



Network II

CS 184

IPSEC

Department of Computer Science
George Washington University

Additional Resources

- Firewalls and Internet Security by Cheswick, Bellovin and Rubin.
 - Chapter 18.
- RFC 2401,2402,2406,2408

Current IP level Security

- IPSec for IPv4 and IPv6.
- Supports:
 - Secure branch office connectivity over Internet
 - Secure remote access over Internet
 - Extranet and intranet connectivity
 - Enhanced electronic commerce security

Security Association

- One way relationship between sender and receiver
- For two way, two associations are required
- Three SA identification parameters
 - IP Destination Address
 - Security Protocol Identifier
 - Specifies whether AH or ESP is being used
 - Security Parameters Index (SPI)
 - Specifies the security parameters associated with the SA

SA Parameters

- Sequence number counter
- Sequence counter overflow
- Anti-reply windows
- AH information
- ESP information
- Lifetime of this association
- IPSec protocol mode
 - Tunnel, transport or wildcard
- Path MTU

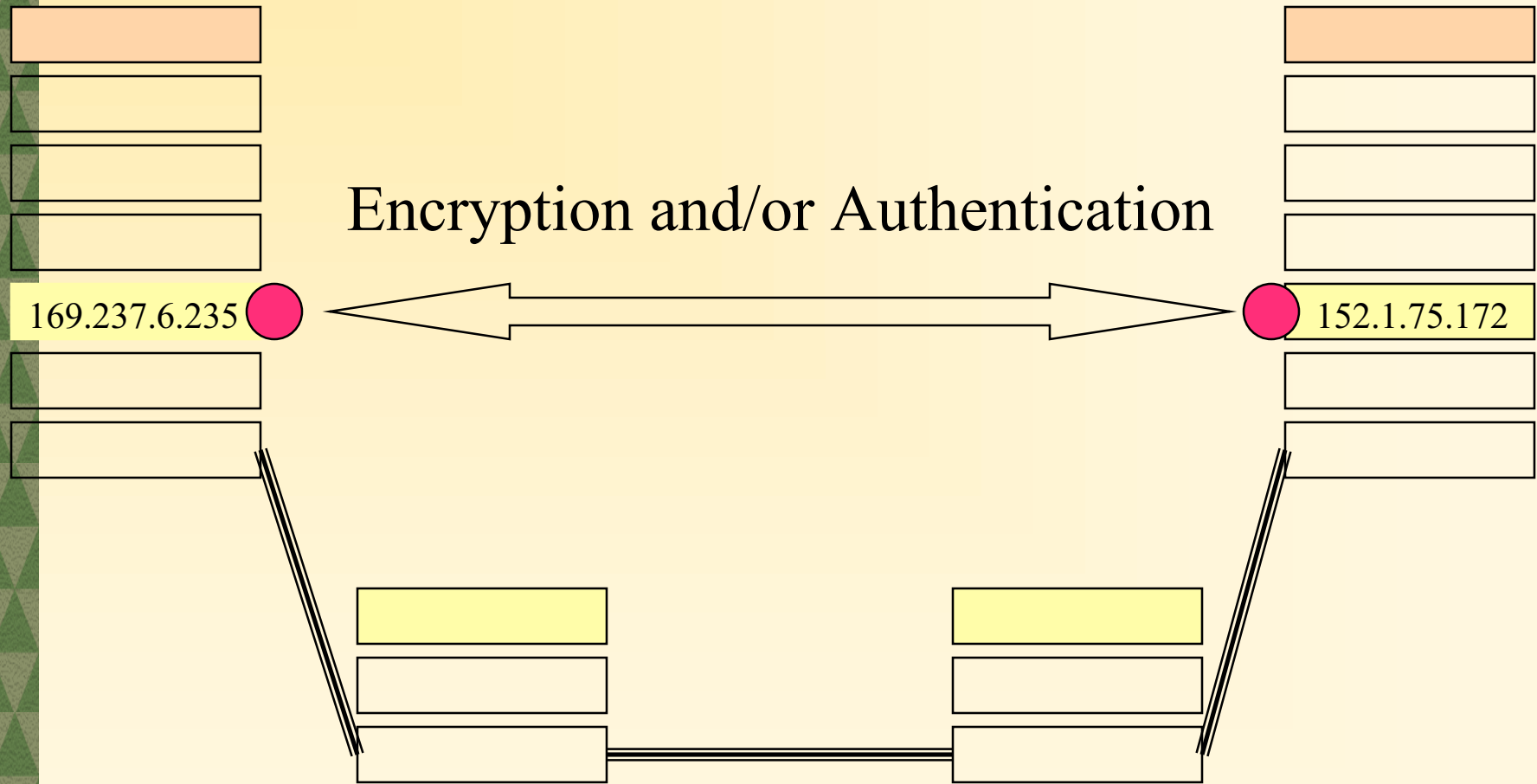
Security Association Databases

- IP needs to know the SAs that exist in order to provide security services
- Security Policy Database (SPD)
 - IPsec uses SPD to handle messages
 - For each IP packet, it decides whether an IPsec service is provided, bypassed, or if the packet is to be discarded
- Security Association Database (SAD)
 - Keeps track of the sequence number
 - AH information (keys, algorithms, lifetimes)
 - ESP information (keys, IVs, algorithms, lifetimes)
 - Lifetime of the SA
 - Protocol mode
 - MTU

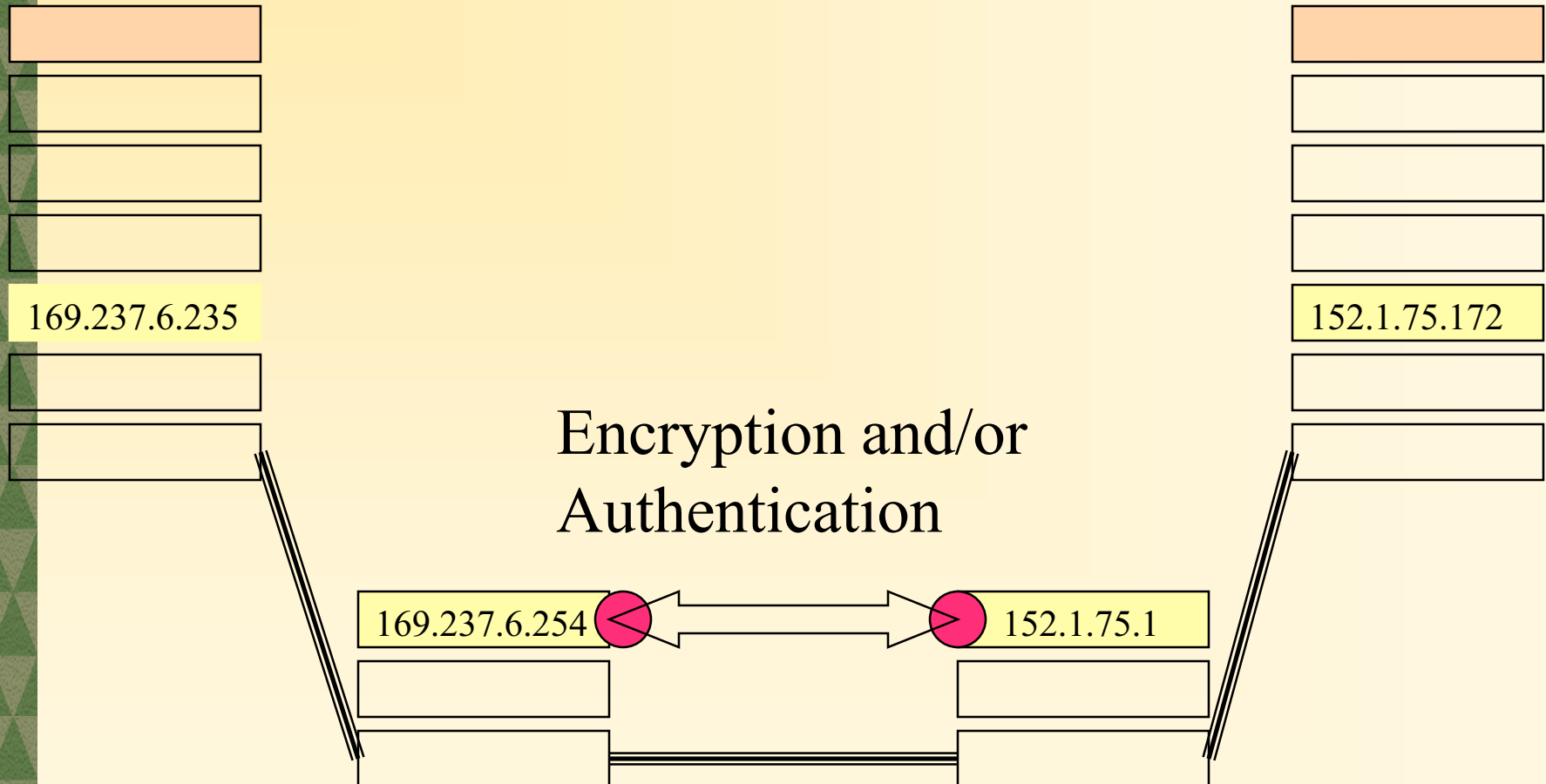
IPSec Protocols

- Authentication header (AH) protocol
 - Message integrity
 - Origin authentication
 - Anti-replay services
- Encapsulating security payload (ESP) protocol
 - Confidentiality
 - Message integrity
 - Origin authentication
 - Anti-replay services
- Internet Key Exchange (IKE)
 - Exchanging keys between entities that need to communicate over the Internet
 - What authentication methods to use, how long to use the keys, etc.

IPSEC SA: End-to-End (Transport Mode)



IPSEC SA: VPN (Tunnel Mode)

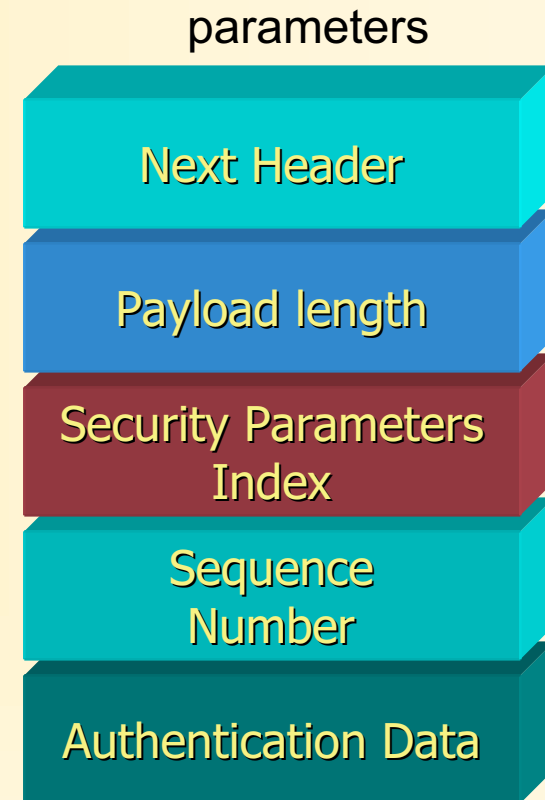


Transport and Tunnel Modes

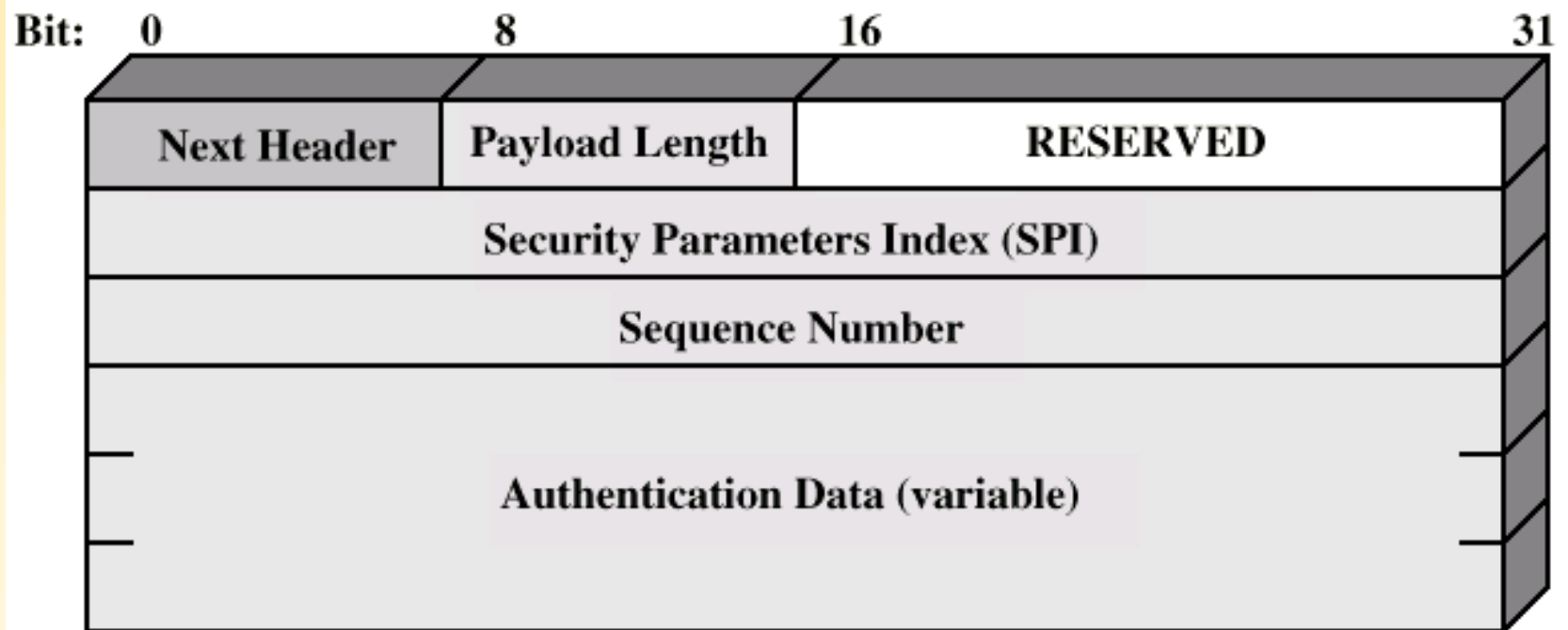
- Transport mode
 - Protection for upper layer protocols
 - Extends to payload of IP packet
 - End to end between hosts
- Tunnel mode
 - Protection for IP packet
 - Entire packet treated as payload for outer IP "packet"
 - No routers examine inner packet
 - May have different source and destination address
 - May be implemented at firewall

Authentication Header (AH)

- Next header
 - Identifies what protocol header follows
- Payload length
 - Indicates the number of 32-bit words in the authentication header
- Security Parameters Index
 - Specifies to the receiver the algorithms, type of keys, and lifetime of the keys used
- Sequence number
 - Counter that increases with each IP packet sent from the same host to the same destination and SA
- Authentication Data



Authentication Header



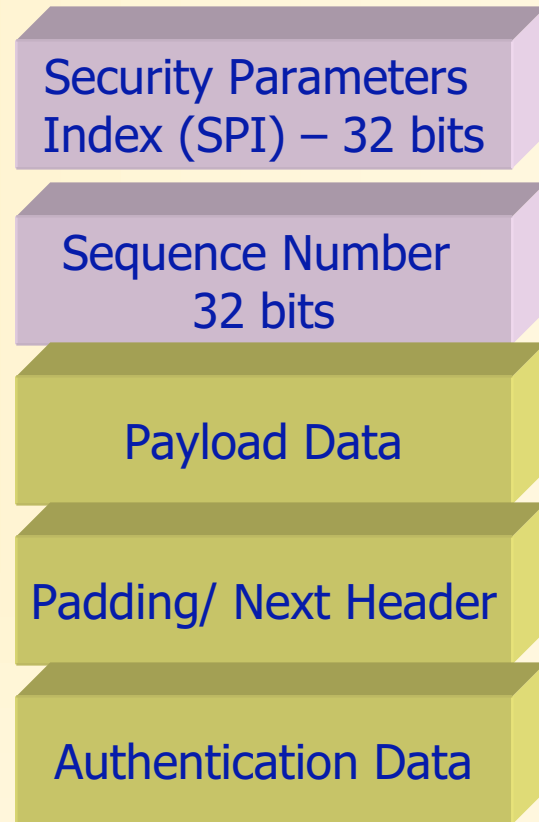
Preventing replay

- Using 32 bit sequence numbers helps detect replay of IP packets
- The sender initializes a sequence number for every SA
 - Each succeeding IP packet within a SA increments the sequence number
- Receiver implements a window size of W to keep track of authenticated packets
- Receiver checks the MAC to see if the packet is authentic

ESP - Encapsulating Security Payload

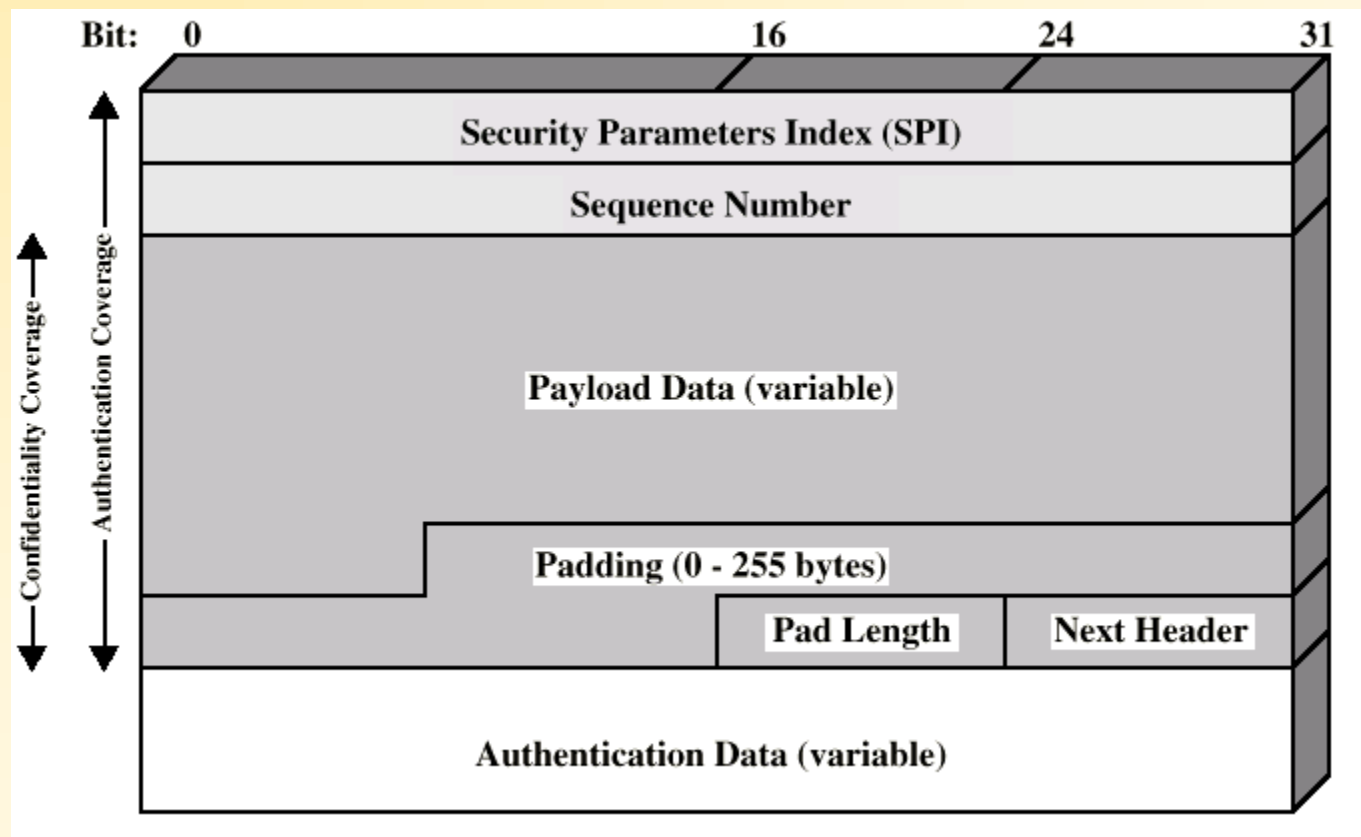
Payload

- Creates a new header in addition to the IP header
- Creates a new trailer
- Encrypts the payload data
- Authenticates the security association
- Prevents replay



Encapsulating Security Payload

- ESP
- Confidentiality services



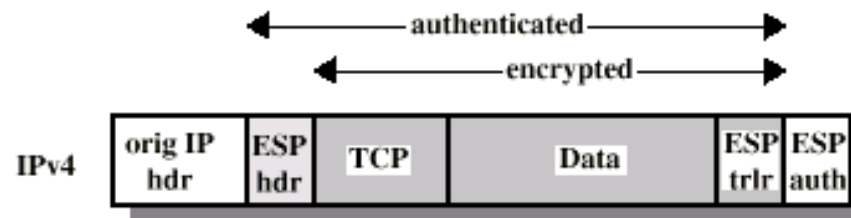
Details of ESP

- Security Parameters Index (SPI)
 - Specifies to the receiver the algorithms, type of keys, and lifetime of the keys used
- Sequence number
 - Counter that increases with each IP packet sent from the same host to the same destination and SA
- Payload
 - Application data carried in the TCP segment
- Padding
 - 0 to 255 bytes of data to enable encryption algorithms to operate properly
 - To mislead sniffers from estimating the amount of data transmitted
- Authentication Data
 - MAC created over the packet

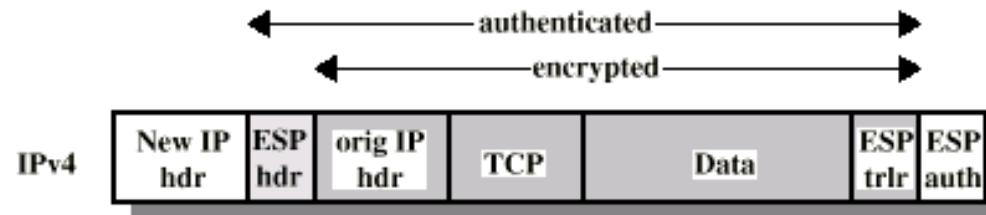
Scope of ESP



(a) Original IP Packet



(b) Transport Mode



(c) Tunnel Mode

Summary Issues

- IPSec provides network level encryption and authentication.
- Two sets of protocols for protection: AH and ESP
- One family of protocols for Key Management: IKE
- Two separate modes:
 - Transport: Host - Host
 - Tunnel: Gateway - Gateway

Homework

1. Practice with Ethereal -- it will be useful for future projects.
2. Review your notes or previous materials on Sockets programming.
3. If you have the Stevens book I recommended, I suggest you read through the Elementary TCP chapter and the beginning of the IO-Multiplexing chapter.
4. :-) Nothing to turn in, but I will ask you about it on Tuesday.

Information Slide

- Lecture slides can be obtained at the course web page
<http://www.seas.gwu.edu/~jonathan/courses/cs184>