CT5191
NETWORK SECURITY & CRYPTOGRAPHY

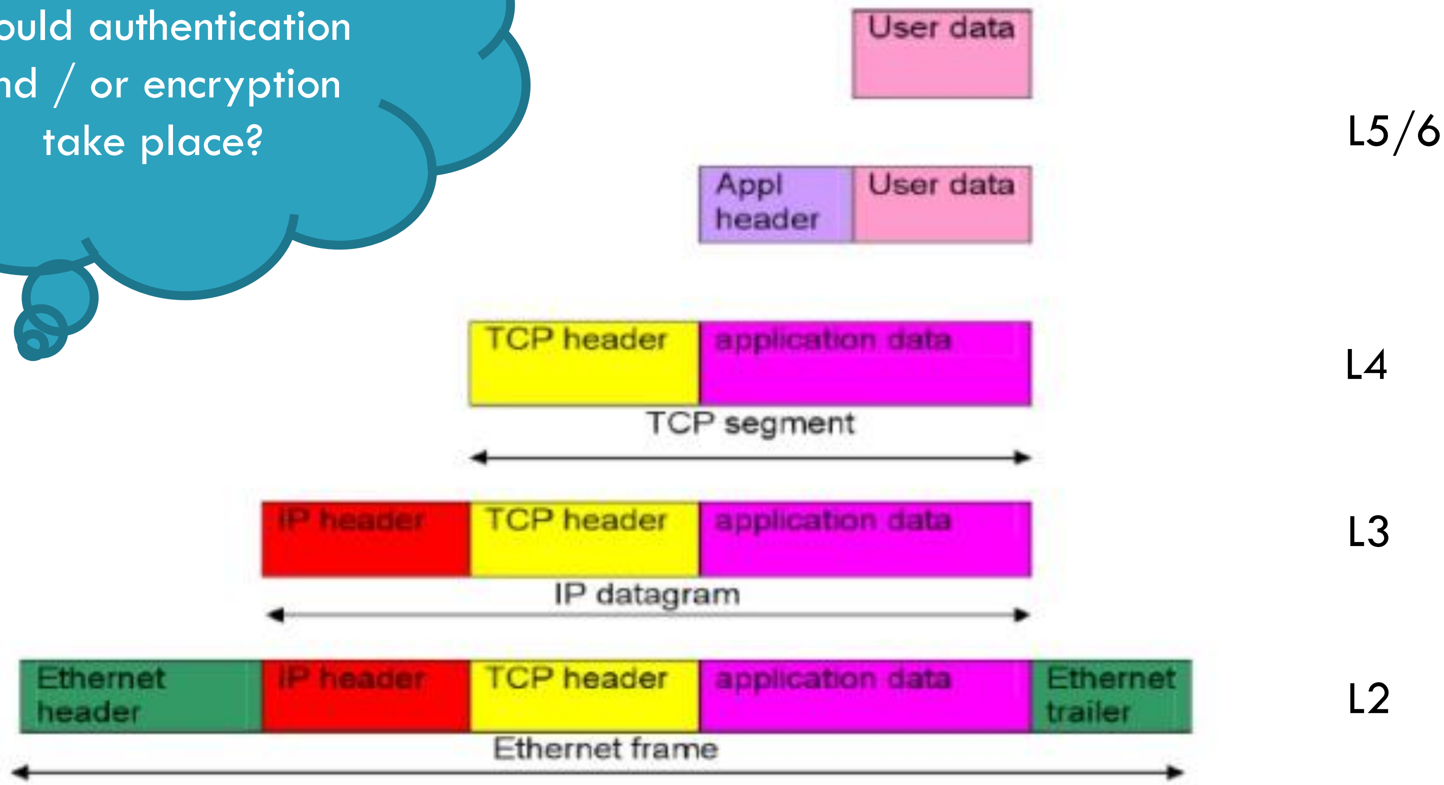
IPSEC

Dr. Michael Schukat

Ollscoil na Gaillimhe
University of Galway

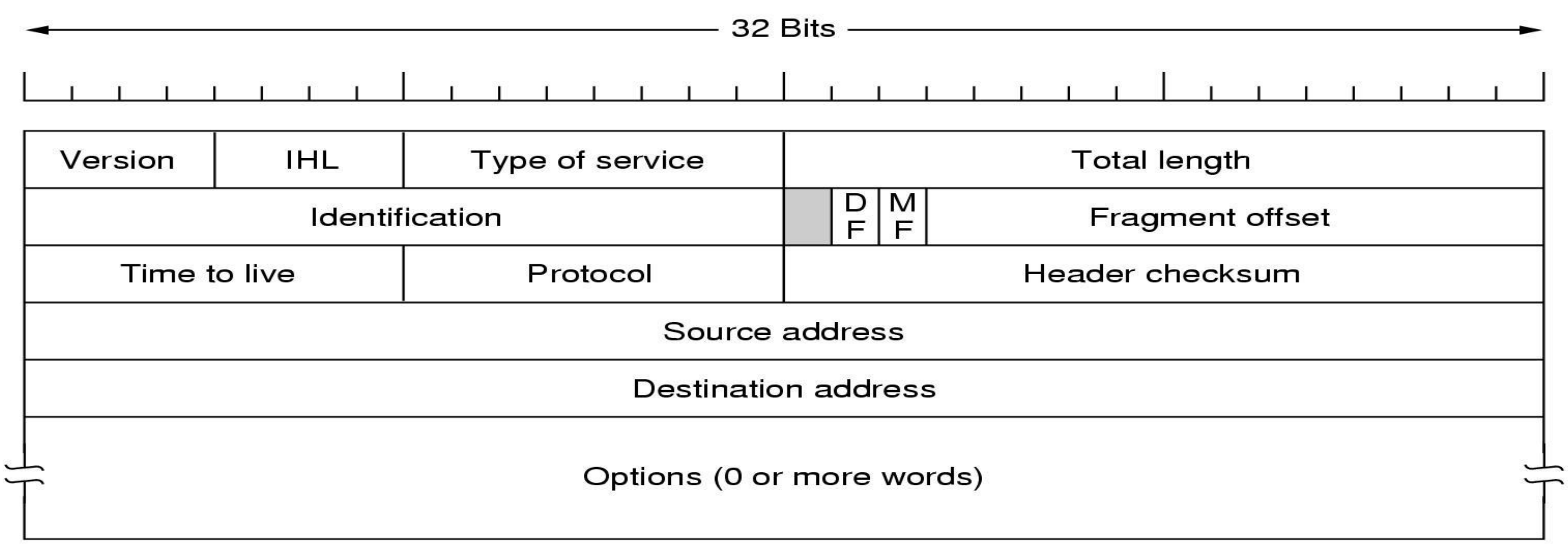
Recap: TCP/ IP Header Hierarchy

On what level(s) should authentication and / or encryption take place?



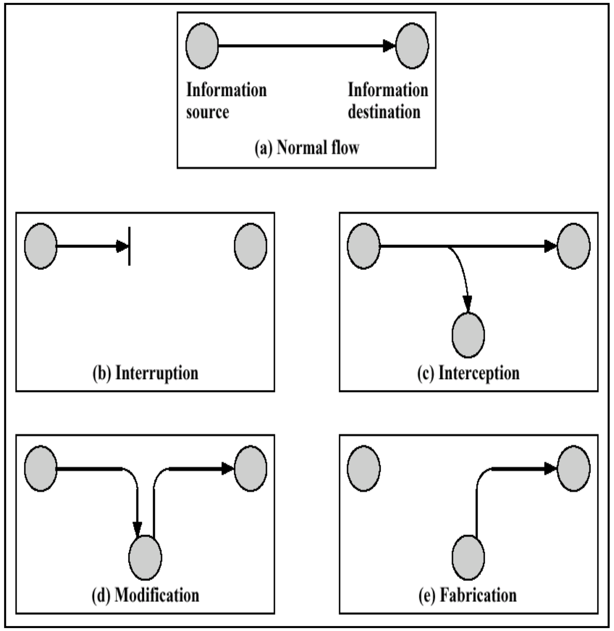
Recap: Issues with the IP Protocol

- IP payload is not encrypted (no confidentiality) and can be manipulated in transit
- IP header fields can be manipulated in transit (CRC can be adjusted on-the-fly → next slide)
  - IP addresses can be spoofed (no authentication)
- IP header has mutable fields that can change during datagram transport

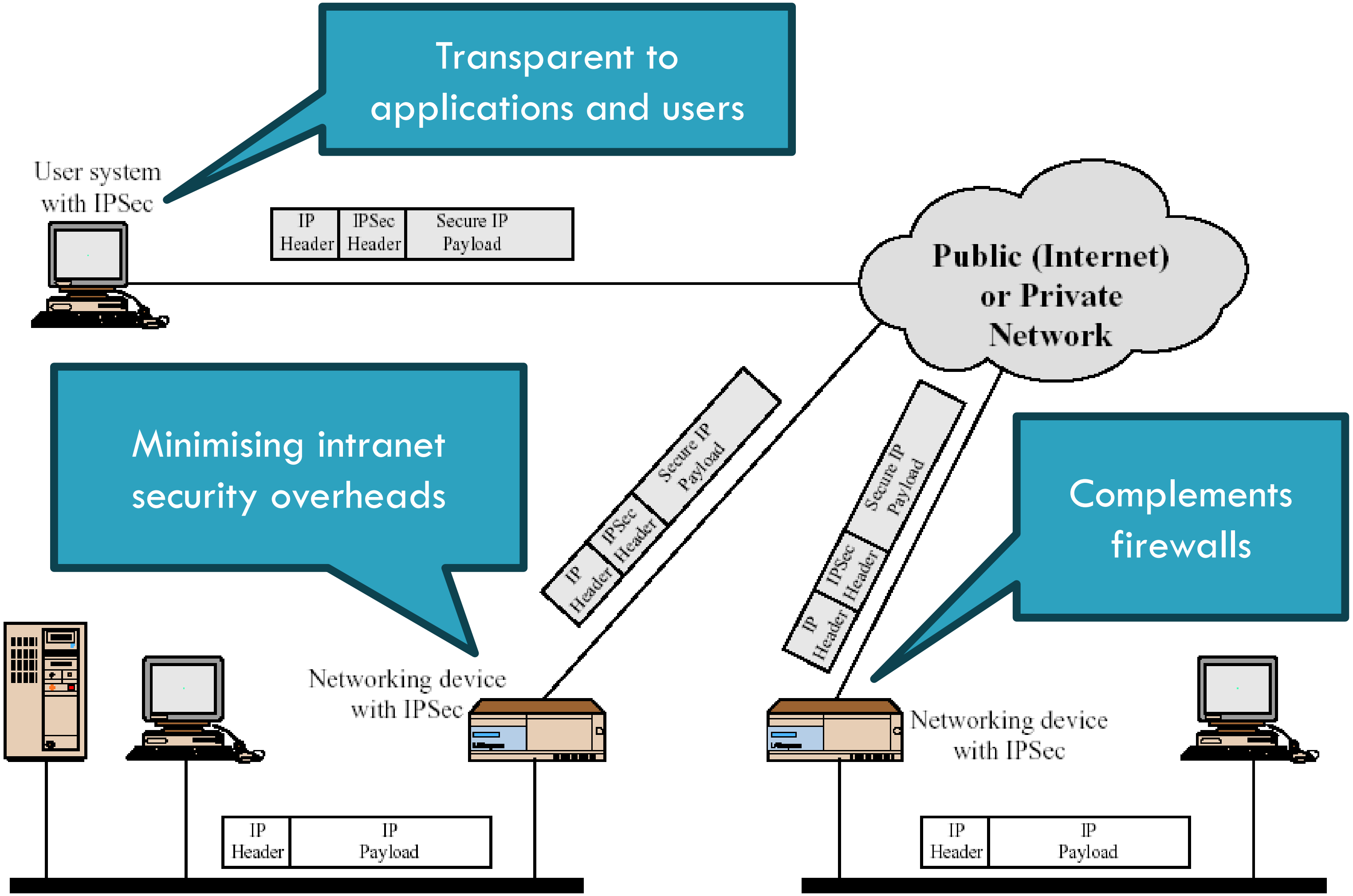


IPsec Overview

- Protocol Standard to protect IP datagrams
- It provides:
  - Data origin authentication
    - → Protection against IP address spoofing
  - Connectionless data integrity authentication
    - → Protection against modification
  - Data content confidentiality
    - → Protection against interception
  - Anti-replay protection
    - Protection against replay attacks / modification
  - Limited traffic flow confidentiality
    - → Protection against interception
    - → (Limited) obfuscation of endpoint IP addresses



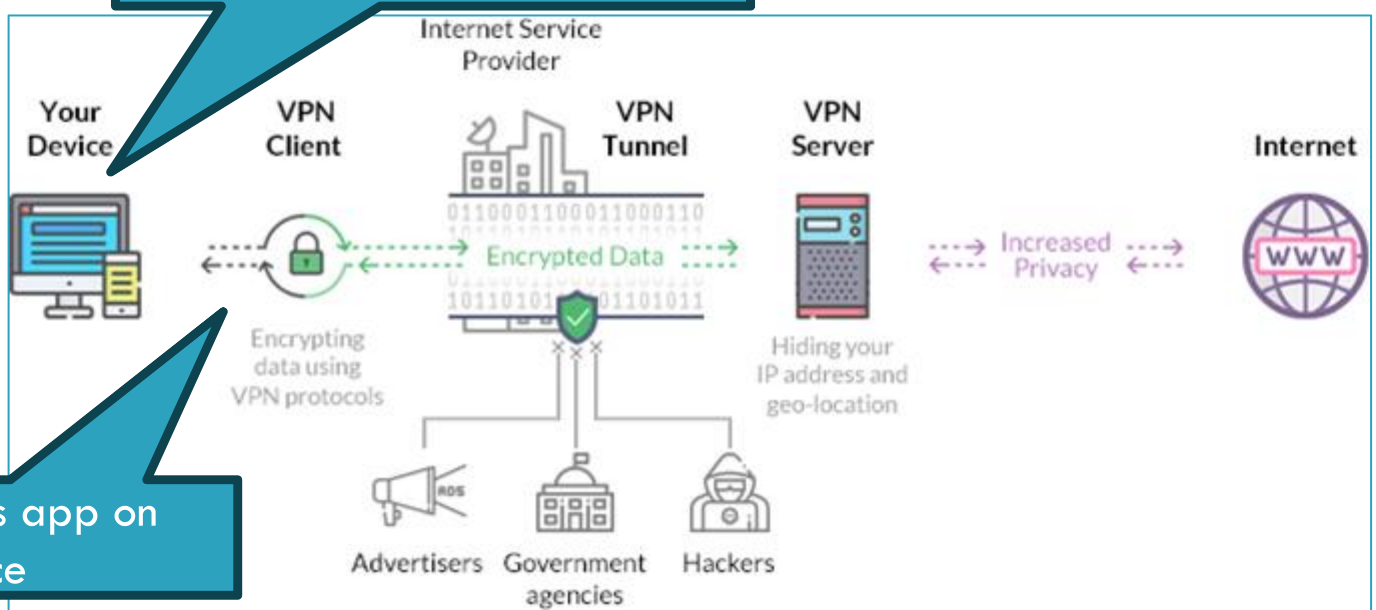
Organisational Use of IPsec



IPsec Virtual Private Networks (VPN) for Individual Users

- VPN service providers enable their customers to protect their identity, as well as their data communication between their computer, across Wi-Fi / LAN and WAN to a trusted gateway (VPN server)

Transparent to applications and users



VPN client is app on device

IPsec Services by Header Type

- IPsec is a network-layer security protocol that provides
  - IP payload encryption (for confidentiality) via **ESP (Encapsulating Security Payload)**
  - IP header and playload authentication via **AH (Authentication Header)**
  - Key management (not covered here)
- As an IP layer protocol extension, it provides secure Internet, LAN, and WAN communication

	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✔	✔	✔
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

Security Associations (SA)

- Key concept for authentication and confidentiality for IP
- One-way relationship between sender and receiver
  - e.g. for a two-way secure peer relationship, two SAs (one for each host) are required

- A SA is uniquely identified by
  - Security parameter index (SPI)
    Unique identifier, which is carried in the IPsec AH and ESP headers
  - IP destination address
  - Security Protocol Identifier: indicates AH or ESP association

SA and the Security Association Database (SAD)

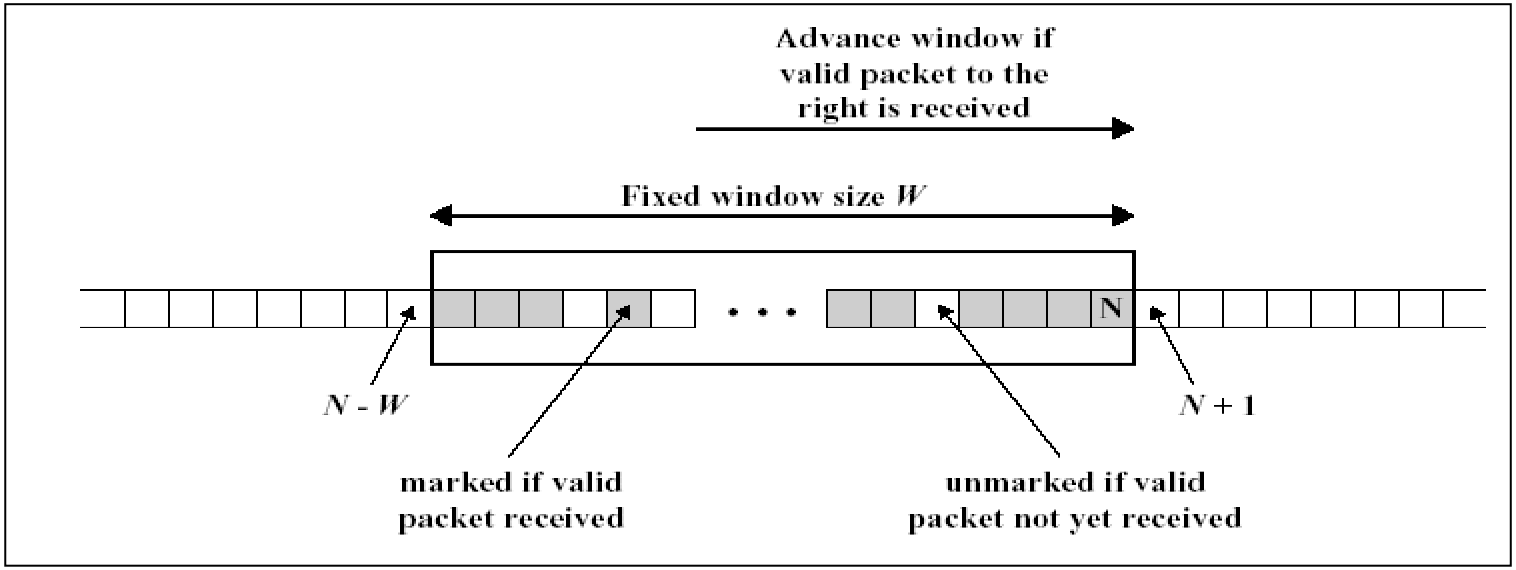
- The SAD contains the parameters associated with each SA, including
  - Sequence number counter:
    32-bit value for packet identification, which is part of AH or ESP header
  - Sequence Counter Overflow flag
  - Anti-replay window
    - Remark: The above 2 parameters are important to prevent replay attacks
  - AH information: Algorithm, key and key lifetime, etc.
  - ESP information: ditto
  - Lifetime of SA (and SPI)
  - IPSec protocol mode: Tunnel or transport mode

Security Policy Database (SPD)

- Each point-to-point link (e.g. host-to-host) is associated with one or more SAs
- This association between links and SA(s) is stored in the SPD, using the following IP header fields (i.e. selectors) as keys:
  - Source / Destination IP address
  - Transport layer protocol
  - Source and destination ports
- For example, in order to process an outgoing IP packet,
  - its selectors are extracted and compared against the SPD entries
  - Zero or more SA references are returned, and their respective SA parameters are retrieved from the SAD
  - Subsequently each SA is processed
- In contrast, The SAs of incoming IPsec packets can be identified by their SPI

The Anti-Replay Window

- A received protected package contains SA selectors, which allow to determine the required SA(s) in the SPD
- The SA entry within the SAD contains state information, e.g. parameters for replay window
- A protected package also contains a unique packet sequence number



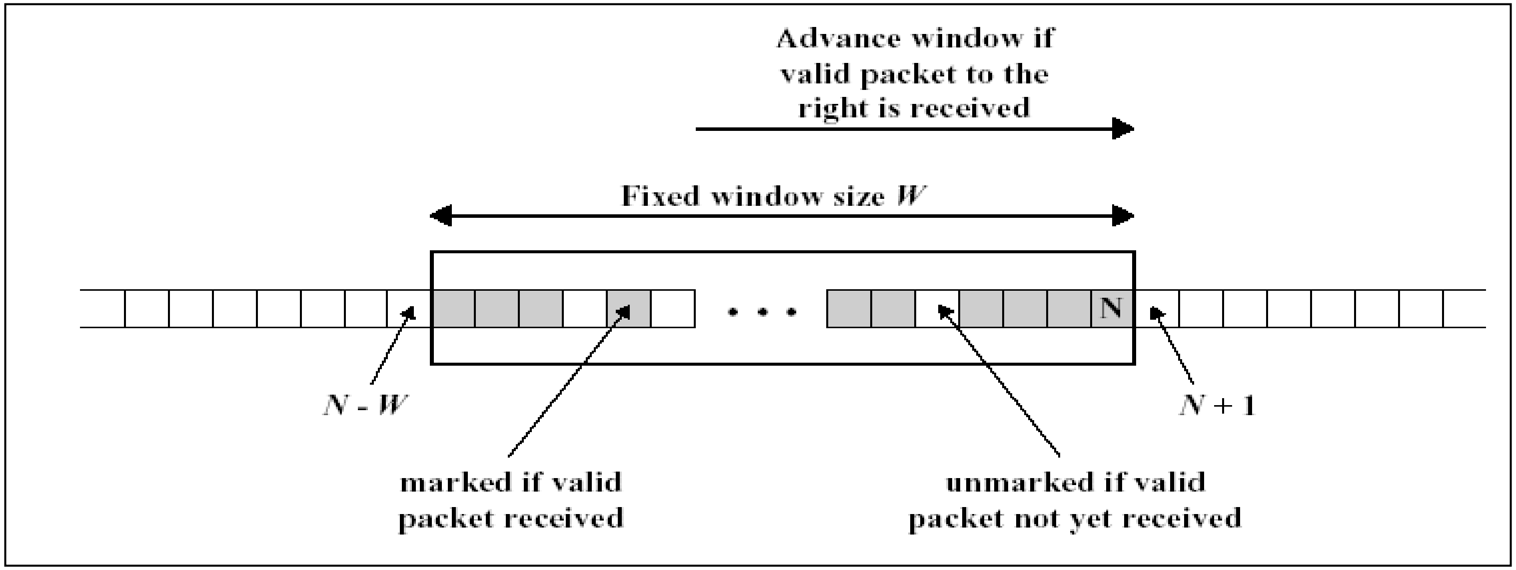
The Anti-Replay Window

- Three scenarios for a received packet:
  - If packet falls within existing window, is new and is authenticated, the corresponding slot will marked, and packet will be processed
  - If packet is right to the window, is new and is authenticated, the window will be advanced, slot will be marked, and packet will be processed
  - If packet is left to the window <u>or</u> authentication fails, it will be discarded, and an alarm will be raised
    - As this could be an indication for a replay attack

Example

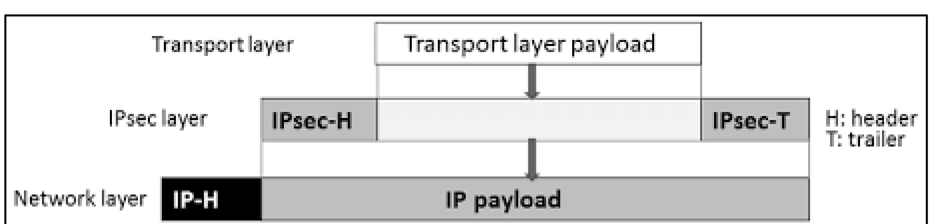
- Consider a receiver with W = 5 and N = 33
- Which of the following incoming (and authenticated) packets will be deemed as a replayed packet and discarded:
- 32, 29, 36, 38, 31, 35

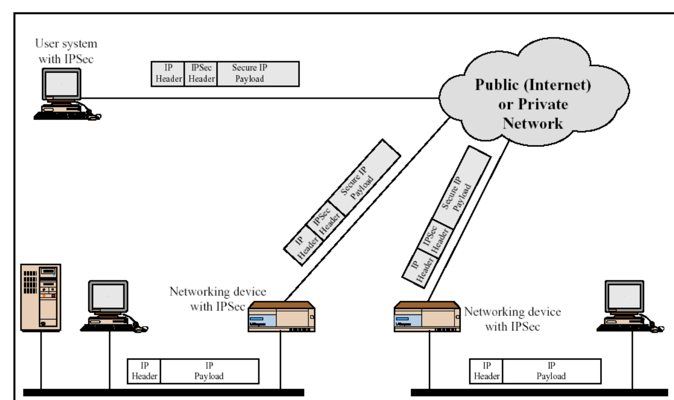
M



IPsec Transport Mode

- Here, the IP header is untouched, and only the payload can be encrypted (via ESP)
  - Therefore, the packet routing is kept intact
- Certain IP header fields (i.e. IP source / destination address) and the payload can be authenticated (via AH)
  - This prevents IP address spoofing, but also NAT, as network address translation invalidates the authenticator (see also NAT traversal)
- Also, transport and application layer are authenticated too, so they cannot be modified in any way in transit, for example by translating the port numbers, unless NAT traversal is used

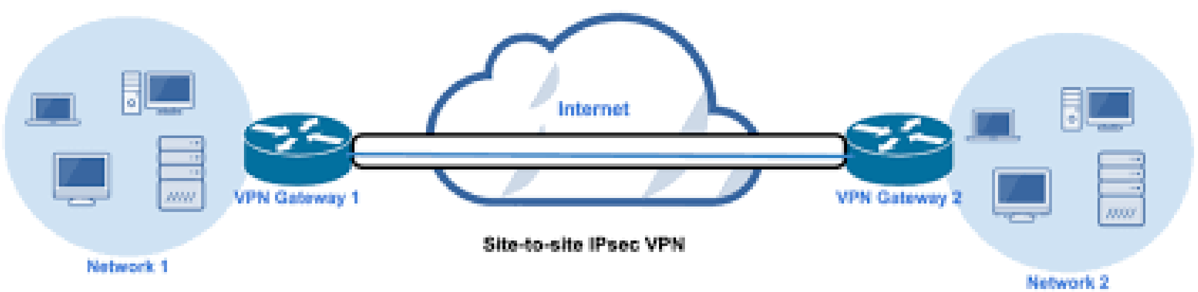




IPsec Tunnel Mode

- Tunnel mode embeds an entire IP packet (as payload) into another (outer) IP packet
  - It secures the IP packet as a whole including its header(s)
- The IP datagram is delivered according to the outer IP header
- Typically for router-to-router or firewall-to-firewall VPN
  - Here IPsec is implemented in a security gateway (router/firewall) that secures all packets coming from within the intranet

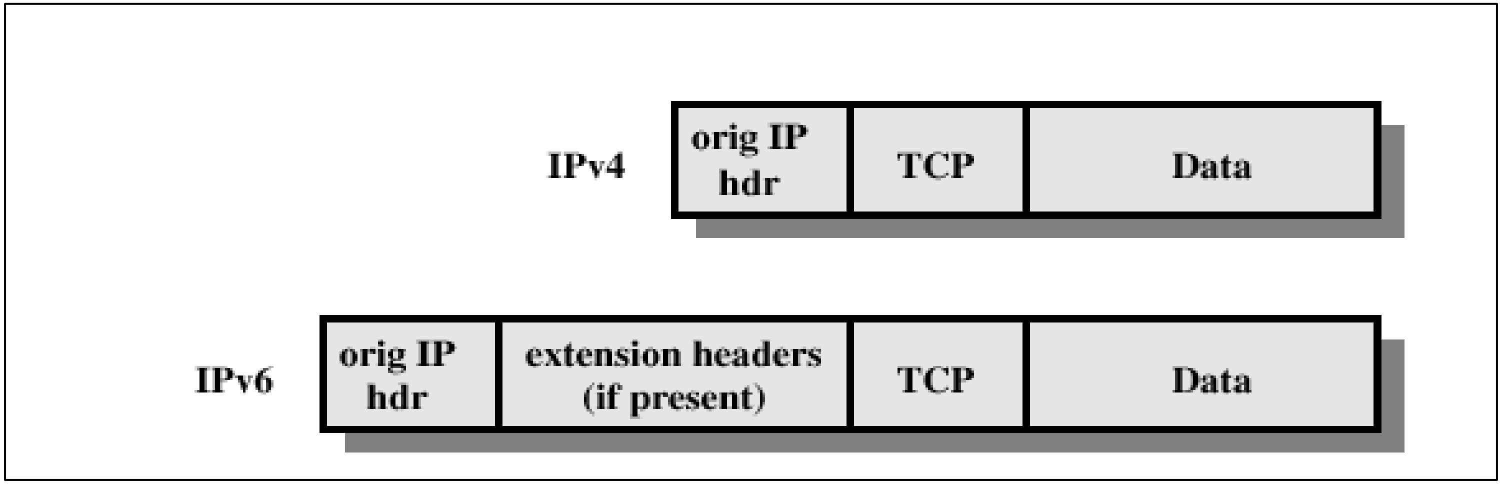
M

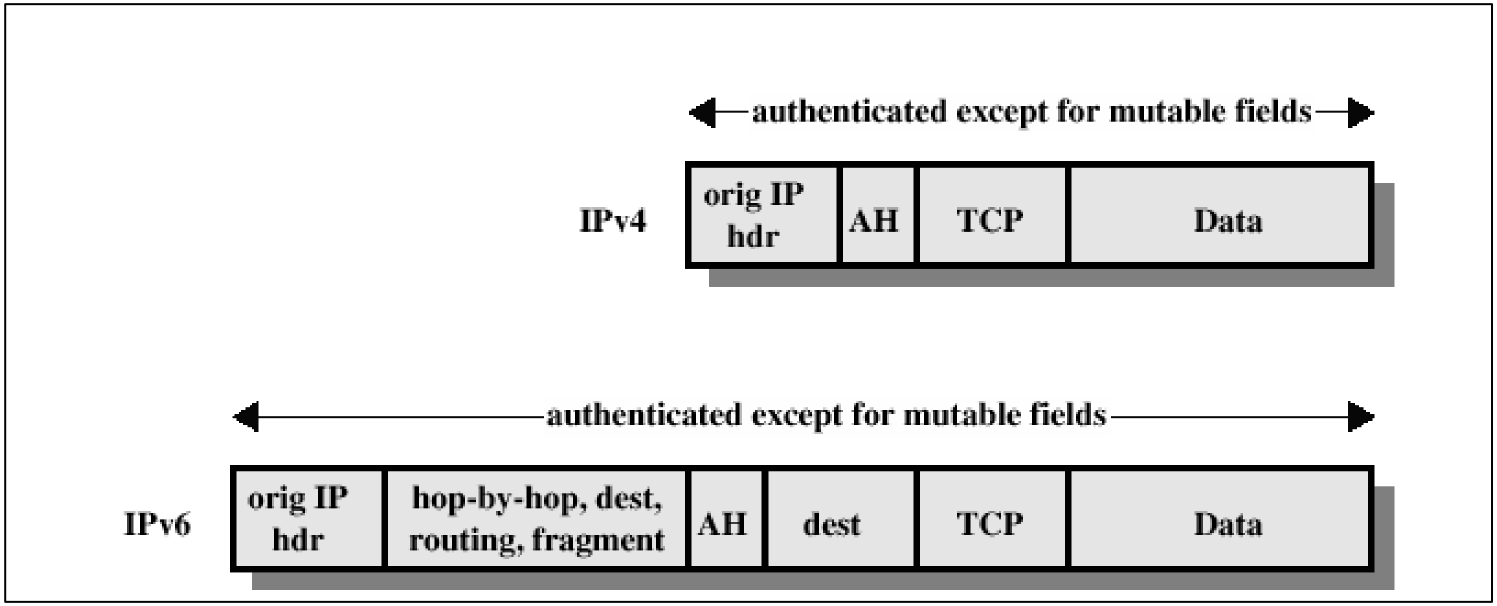


Transport versus Tunnel Mode

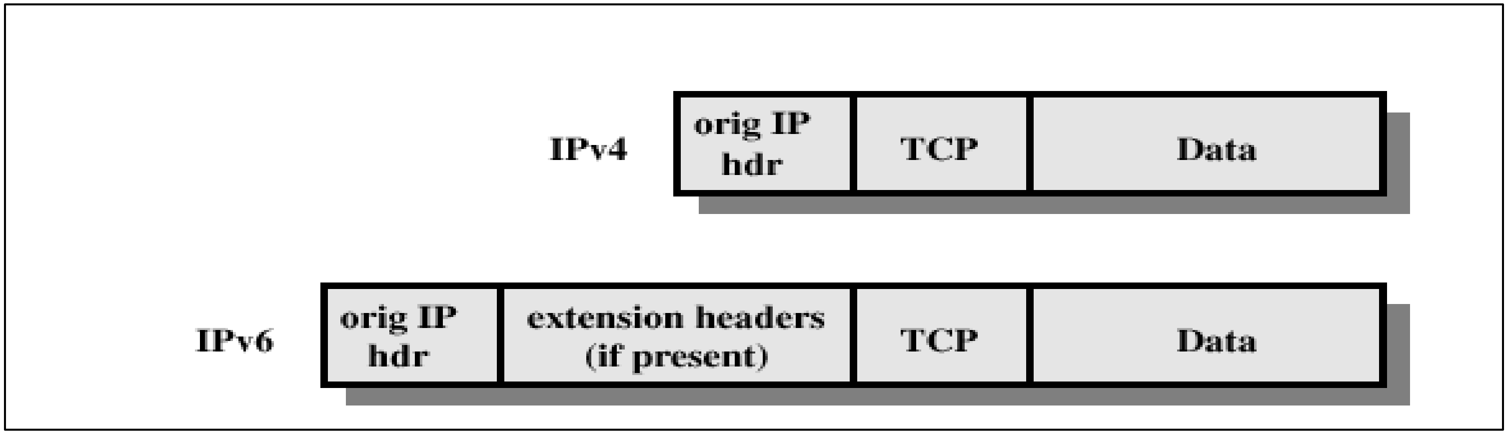
	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts inner IP packet. Authenticates inner IP packet.

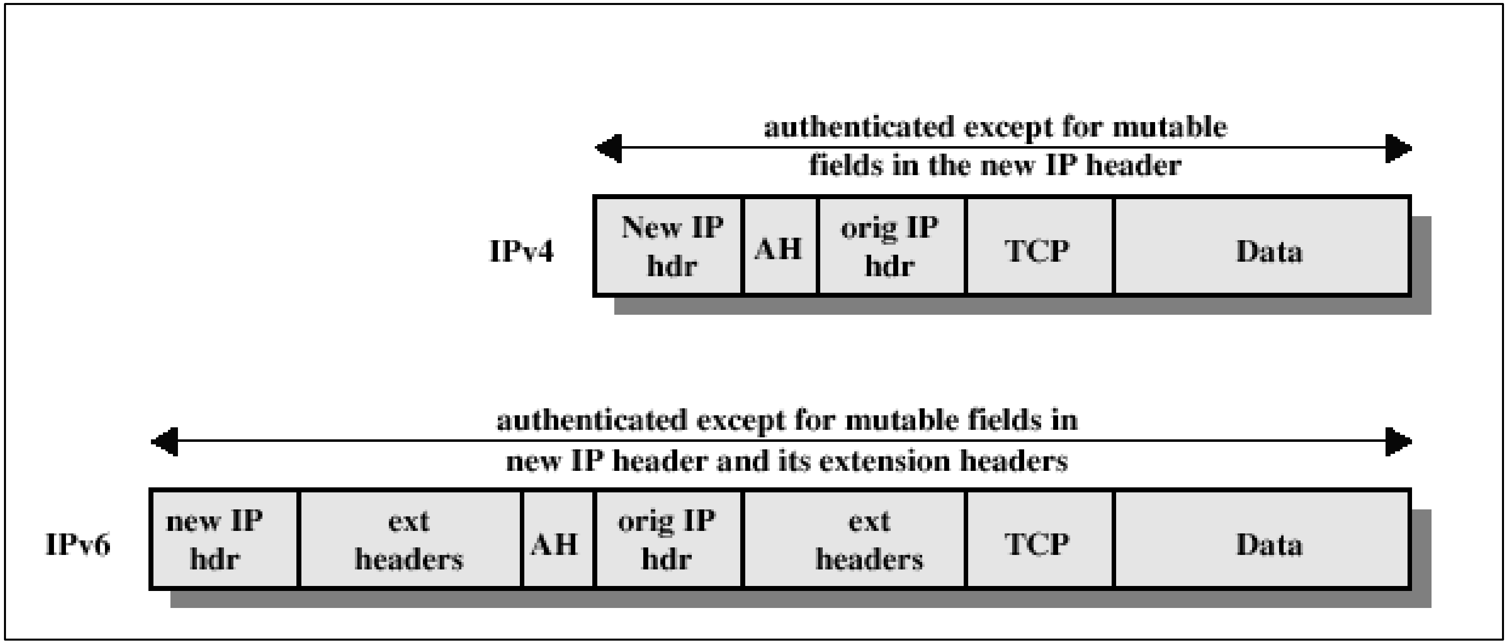
IPsec: AH in Transport Mode





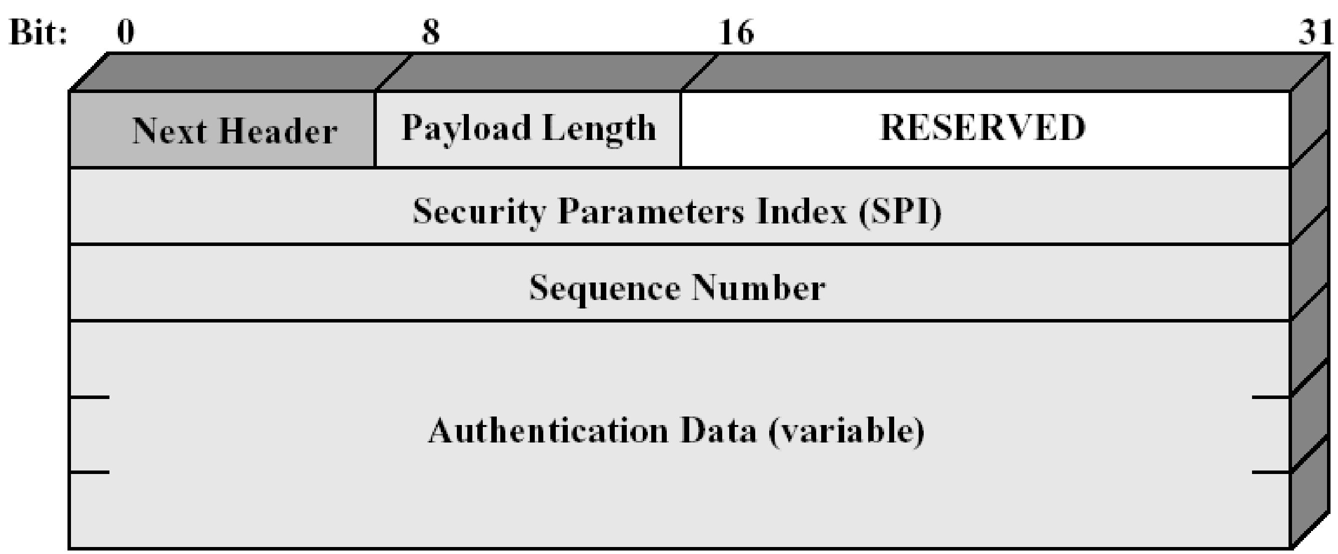
IPsec: AH in Tunnel Mode





The Authentication Header

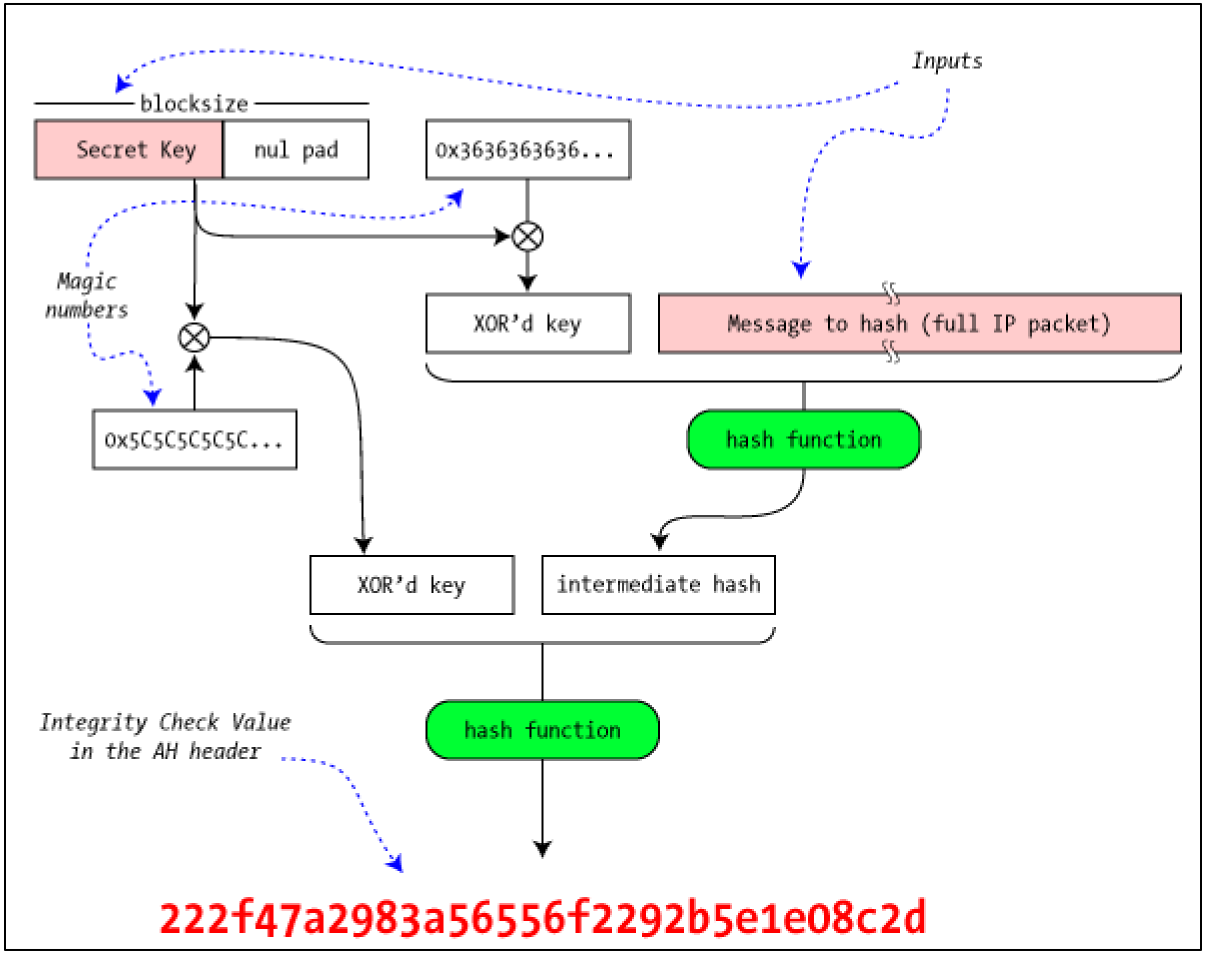
- AH provides data integrity and authentication for IP packets
- AH prevents address spoofing and replay attacks
- Authentication Data is based on keyed hash function (→ later), so both parties share a secret key



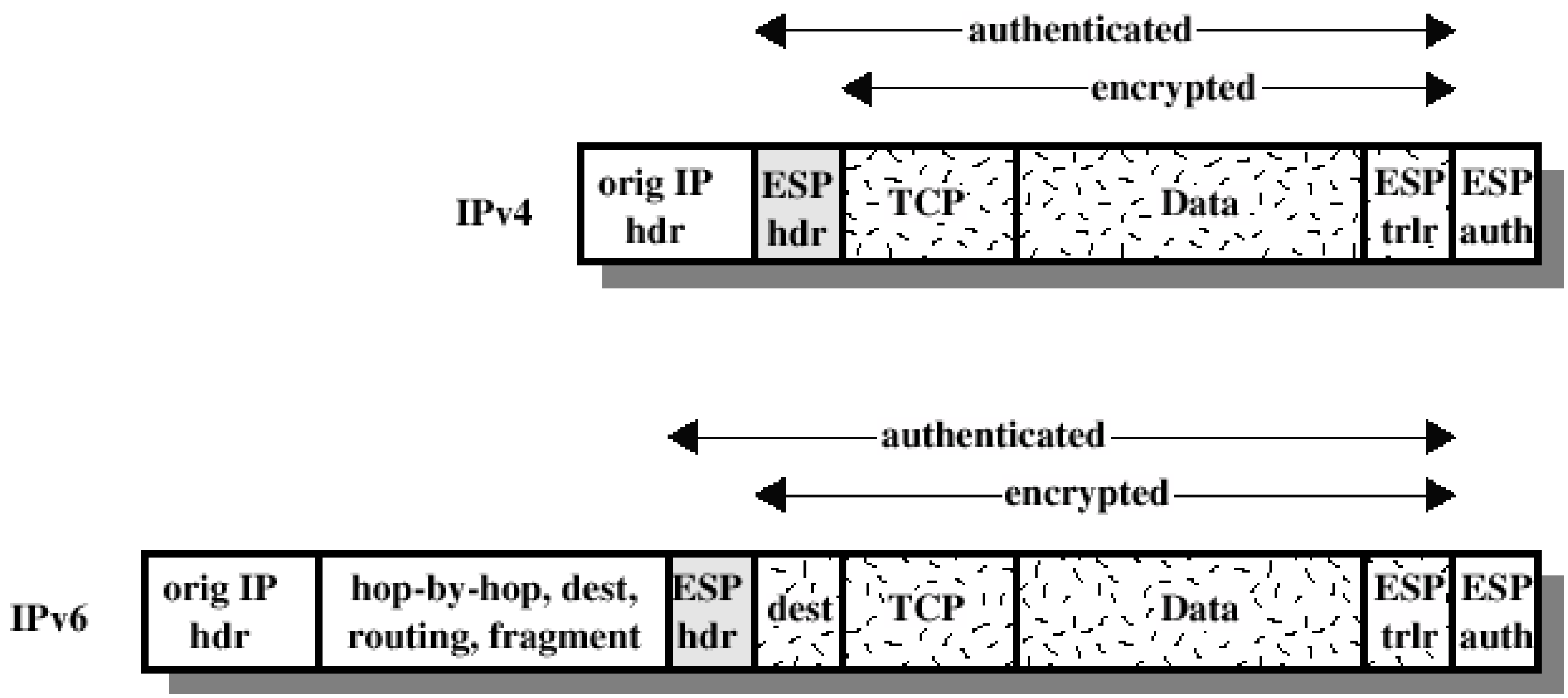
AH Fields

- **Next header** (8 bits): Identifies type of header following this header
- **Payload Length** (8 bits): Length of AH in 32-bit words minus 2
- **Reserved** (16 bits)
- **SPI** (32 bits): Identifies SA
- **Sequence Number** (32 bits): Unique incremented counter value
- **Authentication Data** (variable): Contains Integrity Check Value, i.e. the keyed hash value (next slide)

FYI: ICV for AH Authentication

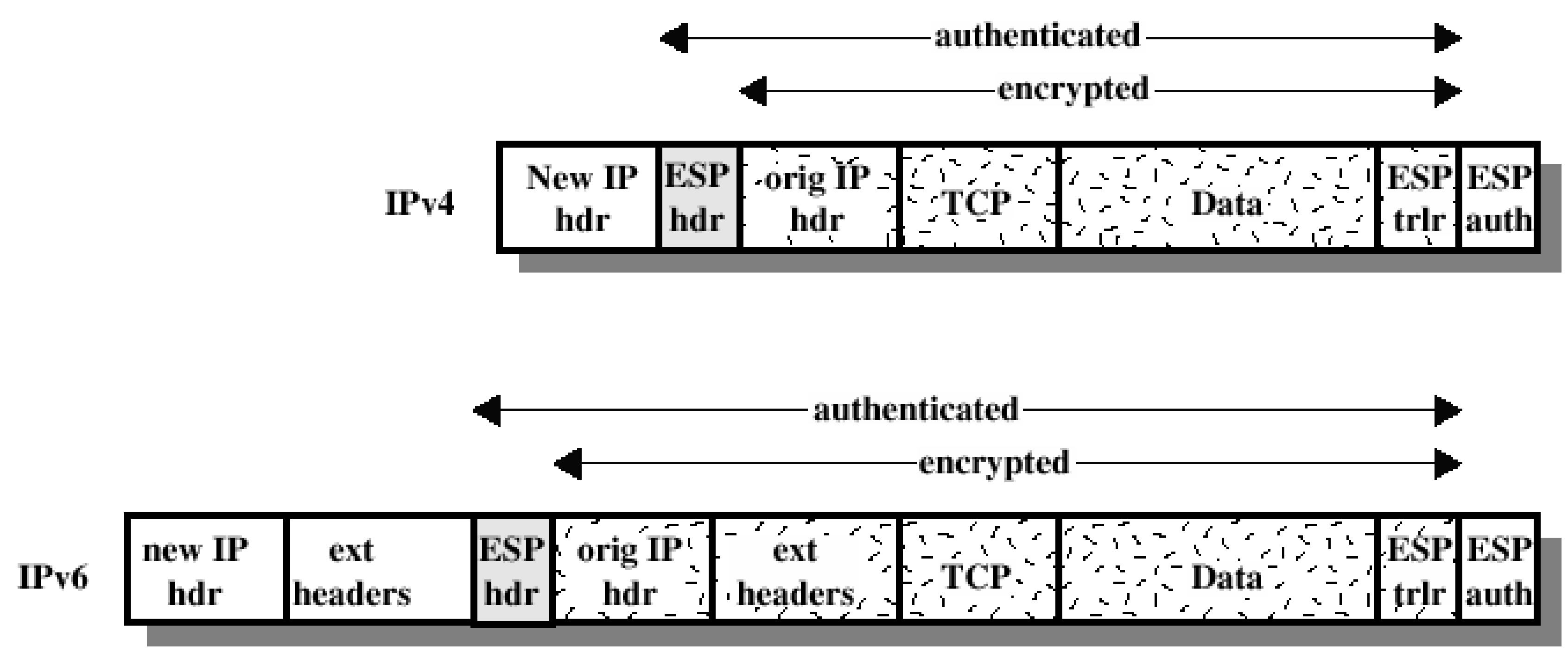


ESP Encryption and (optional) Authentication in Transport Mode



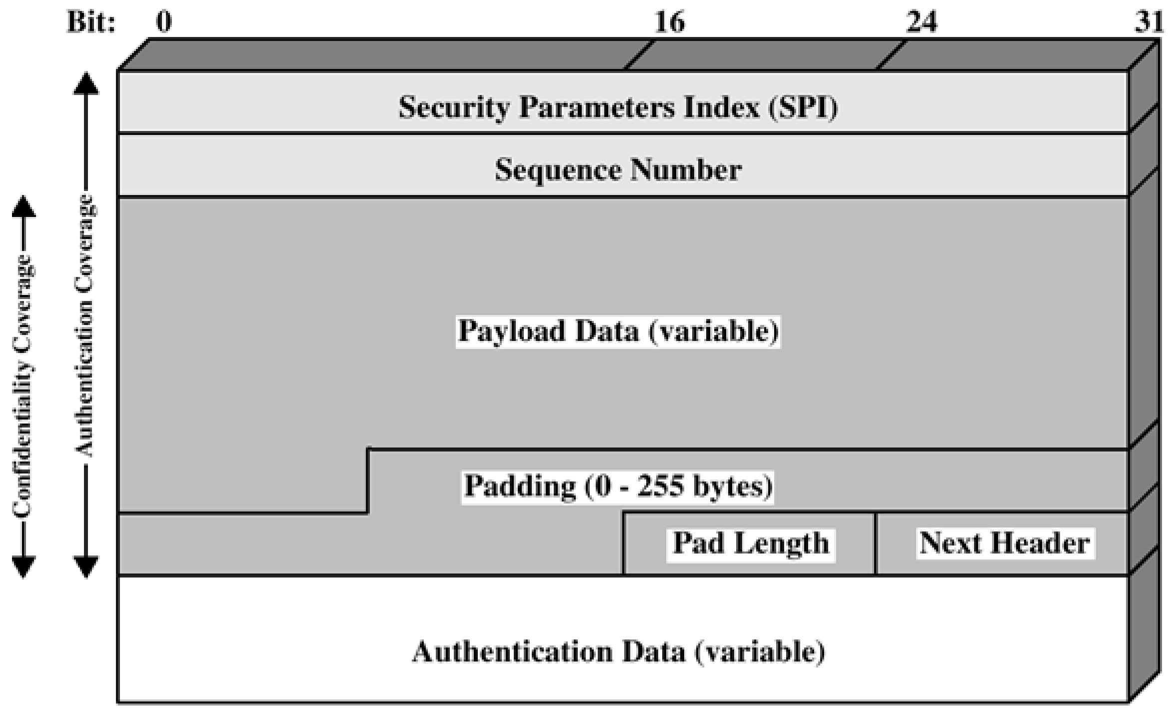
(a) Transport Mode

ESP Encryption and (optional) Authentication in Tunnel Mode



(b) Tunnel Mode

The IPsec ESP Header

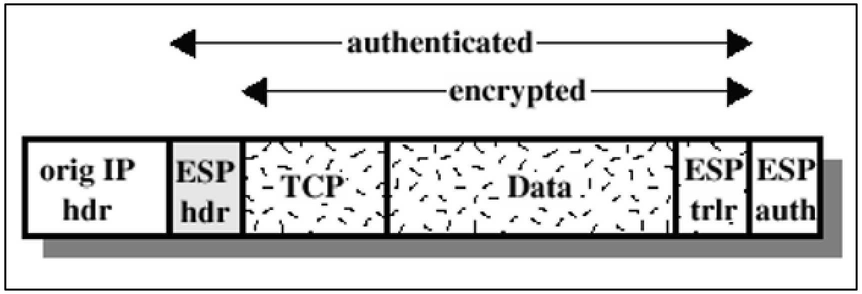


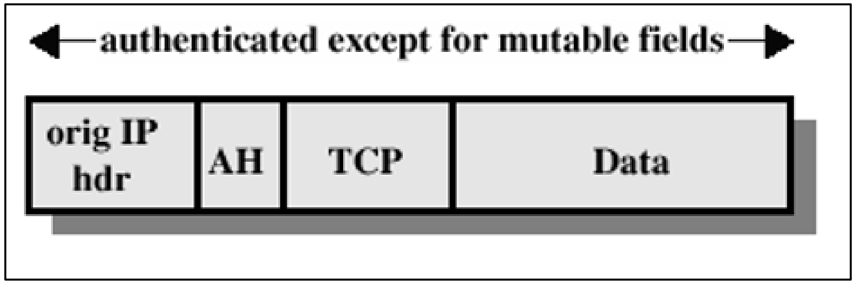
ESP Header and Trailer

- ESP provides encryption using Triple-DES (obsolete by 2025) or AES, in CBC mode
- ESP header contains SPI and sequence number
- Hatched fields contain encoded payload
- ESP trailer contains
  - padding bytes
  - padding length
  - next header field
- Optional ESP auth trailer contains authentication data

Combining Security Associations

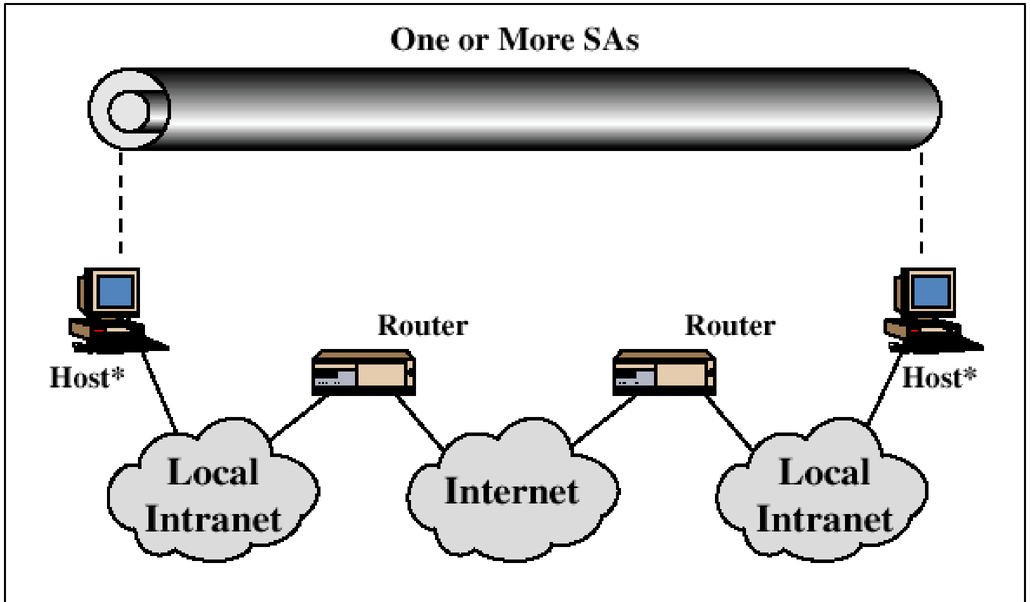
- SA are complementary and provide different scope in tunnel and transport mode
  - ESP+Auth (top) covers less fields than AH (bottom), as non-mutable fields of IP header are not covered
- Therefore, ESP and AH SA can be combined to provide more comprehensive encryption and authentication
- Likewise different SA can be applied at different locations, i.e. within different devices





Combining Security Associations

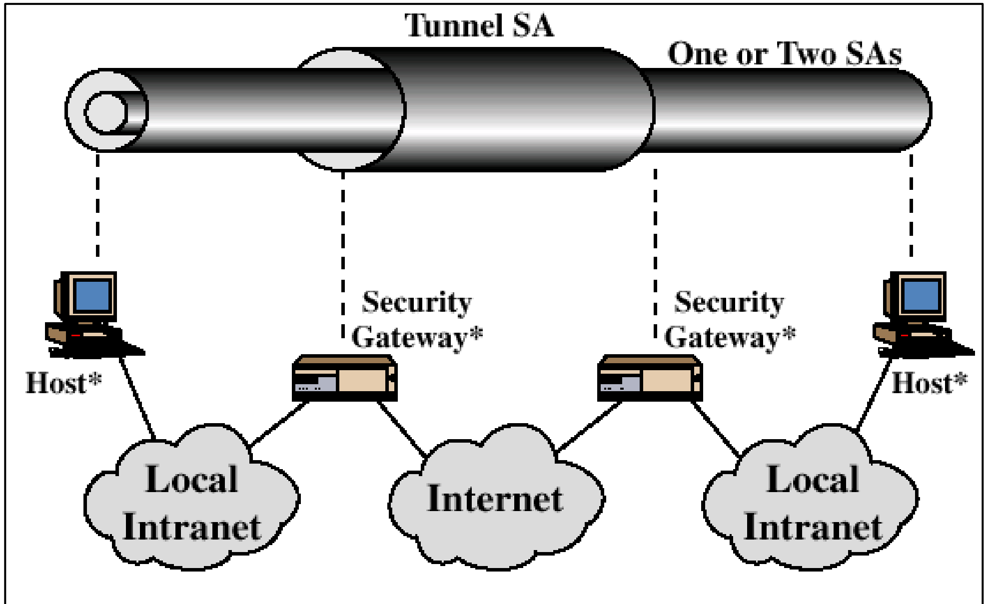
- AH-SA and ESP-SA bundled in transport mode, i.e. ESP-SA inside an AH-SA



(a) Case 1

Combining Security Associations

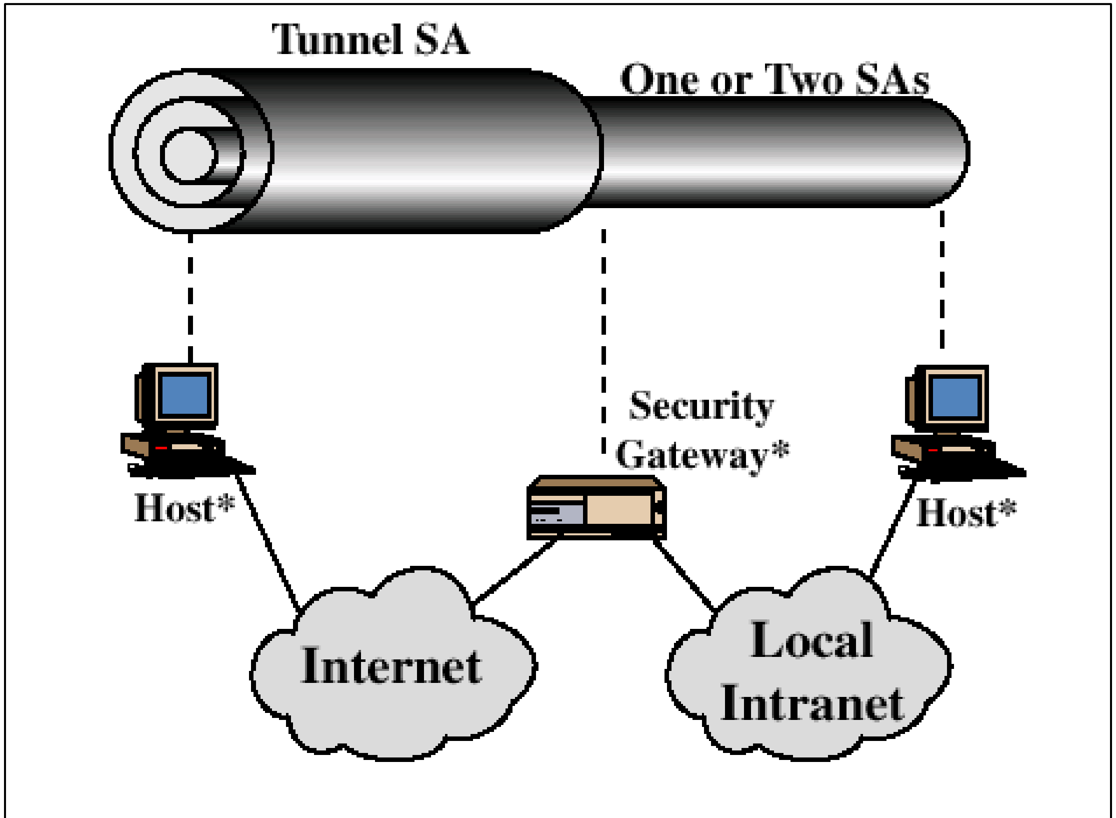
- VPN tunnel with added end-to-end security
- The gateway-to-gateway tunnel provides confidentiality and/or authentication
- Individual users can add any additional IPsec service to meet their needs



(c) Case 3

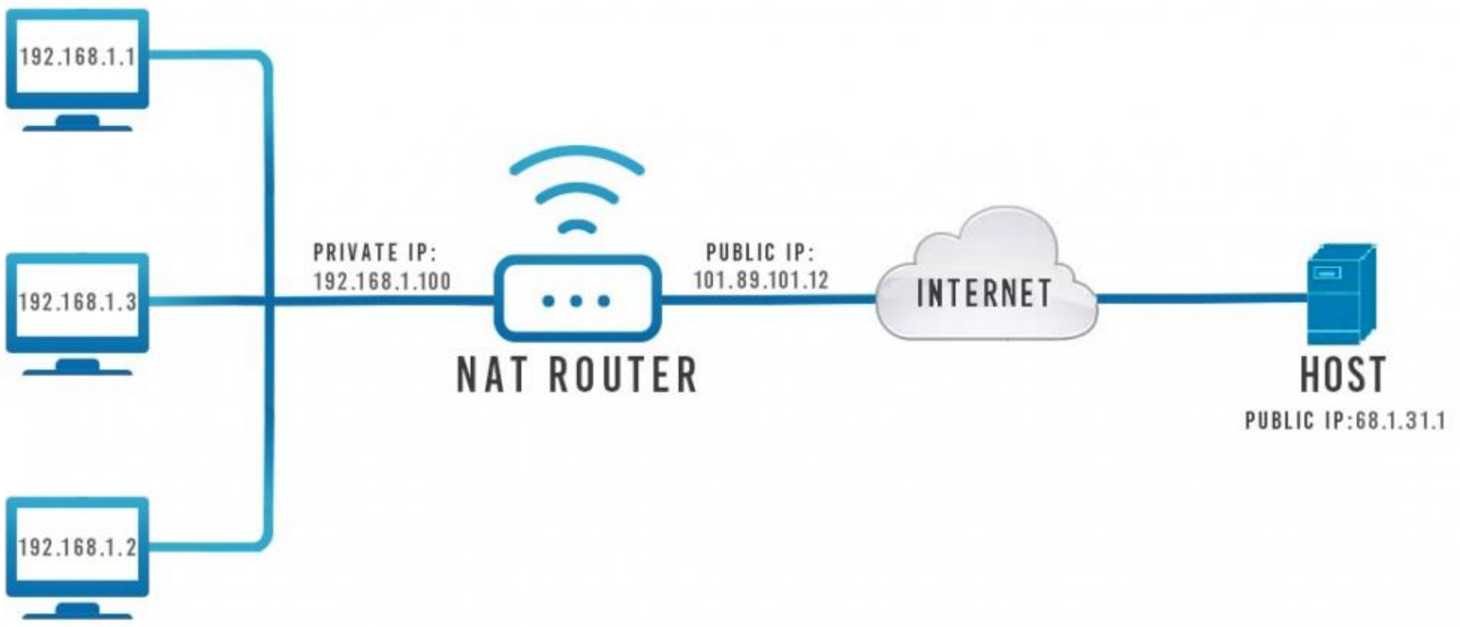
Combining Security Associations

- Remote host connection to server using tunnelling



(d) Case 4

Recap Network Address Translation (NAT)



NAT TABLE

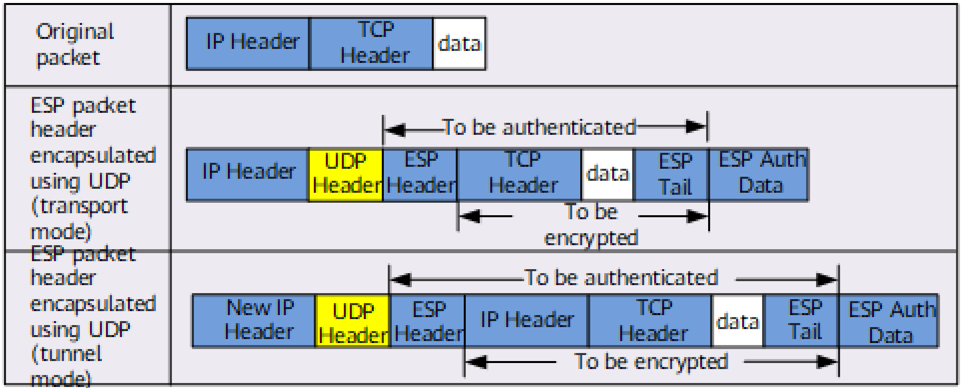
INSIDE PRIVATE IP:PORT	INSIDE PUBLIC IP:PORT	OUTSIDE PUBLIC IP:PORT
192.168.1.1:9688	101.89.101.12:8801	68.1.31.1:23
192.168.1.2:1253	101.89.101.12:5123	68.1.31.1:23
192.168.1.3:1025	101.89.101.12:102	68.1.31.1:23

IPsec and NAT

- With NAT a single public IP address can be shared by multiple endpoints (e.g. Wi-Fi network)
- This requires the NAT router (i.e., access point) to change the sender’s
  - IP address in the IP header
  - port number in the transport layer header (UDP or TCP)
- If IPSec is installed on a client, this causes problems:
  - In AH, the datagram authentication by the receiver will fail
  - In ESP, the NAT router cannot change the encrypted port number

IPsec and NAT Traversal

- NAT traversal is a technique that allows IPSec ESP to work with a NAT router
- It adds a UDP header and a special payload to the IPSec packet, which makes it look like a normal UDP packet to the NAT router
- The router can then perform the address translation on the UDP header, without affecting the IPSec payload
- The IPSec receiver endpoint can then remove the UDP header and process the IPSec packet normally



Summary

- Network security (i.e., data encryption and / or authentication) is important for obvious reasons
- The layered structure of the TCP/IP stack allows positioning the extra security layer in different levels
- Each of these options has its advantages and disadvantages / limitations, for example with regard to
  - the portions of a packet that can be secured
  - Compatibility with network routing, NAT, etc.
- IPsec provides one possible option with encryption / authentication taking place on network layer