IPSec

Outline

- Internet Protocol
  - IPv6
- IPSec
  - Security Association (SA)
  - IPSec Base Protocol (AH, ESP)
  - Encapsulation Mode (transport, tunnel)

IPv6 Header

- Initial motivation:
  - 32-bit address space soon to be completely allocated.
  - Expands addresses to 128 bits
    - 430,000,000,000,000,000,000 for every square inch of earth's surface!
    - Solves IPv4 problem of insufficient address space
- Additional motivation:
  - header format helps speedy processing/forwarding
  - header changes to facilitate QoS

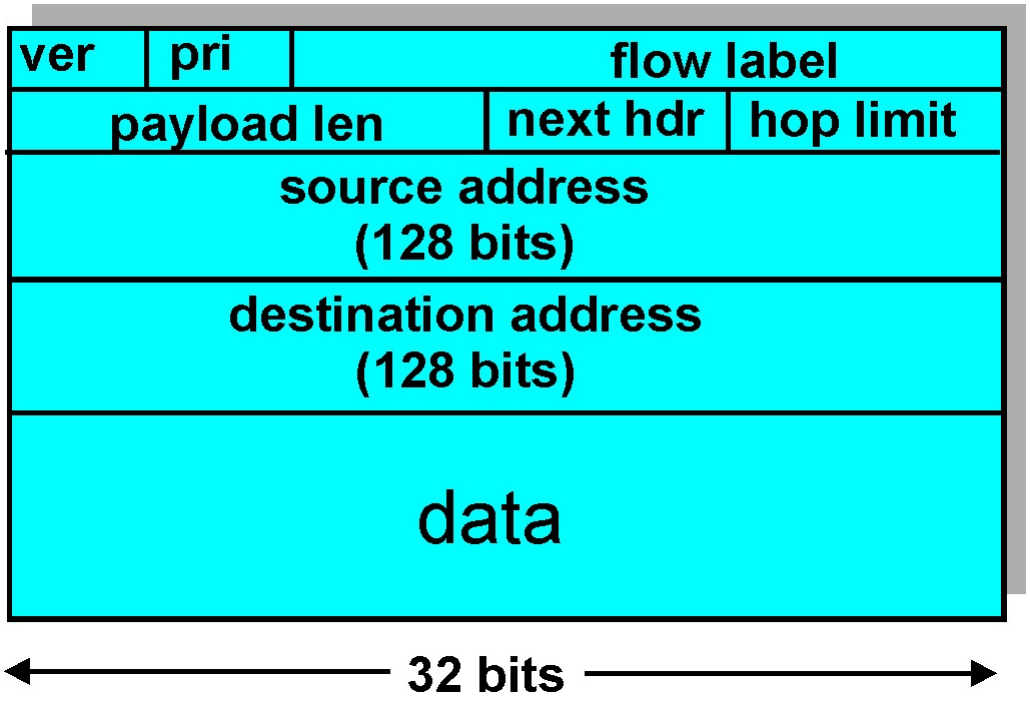
  IPv6 datagram format:
  - fixed-length 40 byte header
  - no fragmentation allowed

IPv6 Header (Cont)

Priority: identify priority among datagrams in flow

Flow Label: identify datagrams in same "flow."
(concept of"flow" not well defined).

Next header: identify upper layer protocol for data



Other Changes from IPv4

- *Checksum*: removed entirely to reduce processing time at each hop
- *Options:* allowed, but outside of header, indicated by "Next Header" field
- *ICMPv6:* new version of ICMP
  - additional message types, e.g. "Packet Too Big"
  - multicast group management functions

IPv6 Security – IPsec mandated

- IPsec is mandated in IPv6
  - This means that all implementations (i.e. hosts, routers, etc) must have IPsec capability to be considered as IPv6-conformant
- When (If?) IPv6 is in widespread use, this means that IPsec will be installed everywhere
  - At the moment, IPsec is more common in network devices (routers, etc) than user hosts, but this would change with IPsec
- All hosts having IPsec => real end-to-end security possible

IPv6 Security

- Enough IP addrs for every imaginable device

  + Real end-to-end security

  = Ability to securely communicate from anything to anything

IPv6 Security – harder to scan networks

- With IPv4, it is easy to scan a network
  - With tools like *nmap*, can scan a typical subnet in a few minutes
  - Returning list of active hosts and open ports
  - Many worms also operate by scanning
    - e.g. Blaster, Slammer
  - Attackers (& worms) scan for proxies, weak services and back doors

see: http://www.insecure.org/nmap/

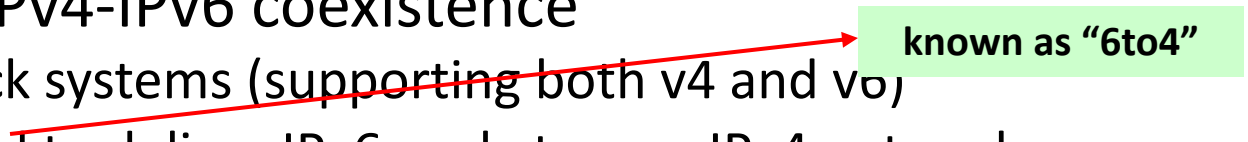
IPv6 Security – harder to scan networks

- With IPv6, sparse address allocation makes such brute force scanning impractical
  - It is 4 billion times harder to scan 1 IPv6 subnet than all of IPv4
- No more Blaster, Slammer, …
- Use of “dense” address allocations makes it easier though

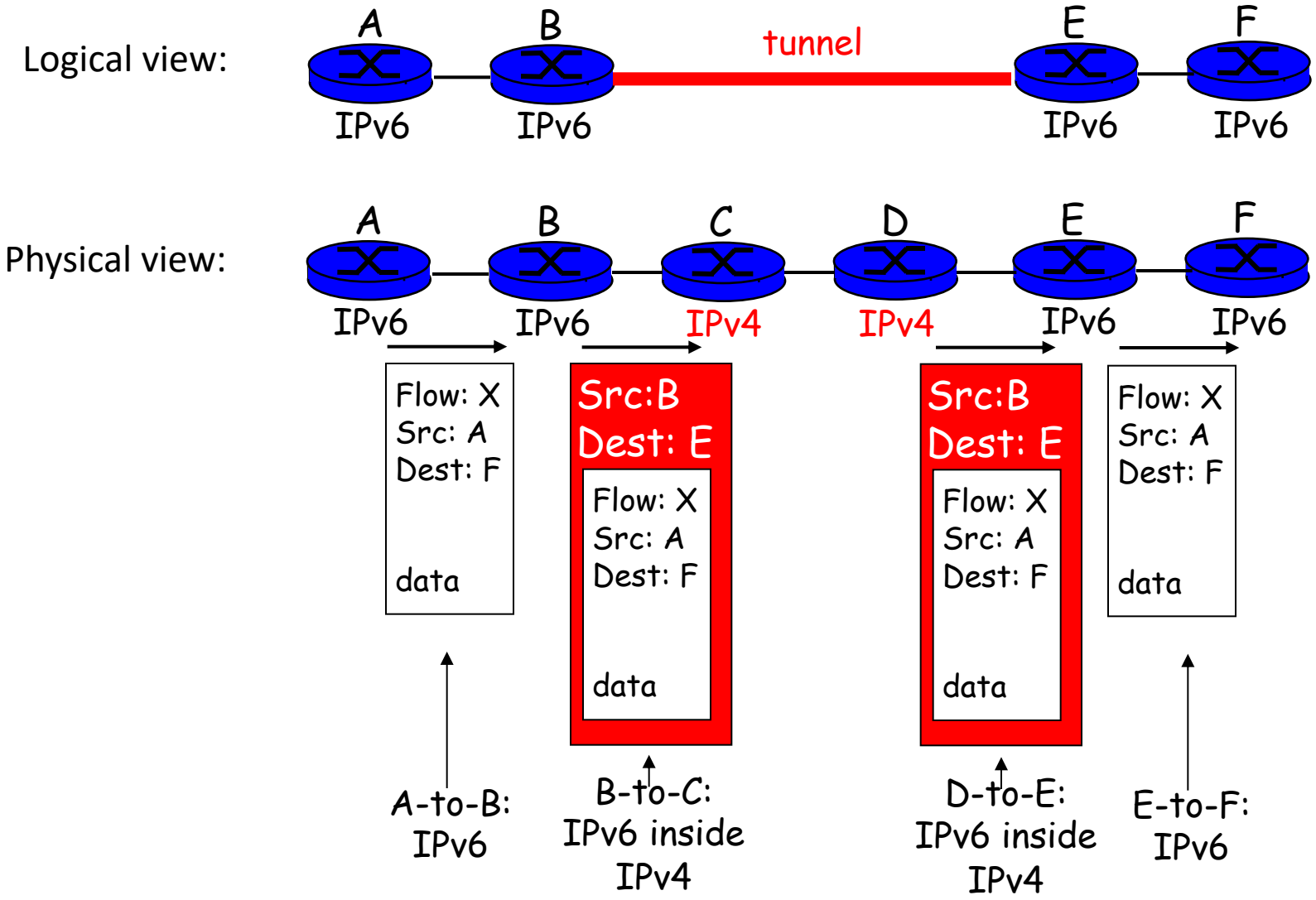
Transition From IPv4 To IPv6

Transition from IPv4 to IPv6 will take time:

- Due to need to support legacy systems and applications, not all system can be upgraded simultaneously
- Instead, organisations deploy IPv6 piecewise with pilot/experimental implementations first
- Thus need for IPv4-IPv6 coexistence
  - Have dual-stack systems (supporting both v4 and v6)
  - Tunnelling used to deliver IPv6 packets over IPv4 networks
- *Tunneling:* IPv6 carried as payload in IPv4 datagram among IPv4 routers



Tunneling


Logical view:
A
B
tunnel
E
F
IPv6
IPv6
IPv6
IPv6
Physical view:
A
B
C
D
E
F
IPv6
IPv6
IPv4
IPv4
IPv6
IPv6
Flow: X
Src: A
Dest: F
data
Src:B
Dest: E
Flow: X
Src: A
Dest: F
data
Src:B
Dest: E
Flow: X
Src: A
Dest: F
data
Flow: X
Src: A
Dest: F
data
A-to-B:
IPv6
B-to-C:
IPv6 inside
IPv4
D-to-E:
IPv6 inside
IPv4
E-to-F:
IPv6

Outline

- Internet Protocol
  - IPv6
- IPSec
  - Security Association (SA)
  - IPSec Base Protocol (AH, ESP)
  - Encapsulation Mode (transport, tunnel)

IP Security (IPsec)

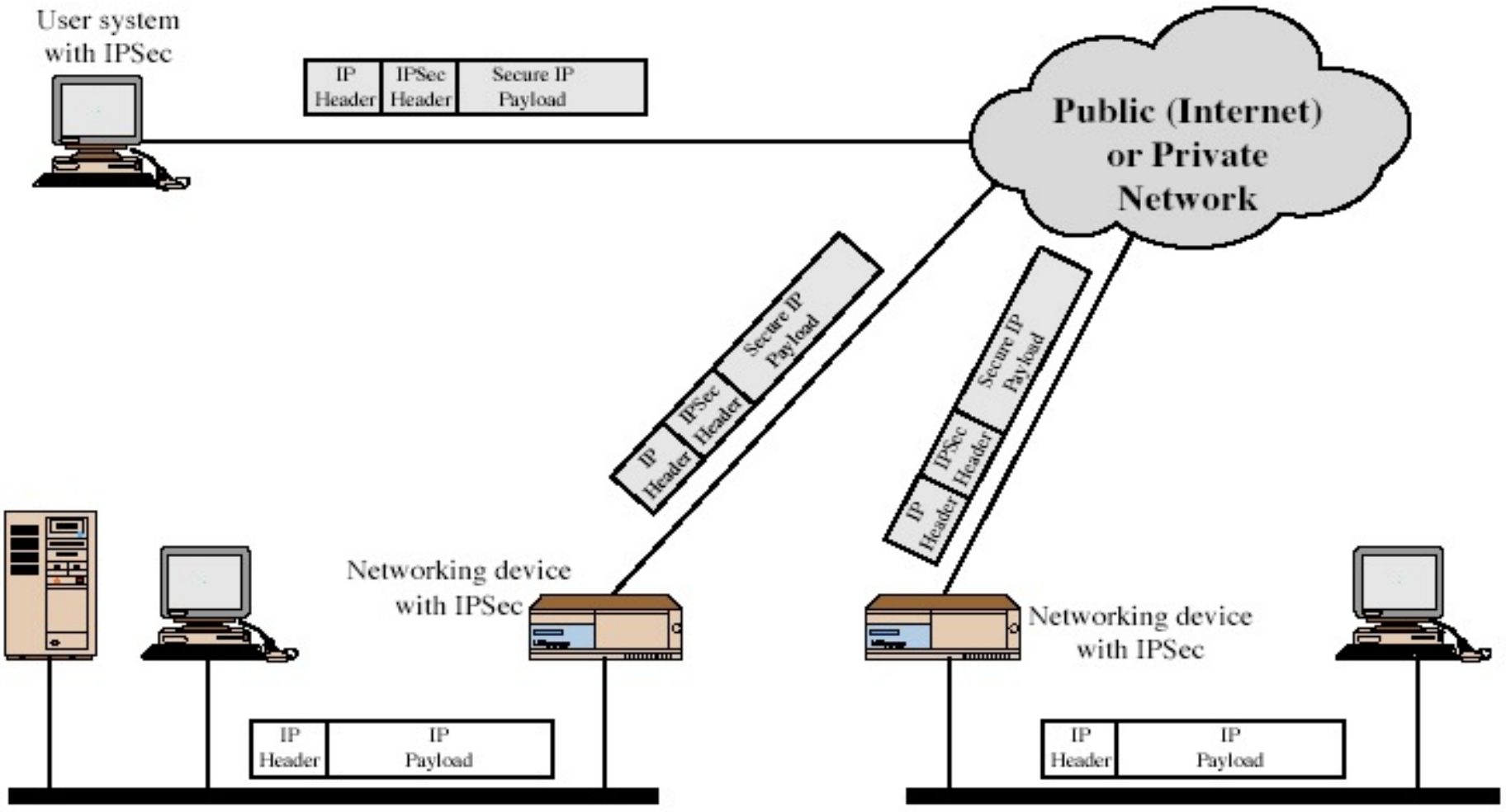
- Suite of protocols from Internet Engineering Task Force (IETF) providing encryption and authentication at the IP layer
  - Arose from needs identified in RFC 1636
  - Specifications in:
    - RFC 2401: Security architecture
    - RFC 2402: Authentication
    - RFC 2406: Encryption
    - RFC 2408: Key management
- Objective is to encrypt and/or authenticate **all** traffic at the IP level.

IP Security Issues

- Eavesdropping
- Modification of packets in transit
- Identity spoofing (forged source IP addresses)
- Denial of service

- Many solutions are application-specific
  - TLS for Web, S/MIME for email, SSH for remote login
- IPSec aims to provide a framework of open standards for secure communications over IP
  - Protect every protocol running on top of IPv4 and IPv6

Typical Usage



IPSec Services

- Data origin authentication
- Confidentiality
- Connectionless and partial sequence integrity
  - Connectionless = integrity for a single IP packet
  - Partial sequence integrity = prevent packet replay
- Limited traffic flow confidentiality
  - Eavesdropper cannot determine who is talking
- These services are transparent to applications above transport (TCP/UDP) layer

Major IPSec Components

- Security Association (SA) Database
  - Each SA refers to all the security parameters of one communication direction
  - For two-way communications, at least two SAs are needed.
- Two Protocols
  - AH – Authentication Header
  - ESP – Encapsulating Security Payload
    1. Encryption only
    2. Encryption with authentication
- Two Encapsulation modes
    1. Transport mode
    2. Tunnel mode

Outline

- Internet Protocol
  - IPv6
- IPSec
  - Security Association (SA)
  - IPSec Base Protocol (AH, ESP)
  - Encapsulation Mode (transport, tunnel)

Security Association (SA)

- In order to communicate, each pair of hosts must set up SA with each other
- Acts as virtual connection for which various parameters are set:
  - Type of protection
  - Algorithms
  - Keys
  - …
- Simplex: a one way relationship between a sender and a receiver.
- For either AH or ESP, but not both

Security Association (SA)

- Each SA *uniquely* identified by:
  - Security Parameters Index (SPI)
    - 32-bit string assigned to this SA (local meaning only)
  - IP destination address of packets
    - May be end user system, or firewall or router
  - Security Protocol Identifier (e.g. AH, ESP)

- For each IP packet, governing SA is identified by:
  - Destination IP address in packet header
  - SPI in extension header (AH or ESP)

Security Association (SA)

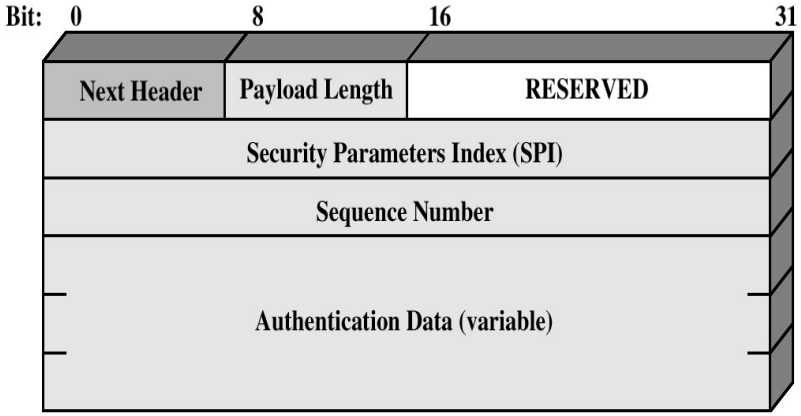
- It contains all the security parameters needed for one way communication
  - Sequence number counter
  - Anti-replay window
  - Protocol (e.g. AH / ESP)
  - Transform mode (e.g. transport / tunnel mode)
  - Protocol parameters (e.g. AES, 128-bit, CBC mode, SHA-1)
  - Lifetime of the SA
  - etc.

Outline

- Internet Protocol
  - IPv6
- IPSec
  - Security Association (SA)
  - IPSec Base Protocol (AH, ESP)
  - Encapsulation Mode (transport, tunnel)

Two IPSec Base Protocols

- **Authentication Header (AH)**
  - Provides message authentication and integrity check of IP data payload, but not confidentiality.
  - Also Provides authentication for as much of the IP header as possible.
  - Next header: TCP, UDP, etc.
  - Sequence Number: Starts at 1, never recycle (optional)



IPSec Authentication Header

Two IPSec Base Protocols

- **Encapsulating Security Payload (ESP)**
  - Provides confidentiality and/or authentication.
  - When not used, the NULL algorithm defined in RFC-2410 is used.
  - The authentication trailer must be omitted if not used.
  - Either encryption or authentication (or both) must be enabled (NULL-NULL is an invalid option)

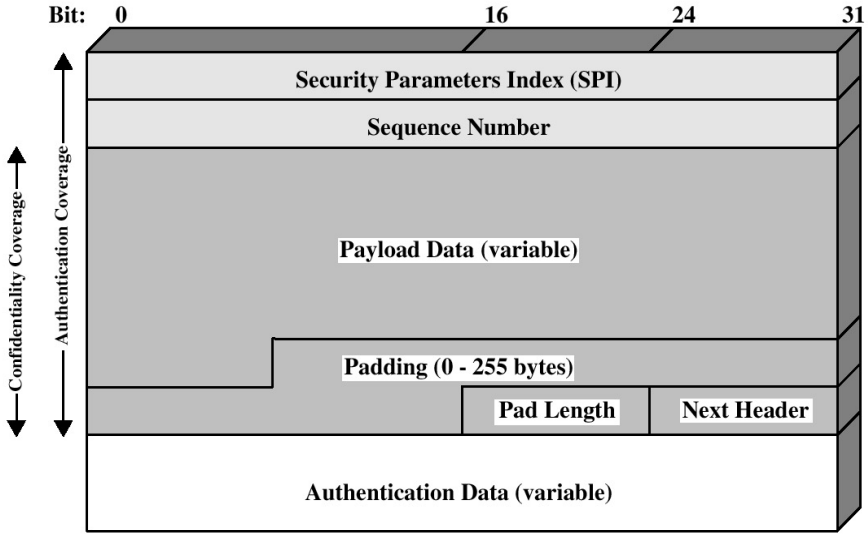


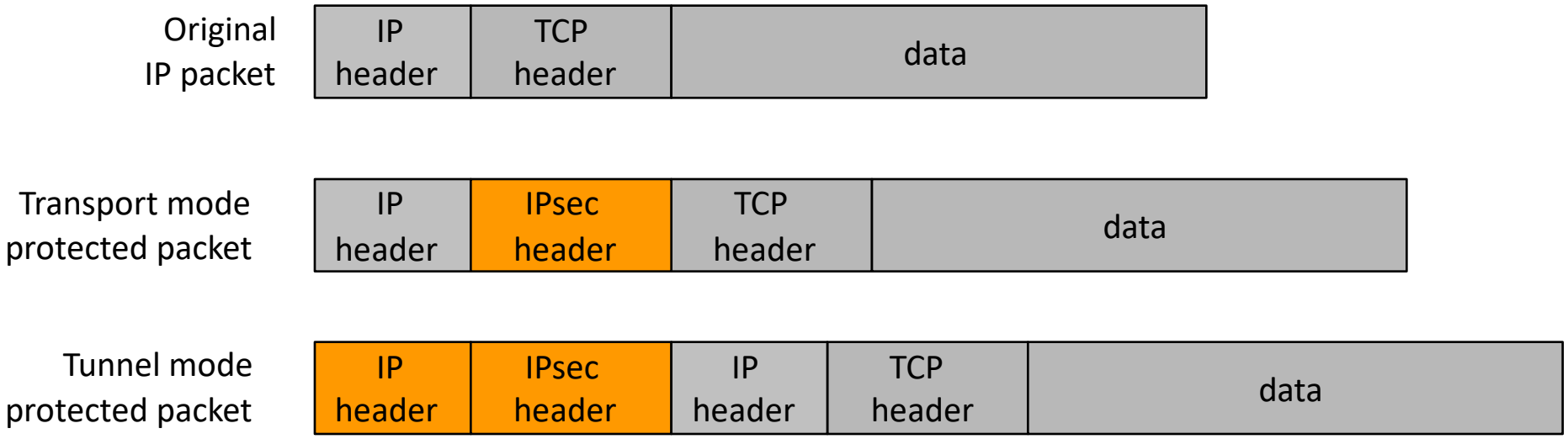
Figure 6.7 IPSec ESP Format

Outline

- Internet Protocol
  - IPv6
- IPSec
  - Security Association (SA)
  - IPSec Base Protocol (AH, ESP)
  - Encapsulation Mode (transport, tunnel)

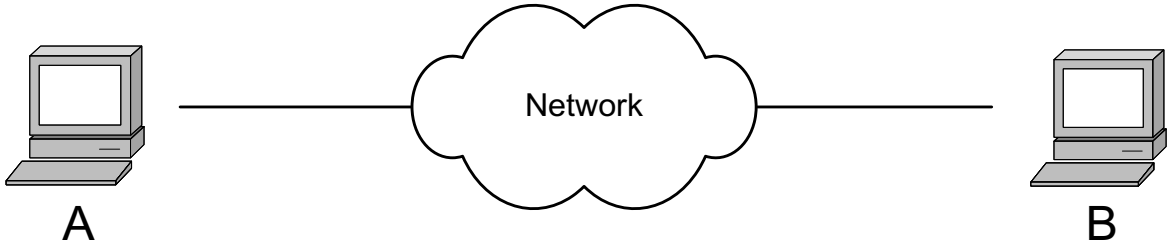
Two Encapsulation Modes

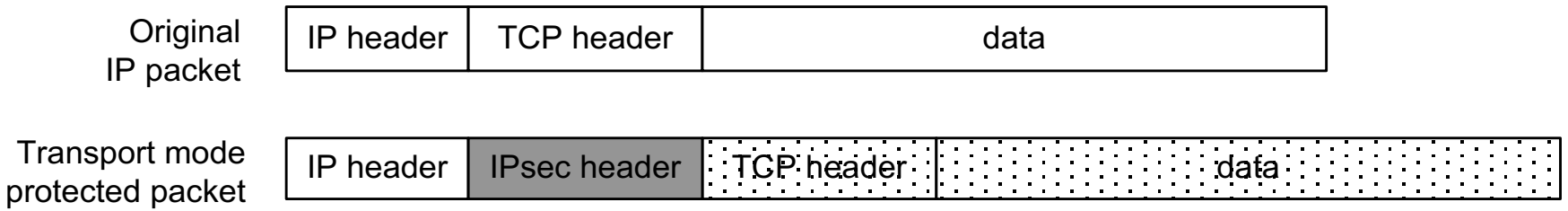
- IPsec defines two encapsulation modes for an IP packet
  - Transport
  - Tunnel



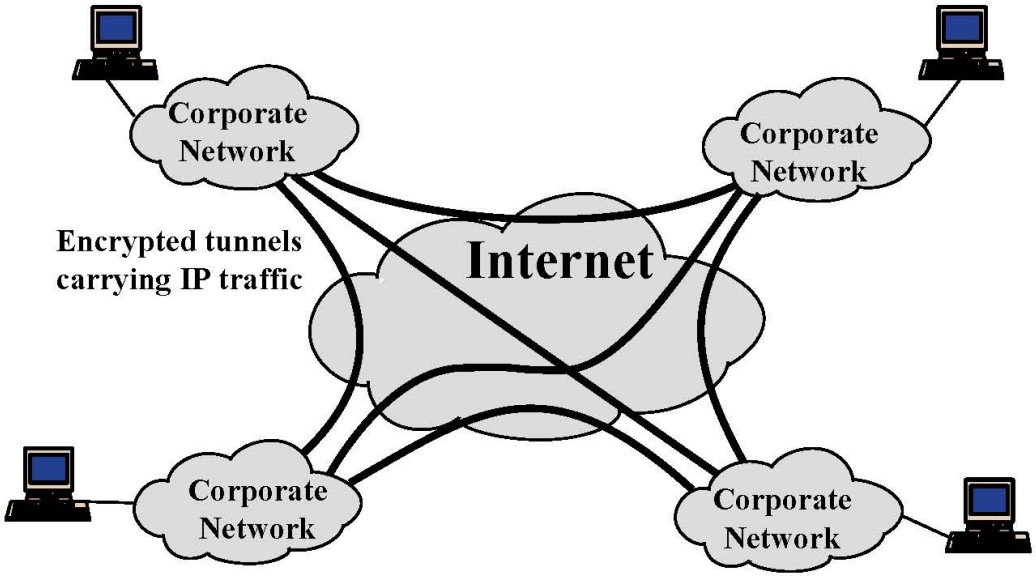
Transport mode

- Intercept Network layer packets
  Encrypt / Authenticate these packets preserving **most** of the original IP header
- End-to-end security between two hosts
  - Typically, client to gateway (e.g., PC to remote host)
- Requires IPSec support at each host



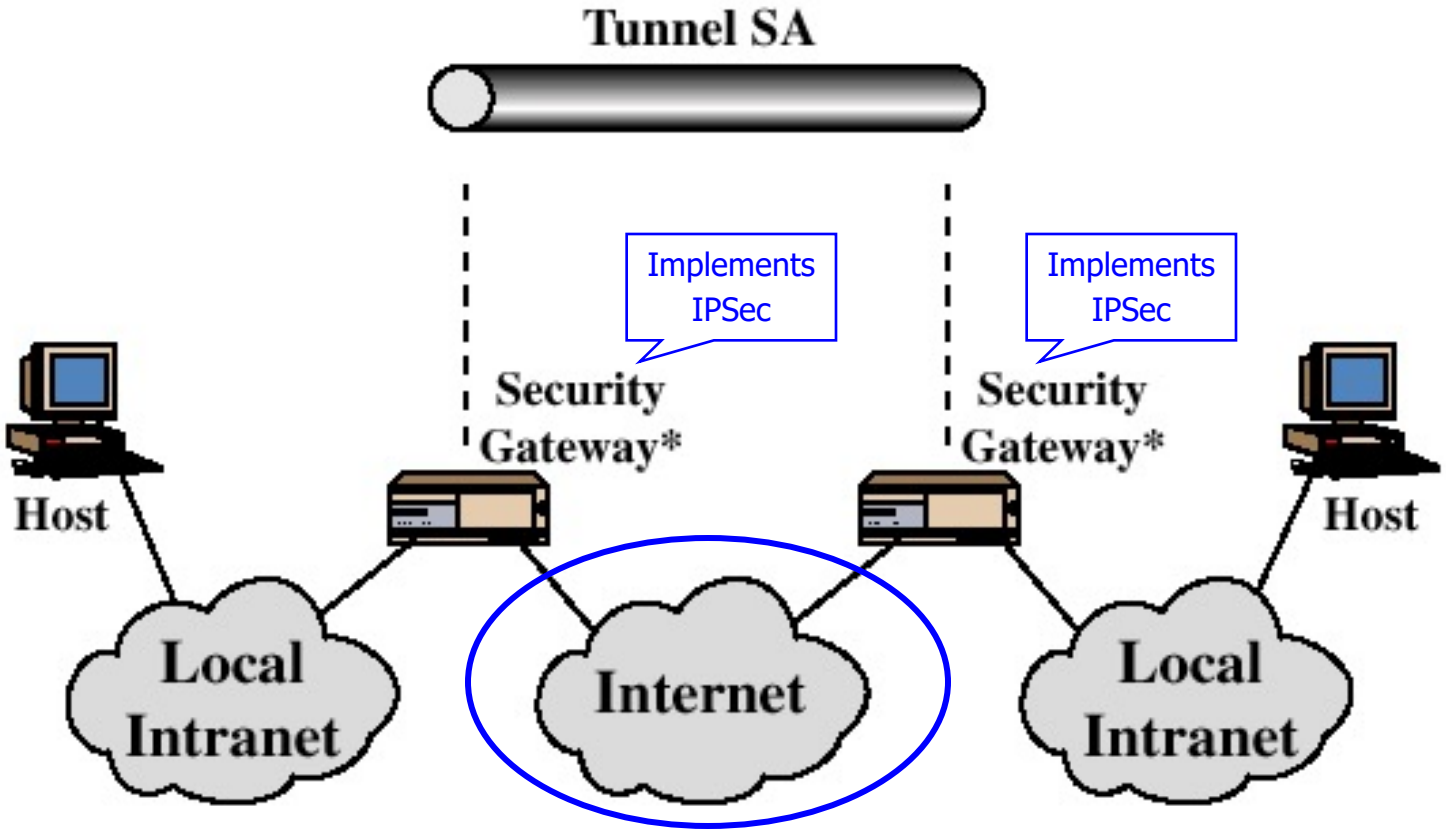


Tunnel Mode



- Gateway-to-gateway security
  - Internal traffic behind gateways not protected
  - Typical application: virtual private network (VPN)
- Only requires IPSec support at gateways

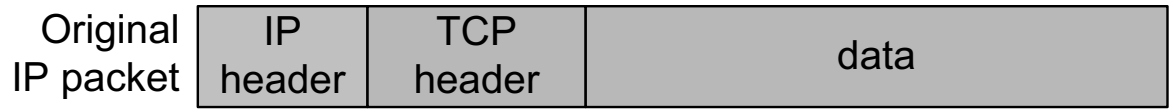
Tunnel Mode Illustration

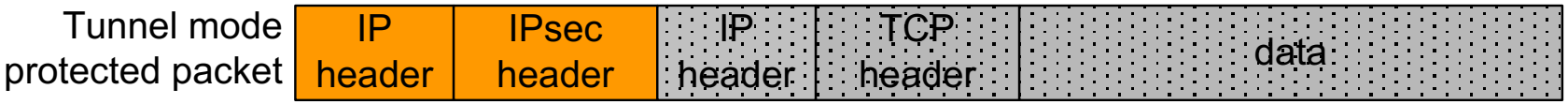


IPSec protects communication on the insecure part of the network

Tunnel mode

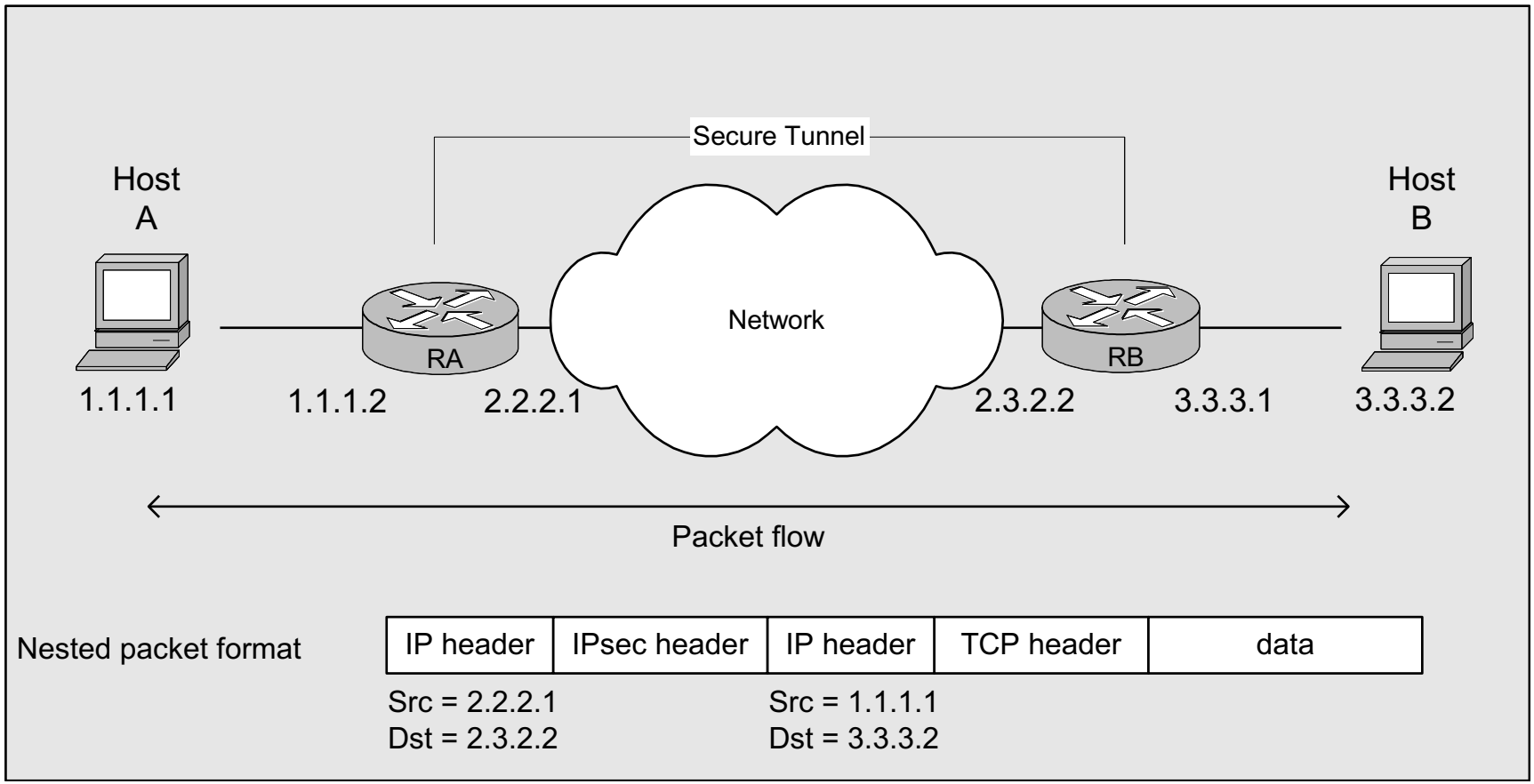
- Intercept Network layer packets
  Encrypt / Authenticate these packets, while encapsulating the original IP packet entirely





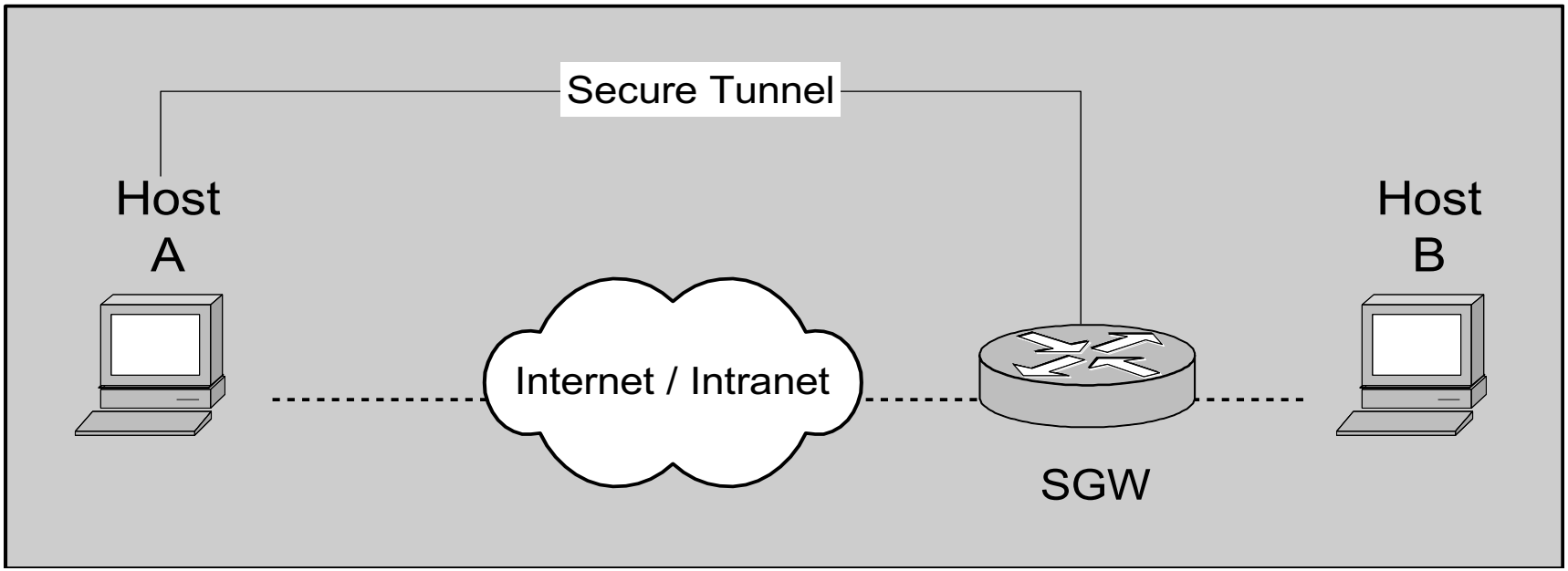
- Versatile and has many deployment modes
  - Host-to-host
  - Host-to-router (i.e. remote access)
  - Router-to-router (a.k.a. Gateway-to-gateway)

Tunnel mode
(Router-to-router / Gateway-to-gateway)



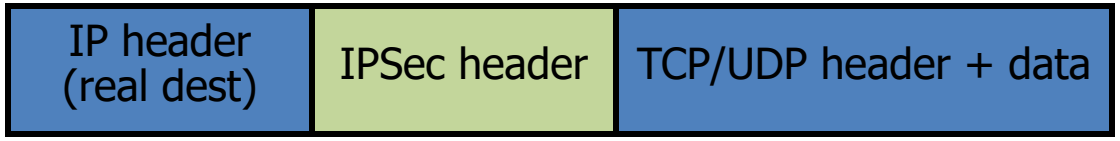
Tunnel mode

(Host-to-Router / Remote Access)

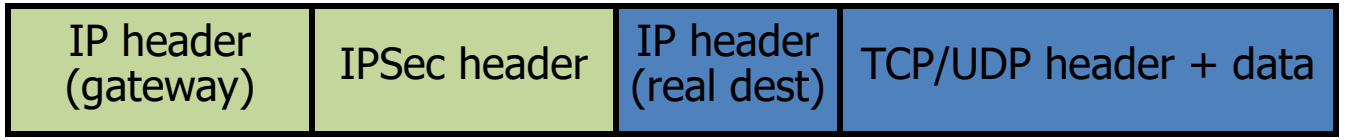


Transport Mode vs. Tunnel Mode

- Transport mode secures packet payload and leaves IP header unchanged



- Tunnel mode encapsulates both IP header and payload into IPSec packets



Encapsulation Modes

	Transport Mode	Tunnel Mode
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers	Authenticates entire inner IP packet plus selected portions of outer IP header
ESP	Encrypts IP payload and any IPv6 extension header	Encrypts inner IP packet
ESP with authentication	Encrypts IP payload and any IPv6 extesion header. Authenticates IP payload but no IP header	Encrypts inner IP packet. Authenticates inner IP packet but no outer IP header

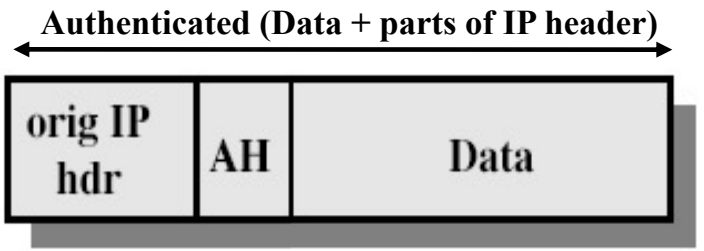
Authentication Header (AH)

- Adds extra field to traditional IP packet
- This is used to verify authenticity & integrity of the packet

Before applying AH:

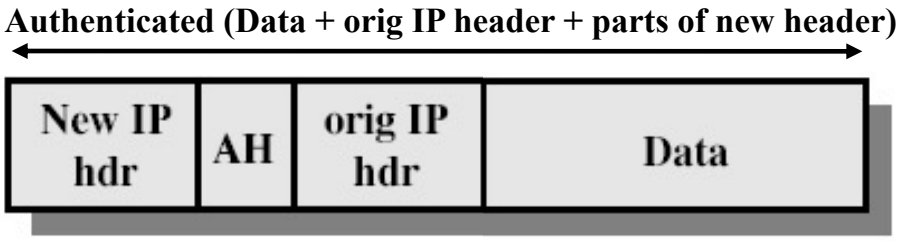
Transport Mode:

- data is authenticated, as well as parts of IP header



Tunnel Mode:

- entire original packet is authenticated + parts of new header



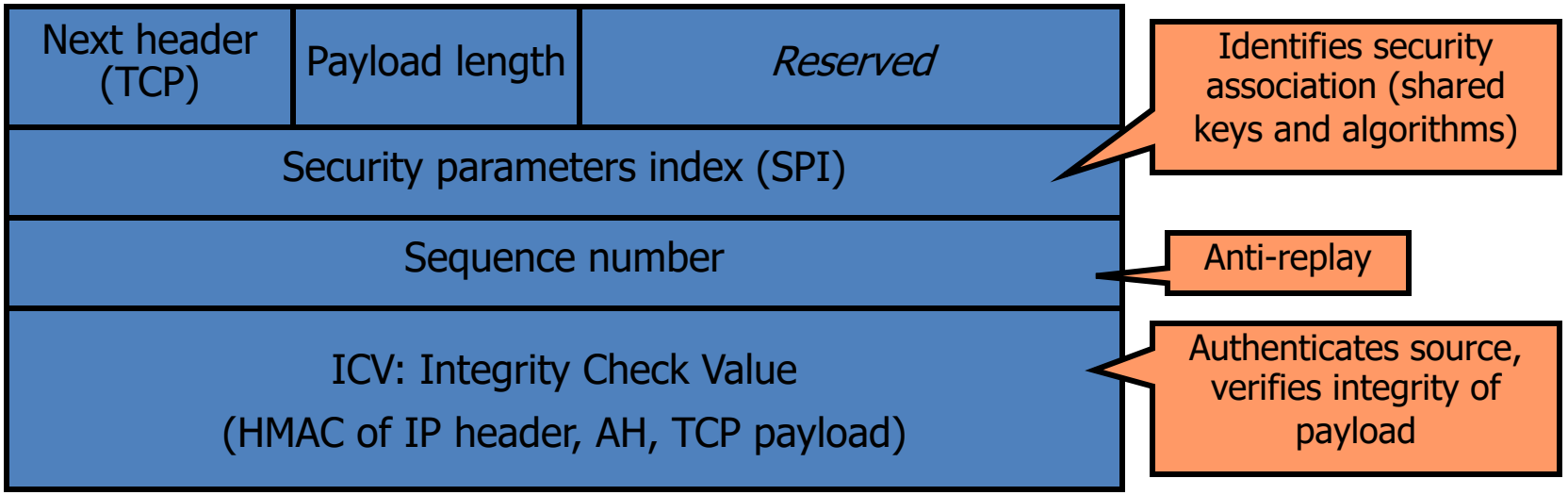
Authentication Header (AH)

- Protection against replay attack with use of sequence number

- Why have an Authentication-only protocol (AH)?
  - May be used where export/import/use of encryption is restricted
  - Faster implementation
  - Receiver can choose whether expend the effort to verify authenticity/integrity

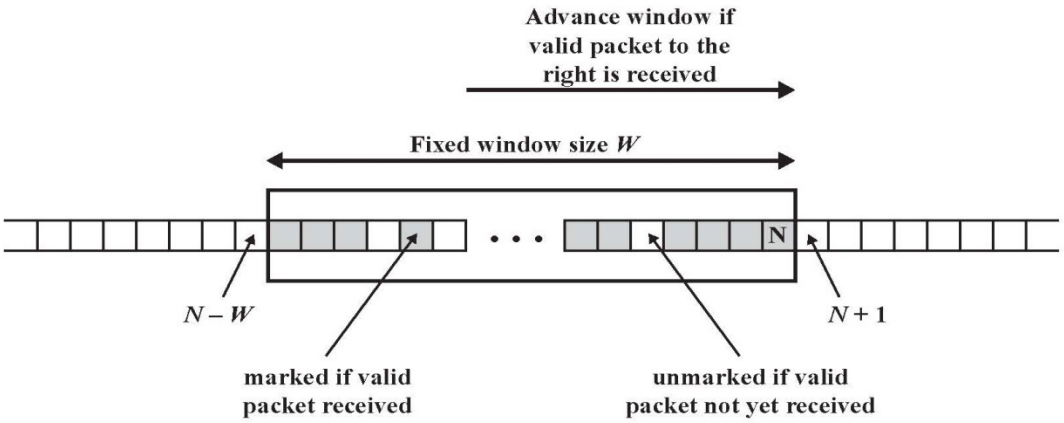
AH: Authentication Header

- Provides integrity and origin authentication
- Authenticates portions of the IP header
- Anti-replay service (to counter denial of service)
- No confidentiality



Prevention of Replay Attacks

- When SA is established, sender initializes 32-bit counter to 0, increments by 1 for each packet
  - If wraps around 2^{32}-1, new SA must be established
- Recipient maintains a sliding 64-bit window
  - If a packet with high sequence number is received, do not advance window until packet is authenticated

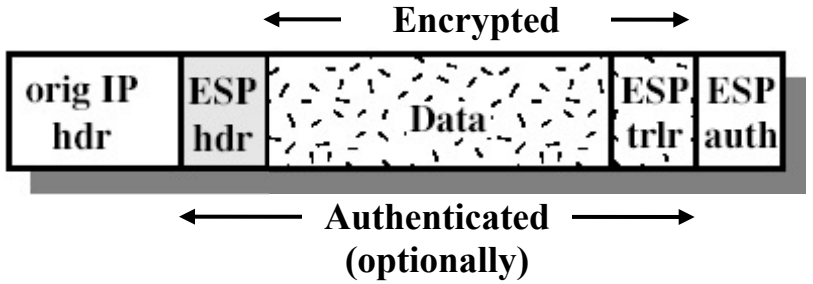


Encapsulating Security Payload (ESP)

Original IP packet:

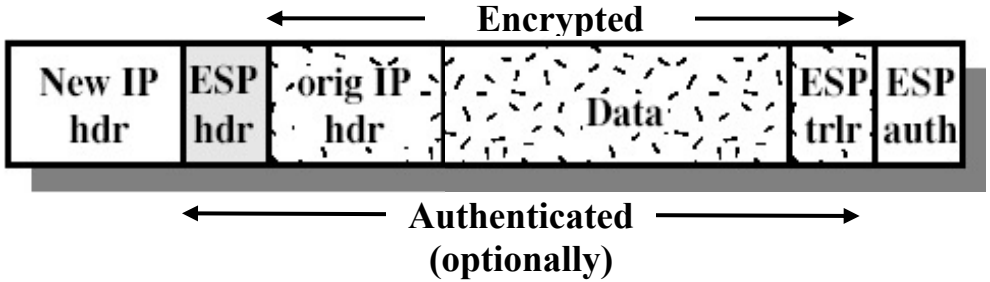
Transport Mode:

- only data is encrypted & authenticated

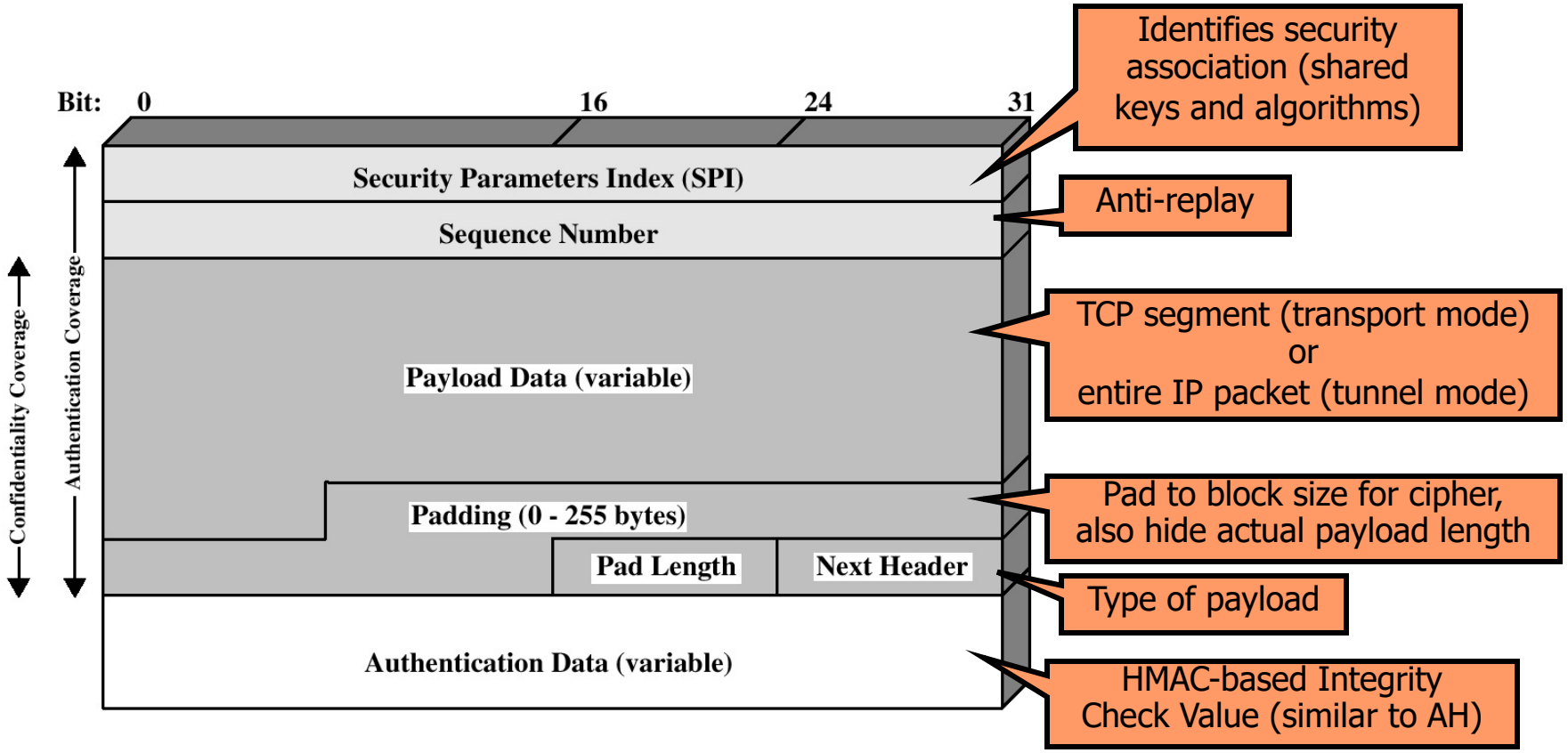


Tunnel Mode:

- entire packet encrypted & authenticated



ESP Packet


Bit: 0
16
24
31
Security Parameters Index (SPI)
Sequence Number
Payload Data (variable)
Padding (0 - 255 bytes)
Pad Length
Next Header
Authentication Data (variable)
Confidentiality Coverage
Authentication Coverage
Identifies security association (shared keys and algorithms)
Anti-replay
TCP segment (transport mode) or entire IP packet (tunnel mode)
Pad to block size for cipher, also hide actual payload length
Type of payload
HMAC-based Integrity Check Value (similar to AH)

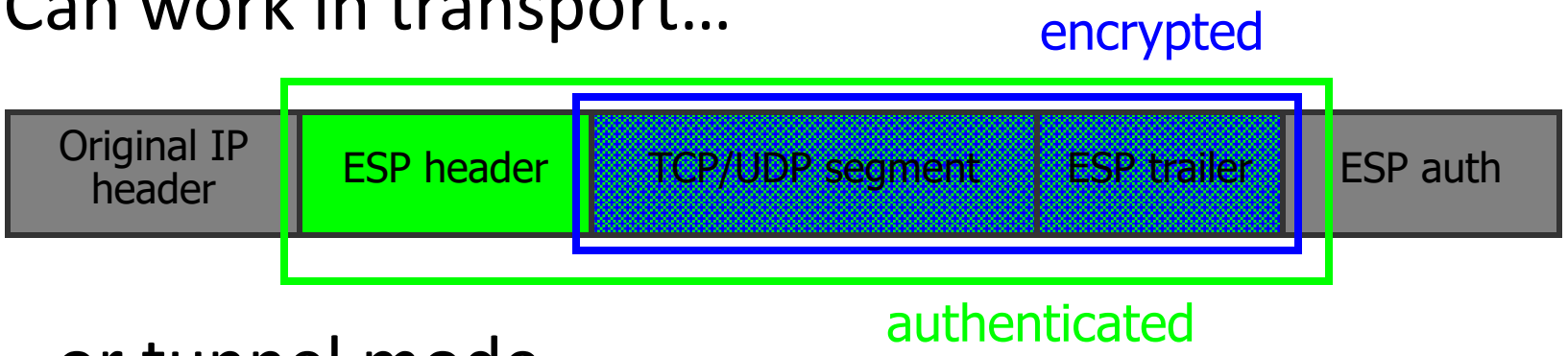
Encapsulating Security Payload (ESP)

- Content of IP packet is encrypted and encapsulated between header and trailer fields.

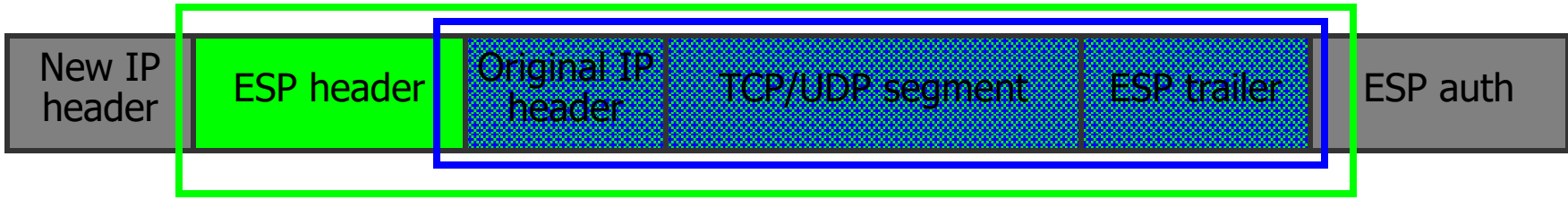
- Authentication data optionally added

Authentication + Confidentiality (ESP)

- Confidentiality and integrity for packet payload
  - Symmetric cipher negotiated as part of security assoc
- Provides authentication (similar to AH)
- Can work in transport…



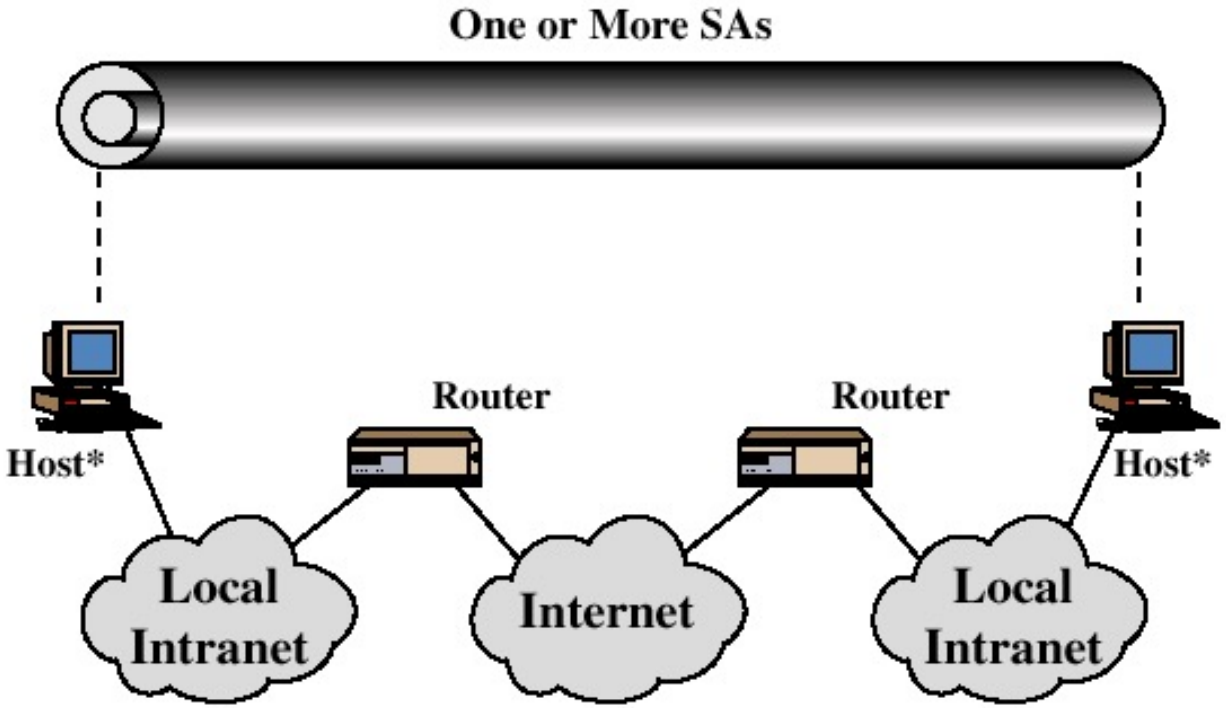
- …or tunnel mode



Combining Security Associations

- SAs can implement either AH or ESP
- to implement both need to combine SAs
  - form a security bundle
- have 4 cases (see next)

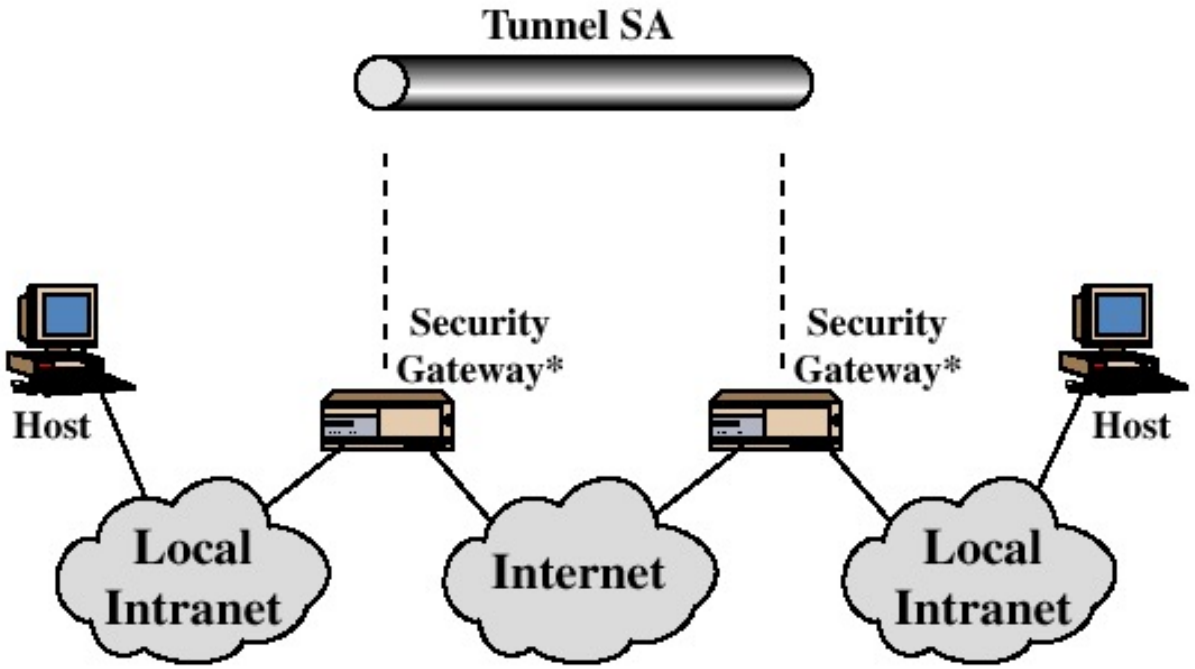
Selection of Protocol Modes
(Host-to-Host)



(a) Case 1

- Transport Mode
- Tunnel Mode

Selection of Protocol Modes
(Router-to-Router)

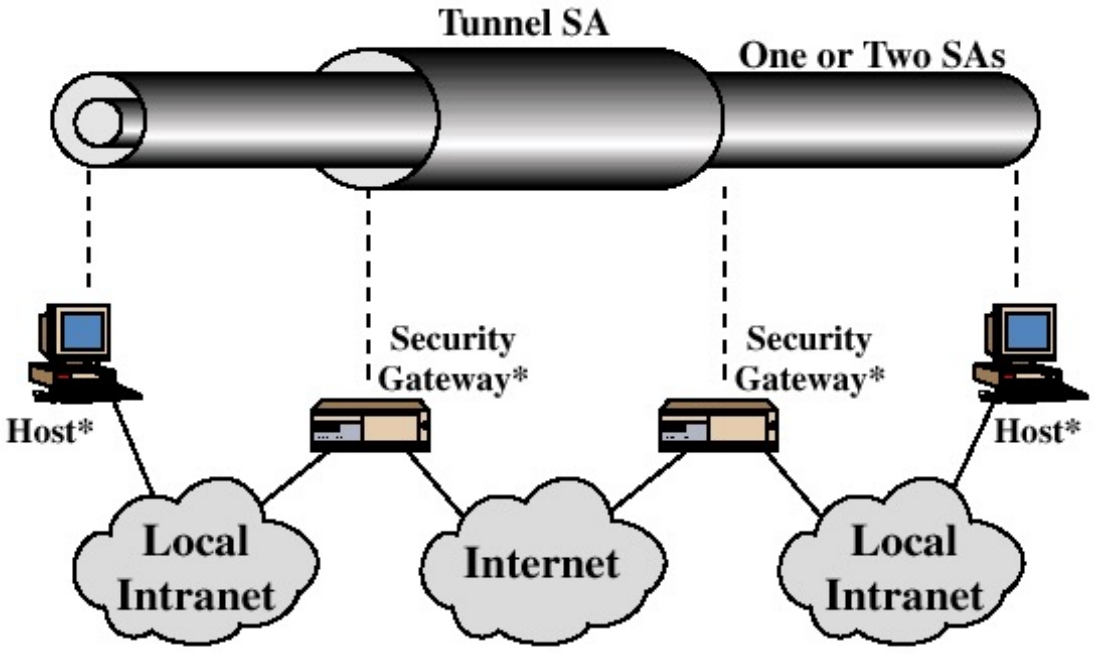


(b) Case 2

- Tunnel Mode

Selection of Protocol Modes

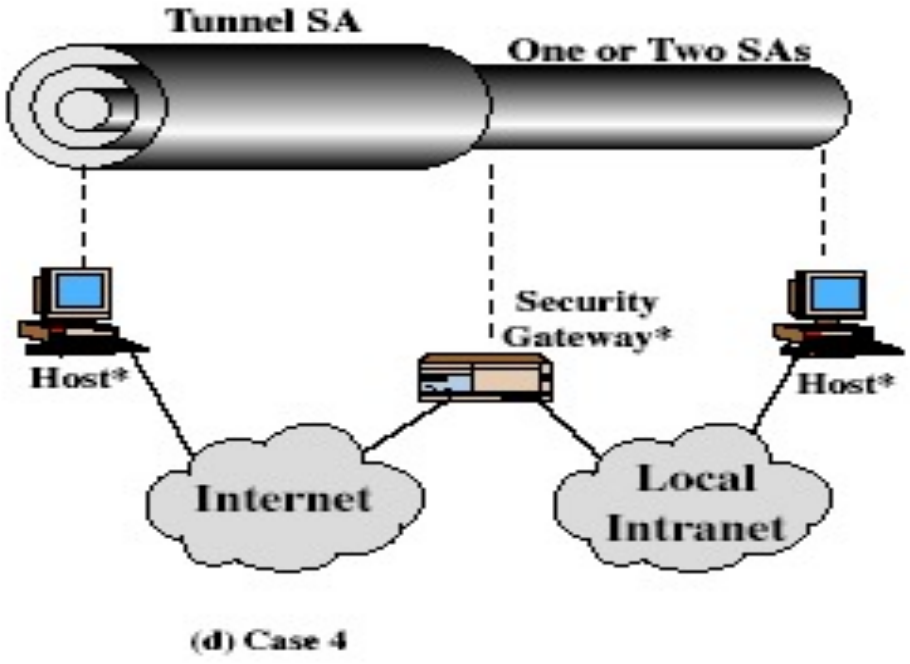
(Pass-through IPSec)



(c) Case 3

- Tunnel mode for gateway-to-gateway
- Transport mode / tunnel mode for host-to-host

Selection of Protocol Modes
(Remote access)



- Tunnel mode for host-to-gateway
- Transport mode / tunnel mode for gateway-to-host

IPsec Benefits

- Provides a level of security for all applications.
  - Allows deployment of new/emerging applications that may not have their own security.
- Transparent to transport layer
- Transparent to end-users
  - No need for training, key issue, key revocation, etc.
- Can be provided to individual users where needed (e.g. off-site workers)
- Extensible to new, stronger, cryptographic methods as these become available

IPsec Drawbacks

- Processing performance overhead
  - Protection is applied to all traffic, though only a small portion may be security-sensitive
- Blocks access to non-IPsec hosts
- Hosts must have security association
  - Not great for short-lived connections
- Not practical for broadcast

Uses of IPsec

- **Virtual Private Network (VPN) establishment**
  - For connecting remote offices and users using public Internet
- **Low-cost remote access**
  - e.g. teleworker gains secure access to company network via local call to ISP
- **Extranet connectivity**
  - Secure communication with partners, suppliers, etc.

Standards

- RFC2401 IPSec
- RFC2402 AH
- RFC2403 HMAC MD5
- RFC2404 HMAC SHA-1
- RFC2405 DES CBC with IV
- RFC2406 IP ESP
- RFC2407 DOI for ISAKMP
- RFC2408 ISAKMP
- RFC2409 IKE

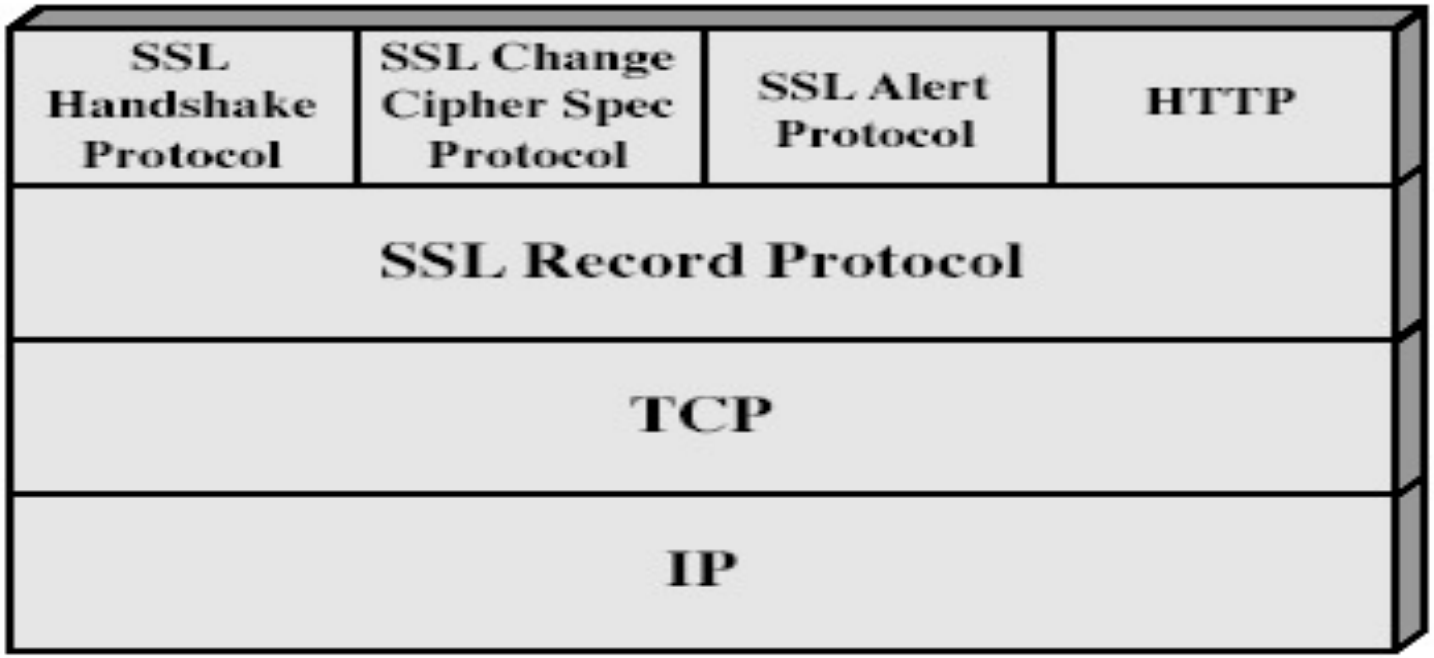
Web Security

- Web now widely used by business, government, individuals
- but Internet & Web are vulnerable
- have a variety of threats
  - integrity
  - confidentiality
  - denial of service
  - authentication
- need added security mechanisms

SSL (Secure Socket Layer)

- transport layer security service
- originally developed by Netscape
- version 3 designed with public input
- subsequently became Internet standard known as TLS (Transport Layer Security)
- uses TCP to provide a reliable end-to-end service
- SSL has two layers of protocols

SSL Architecture



SSL Architecture

- **SSL session**
  - an association between client & server
  - created by the Handshake Protocol
  - define a set of cryptographic parameters
  - may be shared by multiple SSL connections
- **SSL connection**
  - a transient, peer-to-peer, communications link
  - associated with 1 SSL session

SSL Record Protocol

- **confidentiality**
  - using symmetric encryption with a shared secret key defined by Handshake Protocol
  - IDEA, RC2-40, DES-40, DES, 3DES, RC4-40, RC4-128
  - message is compressed before encryption
- **message integrity**
  - using a MAC with shared secret key
  - similar to HMAC but with different padding

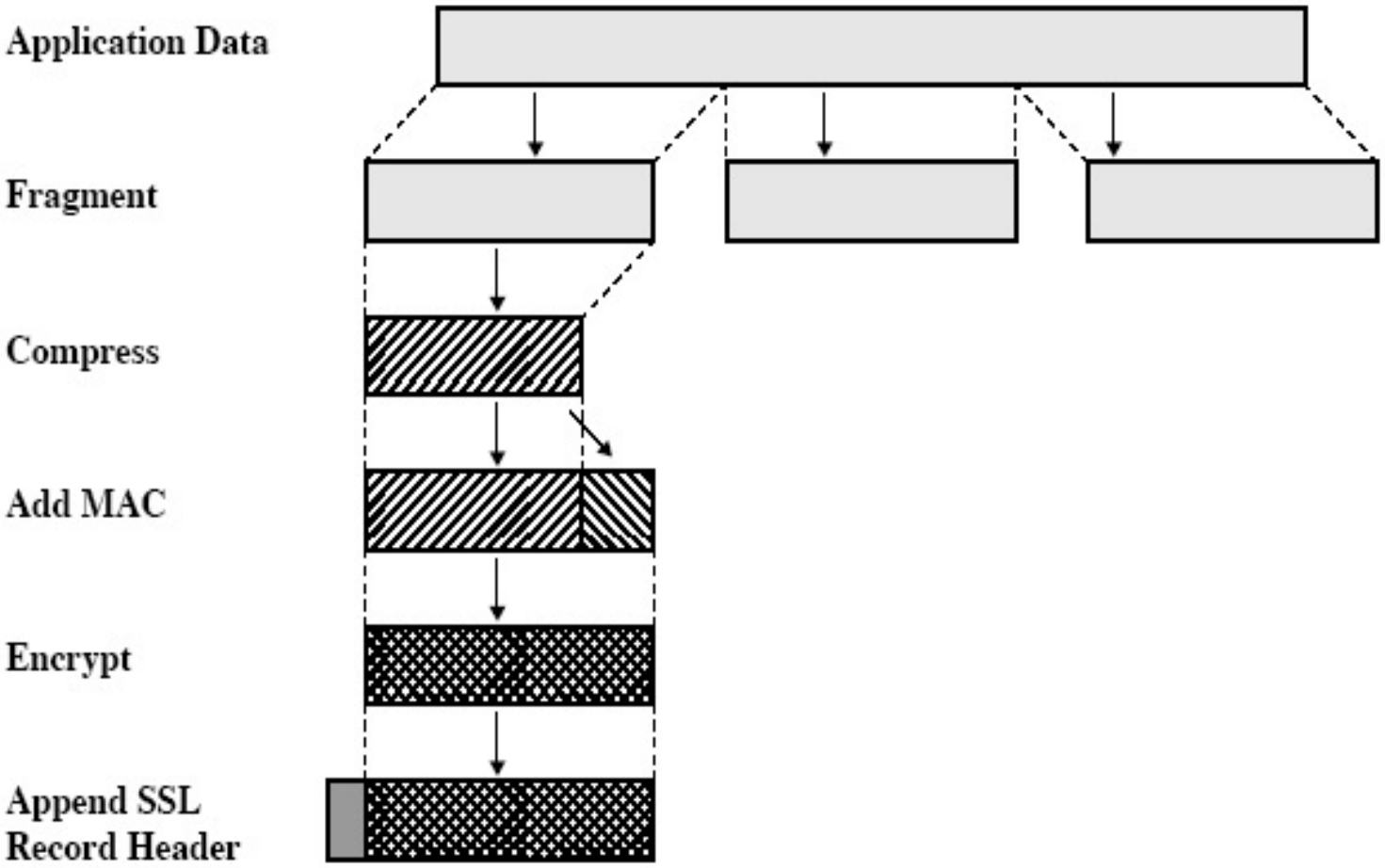


Figure 17.3 SSL Record Protocol Operation

SSL Change Cipher Spec Protocol

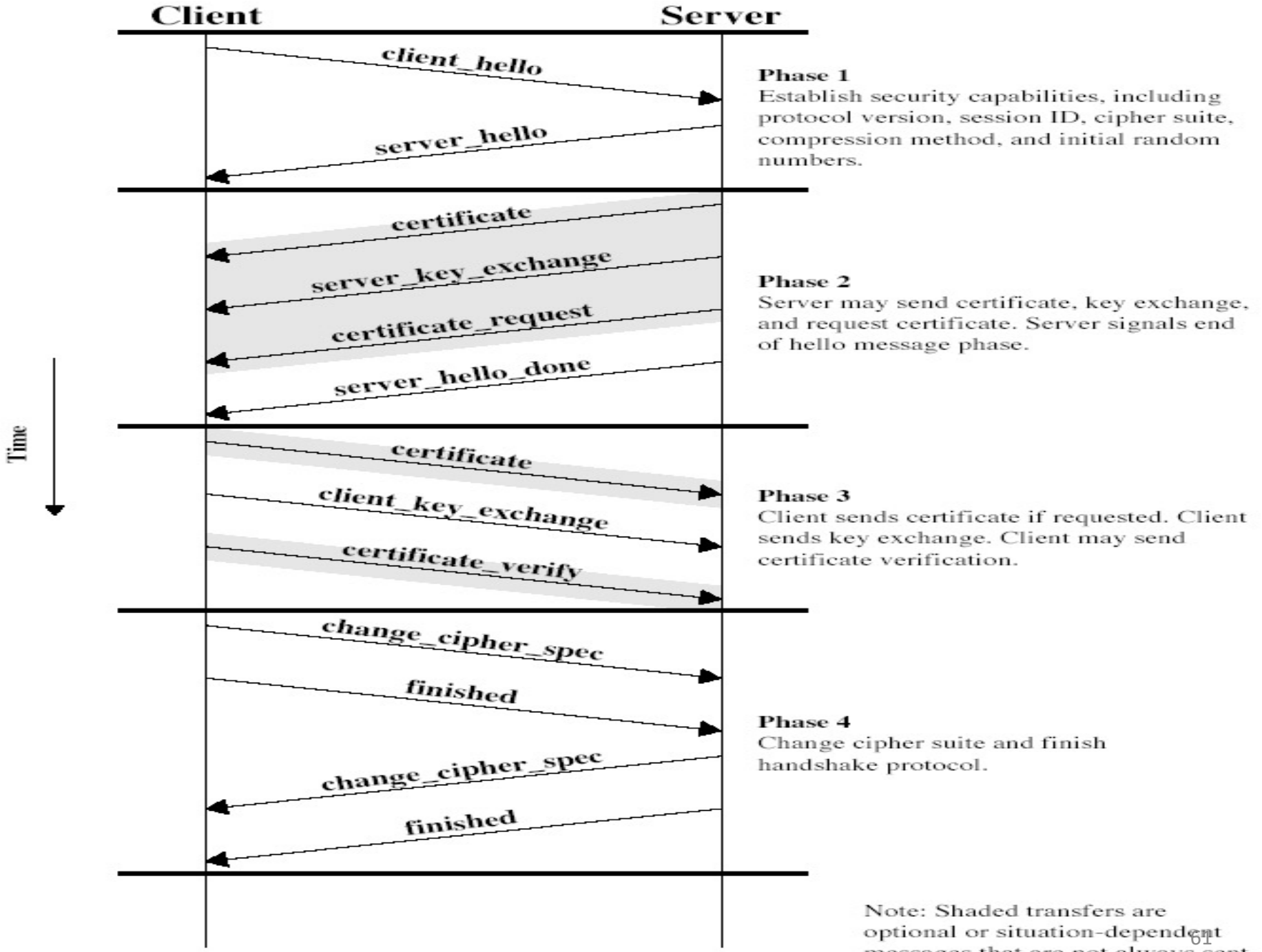
- one of 3 SSL specific protocols which use the SSL Record protocol
- a single message
- causes pending state to become current
- hence updating the cipher suite in use

SSL Alert Protocol

- conveys SSL-related alerts to peer entity
- severity
  - warning or fatal
- specific alert
  - unexpected message, bad record mac, decompression failure, handshake failure, illegal parameter
  - no certificate, bad certificate, unsupported certificate, certificate revoked, certificate expired, certificate unknown
- compressed & encrypted like all SSL data

SSL Handshake Protocol

- allows server & client to:
  - authenticate each other
  - to negotiate encryption & MAC algorithms
  - to negotiate cryptographic keys to be used
- comprises a series of messages in phases
  - Establish Security Capabilities
  - Server Authentication and Key Exchange
  - Client Authentication and Key Exchange
  - Finish


Client
Server
client_hello
server_hello
certificate
server_key_exchange
certificate_request
server_hello_done
certificate
client_key_exchange
certificate_verify
change_cipher_spec
finished
change_cipher_spec
finished
Time
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.
Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.
Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.
Phase 4
Change cipher suite and finish handshake protocol.
Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

TLS (Transport Layer Security)

- IETF standard RFC 2246 similar to SSLv3
- with minor differences
  - in record format version number
  - uses HMAC for MAC
  - a pseudo-random function expands secrets
  - has additional alert codes
  - some changes in supported ciphers
  - changes in certificate negotiations
  - changes in use of padding

IEEE 802.11 security

- *war-driving:* drive around Bay area, see what 802.11 networks available?
  - More than 9000 accessible from public roadways
  - 85% use no encryption/authentication
  - packet-sniffing and various attacks easy!
- securing 802.11
  - encryption, authentication
  - first attempt at 802.11 security: Wired Equivalent Privacy (WEP): a failure
  - current attempt: 802.11i

Wired Equivalent Privacy (WEP):

- authentication
  - host requests authentication from access point
  - access point sends 128 bit nonce
  - host encrypts nonce using shared symmetric key
  - access point decrypts nonce, authenticates host
- no key distribution mechanism
- authentication: knowing the shared key is enough

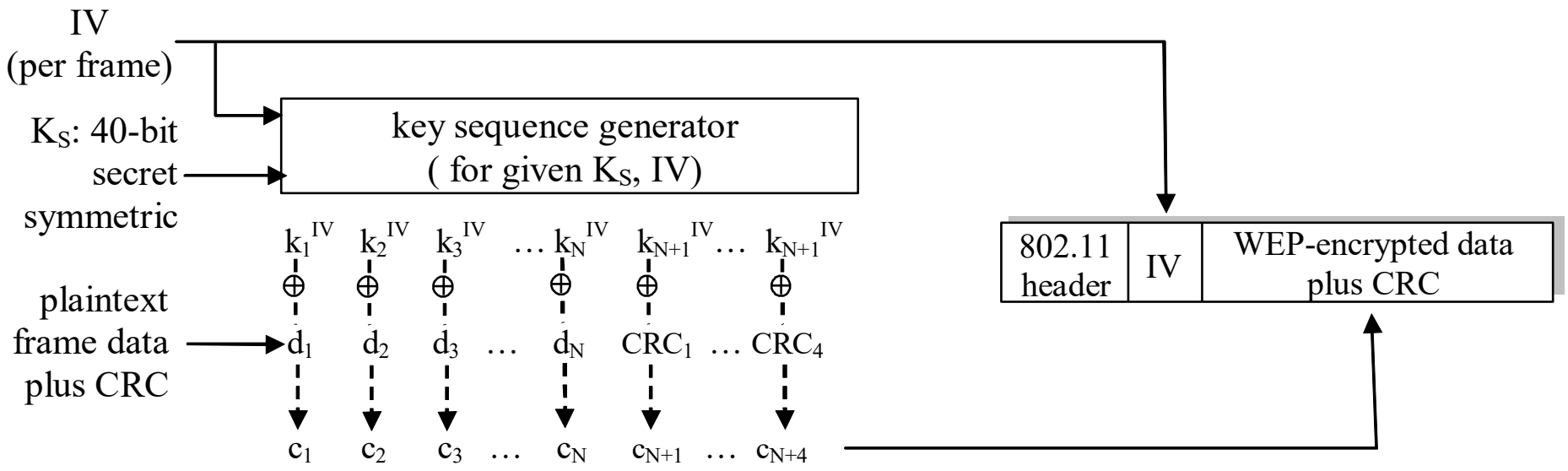
WEP data encryption

- host/AP share 40 bit symmetric key (semi-permanent)
- host appends 24-bit initialization vector (IV) to create 64-bit key
- 64 bit key used to generate stream of keys, k_i^{IV}
- k_i^{IV} used to encrypt ith byte, d_i, in frame:

$$c_i = d_i \text{ XOR } k_i^{IV}$$

- IV and encrypted bytes, c_i sent in frame

802.11 WEP encryption



Sender-side WEP encryption

Breaking 802.11 WEP encryption

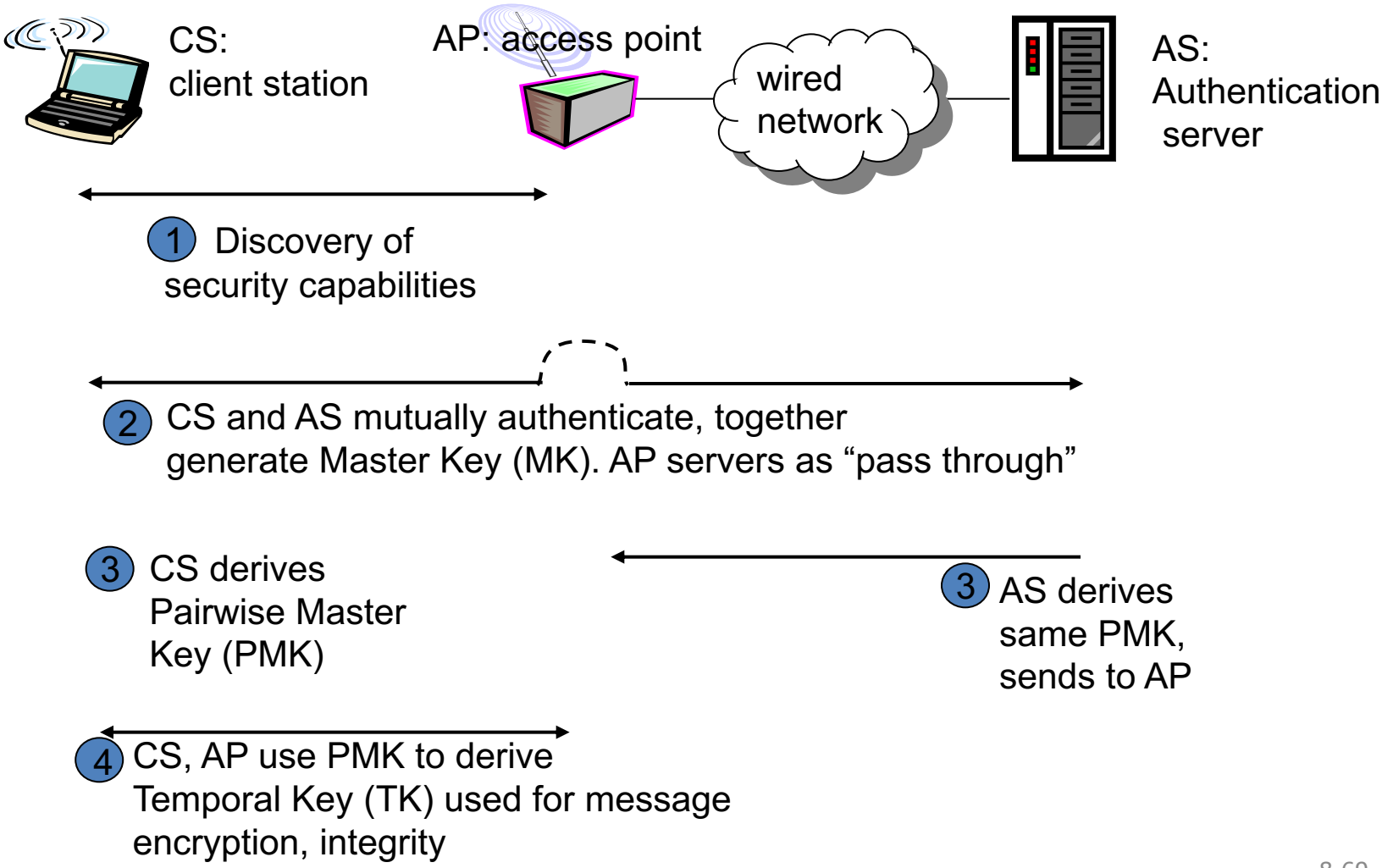
security hole:

- 24-bit IV, one IV per frame, -> IV's eventually reused
- IV transmitted in plaintext -> IV reuse detected
- attack:
  - Trudy causes Alice to encrypt known plaintext d_1 d_2 d_3 d_4 …
  - Trudy sees: $c_i = d_i$ XOR k_i^{IV}
  - Trudy knows c_i d_i, so can compute k_i^{IV}
  - Trudy knows encrypting key sequence k_1^{IV} k_2^{IV} k_3^{IV} …
  - Next time IV is used, Trudy can decrypt!

802.11i: improved security

- numerous (stronger) forms of encryption possible
- provides key distribution
- uses authentication server separate from access point

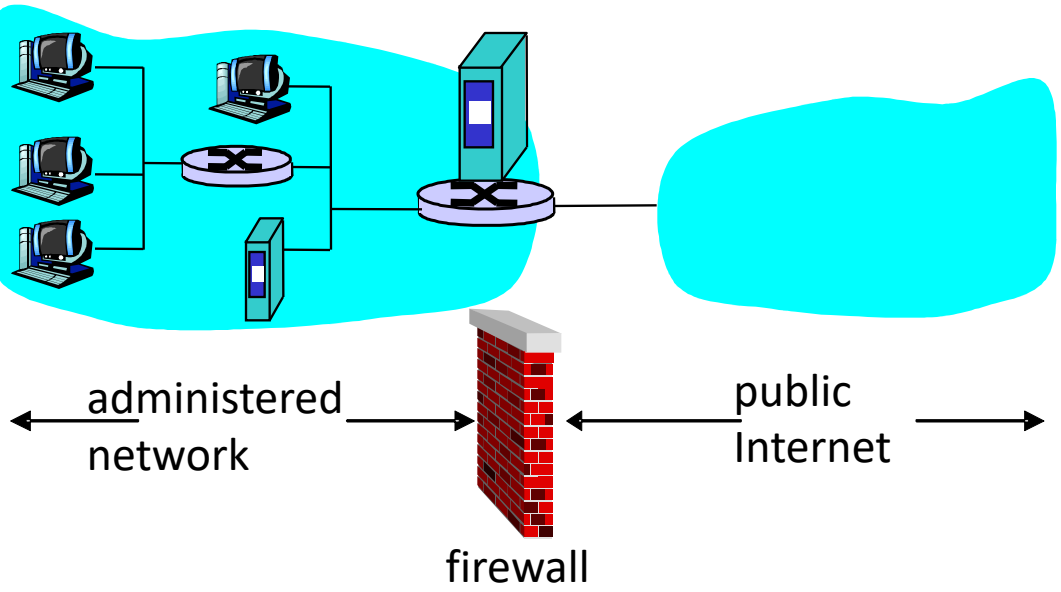
802.11i: four phases of operation



Firewalls

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



Firewalls: Why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections

prevent illegal modification/access of internal data.

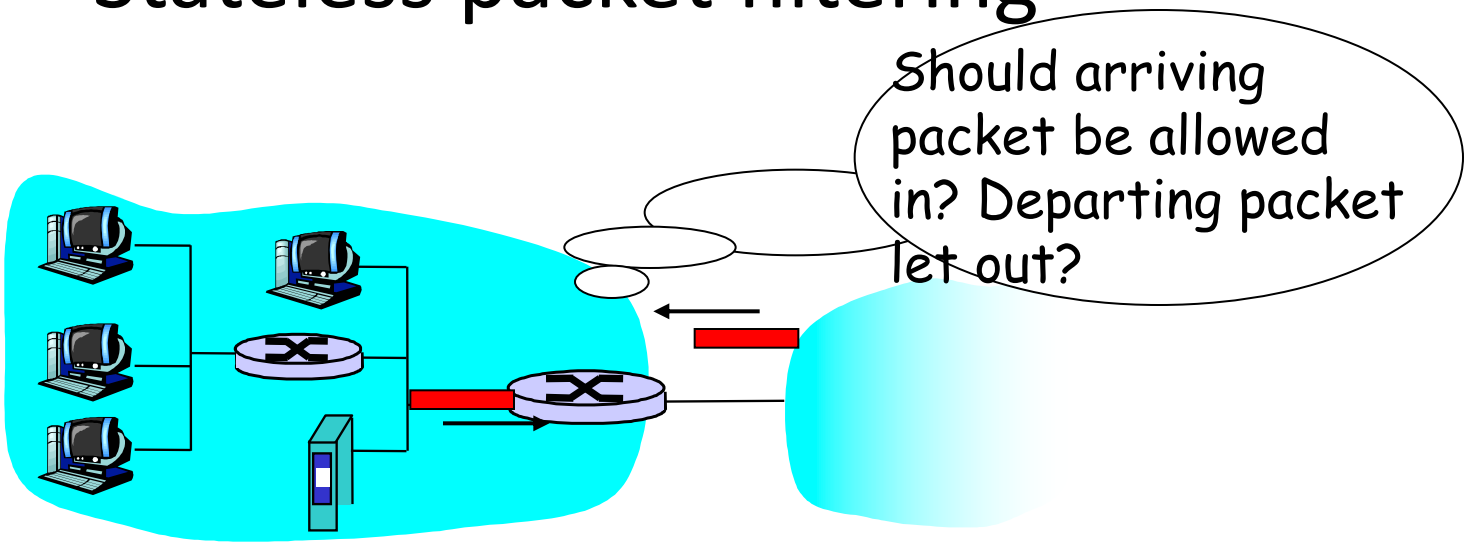
- e.g., attacker replaces CIA’s homepage with something else

allow only authorized access to inside network (set of authenticated users/hosts)

three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

Stateless packet filtering



- internal network connected to Internet via router firewall
- router filters packet-by-packet, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

Stateless packet filtering: example

- example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
  - all incoming, outgoing UDP flows and telnet connections are blocked.
- example 2: Block inbound TCP segments with ACK=0.
  - prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Stateless packet filtering: more examples

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Access Control Lists

- *ACL:* table of rules, applied top to bottom to incoming packets: (action, condition) pairs

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80 (web)	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53 (DNS)	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Stateful packet filtering

- stateless packet filter: heavy handed tool
  - admits packets that "make no sense," e.g., dest port = 80, ACK bit set, even though no TCP connection established:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *stateful packet filter:* track status of every TCP connection
  - track connection setup (SYN), teardown (FIN): can determine whether incoming, outgoing packets "makes sense"
  - timeout inactive connections at firewall: no longer admit packets

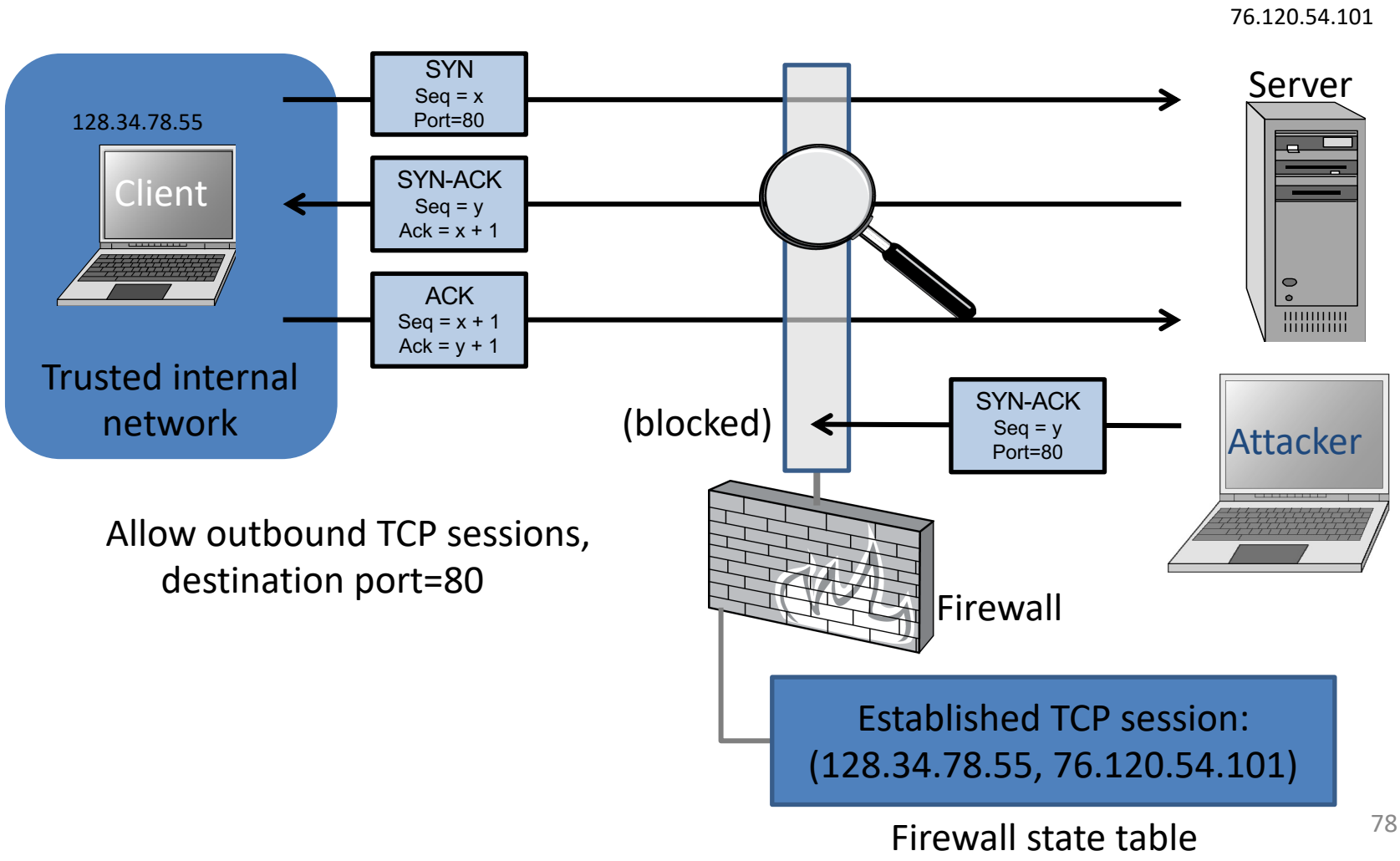
Stateful packet filtering

- ACL augmented to indicate need to check connection state table before admitting packet

action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

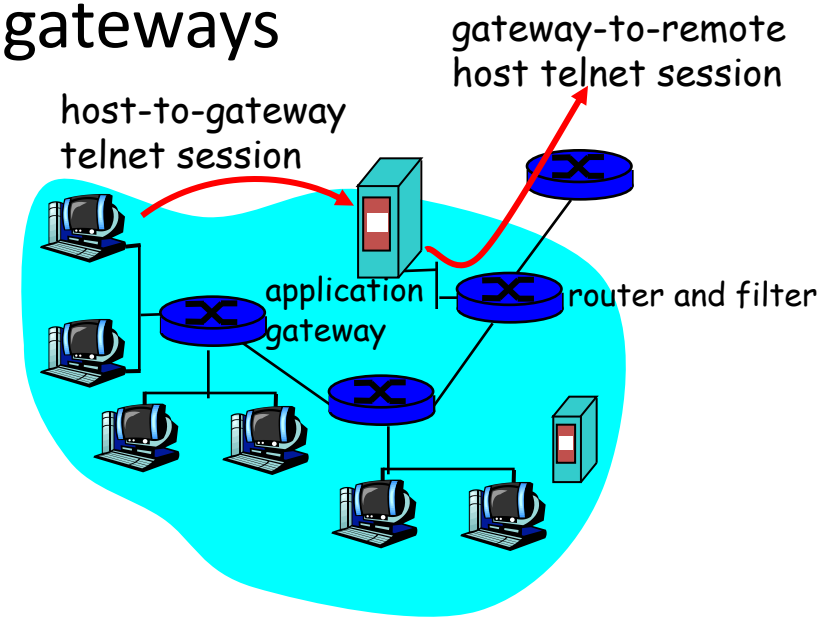
Statefull Firewall Example

- Allow only requested TCP connections:



Application gateways

- filters packets on application data as well as on IP/TCP/UDP fields.
- example: allow select internal users to telnet outside.



1. require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.

Limitations of firewalls and gateways

- IP spoofing: router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway.
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP.
- tradeoff: degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks.

Intrusion detection systems

- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- *IDS: intrusion detection system*
  - *deep packet inspection:* look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among multiple packets
    - port scanning
    - network mapping
    - DoS attack

Intrusion detection systems

- multiple IDSs: different types of checking at different locations