Virtual Private Networks (VPNs)

Understand the principles and mechanisms of VPN technologies and use it to achieve private communications over public networks

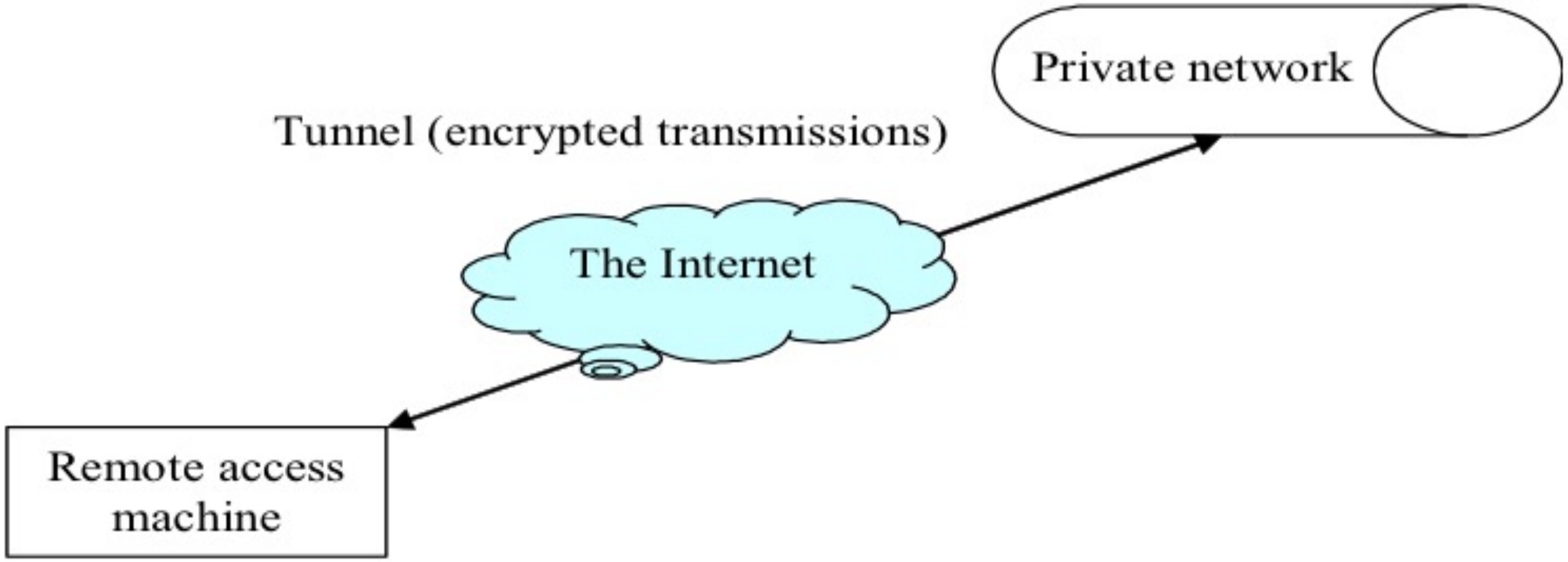
Source:
Main textbook: chapter 22.5.
Also VPNs and VPN Technologies by Cisco Press, available here at https://www.ciscopress.com/articles/article.asp?p=24833

Overview

- VPN Overview
- VPN Technologies
  - Point-to-point tunnelling protocol (PPTP) (not covered)
  - IP Security (IPSec)
- Conclusions

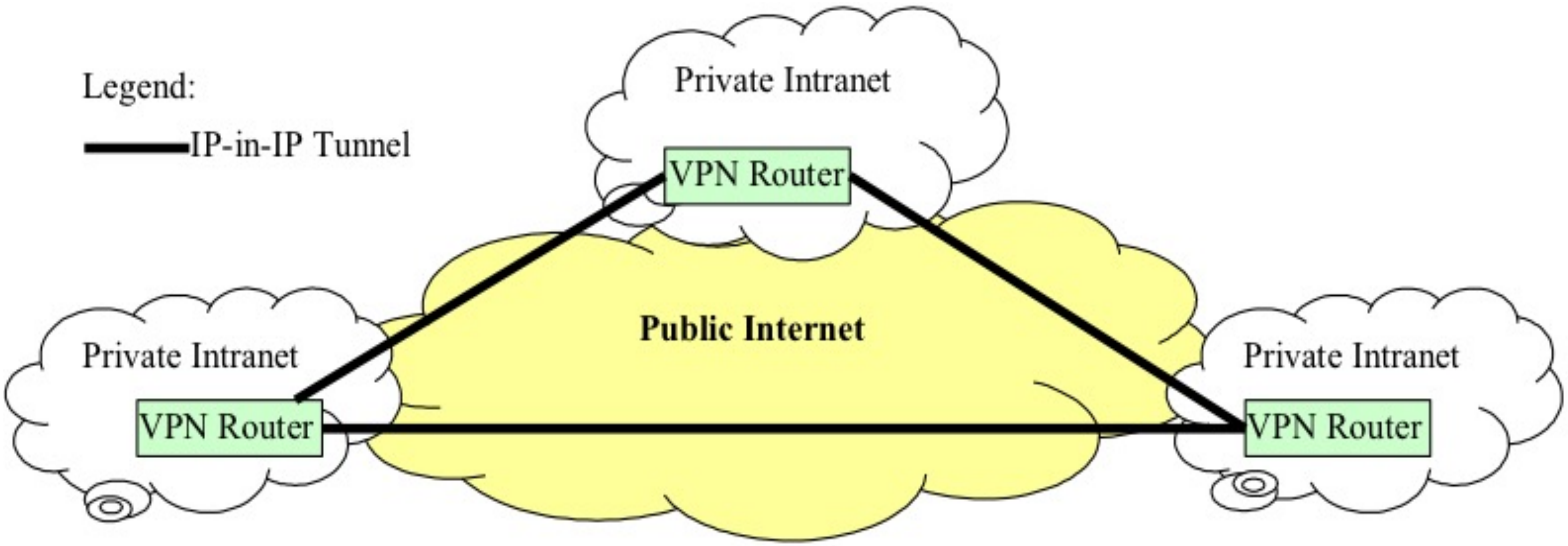
VPN Overview - What is a VPN?

- A VPN is a security solution, making use of tunnelling, encryption, authentication, and access control technologies to allow you to achieve private communication over public networks such as the Internet.



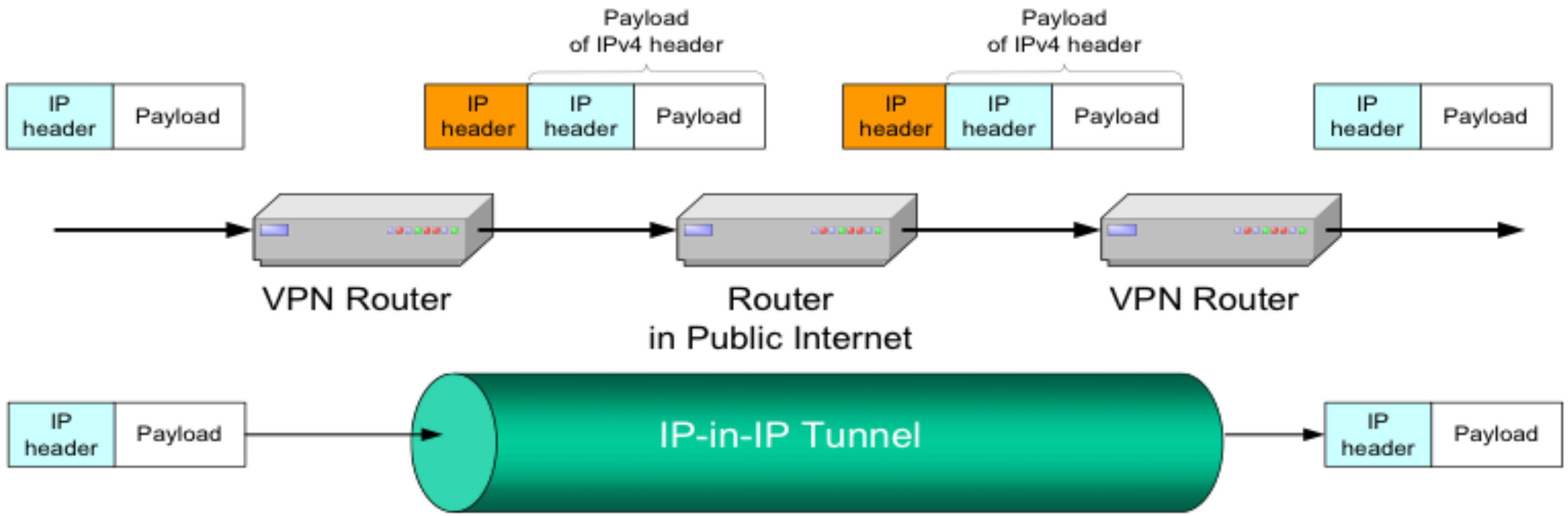
VPN Overview - What is a VPN?

- Tunnelling includes encapsulation, transmission and decapsulation; encapsulation is to wrap data with a header that provides routing information allowing it to transmit across the Internet to reach its destination so as to emulate a dedicated point-to-point link.



VPN Overview - What is a VPN?

- **In IP-in-IP encapsulation**, IP packets are encapsulated in another IP packet.



VPN Overview - What is a VPN?

- VPN Routers (or VPN Gateways) are located at the corporate network perimeter; they perform tunneling, authentication, and data encryption/decryption.
- They can be categorized as Standalone or Integrated.
  - Standalone VPNs incorporate purpose-built devices.
  - Integrated implementations add VPN functionality to existing devices such as routers, firewalls.
    - Router based VPNs add encryption support to existing routers and can keep the upgrade costs of VPN low.
    - Firewall based VPNs are a workable solution for small networks with low traffic volume.

VPN Overview - What is a VPN?

- VPN Client
  - is software used for remote VPN access.
  - creates a secure path from the remote client computer to a VPN gateway.
  - can be loaded onto an individual computer requesting remote access **or** a router that establishes a peer-to-peer (router-to-router) VPN connection.
- During tunnel setup, the devices on each side of the tunnel agree on the details of authentication and encryption.
  - Authentication is for identifying VPN users and devices and for ensuring the authenticity of data;
  - Encryption is for protecting the confidentiality of data while transit across the Internet.

The University of Manchester

VPN Overview – VPN Types

Types	Applications	Alternatives	Benefits
Remote Access VPN	Remote Connectivity	Dedicated Dial ISDN	Ubiquitous Access Lower Cost
Intranet VPN	Site-to-Site Internal Connectivity	Leased Line	Extended Connectivity Lower Cost
Extranet VPN	Business-to-Business External Connectivity	Fax, Snail Post	Facilitates eTransaction and eCommerce

VPN Overview - Why do we need it?

- Security risks on the Internet:
  - Loss of privacy (packet sniffing) - a perpetrator may observe confidential data as it traverses the Internet.
  - Loss of data integrity - data may be modified maliciously or accidentally.
  - Identity spoofing - impersonation.
  - Denial of Service - attacks to cause computer systems to crash.

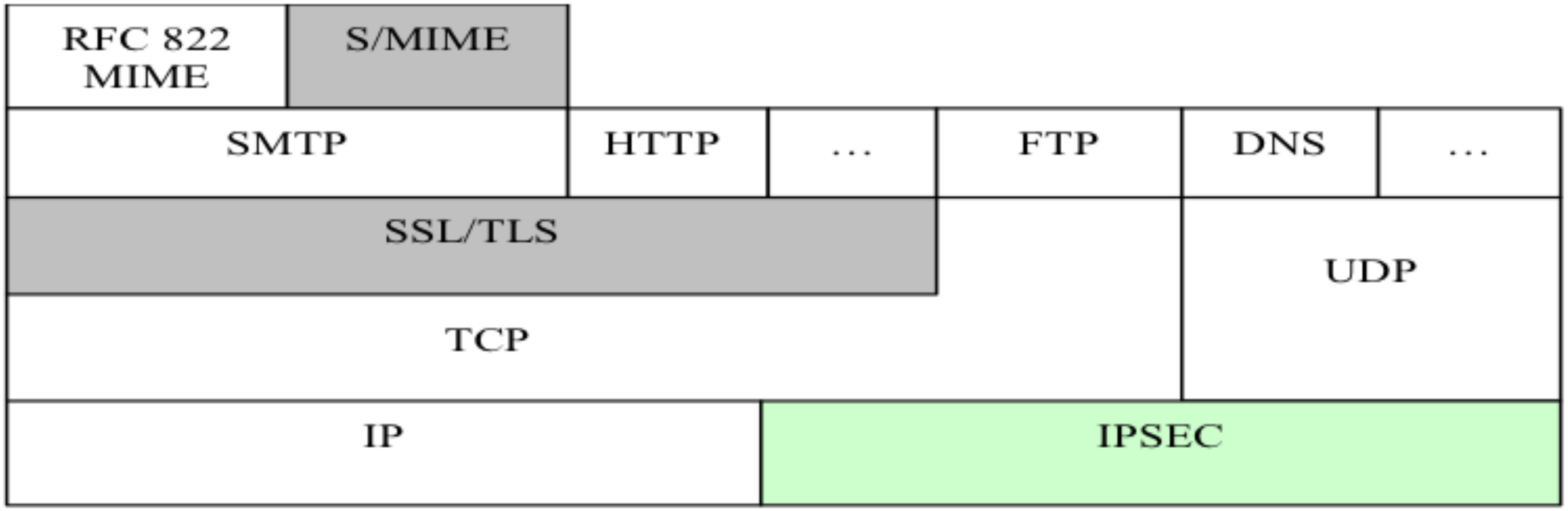
Confidentiality - Encryption

Authenticity (Integrity) - HMAC

Entity Authentication - Keyed hash token, Public key encryption, or Digital signatures

IPSec Overview - Its position in the protocol stack

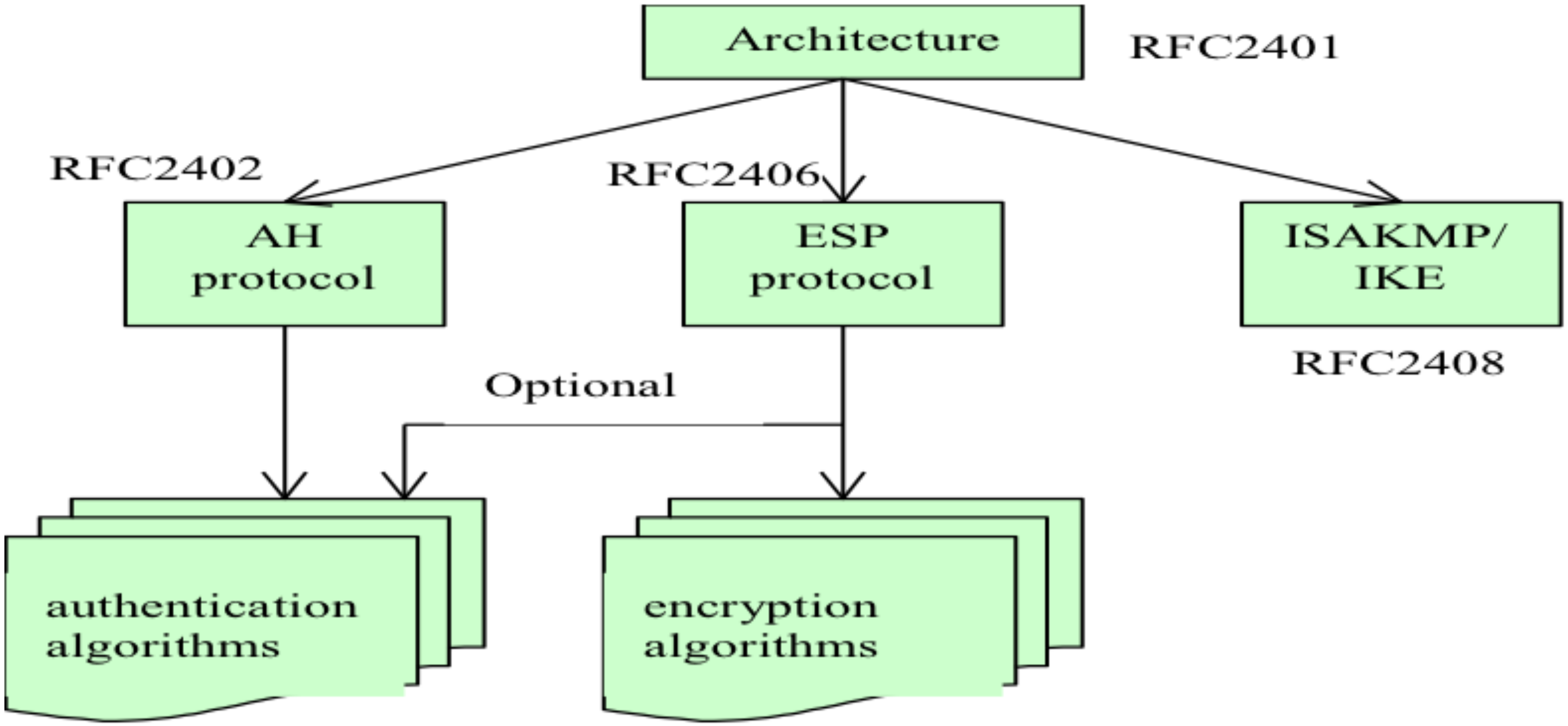
- IPSec Overview
- AH (Authentication Header) Protocol
- ESP (Encapsulating Security Payload) Protocol
- IP Security Summary



IPSec Overview - What it provides

- It operates at the IP (network) layer
- It provides security protection
  - for the transport layer, including all TCP and UDP, traffic;
  - for all other traffic carried in the data field of the IP packet, e.g. ICMP messages;
  - also for IP packets (IPv4 and IPv6) when using tunnel mode.
- This protection is transparent, i.e. there is no need to modify applications or transport-layer protocols to work with IPSec, and can be applied to all the application-level programs.

IP Security Overview - Components



IP Security Overview - Components

- **Security Association (SA)**
  - refers to a set of attributes negotiated between two end-points for the protection of **IP traffic** for the SA.
    - Authentication mechanism
    - Encryption algorithm
    - Algorithm mode
    - A shared session key
    - Initialisation Vector (IV), etc.

Default: HMAC

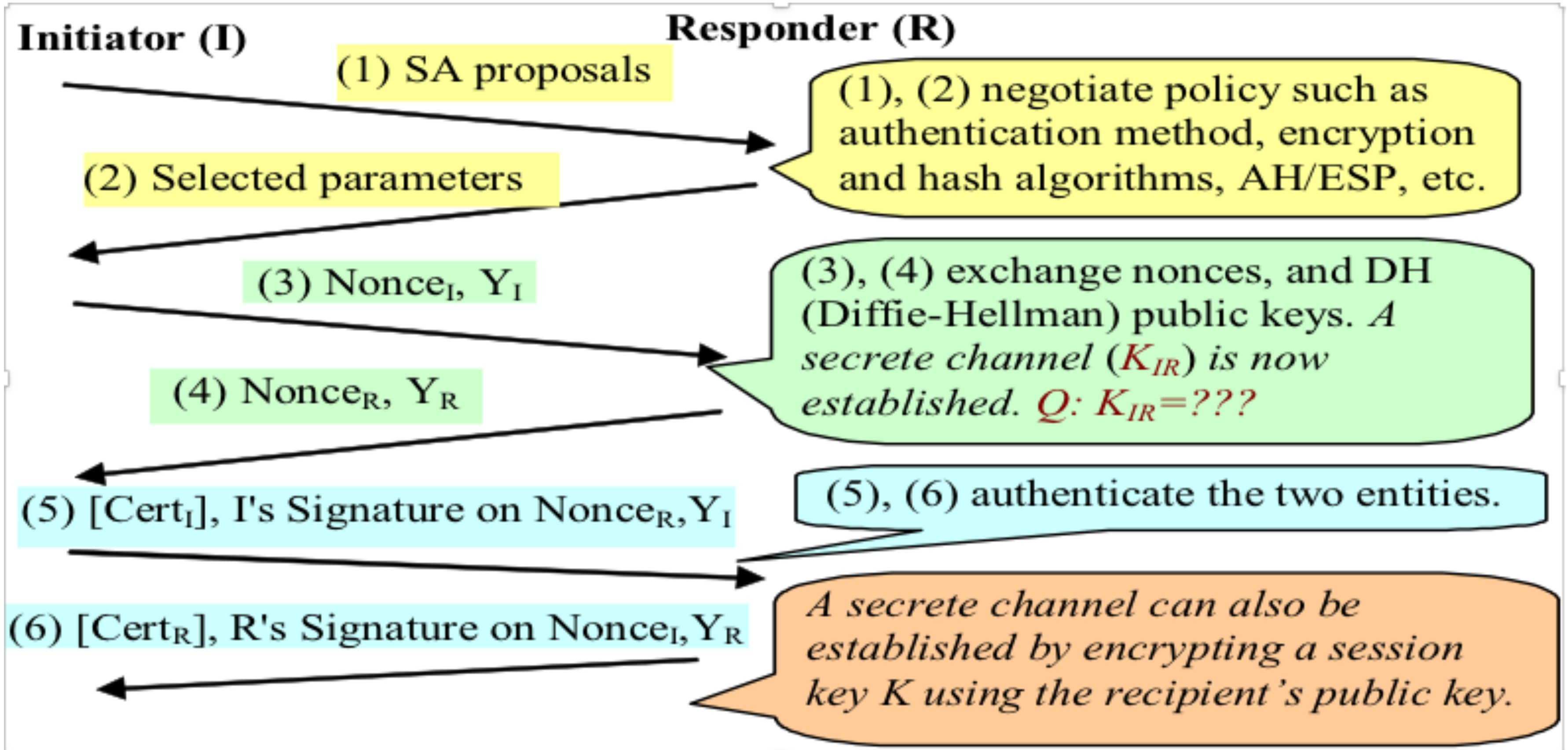
Default: DES - CBC

  - is unidirectional, so for two-way secure exchange two *SA*s are needed.
  - is uniquely identified by
    - a random 32-bit value SPI (secure parameter index = SPI);
    - destination (tunnel ending point) IP address;
    - an identifier of the security protocol (AH or ESP).

IP Security Overview – Session key establishment

- Manual establishment
  - Manually configure keying material and SA data for each system;
  - Practical in small, static environments; Do not scale well.
- Automated key establishment
  - *ISAKMP* (Internet SA Key Management Protocol)
    - defines procedures and packet formats to establish, negotiate, modify and delete SA.
  - IKE (Internet Key Exchange)
    - provides facilities to negotiate and derive keying material for establishing a session key.
      - DH-DSA: using Diffie-Hellman (DH) key agreement for deriving key material between peers on a public network, and DSA to sign the DH exchanges to counter the man-in-the-middle attack.
      - Public key cryptography: using recipient's public key for secure session key transportation.

IP Security Overview - Establishing an SA and session key



IP Security Overview - Authentication methods

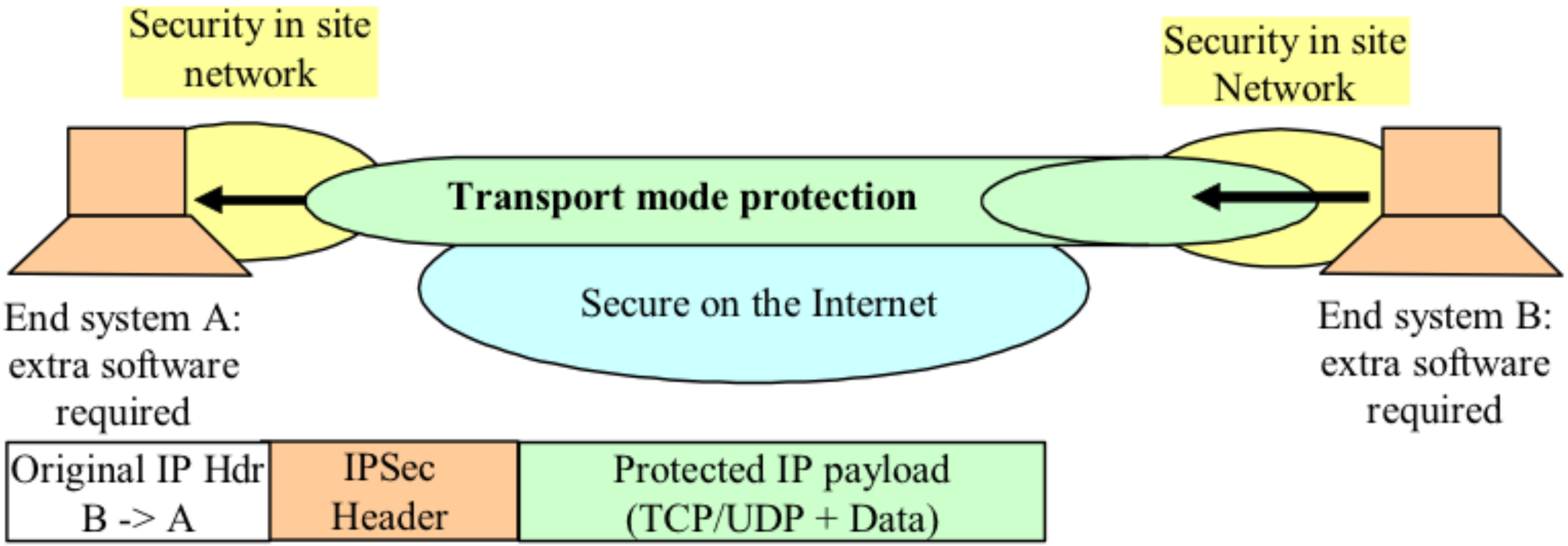
- ISAKMP/IKE supports multiple authentication methods:
  - *Symmetric key cryptography (scheme one)*
    - The same key is pre-installed on each host.
    - The peers authenticate each other by computing and sending a keyed hash of data that includes the pre-shared keys.
  - *Public key encryption (scheme two)*
    - Each party generates a pseudo-random number (nonce) and encrypts it and its ID using the other party's public key;
    - The ability to decrypt the data with the local private key authenticates the parties to each other.
    - The method requires the ability to generate random numbers, and perform public-key encryption/decryption;
    - It does not provide non-repudiation (as in scheme one).
    - Currently, only RSA algorithm is supported.

IP Security Overview - Authentication methods

- *Digital signature (scheme three)*
  - Each device signs some data contributed by the other entity;
  - This method is similar to scheme two, except that it provides non-repudiation;
  - Both RSA and DSS are supported.

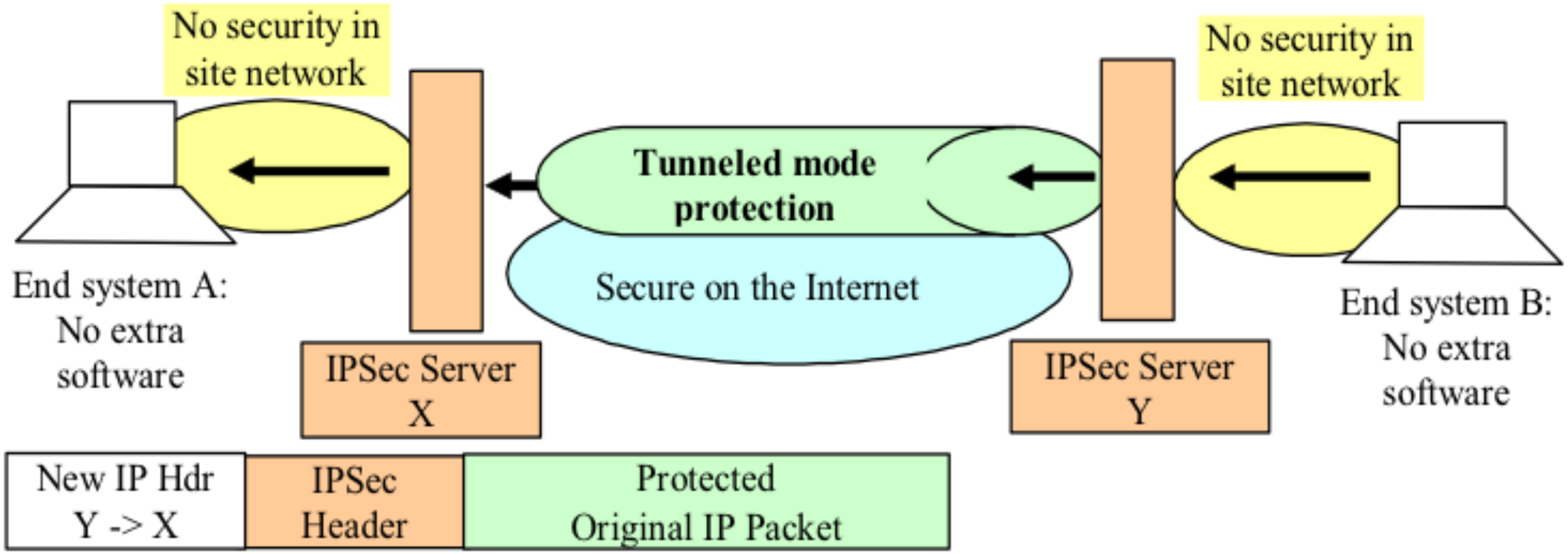
- Once SA(s) is negotiated and session key established, packets are forwarded using traffic protocols, AH and/or ESP.
- IPSec (AH and ESP) may be employed in one of the two ways - *transport* and *tunnel* modes (or *a combination of them*) (the packet formats given next are based upon IPv4).

IP Security Overview - Transport Mode



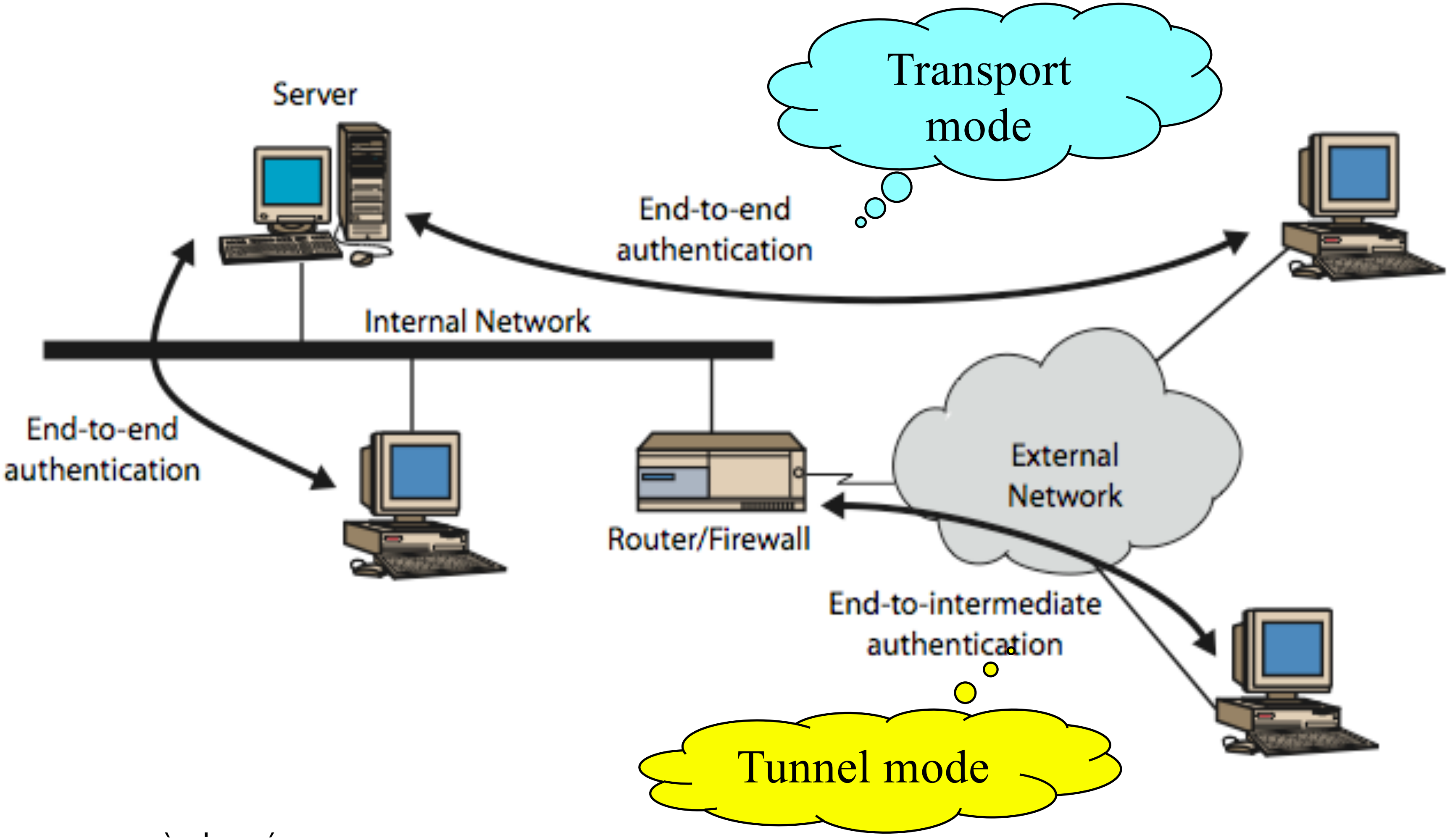
Transport mode: only applicable to **host implementations**; protects **IP payload** => TCP or UDP; adds a few bytes to each packet; original source/destination IP addresses are visible thus enabling special processing such as QoS, but traffic analysis is possible.

IP Security Overview - Tunnel Mode

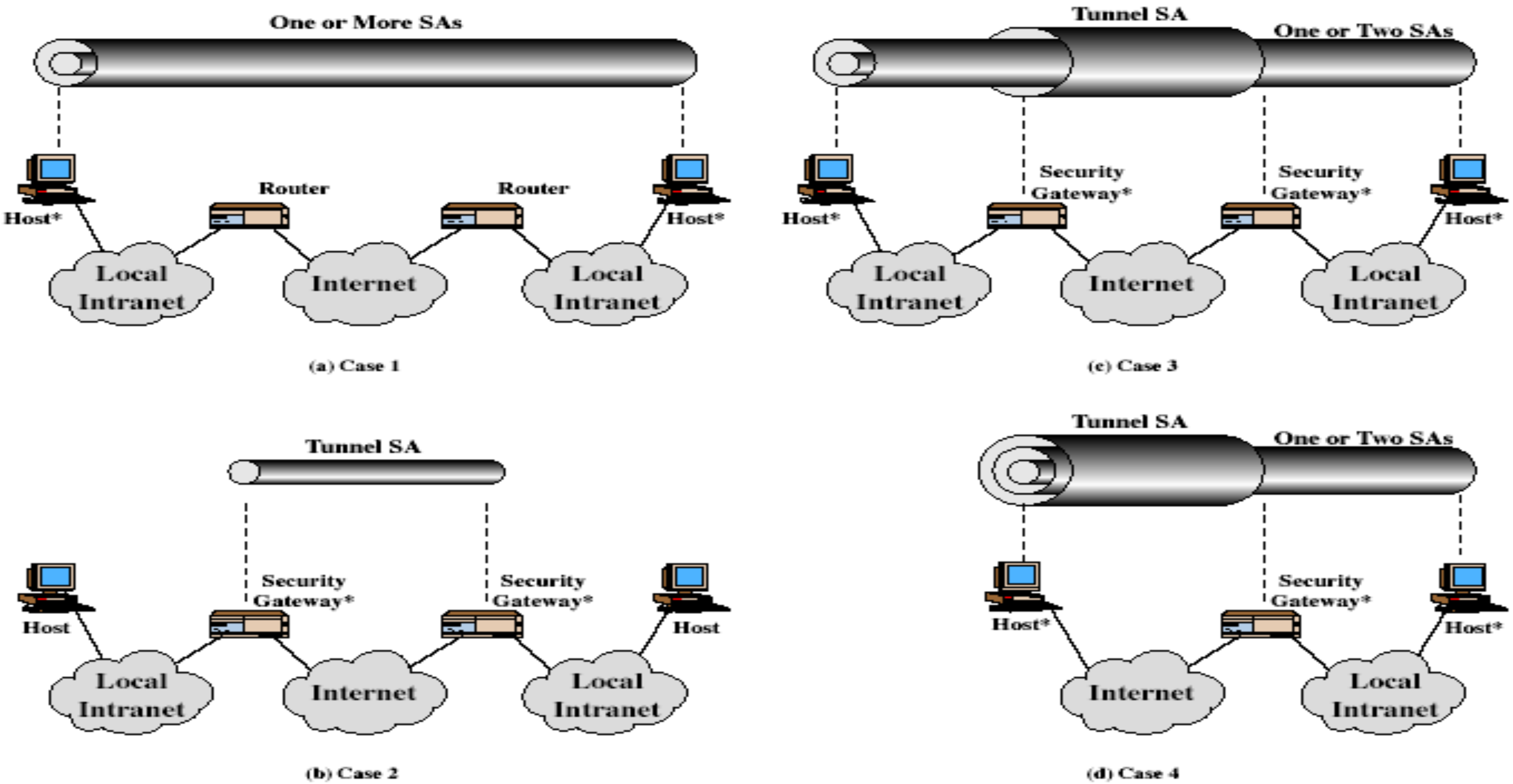


Tunnel mode: employed in either hosts or security gateways; the entire **original IP datagram** is protected (it becomes the payload in a **new IP packet);** allows a network device, e.g. router, to act as an IPSec proxy performing IPSec processing on behalf of the hosts; hosts do not need to be modified; protects against traffic analysis.

IP Security Overview - Remote Dial-up



IP Security Overview – Combining SAs



IP Security Overview – Combining SAs

- Multiple SAs may be combined into an SA bundle.
- An SA can only implement either AH or ESP, so in cases such as the following, one may combine more than one SAs into a bundle:
  - to have both services; and/or
  - different flows in one communication path requires different services.
- SAs can be combined into bundles in the following two ways:
  - Transport Adjacency:
    - Apply ESP in transport mode without authentication;
    - Apply AH in transport mode.
  - Iterated Tunneling (multiple nested tunnels):
    - use multiple IPSec services through IP tunneling; multiple SAs in one bundle may terminate at different or same endpoints.

IP Security Overview – Traffic security protocols

- Each of the IPSec traffic protocols defines a new set of headers to be added to IP datagrams.
- *Authentication Header (AH)* provides
  - data origin authentication,
    - data integrity, and
    - anti-replay.
  - does not provide confidentiality protection.

IP Security Overview - Traffic security protocols

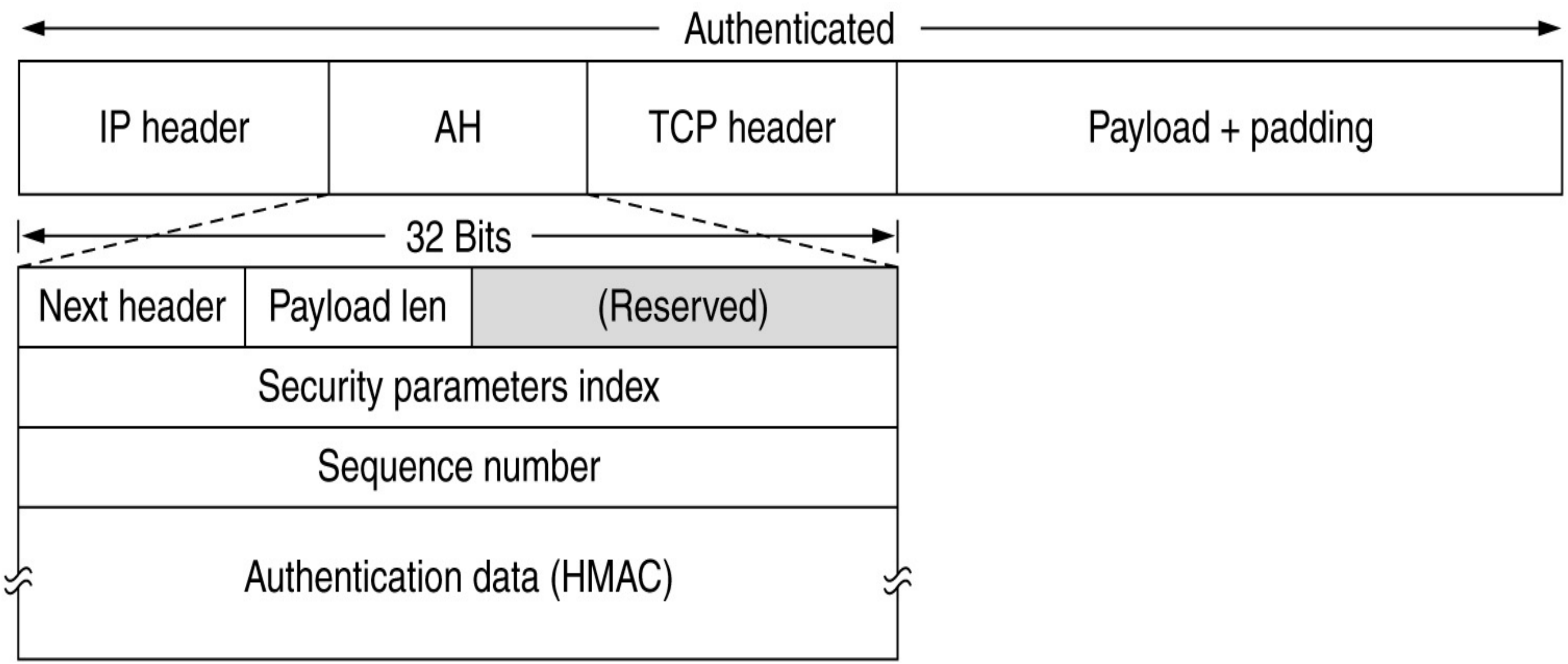
- *Encapsulating security payload (ESP)* provides
  - confidentiality (encryption) protection;
  - partial traffic flow confidentiality; and
  - optional service
    - data origin authentication,
    - data integrity,
    - anti-replay.

AH has these protections

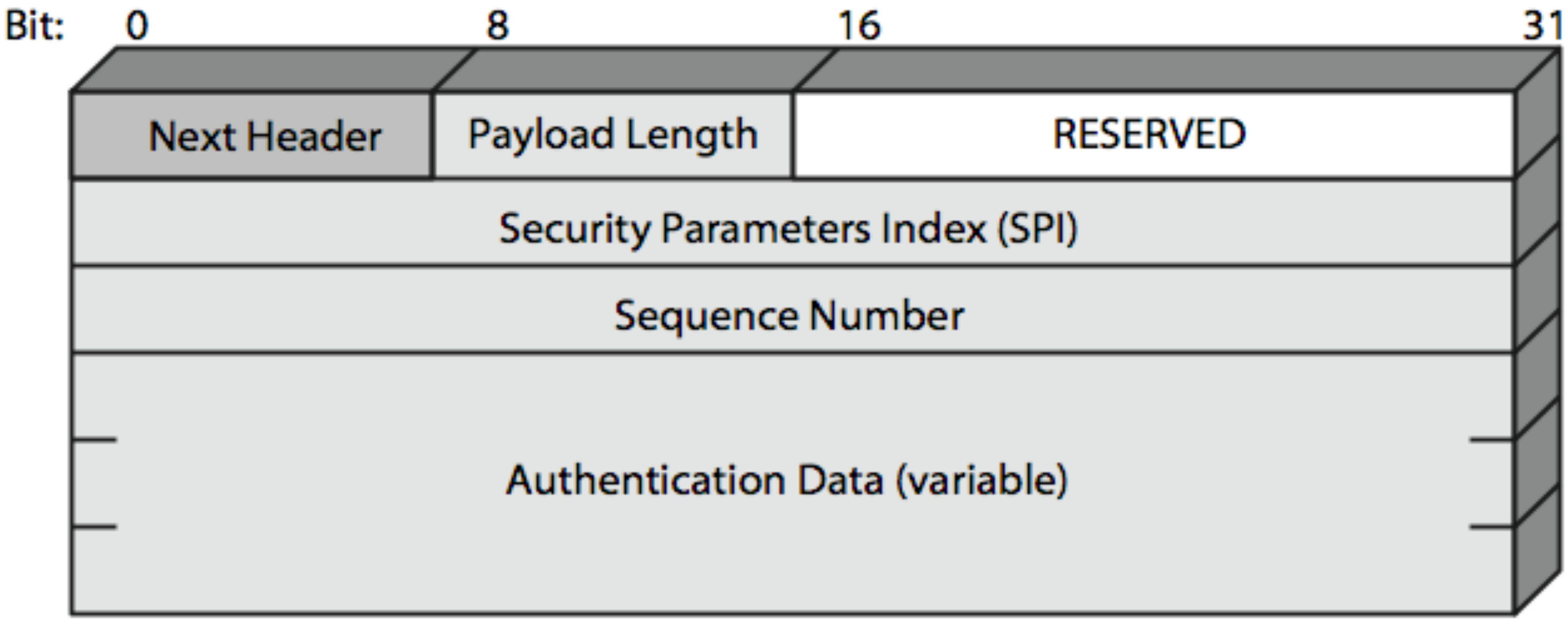
- uses keyed-hash function, HMAC, for data integrity and authentication protection (no non-repudiation protection):
  - HMAC-MD5-96 & HMAC-SHA-1-96.
- uses bulk encryption algorithms, 3-key triple DES, AES, IDEA, CAST, Blowfish and RC5, for confidentiality protection.

Authentication Header (AH) – Format

- The IPsec authentication header in transport mode for IPv4.



Authentication Header (AH) – Format



AH – Format

4 – IP
6 – TCP
17 - UDP

- NextHeader – specifies the type of header immediately following the Authentication Header.
- PayloadLength – the length of AH in 4-byte unit, minus '2'.
- Reserved – not used for now (set to 0).
- SPI (security parameter index) – identifies a SA.
- SequenceNumber – contains a monotonically increasing counter to protect against replay.
- AuthenticationData – contains the message authentication code (MAC) for this packet (typical 96 bits long).

AH - Transport and tunnel modes for IPv4

Original IPv4 packet:

Original IP header	TCP/UDP header	DATA

AH in transport mode:
← Authenticated except for mutable fields in IP header →

Original IP header	AH	TCP/UDP header	DATA

AH in tunnel mode:
← Authenticated except for mutable fields in the outer IP header →

New IP header	AH	Original IP header	TCP/UDP header	DATA

AH - MAC computation

- The default MAC algo is HMAC built on keyed one-way hash function (e.g. MD5 or SHA-1 – which is detailed in the SA);
- It is truncated to the first 96 bits;
- It is stored in the AH AuthenticationData field.
- The following rules are applied to IP Headers (transport mode) and New IP Headers (tunnel mode) when computing the MAC:
  - Mutable IP header fields, e.g. TOS, Flags, Fragment Offset, TTL and Header Checksum are zeroed prior to MAC calculation. All other (immutable) fields are included.
  - The AH AuthenticationData field is zeroed. All other AH header fields are included.
  - The entire upper-level protocol data are included.

AH - Integrity & Authentication Services

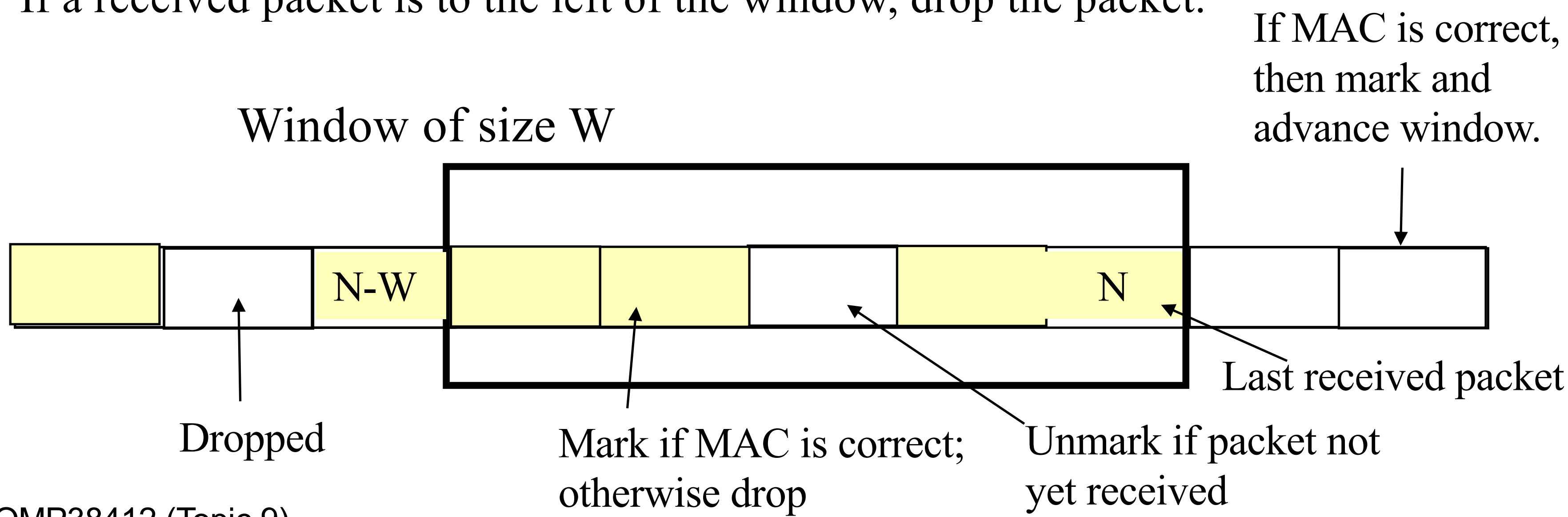
- Outbound packet processing (by sender)
  - SA lookup
  - Sequence number generation - must not cycle for anti-replay
  - MAC calculation
- Inbound packet processing (by receiver)
  - Re-assembly (if IP packet has been fragmented)
  - SA lookup
  - Sequence number verification
  - MAC verification
    - computes MAC and verifies that it is the same as the MAC included in AuthenticationData field.

AH – Anti-Replay

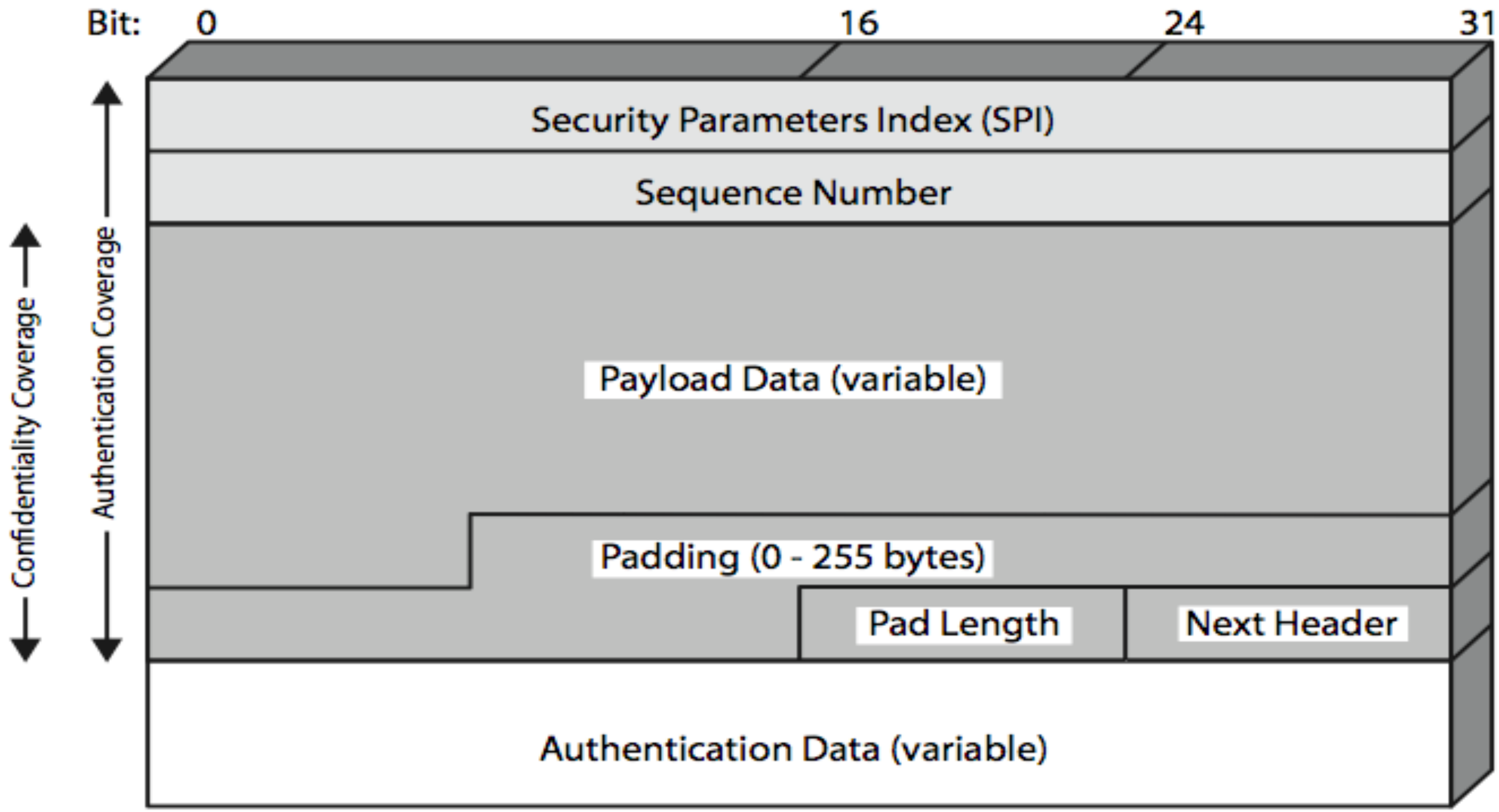
- Replay: retransmits a packet to the intended destination.
- The seq.no. field is used to thwart such attacks.
- For a new SA, seq.no. is initialized as 1 for the 1^{st} packet, and increate it by 1 for each outgoing packet (up to 2^{32} -1). If this limit is reached, then a new SA with a new key should be negotiated.
- IP service is connectionless and unreliable, but IPSec requires the receiver implement a (default) window of size W=64 to track the out-of-order packets received, and to ensure that ‘old’ or ‘duplicated/replayed’ packets are discarded.

AH – Anti-Replay

- A window size, W, specifies number of out-of-order packets that are tracked.
- The right edge of the window shows the highest seq. no, N, of the packet received so far.
- For packets with sequence numbers in the range from N-W+1 to N: if MAC is correct, then mark it; otherwise, drop.
- If a received packet is to the right of the window and is correctly authenticated, mark the packet and advance the window.
- If a received packet is to the left of the window, drop the packet.



Encapsulating Security Payload (ESP) – Format

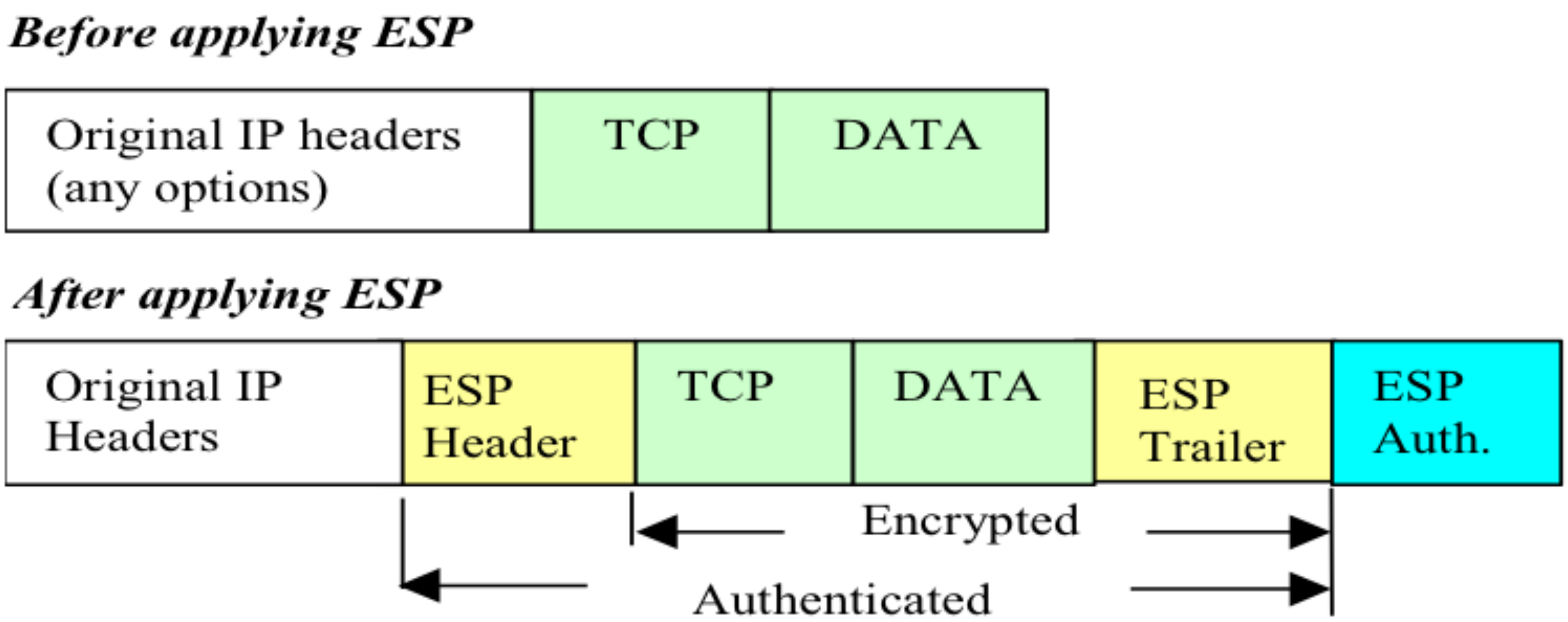


ESP - Format

- PayloadData – is a transport level segment, e.g. TCP segment, (transport mode), or IP packet (tunnel mode) that is protected by encryption.
- Padding – to expand the plaintext (consisted of PayloadData, Padding, PadLth, NextHdr) to the required length e.g. by a block cipher; be aligned on a 4-byte boundary; and to provide partial traffic flow confidentiality.
- PadLth – indicates the number of pad bytes immediately preceding this field.
- NextHdr – identifies the type of data contained in the PayloadData field by identifying the first header in that payload.
- AuthenticationData – contains MAC computed over the ESP packet minus AuthenticationData.
- Other headers are the same as in AH.

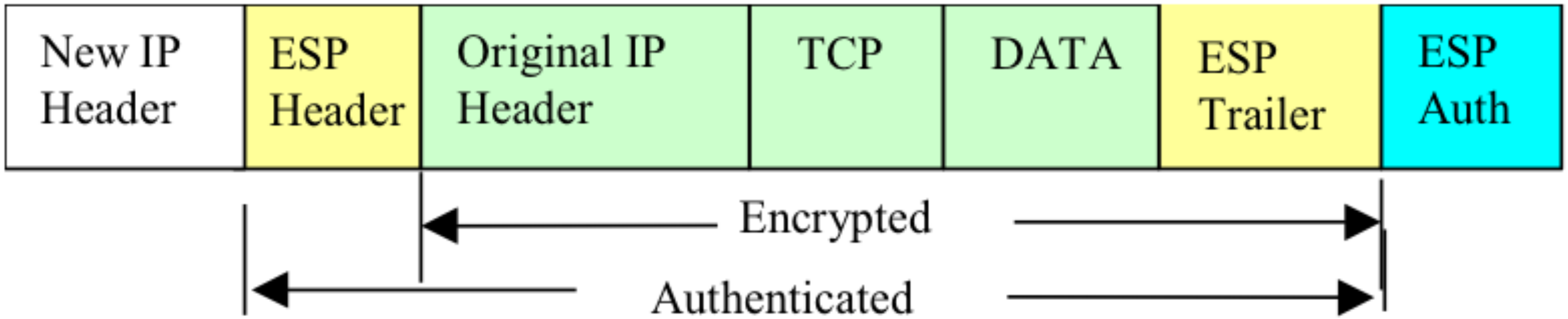
ESP - The transport mode

- ESP Trailer is consisted of Padding, PadLength, and NextHeader.



ESP - The tunnel mode

- The New IP Header just contains enough information for routing at intermediate nodes but not for traffic analysis (based on destination addresses).
- In this mode, encryption only occurs between external host and security gateway, or between security gateways.



ESP - Outbound packet processing

- SA lookup
- Packet encryption
  - Encapsulate relevant data into the ESP payload field.
  - Add any necessary padding.
  - Encrypts the result (PayloadData, Padding, PadLength, and NextHeader) using the key, encryption algorithm indicated by the SA.
- Sequence number generation.
- MAC calculation (if authentication is selected by the SA).

Why is the encryption performed before MACing?

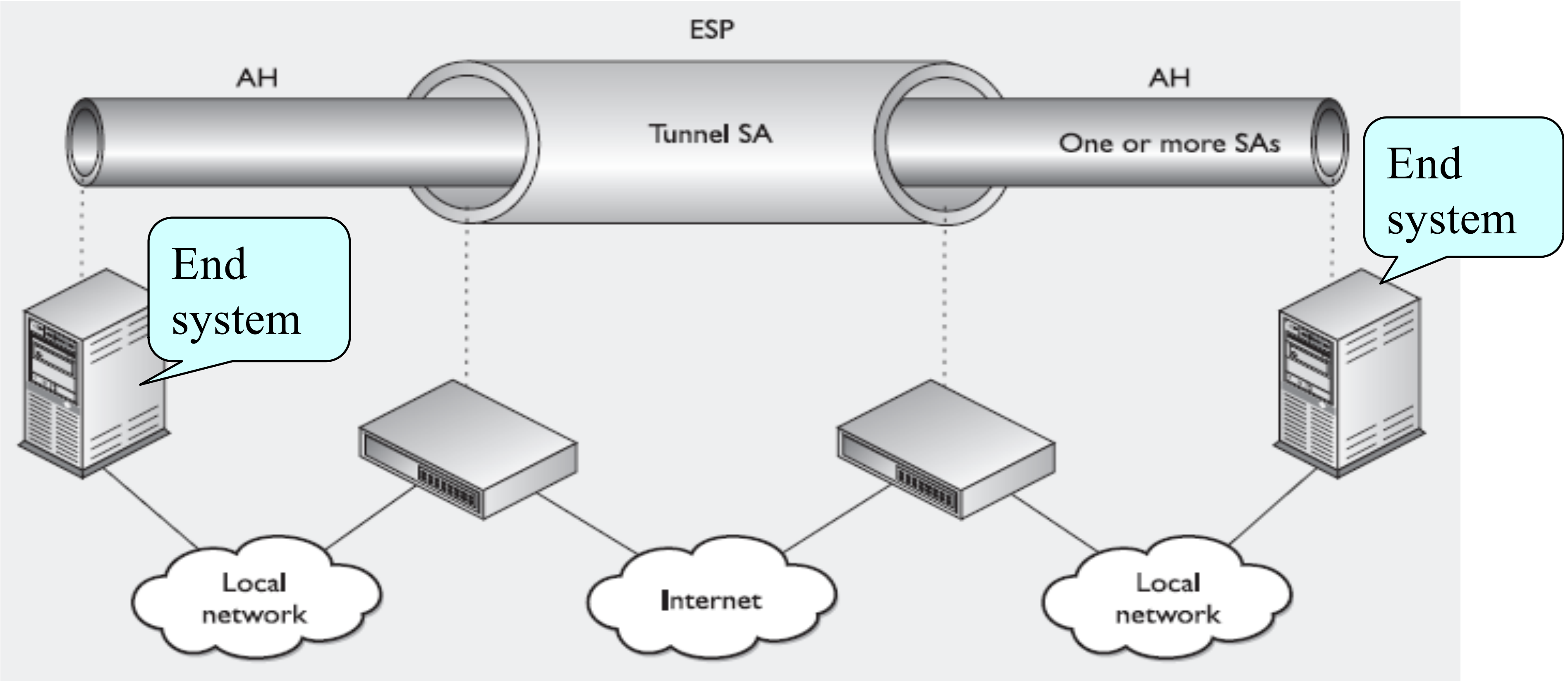
ESP - Inbound packet processing

- Re-assembly (if IP packet has been fragmented by the routers en route)
- SA lookup
- Sequence number verification
- MAC verification
- Packet decryption
  - Decrypt the relevant data.
  - Process any padding as specified in the encryption algorithm specification.
  - Reconstructs the original IP datagram.

What can you observe from this order of operations?

The University
of Manchester

Combined use of ESP and AH



IP Security Summary - Services

	AH	ESP	ESP with authentication
Access control	√	√	√
Connectionless integrity	√		√
Data origin authentication	√		√
Rejection of replayed packets	√		√
Confidentiality		√	√
Limited traffic flow confidentiality		√	√

Exercise Question – E9.1

- What is the major difference between transport mode and tunnel mode in IPSec ESP, and any implications?

Exercise Question – E9.2

One of the ISAKMP key exchange protocols, Identity Protection Exchange, is given below:

Outlined protocol	**Description**
(1) $I \rightarrow R$: SA_I	Begin ISAKMP-SA negotiation; ISAKMP = Internet SA Key Management Protocol.
(2) $R \rightarrow I$: SA_R	Basic SA agreed upon.
(3) $I \rightarrow R$: Y_I, $NONCE_I$	I's DH public key generated and transmitted to R.
(4) $R \rightarrow I$: Y_R, $NONCE_R$	R's DH public key generated and transmitted to I.
(5)* $I \rightarrow R$: ID_I, $AUTH_I$	Initiator (I) identity verified by responder (R)
(6)* $R \rightarrow I$: ID_R, $AUTH_R$	Responder's identity verified by I; SA established
	** signifies that the message content is encrypted with the key established using the DH method*

With the use of a diagram, explain whether or not the identity ID_I of the initiator I could be revealed to a third party (≠ responder R). You should justify your answer.

Conclusions (1/2)

- IPSec is designed to provide interoperable, high quality, crypto-based security services for IPv4 and IPv6, offering protection for IP and/or upper layer protocols, such as TCP, UDP, ICMP.
- AH ensures integrity and origin authentication of data, and is an appropriate protocol to use when confidentiality is not required/permitted.
- ESP protects confidentiality, integrity and origin authentication of data. The scope of the authentication offered by ESP is narrower than it is for AH.

Conclusions (2/2)

- Because these security services use shared secrets (cryptographic keys), IPSec relies on a separate set of mechanisms - ISAKMP/IKE, for putting these keys in place.
- It is important to note that IPSec is only as strong as the algorithms chosen by the individuals for its implementation.
- Its security also depends on other factors such as OS security, random number sources, system management protocols and practices, etc.
- IPSec is mostly commonly used as a VPN solution (it is usually implemented in a user host, or a security gateway, e.g. a router or a firewall).