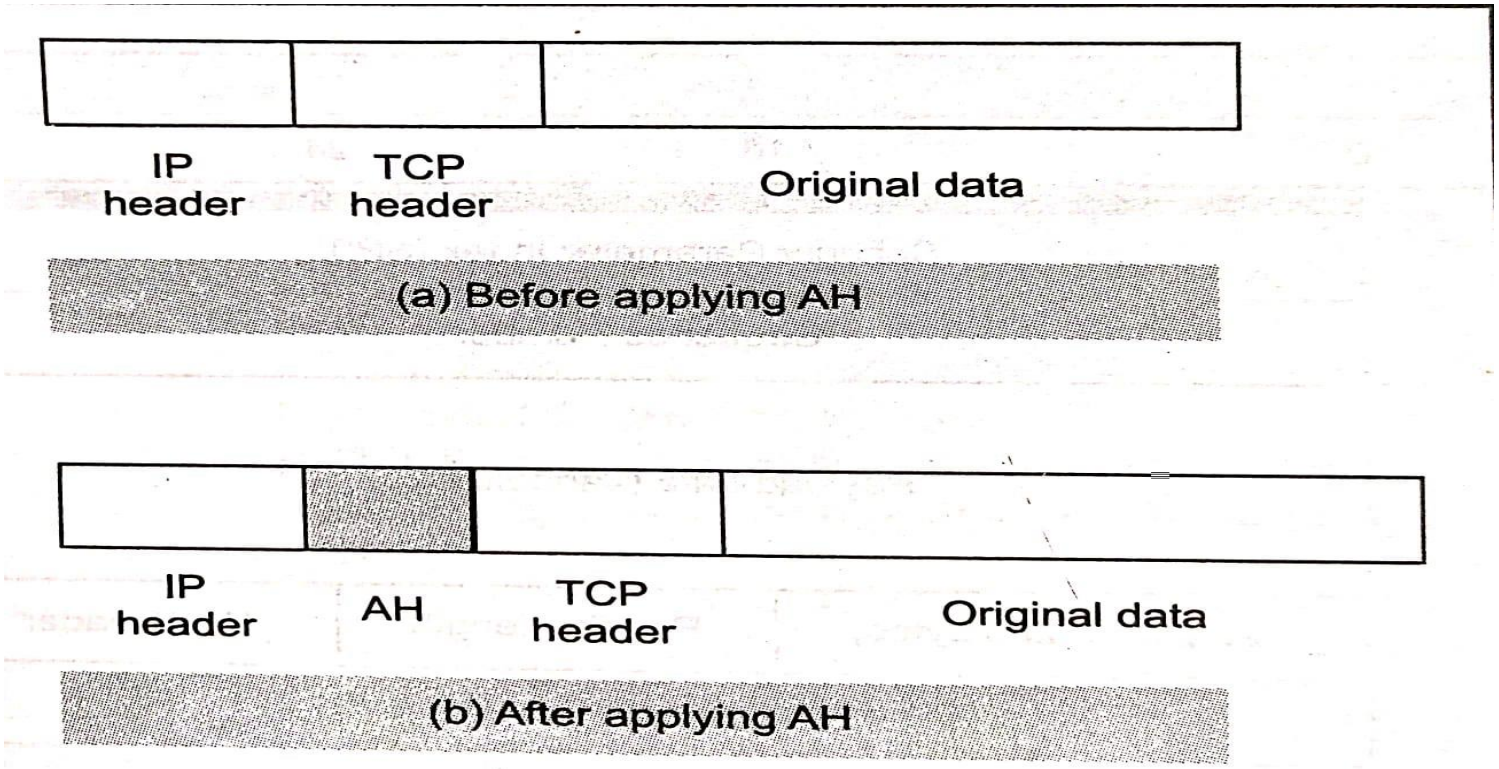
- Now, when a receiver receives a packet, it performs the following action depending on the sequence number of the packet
  - If the sequence number of the received packet falls within the window, and if the packet is new, its MAC is checked. If the MAC is successfully validated, the corresponding slot in the window is marked. The window itself does not move to the right hand side.
  - If the received packet is to the right of the window i.e. the sequence number of the packet is > N and if the packet is new, the MAC is checked. If the packet is authenticated successfully, the window is advanced to the right in such a way that the right edge of the window now matches with the sequence number of this packet. That is, this sequence number now becomes the new N.

How AH Deals with Replay attacks?

- Now, when a receiver receives a packet, it performs the following action depending on the sequence number of the packet
  - If the received packet is to the left of the window i.e. the sequence number of the packet is < (N-W), or if the MAC check fails, the packet is rejected, and an audible event is triggered.

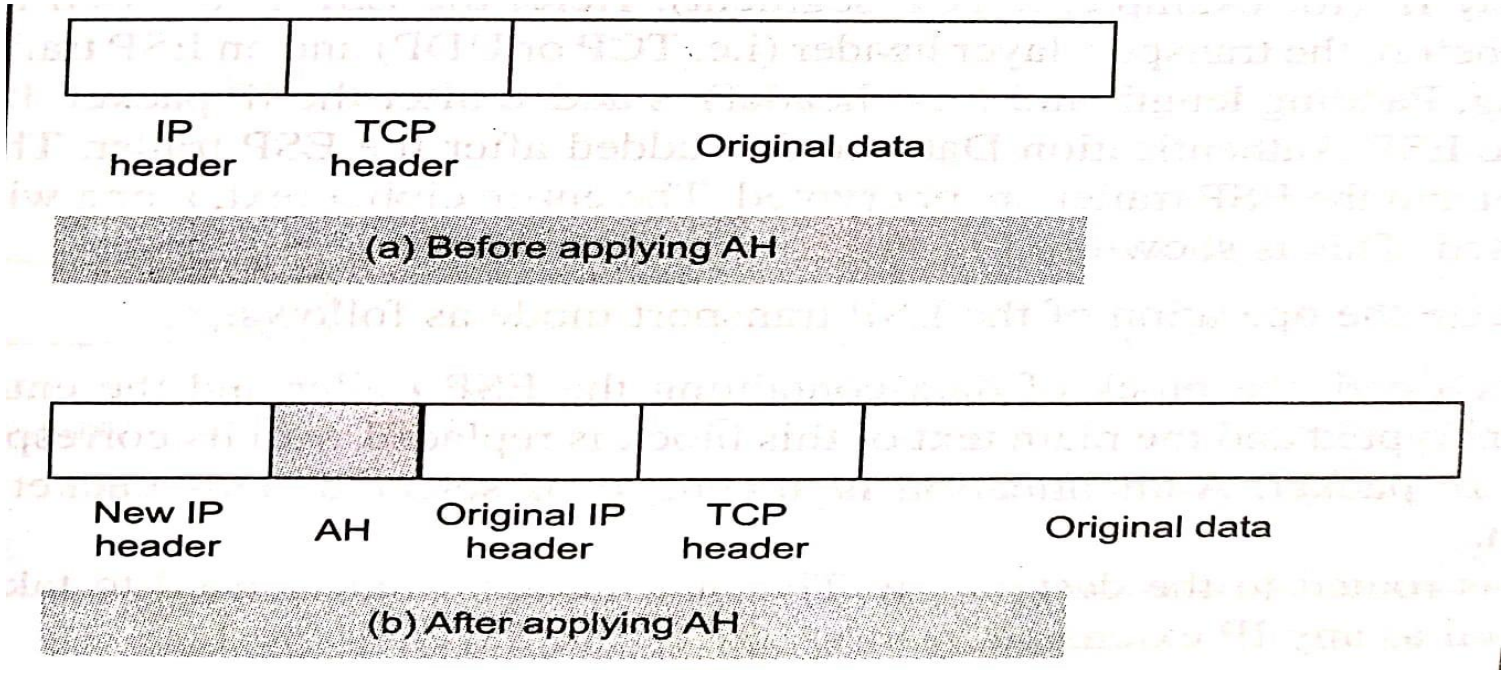
AH mode Operations

- **AH transport mode:**
- In the transport mode, the position of the Authentication Header (AH) is between the original IP header and the original TCP header of the IP packet.



AH mode Operations

- **AH tunnel mode:**
- In the tunnel mode, the entire original IP packet is authenticated and the AH is inserted between the original IP header and a new outer IP header.
- The inner IP header contains the ultimate source and destination IP addresses, whereas the outer IP header possibly contains different IP addresses (e.g. IP addresses of the firewalls or other security gateways).

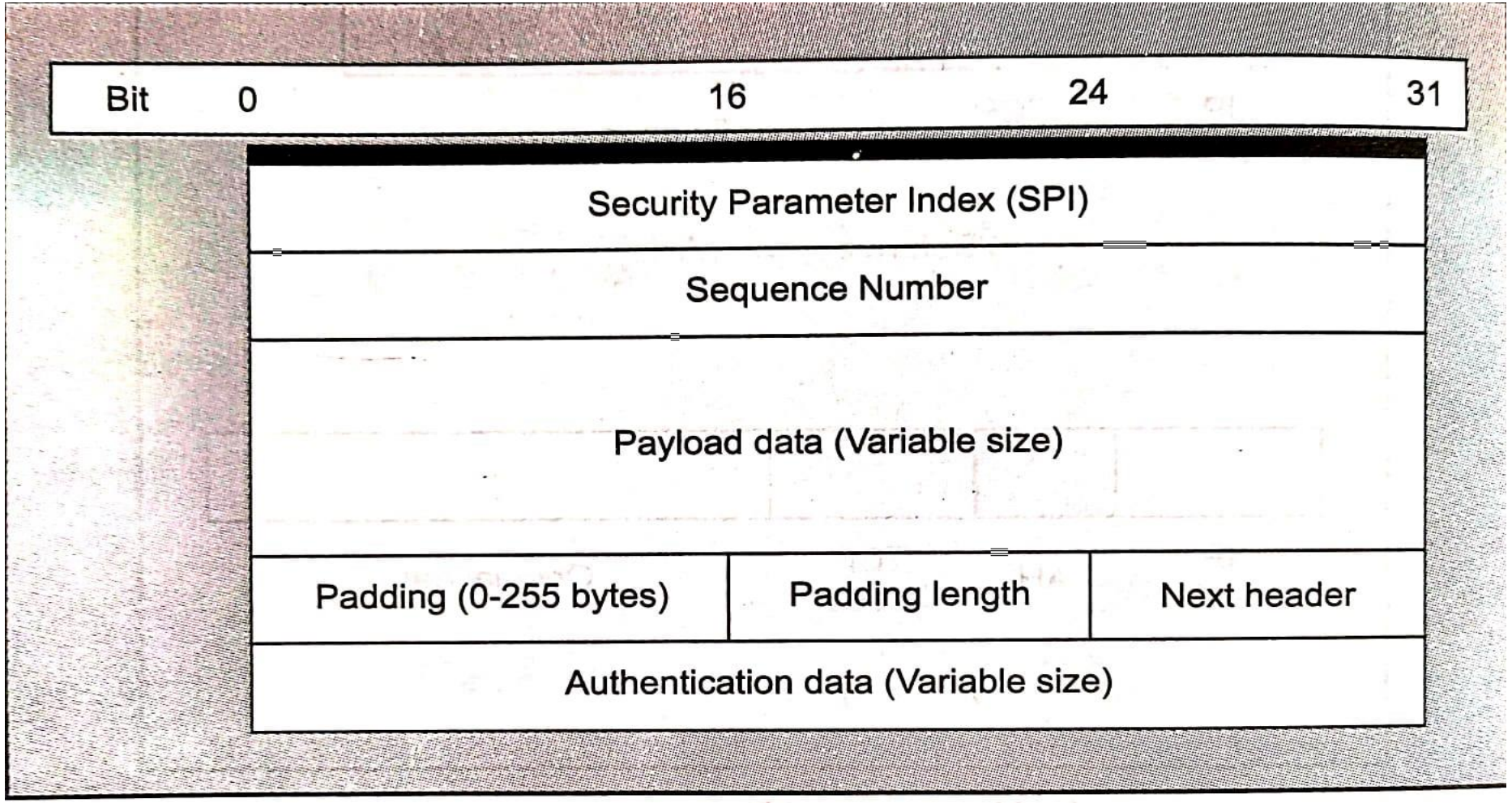


Encapsulating Security Payload (ESP)

- The Encapsulating Security Payload (ESP) protocol **provides confidentiality and integrity** of messages.
- ESP is based on symmetric key cryptography techniques.
- ESP can be used in isolation or it can be combined with AH.
- The ESP packet contains four fixed-length fields and three variable-length fields.
- **Security Parameter Index (SPI)**
- This 32-bit field is used in combination with the source and destination addresses as well as the IPSec protocol used (AH or ESP) to uniquely identify the Security Association (SA) for the traffic to which a datagram belongs.

Encapsulating Security Payload (ESP)

- The Encapsulating Security Payload (ESP) protocol structure



Encapsulating Security Payload (ESP)

- **Sequence number**
  - This 32-bit field is used to prevent replay attacks
- **Payload data**
  - This variable-length field contains the transport layer segment (transport mode) or IP packet (tunnel mode), which is protected by Padding encryption.
- **Padding**
  - This field contains the padding bits, if any
  - These are used by encryption algorithm or for aligning the padding length field, so that it begins at the third byte within the 4-byte word

Encapsulating Security Payload (ESP)

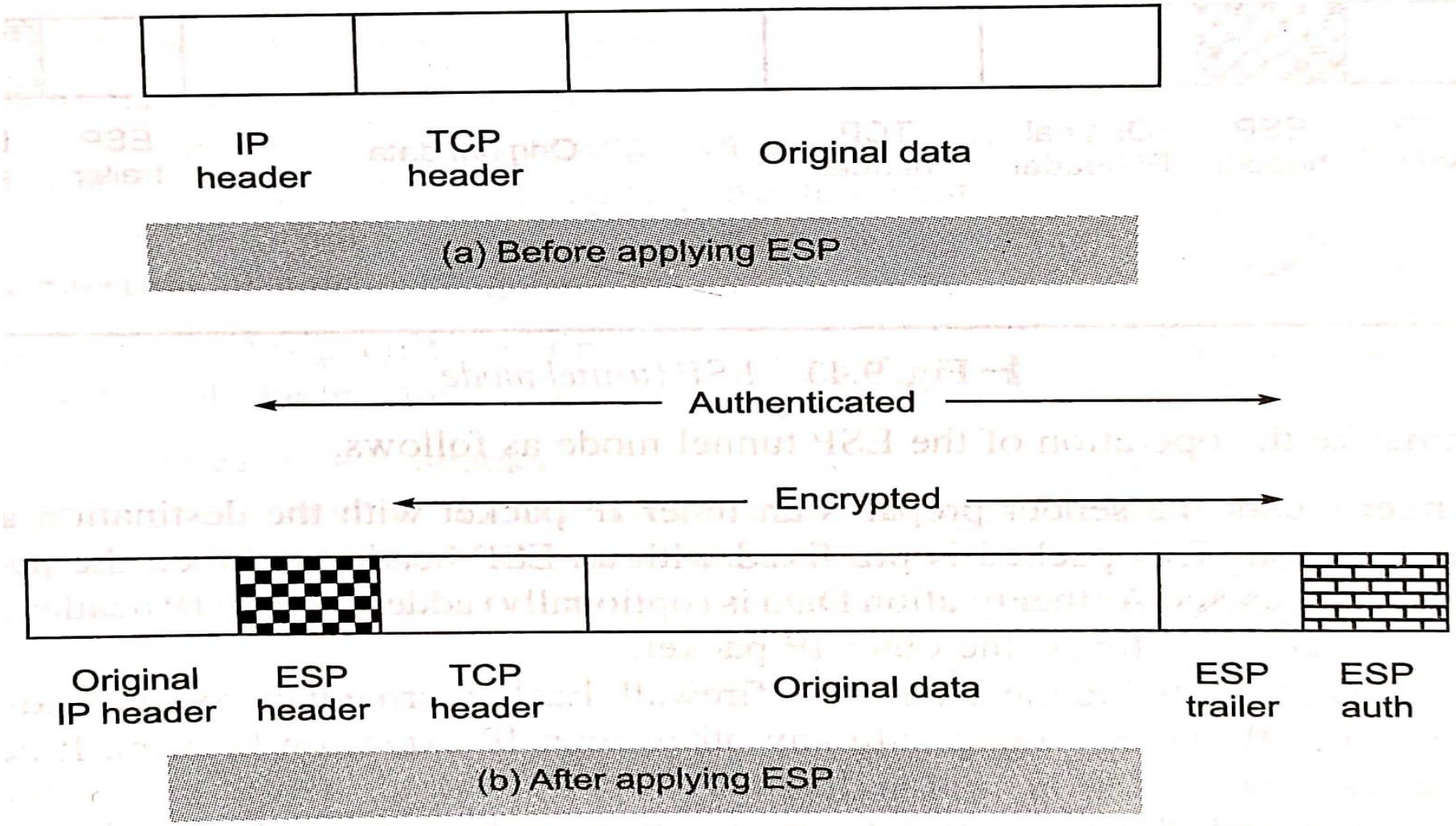
- **Padding Length**
  - This 8-bit field specifies the number of padding bytes in the immediately preceding field.
- **Next Header**
  - This 8-bit field identifies the type of encapsulated data in the payload.
  - For example, a value 6 in this field indicates that the payload contains TCP data.
- **Authentication Data**
  - This variable-length field contains the authentication data, called as the Integrity Check Value (ICV), for the datagram.
  - This is calculated over the length of the ESP packet minus the Authentication Data field.

ESP Transport mode operation

- Transport mode ESP is used **to encrypt** and optionally **authenticate** the data carried by IP (for example, a TCP segment). Here, the **ESP is inserted into the IP packet** immediately before the transport layer header (i.e. TCP or UDP) and an ESP trailer (containing the fields Padding, Padding length and Next header) is added after the IP packet.
- If authentication is also used, the ESP Authentication Data field is added after the ESP trailer.
- The entire transport layer segment and the ESP trailer are encrypted.
- The entire cipher text, along with the ESP header is authenticated

ESP Transport mode operation

- Transport mode ESP



ESP Transport mode operation

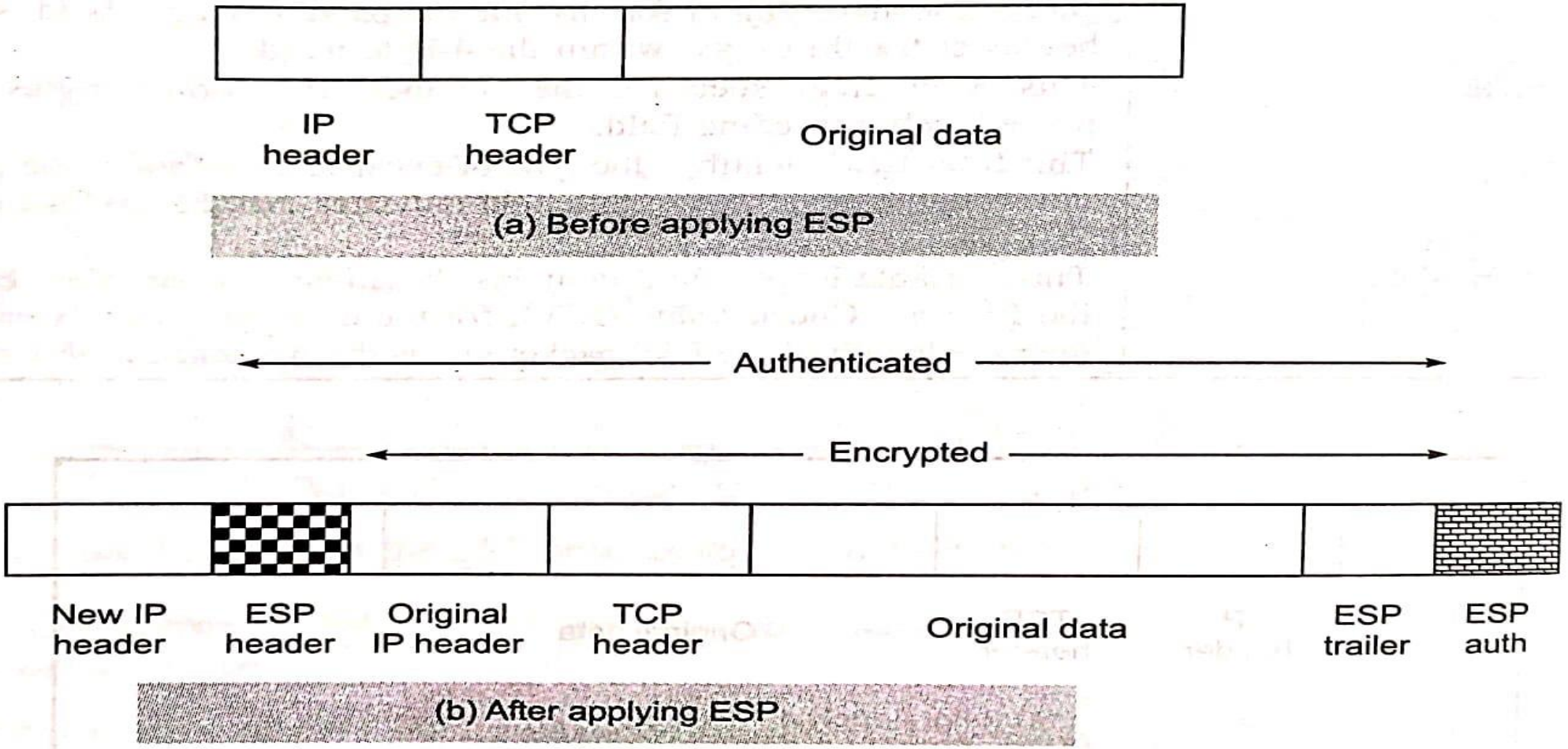
- **We can summarize the operation of the ESP transport mode as follows.**
- At the sender's end, the **block of data containing the ESP trailer and the entire transport layer segment is encrypted** and the plain text of this block is replaced with its corresponding cipher text to form the IP packet. Authentication is appended, if selected. This packet is now ready for transmission.
- The packet is routed to the destination. The intermediate routers need to take a look at the IP header as well as any IP extension headers, but not at the cipher text.
- At the receiver's end, the IP header plus any plain text IP extension headers are examined. The remaining portion of the packet is then decrypted to retrieve the original plain text transport layer segment.

ESP Tunnel mode operation

- The tunnel mode **ESP encrypts an entire IP packet.**
- Here, the ESP header is pre-fixed to the packet and then the packet along with the ESP trailer is encrypted.
- As we know, the IP header contains the destination address as well as intermediate routing information. Therefore, this packet cannot be transmitted as it is.
- Otherwise, the delivery of the packet would be impossible.
- Therefore, a new Ip header is added, which contains sufficient information for routing.

ESP Tunnel mode operation

- Tunnel mode ESP



ESP Transport mode operation

- We can summarize the operation of the ESP tunnel mode as follows.
- At the sender's end, the sender prepares an inner IP packet with the destination address as the internal destination. This packed is pre-fixed with an ESP header and then the packet and ESP trailer are encrypted and Authentication Data is (optionally) added. A new IP header is added to the start of this block. This forms the outer IP packet.
- The outer packet is routed to the destination firewall. Each intermediate router needs to check and process the outer IP header, along with any other outer IP extension headers. It need not know about the cipher text.
- At the receiver's end, the destination firewall processes the outer IP header plus any extension headers and recovers the plain text from the cipher text. The packet is then sent to the actual destination host.

References:

- Atul Kahate,"Cryptography and Network Security", second edition, Tata McGraw Hill
- William Stallings, "Cryptography and Network Security-Principles and practice"