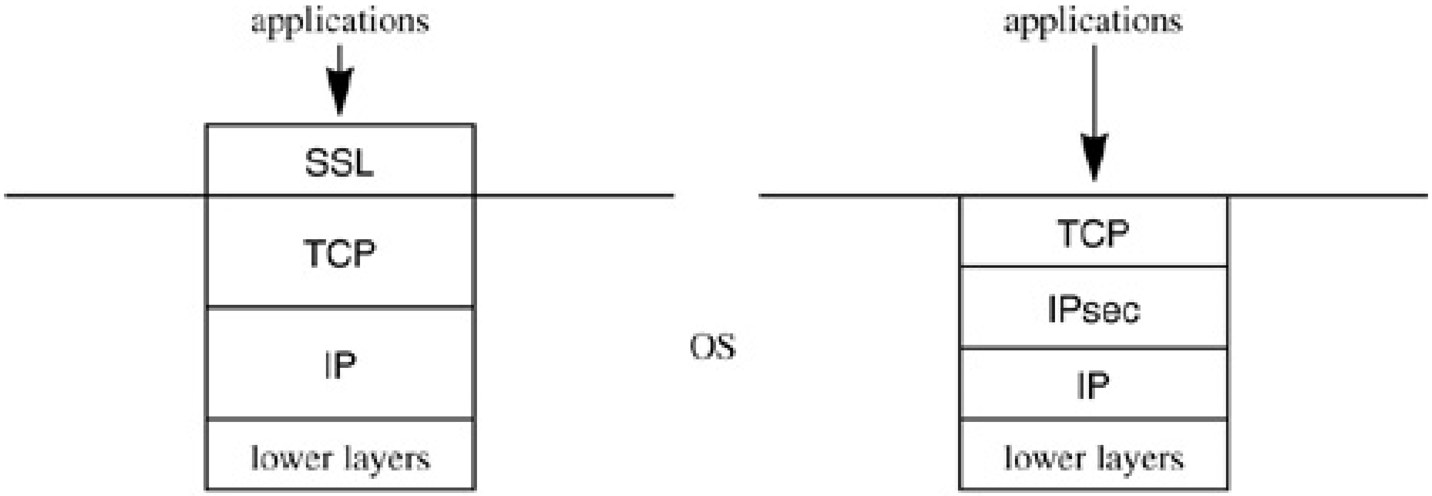
IPSec

Presentation by:
V. Balasubramanian
SSN College of Engineering

Introduction

- SSL/TLS and SSH are said to be "implemented at layer 4",
- whereas IPsec is said to be "implemented at layer 3".

Contd…



applications

SSL

TCP

IP

lower layers

OS

applications

TCP

IPsec

IP

lower layers

SSL/TLS or SSH operate above TCP.
OS doesn't change. Applications do.

IPsec is within the OS. OS changes.
Applications and API to TCP are unchanged.

SSL

- SSL is that it is easier to deploy something if you don't have to change the operating system, so these protocols act "above TCP".
- It requires the applications to interface to SSL instead of TCP. The name Secure Sockets Layer comes from the most popular API to TCP, which is called "sockets".

IPSec

- IPsec - implementing security within the operating system automatically causes all applications to be protected without the applications having to be modified.
- TCP will not be participating in the cryptography.
- TCP checksum.

Problem

- If malicious data is inserted into the packet stream, as long as the bogus data passes the (noncryptograpic) TCP checksum.
- TCP will acknowledge such data and send it up to SSL.
- SSL will discard it because the integrity check will indicate the data is bogus.

Contd…

- SSL will discard it because the integrity check will indicate the data is bogus, but there is no way for SSL to tell TCP to accept the real data at this point.
- When the real data arrives, TCP will assume it is duplicate data and discard it.

IPSec

- IPsec's approach of cryptographically protecting each packet independently can better protect against such an attack.
- It causes the traffic on the path between the communicating parties to be encrypted, hiding it from eavesdroppers.

Contd…

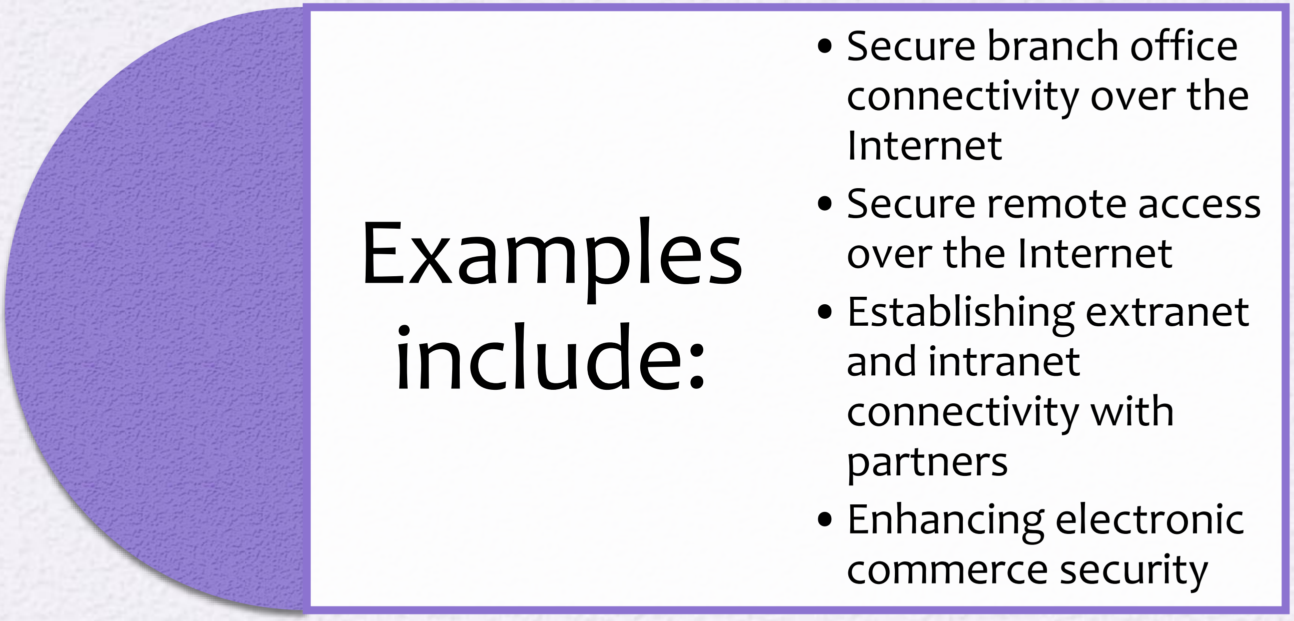
- An attacker can launch a successful denial-of-service attack by inserting a single packet into the data stream.

Application Specific Security

- electronic mail (S/MIME, PGP), client/server (Kerberos), Web access (Secure Sockets Layer).
- security concerns that cut across protocol layers.
- implementing security at the IP level, -secure networking not only for applications / security-ignorant applications.

Applications of IPsec

- IPsec provides the capability to secure communications across a LAN, private and public WANs, and the Internet



Examples include:

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security

- Principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level
  - Thus all distributed applications (remote logon, client/server, e-mail, file transfer, Web access) can be secured

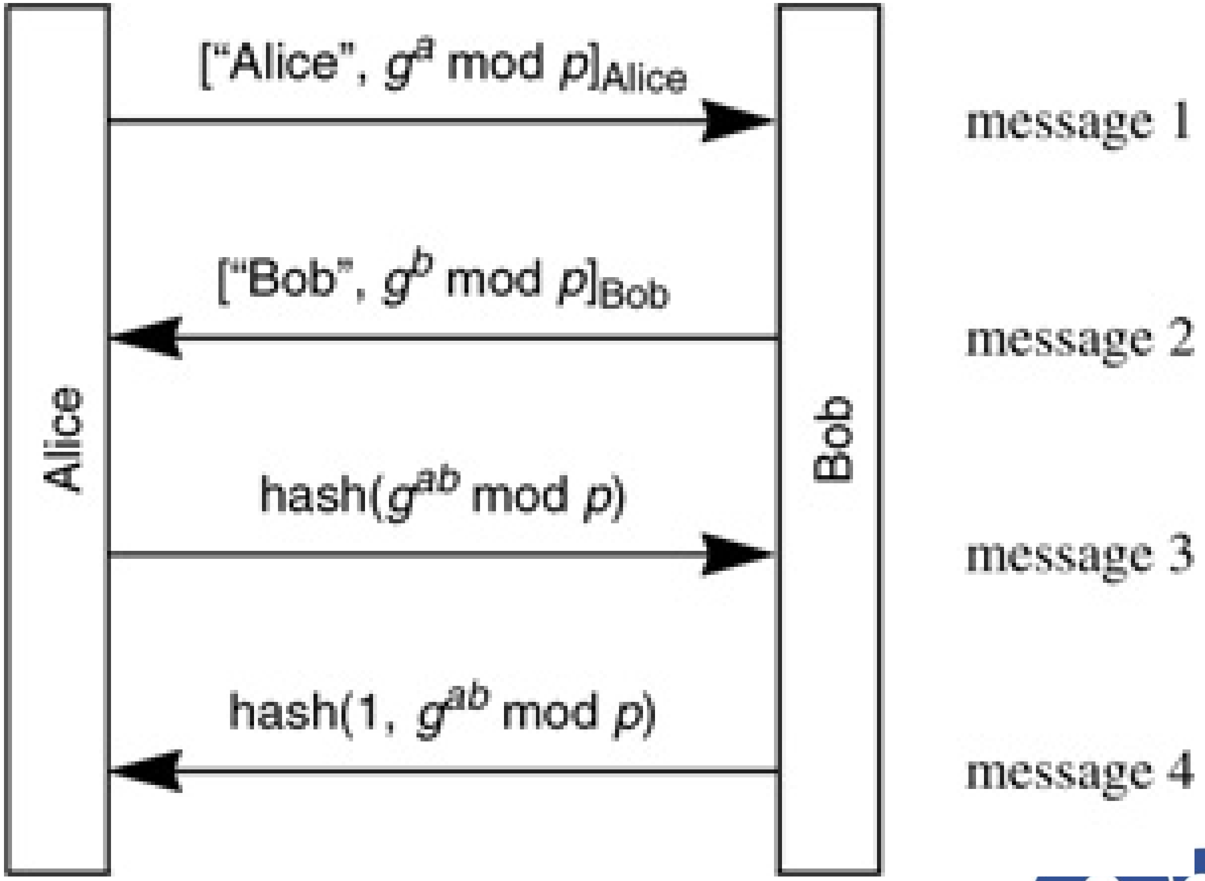
- IP-level security encompasses three functional areas: authentication, confidentiality, and key management.
- The authentication mechanism: assures that a received packet was, in fact, transmitted by the party identified as the source.

Contd…

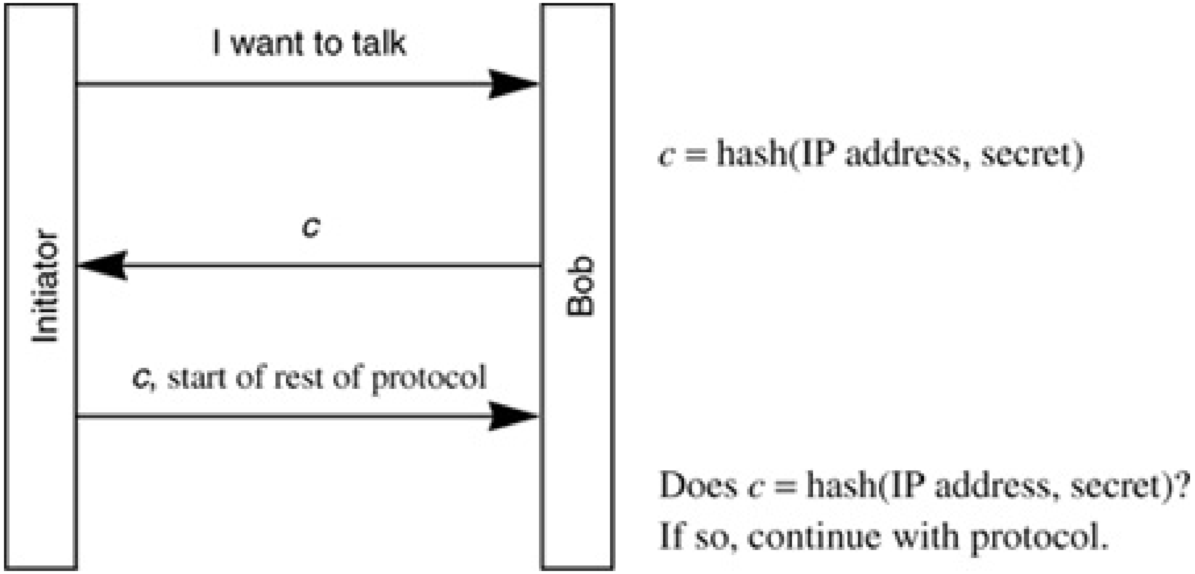
- The confidentiality facility enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.
- The key management facility is concerned with the secure exchange of keys.

Session Key Establishments

Diffie-Hellman for perfect forward secrecy using signature keys


Alice
Bob
["Alice", g^a mod p]$_{\text{Alice}}$
message 1
["Bob", g^b mod p]$_{\text{Bob}}$
message 2
hash(g^{ab} mod p)
message 3
hash(1, g^{ab} mod p)
message 4

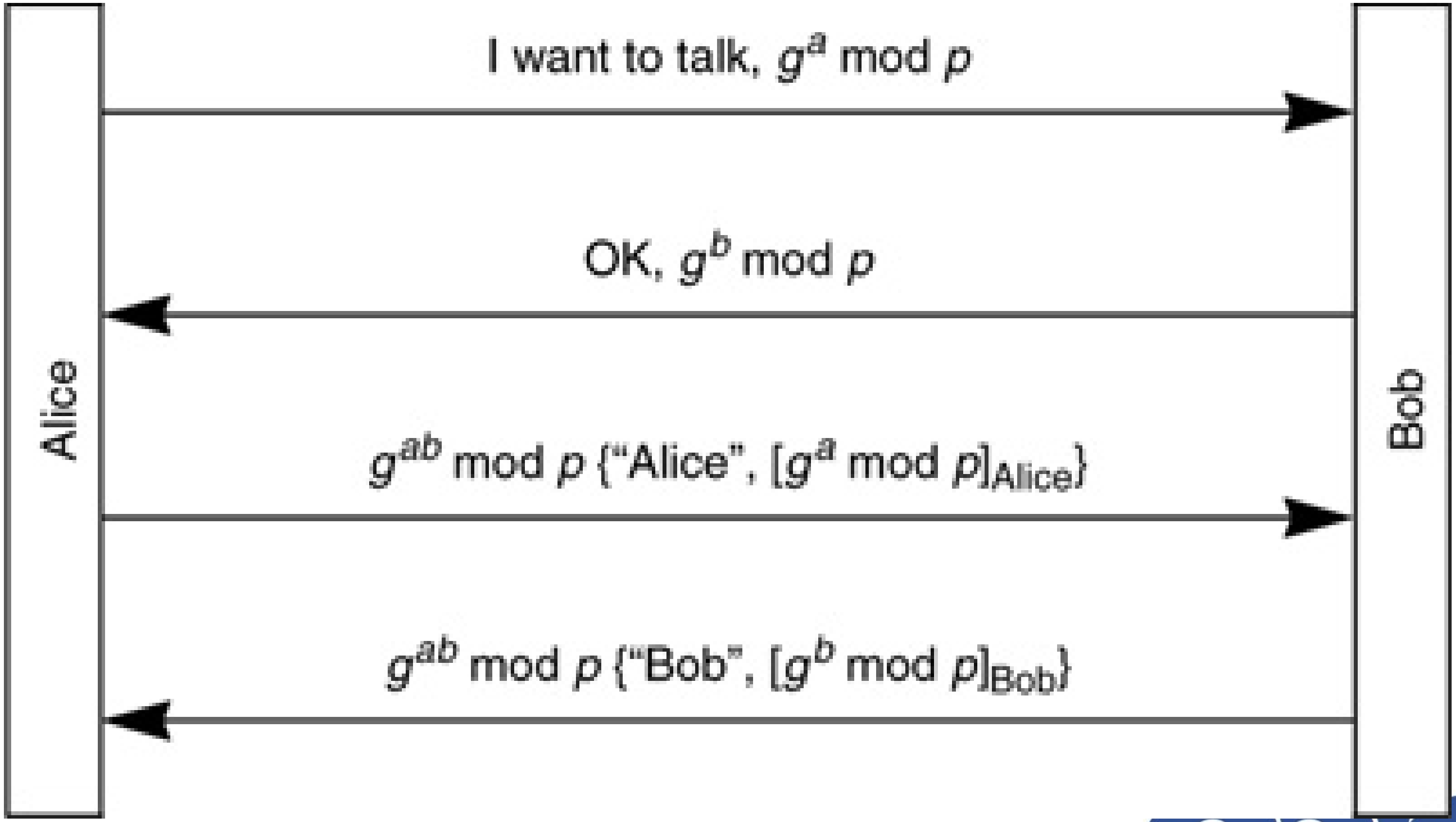
Stateless cookie protocol



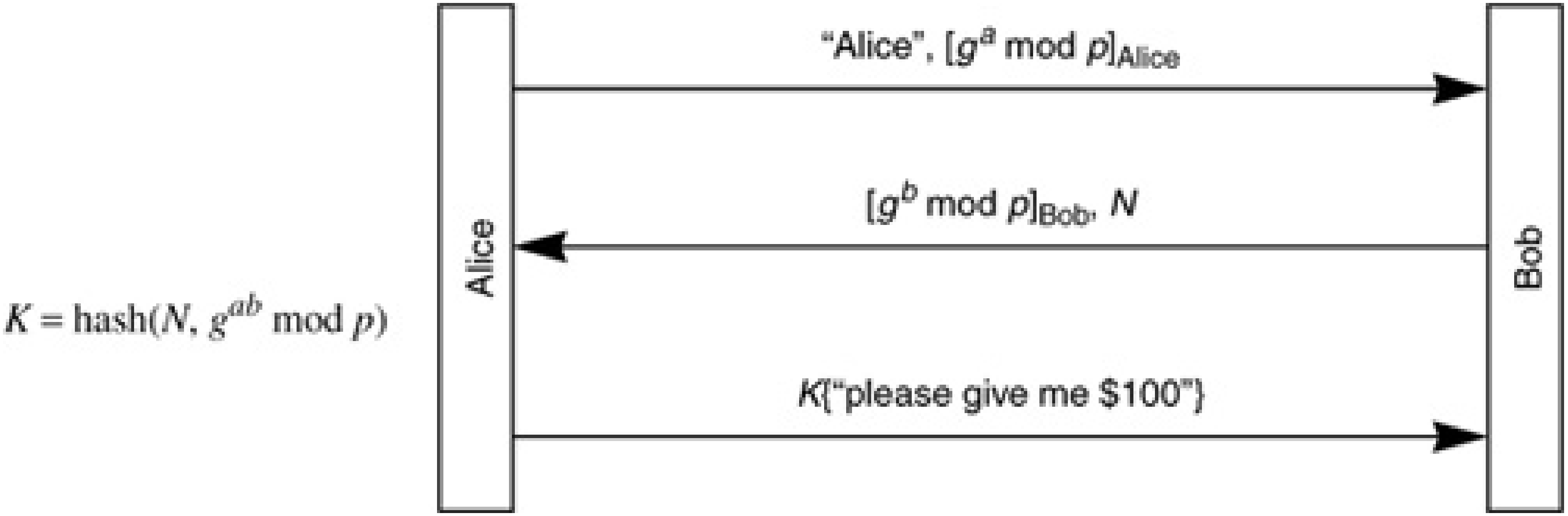
c = hash(IP address, secret)

Does c = hash(IP address, secret)?
If so, continue with protocol.

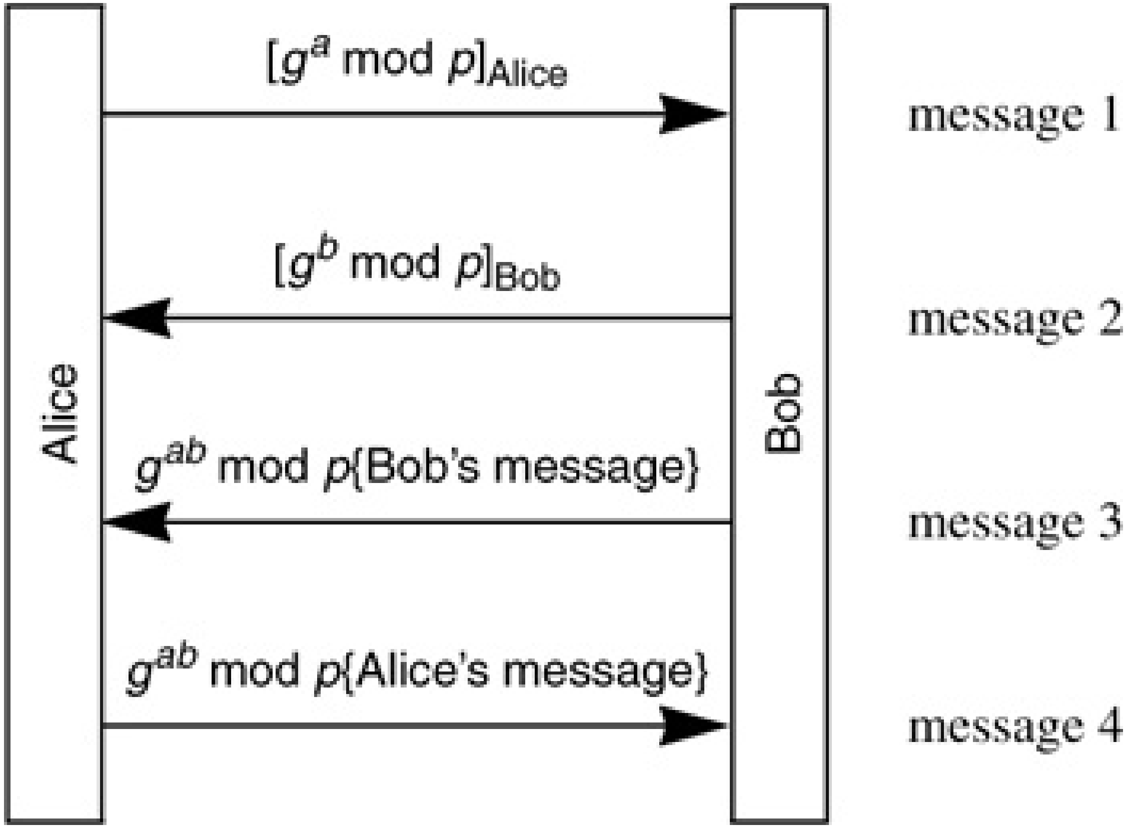
Identity Hiding


Alice
Bob
I want to talk, $g^a \bmod p$
OK, $g^b \bmod p$
$g^{ab} \bmod p$ {"Alice", $[g^a \bmod p]_{\text{Alice}}$}
$g^{ab} \bmod p$ {"Bob", $[g^b \bmod p]_{\text{Bob}}$}

Using a nonce so Bob knows it's not replayed messages from Alice


"Alice", $[g^a \bmod p]_{\text{Alice}}$
$[g^b \bmod p]_{\text{Bob}}$, N
$K\{$"please give me \$100"$\}$
Alice
Bob
$K = \text{hash}(N, g^{ab} \bmod p)$

Parallel Computing used in Lotus Notes


Alice
Bob
$[g^a \bmod p]_{\text{Alice}}$
message 1
$[g^b \bmod p]_{\text{Bob}}$
message 2
$g^{ab} \bmod p$\{Bob's message\}
message 3
$g^{ab} \bmod p$\{Alice's message\}
message 4

IPSec

- IPsec is an IETF standard for real-time communication security.
- The main pieces of IPsec are AH and ESP (Authentication Header-Encapsulation Security Payload) -for carrying cryptographically protected data, and
- IKE (Internet Key Exchange), which is a protocol for authenticating and establishing a session key.

Contd…

- IPsec assumes that two nodes already have a shared session key, which might have been configured manually, or established through IKE.

Example

- Since Bob might be receiving IPsec-protected packets from many sources, maybe even different processes using the same source IP address, there has to be a way for Bob to know which cryptographic key and which algorithms to use to process the packet.

- This is done by inserting an IPsec header (AH and/or ESP) into the IP packet which tells Bob to which security association the packet belongs.
- IPsec works with IPv4 or with IPv6.

Benefits of IPSec

- Some of the 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
    - Traffic within a company or workgroup does not incur the overhead of security-related processing
  - 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
  - IPsec is below the transport layer (TCP, UDP) and so is transparent to applications
    - There is no need to change software on a user or server system when IPsec is implemented in the firewall or router
  - IPsec can be transparent to end users
    - There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization
  - 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

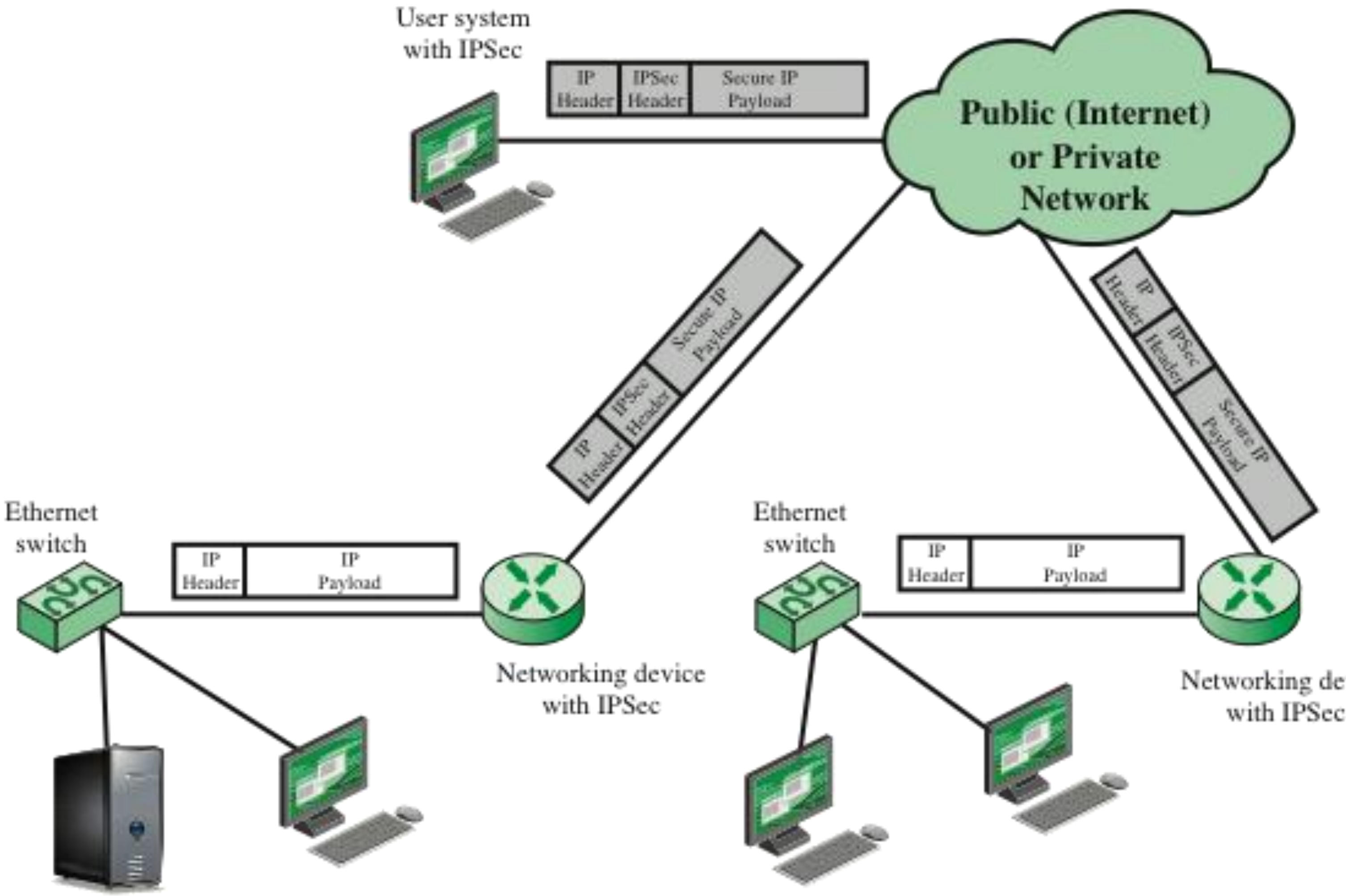


Figure 20.1 An IP Security Scenario

Security Associations

- An IPsec security association (SA) is a cryptographically protected connection.
- Associated with each end of the SA is a cryptographic key and other information such as the identity of the other end, the sequence number currently being used, and the cryptographic services being used (e.g., integrity only, or encryption + integrity, and which cryptographic algorithms should be used).

- The SA is considered unidirectional, so a conversation between Alice and Bob will consist of two SAs, one in each direction.
- The IPsec header includes a field known as the SPI (SECURITY PARAMETER INDEX) which identifies the security association.

SA

- The SA is defined by the triple <SPI, destination address, flag for whether it's AH or ESP>.

IPSec

- IPSec acts at the network layer, protecting and authenticating IP packets between a PIX (Private Internet Exchange)Firewall and other participating IPSec devices (peers), such as other PIX Firewalls

- **Data confidentiality**—The IPSec sender can encrypt packets before transmitting them across a network.
- **Data integrity**—The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- **Data origin authentication**—The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- **Antireplay**—The IPSec receiver can detect and reject replayed packets.

- IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers at the IP layer.

- IPSec consists of the following two main protocols:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

- Data Encryption Standard (DES)
- Triple DES (3DES)
- Diffie-Hellman (D-H)
- Message Digest 5 (MD5)
- Secure Hash Algorithm-1 (SHA-1)
- Rivest, Shamir, and Adelman (RSA) Signatures
- Internet Key Exchange (IKE)
- Certificate Authorities (CAs)

IPSec - Authentication Header

- Authentication Header (AH) provides authentication and integrity to the datagrams passed between two systems.
- It achieves this by applying a keyed one-way hash function to the datagram to create a message digest. If any part of the datagram is changed during transit, it will be detected by the receiver.

- AH can also enforce antireplay protection by requiring that a receiving host sets the replay bit in the header to indicate that the packet has been seen.

AH (Authentication Header)

1	next header
1	payload length
2	unused
4	SPI (Security Parameter Index)
4	sequence number
variable	authentication data

AH

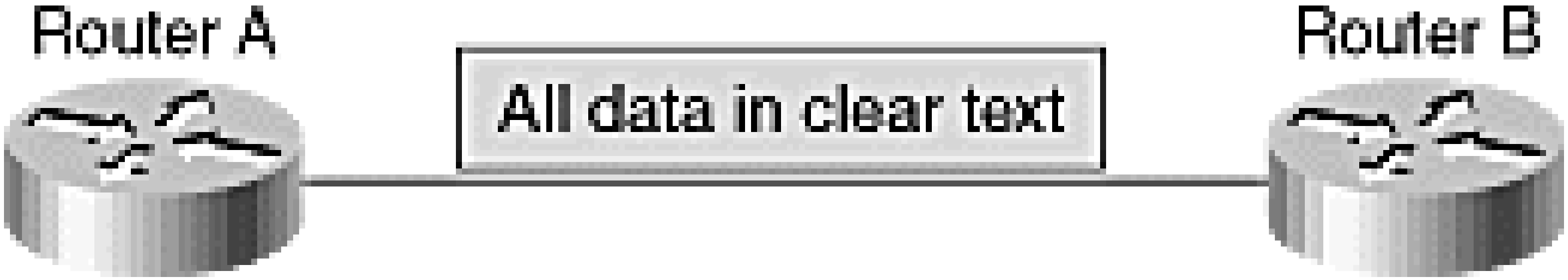
- NEXT HEADER. if TCP follows the AH header, then NEXT HEADER is 6.
- PAYLOAD LENGTH. The size of the AH header in 32-bit chunks, not counting the first 8 octets.
- SPI.
- SEQUENCE NUMBER. sequence number is assigned by AH and used so that AH can recognize replayed packets and discard them.
- AUTHENTICATION DATA. This is the cryptographic integrity check on the data.

Mutable fields

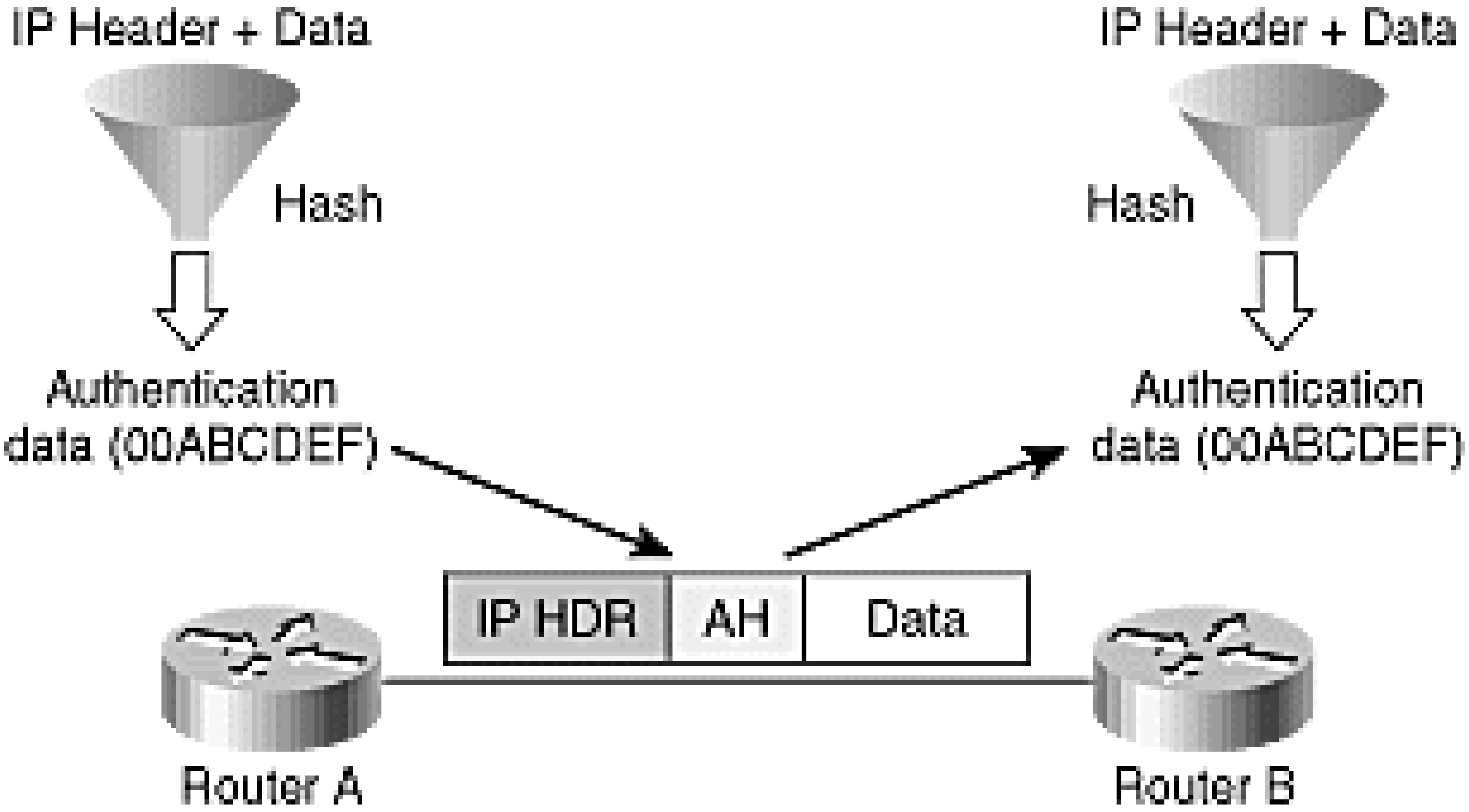
- TYPE OF SERVICE, FLAGS, FRAGMENT OFFSET, TIME TO LIVE, and HEADER CHECKSUM.

Steps

- The IP header and data payload is hashed.
- The hash is used to build a new AH header, which is appended to the original packet.
- The new packet is transmitted to the IPSec peer router.
- The peer router hashes the IP header and data payload, extracts the transmitted hash from the AH header, and compares the two hashes. The hashes must match exactly.

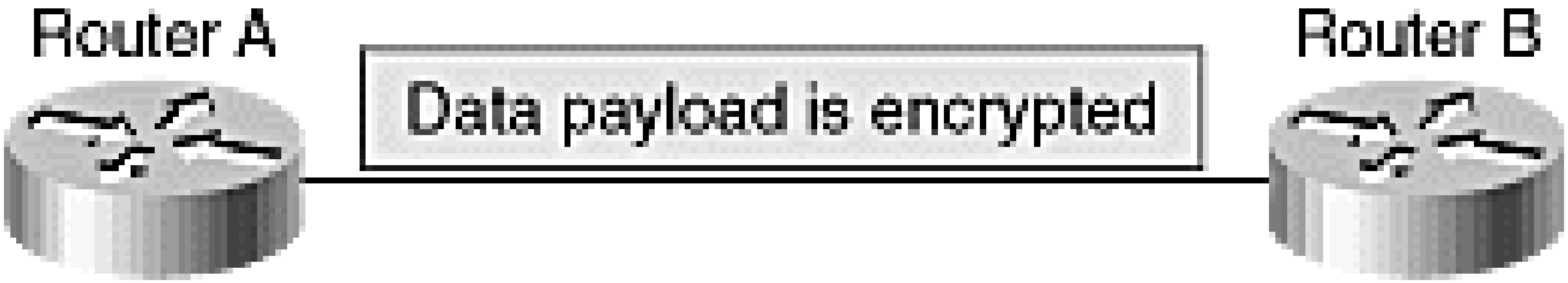


- Ensures data integrity
- Provides origin authentication—ensures packets definitely came from peer router
- Uses keyed-hash mechanism
- Does NOT provide confidentiality (no encryption)
- Provides optional replay protection


IP Header + Data
Hash
Authentication data (00ABCDEF)
IP Header + Data
Hash
Authentication data (00ABCDEF)
IP HDR
AH
Data
Router A
Router B

IP Security Protocol—Encapsulating Security Payload (ESP)

- Encapsulating Security Payload (ESP) is a security protocol used to provide confidentiality (encryption), data origin authentication, integrity, optional antireplay service, and limited traffic flow confidentiality by defeating traffic flow analysis



- Data confidentiality (encryption)
- Limited traffic flow confidentiality
- Data integrity
- Optional data origin authentication
- Anti-replay protection
- Does not protect IP header

# octets	
4	SPI (Security Parameters Index)
4	sequence number
variable	IV (initialization vector)
variable	data
variable	padding
1	padding length (in units of octets)
1	next header/protocol type
variable	authentication data

Confidentiality

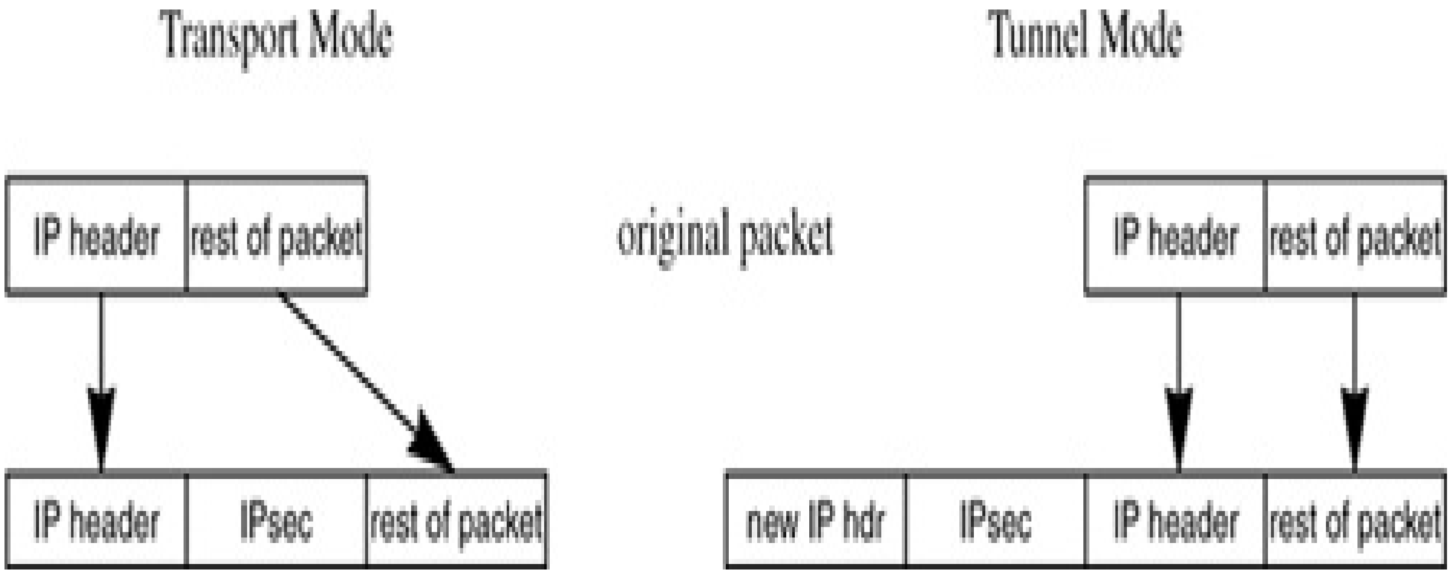
- Data Encryption Standard (DES)
- Triple DES (3DES)
- Diffie-Hellman (D-H)
- Message Digest 5 (MD5)
- Secure Hash Algorithm-1 (SHA-1)
- Rivest, Shamir, and Adelman (RSA) Signatures
- Internet Key Exchange (IKE)
- Certificate Authorities (CAs)

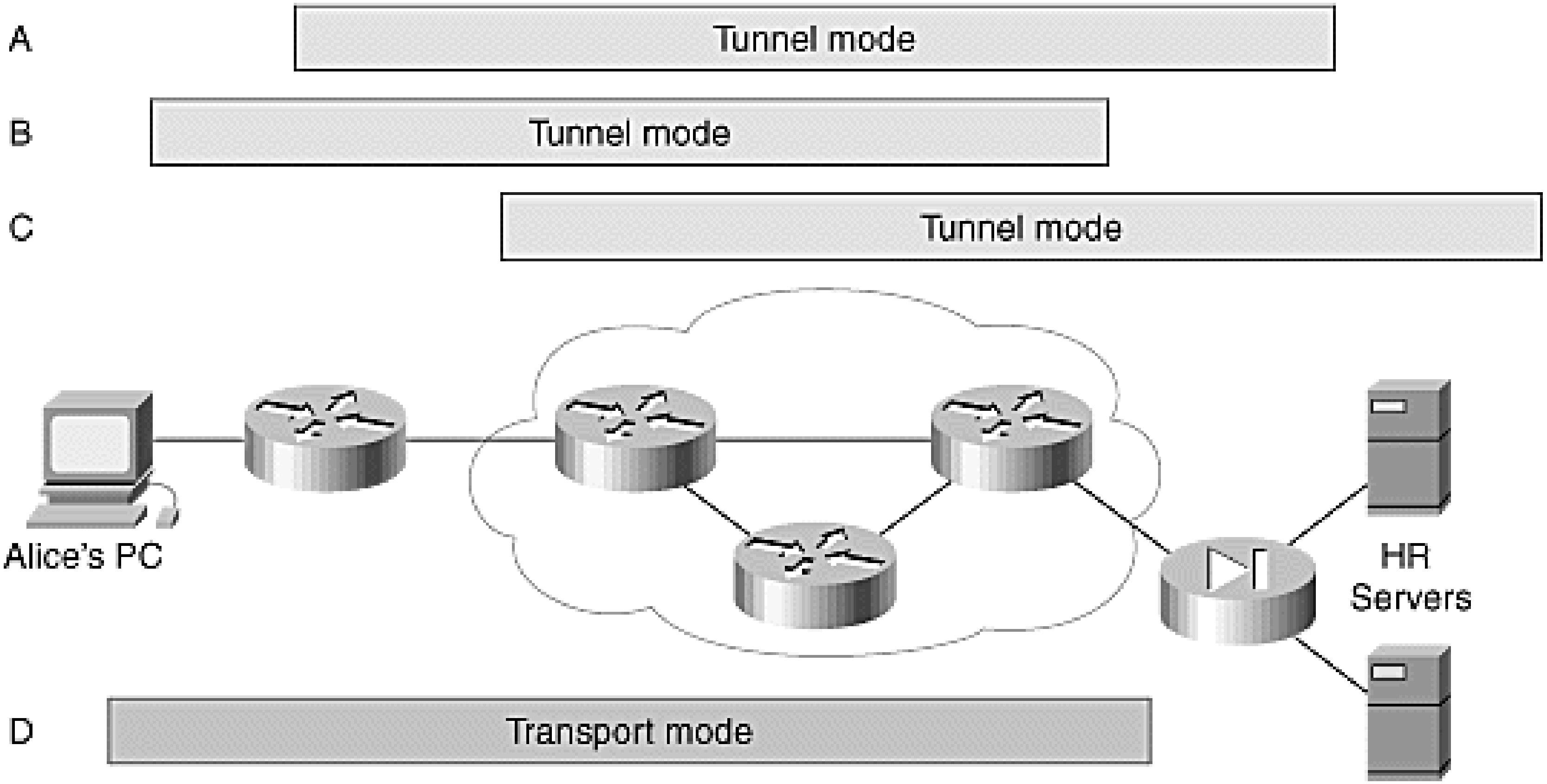
Internet Key Exchange

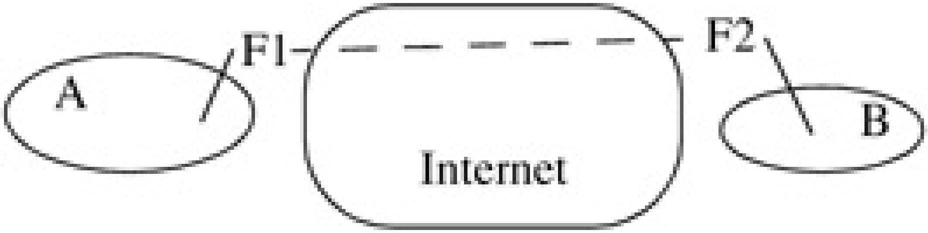
- Internet Key Exchange (IKE) is a hybrid protocol that provides utility services for IPSec: authentication of the IPSec peers, negotiation of IKE and IPSec security associations, and establishment of keys for encryption algorithms used by IPSec.

Modes

- IPSec can be run in either *tunnel* or *transport* modes


Transport Mode
Tunnel Mode
IP header
rest of packet
original packet
IP header
rest of packet
IP header
IPsec
rest of packet
new IP hdr
IPsec
IP header
rest of packet


A
Tunnel mode
B
Tunnel mode
C
Tunnel mode
Alice's PC
HR
Servers
D
Transport mode



added by firewall F1		original packet	
IP: src = F1, dst = F2	ESP	IP: src = A, dst = B	

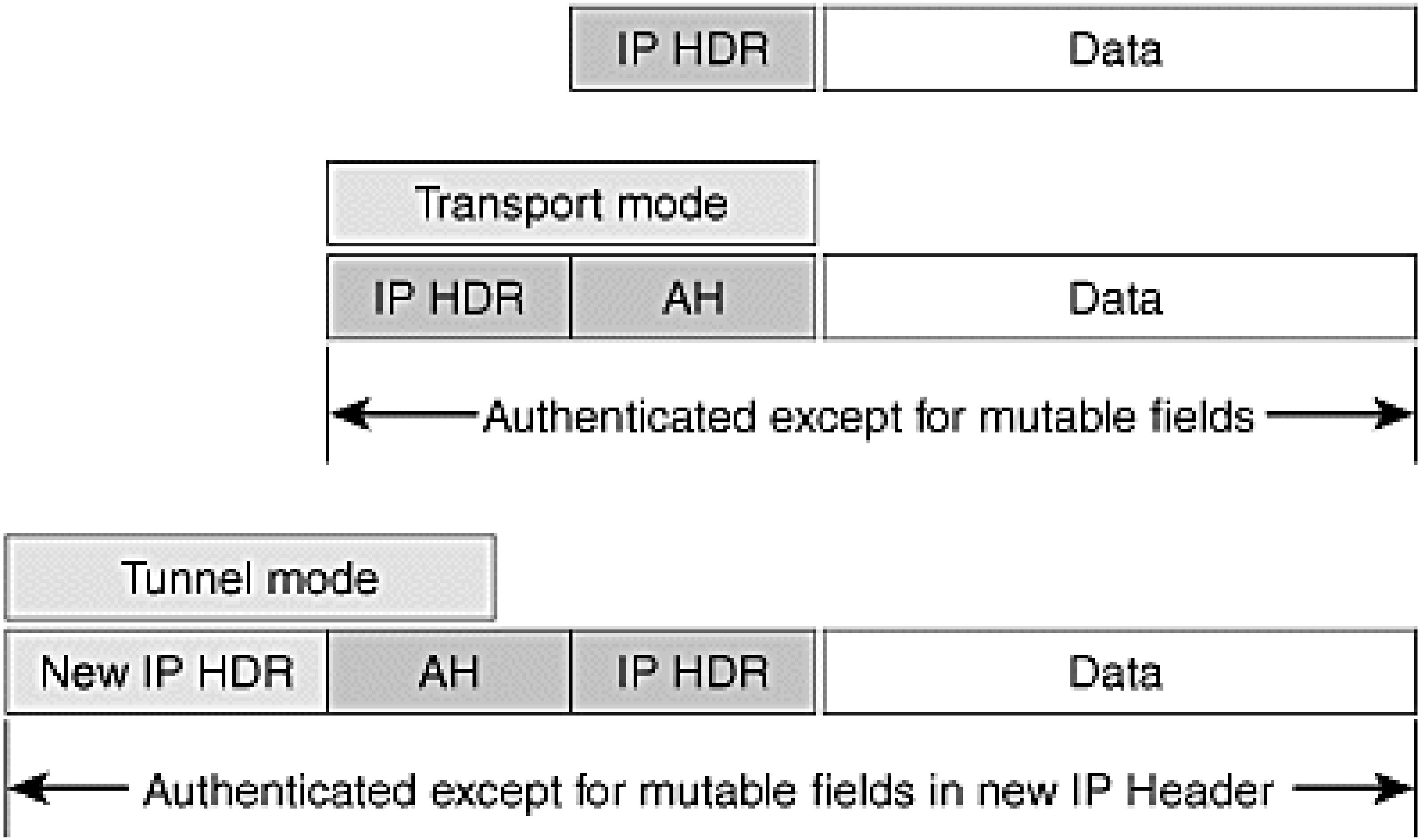
- Tunnel mode is most commonly used between gateways or from an end station to a gateway.
- Transport mode is used between end stations or between an end station and a gateway, if the gateway is being treated as a host;

- **Example A**—Tunnel mode is most commonly used to encrypt traffic between secure IPSec gateways, **Example B**—Tunnel mode is also used to connect an end station running IPSec software, such as the Cisco Secure VPN Client, to an IPSec gateway.

Contd…

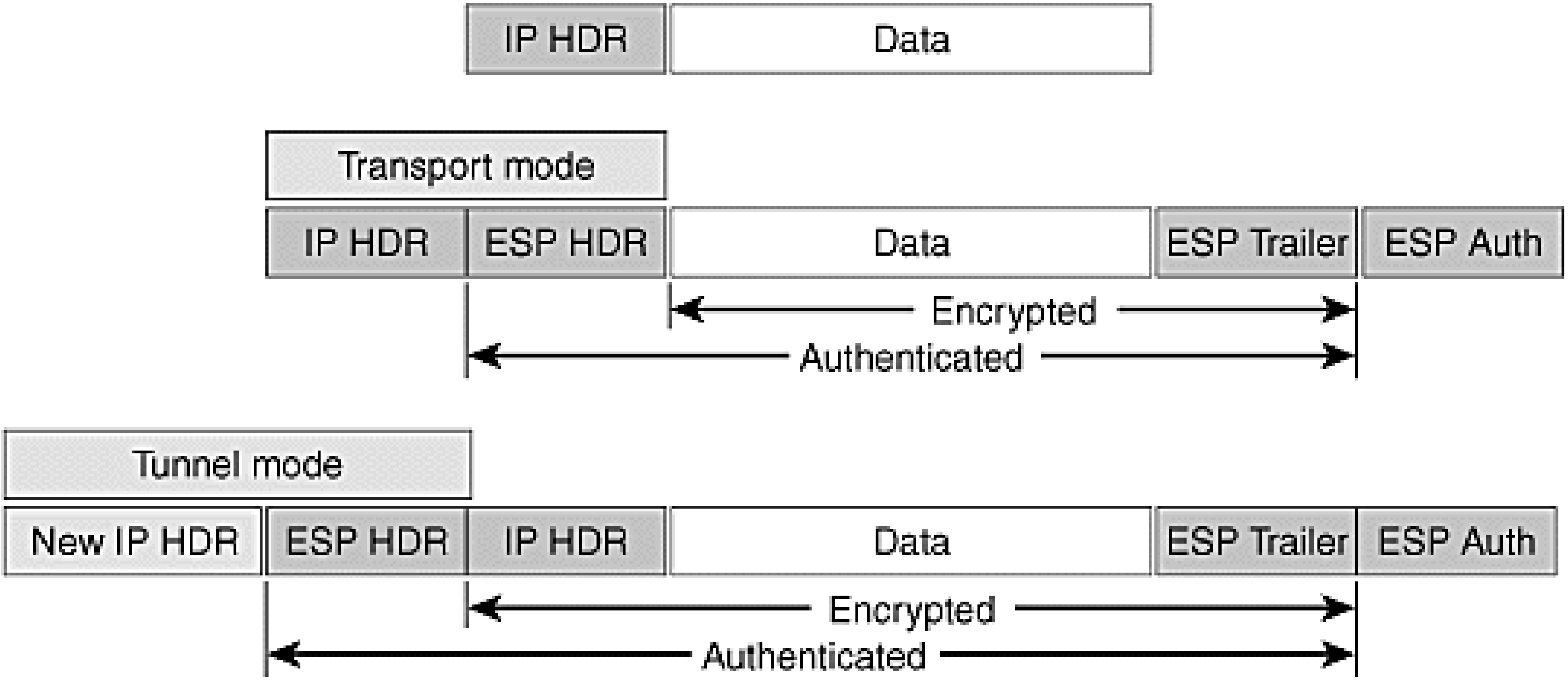
- **Example C**—In Example C, tunnel mode is used to set up an IPSec tunnel between the Cisco router and a server running IPSec software. **Example D**—Transport mode is used between end stations supporting IPSec or between an end station and a gateway if the gateway is being treated as a host. Transport mode is used to set up an encrypted Telnet session from Alice's PC running Cisco Secure VPN Client software

AH Tunnel Versus Transport Mode


IP HDR
Data
Transport mode
IP HDR
AH
Data
Authenticated except for mutable fields
Tunnel mode
New IP HDR
AH
IP HDR
Data
Authenticated except for mutable fields in new IP Header

- In transport mode, AH services protect the external IP header along with the data payload. AH services protect all the fields in the header that do not change in transport.
- In tunnel mode, the entire original header is authenticated, a new IP header is built, and the new IP header is protected in the same way.

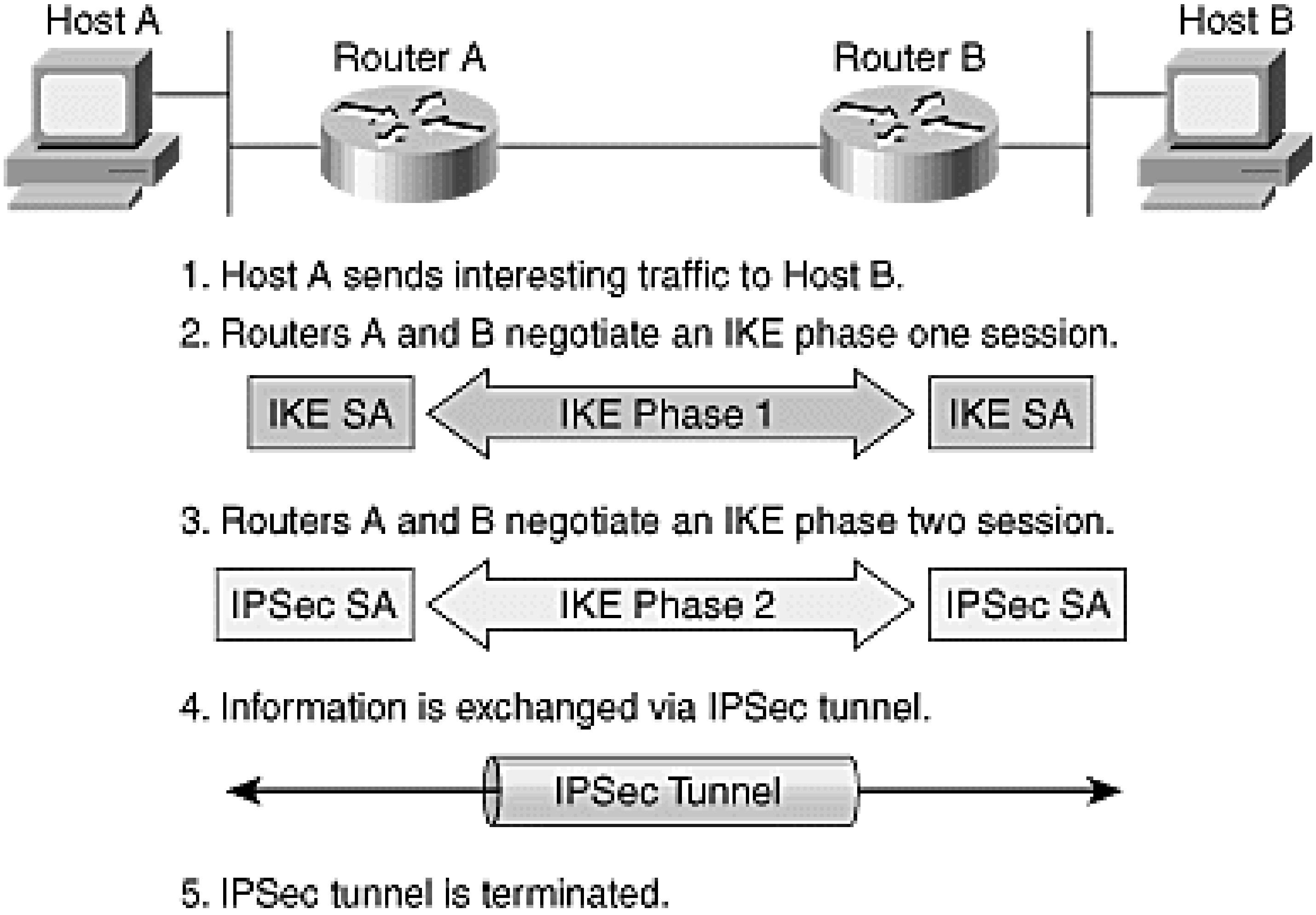
ESP Tunnel Versus Transport Mode



- In transport mode, the IP payload is encrypted and the original headers are left intact. The ESP header is inserted after the IP header and before the upper-layer protocol header. The upper-layer protocols are encrypted and authenticated along with the ESP header.

- In tunnel mode, the original IP header is well protected because the entire original IP datagram is encrypted. With an ESP authentication mechanism, the original IP datagram and the ESP header are included;

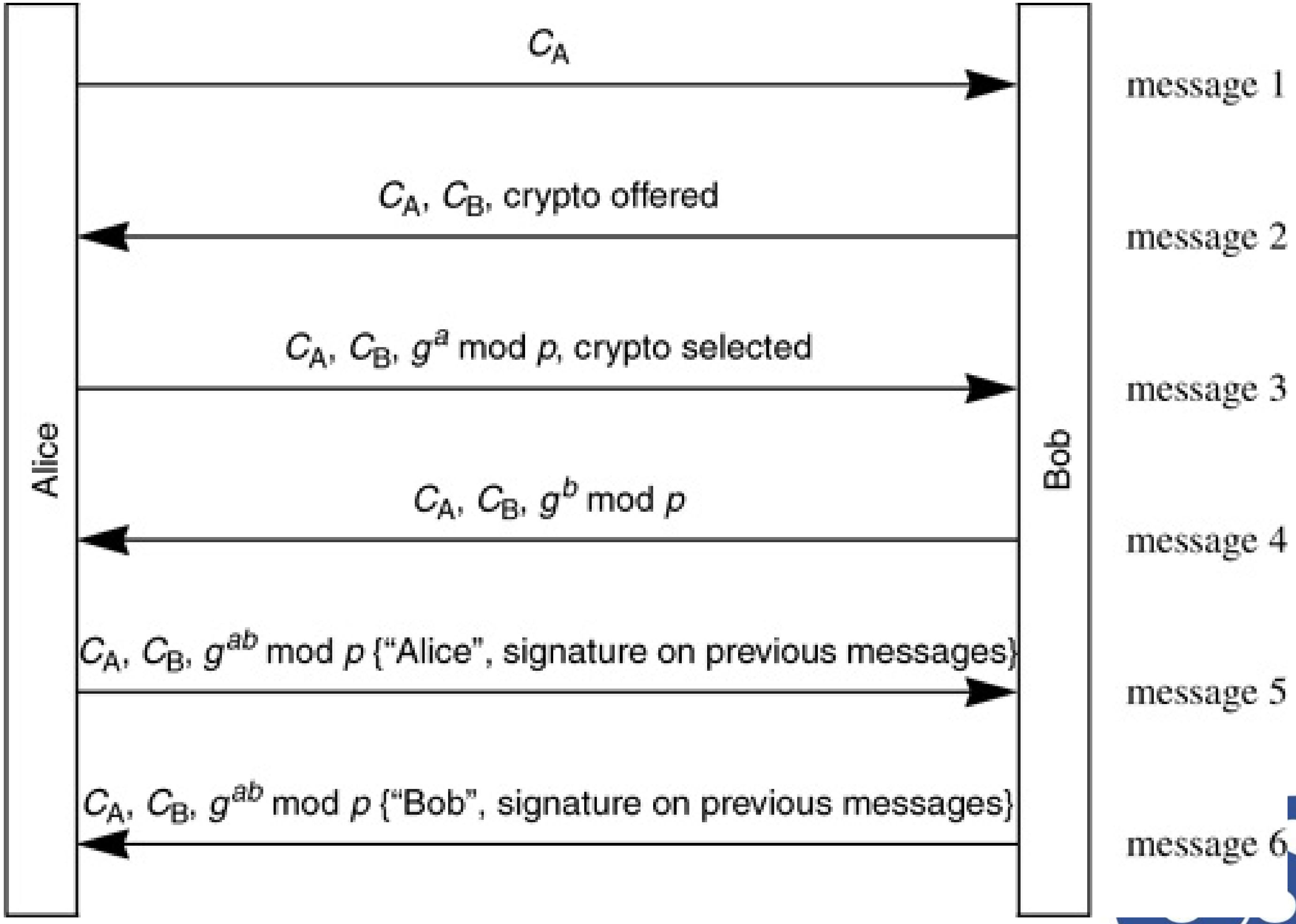
IPSec Works



1. Host A sends interesting traffic to Host B.
2. Routers A and B negotiate an IKE phase one session.
3. Routers A and B negotiate an IKE phase two session.
4. Information is exchanged via IPSec tunnel.
5. IPSec tunnel is terminated.

- IKE negotiates the IPSec security associations (SAs). This process requires that the IPSec systems first authenticate themselves to each other and establish ISAKMP (Internet Security Association and Key Management Protocol), or IKE, shared keys.

Photuris


Alice
Bob
C_A
message 1
C_A, C_B, crypto offered
message 2
C_A, C_B, g^a mod p, crypto selected
message 3
C_A, C_B, g^b mod p
message 4
C_A, C_B, g^{ab} mod p {"Alice", signature on previous messages}
message 5
C_A, C_B, g^{ab} mod p {"Bob", signature on previous messages}
message 6

Simple Key-Management for Internet Protocols

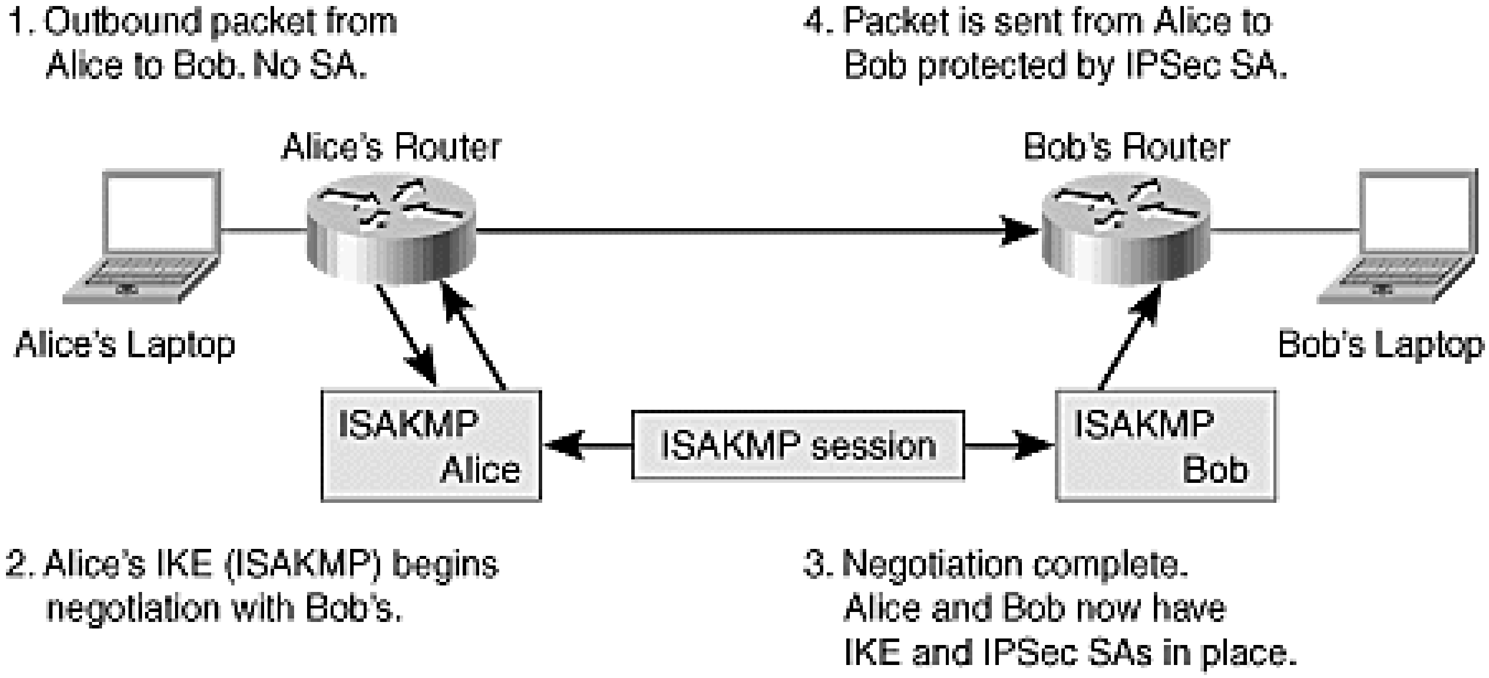
- long term Diffie-Hellman public keys (e.g., g^a mod p). Assuming Alice knows Bob's public key (g^b mod p), and her own private key (a), then she can compute g^{ab} mod p, the shared secret between herself and Bob.

IKE

- IKE defines two phases
- In phase one, IKE creates an authenticated secure channel between the two IKE peers that is called the IKE Security Association. The Diffie-Hellman key agreement is always performed in this phase.
- An ESP or AH SA would be established through phase 2

Phase 1

- Authenticates and protects the identities of the IPSec peers
- Negotiates a matching IKE SA policy between peers to protect the IKE exchange
- Performs an authenticated Diffie-Hellman exchange with the end result of having matching shared secret keys
- Sets up a secure tunnel to negotiate IKE phase two parameters



1. Outbound packet from Alice to Bob. No SA.

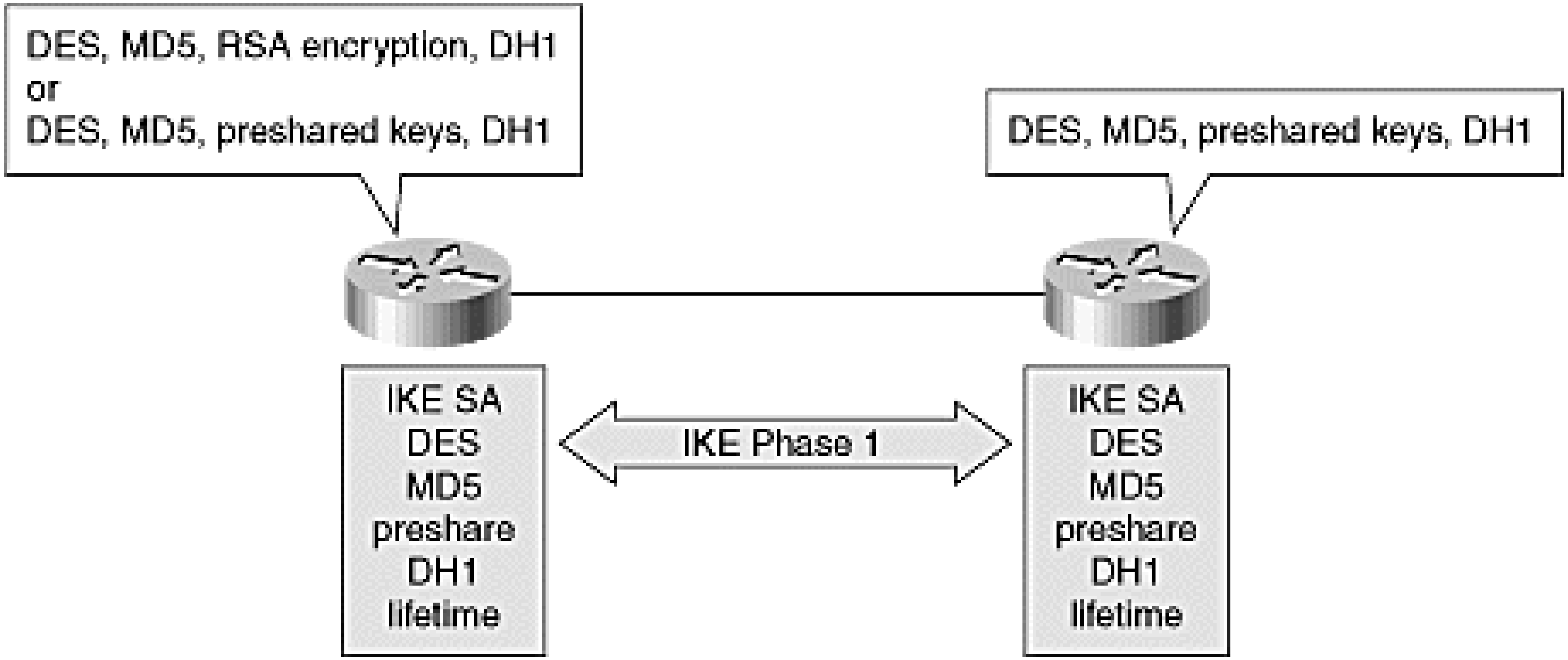
4. Packet is sent from Alice to Bob protected by IPSec SA.

2. Alice's IKE (ISAKMP) begins negotiation with Bob's.

3. Negotiation complete. Alice and Bob now have IKE and IPSec SAs in place.

- IKE sets up a secure channel to negotiate the IPSec security associations.

Phase 1



DES, MD5, RSA encryption, DH1
or
DES, MD5, preshared keys, DH1

DES, MD5, preshared keys, DH1

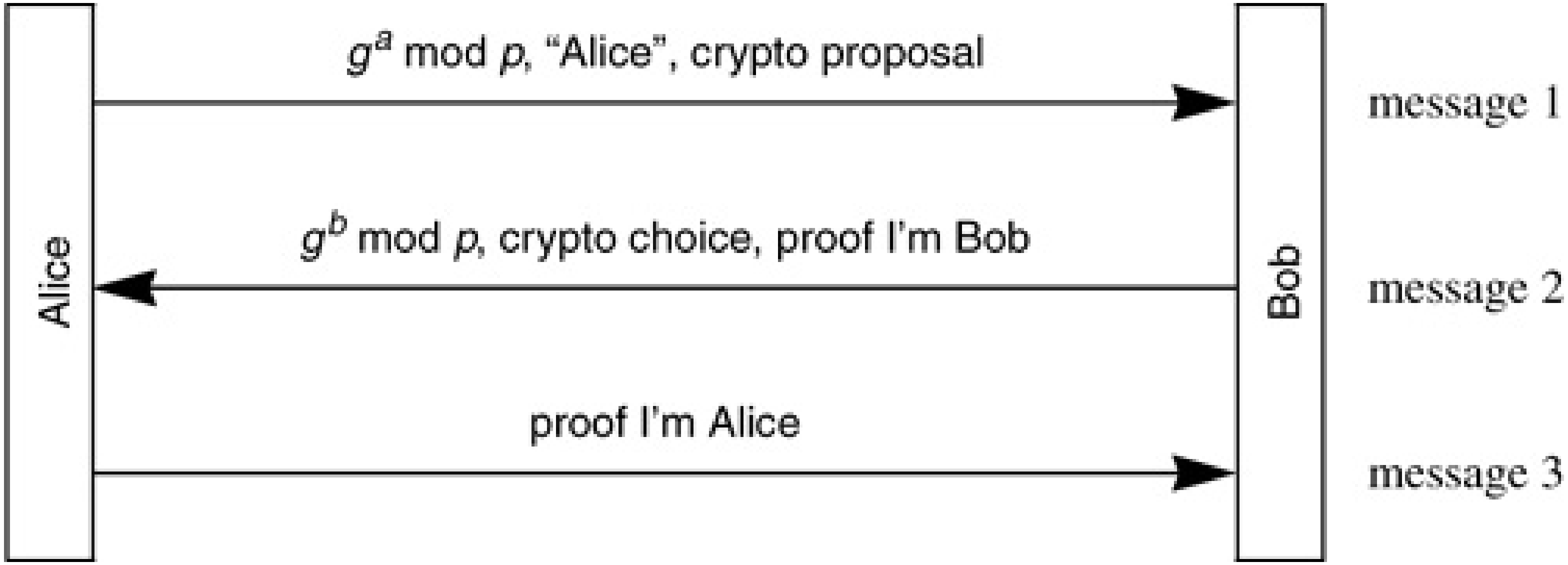
IKE SA
DES
MD5
preshare
DH1
lifetime

IKE Phase 1

IKE SA
DES
MD5
preshare
DH1
lifetime

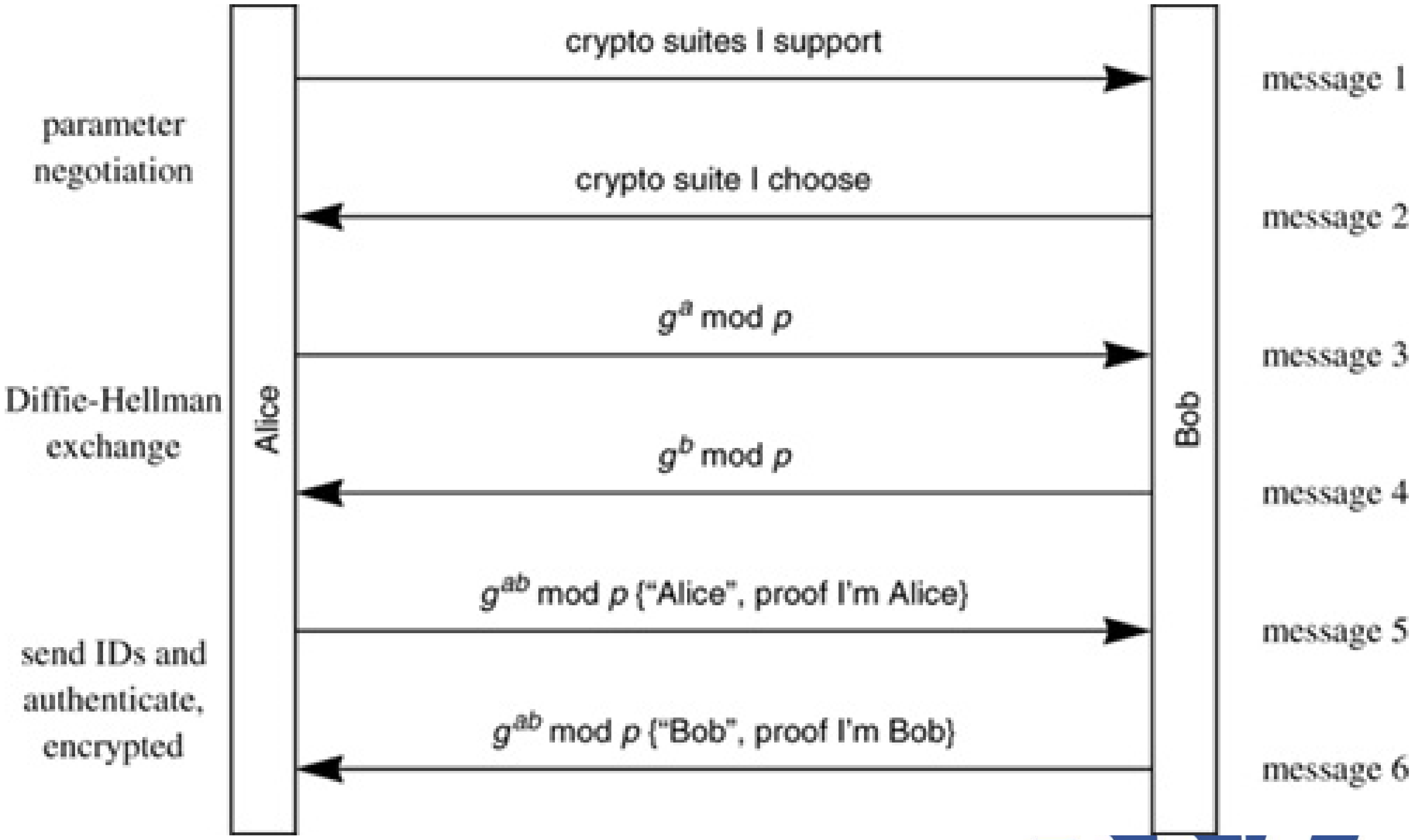
- Authenticates IPSec peers
- Negotiates matching policy to protect IKE exchange
- Exchanges keys via Diffie-Hellman
- Establishes IKE security association

IKE Phase I Aggressive mode


g^a mod p, "Alice", crypto proposal
message 1
Alice
Bob
g^b mod p, crypto choice, proof I'm Bob
message 2
proof I'm Alice
message 3

- In the first exchange, almost everything is squeezed into the proposed IKE SA values, the Diffie-Hellman public key, a nonce that the other party signs, and an identity packet, which can be used to verify the initiator's identity through a third party.

Main mode



Alice

Bob

parameter negotiation

crypto suites I support — message 1

crypto suite I choose — message 2

Diffie-Hellman exchange

g^a mod p — message 3

g^b mod p — message 4

send IDs and authenticate, encrypted

g^{ab} mod p {"Alice", proof I'm Alice} — message 5

g^{ab} mod p {"Bob", proof I'm Bob} — message 6

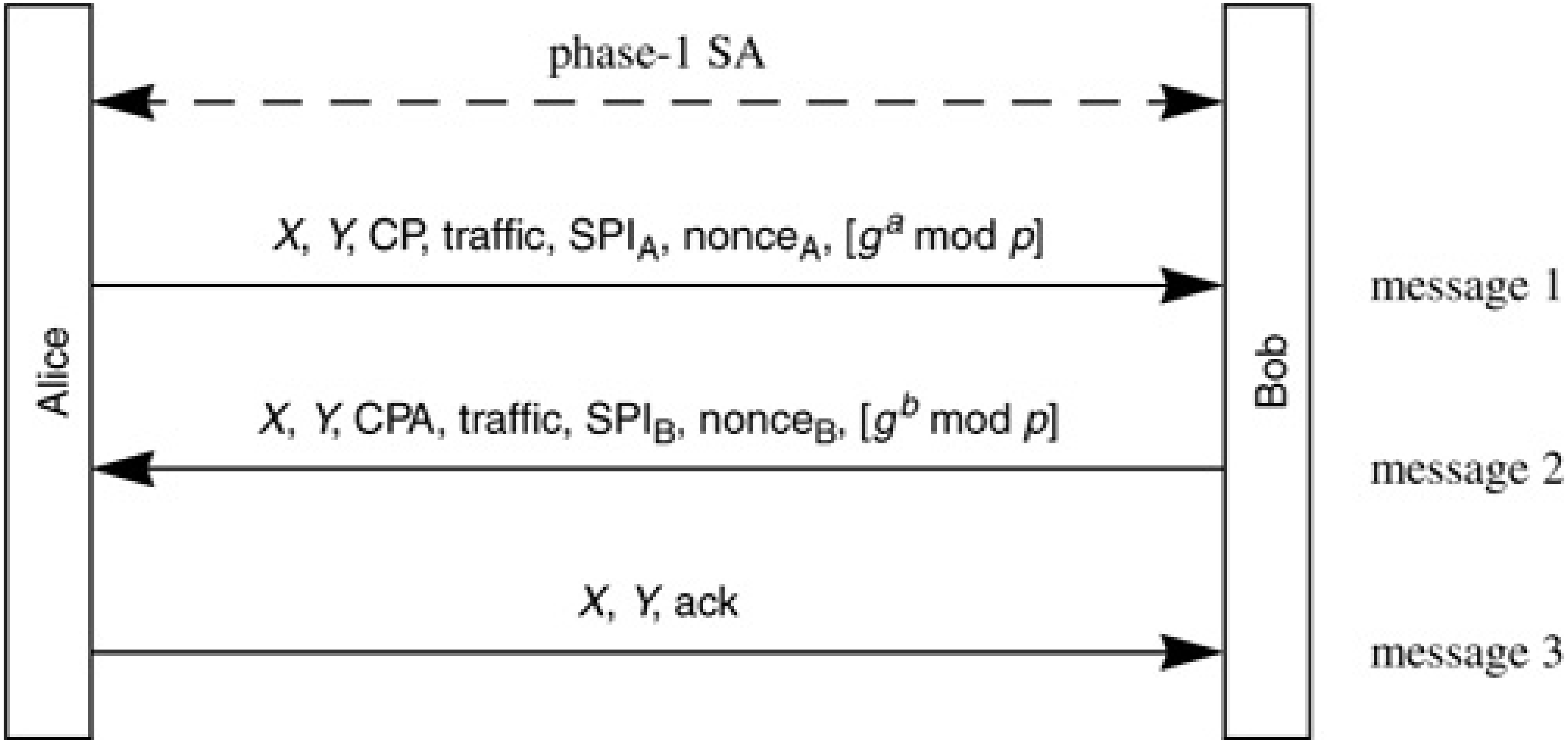
Identity

- IP address of the peer (four octets), such as 172.30.2.2
- Fully qualified domain name (FQDN), such as student@cisco.com

Methods to authenticate

- **Preshared keys**—A key value entered into each peer manually (out of band) used to authenticate the peer
- **RSA signatures**—Use a digital certificate authenticated by an RSA signature
- **RSA encrypted nonces**—Use RSA encryption to encrypt a nonce value (a random number generated by the peer) and other values

IKE Phase 2


phase-1 SA
Alice
Bob
X, Y, CP, traffic, SPI_A, nonce_A, [$g^a \bmod p$]
message 1
X, Y, CPA, traffic, SPI_B, nonce_B, [$g^b \bmod p$]
message 2
X, Y, ack
message 3