Unit: Network Security

B.Tech VIII

NETWORK AND SYSTEM SECURITY (CORE ELECTIVE - 5) (CS424)

Book :

Computer Security: Principles and Practice
By William Stallings

Chapter 22: Internet Security Protocols and Standards
Chapter 23 Internet Authentication Applications
Chapter 24 Wireless Network Security

Contents

- **Chapter 22: Internet Security Protocols and Standards**
  - IPv4 and IPv6 Security
  - IPSec Protocol,
  - Internet Authentication Applications
  - Kerberos, X.509

IPv4 and IPv6 Security

IPv4 and IPv6 Security

- Several **Application level security Protocols**
  - For mail(S/MIME), Client/Server (Kerberos), Web Access (SSL).
  - Need some security at network level.
  - **Example**: An enterprise can run a secure, private TCP/IP network by disallowing links to untrusted sites, encrypting packets that leave the premises, and authenticating packets that enter the premise.
  - An organization can ensure secure networking by implementing security at the IP level.
  - At Network layer, **IP (Internet Protocol)** is used.

IPv4 and IPv6 Security

- IPv4 does not provide any mandatory security measures, and it depends on the application being used.
- **Internet Architecture Board (IAB)** included authentication and encryption as necessary security features in the next-generation IP, i.e. IPv6.
- These security capabilities were designed to be usable both with the current IPv4 and the future IPv6.
- IP-level security encompasses three functional areas:
  - Authentication
  - Confidentiality
  - Key management

IPv4 and IPv6 Security

- **Authentication**
  - Assures that a received packet was transmitted by the party identified as the source in the packet header.
  - Assures that the packet has not been altered in transit.
- **Confidentiality**
  - Facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.
- **Key management**
  - Concerned with the secure exchange of keys.
- **The protocol which offers all these functionalities at IP layer is IPsec (IP Security)**

IPv4 and IPv6 Security

- The current version of IPsec i.e. **IPsecv3**, encompasses authentication and confidentiality.
- Key management is provided by the Internet Key Exchange standard, **IKEv2.**

Applications of IPsec

- IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
- **Example:**
  - **Secure branch office connectivity over the Internet**:
    - A company can build a secure virtual private network among its branch offices over the Internet or over a public WAN.
  - **Secure remote access over the Internet**:
    - An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider and gain secure access to a company network.
  - **Establishing extranet and intranet connectivity with partners:**
    - IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

Applications of IPsec

- IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
- **Example(Cont..):**
  - **Enhancing electronic commerce security:**
    - Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security.
- **Principle Feature of IPsec**
  - It can encrypt and/or authenticate *all* traffic at the IP level.
  - Thus, all distributed applications, including remote logon, client/server, e-mail, file transfer, Web access, and so on, can be secured.

Benefits of IPsec

1. **IPsec is implemented in a firewall or router**
   - Offers strong security to all traffic crossing the perimeter.
   - Avoids the additional overhead for security processing to entire traffic.
   - IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
2. **IPsec is transparent to applications**
   - IPsec is below the transport layer (TCP, UDP).
   - No change in software at client/server is required if implemented in the firewall/router.
   - If IPsec is implemented in end systems, upper-layer software, including applications, is not affected.

Benefits of IPsec(Cont..)

3. **IPsec can be transparent to end users**
   - No need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

4. **IPsec can provide security for individual users**
   - Useful for off-site workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

IPsec- In Detail

- It is an **Internet Engineering Task Force (IETF)** standard suite of protocols .
- Offers security between 2 communication points across the IP network.
- Provides data authentication, integrity, and confidentiality.
- Defines the encrypted, decrypted and authenticated packets.
- The protocols needed for secure key exchange and key management are defined in IPsec.

IPsec- In Detail

- IPsec can be used to do the following things:
  - To encrypt application layer data.
  - To provide security for routers sending routing data across the public internet.
  - To provide authentication without encryption, like to authenticate the data originates from a known sender.
  - To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a **Virtual Private Network (VPN)** connection.

IPsec- In Detail

- **Components of IP Security**

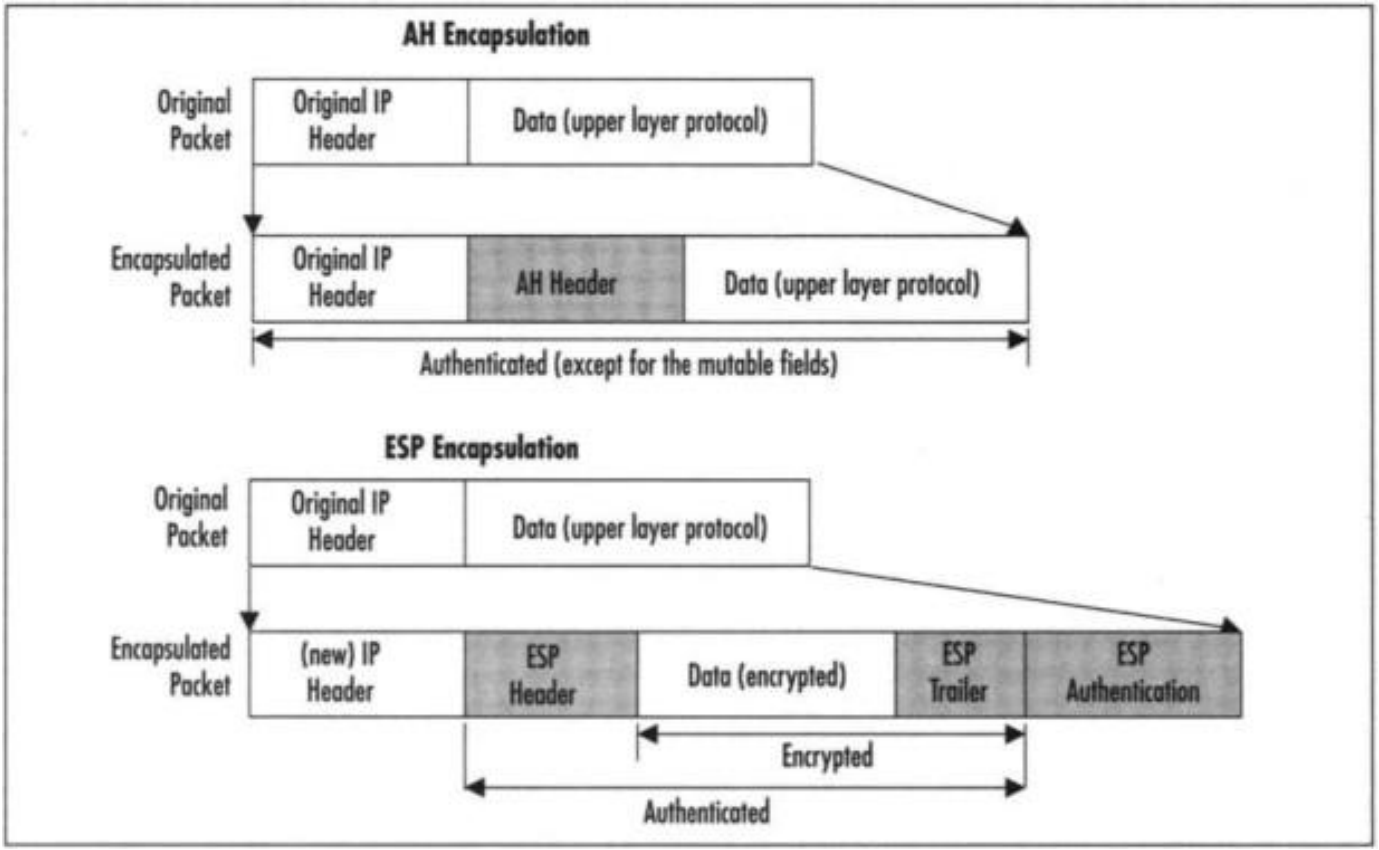
1. **Encapsulating Security Payload (ESP) Protocol**
   - It provides data integrity, encryption, authentication and anti replay.
   - It also provides authentication for payload.
2. **Authentication Header (AH) Protocol**
   - It also provides data integrity, authentication and anti replay and it does not provide encryption.
   - The anti replay protection, protects against unauthorized transmission of packets.
   - It does not protect data's confidentiality.

IPsec- In Detail

- **Components of IP Security (Cont..)**

3. **Internet Key Exchange (IKE)**
   - It is used to dynamically exchange encryption keys over **Security Association (SA)** between 2 devices.
   - An SA establishes shared security attributes between 2 network entities to support secure communication.
   - The Key Management Protocol (ISAKMP) and Internet Security Association provide a framework for authentication and key exchange.
   - ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

IPsec – in Detail



IPsec Packet format

Security Associations(SA)

- An Security Association (SA) is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.
- If a peer relationship is needed, for two-way secure exchange, then two SAs are required.
- Security services are afforded to an SA for the use of ESP.

Security Associations(SA)

- SA is uniquely identified by three parameters:
  - **Security Parameter Index (SPI):**
    - A bit string assigned to this SA and having local significance only.
    - The SPI is carried in an ESP header to enable the receiving system to select the SA under which a received packet will be processed.
  - **IP destination address**:
    - This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router.
  - **Protocol identifier**:
    - This field in the outer IP header indicates whether the association is an AH or ESP security association.

Security Associations(SA)

- An IPsec implementation includes an **SA database** that defines the parameters associated with each SA.
- SA is characterized by the following parameters:

1. **Sequence number counter**: A 32-bit value used to generate the Sequence Number field in AH or ESP headers.
2. **Sequence counter overflow**: A flag indicating whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on this SA.
3. **Antireplay window**: Used to determine whether an inbound AH or ESP packet is a replay, by defining a sliding window within which the sequence number must fall.

Security Associations(SA)

4. **AH information:** Authentication algorithm, keys, key lifetimes, and related parameters being used with AH.
5. **ESP information:** Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP.
6. **Lifetime of this security association:** A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur.
7. **IPsec protocol mode:** Tunnel, transport, or wildcard (required for all implementations).
8. **Path MTU:** Any observed path maximum transmission unit (maximum size of a packet that can be transmitted without fragmentation).

ESP Packet

- The **Encapsulating Security Payload(ESP)** provides confidentiality services for the message contents.
- As an optional feature, ESP can also provide an authentication service.

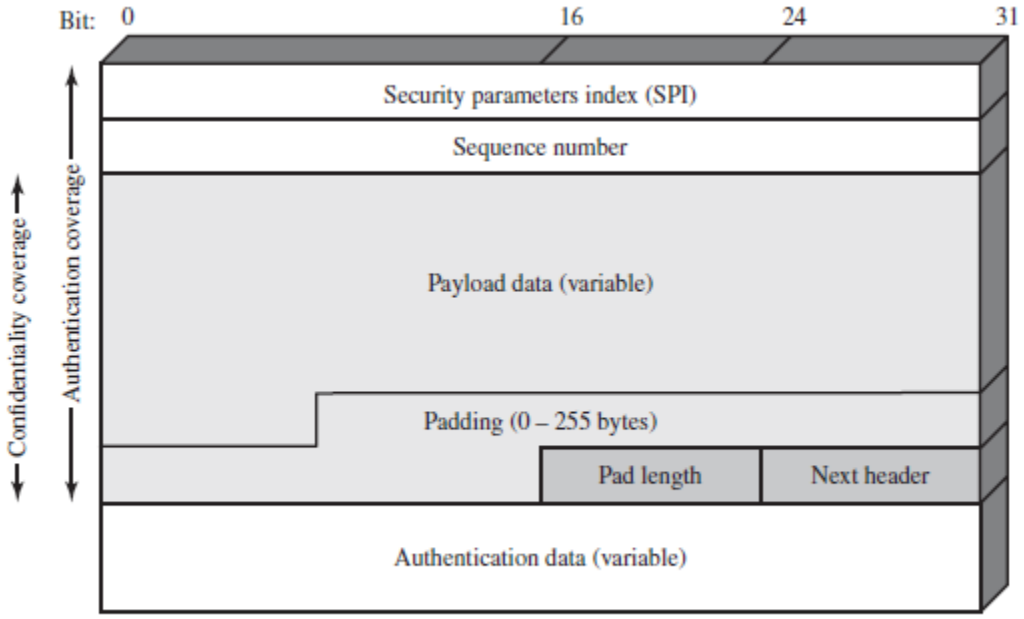


Figure 22.8 **IPsec ESP Format**

ESP Packet

- ESP packet includes several fields:
- **Security Parameters Index(32 bits)**: Identifies a security association.
- **Sequence Number(32 bits)**: A monotonically increasing counter value.

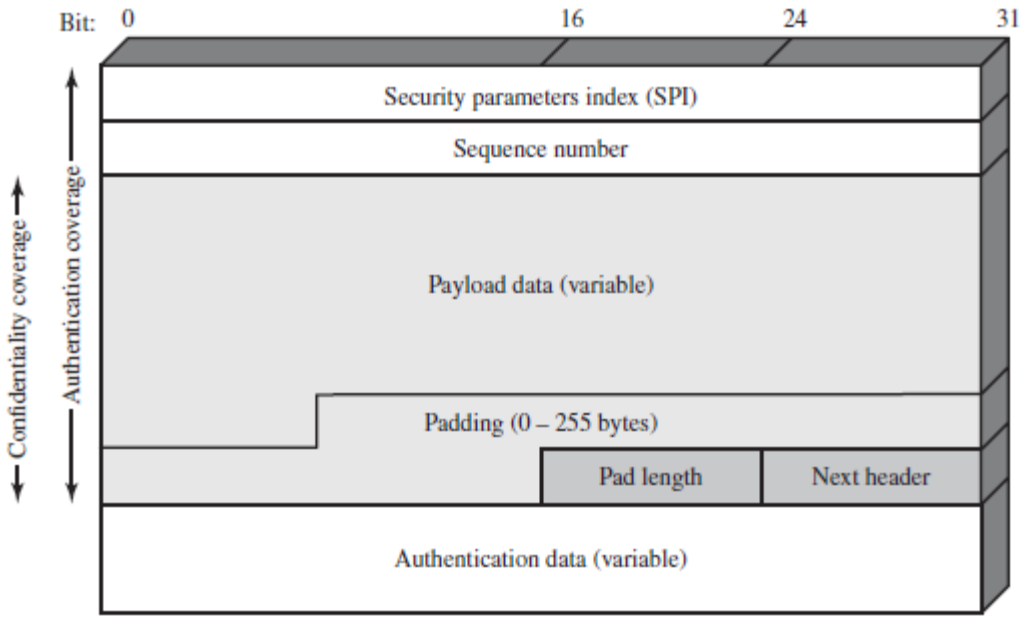


Figure 22.8 **IPsec ESP Format**

ESP Packet

- ESP packet includes several fields:
- **Payload Data (variable)**: This is a transport-level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.

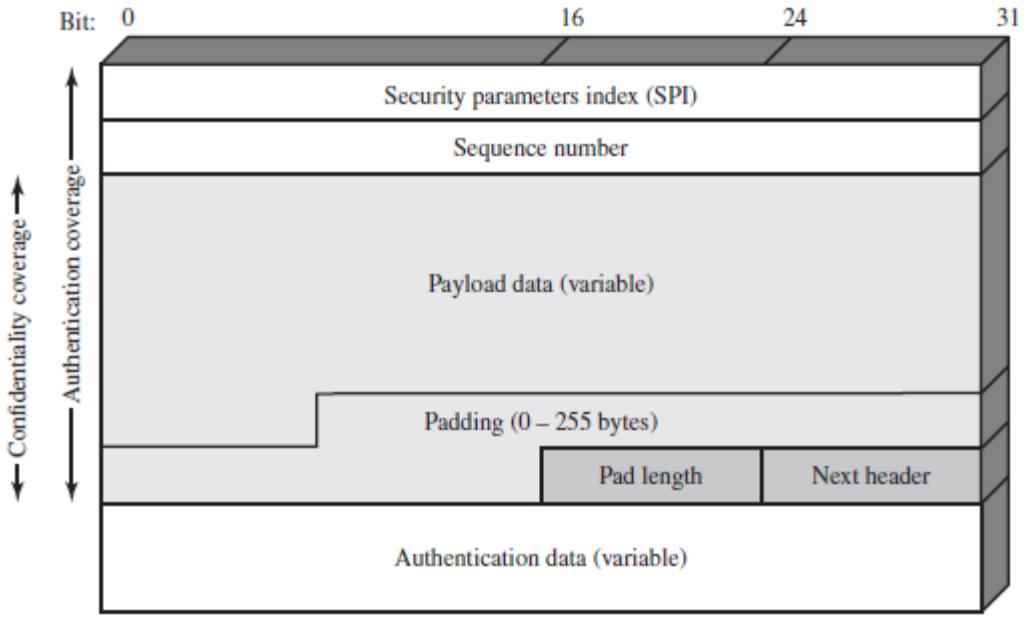


Figure 22.8 **IPsec ESP Format**

ESP Packet

- ESP packet includes several fields:
- **Padding (0–255 bytes)**: May be required if the encryption algorithm requires the plaintext to be a multiple of some number of octets.

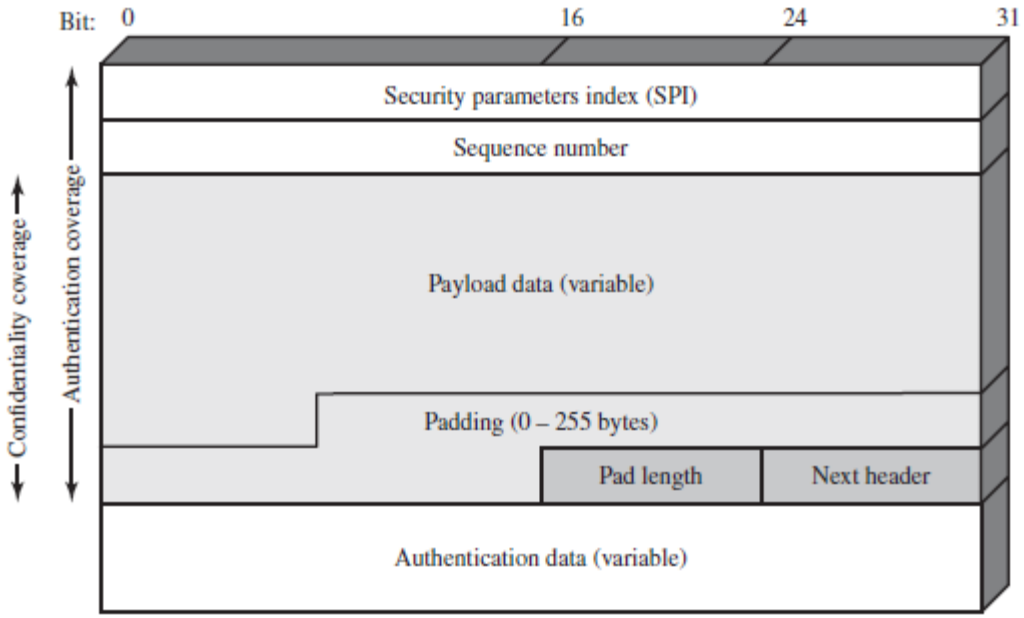


Figure 22.8 **IPsec ESP Format**

ESP Packet

- ESP packet includes several fields:
- **Pad Length (8 bits)**: Indicates the number of pad bytes immediately preceding this field.

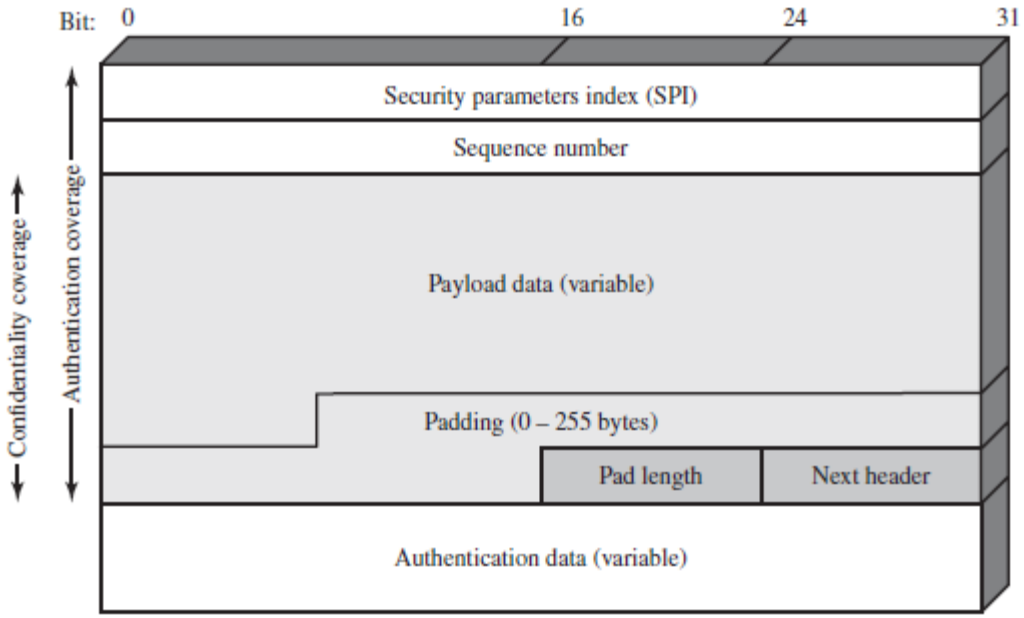


Figure 22.8 **IPsec ESP Format**

ESP Packet

- ESP packet includes several fields:
- **Next Header (8 bits)**: Identifies the type of data contained in the Payload Data field by identifying the first header in that payload (e.g., an extension header in IPv6, or an upper-layer protocol such as TCP).

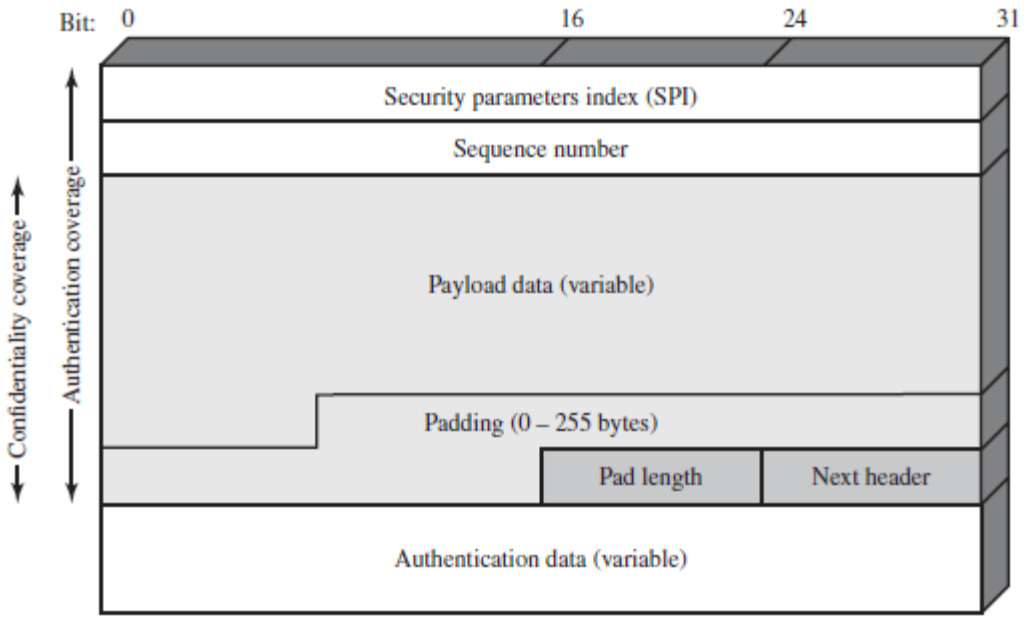


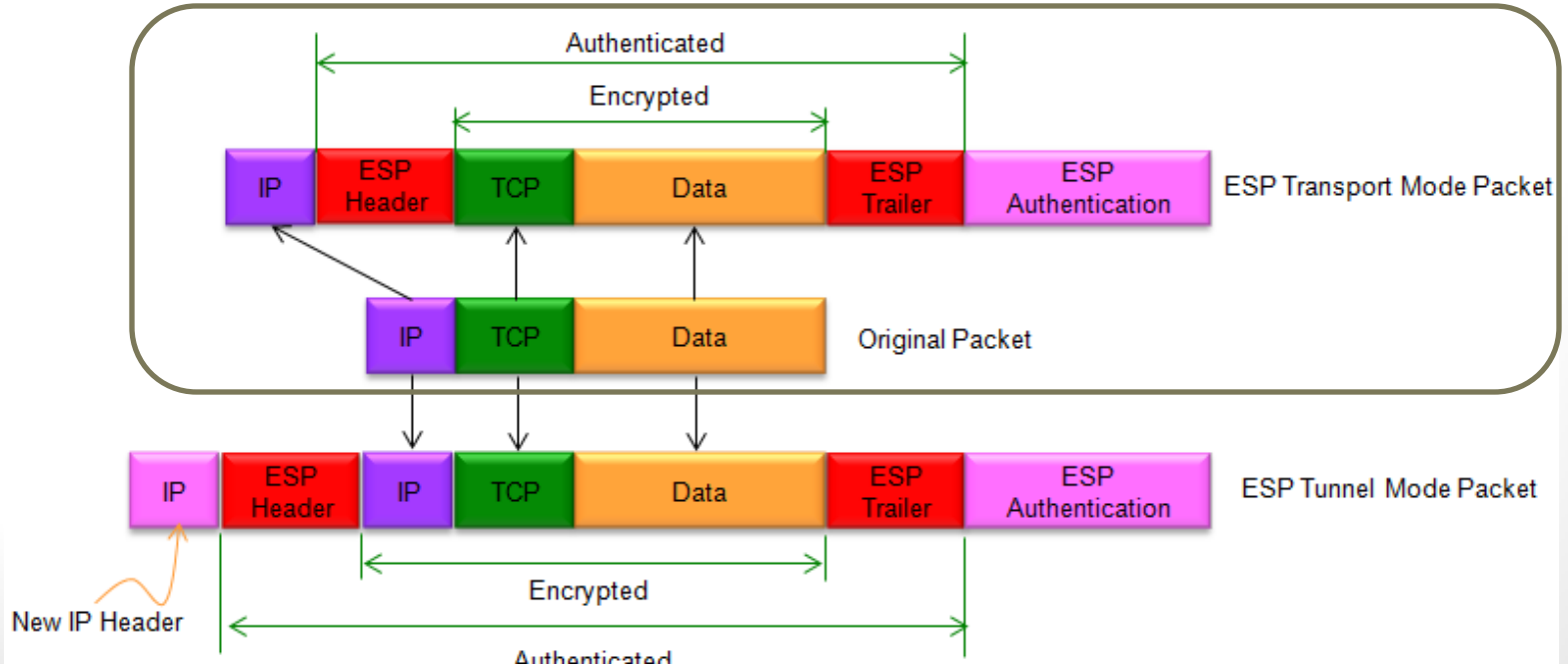
Figure 22.8 **IPsec ESP Format**

IPsec modes

- Both AH and ESP can operate in either
  - **Transport mode**
  - **Tunnel mode**

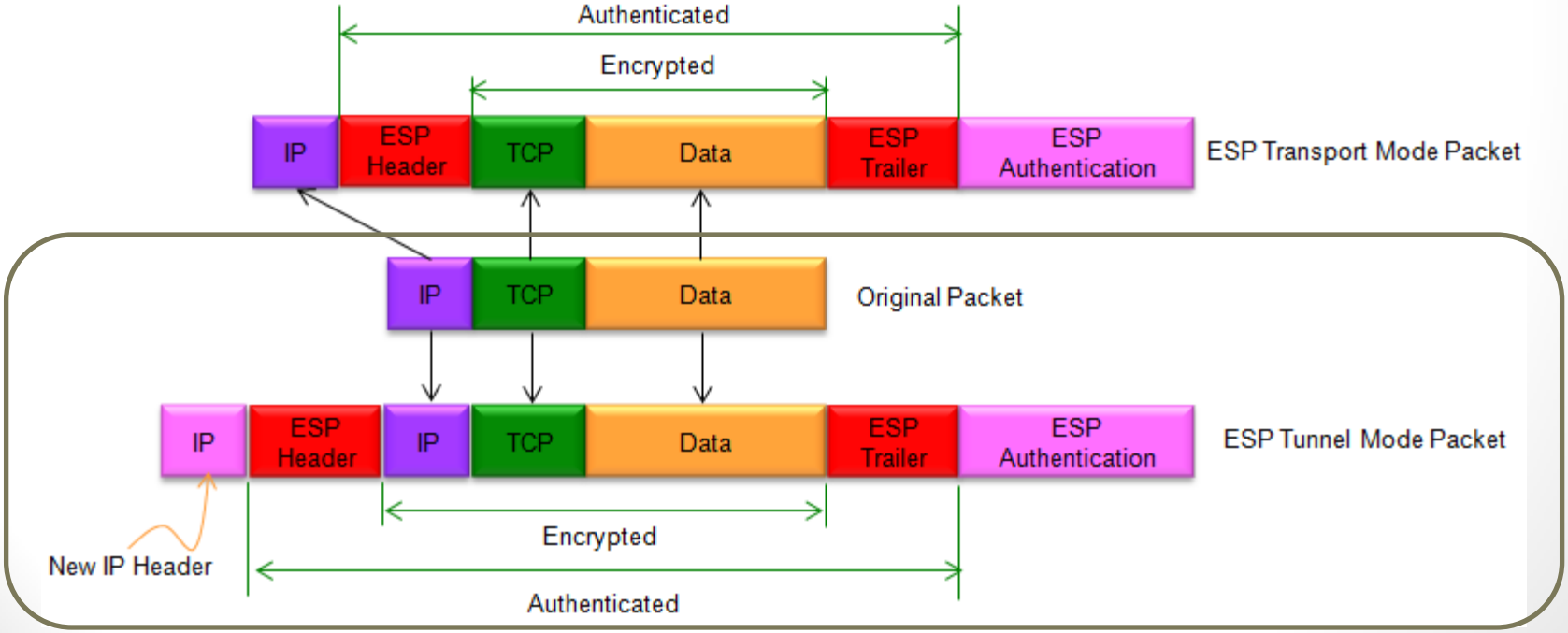
IPsec modes

- **Transport mode**
  - Transport mode provides protection primarily for upper layer protocols.
  - In transport mode, only the payload of the IP packet is usually encrypted and/or authenticated.
  - The routing is intact, since the IP header is neither modified nor encrypted.



IPsec modes

- **Tunnel mode**
  - Tunnel mode provides protection to the entire IP packet.
  - The entire IP packet is encrypted and/or authenticated.
  - It is then encapsulated into a new IP packet with a new IP header.



IPsec modes

- **Tunnel mode(Cont..)**
  - The entire original, inner, packet travels through a tunnel from one point of an IP network to another; no routers along the way are able to examine the inner IP header.
  - **Because the original packet is encapsulated, the new, larger packet may have totally different source and destination addresses, adding to the security.**
  - Tunnel mode is used to create VPNs for network-to-network communications (e.g., between routers to linksites), device-to-network communications (e.g., remote user access) and device-to-device communications (e.g., private chat).

IPsec modes

- **Example :** How tunnel mode IPsec operates?
  - Host A on a network generates an IP packet with the destination address of host B on another network.
  - This packet is routed from the originating host to a firewall or secure router at the boundary of A's network.
  - The firewall filters all outgoing packets to determine the need for IPsec processing. If this packet from A to B requires IPsec, the firewall performs IPsec processing and encapsulates the packet with an outer IP header.
  - The source IP address of this outer IP packet is the IP of Node where firewall is available, and the destination address may be a firewall that forms the boundary to B's local network.
  - This packet is now routed to B's firewall, with intermediate routers examining only the outer IP header.
  - At B's firewall, the outer IP header is stripped off, and the inner packet is delivered to B.