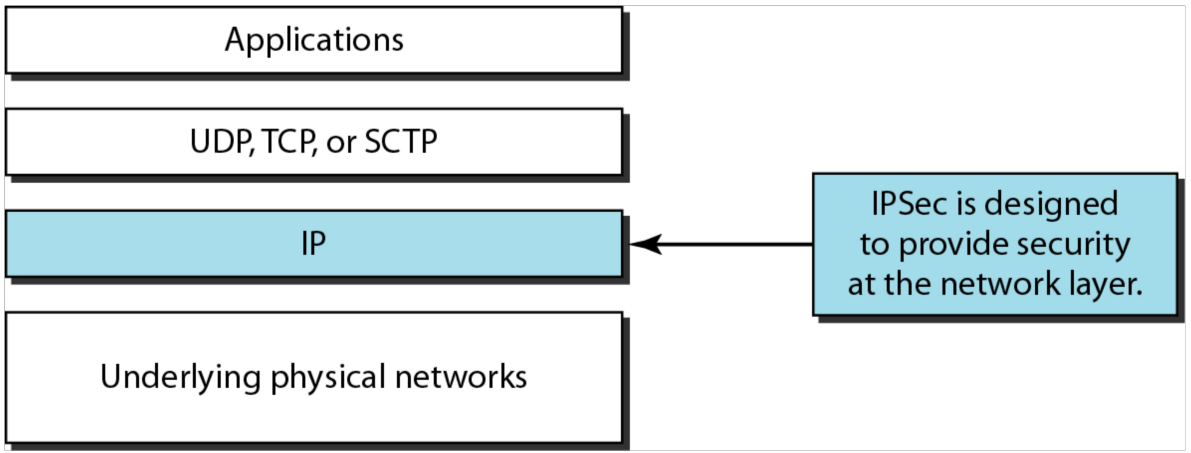
Module 5

Network Security and Applications

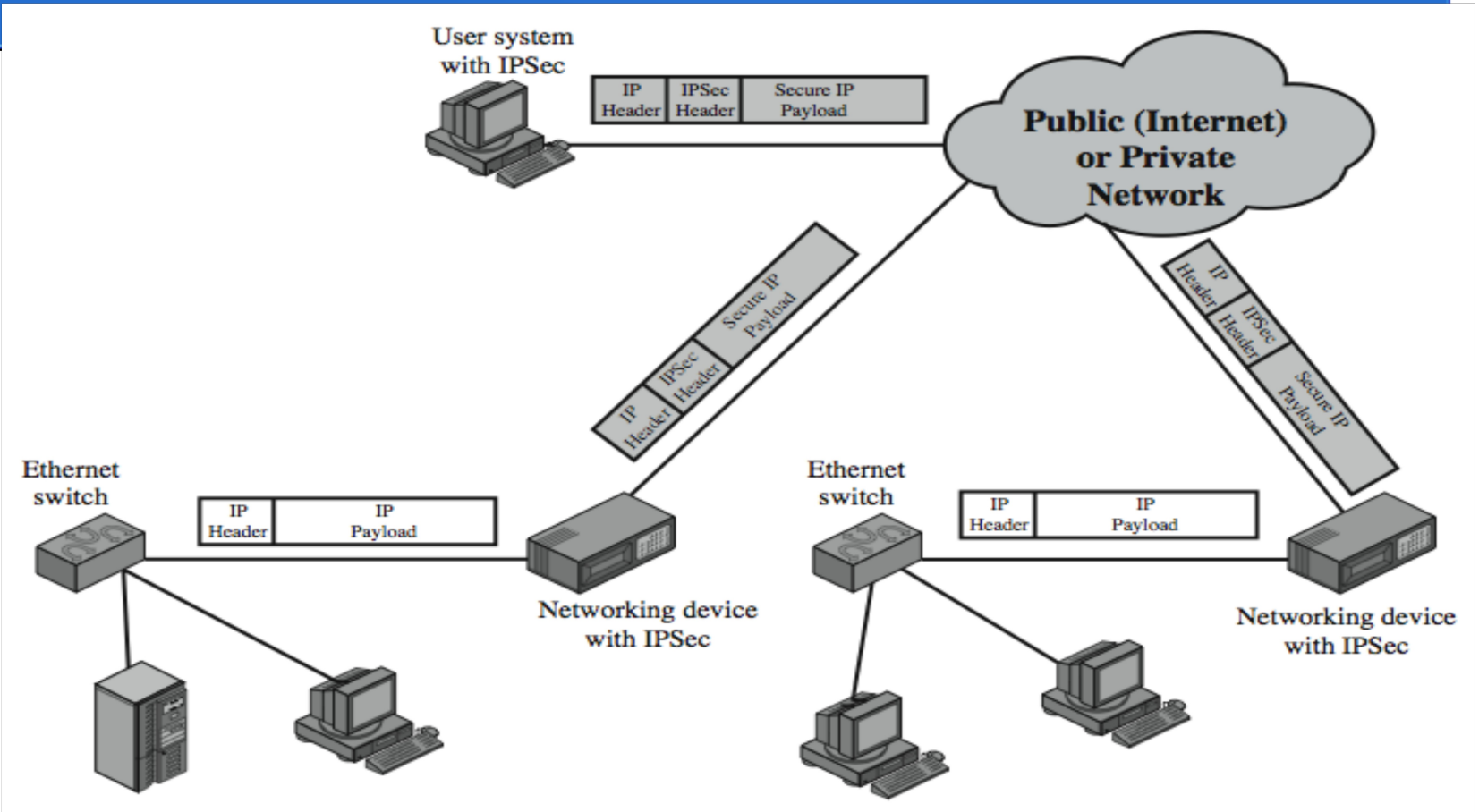
IPSec


Applications
UDP, TCP, or SCTP
IP
Underlying physical networks
IPSec is designed to provide security at the network layer.

IPSec

- IP Security (IPSec) is a collection of protocols designed to provide security for a packet at the network level
- IPSec helps to create authenticated and confidential packets for the IP layer
- The main feature of IPSec is that, it can encrypt and/or authenticate all traffic at the IP level which in turn provides security to all services like e-mails, client/server, file transfer, remote login etc.

IPSec


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
Secure IP Payload
IPSec Header
IP Header
IP Header
IPSec Header
Secure IP Payload
Ethernet switch
IP Header
IP Payload
Networking device with IPSec
Ethernet switch
IP Header
IP Payload
Networking device with IPSec

Applications

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security

Benefits

- When IPsec is implemented in firewall or router, it provides strong security applicable to all traffic crossing the perimeter
  - Traffic within company/workgroup has no overhead from security-related processing
- IPsec in firewall resists bypass if all outside traffic must use IP and the firewall is the only way Internet traffic enters organization
- IPsec below the transport layer (TCP, UDP); transparent to applications
  - No need to change software on a user or server system when IPsec is implemented in the firewall or router
- IPsec can be transparent to end users
  - No need to train users on security mechanisms, issue keys on a per-user basis, or revoke keys when users leave organization
- IPsec can provide security for individual users if needed
  - Useful for offsite workers, setting up secure virtual subnetwork within an organization for sensitive applications

Services

- Authentication
- Confidentiality
- Key management

Modes

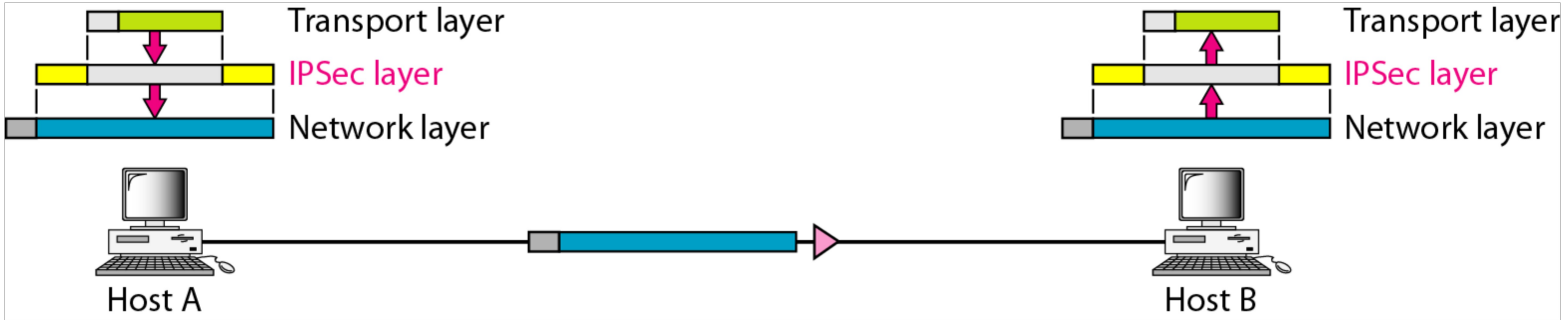
- Transport Mode
- Tunnel Mode

Transport Mode

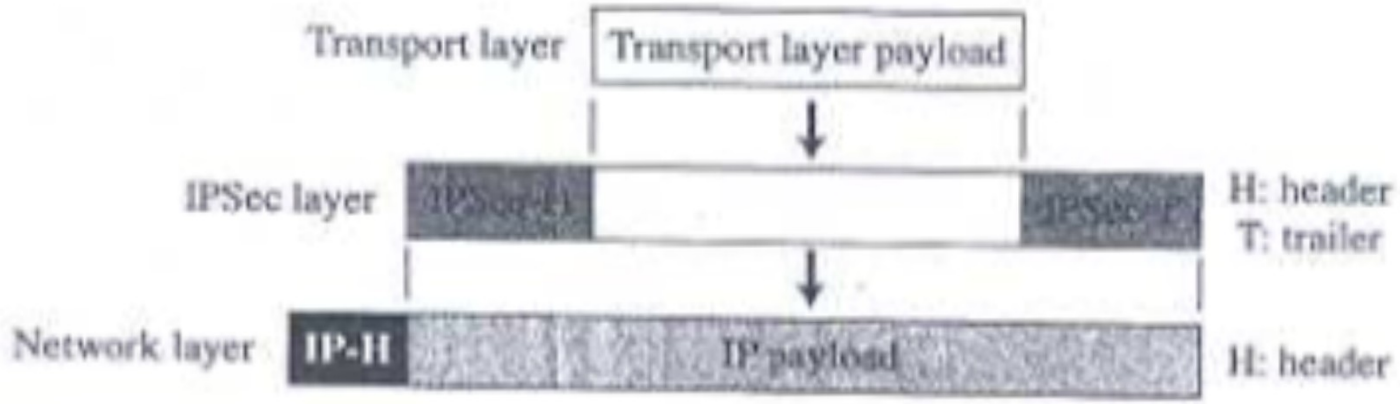
- This mode protects the network layer payload to be encapsulated in the network layer
- It does not protect the whole IP packet. It protects only the packet from transport layer (IP payload)
- In this mode, IPSec header and trailer is added to the information coming from transport layer.
- IP header is added later

Transport Mode

- This mode is used when we need host-to-host (end to end) data protection
- The sender uses IPSec to authenticate and encrypt the payload delivered from transport layer
- The receiver uses IPSec to check the authentication and decrypt the IP packet

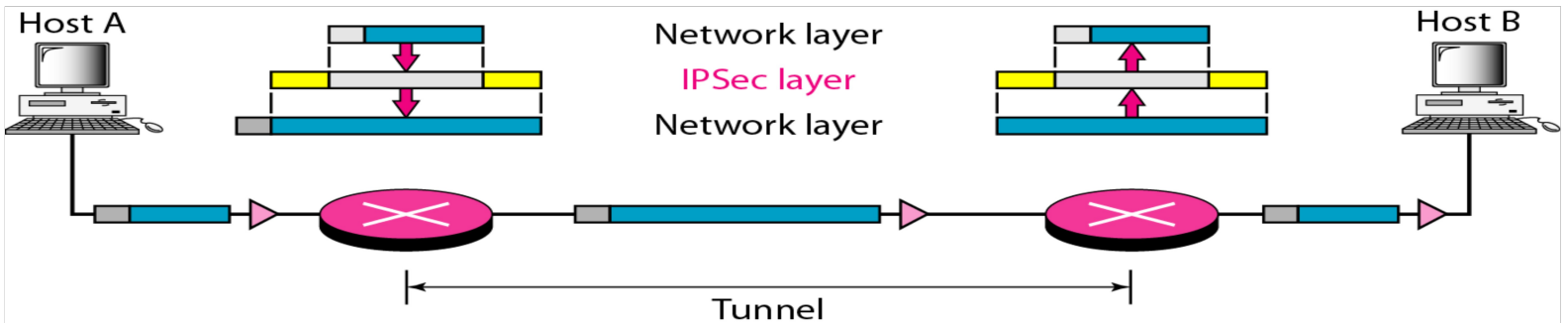


Transport Mode

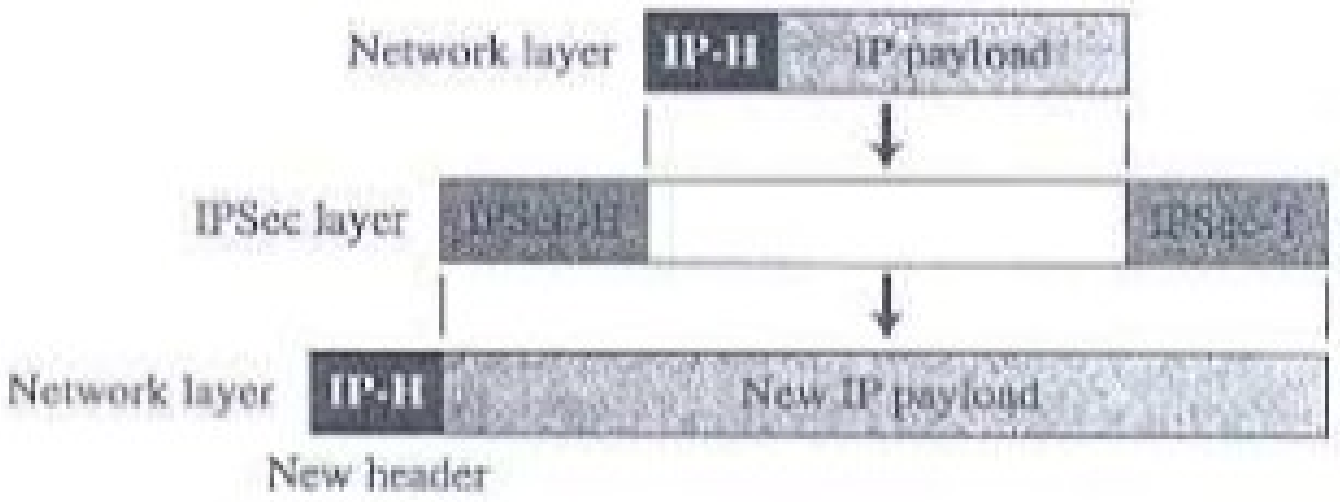


Tunnel Mode

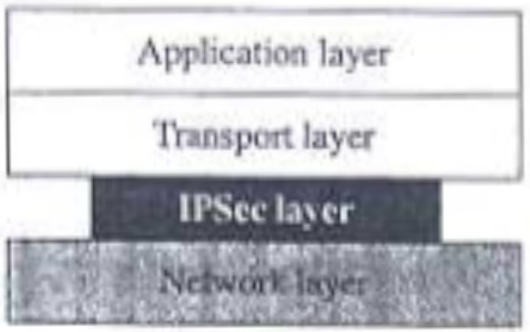
- This mode protects the entire IP packet
- It takes an IP packet (including the header), applies IPSec security methods to the entire packet and then adds a new IP header
- This new IP header has different information than the original IP header
- Tunnel mode is used between two routers, between a host and a router or between a router and a host



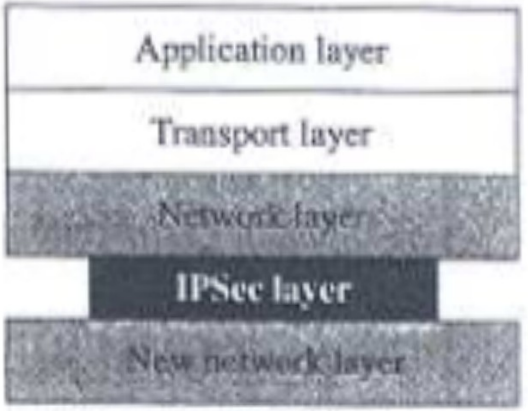
Tunnel Mode


Network layer
IP-H
IP payload
IPSec layer
Network layer
IP-H
New IP payload
New header

Transport Mode Vs Tunnel Mode



Transport Mode



Tunnel Mode