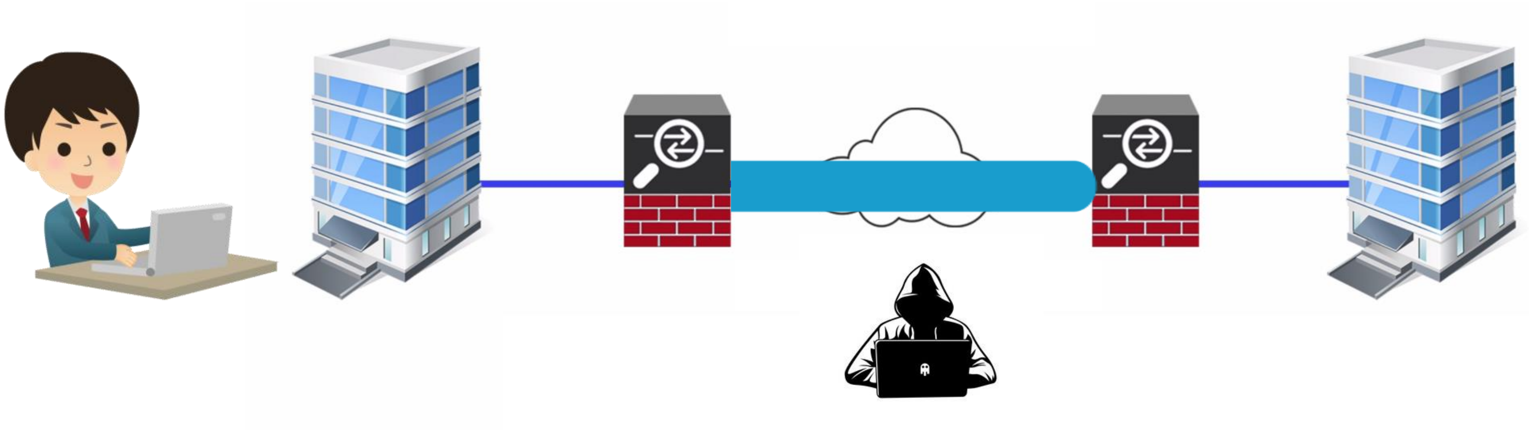


Computer Security

Network Security (IPSec protocol)

Security is always excessive until it’s not enough.
-Robbie Sinclair

Tamer ABUHMED
Department of Computer Science & Engineering
Sungkyunkwan University

SUNG KYUN KWAN UNIVERSITY

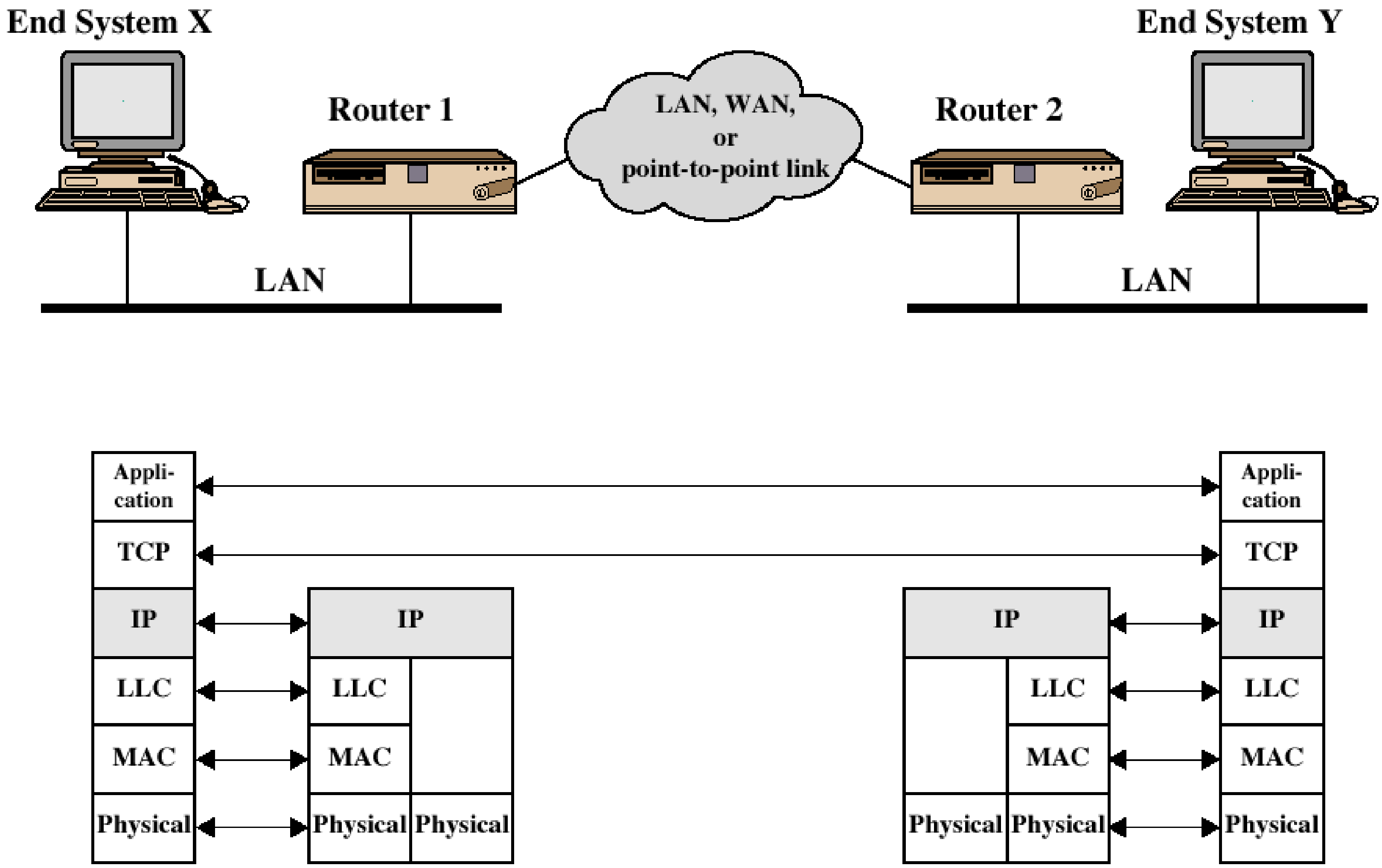
Outline

- Internetwork Protocol (IP)
- IPv4 , IPv6
- IPSec overview
- IPSec Protocols
- IPSec Modes
- Key Management in IPSec
- Key Exchange in IPSec

Internetwork Protocol (IP)

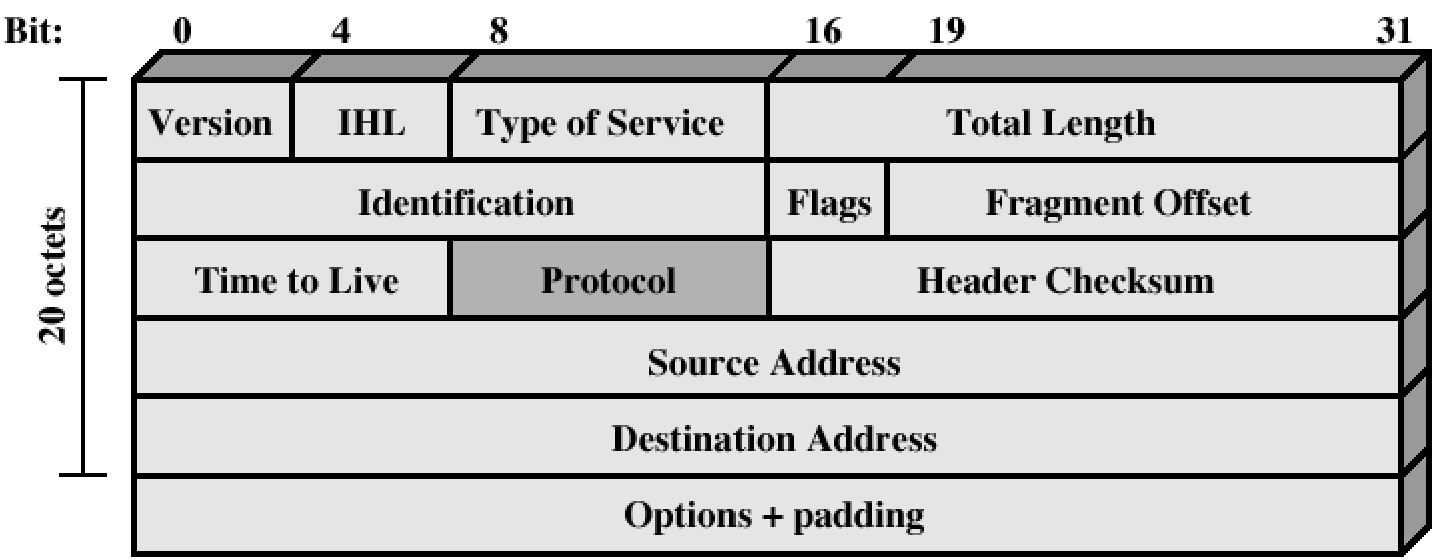
- Aim
  - provide interconnection across different networks
- implemented in every end user and in routers
- IP is an unreliable protocol
  - IP datagrams may be lost
  - IP datagrams may arrive out of order
  - TCP takes care of those problems

Internetwork Protocol (IP)



IPv4

- The IP version that we are currently using on SU campus
  - actually most IP networks are IPv4



(a) IPv4 Header

Data (Payload) follows the header

IPv6

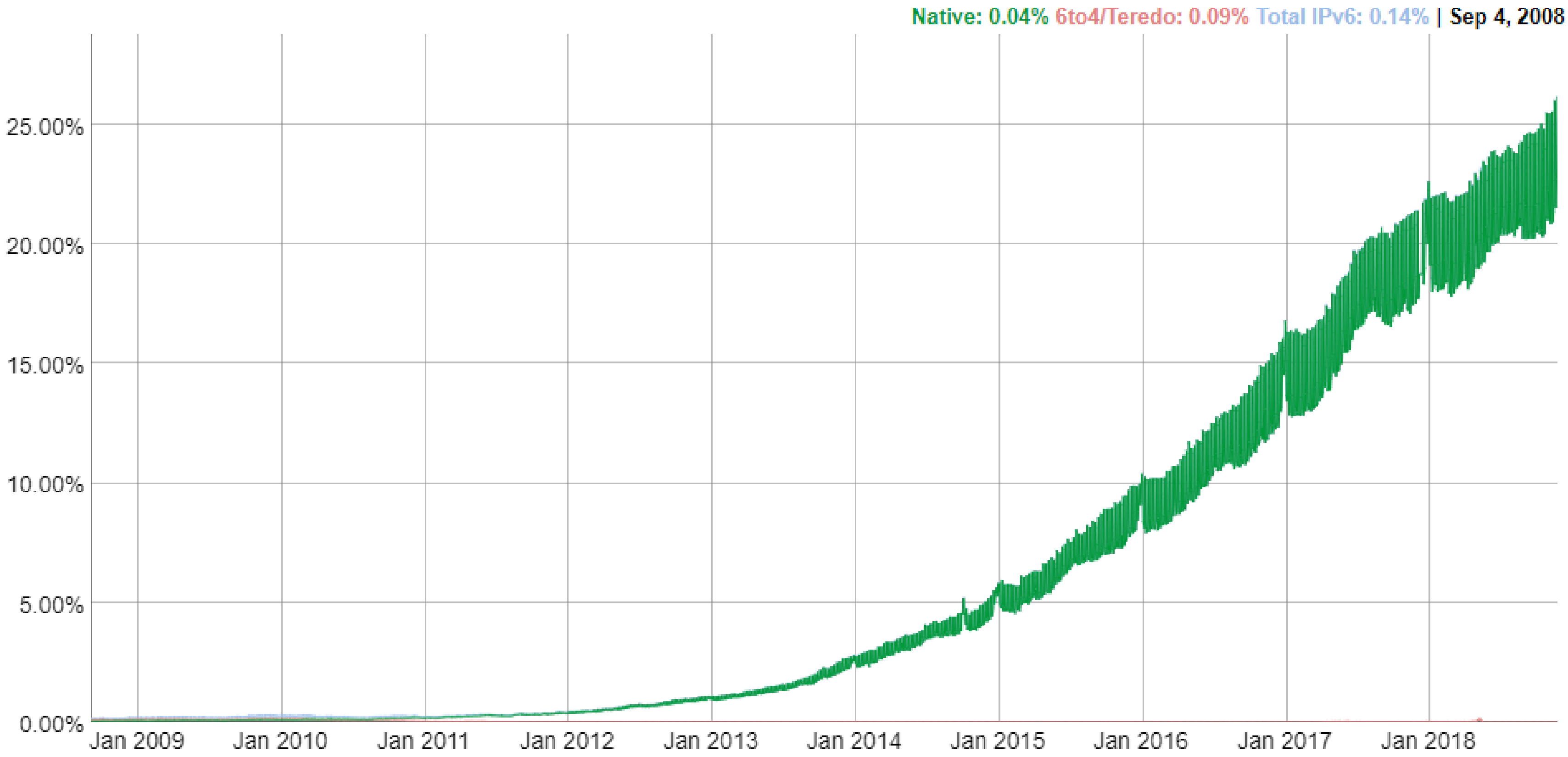
- Next generation IP
  - driving force was the inadequateness of IPv4 address space
- IPv6 header
  - modular approach
  - base header + extension headers
  - base header is longer than v4, but number of fields is smaller

IPv6

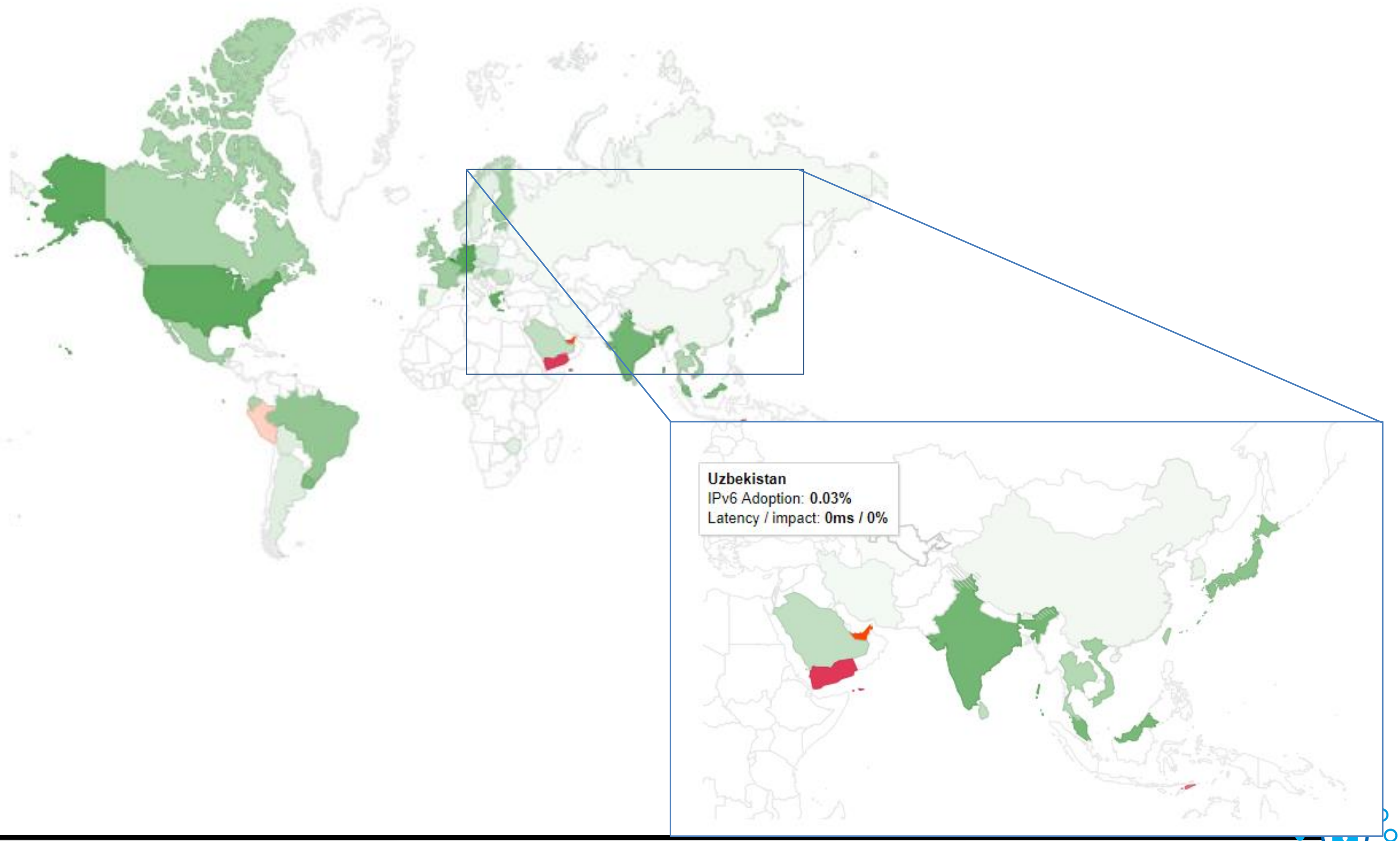
Google collects statistics about IPv6 adoption in the Internet

IPv6 Adoption

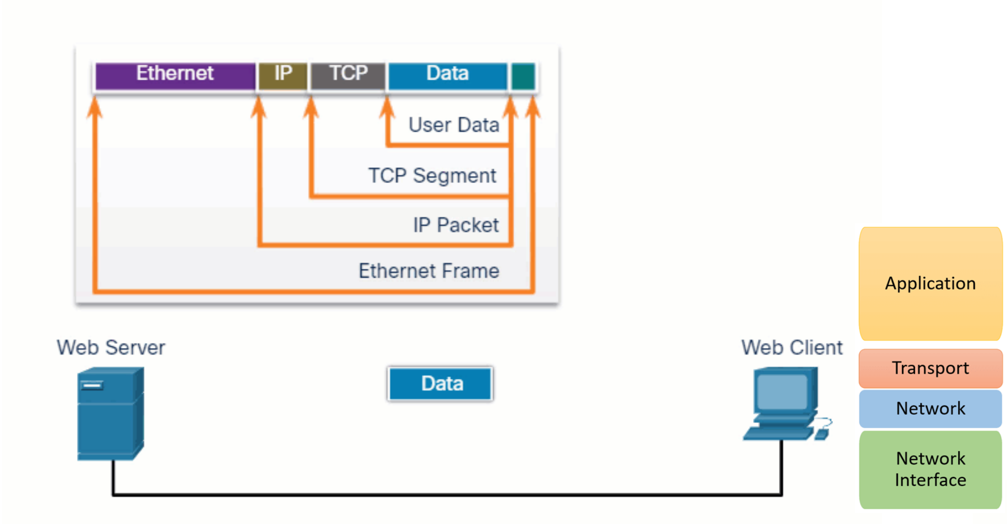
We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.

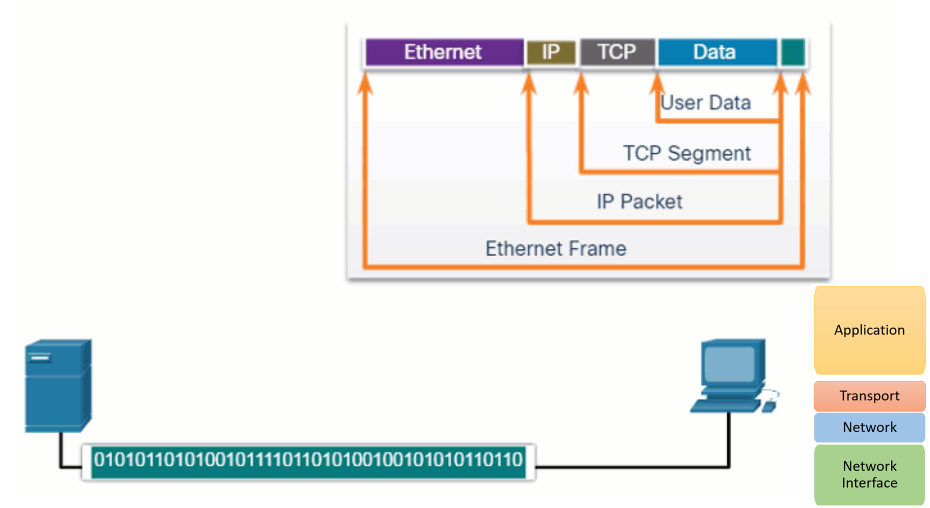


IPv6 World wide

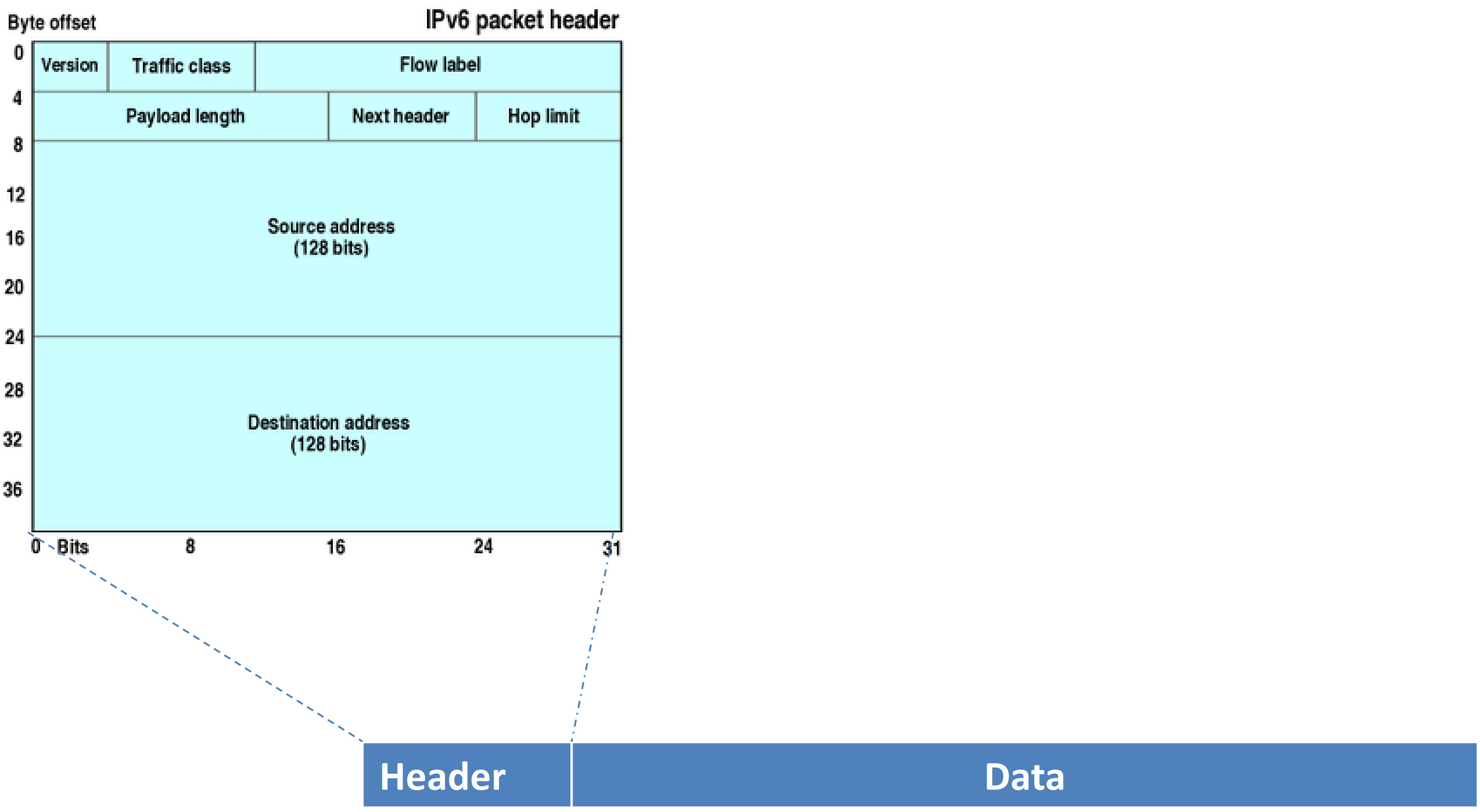


Network


Ethernet
IP
TCP
Data
User Data
TCP Segment
IP Packet
Ethernet Frame
Web Server
Data
Web Client
Application
Transport
Network
Network Interface


Ethernet
IP
TCP
Data
User Data
TCP Segment
IP Packet
Ethernet Frame
0101011010100101111011010100100101010110110
Application
Transport
Network
Network Interface

IPv6 header



Byte offset
IPv6 packet header
0
4
8
12
16
20
24
28
32
36
Version
Traffic class
Flow label
Payload length
Next header
Hop limit
Source address
(128 bits)
Destination address
(128 bits)
0
Bits
8
16
24
31
Header
Data

Is IP Secure?

- Content (Payload) is not encrypted
  - confidentiality is not provided
  - IP sniffers are available on the net
- IP addresses may be spoofed
  - authentication based on IP addresses can be broken
- So IP is not secure

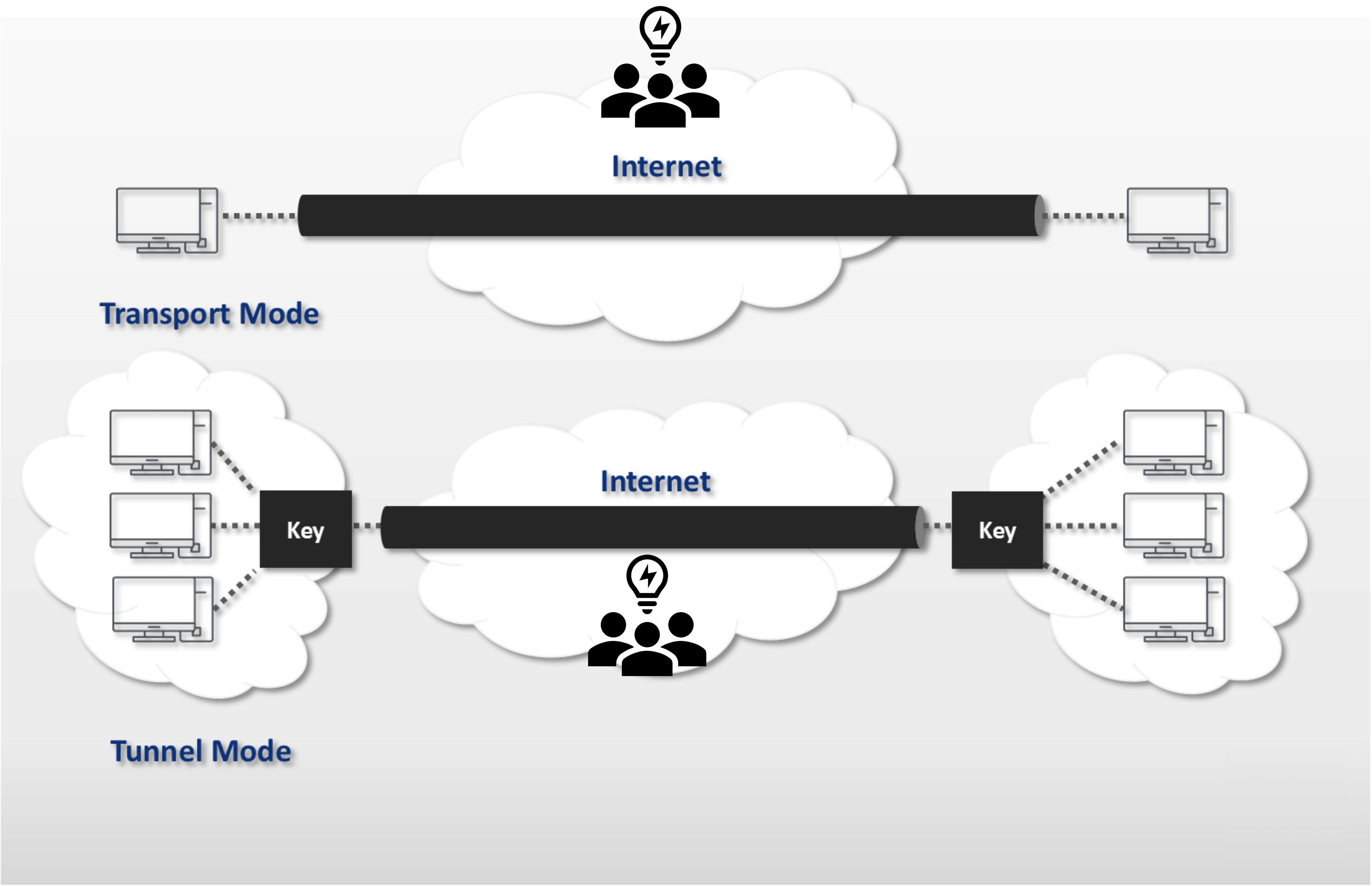
Where to provide security?

- Application-layer?
  - S/MIME, PGP – email security
  - Kerberos – client / server
  - SSH – secure telnet
- Transport level?
  - SSL / TLS
  - between TCP and Application
- IP level
  - IPSec

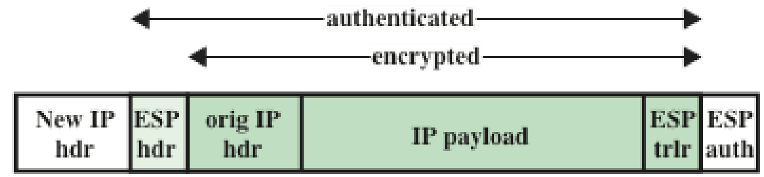
IPSec

- general IP Security mechanisms
- provides authentication and confidentiality at IP level
  - also has key management features
- Applications
  - VPNs (Virtual Private Networks)
    - Interconnected LANs over the insecure Internet
    - router-to-router
  - Secure remote access, e.g. to ISPs
    - individual-to-router
- IPSec support is mandatory for IPv6 products, optional for v4
  - many manufacturers support IPSec in their v4 products

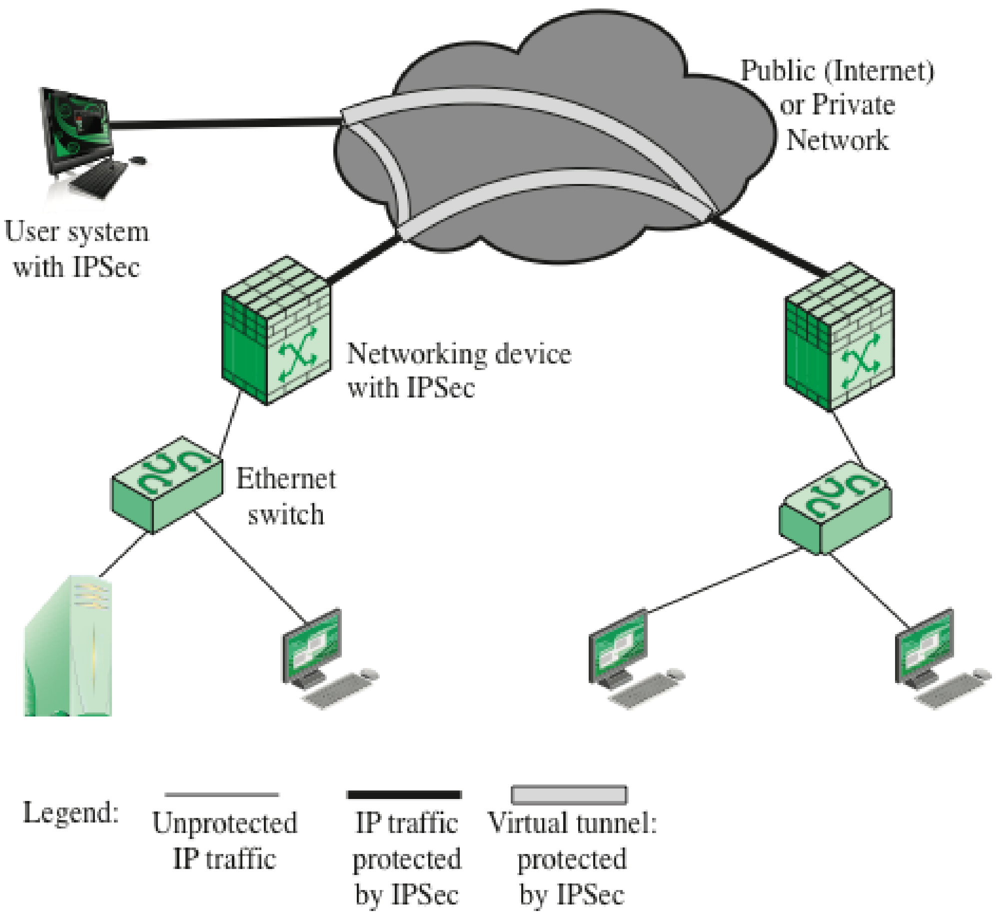
IPSec



IPSec Application Scenarios



(a) Tunnel-mode format

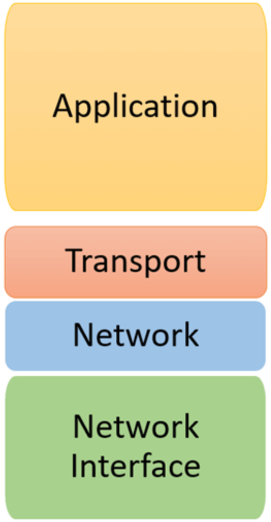


(b) Example configuration

Benefits of IPSec

- in a firewall/router, IPSec provides strong security to all traffic entering the network
  - without passing the security overhead to the internal network and workstations
  - user transparent: no need to assume security-aware users, no per-user keys

- IPSec is below transport layer
  - transparent to applications
  - No need to upgrade applications when IPSec is used, if IPSec is implemented and configured in user machines



IPSec Documentation and Standards

- IPSec and its specifications are quite complex
- defined in numerous RFCs
  - most important RFCs are 4301 (Overview of security architecture), 4302 (AH - Authentication Header), 4303 (ESP – Encapsulating Security Payload – for encryption), 7296 (IKEv2 – Key Management)
  - many others, see IETF IPSec Working Group website
    - http://datatracker.ietf.org/wg/ipsec/charter/

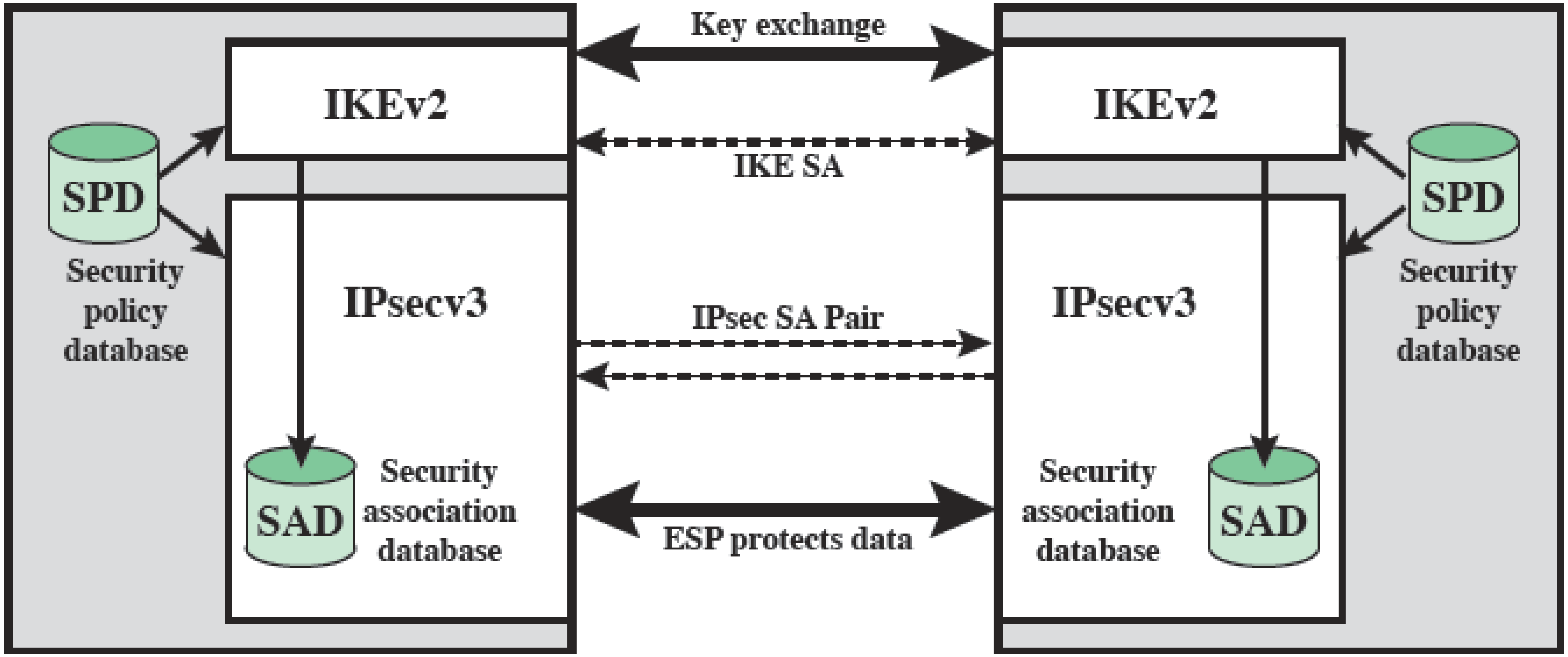
IPSec Protocols

- Authentication Header (AH)
  - defines the **authentication** protocol
  - no encryption
  - Since ESP covers authentication, it is not recommended anymore
    - But we will talk about it
- Encapsulating Security Payload (ESP)
  - provides **encryption**
  - optionally **authentication**
- Crypto algorithms that support those protocols are generally defined in the protocol documentation
- Key distribution and management are also in different RFCs

IPSec Services

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

IPSec General Architecture (Big Picture)



Security Associations (SA)

- a one-way relationship between sender & receiver
  - specifies IPSec related parameters
- Identified by 3 parameters:
  - Destination IP Address
  - Security Protocol: AH or ESP
  - Security Parameters Index (SPI)
    - A local 32-bit identifier (to be carried later to endpoints within AH and ESP)
- There are several other parameters associated with an SA
  - stored locally in Security Association Databases (SAD)

SA Parameters (some of them)

- Anti-replay related
  - Sequence Number Counter
    - to generate sequence numbers
  - Anti-replay window
    - something like sliding-window; will be discussed later.
- AH info
  - authentication algorithms, keys, key lifetimes, etc.
- ESP info
  - encryption (and authentication) algorithms, keys, key lifetimes, etc.
- Lifetime of SA
- IPSec Mode: Transport or Tunnel

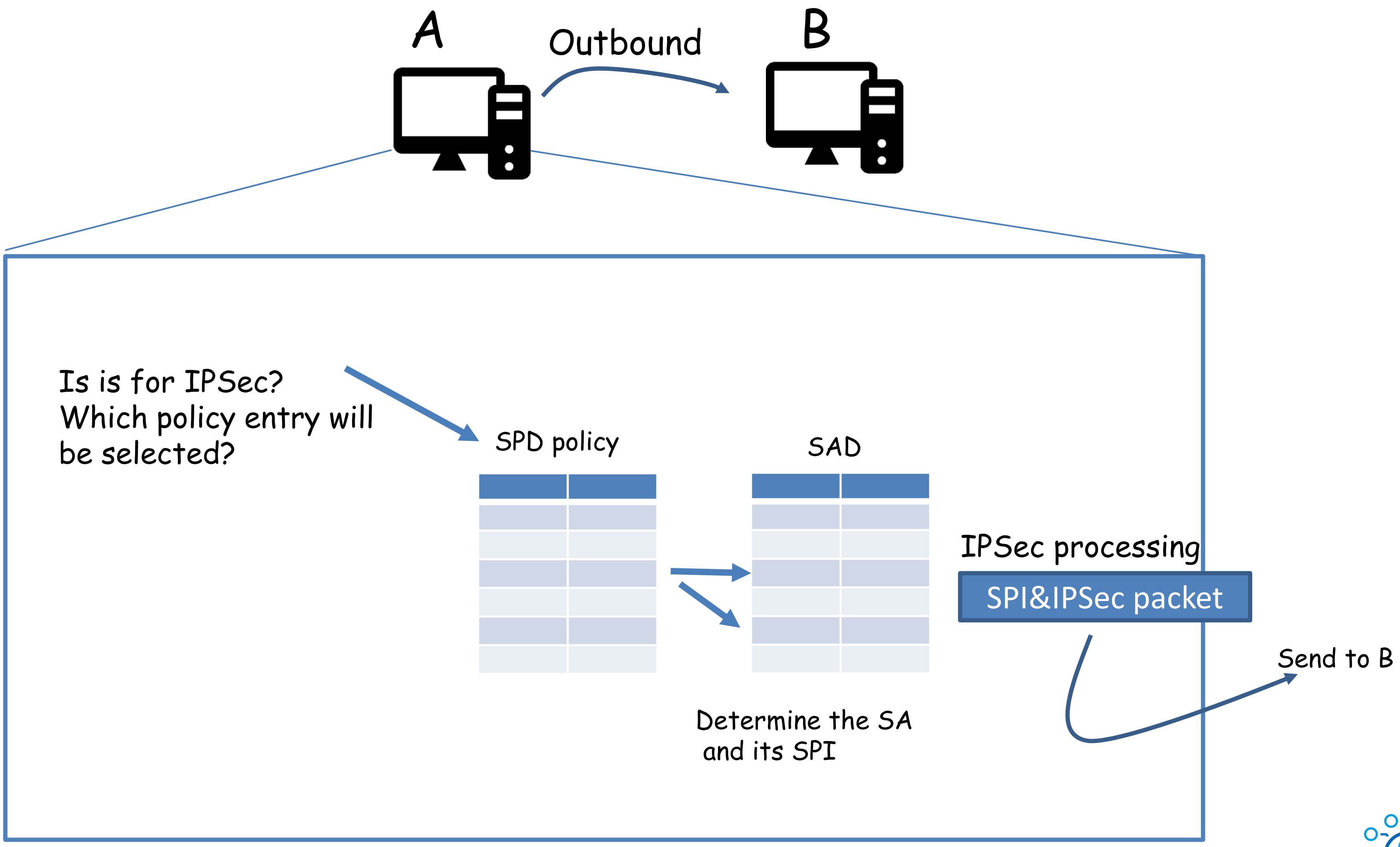
SA, AH – ESP, and key management

- SAs are in databases
  - both in sender and receiver
- AH and ESP use the cryptographic primitives and other info in SA
- Key Management Protocols (will discuss later) are to establish SA
- So
  - AH / ESP are independent of key management

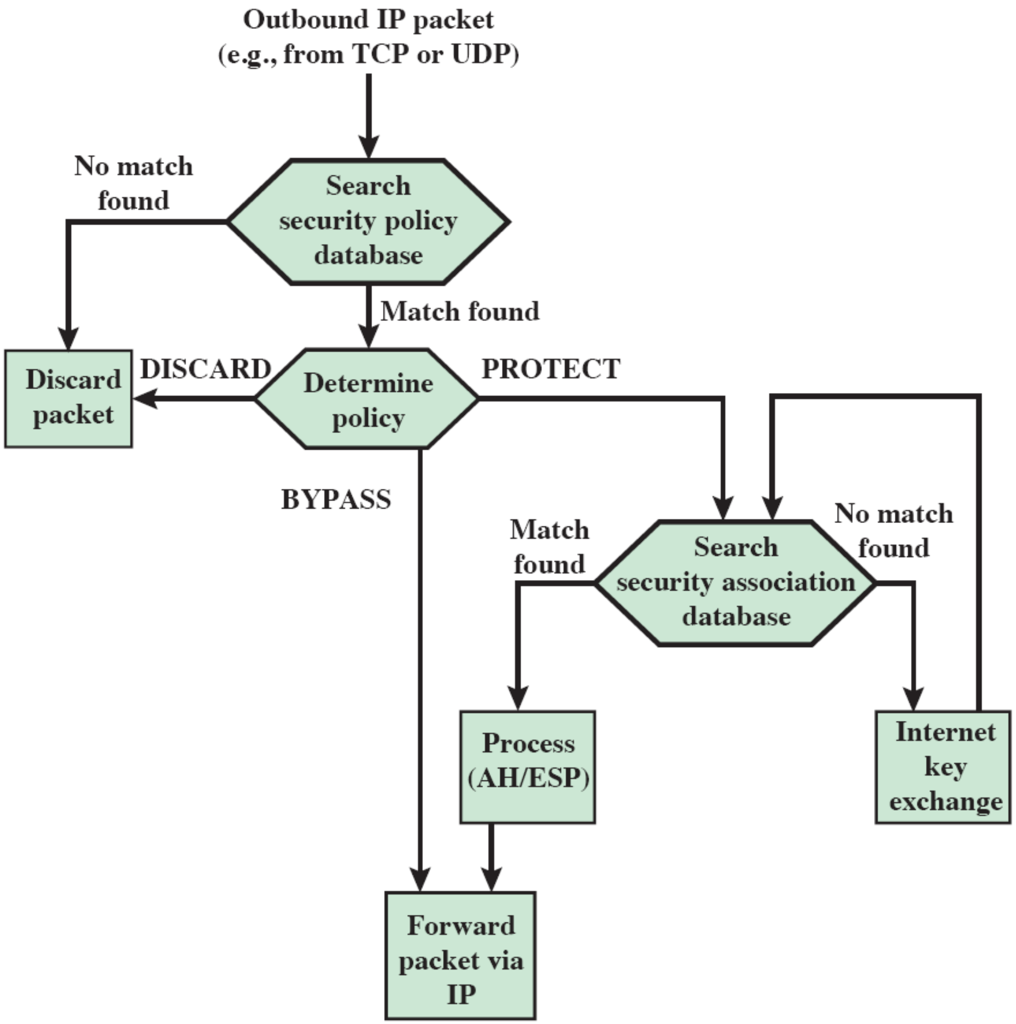
SA Selectors

- IPSec is a flexible protocol
  - traffic from IP address X to IP address Y may use several SAs
    - or no SA if that particular traffic will not be secured
- Security Policy Database (SPD) is used to assign a particular IP traffic to an SA
  - fields of an SPD entry are called selectors
- Outbound processing
  - compare the selector fields of SPD with the one in the IP traffic
  - Determine the SA, if any
  - If there exists an SA, do the AH or ESP processing
- Inbound processing
  - Check the incoming IPSec packet and process with AH or ESP
  - Discard in case of an anomaly

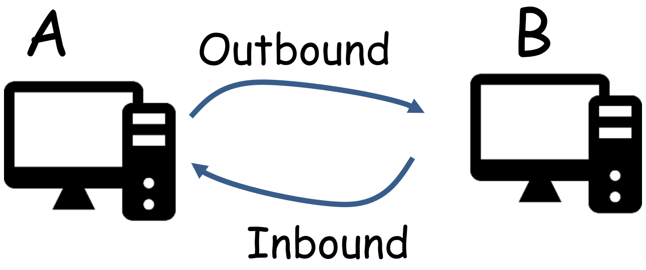
Outbound Processing Model



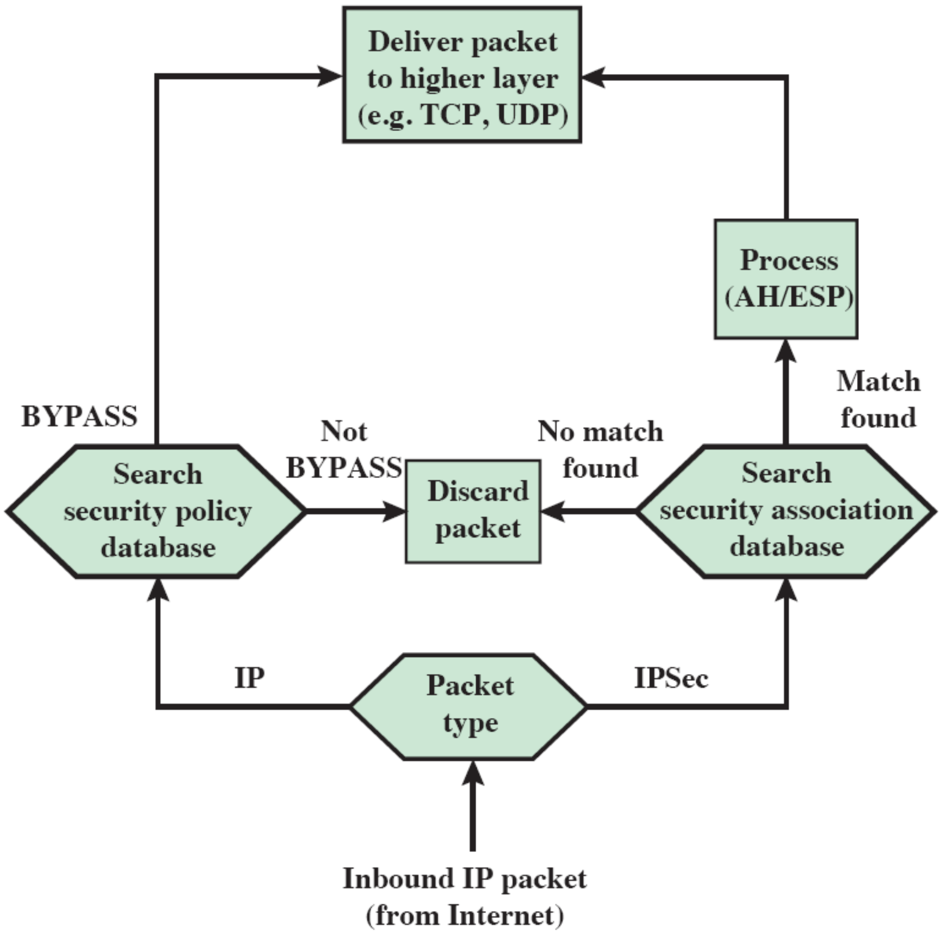
Outbound Processing Model



Inbound Processing Model



Inbound traffic is the traffic coming to computer A



Some SA Selectors

- Destination and Source IP addresses
  - range, list and wildcards allowed
- Transport Layer Protocol
  - TCP, UDP, ICMP, all
- Source and Destination Ports
  - list and wildcards allowed
  - from TCP or UDP header
- etc.

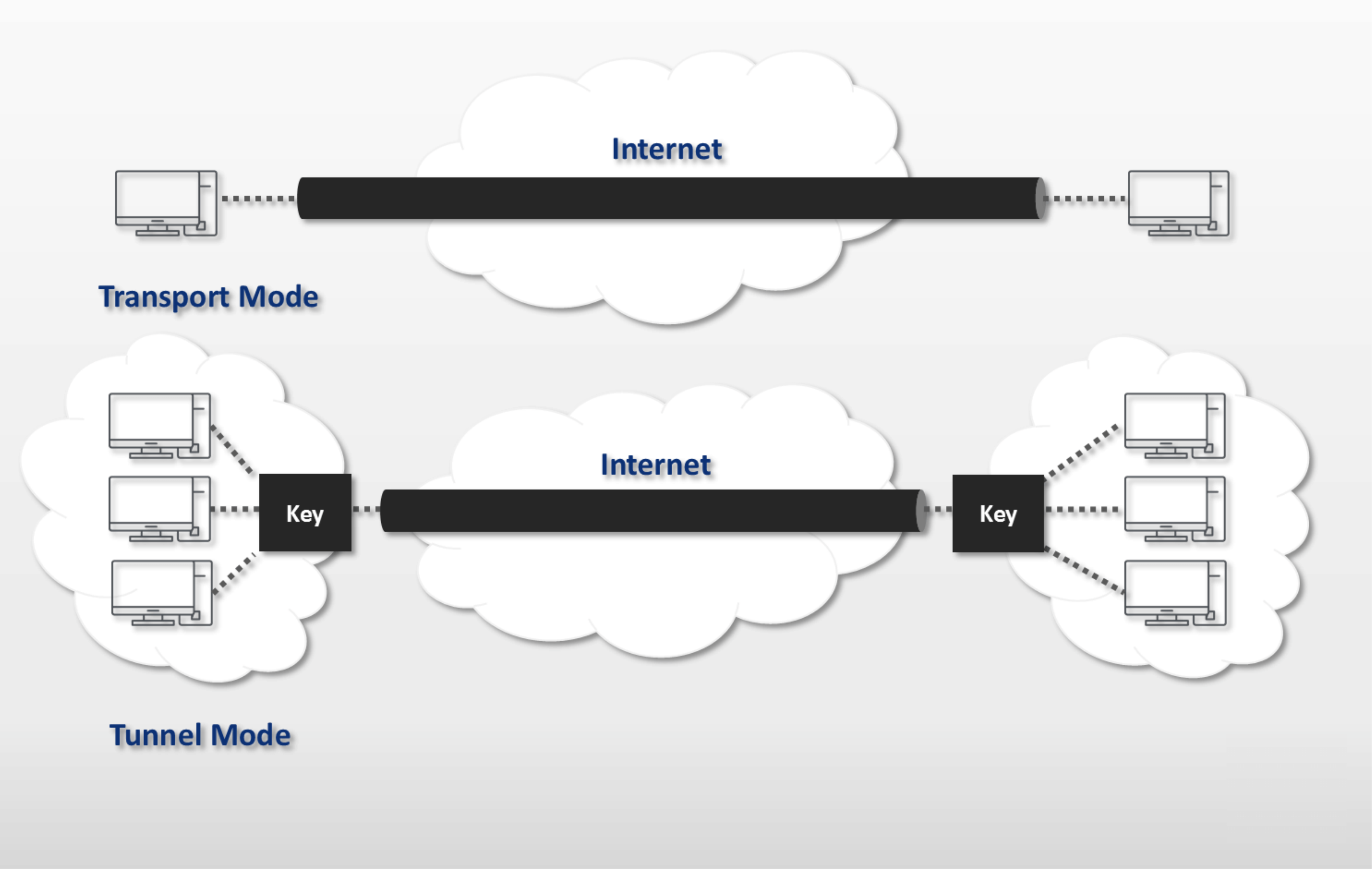
Host (IP Addr: 1.2.3.101) SPD Example

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Transport and Tunnel Modes

- Both AH and ESP support these two modes
  - differently (will see later)
- Transport Mode
  - security is basically for the IP payload (upper-level protocol data)
  - IP header is not protected (except some fields in AH)
  - Typically for end-to-end communication
- Tunnel Mode
  - secures the IP packet as a whole incl. header(s)
  - actually puts all IP packet within another (outer) one
  - packet is delivered according to the outer IP header
  - Typically for router-to-router, or firewall-to-firewall communication

IPSec modes



Authentication Header (AH)

- Provides support for data integrity and authentication of IP packets
  - malicious modifications are detected
  - address spoofing is prevented
  - replays are detected via sequence numbers
- Authentication is based on use of a MAC
  - parties must share a secret key
    - in SA

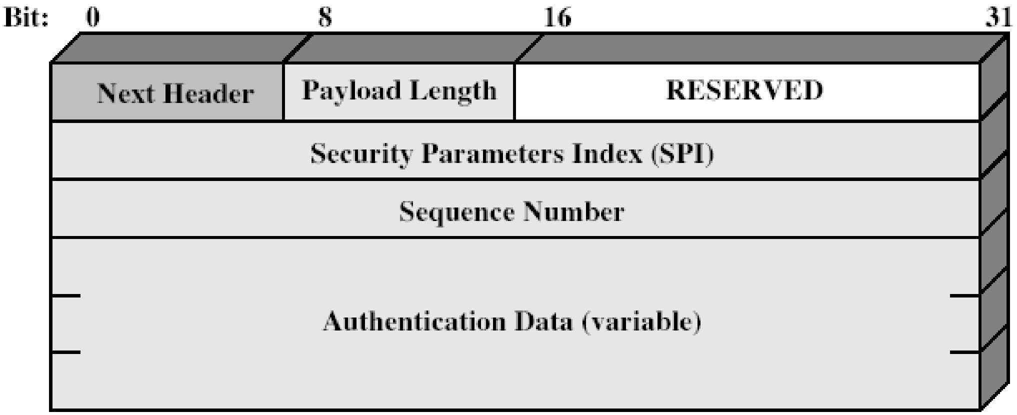
Authentication Header

Next Header: specifies next header or upper layer protocol

Payload length: to specify header length

SPI: to identify SA

Sequence number: used for replay control



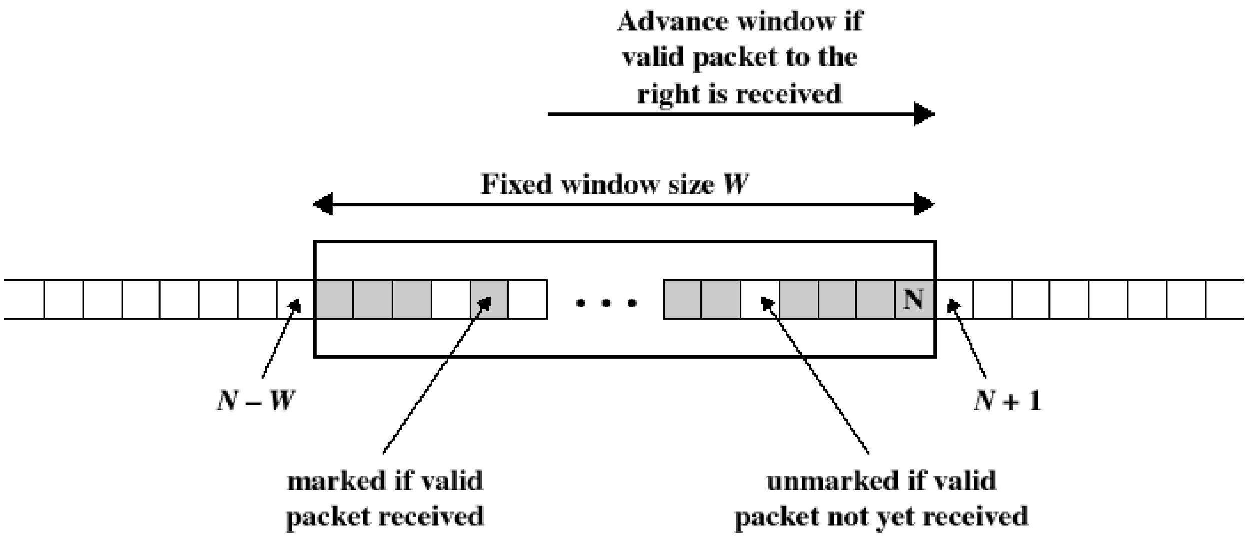
Authentication data: MAC value (variable length)

AH – Anti-replay Service

- Detection of duplicate packets
- Sequence numbers
  - associated with SAs
  - 32-bit value
  - when an SA is created, initialized to 0
    - when it reaches 2^{32}-1, SA must be terminated
    - not to allow overflows
  - sender increments the replay counter and puts into each AH (sequence number field)
- Problem: IP is unreliable, so the receiver may receive IP packets out of order
  - Solution is window-based mechanism
    - Implemented at receiver side

AH – Anti-replay Service

window size W
(default is 64)



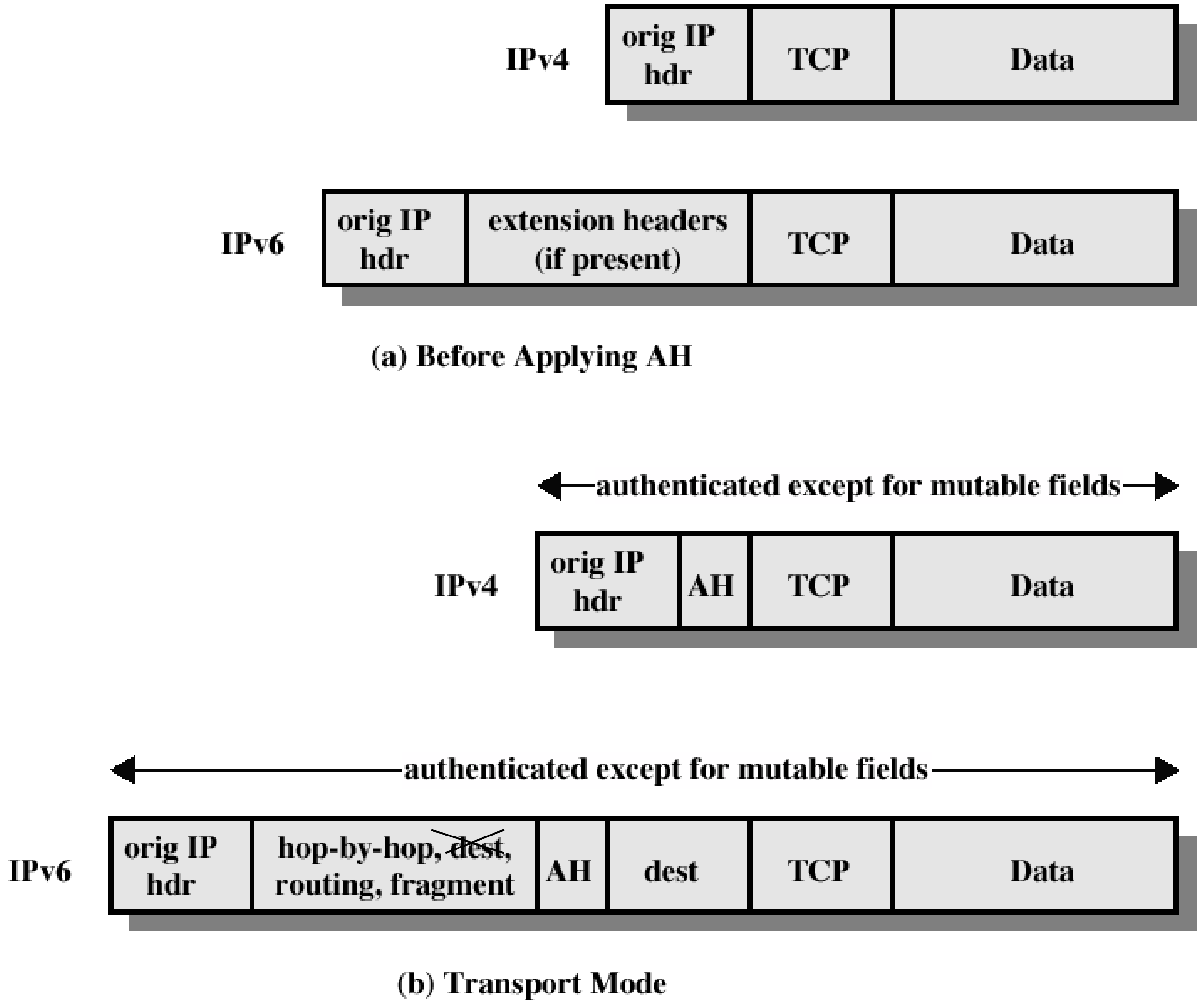
N: highest seq. number for a valid paket recevied so far

- If a received packet falls in the window
  - if authenticated and unmarked, mark it
  - if marked, then replay!
- If a received packet is > N
  - if authenticated, advance the window so that this packet is at the rightmost edge and mark it
- If a received packet is <= N-W
  - packet is discarded

AH - Integrity Check Value (ICV)

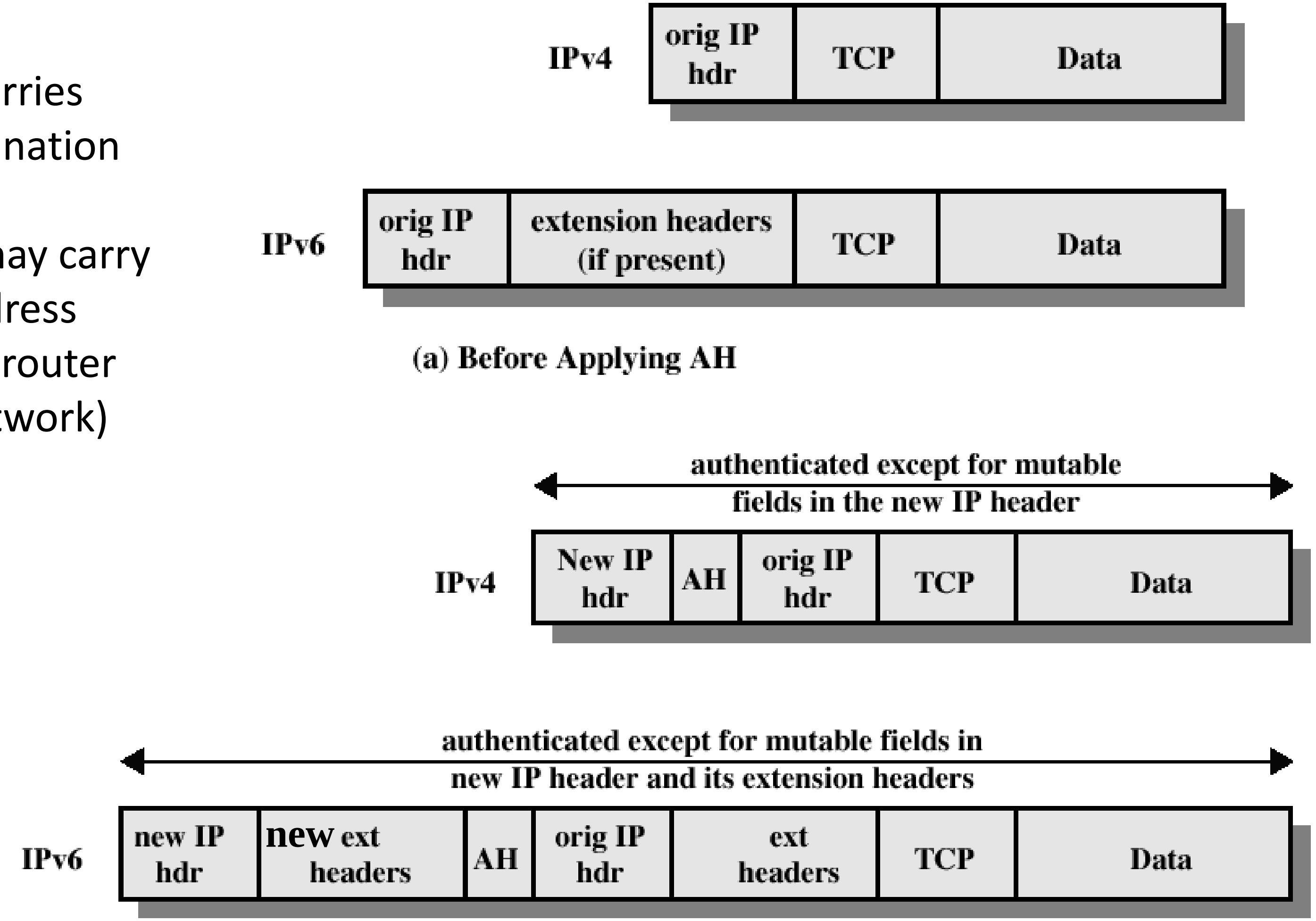
- Actually it is a MAC
- HMAC is used
  - with a secure hash algorithm
  - default length of authentication data field is 96
    - so HMAC output is truncated
- MAC is calculated over
  - IP payload (upper layer protocol data)
  - IP Headers that are “immutable” or “mutable but predictable” at destination
    - e.g. source address (immutable), destination address (mutable but predictable)
    - Time to live field is mutable. Such mutable fields are zeroed for MAC calculation
  - AH header (except authentication data of course, since authentication data is the MAC itself)

AH – Transport Mode



AH – Tunnel Mode

Inner IP packet carries the ultimate destination address
Outer IP packet may carry another dest. address (e.g. address of a router at destination network)

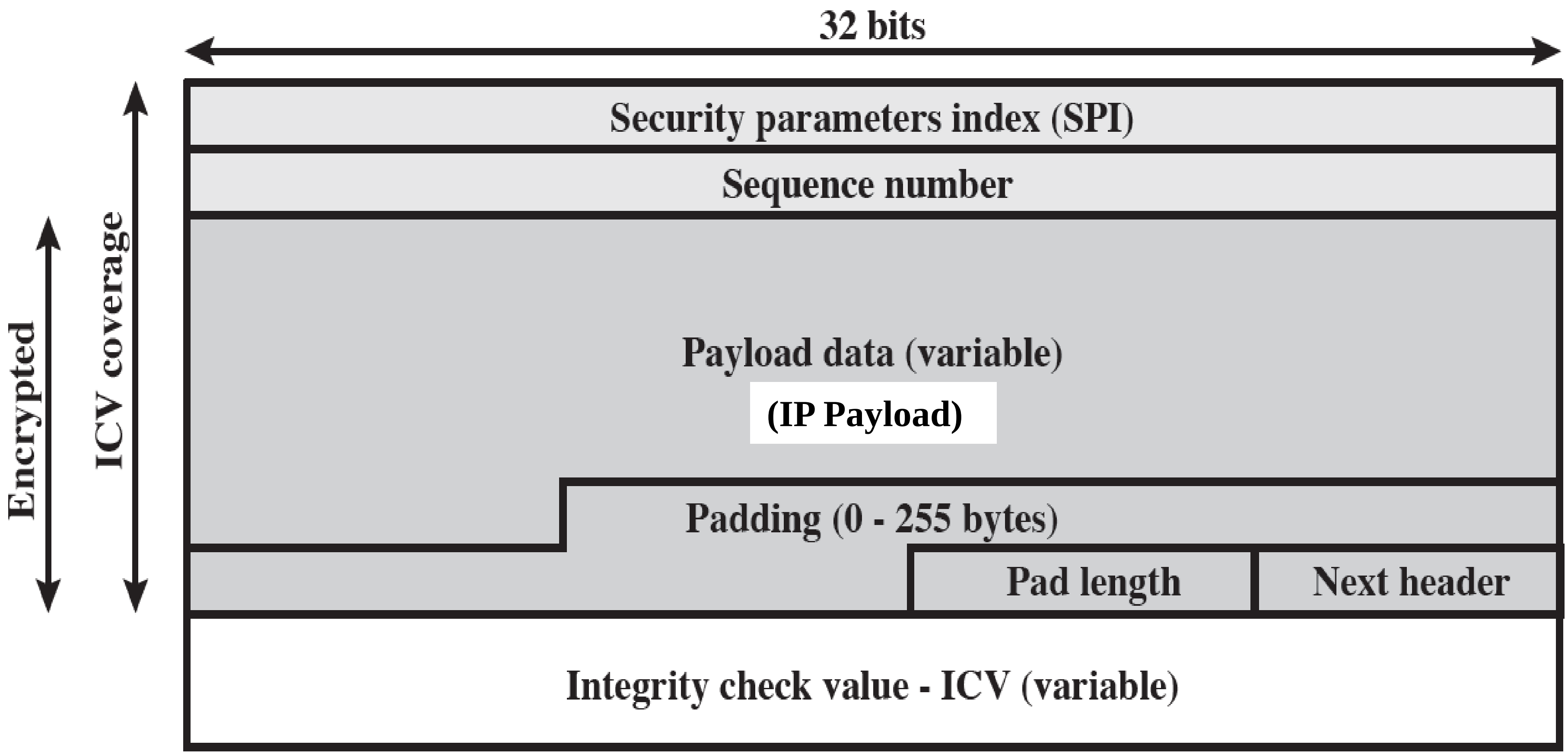


(c) Tunnel Mode

Encapsulating Security Payload (ESP)

- provides
  - message content confidentiality
    - via encryption
  - limited traffic flow confidentiality and measures for traffic analysis
    - by padding (may arbitrarily increase the data)
    - by encrypting the source and destination addresses in tunnel mode
  - optionally authentication services as in AH
    - via MAC (HMAC), sequence numbers
- supports range of ciphers, modes
  - DES, Triple-DES, RC5, IDEA, Blowfish, etc.
  - CBC is the most common mode

Encapsulating Security Payload

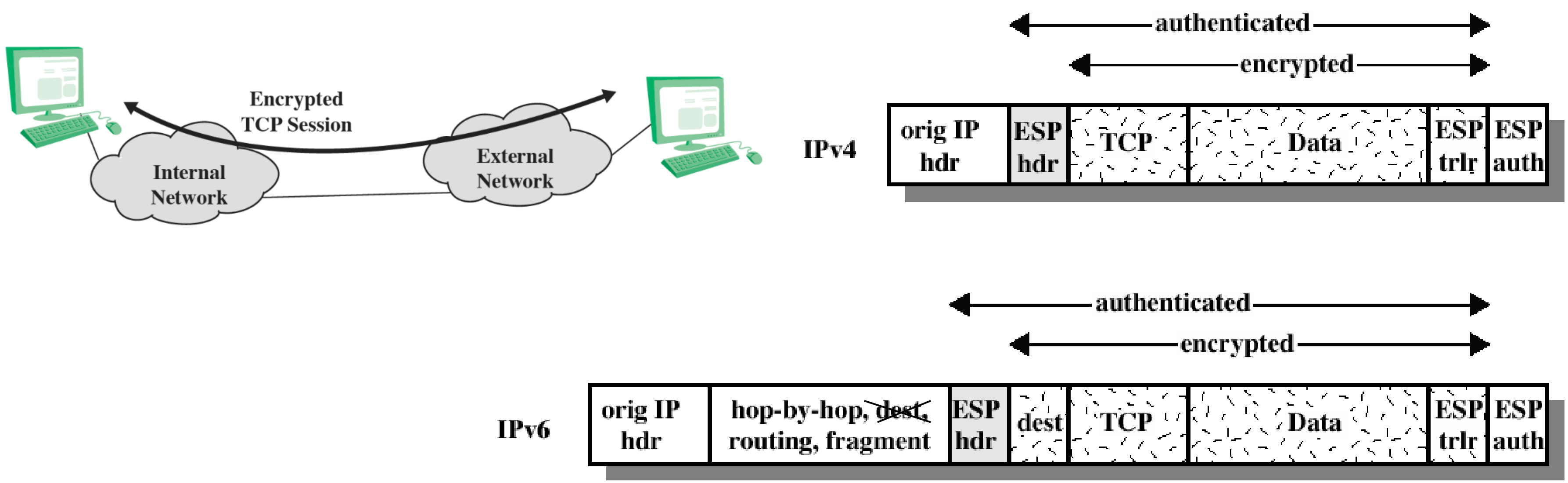


Padding in ESP

- several purposes and reasons
  - encryption algorithm may require the plaintext to be multiple of some integer *n*
  - ESP format requires 32-bit words
  - additional padding may help to provide partial traffic flow confidentiality by concealing the actual length of data
    - Other than the existing padding field, extra padding can be added to the end of the payload to improve traffic flow confidentiality

Transport Mode ESP

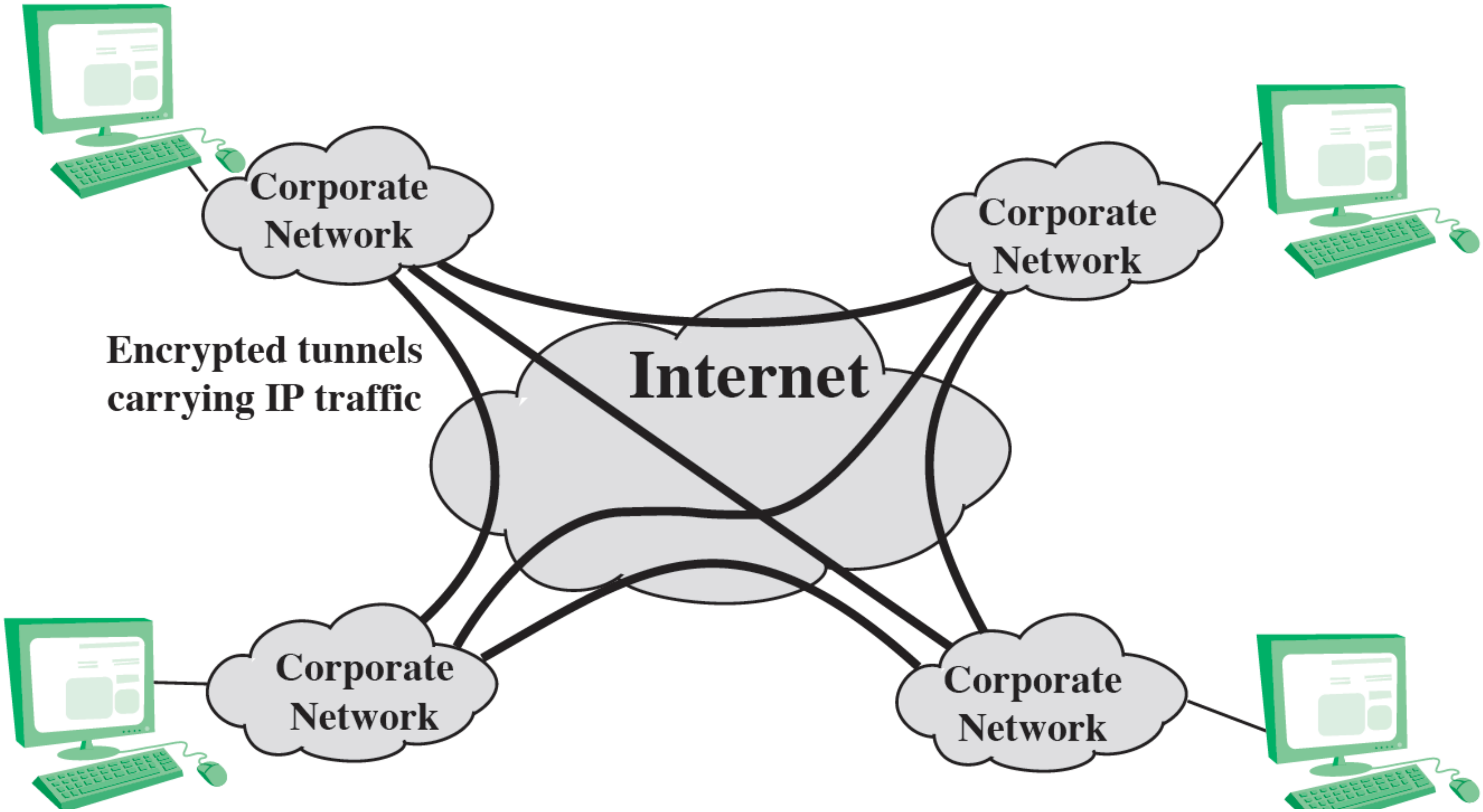
- transport mode is used to encrypt & optionally authenticate IP payload (e.g. TCP segment)
  - data protected but IP header left in clear
  - so source and destination addresses are not encrypted
  - Mostly for host to host (end-to-end) traffic



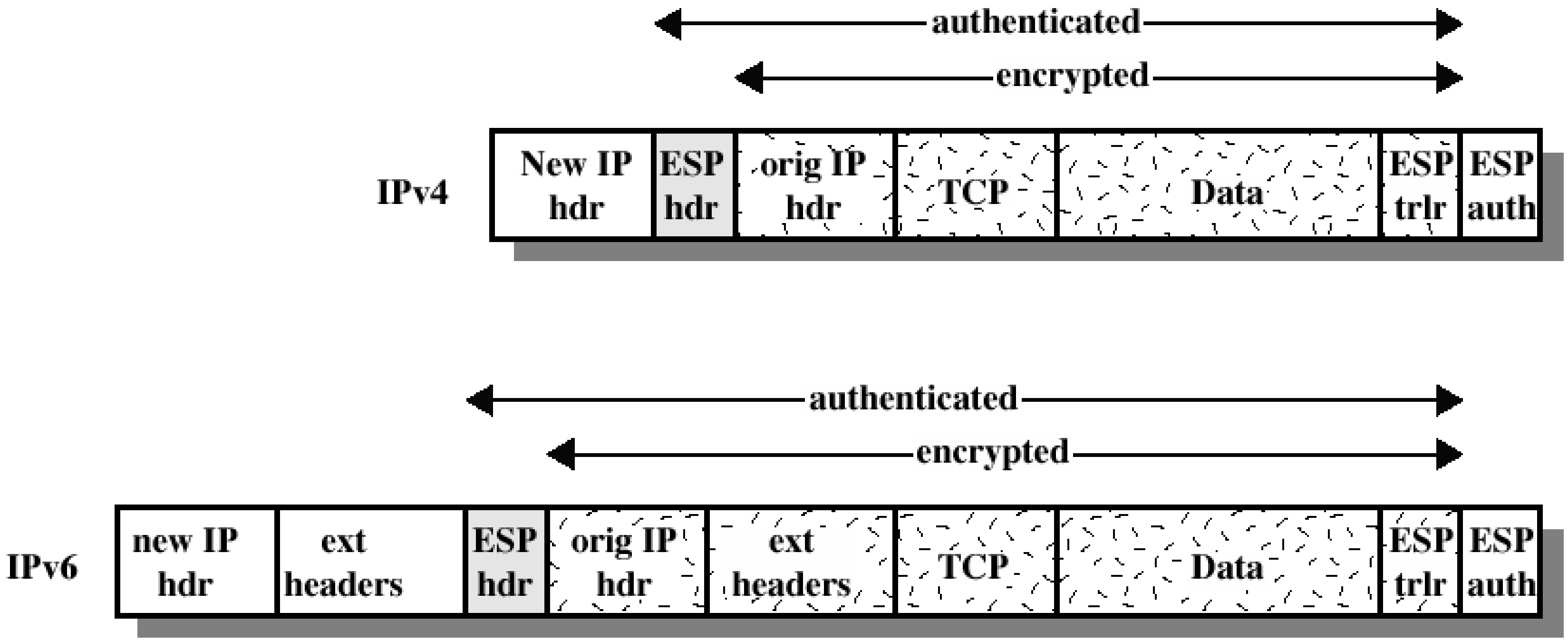
Tunnel Mode ESP

- Encrypts and optionally authenticates the entire IP packet
  - add new (outer) IP header for processing at intermediate routers
    - may not be the same as the inner (original) IP header, so traffic analysis can somehow be prevented
  - good for VPNs, gateway to gateway (router to router) security
    - hosts in internal network do not get bothered with security related processing
    - number of keys reduced
    - thwarts traffic analysis based on ultimate destination

Tunnel Mode ESP

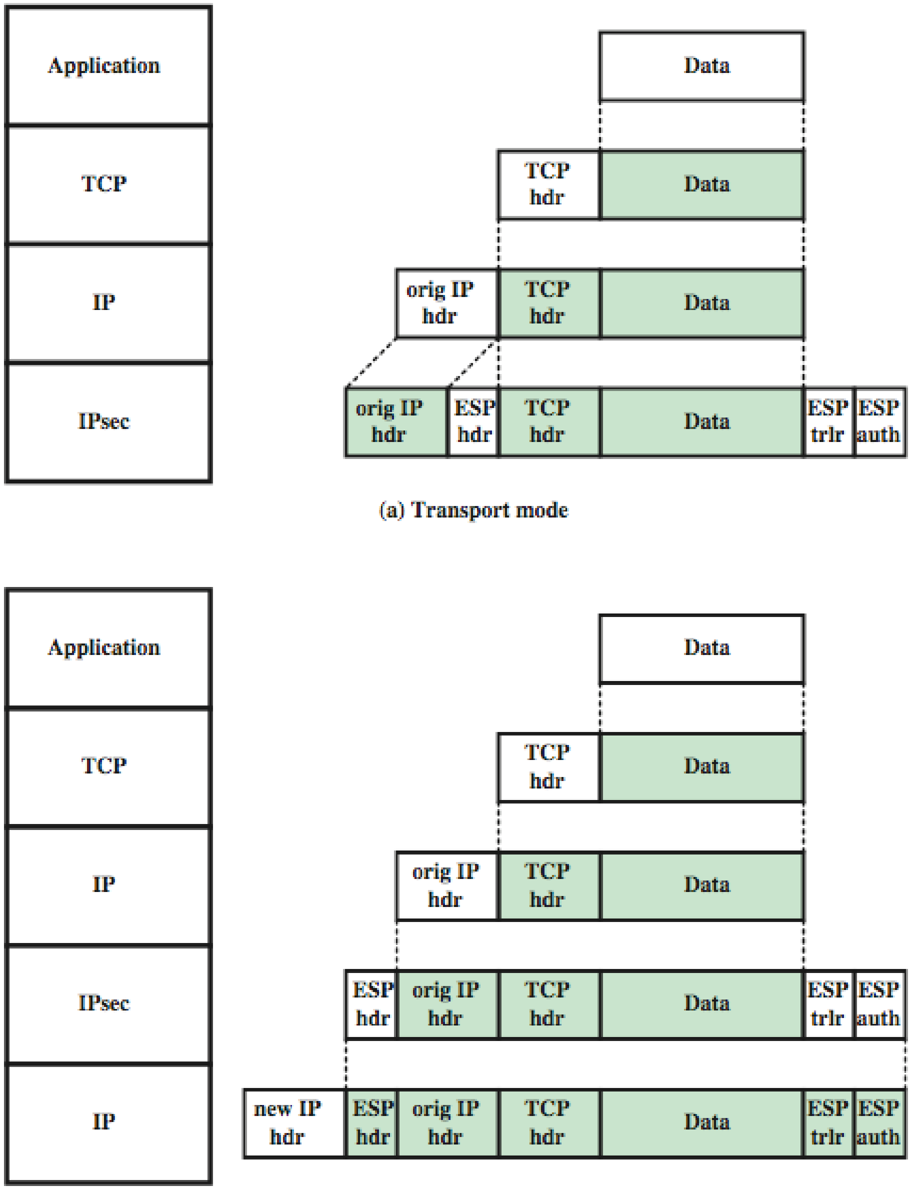


Tunnel Mode ESP



(b) Tunnel Mode

Protocol Operations for ESP



(a) Transport mode

(b) Tunnel mode

Transport and Tunnel Modes

	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 entire 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 entire inner IP packet. Authenticates inner IP packet.

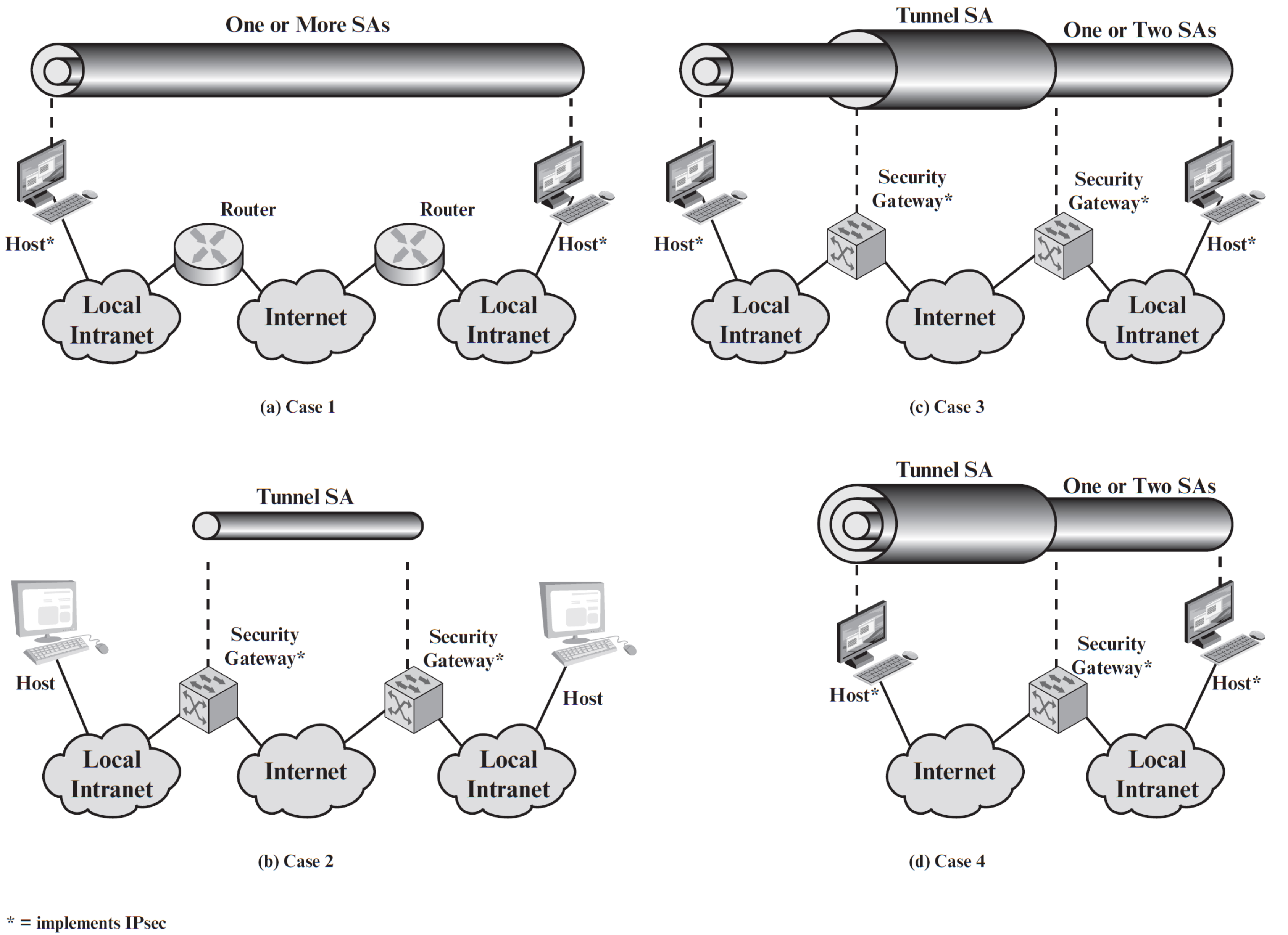


Figure 20.10 Basic Combinations of Security Associations

Combining Security Associations

- SAs can implement either AH or ESP
- to implement both, need to combine SAs
  - form a security association bundle
- A possible case: End-to-end Authentication + Confidentiality
  - Solution1: use ESP with authentication option on
  - Solution2: apply ESP SA (no auth.) first, then apply AH SA
  - Solution3: Apply AH SA first, then ESP SA
    - encryption is after the authentication

Key Management in IPSec

- Ultimate aim
  - generate and manage SAs for AH and ESP
  - asymmetric
    - receiver and initiator have different SAs
- can be manual or automated
  - manual key management
    - sysadmin manually configures every system
  - automated key management
    - on demand creation of keys for SA’s in large systems

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
- IKEv2 does not even use the terms Oakley and ISAKMP, but the basic functionality is the same

IKE Key Determination

- Actually Oakley
- Key exchange protocol based on Diffie-Hellman
- have extra features
  - cookies
    - precaution against clogging (denial-of-service) attacks
      - makes the attack more difficult
    - cookies are unique values based on connection info and generated using a locally known secret (thus not guessable)
      - Generated using hash over these info
      - In IKE, cookies became SPI
    - used at every message during the protocol (carried in header)
  - predefined groups
    - fixed DH global parameters
    - regular DH and ECDH
  - nonces
    - against replay attacks
  - authentication (via symmetric or asymmetric crypto)

ISAKMP

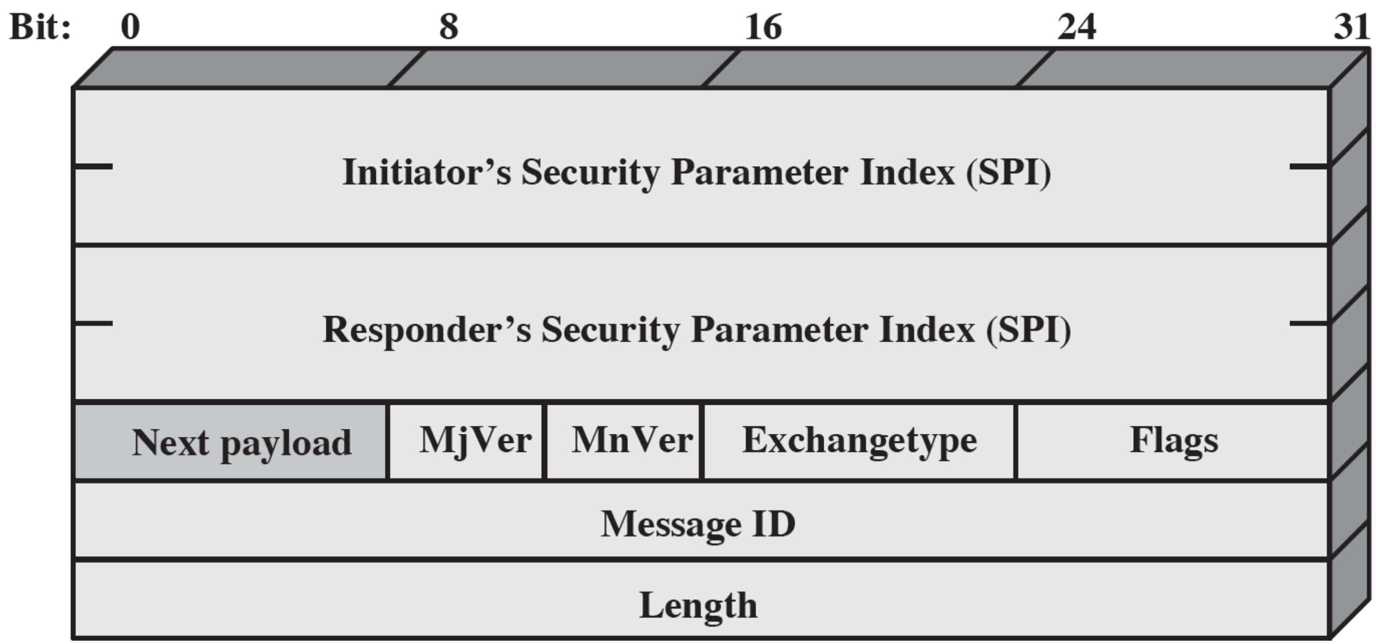
- Internet Security Association and Key Management Protocol
- defines procedures and message formats to establish, negotiate, modify and delete SAs
  - SA-centric, so some calls it only a SA management protocol
    - but we have keys in SAs
  - ISAKMP is NOT key exchange protocol
- independent of key exchange protocol, encryption algorithm and authentication method
- IKE combines everything
  - Actually ISAKMP has been adopted by IKEv2 (whatever we say about ISAKMP in the lecture has been explained as IKEv2 features in the textbook)

ISAKMP

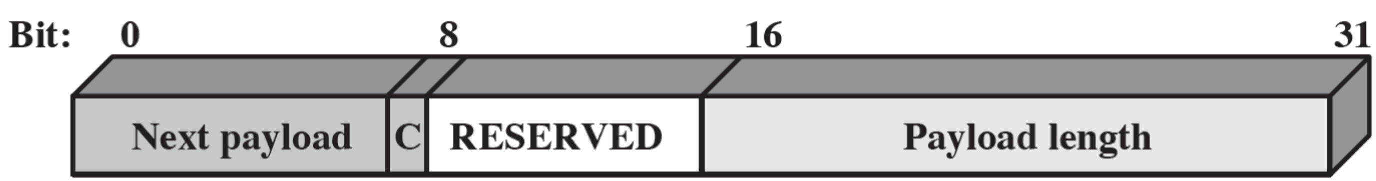
- Typical SA establishment protocol run in ISAKMP
  - Negotiate capabilities
    - encryption algorithms, authentication methods, key exchange methods, etc.
  - Exchange keys
    - using the method agreed above
  - Authenticate the exchange
    - digital signatures based on certificates
    - public-key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

IKE (ISAKMP) Header

In ISAKMP, Security Parameter Index (SPI) fields were named as cookie. Actually SPIs are cookies, although their main functionality is to identify SAs.



(a) IKE Header



(b) Generic Payload Header

ISAKMP/IKE Payloads

- ISAKMP/IKE 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 begin the key exchange process
    - Proposal and Transform payloads (included in SA payload)
      - to exchange the security and crypto capabilities
  - Key Exchange payload
    - to transfer the key exchange info
  - Others (e.g. nonce, identification (typically IP addr., certificate, certificate request, authentication, …)
  - See and study all payload types in Table 20.3 (page 690) and related text.

ISAKMP/IKE Protocol Flow (Message Exchange)

- negotiate / key exchange / authenticate
- 5 such ISAKMP message exchanges are proposed
  - later IKE rearranged them; but the IKE exchanges explained in the book is too confusing
  - thus will go over two important ISAKMP exchanges from the old version of the book here
    - identity-protection exchange
    - aggressive exchange
  - each message is one ISAKMP/IKE message (header + payloads)
    - main header includes cookies (SPI in IKE) 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;	Key generated
(4) **R → I:** KE;	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; ID_I	Begin ISAKMP-SA negotiation and key exchange
(2) **R → I:** SA; KE; 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
- Current IKE version is IKEv2
  - which is explained in the book independent of Oakley, ISAKMP and others
  - Basically IKEv2 also uses Oakley and ISAKMP, but without using their names. In the lecture, the natural evolution has been explained

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 are encrypted using previously known public keys
      - Without knowing the corresponding private key, the protocol cannot continue
    - no certificates, so no non-repudiation
  - pre-shared key
    - symmetric method
    - simplest, no public key crypto
- Material to be authenticated /signed 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)
  - CREATE_CHILD_SA exchange (only 2 messages)
  - IKE SA is used to protect this exchange
  - Several SAs can be established in this way

Summary

- Internetwork Protocol (IP)
- IPv4 , IPv6
- IPSec overview
- IPSec Protocols
- IPSec Modes
- Key Management in IPSec
- Key Exchange in IPSec