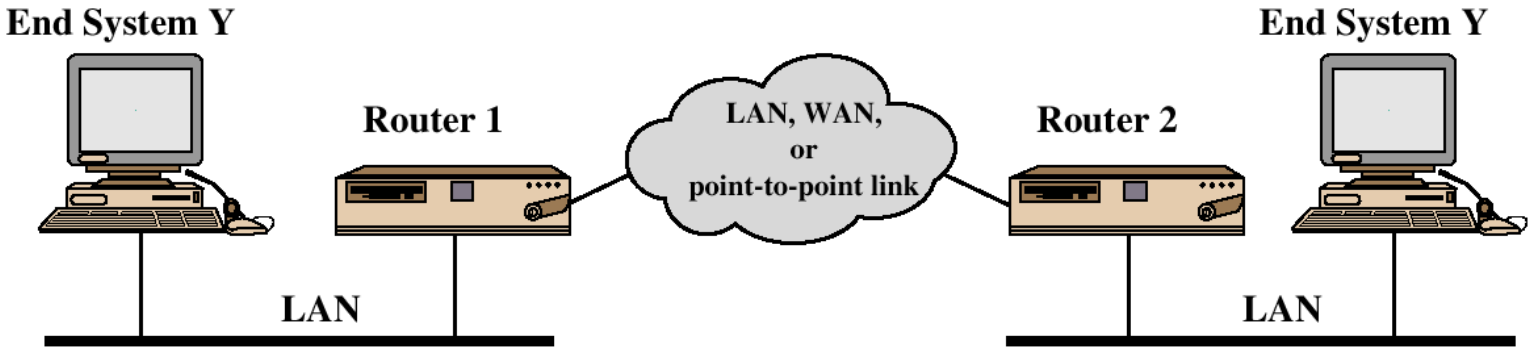
Chapter 6

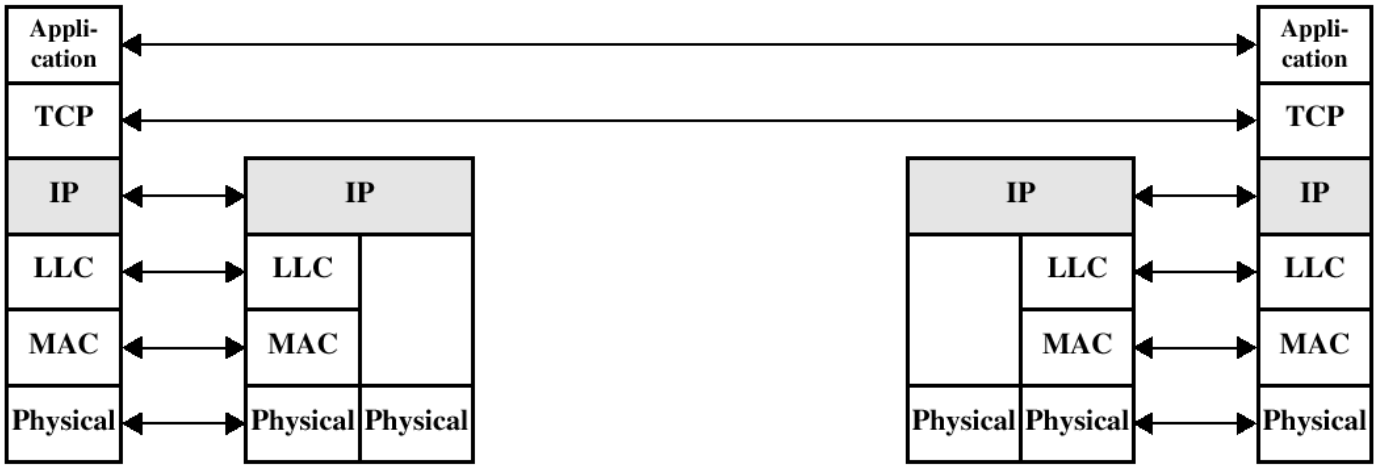
IP Security

Outline

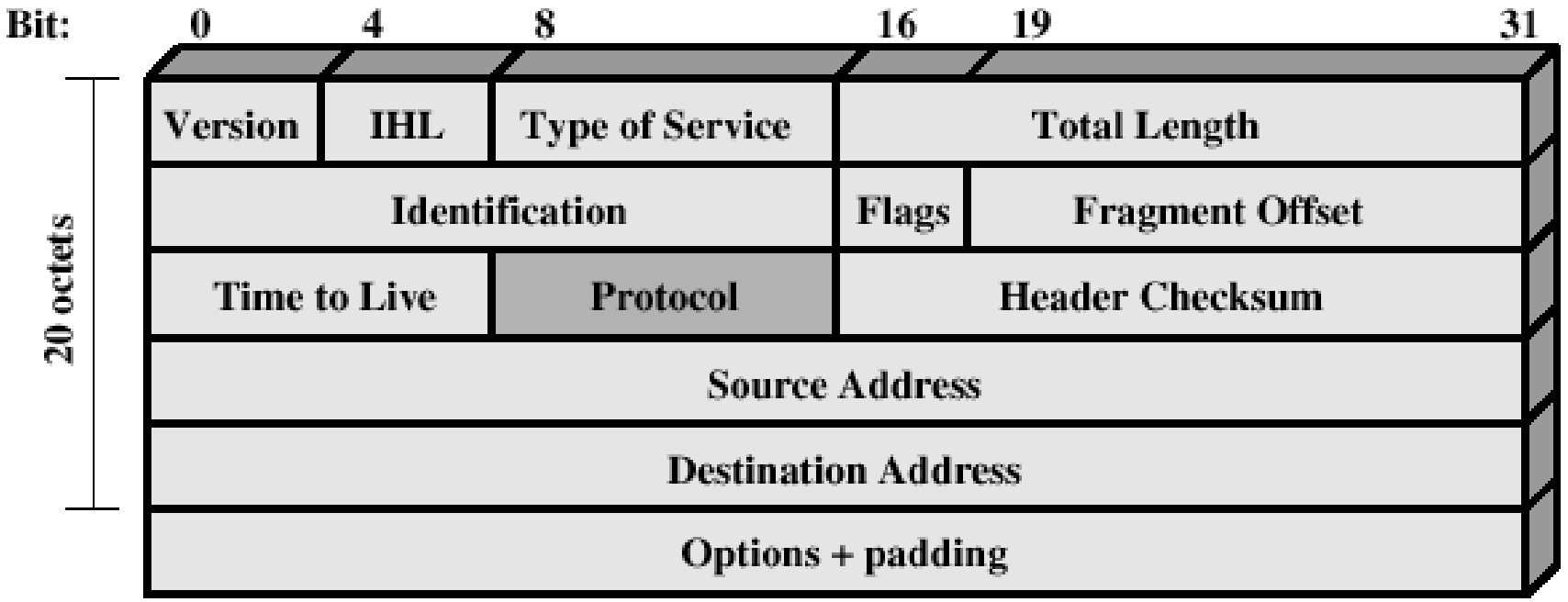
- Internetworking and Internet Protocols (Appendix 6A)
- IP Security Overview
- IP Security Architecture
- Authentication Header
- Encapsulating Security Payload
- Combinations of Security Associations
- Key Management

TCP/IP Example

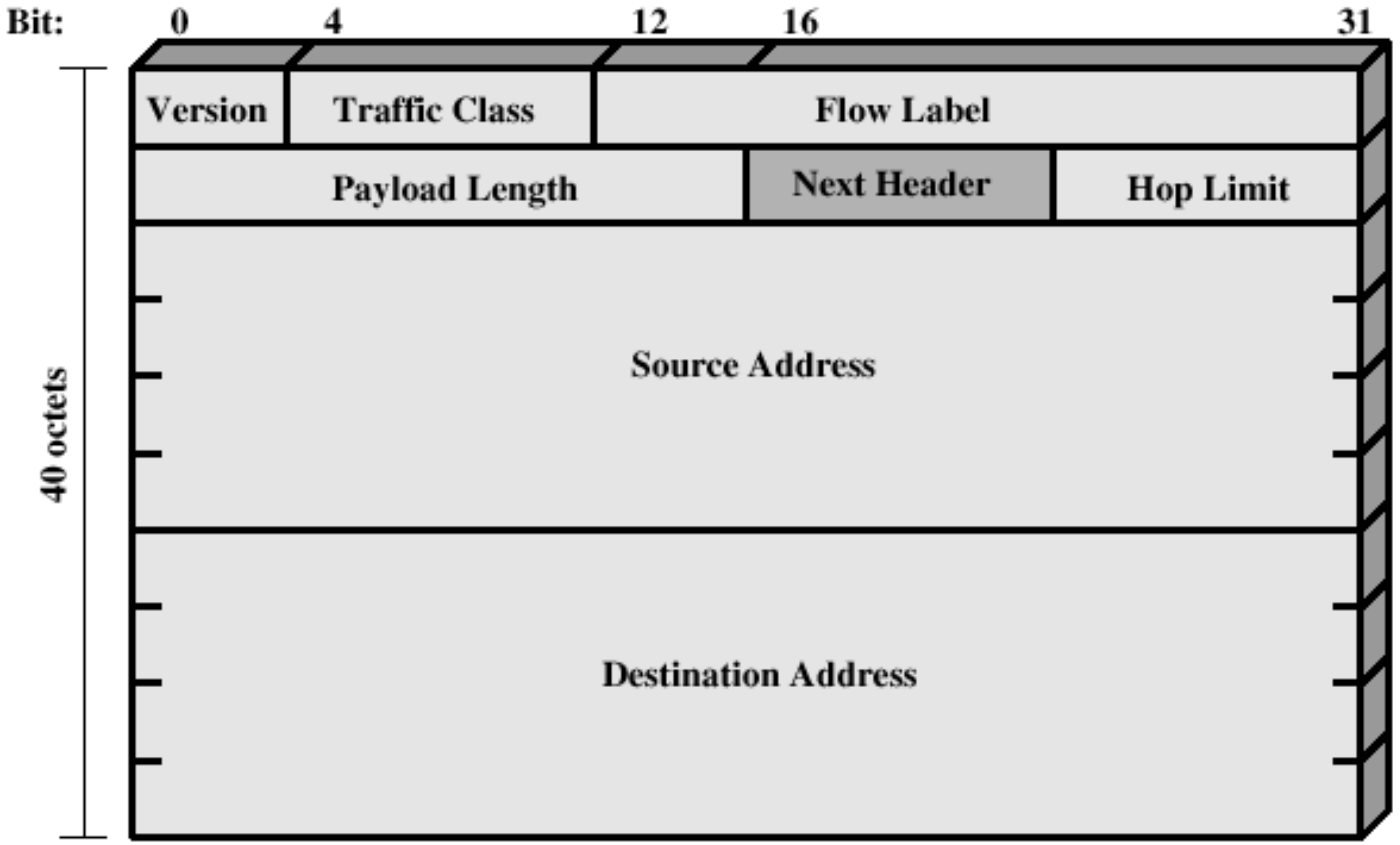




IPv4 Header


Bit:
0
4
8
16
19
31
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + padding
20 octets

IPv6 Header


Bit:
0
4
12
16
31
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
40 octets

IP Security Overview

- **IP level security encompasses three functional areas :**
  - Authentication
  - Confidentiality
  - Key Management

- **IP level security, using the above functionalities, provides secure communications on the network layer**
  - independent of applications used on the end systems with or without security mechanisms

IP Security Overview

IPSec is not a single protocol. Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.

IPsec (Internet Protocol Security) is a **Suite** of standards for security at the **Network-Layer** of network communication rather than at the Application-Layer.

IP Security Overview

- Applications of IPSec
  - Secure branch office connectivity over the Internet
  - Secure remote access over the Internet
  - Establsihing extranet and intranet connectivity with partners
  - Enhancing electronic commerce security
  - Generic modules that can be replaced
    - » Crypto algorithms
    - » Protocols
    - » Key exchange

The IETF IPsec group

- The group
  - 2 Chairs (CISCO, MIT)
  - 2 Directors (MIT, NORTEL)
  - 1 Advisor (MIT)
  - Till San Francisco Meeting , CA, March 16-21, 2003
  - After it, Till Dallas Meeting, TX, March 19-24, 2006 it was PKI4IPSEC

9

WGs in Security Area

Security Area

Area Directors:

- Stephen Farrell <stephen.farrell@cs.tcd.ie>
- Kathleen Moriarty <Kathleen.Moriarty.ietf@gmail.com>

Area Specific Web Page:

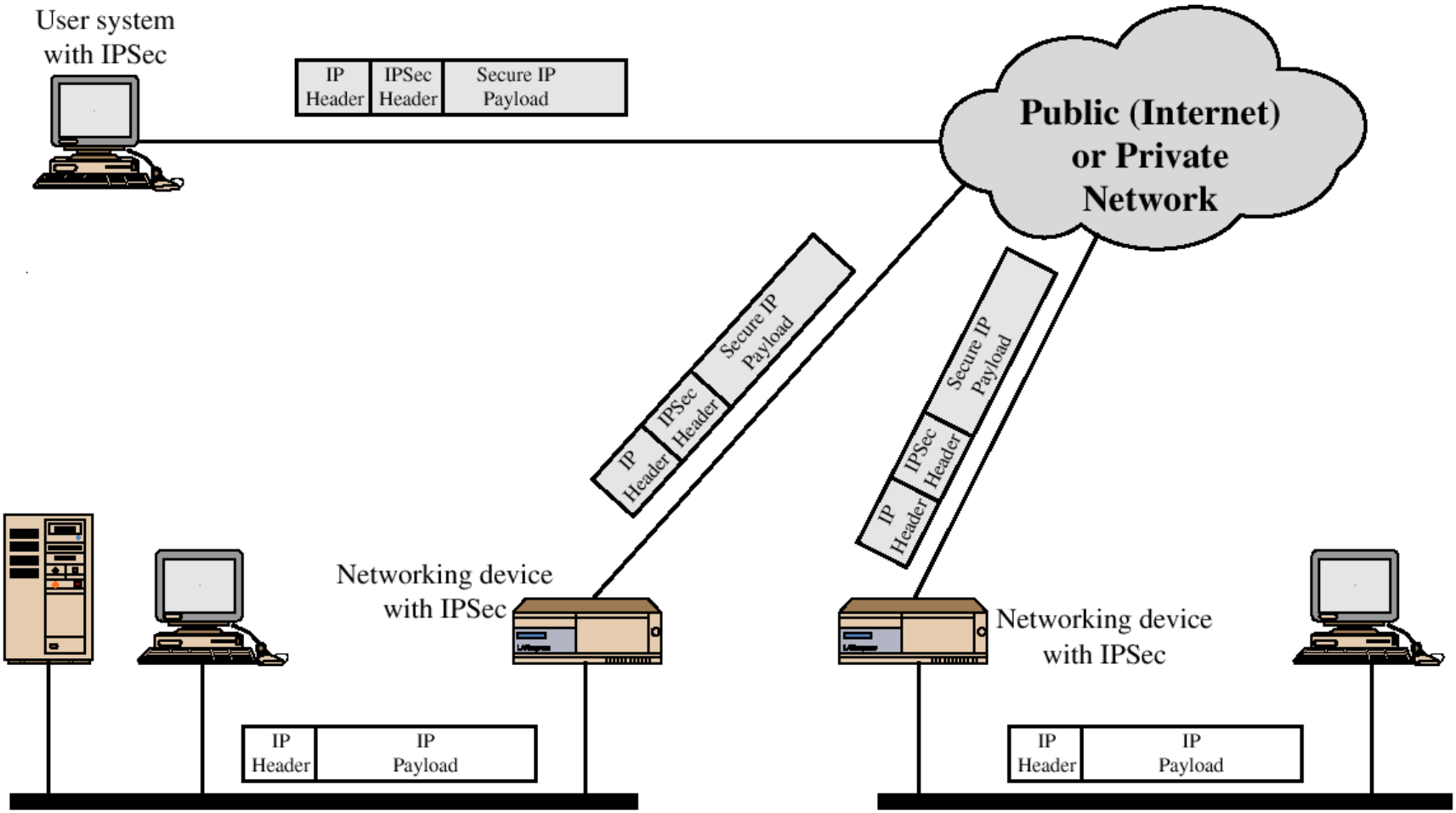
Security Area Web Page

Active Working Groups:

abfab	Application Bridging for Federated Access Beyond web	Leif Johansson, Klaas Wierenga
dane	DNS-based Authentication of Named Entities	Olafur Gudmundsson, Warren Kumari
dice	DTLS In Constrained Environments	Dorothy Gellert, Zach Shelby
emu	EAP Method Update	Alan DeKok, Joseph Salowey
httpauth	Hypertext Transfer Protocol Authentication	Matt Lepinski, Yoav Nir
ipsecme	IP Security Maintenance and Extensions	Paul Hoffman, Yaron Sheffer
jose	Javascript Object Signing and Encryption	Karen O'Donoghue, Jim Schaad
kitten	Common Authentication Technology Next Generation	Shawn Emery, Sam Hartman, Josh Howlett
mile	Managed Incident Lightweight Exchange	Alexey Melnikov, Takeshi Takahashi
nea	Network Endpoint Assessment	Stephen Hanna, Susan Thomson
oauth	Web Authorization Protocol	Derek Atkins, Hannes Tschofenig
sacm	Security Automation and Continuous Monitoring	Adam Montville, Dan Romascanu
tls	Transport Layer Security	Eric Rescorla, Joseph Salowey, Sean Turner
trans	Public Notary Transparency	Melinda Shore

10

IP Security Scenario



IP Security Overview

- Benefits of IPSec
  - When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter
  - IP 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
  - IPsec is below transport layer (TCP, UDP) and transparent to applications: no need to change applications
  - IPsec can be transparent to end users
  - Provide security for individual users: for offsite workers and for setting up a secure virtual subnetwork

Routing Applications

- IPSec can assure that:
  - A router or neighbor advertisement comes from an authorized router
  - A redirect message comes from the router to which the initial packet was sent
  - A routing update is not forged
- Routing protocol such as OSPF should be run on top of security associations between routers that are defined by IPsec

IP Security Architecture

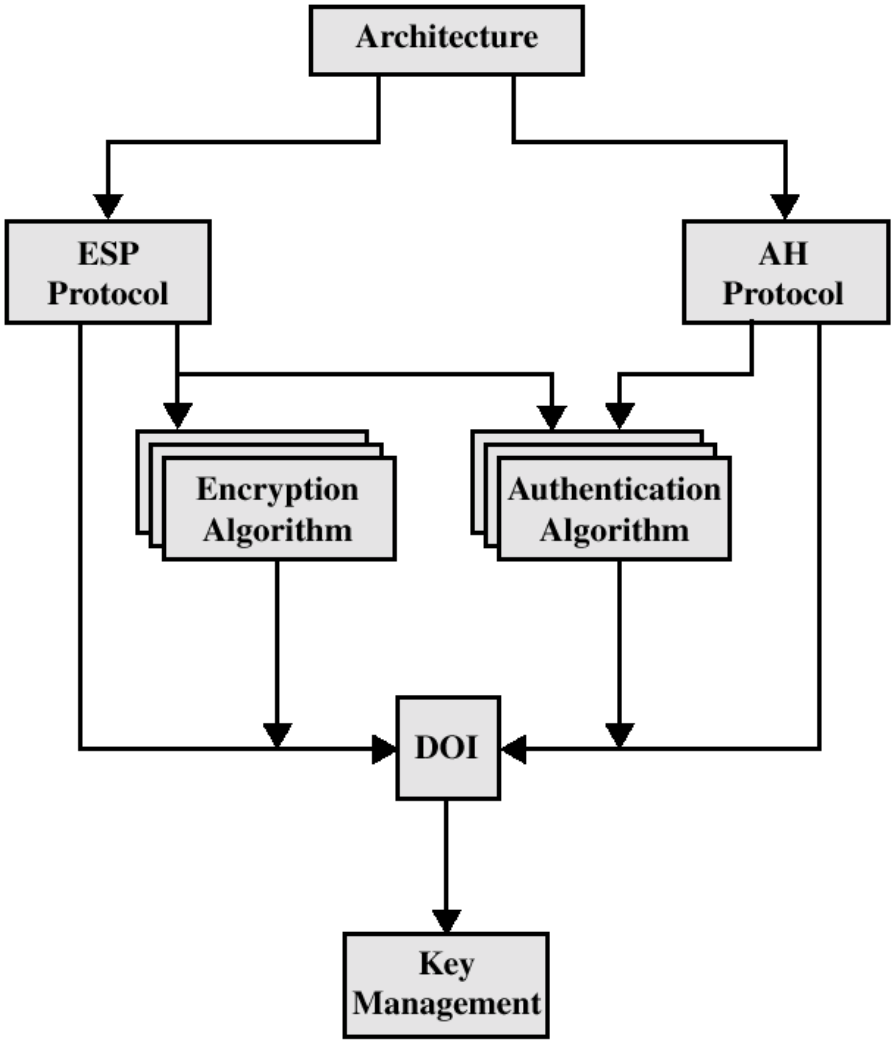
- IPSec documents:
  - RFC 2401: An overview of security architecture
  - RFC 2402: Description of a packet encryption extension to IPv4 and IPv6
  - RFC 2406: Description of a packet encryption extension to IPv4 and IPv6
  - RFC 2408: Specification of key managament capabilities

IP Security Architecture

- **Support for IPsec features is :**
  - mandatory for IPv6
  - optional for IPv4

- **The security features are implemented as extension headers :**
  - Authentication : Authentication Header (AH)
  - Encryption : Encapsulating Security Payload(ESP) header

IPSec Document Overview



IPSec Services

- Access Control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
- Confidentiality (encryption)
- Limited traffic flow confidentiallity

IPsec Services

	AH	ESP (encryption only)	ESP (encryption and authentication)
integrity	✓		✓
data origin authentication	✓		✓
replay detection	✓	✓	✓
confidentiality		✓	✓
limited traffic flow confidentiality		✓	✓

Security Associations (SA)

- A one way relationsship between a sender and a receiver.
- Identified by three parameters:
  - Security Parameter Index (SPI)
  - IP Destination address
  - Security Protocol Identifier : whether AH or ESP

SA parameters

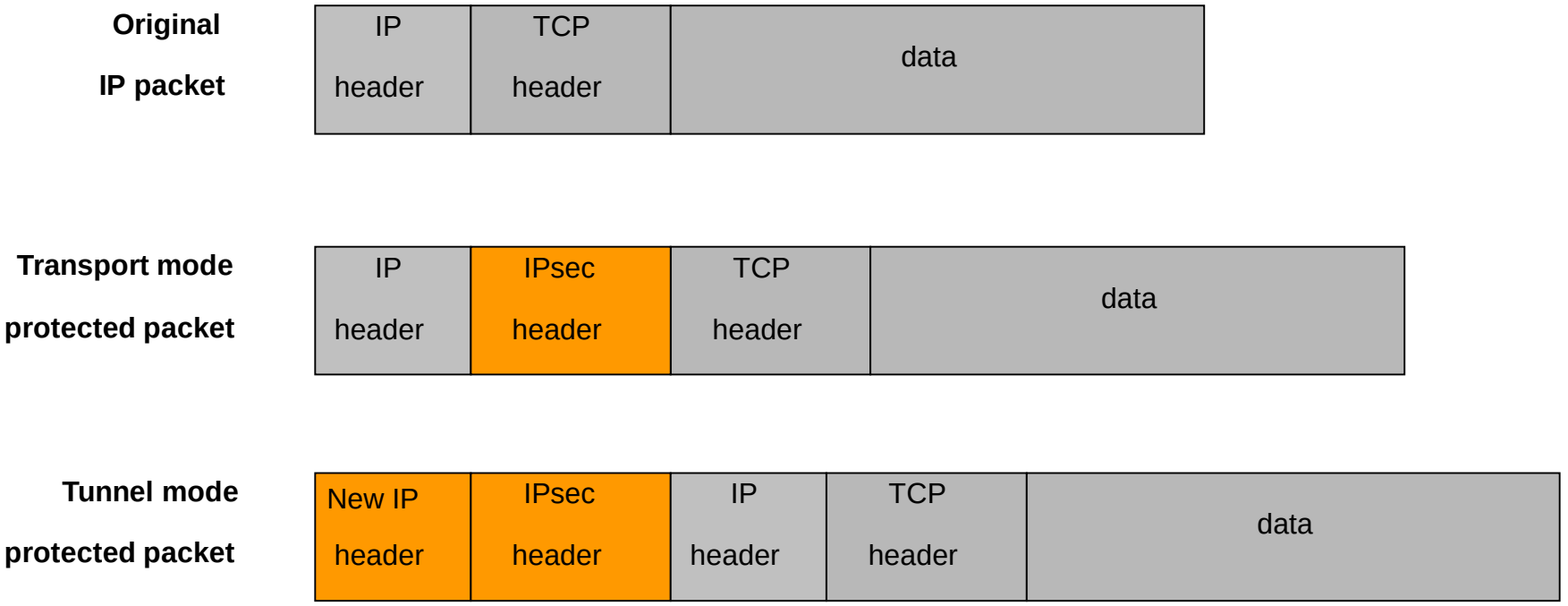
- Sequence number counter: 32 bit value used to generate the Sequence Number field in AH or ESP headers
- Sequence Counter Overflows
- Anti-Replay Window: used whether an inbound AH or ESP packet is a replay
- AH Information: authentication algorithm, keys, key lifetimes, related parameters being used with AH

SA parameters

- ESP Information: authentication algorithm, keys, key lifetimes, related parameters being used with ESP
- Lifetime of this security association
- IPsec protocol mode: tunnel, transport, or wildcard
- Path MTU

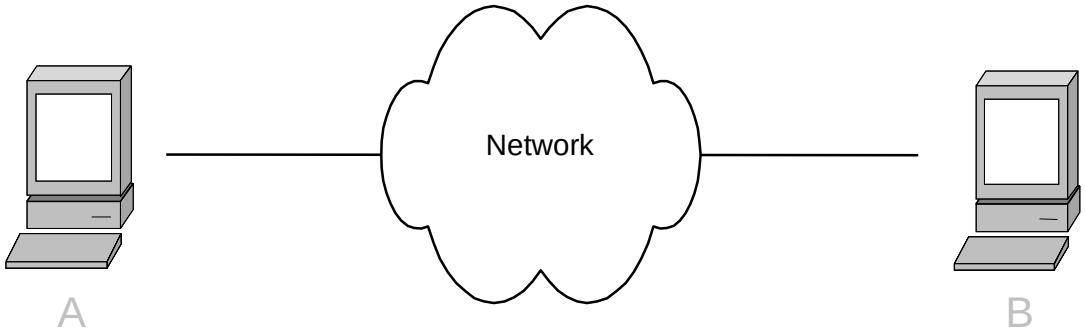
Transport and Tunnel Modes

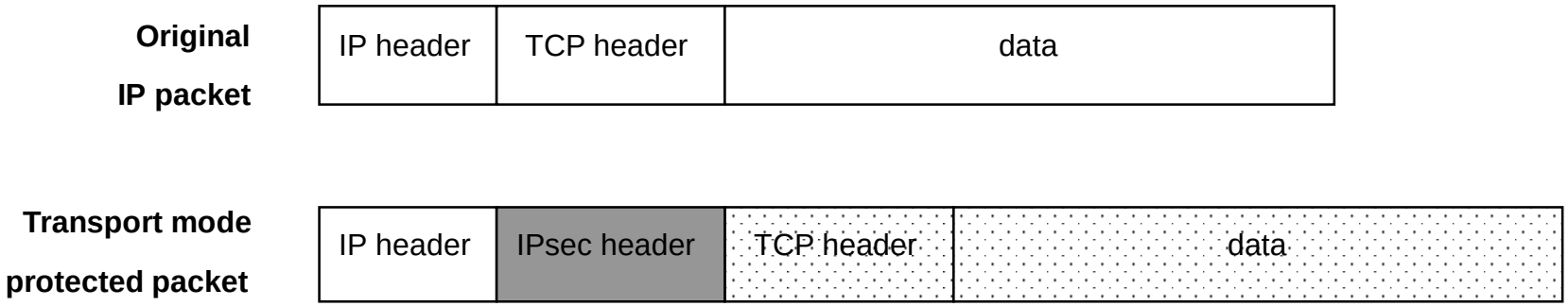
- Both AH and ESP support two modes of use for IP-Packet transmissions
- Packet formats for the modes



Transport mode

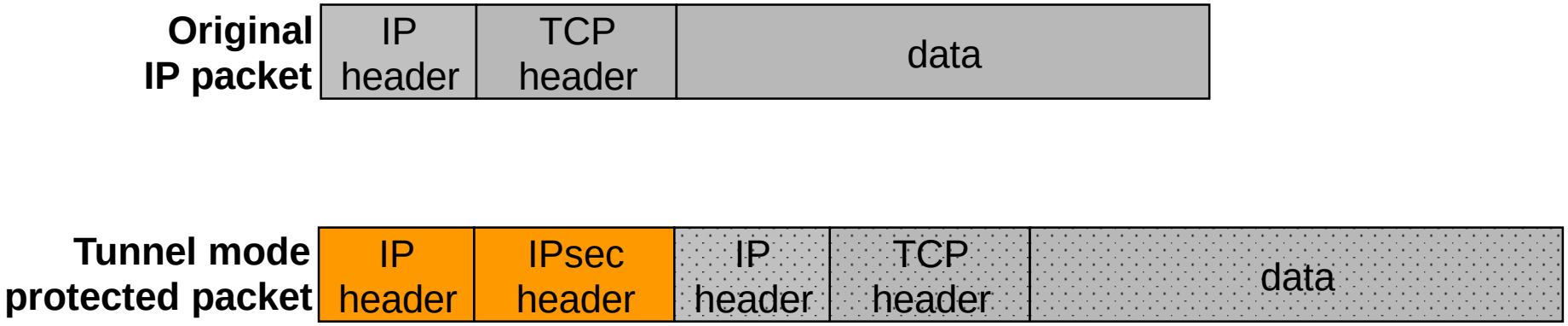
- Intercept Network layer packets
  Encrypt / Authenticate these packets
  preserving most of the original IP header





Tunnel mode

- Intercept Network layer packets
  Encrypt / Authenticate these packets, while encapsulating the whole original IP packet



An Example of Tunnel Mode

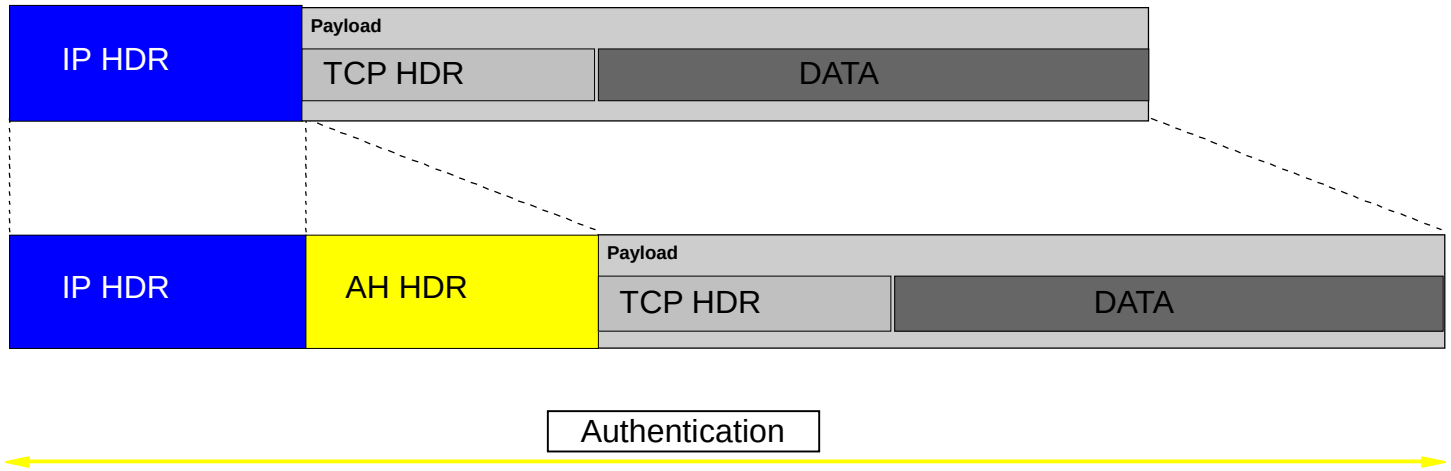
- **Host A on a network generates a IP packet for host B on another network**
- **The packet is routed from Host A to Firewall A**
  - The firewall A performs IPsec processing on the packet
  - The source address of outer header is firewall A
  - The destination address may be firewall B
- **The packet is routed from firewall A to firewall B**
  - Intermediate routers examine only the outer IP header
  - Firewall B strips the outer IP header and delivers it to B

Tunnel/Transport Mode Functionality

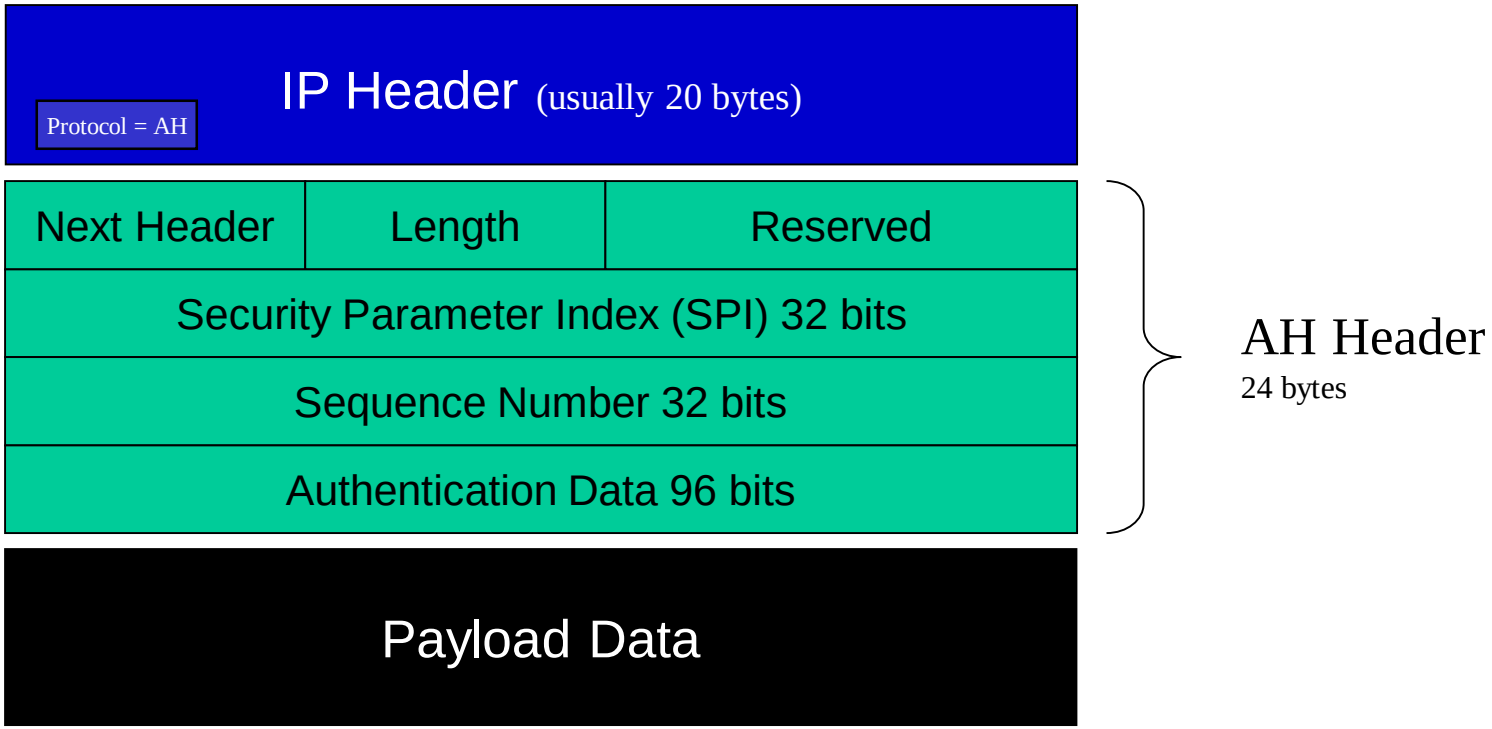
	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload and any IPv6 extesion header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extesion header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet.

IPsec Auth. Header

- **AH protocol is applied to AH for data integrity and authentication**
- **Authentication is based on the use of a MAC**
  - The two parties must share a secret key



IPsec Auth. Header

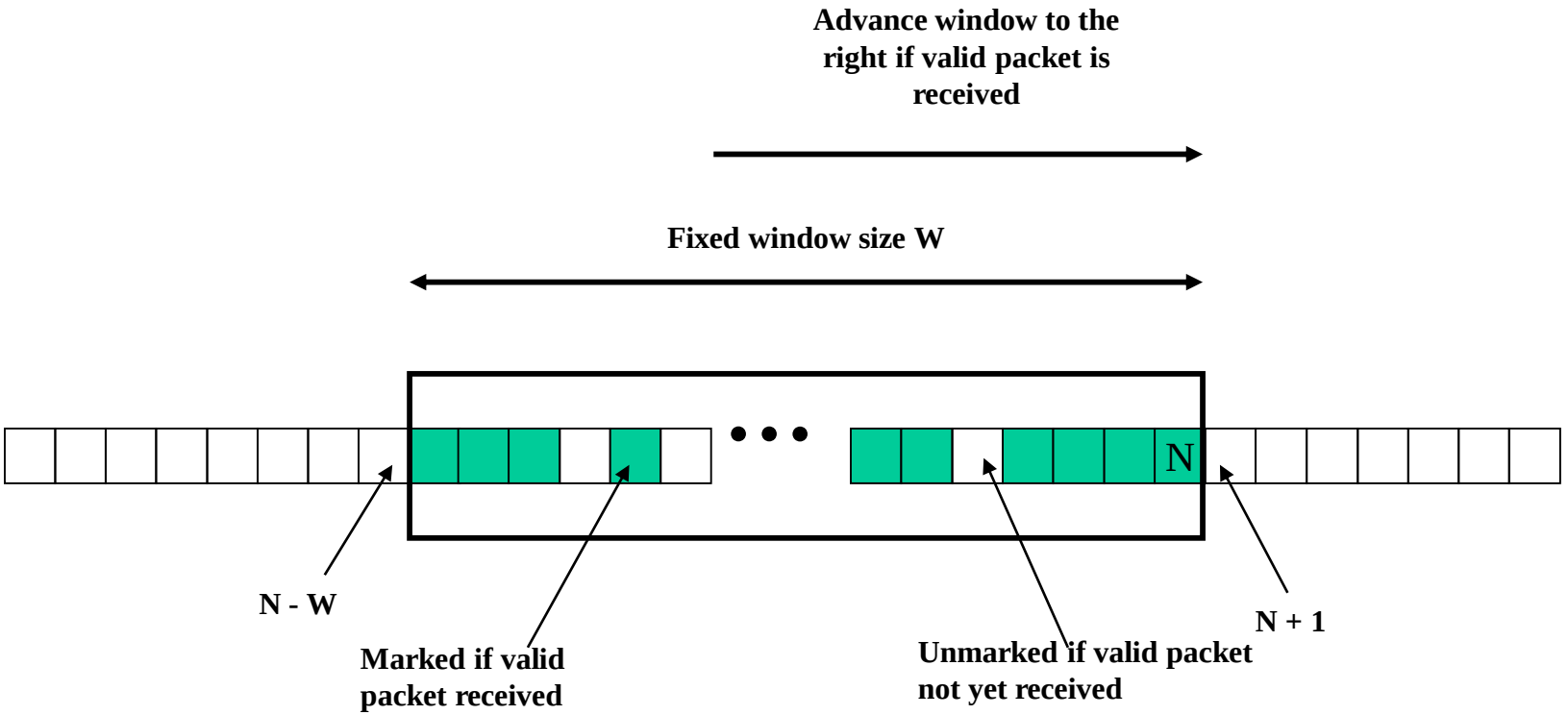


Next header: TCP, UDP etc.
Sequence number: Start at 1, never recycle (optional)

Anti-Replay Service

- **The sequence number field is used to thwart the replay attack.**
  - The sequence number is set to zero with a new SA established
  - The number is incremented by 1 for each packet sent on the SA
  - The SA is terminated or negotiated with a new key if $N = 2^{32} - 1$
- **A window of size W is implemented in order for IP packets to be delivered in reliable manner (with a default of W=64)**

Anti-Replay Service



Antireplay Mechanism

Integrity Check Value (ICV)

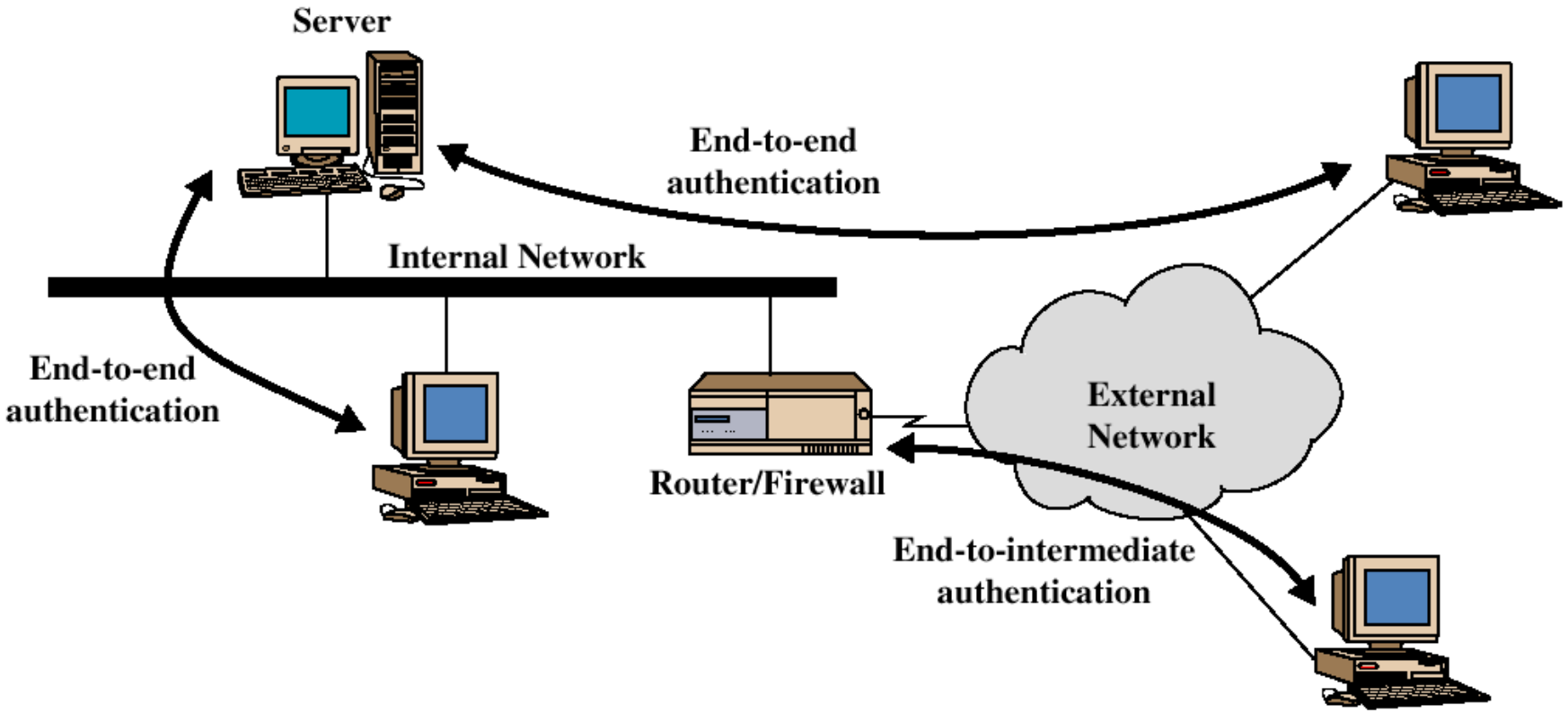
- **The Authentication Data field holds the ICV**
- **The ICV is a truncated version of a MAC produced by HMAC**
  - **HMAC-MD5-96**
  - **HMAC-SHA-1-96**
- **The first 96 bits of the MAC is the default length for the field**
- **The MAC is calculated over**
  - **IP header fields to be immutable in transit or to be predictable in value on arrival**
  - **The AH header other than the Authentication Data field (set to zero)**
  - **The entire upper-level protocol data (e.g. a TCP segment)**

※ Others are set to zero for the purposes of calculation

Integrity Check Value (ICV)

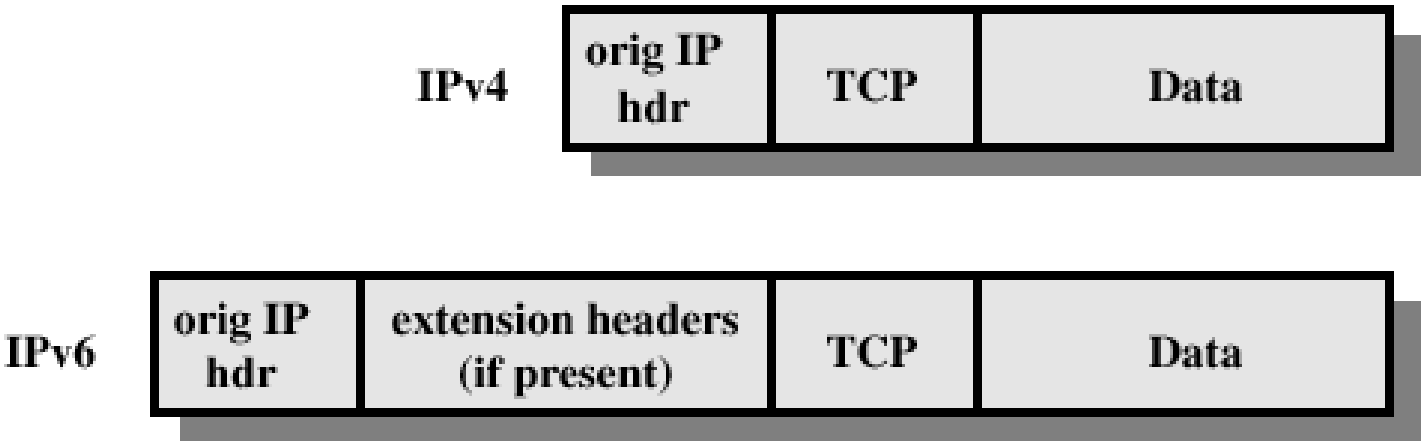
- **Examples of immutable fields**
  - **Internet Header Length and Source Address**
- **Example of mutable but predictable field**
  - **Destination Address (with loose or strict source routing)**
- **Examples of mutable fields**
  - **Time to LIVE and Header Checksum fields**

Transport and Tunnel Modes

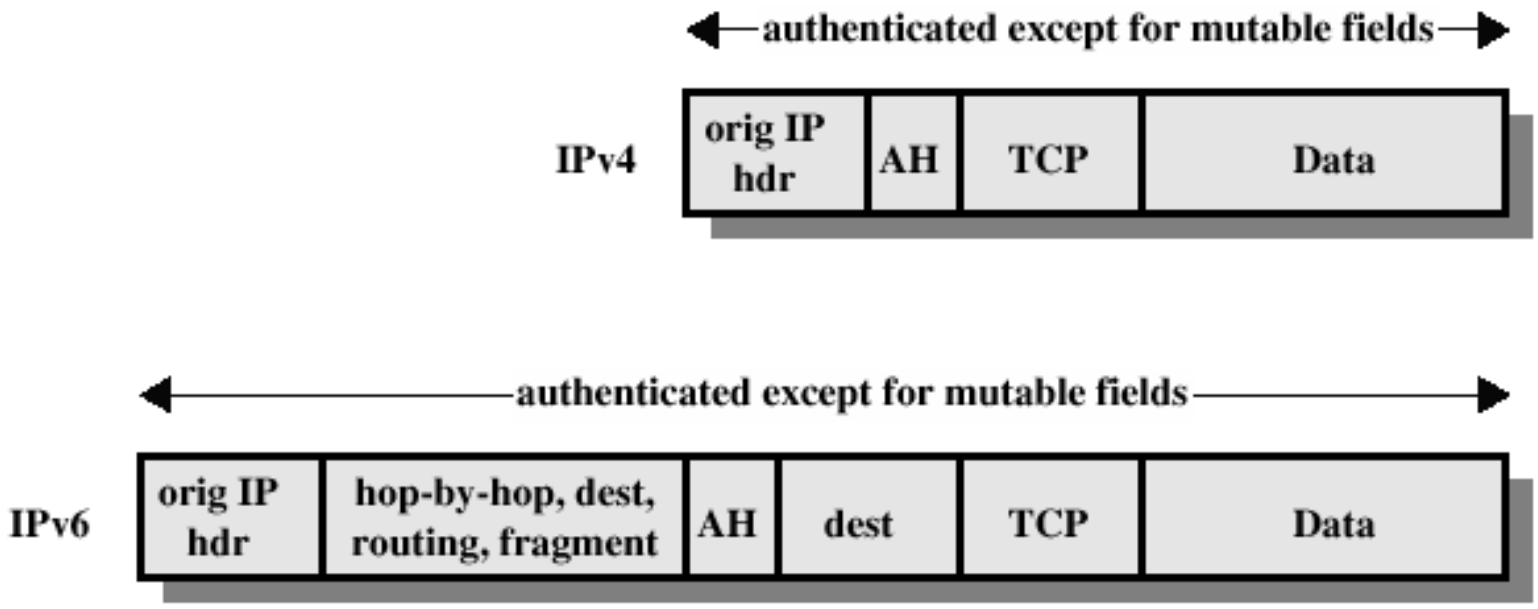


- **Transport mode : end-to-end authentication**
- **Tunnel mode : end-to-intermediate authentication**

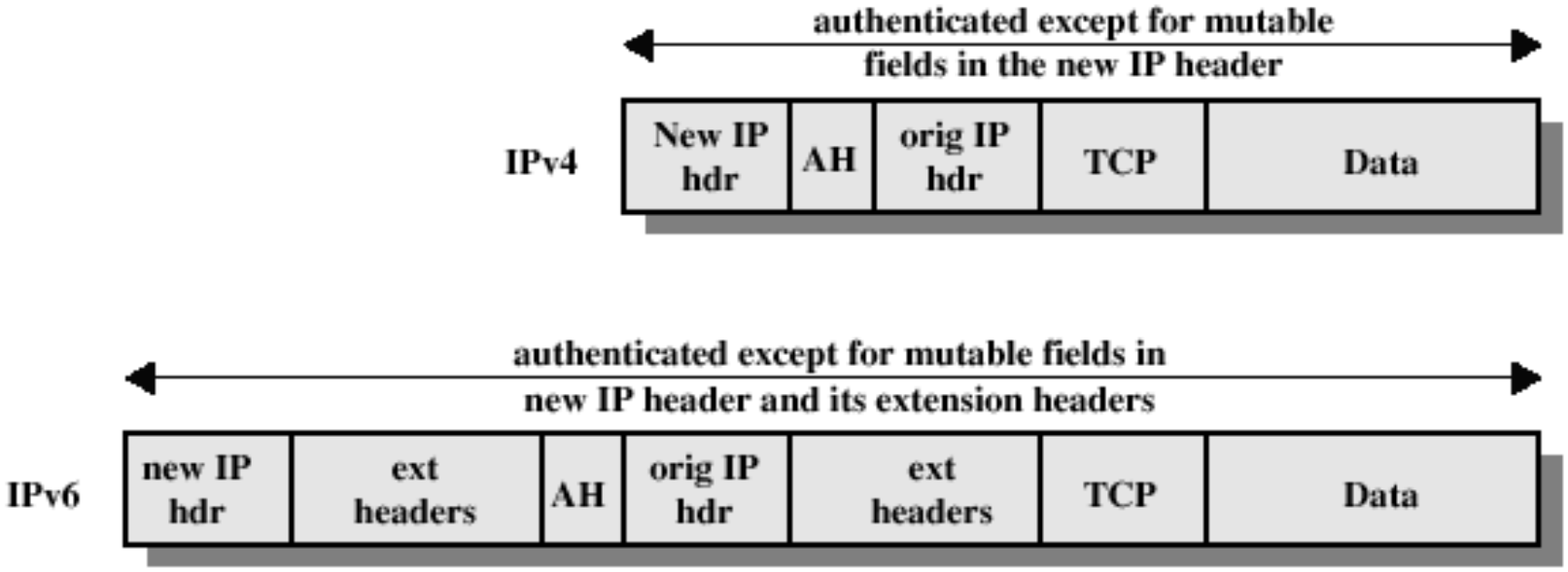
Before Applying AH



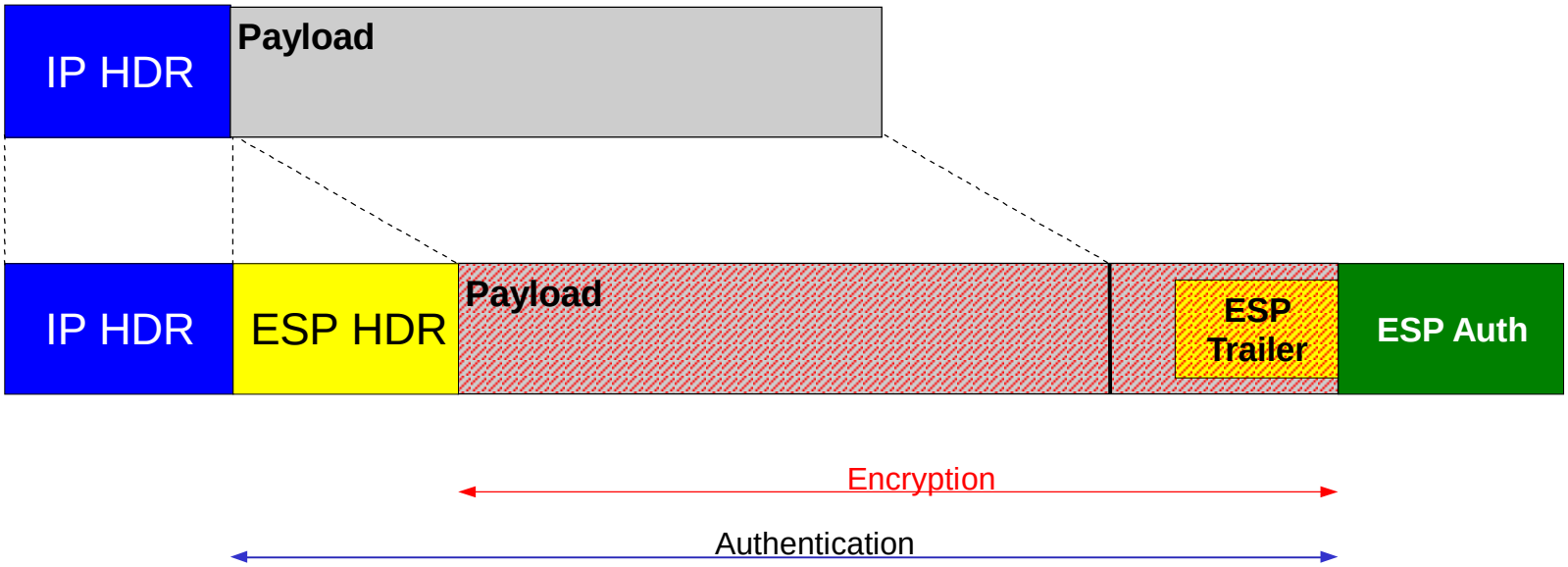
Transport Mode (AH)



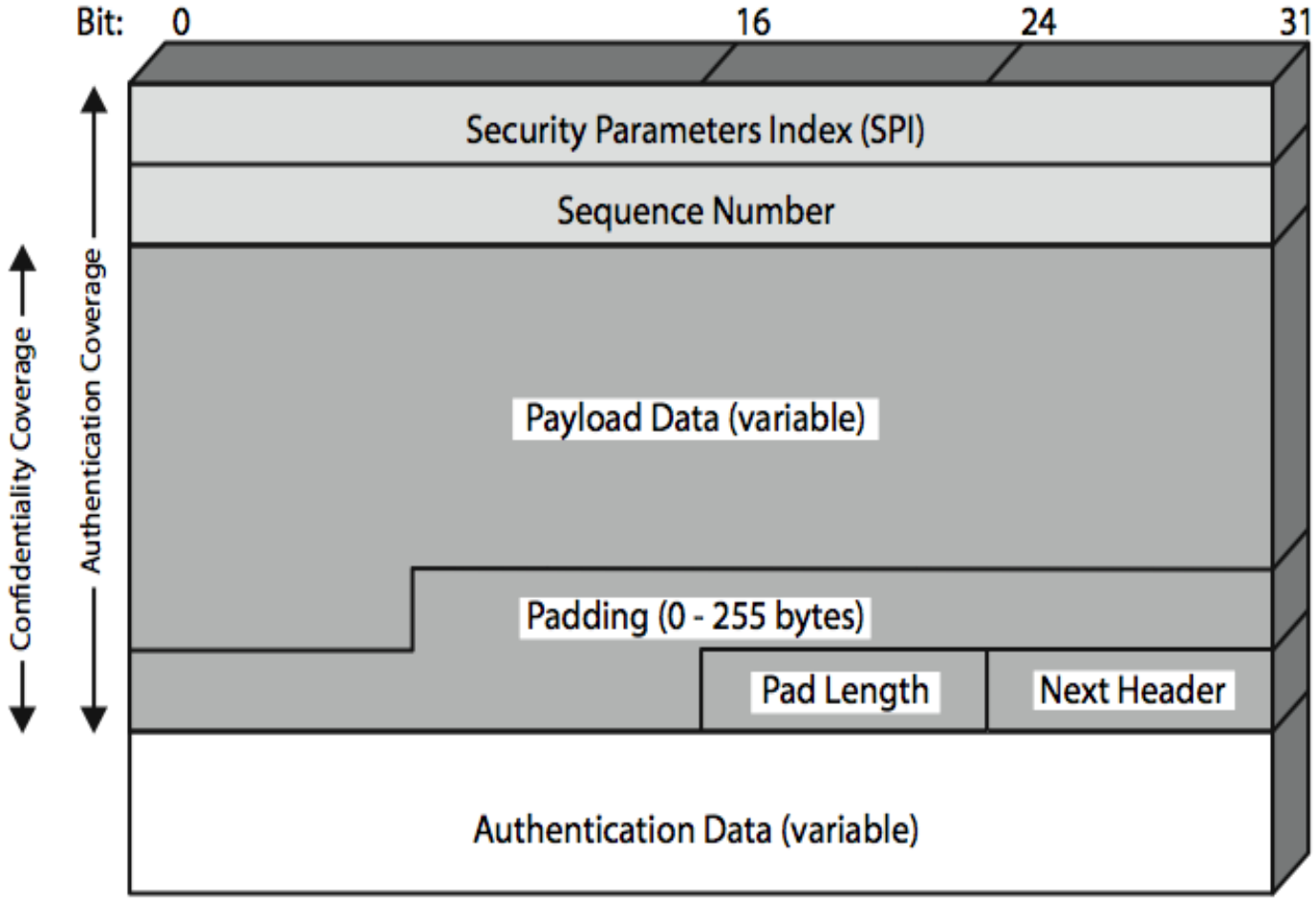
Tunnel Mode (AH)



IPsec ESP Header



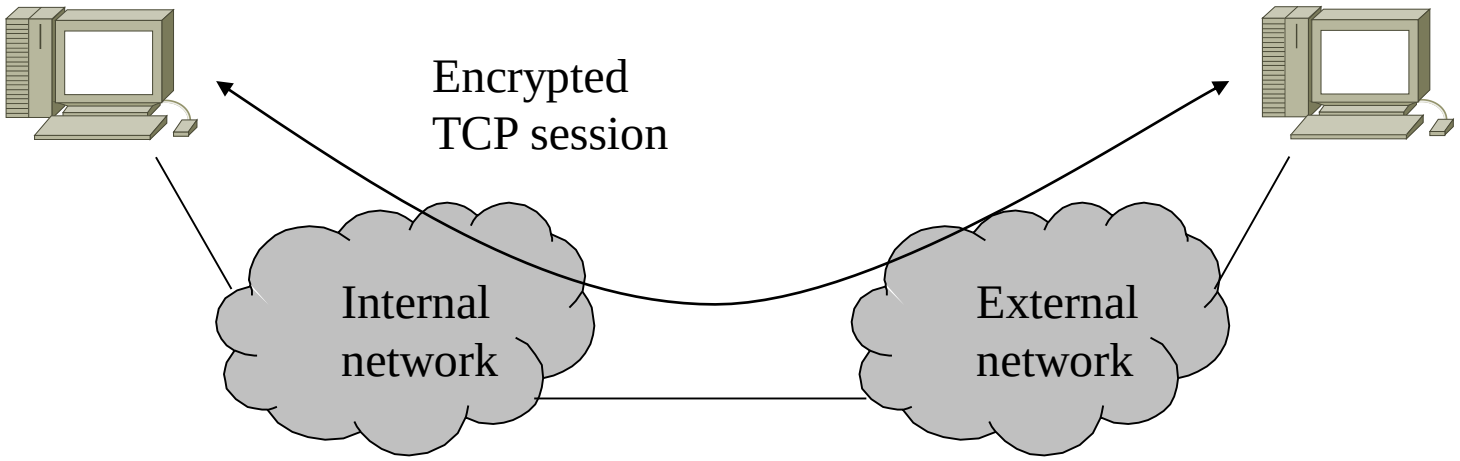
IPsec ESP format



Encryption and Authentication Algorithms

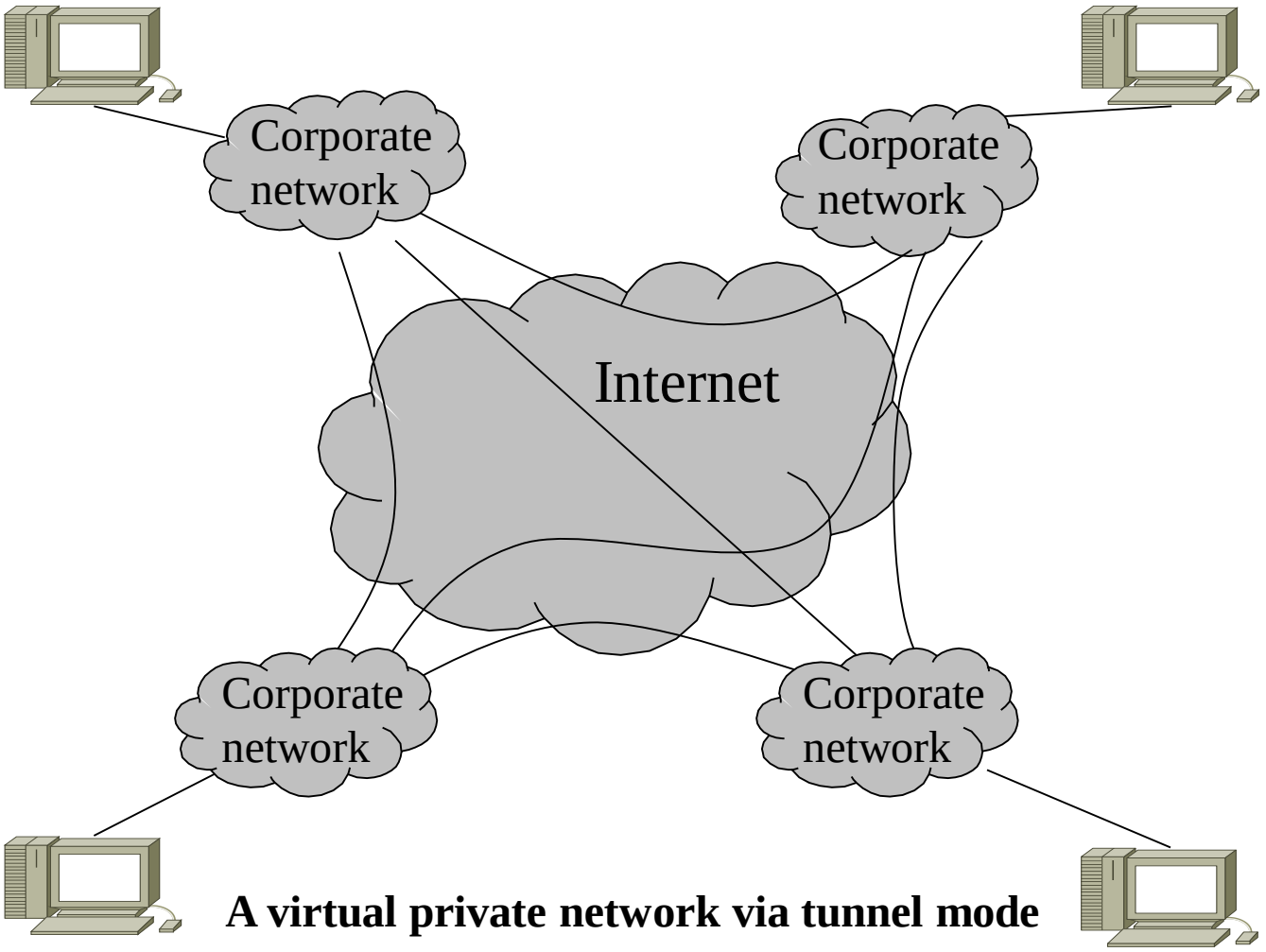
- Encryption:
  - Three-key triple DES
  - RC5
  - IDEA
  - Three-key triple IDEA
  - CAST
  - Blowfish
- Authentication:
  - HMAC-MD5-96
  - HMAC-SHA-1-96

Transport and Tunnel Modes (ESP)



Transport-level security, using a transport mode SA

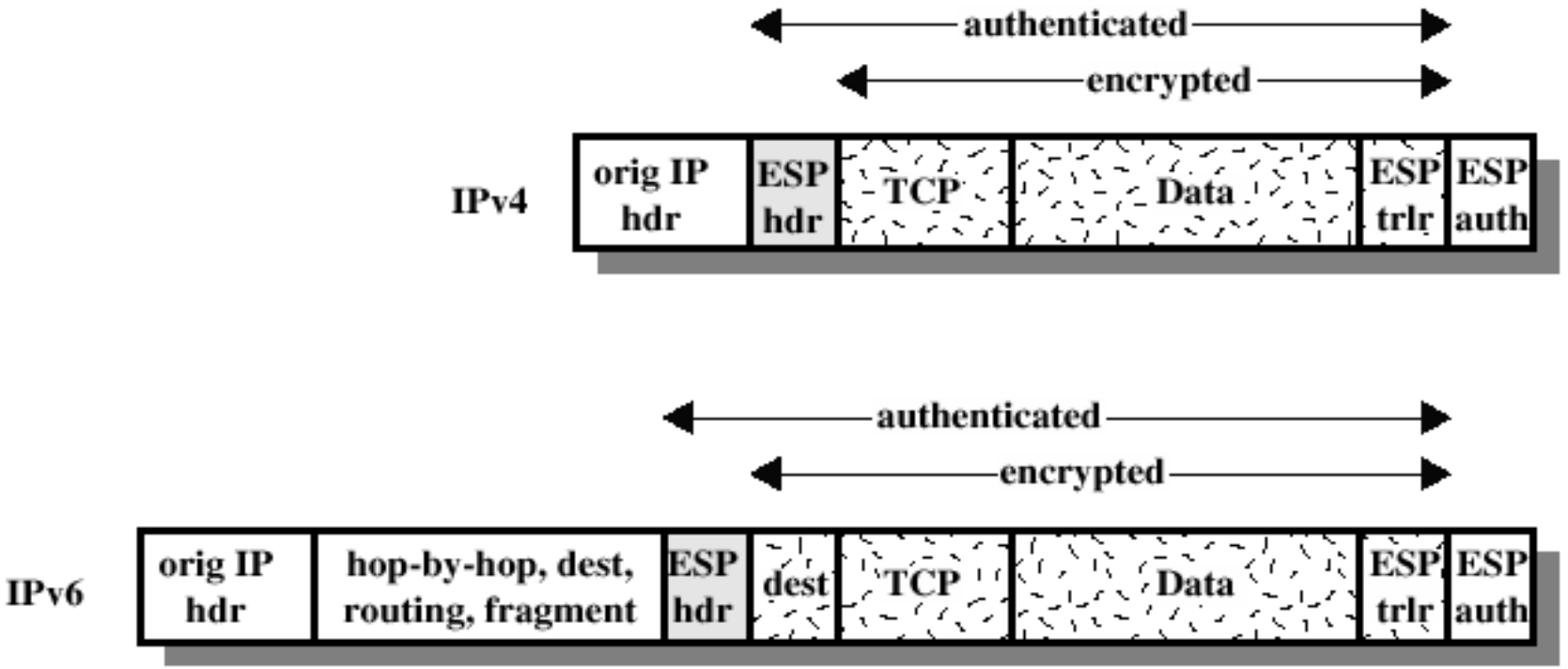
Transport and Tunnel Modes (ESP)



A virtual private network via tunnel mode

Transport Mode ESP

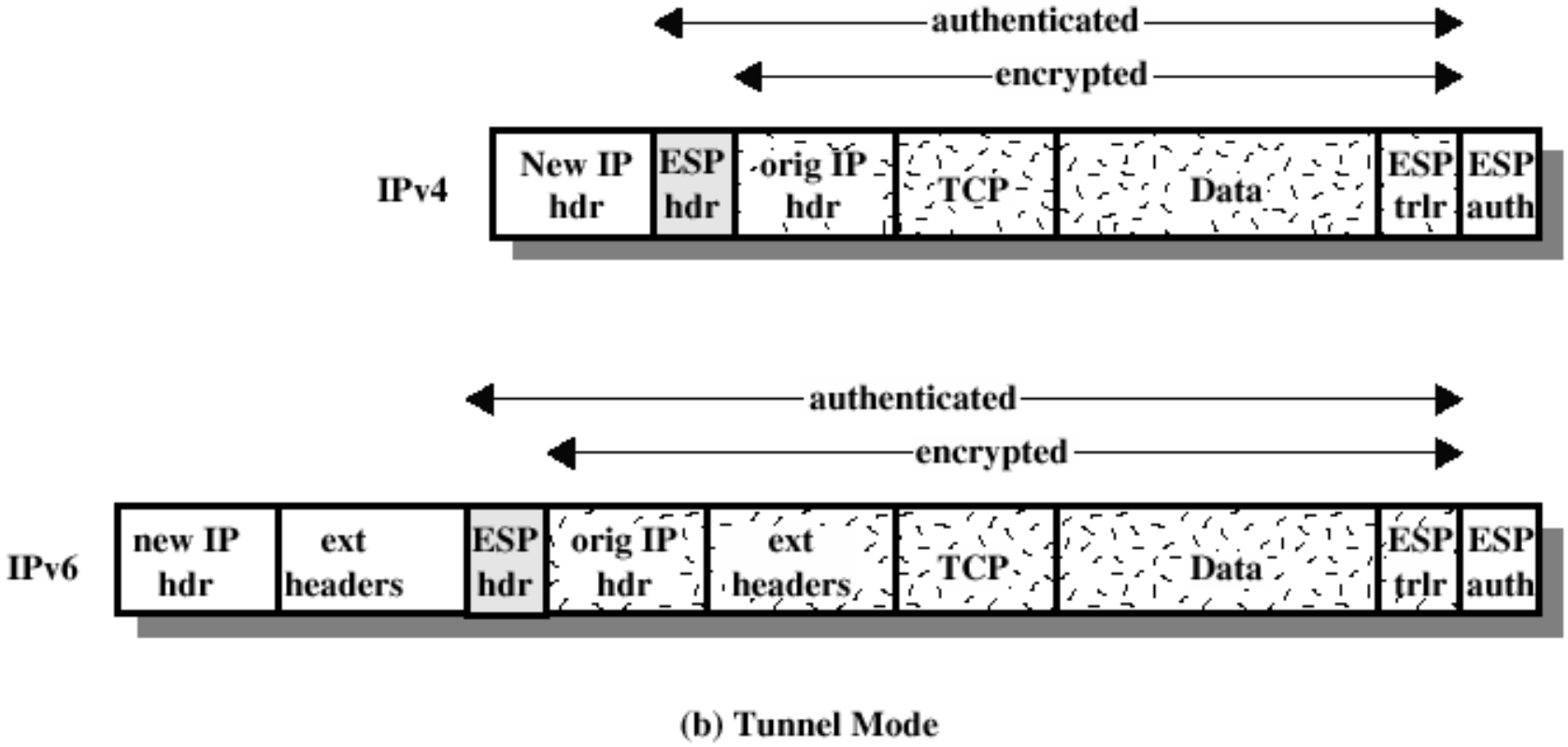
- Used to encrypt/authenticate(optionally) the IP payload
- No need to implement confidentiality in every appl.
- Possibility of traffic analysis as one drawback



(a) Transport Mode

Tunnel Mode ESP

- **Used to encrypt an entire IP packet**
- **Used to encounter traffic analysis**



(b) Tunnel Mode

Combining Security Association

- An SA can implement either the AH or ESP protocol but not both
- A particular traffic may call for the both services from AH and ESP
  - IPsec services between hosts,
  - For the same flow, separate services between security gateways
- Multiple SAs must be employed to achieve the desired IPsec services
- The two ways for the SAs to be combined into bundles :
  - Transport adjacency : refers to applying more than one security protocol without invoking tunneling
  - Iterated tunneling : refers to the application of multiple layers of security protocols effected through IP tunneling
- The two approaches can be combined by applying a transport SA b/w hosts through a tunnel SA b/w security gateways

Authentication Plus Confidentiality

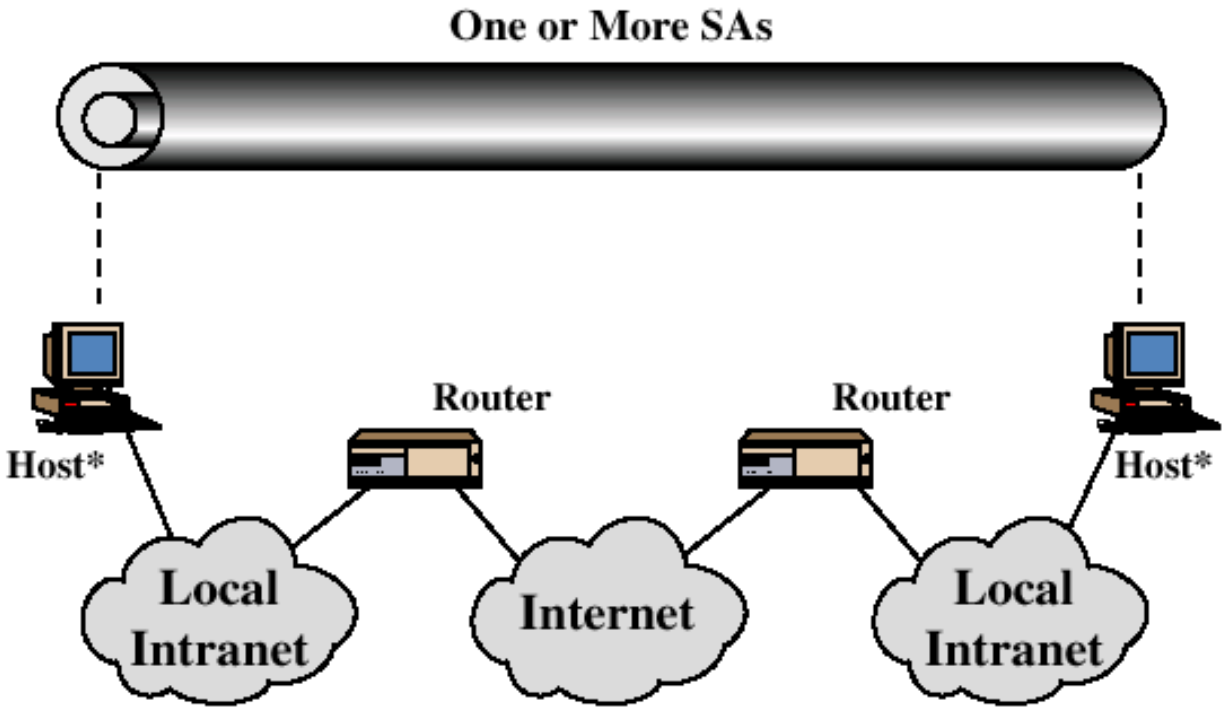
1. ESP with Autentication Options : In this approach, the user first applies ESP, then appends the auth. data field.

2. Transport Adjacency : Use of two bundled transport SAs with the inner being an ESP SA and the outer being an AH SA

3. Transport-Tunnel Bundle : The use of authentication. prior to encryption

- The auth. Data is protected
- The plain message is stored with its auth. info. for late reference

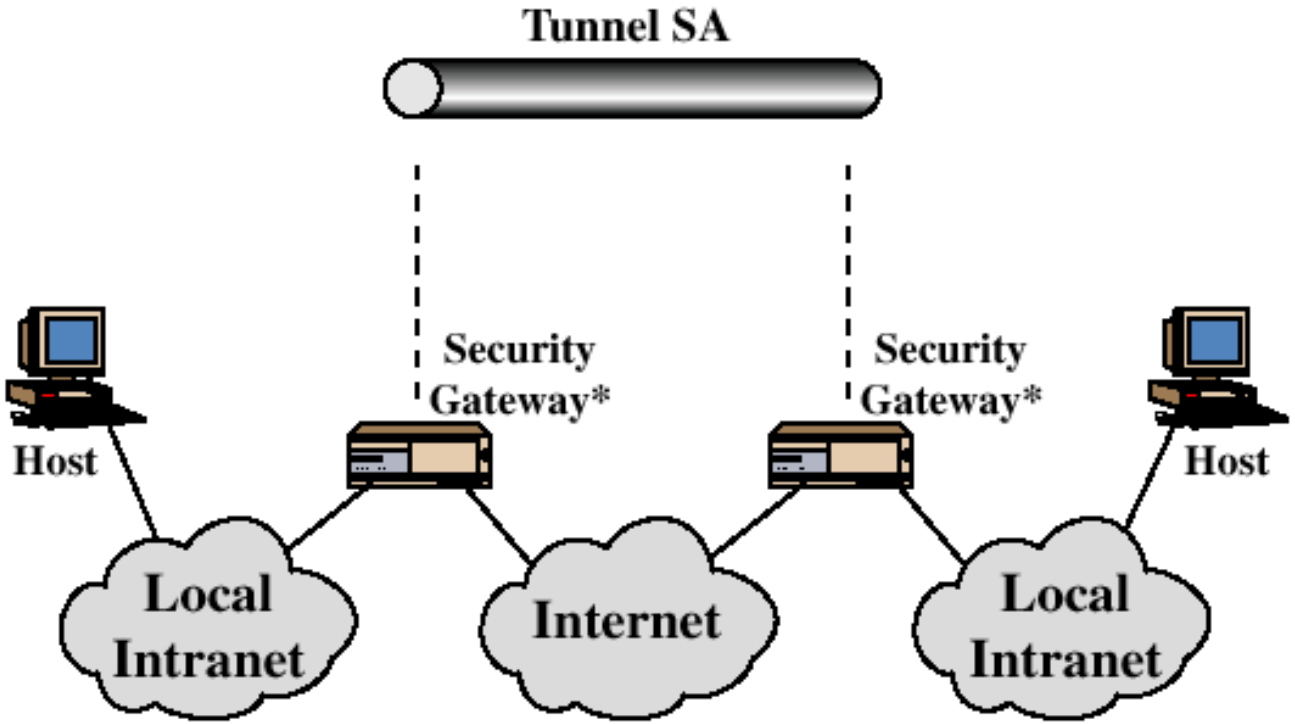
Basic Combinations of SAs



(a) Case 1

- IPsec services b/w hosts with IPsec capability
- Sharing a secret key b/w hosts

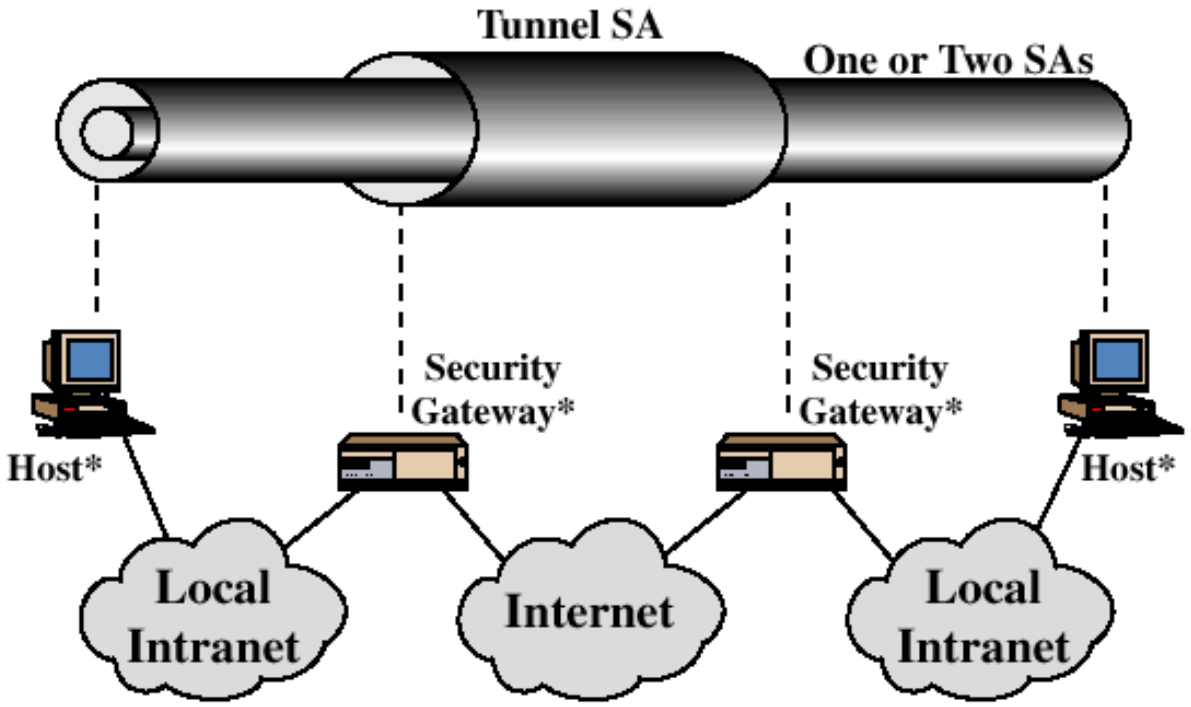
Basic Combinations of SAs



(b) Case 2

- IPsec services only b/w gateways
- Support of simple virtual private network
- The tunnel could support AH, ESP, or ESP with the authentication service

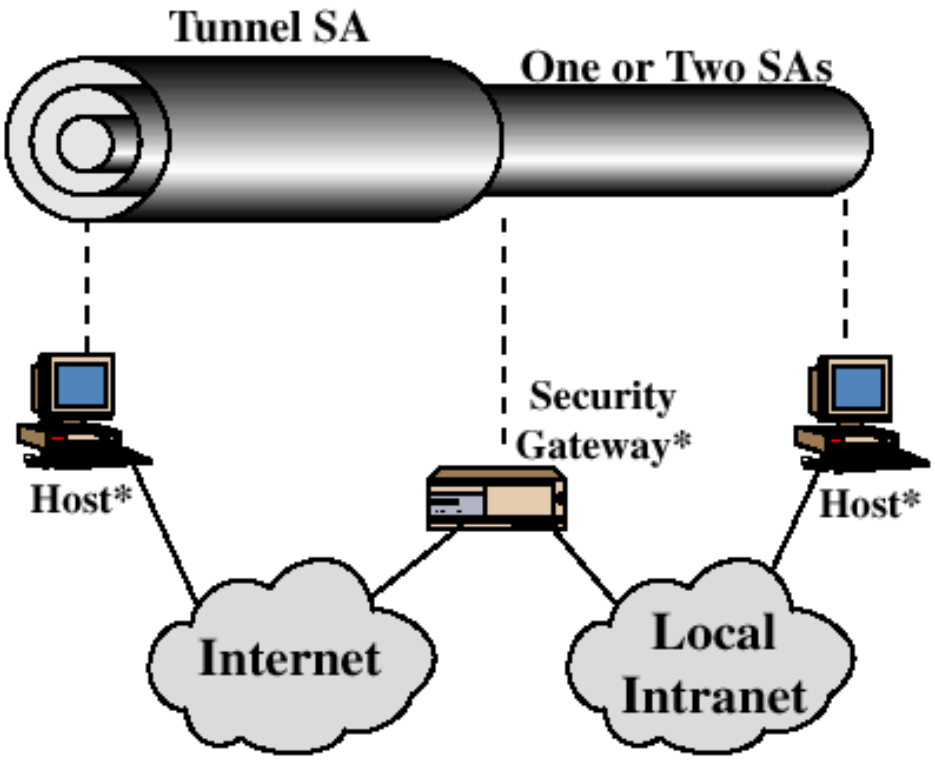
Basic Combinations of SAs



(c) Case 3

- **Adding E-to-E security on case 2**

Basic Combinations of SAs



(d) Case 4

- **Providing support for a remote host that uses the Internet to reach an organization's firewall and then to gain access to some server or workstation behind the firewall.**

Key Management

- **The determination and distribution of secret keys**
- **Four keys for communication b/w two applications**
  - **Pairs for both AH and ESP**
- **Two types of key management**
  - **Manual :** for small, relatively static environment
  - **Automated :** On-demand creation of key for SAs under a large distributed environment.
- **The default automated key Mgmt protocol for IPsec**
  - **Oakley Key Determination Protocol : key exchange protocol based on Diffie Hellman**
  - **ISAKMP :** Internet Security Association and Key Mgmt Protocol
    - providing a framework for Internet key management
    - providing the specific protocol support, including formats, for negotiation attributes

Key Management in IPSec

- Complex system
  - not a single protocol (theoretically)
  - different protocols with different roles
    - intersection is IPsec
    - but may be used for other purposes as well
- Several protocols are offered by IPSec WG of IETF
  - Oakley, SKEME, SKIP, Photuris
  - ISAKMP, IKE
- IKE seems to be the IPSec key management protocol but it is actually a combination of Oakley, SKEME and uses ISAKMP structure

Oakley

- Key exchange protocol based on Diffie-Hellman has extra features:
  - cookies
    - precaution against clogging (denial-of-service) attacks
      - makes the attack more difficult
    - cookies are unique values based on connection info (kind of socket identifiers):source address/destination address/source port#, destination port#)
    - used at every message during the protocol
  - predefined groups
    - fixed DH global parameters
    - regular DH and EC DH (elliptic curve Diffie-Hellman)
  - nonces
    - against replay attacks
  - authentication (via symmetric or asymmetric crypto)

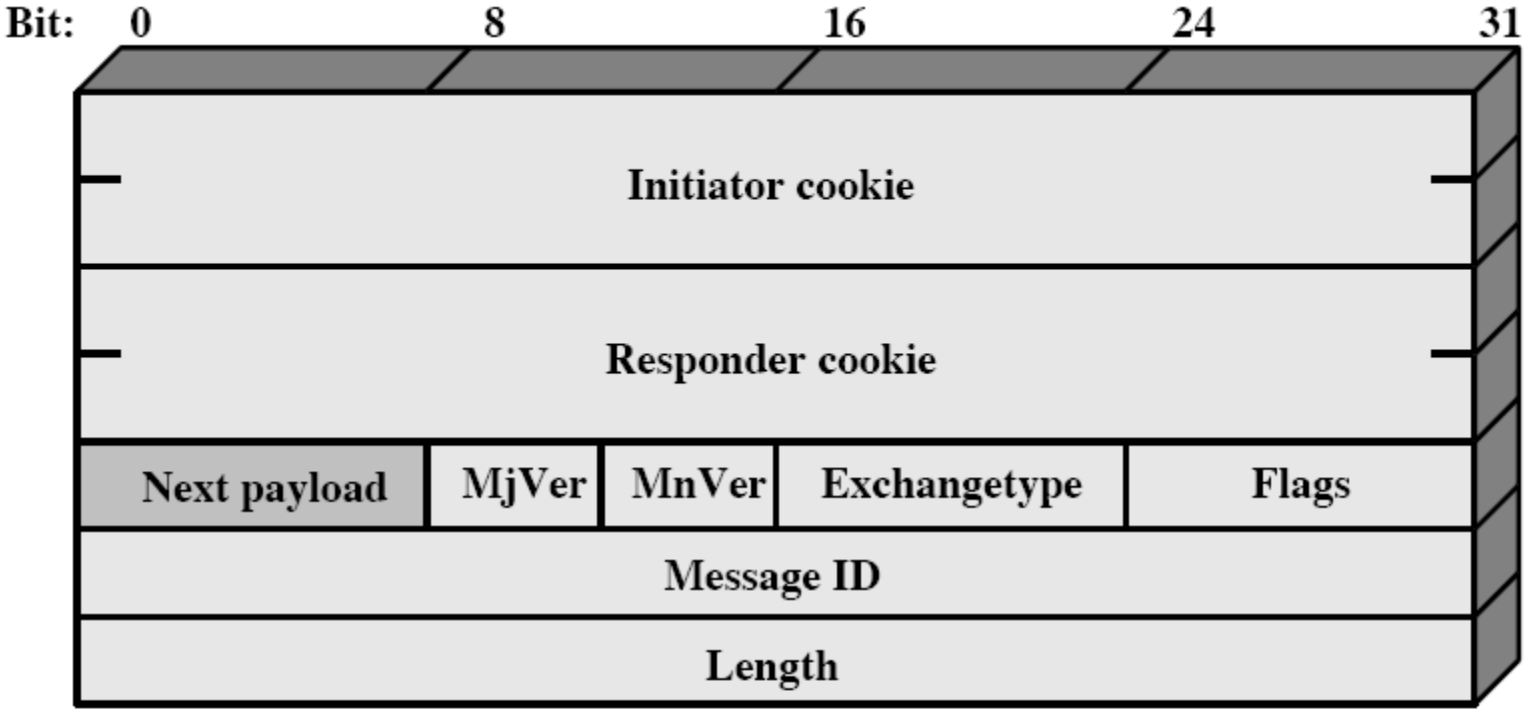
ISAKMP

- Internet Security Association and Key Management Protocol
- defines procedures and message formats to establish, negotiate, modify and delete SAs
  - SA-centric, so some call it only a SA management protocol
    - but we have keys in SAs
  - ISAKMP is NOT key exchange protocol
- independent of key exchange protocol, encryption algorithm and authentication method
- IKE combines everything
- DoI (Domain of Interpretation) Concept
  - the scope of SA (not only IPSec)

ISAKMP

- Typical SA establishment protocol runs in ISAKMP
  - Negotiate capabilities
    - DoI, encryption algorithms, authentication methods, key exchange methods, etc.
  - Exchange keys
    - using the method agreed above
  - Authenticate the exchange
    - digital signatures based on certificates
    - public-key authentication using previously exchanged public keys
    - symmetric crypto based authentication based on previously shared secret (e.g. manual entry)

ISAKMP Header



(a) ISAKMP Header

(b) Generic Payload Header

ISAKMP Payloads

- ISAKMP has several payload types
  - chaining (each payload points to the next one)
  - they are used to carry different types of information for SA generation and management
- Some payload types
  - SA payload
    - to exchange the DoI information
  - Proposal and Transform payloads
    - to exchange the security and crypto capabilities in the DoI
  - Key Exchange payload
    - to exchange the key exchange info
  - Others (e.g. nonce, identification, certificate, certificate request, signature, …)

ISAKMP Protocol Flow (Message Exchange)

- negotiate / key exchange / authenticate
- 5 such ISAKMP message exchanges are proposed
  - will go over two important ones here
    - identity-protection exchange
    - aggressive exchange
  - each message is one ISAKMP message (header + payloads)
    - main header includes cookies for each message
    - each step specifies which payloads exist
    - SA payload means (SA + proposal + transform) payloads

Identity Protection Exchange

(b) Identity Protection Exchange	
(1) **I → R:** SA	Begin ISAKMP-SA negotiation
(2) **R → I:** SA	Basic SA agreed upon
(3) **I → R:** KE; NONCE	Key generated
(4) **R → I:** KE; NONCE	Key generated
(5)* **I → R:** ID_I; AUTH	Initiator identity verified by responder
(6)* **R → I:** ID_R; AUTH	Responder identity verified by initiator; SA established

* means encrypted message payload
  - that is why identity is protected
- AUTH is the authentication information, such as digital signatures

Aggressive Exchange

(d) Aggressive Exchange	
(1) **I → R:** SA; KE; NONCE; ID_I	Begin ISAKMP-SA negotiation and key exchange
(2) **R → I:** SA; KE; NONCE; ID_R; AUTH	Initiator identity verified by responder; Key generated; Basic SA agreed upon
(3)* **I → R:** AUTH	Responder identity verified by initiator; SA established

- minimizes the number of exchanges but does not provide identity protection

IKE (Internet Key Exchange)

- now we are ready to go over IKE
  - the actual protocol used in IPSec
  - uses parts of Oakley and SKEME
    - and ISAKMP messages
  - to exchange authenticated keying material
- Analogy for the protocols
  - ISAKMP: railways, highways, roads
  - Oakley, SKEME: prototypes for cars, trains, buses (and other vehicles)
  - IKE: a system that has several vehicles running on railways, highways, roads

IKE

- Perfect forward secrecy (from SKEME)
  - disclosure of longterm secret keying material does not compromise the secrecy of exchanged keys from earlier runs
- PFS in IKE (basic idea)
  - Use a different DH key-pair on each exchange
    - of course they have to be authenticated, probably with a digital signature mechanism
    - however, disclosure of the private key (long-term key) for signature does not disclose earlier session keys

IKE

- Authentication Methods of IKE
  - certificate based public key signature
    - certificates are exchanged
  - public-key encryption
    - Some key material exchanged using previously known public keys
    - no certificates, so no non-repudiation
  - pre-shared key
    - symmetric method
    - simplest, no public key crypto
- Material to be authenticated is derived from the messages exchanged

Phases of IKE

- Phase 1: establish IKE SA
  - Main mode (DH with identity protection)
    - ISAKMP identity protection exchange
  - Aggressive mode (DH without identity protection)
    - ISAKMP aggressive mode

- Phase 2: establishes SA for target protocol (AH or ESP)
  - Quick mode (only 3 exchanges)
  - IKE SA is used to protect this exchange
  - Several SAs can be established in quick mode

Summary

- IP Security (IPsec) is a capability that can be added to either current version of the Internet Protocol (IPv4 or IPv6), by means of additional headers

- IPsec encompassed 3 functional areas: authentication, confidentiality, and key management

- Authentication makes use of the HMAC and can be applied to the entire original IP packet(tunnel mode) or all of the packet except for the IP header (transport mode)

- Confidentiality is provided by an encryption format known as encapsulating security payload: tunnel and transport modes