IP Security

- IP Security Overview
- IP Security Architecture & Services
- Authentication Header
- Encapsulating Security Payload

Key Points

- 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 encompasses three functional areas: authentication, confidentiality, and key management.
- Authentication makes use of the HMAC message authentication code. Authentication can be applied to the entire original IP packet (tunnel mode) or to all of the packet except for the IP header (transport mode).
- Confidentiality is provided by an encryption format known as encapsulating security payload. Both tunnel and transport modes can be accommodated.

Functional areas of IPSec

- **The authentication mechanism** assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header. In addition, this mechanism assures that the packet has not been altered in transit.
- **The confidentiality facility** enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.
- **The key management facility** is concerned with the secure exchange of keys.

Functional areas of IPSec

- By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security-ignorant applications.

Applications of IPSec

- IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet.
- **Secure branch office connectivity over the Internet**
  - A company can build a secure virtual private network over the Internet or over a public WAN.
  - This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.

Applications of IPSec

- **Secure remote access over the Internet**
  - **An end user whose system is equipped with IP** security protocols can make a local call to an Internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees.
- **Establishing extranet and intranet connectivity with partners**
  - IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

Applications of IPSec

- **Enhancing electronic commerce security**
  - Even though some Web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security.
- The principal feature of IPSec that enables it to support these varied applications is that it can encrypt and/or authenticate *all traffic at the IP level*.
- *Thus, all distributed applications, including remote logon,* client/server, e-mail, file transfer, Web access, and so on, can be secured.

An IP Security Scenario

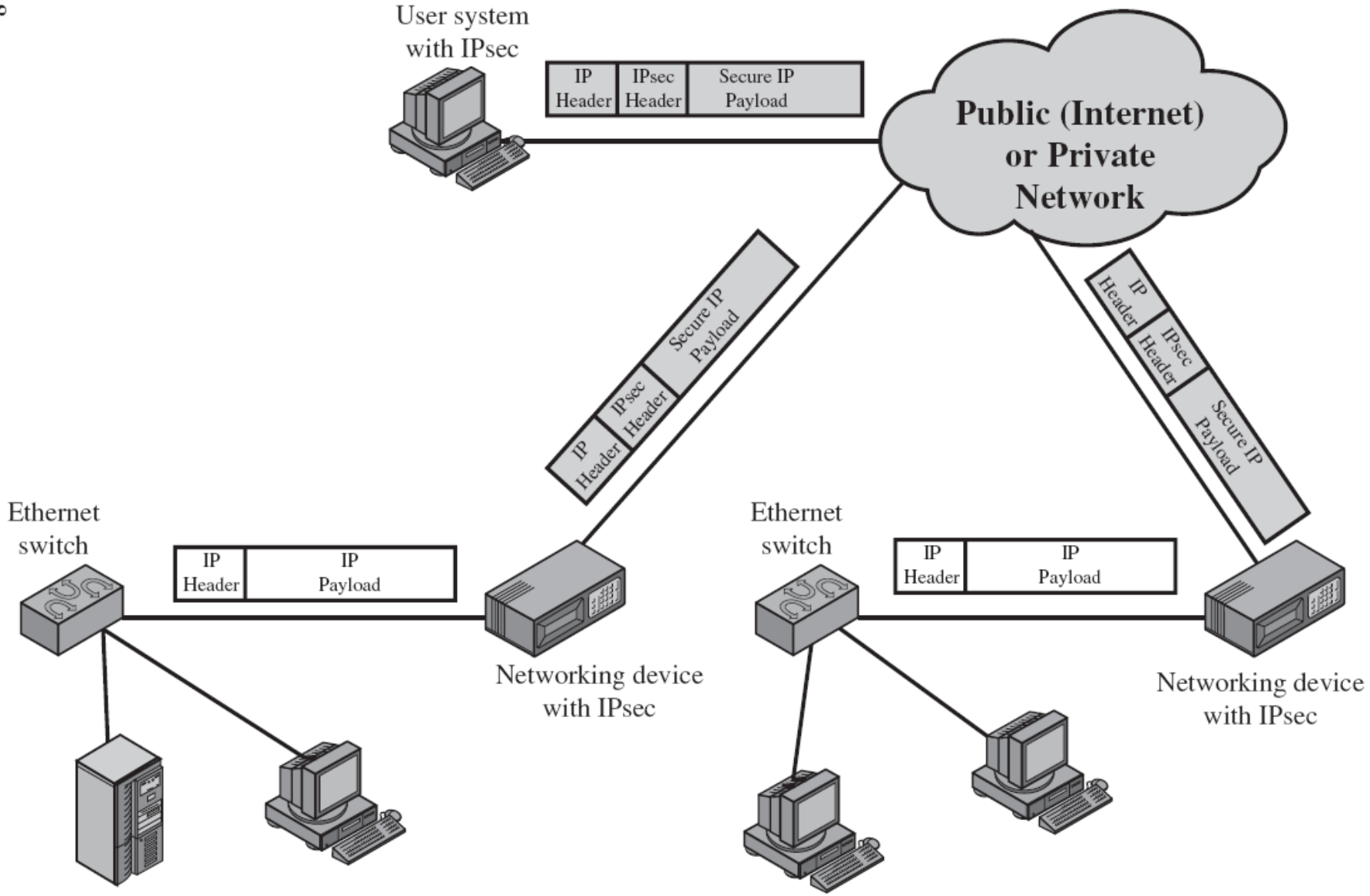


Figure 19.1 An IP Security Scenario

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.
- IPSec 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.

Benefits of IPSec

- IPSec is below the transport layer (TCP, UDP) and so is transparent to applications.
- IPSec can be transparent to end users.
- IPSec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

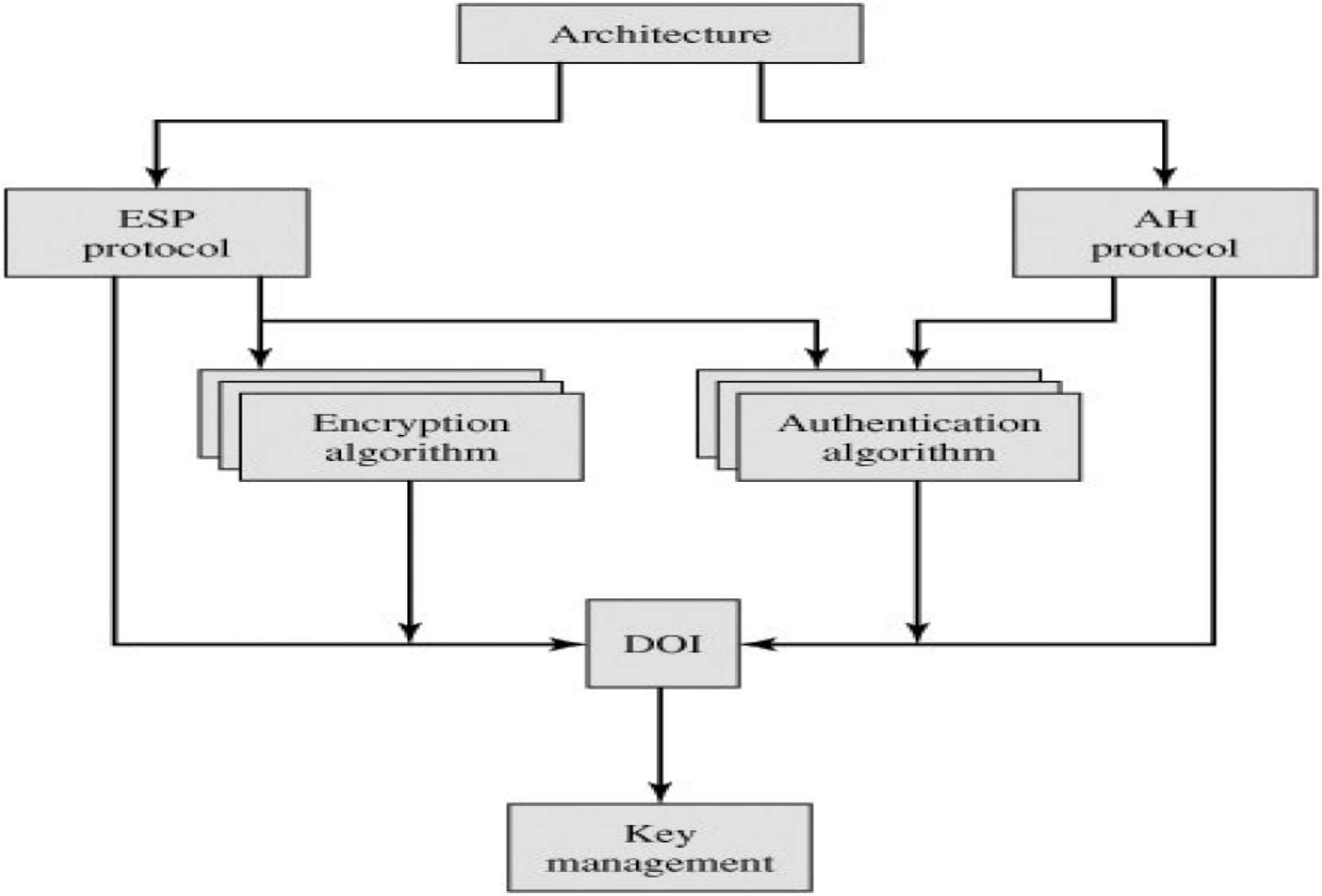
Routing Applications

- IPSec can assure that
  - A router advertisement comes from an authorized router
  - A 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.

IP Security Architecture

- The IPSec specification consists of numerous documents. The most important of these, issued in November of 1998, are RFCs 2401, 2402, 2406, and 2408:
- RFC 2401: An overview of a security architecture
- RFC 2402: Description of a packet authentication extension to IPv4 and IPv6
- RFC 2406: Description of a packet encryption extension to IPv4 and IPv6
- RFC 2408: Specification of key management capabilities

IPSec Document Overview



IPSec Document Overview

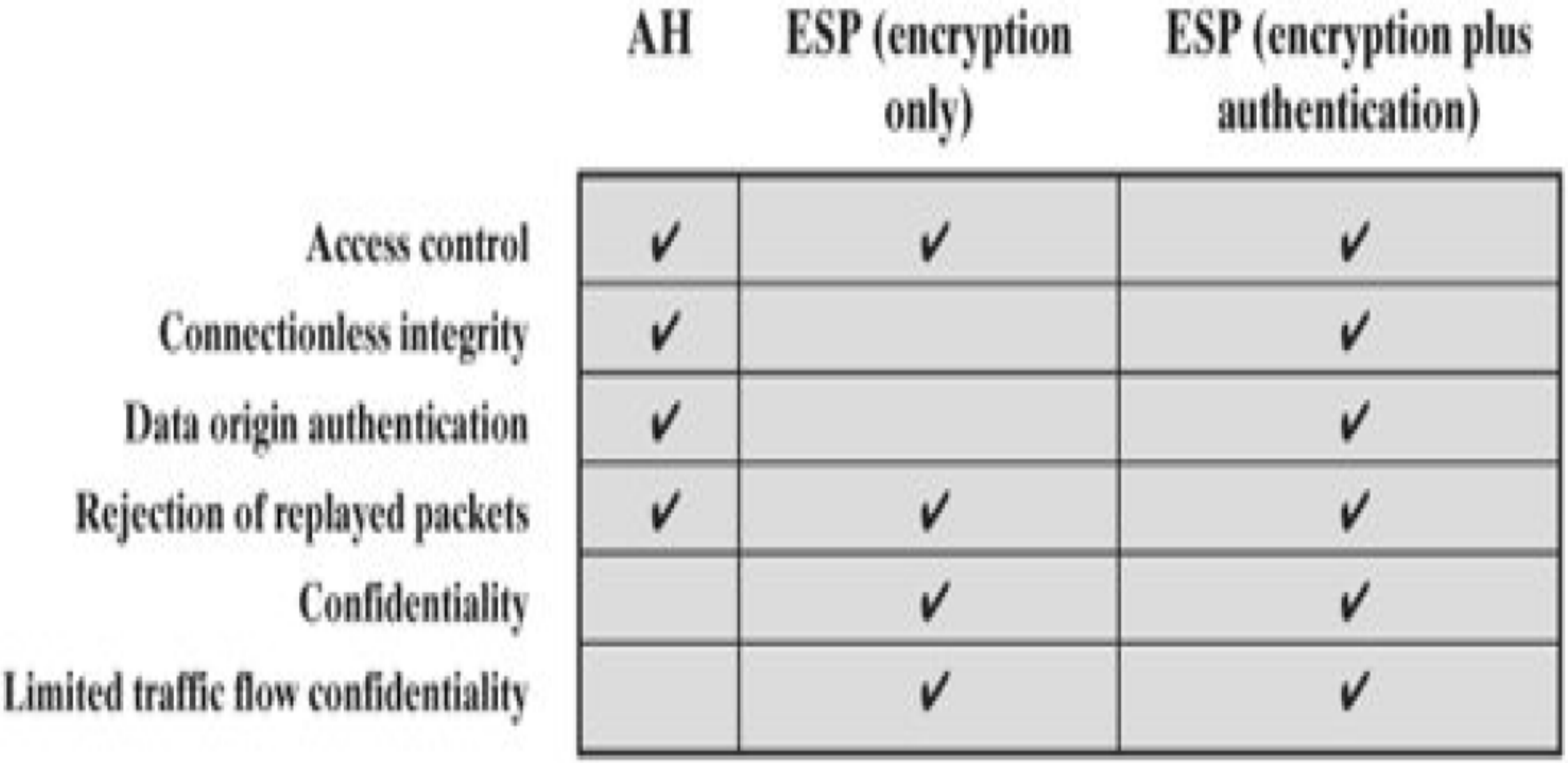
- **Architecture:**
  - Covers the general concepts, security requirements, definitions, and mechanisms defining IPSec technology.
- **Encapsulating Security Payload (ESP)**
  - Covers the packet format and general issues related to the use of the ESP for packet encryption and, optionally, authentication.
- **Authentication Header (AH)**
  - Covers the packet format and general issues related to the use of AH for packet authentication.

IPSec Document Overview

- **Encryption Algorithm**
  - A set of documents that describe how various encryption algorithms are used for ESP.
- **Authentication Algorithm**
  - A set of documents that describe how various authentication algorithms are used for AH and for the authentication option of ESP.
- **Key Management**
  - Documents that describe key management schemes.
- **Domain of Interpretation (DOI)**
  - Contains values needed for the other documents to relate to each other. These include identifiers for approved encryption and authentication algorithms, as well as operational parameters such as key lifetime.

IPSec Services

[View full size image]

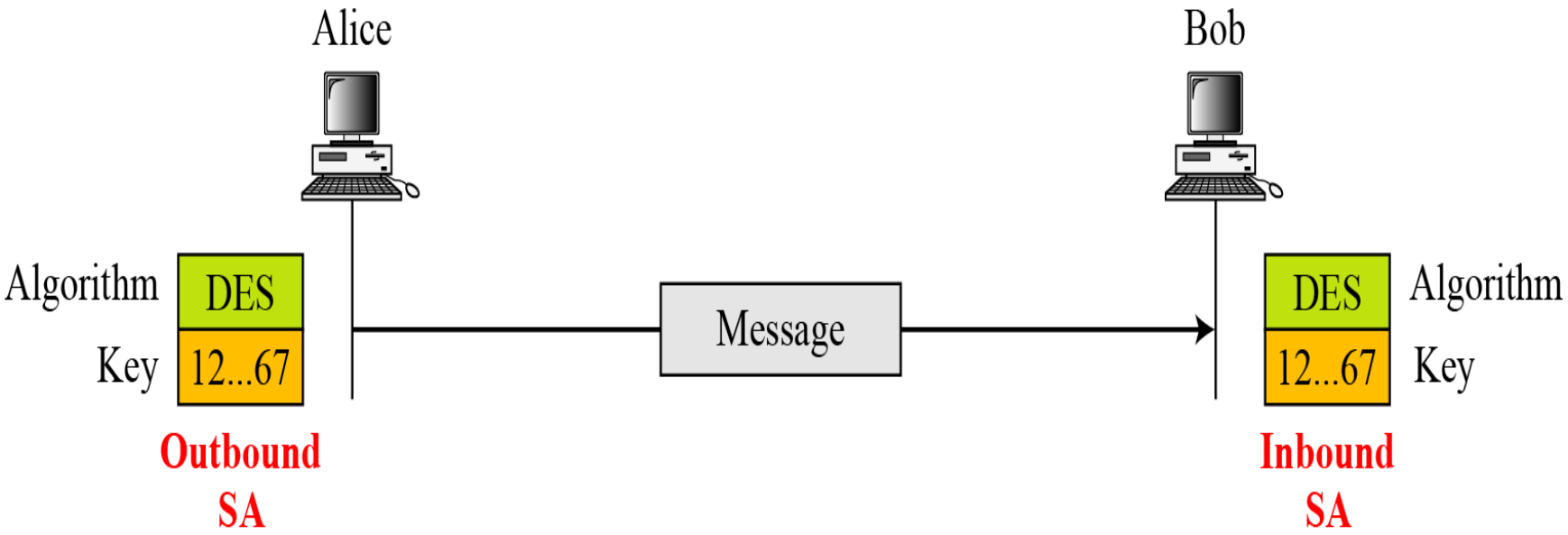


	AH	ESP (encryption only)	ESP (encryption plus authentication)
Access control	✔	✔	✔
Connectionless integrity	✔		✔
Data origin authentication	✔		✔
Rejection of replayed packets	✔	✔	✔
Confidentiality		✔	✔
Limited traffic flow confidentiality		✔	✔

Security Associations

- An association is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.
- IPSec requires a logical relationship, called a Security Association (SA), between two hosts.
- If a peer relationship is needed, for two-way secure exchange, then two security associations are required. Security services are afforded to an SA for the use of AH or ESP, but not both.

Security Associations



Security Associations

- A security association is uniquely identified by three parameters:
- **Security Parameters Index (SPI): A bit string assigned to this SA and having local** significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
- **IP Destination Address: Currently, only unicast addresses are allowed; this is the address of** the destination endpoint of the SA, which may be an end user system or a network system such as a firewall or router.
- **Security Protocol Identifier: This indicates whether the association is an AH or ESP security** association.

Security Associations

Index	SN	OF	ARW	AH/ESP	LT	Mode	MTU
< SPI, DA, P >							
< SPI, DA, P >							
< SPI, DA, P >							
< SPI, DA, P >							

Security Association Database

Legend:

SPI: Security Parameter Index

DA: Destination Address

AH/ESP: Information for either one

P: Protocol

Mode: IPSec Mode Flag

SN: Sequence Number

OF: Overflow Flag

ARW: Anti-Replay Window

LT: Lifetime

MTU: Path MTU (Maximum Transfer Unit)

SA Parameters

- In each IPSec implementation, there is a nominal Security Association Database that defines the parameters associated with each SA.
- A security association is normally defined by the following parameters:
- **Sequence Number Counter**
  - A 32-bit value used to generate the Sequence Number field in AH or ESP headers
- **Sequence Counter Overflow**
  - A flag indicating whether overflow of the Sequence Number

SA Parameters

- **Anti-Replay Window**
  - Used to determine whether an inbound AH or ESP packet is a replay.
- **AH Information**
  - Authentication algorithm, keys, key lifetimes, and related parameters being used with AH.
- **ESP Information**
  - Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP
- **Lifetime of This Security Association**
  - A time interval or byte count after which an SA must be replaced with a new SA (and new SPI) or terminated, plus an indication of which of these actions should occur (required for all implementations).

SA Parameters

- **IPSec Protocol Mode**
  - Tunnel, transport, or wildcard (required for all implementations).
- **Path MTU**
  - **Any observed path maximum transmission unit (maximum size of a packet that can** be transmitted without fragmentation)

Security Associations

- Another import aspect of IPSec is the Security Policy (SP), which defines the type of security applied to a packet when it is to be sent or when it has arrived.
- Before using the SAD a host must determine the predefined policy for the packet.

Security Policy Database

Index	Policy
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	
< SA, DA, Name, P, SPort, DPort >	

Legend:

SA: Source Address

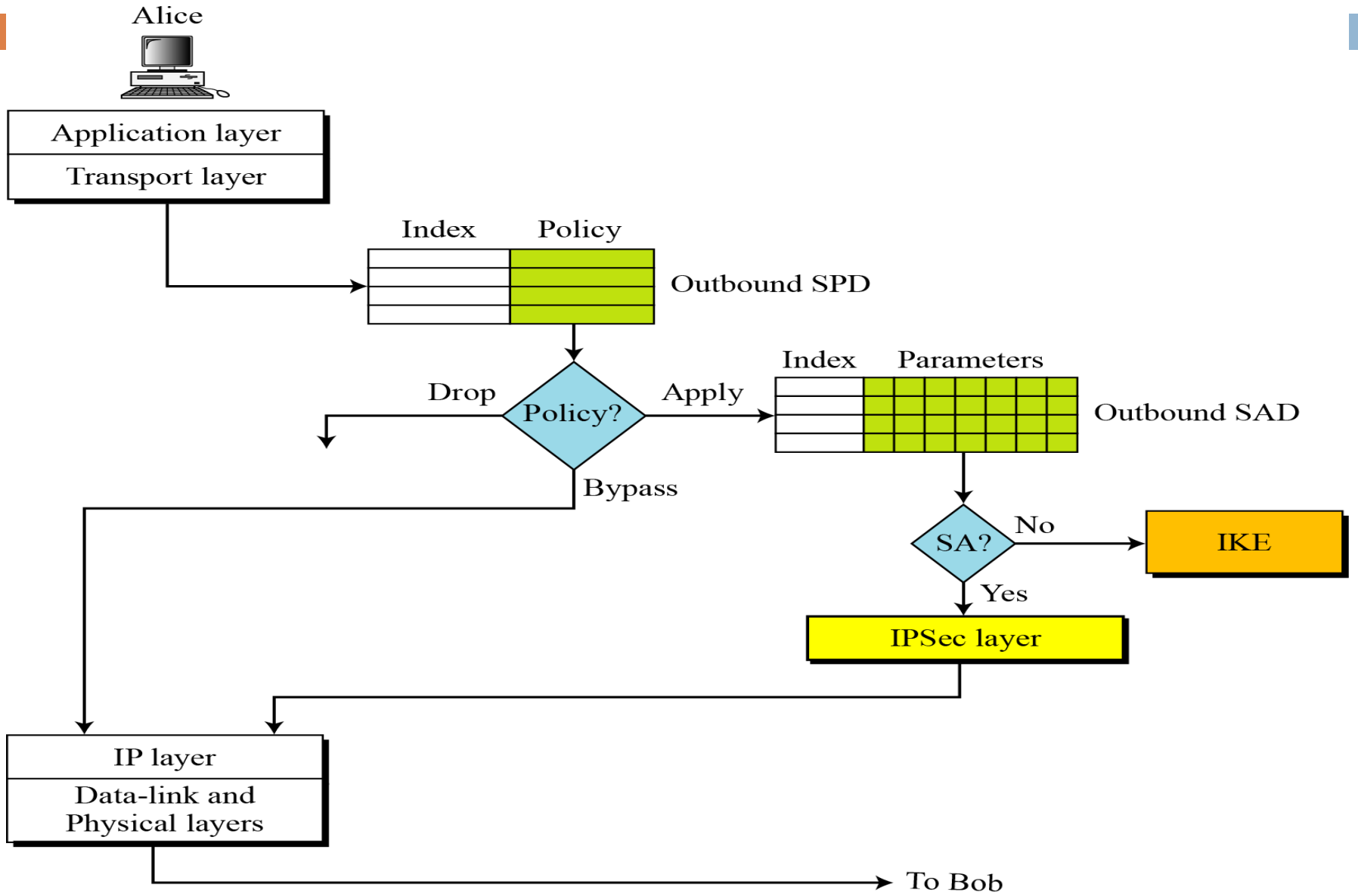
DA: Destination Address

P: Protocol

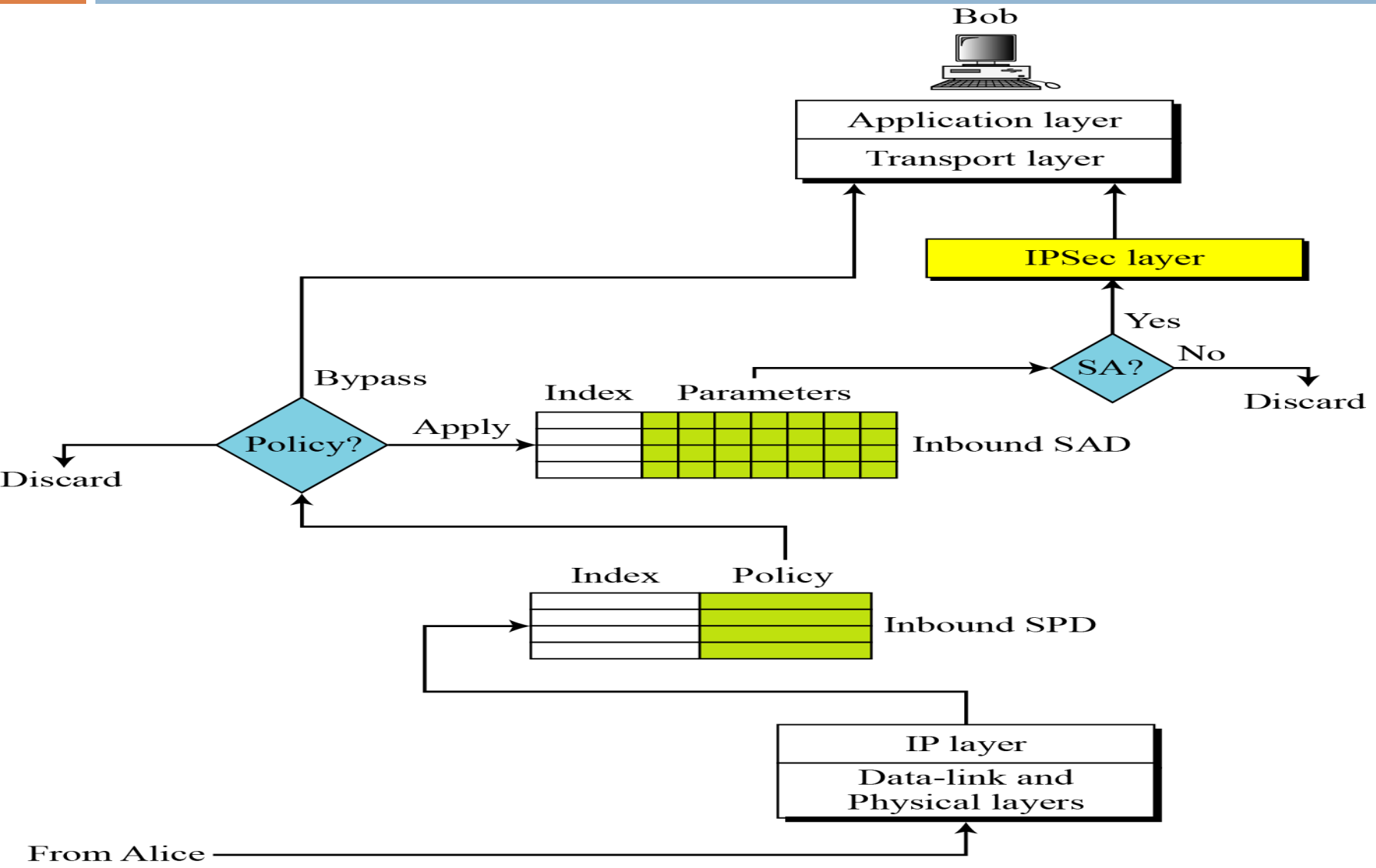
SPort: Source Port

DPort: Destination Port

SA Selectors



Inbound processing



Transport and Tunnel Modes

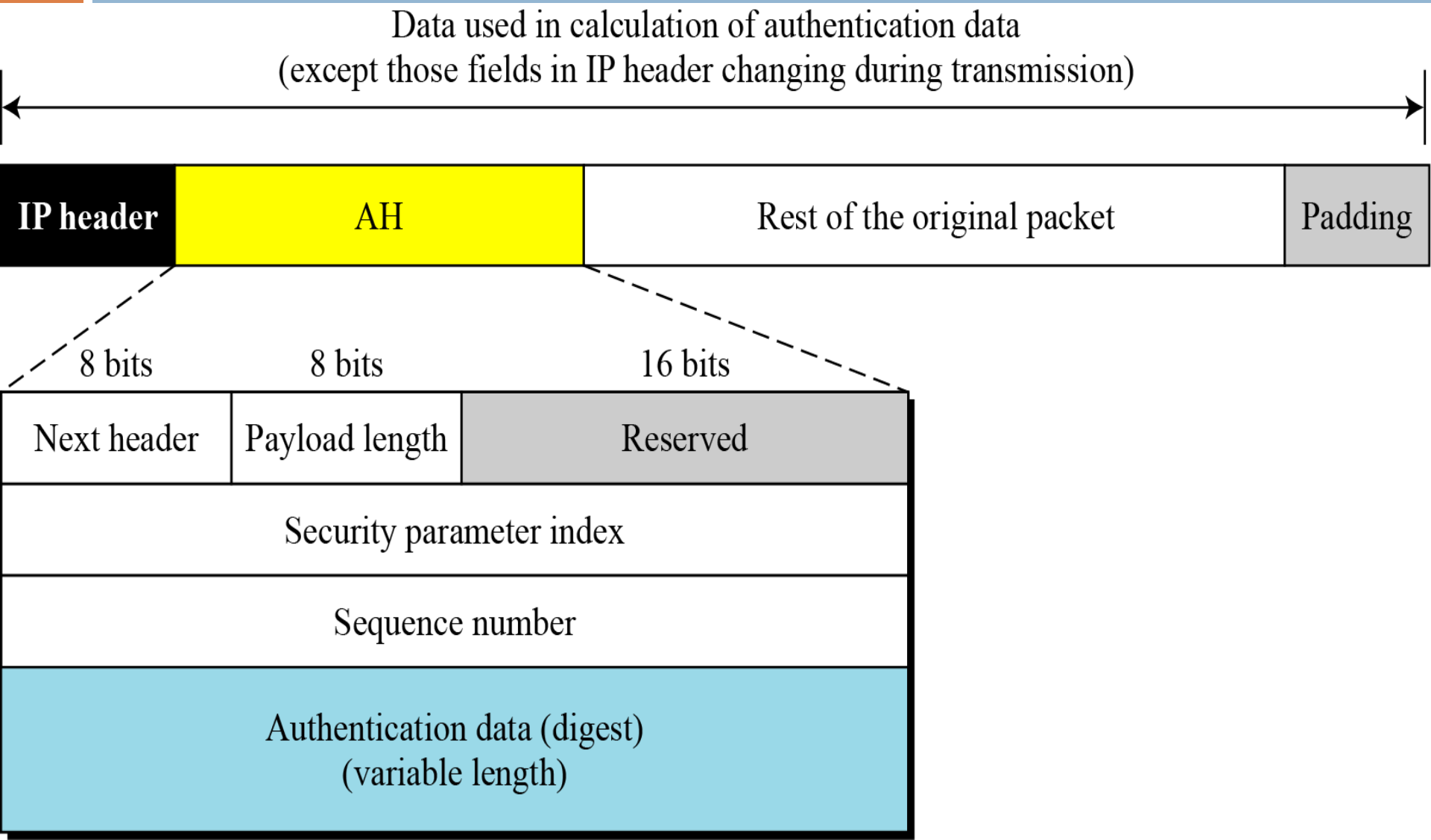
- Transport mode provides protection primarily for upper-layer protocols. That is, transport mode protection extends to the payload of an IP packet.
- Transport mode is used for end-to-end communication between two hosts.
- Tunnel mode provides protection to the entire IP packet.
- Tunnel mode is used when one or both ends of an SA are a security gateway, such as a firewall or router that implements IPSec.

Transport and Tunnel Modes

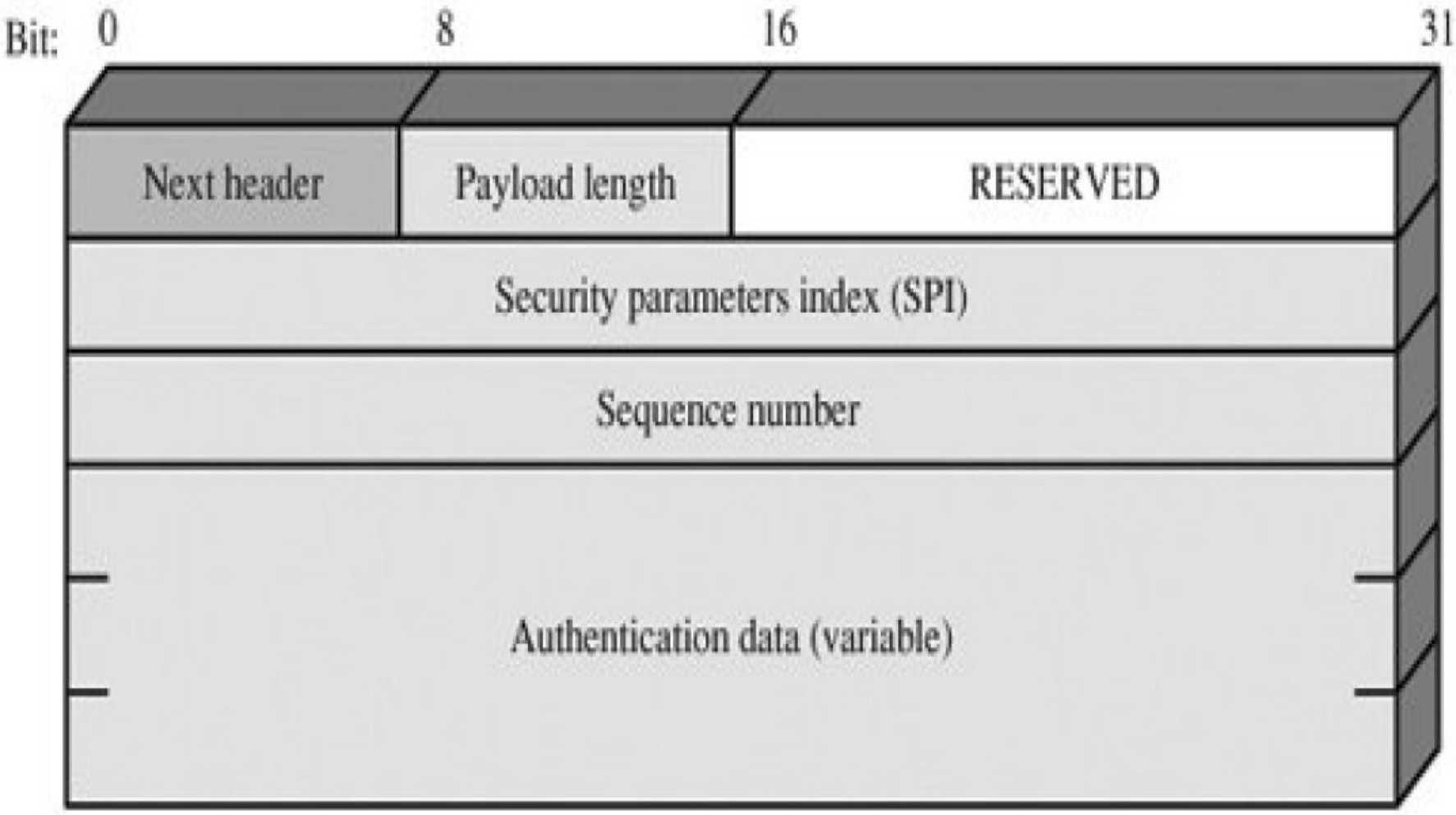
Table 16.2. Tunnel Mode and Transport Mode Functionality

	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 (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.

Authentication Header



Authentication Header



Authentication Header

- **Next Header (8 bits): Identifies the type of header immediately following this header.**
- **Payload Length (8 bits): Length of Authentication Header**
- **Reserved (16 bits): For future use.**
- **Security Parameters Index (32 bits): Identifies a security association.**
- **Sequence Number (32 bits): A monotonically increasing counter value.**
- **Authentication Data (variable): A variable-length field (must be an integral number of 32-bit** words) that contains the Integrity Check Value (ICV), or MAC, for this packet.

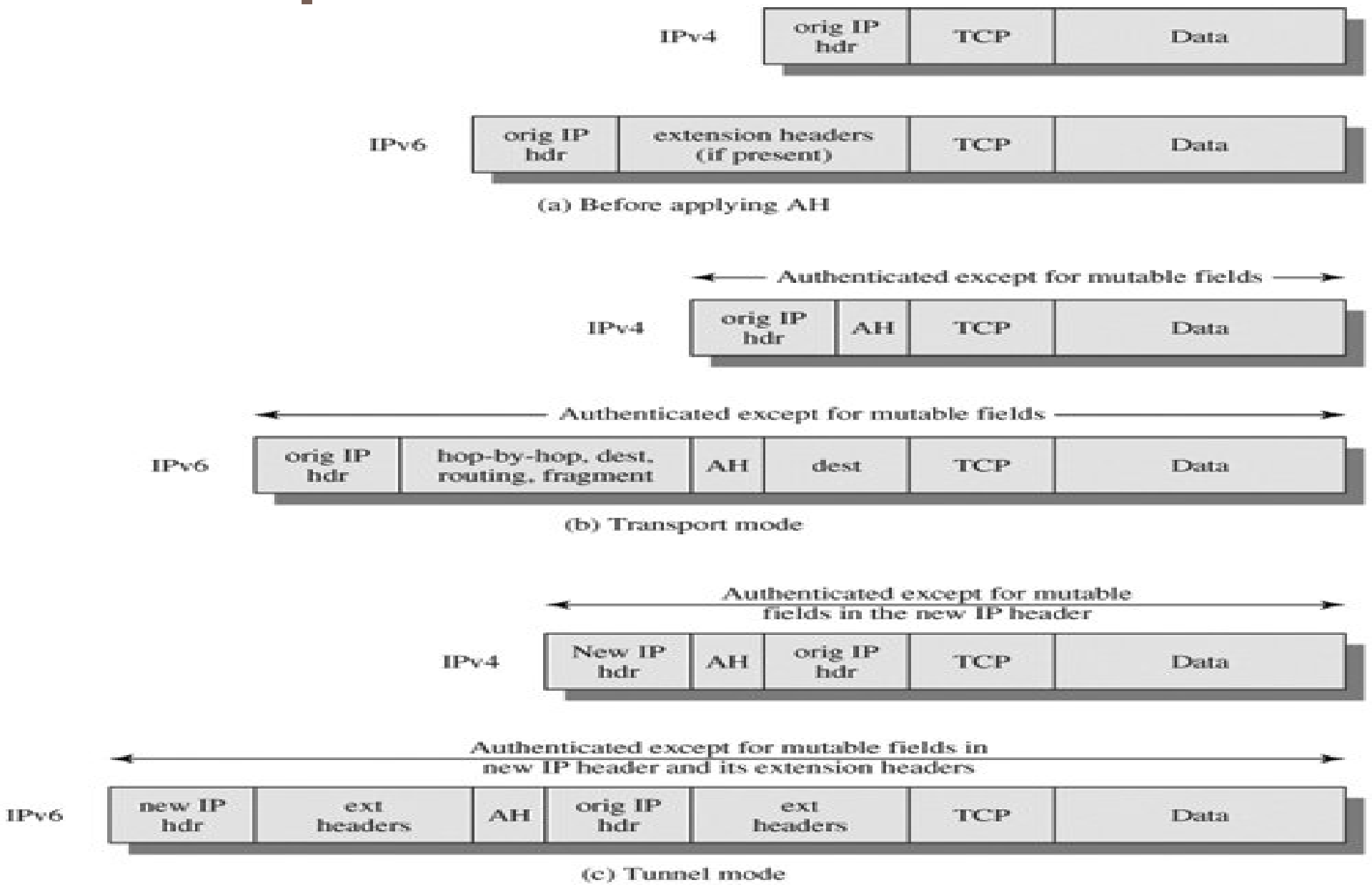
Integrity Check Value

- The Authentication Data field holds a value referred to as the Integrity Check Value.
- The ICV is a message authentication code or a truncated version of a code produced by a MAC algorithm.
- The current specification dictates that a compliant implementation must support
- HMAC-MD5-96
- HMAC-SHA-1-96

Transport and Tunnel Modes AH

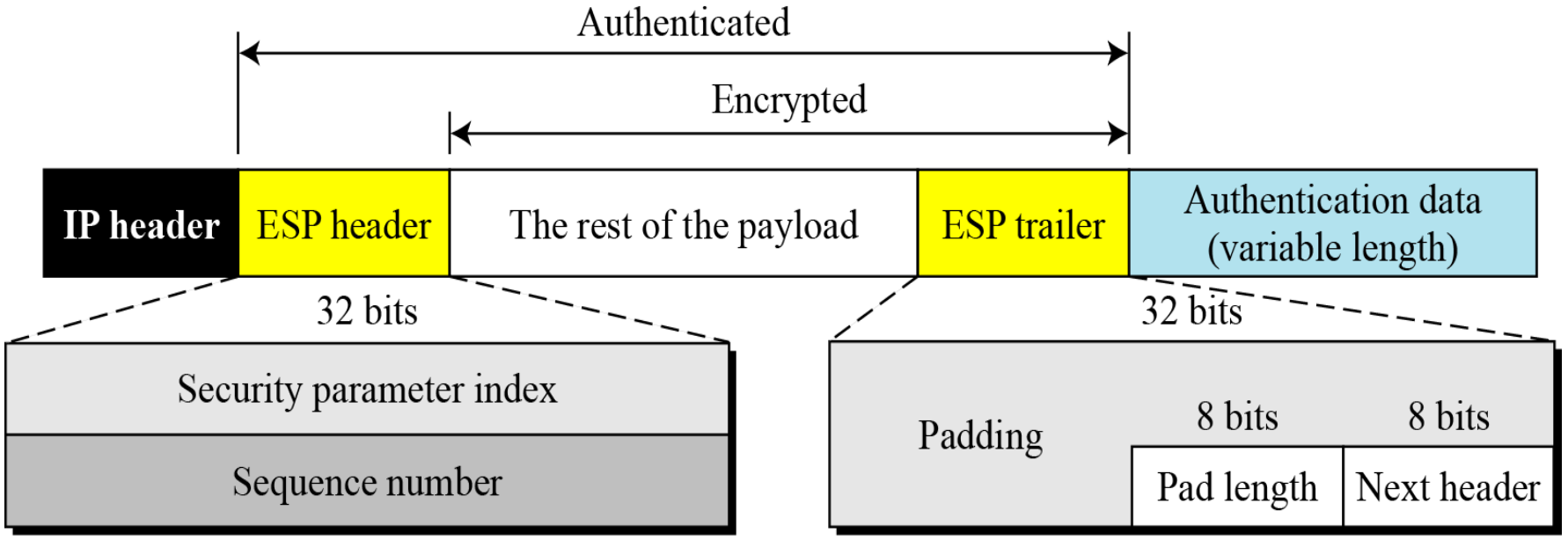
- AH in transport mode authenticates the IP payload and selected portions of the IP header.
- AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header.

Transport and Tunnel Modes AH

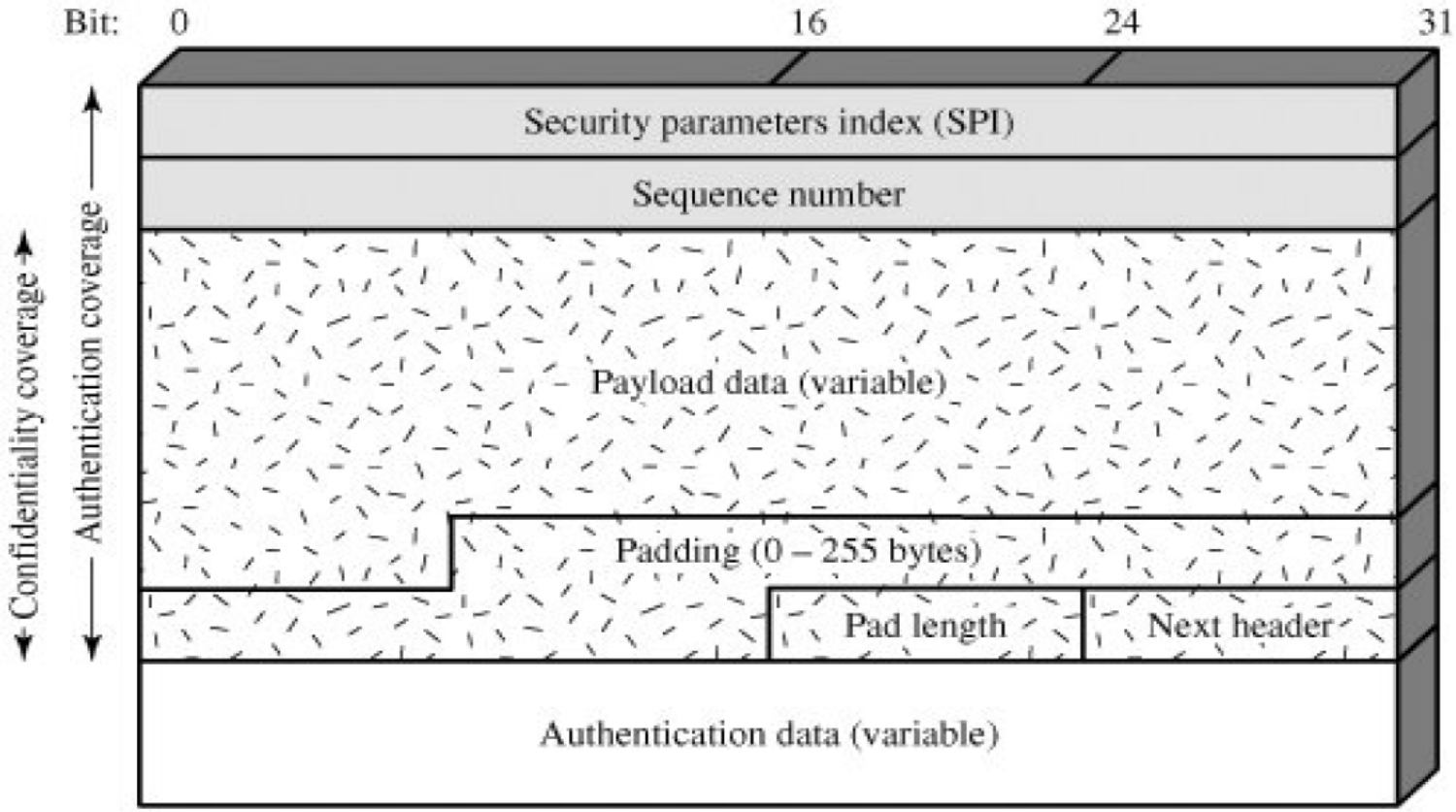


Encapsulating Security Payload

- ESP provides source authentication, data integrity, and privacy.



Encapsulating Security Payload



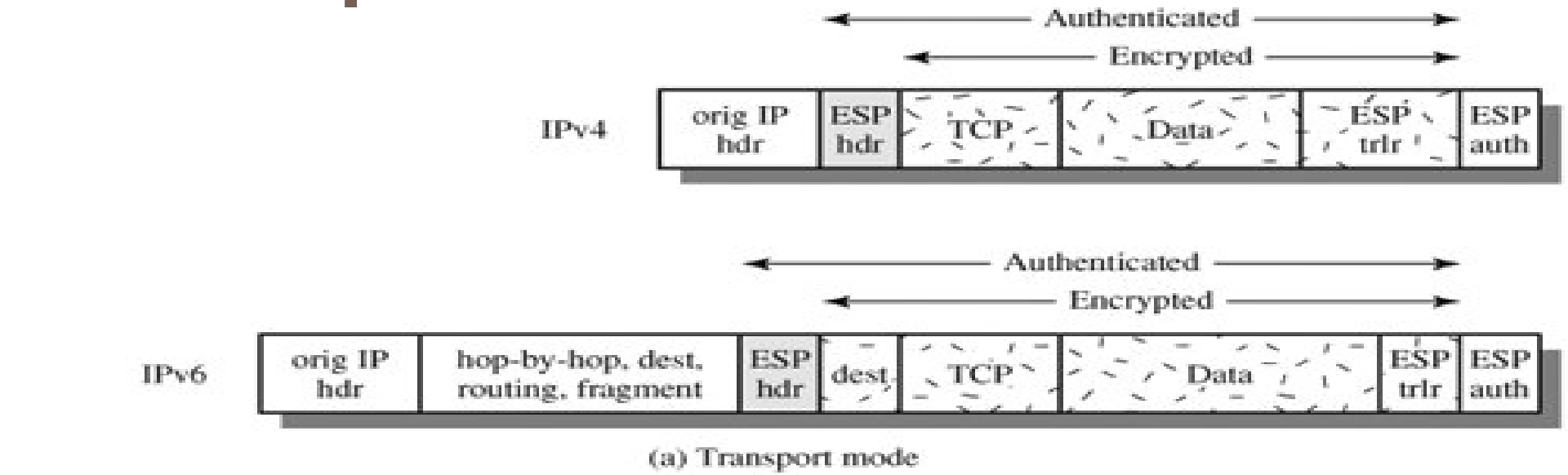
Encryption and Authentication Algorithms-ESP

- Three-key triple DES
- RC5
- IDEA
- Three-key triple IDEA
- CAST
- Blowfish
- As with AH, ESP supports the use of a MAC with a default length of 96 bits. Also as with AH, the current specification dictates that a compliant implementation must support HMAC-MD5-96 and HMAC-SHA-1-96.

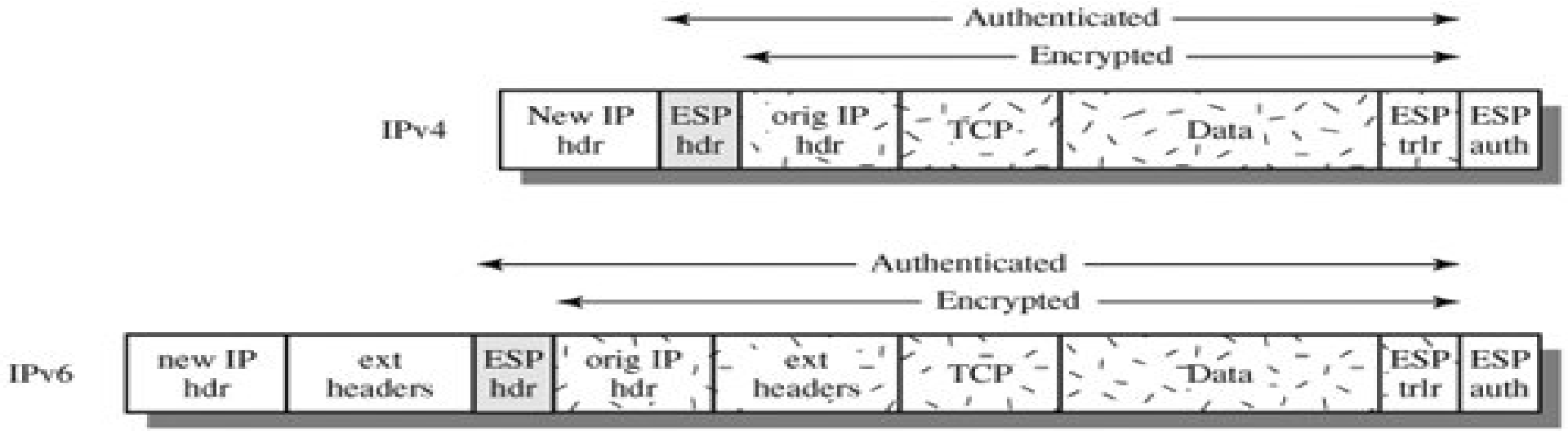
Transport and Tunnel Modes-ESP

- ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header.
- ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header.

Transport and Tunnel Modes-ESP



(a) Transport mode



(b) Tunnel mode

Overview

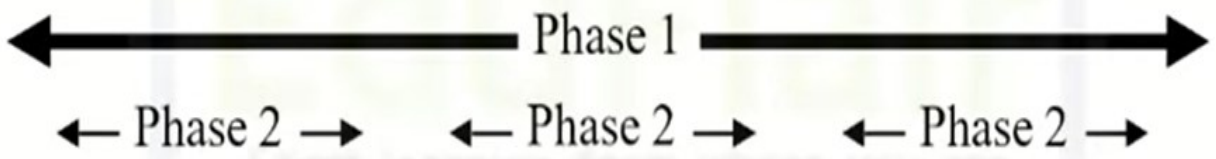
- IPSec review
- Internet Key Exchange
  - Phase 1 (Main mode / Aggressive mode)
  - Phase 2 (Quick mode)
- IKE Authentication methods

Overview of IPSec

- The IP protocol itself doesn't have any security features at all.
- IPSec is a framework that helps us to protect IP traffic on the network layer.
- IPSec can protect our traffic with the following features:
  - Confidentiality
  - Integrity
  - Authentication
  - Anti-replay

Internet Key Exchange

- Before we can protect any IP packets, we need two IPSec entity that build the IPSec tunnel.
- To establish an IPSec tunnel, we use a protocol called IKE (Internet Key Exchange).
- There are two phases:
  - **IKE phase 1**: Mutual authentication and session keys
  - **IKE phase 2**: Use results of phase 1 to create multiple associations between the same entities



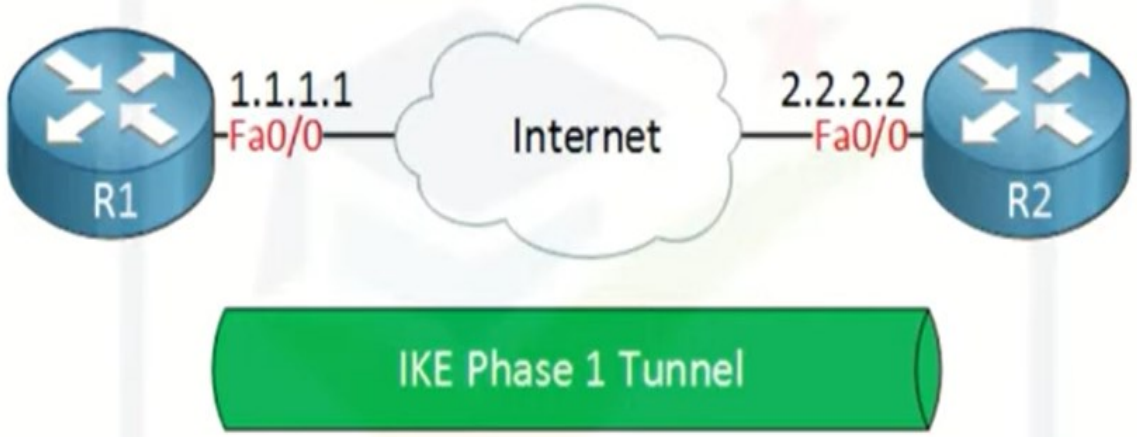
IKE Phase 1

IKE Phase 1

- Two peers negotiate about the encryption, authentication, hashing and other protocols that they want to use and some other parameters that are required.
- In this phase, an ISAKMP (Internet Security Association and Key Management Protocol) session is established.
- This is also called the ISAKMP tunnel or IKE phase 1 tunnel.
- The collection of parameters that the two devices will use is called a SA (Security Association).

IKE Phase 1

Example of two routers that have established the IKE phase 1 tunnel:



- Only used for management traffic.
- This tunnel is used as a secure method to establish the second tunnel called the IKE phase 2 tunnel or IPsec tunnel and for management traffic like keepalives.

Steps in Phase 1

The main purpose of IKE phase 1 is to establish a secure tunnel that we can use for IKE phase 2.

We can break down phase 1 in three simple steps:

Step 1 : Negotiation :The two peers will negotiate about the following items:

- Hashing (MD5, SHA)
- Authentication (Pre-shared keys, DSS, etc)
- DH (Diffie Hellman) parameters
- Lifetime
- Encryption (DES, 3DES, IDEA)

Step 2: DH Key Exchange: Both entities use the DH group that they negotiated to exchange keying material. The end result will be that both peers will have a shared key.

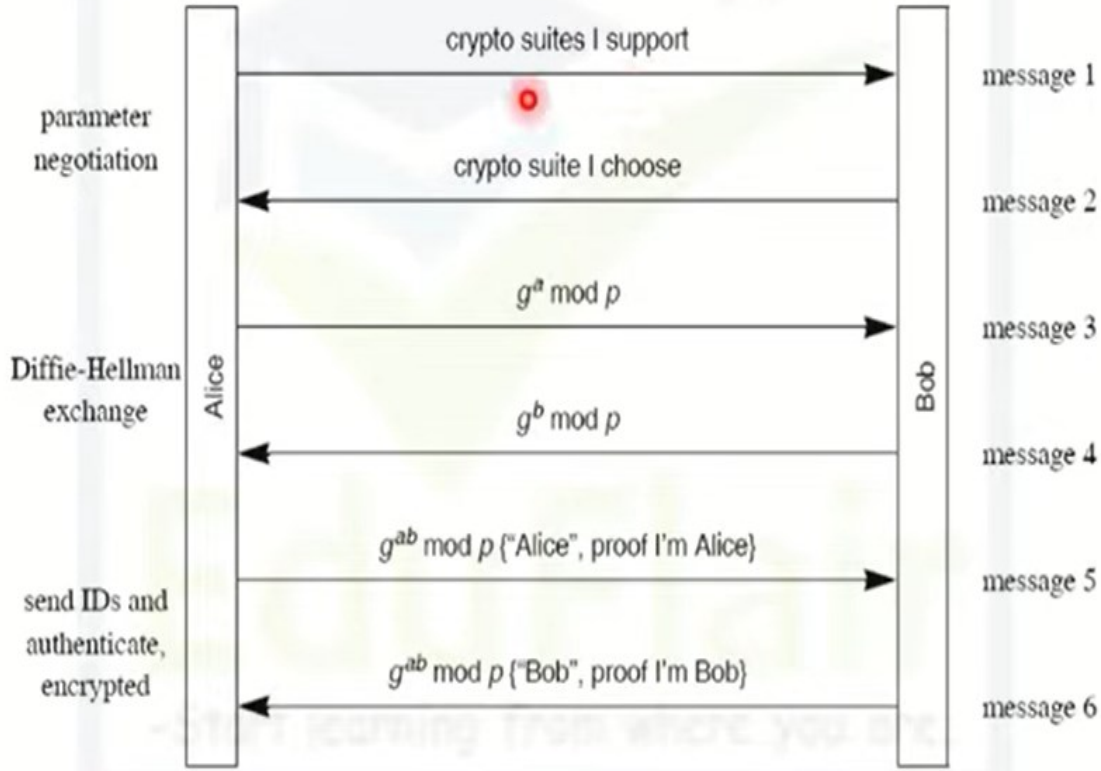
Step 3: Authentication: The two peers will authenticate each other using the authentication method that they agreed upon on in the negotiation. The end result is a IKE phase 1 tunnel (ISAKMP tunnel) which is bidirectional.

Modes of Phase 1

- The three steps above can be completed using two different modes:
  - Main mode
  - Aggressive mode
- Main mode uses six messages while aggressive mode only uses three messages.
- Main mode is considered more secure.

IKE Main Mode

- Allows ability to hide end-point identifiers and to select crypto algorithms ⇒ requires 6 messages



IKE Main Mode

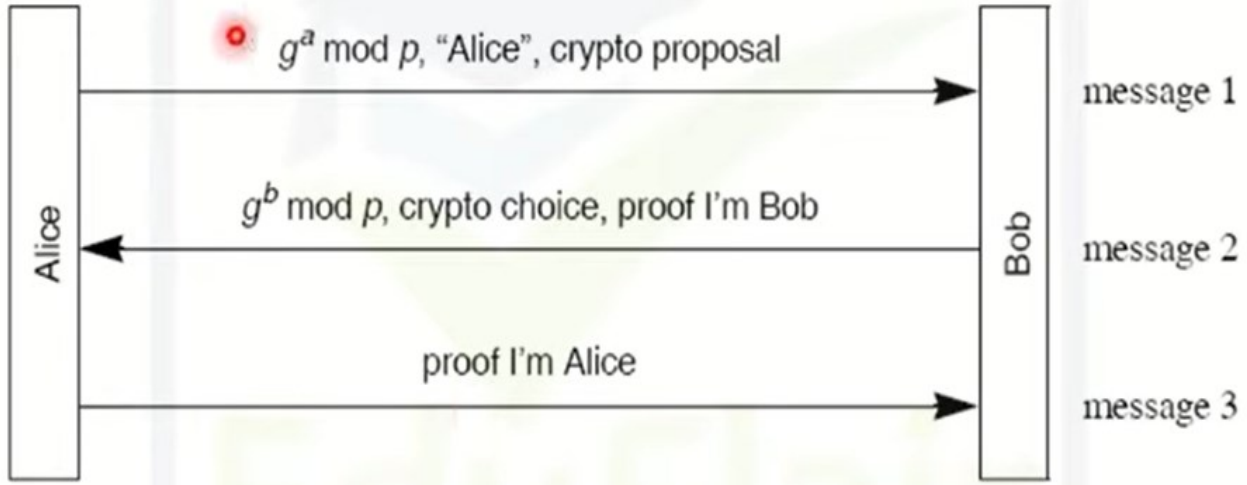
•The first two messages negotiate policy;

• the next two exchange Diffie-Hellman public values and nonces necessary for the exchange;

• and the last two messages authenticate the Diffie-Hellman Exchange.

IKE Aggressive Mode

- End-points ID not hidden ⇒ Requires only three messages



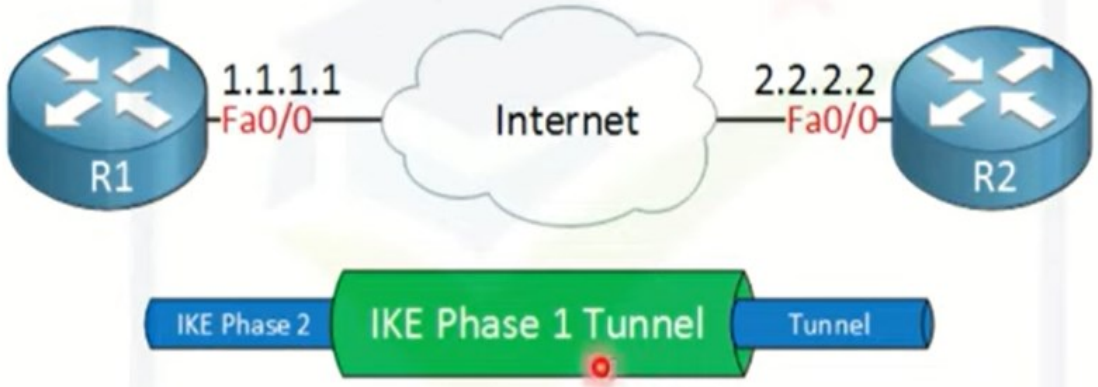
IKE Authentication Methods

1. Original Public Key Encryption (separately encrypt each field with other sides public key)
2. Revised Public Key Encryption (Encrypt session key with public key. Use session key to encrypt the rest)
3. Public key signature
4. Pre-shared secret key

4 Methods × 2 Modes = 8 variants of Phase 1

IKE Phase 2

Example of two routers completed phase 2:

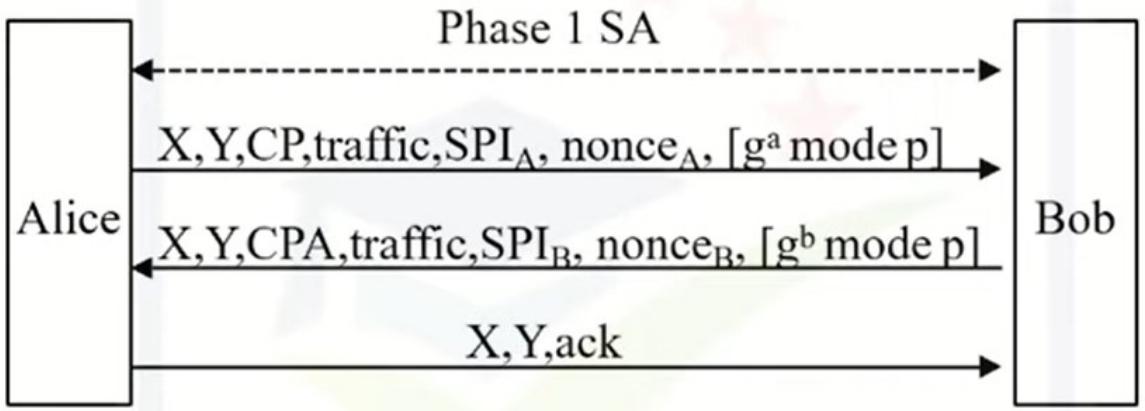


- Once IKE phase 2 is completed, we have an IKE phase 2 tunnel (or IPsec tunnel) that we can use to protect our user data.

IKE Phase 2

- IPsec (AH or ESP) SA can be set up in Phase 2
  $\Rightarrow$ Negotiate crypto parameters, another optional DH (for perfect forward secrecy), traffic selectors
- Traffic selector = IP address or mask, IP protocol type, and TCP/UDP port
- If traffic selector is wider than the acceptable, the request will be refused
- Phase 2 is also known as **quick mode.**

IKE Phase 2 (Cont)



- X = pair of cookies generated in phase 1
- Y = a 32-bit number to distinguish different phase 2 sessions
- CP = Crypto Proposal, CPA = Crypto Proposal Accepted
- X and Y are in clear rest of the phase 2 messages are encrypted and integrity protected
- IV = ack of the previous message.