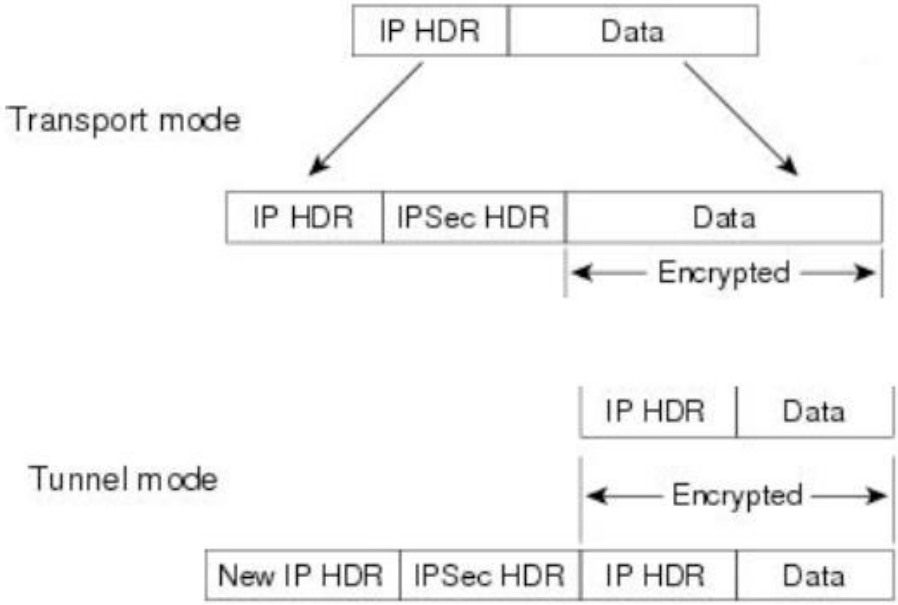
IPv6 Security Features

1. IPsec is mandatory in IPv6
2. Since IPsec become part of the IPv6 protocol all node can secure their IP traffic if they have required keying infrastructure
3. In build IPsec does not replace standard network security requirement but introduce added layer of security with existing IP network

IPsec Transport and Tunnel Mode

IPsec has two mode of encapsulation

1. Transport mode : Provide end to end security between two end station
2. Tunnel mode : Provide secure connection between two gateway (router). Unencrypted data from end system go through encrypted tunnel provided by the source and destination gateways
3. IPsec Transport and Tunnel Mode



IPsec Security Services

IPsec has two types of security services:

1. **Authenticated Header (AH)**: The protection is made by computing a cryptographic checksum over the protected fields.
2. **Encapsulating Security Payload (ESP)**: Compared to AH, ESP adds confidentiality (encryption), but has a more limited integrity protection, covering only the payload.

IPsec Security Services

Services Provided by AH and ESP:

1. Authenticated Header (AH):
    a. Integrity of the whole packet
    b. Authentication of the source
    c. Replay protection
2. Encapsulating Security Payload (ESP):
    a. Confidentiality
    b. Integrity of the inner packet
    c. Authentication of the source
    d. Replay protection

IPsec Pre-establish Security Association

IPsec peer need a pre-establish security association before they start sending packets

1. This involves standard key exchange and cryptographic algorithm
2. Standard IKE (Internet Key Exchange) protocol is used for IPsec of IPv6

Symmetric and Asymmetric Keying

There are two basic types of keying solutions:

1. Symmetric : Same key will be used to encrypt and decrypt data packet. Since same key is used for encryption and decryption its simple and faster. Key need to share out of band. Tunnel mode symmetric key
2. Asymmetric : Asymmetric keying use public key and private key for encryption and decryption. Key can be share in band. Transport mode use asymmetric key