MONASH University
Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

MONASH University
Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

Lecture 8
IP Security

Unit Objectives

- ✓ OSI security architecture
  - **common security standards and protocols for network security applications**
  - **common information risks and requirements**
- ✓ operation of private key encryption techniques
- ✓ operation of public encryption techniques
- ✓ concepts and techniques for digital signatures, authentication and non-repudiation
- ✓ security threats of web servers, and their possible countermeasures
- ✓ Wireless Network Security Issues
- ✓ security threats of email systems and their possible countermeasures
- ✓ IP security
- • intrusion detection techniques for security purpose
- • risk of malicious software, virus and worm threats, and countermeasures
- • firewall deployment and configuration to enhance protection of information assets
- • network management protocol for security purpose

Review of Last Lecture

- **Security of email system is extremely important as this is the most widely used network-based application**
  - abuse of email (e.g., spreading of virus) is increasing
  - small change of financial data in email may bring disastrous consequences
- **Four key requirements of email security are:**
  - > Confidentiality, authentication, message integrity and non-repudiation of origin
- **Three main schemes that have emerged during past few years for email security are: PGP, S/MIME and DKIM**
- **PGP offers five services: Authentication, Confidentiality, Compression, E-mail compatibility and Segmentation**
- **PGP introduces the concept of key rings, key rings store key id, public keys, trust levels**
- **PGP is mainly for personal e-mail security, in future, S/MIME will probably emerge as the industry standard**
- **S/MIME secures MIME entity with encryption and digital signature with X509.v3 certificates**
- **DKIM: cryptographically signing email messages, domain claims responsibility, transparent to user**

Lecture 8: Objectives

- **Be familiar with Internet Protocol Security (IPSec) capabilities**
- **Understand IPSec Architecture**
- **Understand Encapsulating Security Payload (ESP)**
- **Be familiar with transport and tunnel modes of operation**
- **Appreciate the concept of security association and combining SAs**
- **Understand key management in IPSec**

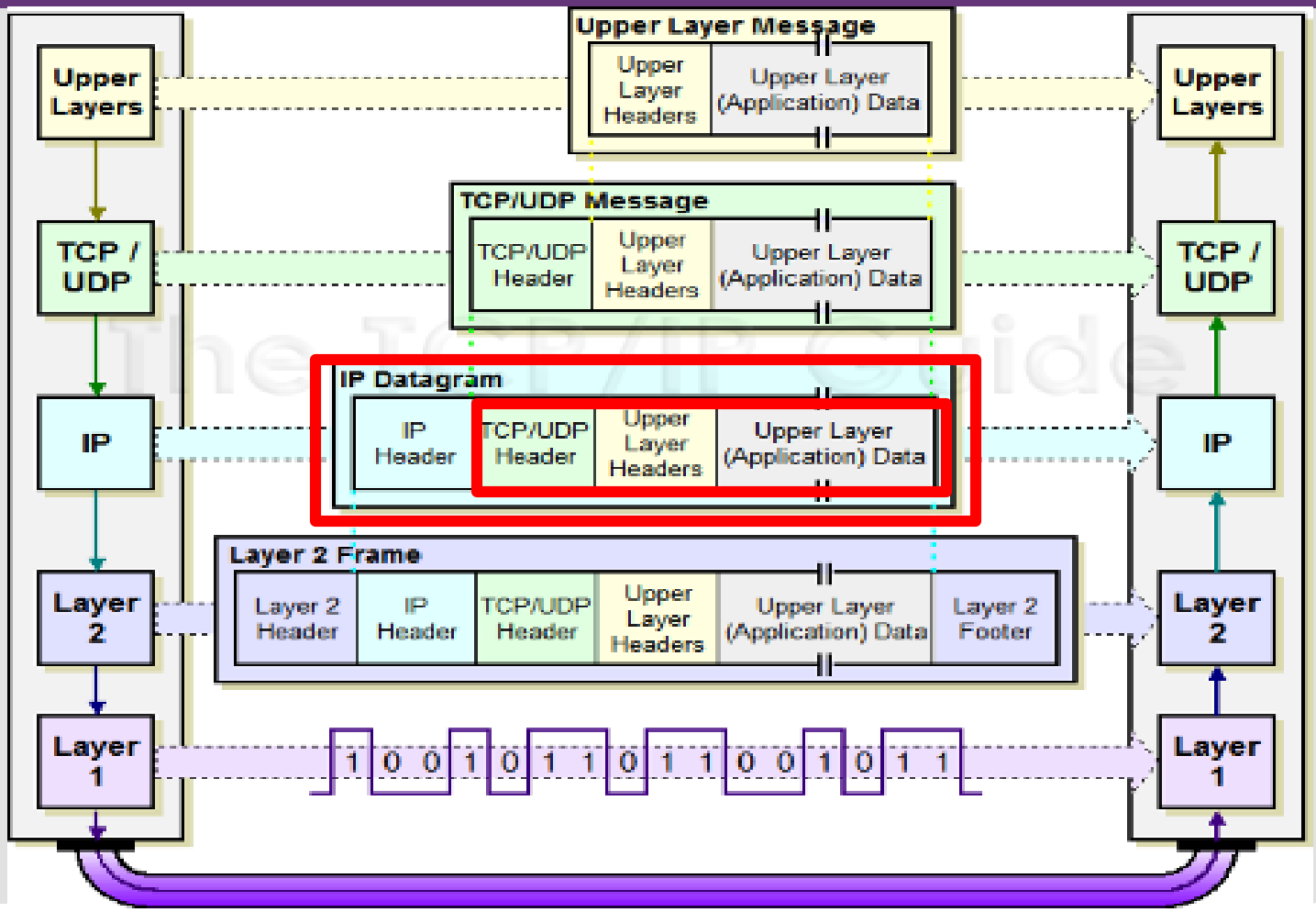
Lecture : Outline

- **IP Security**
- **Review of TCP/IP, IPv4 & IPv6**
- **Introduction to IPSec**
- **Security Association (SA)**
- **Encapsulating Security Payload (ESP)**
- **IPSec Operation modes**
- **Combining Security Association**
- **IPSec Key Management**

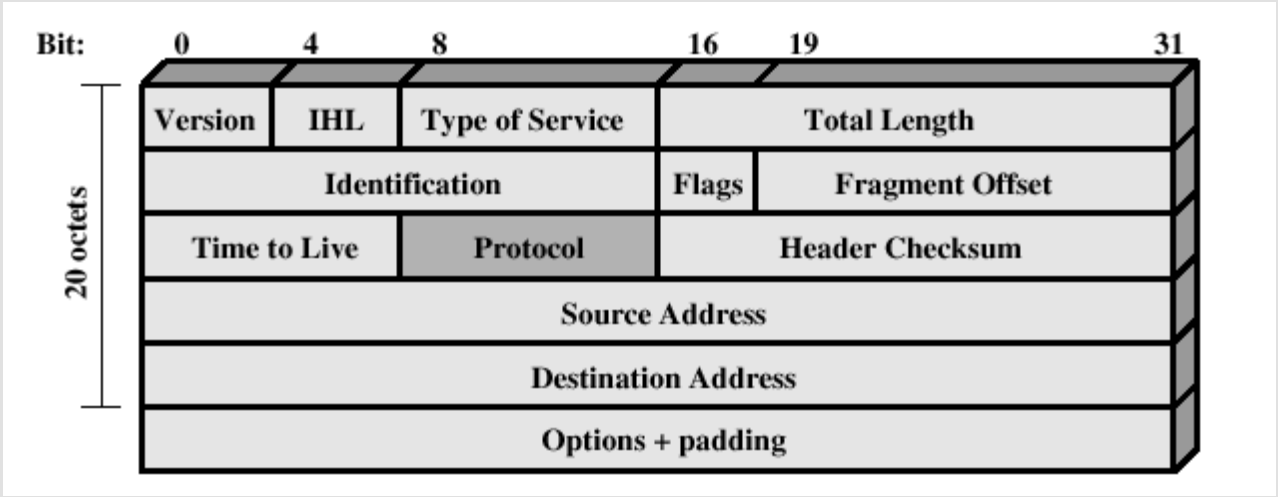
IP Security

- **have a range of application specific security mechanisms**
  - eg. S/MIME, PGP, Kerberos, SSL/HTTPS
- **however there are security concerns that cut across protocol layers**
- **would like security implemented by the network for all applications**

Encapsulation (5 layer TCP/ IP model)



Brief Preliminary: IPv4 header



- **Header length = 20 octets**
- **Some fields may change on route, i.e., 'Time to Live', 'Fragment Offset'**
- **'Header Checksum' is meant to protect header from corruption**
- **But hackers can purposely change header fields as well as checksum**

Brief Preliminary: TCP/IP Protocol

- **Internet Protocol is implemented at Network layer**
- **End systems and all intermediate nodes (router, gateway etc.) implements IP**
- **Packets are routed by IP**
- **No built-in security feature in IP**

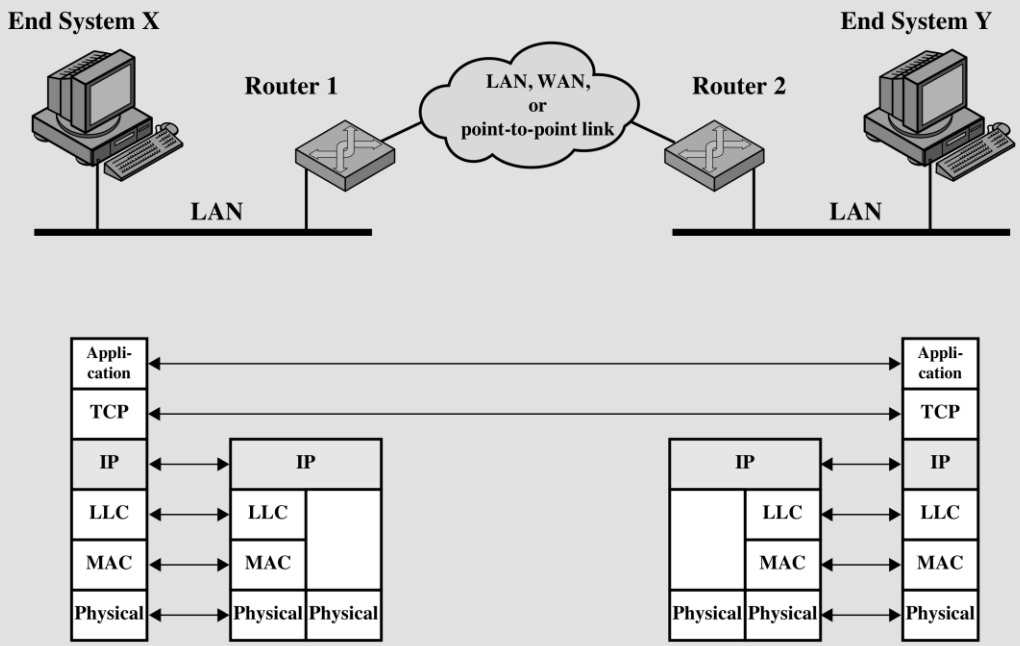
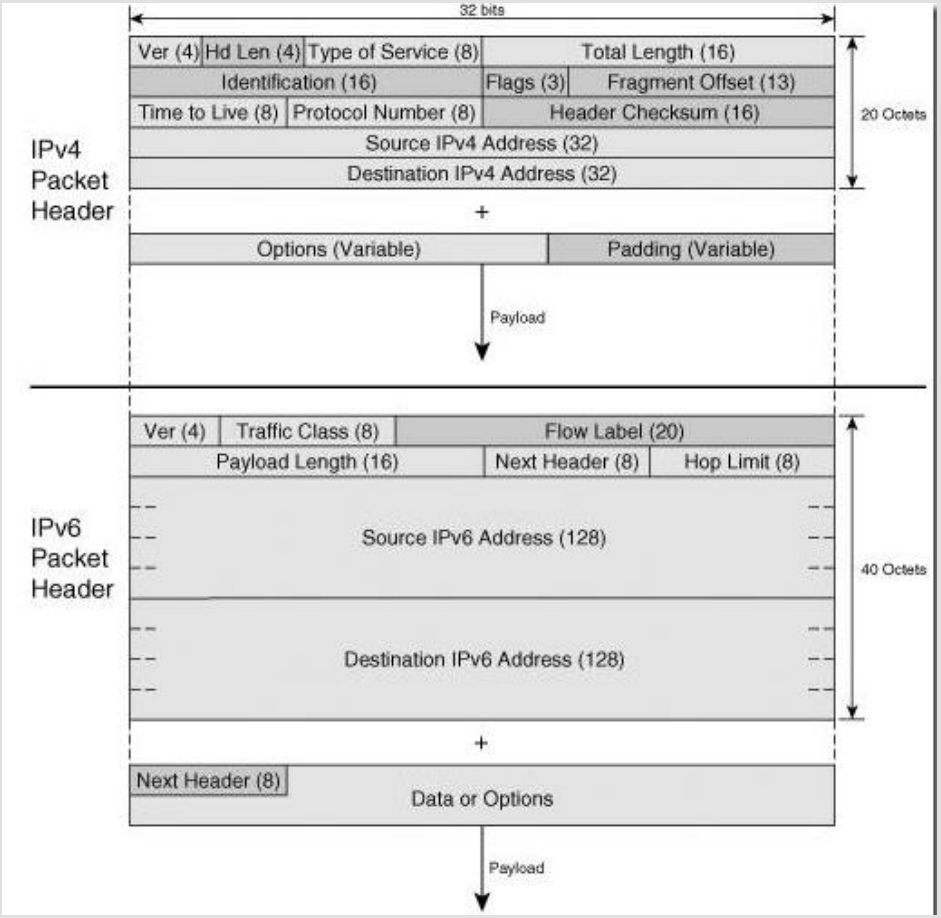


Figure 16.13 Configuration for TCP/IP Example

Brief Preliminary: IPv6 header

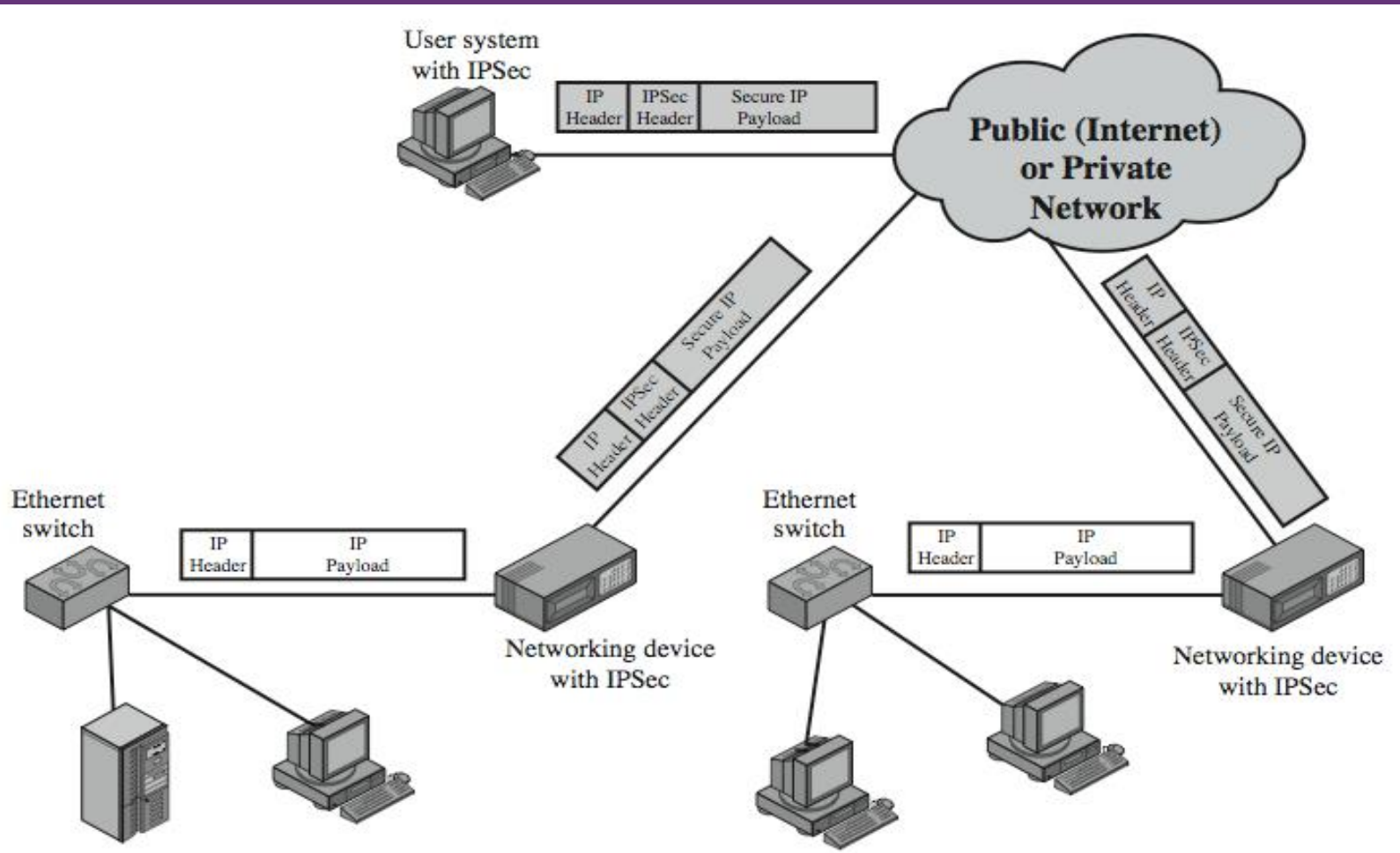
- **Header length = 40 octets**
- **Next Header field tells the receiver how to interpret the data which follows the header. If the packet contains options, this field contains the option type of the next option. The "Next Header" field of the last option, points to the upper-layer protocol that is carried in the packet's payload.**
- **IPv6 Optional Extension headers carry options that are used for special treatment of a packet in the network, e.g., for routing, fragmentation, and for security using the IPsec framework.**



IPSec

- **IPSec is a set of protocols to provide high quality, interoperable, and cryptology-based security for IP packets**
- **IPSec Provides**
  - **authentication**
  - **confidentiality**
  - **key management**
- **applicable to use over LANs, across public & private WANs, & for the Internet**
- **IPSec needs are identified in 1994 report**
  - need authentication, encryption in IPv4 & IPv6

IP Security Uses



Benefits of IPSec

- When implemented in a firewall/router it provides strong security to all traffic crossing the perimeter
- When implemented in a firewall/router it is resistant to any traffic bypass
- It is Implemented below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users
- secures routing architecture

IPSec Applications

- **IPSec can assure that:**
  - a router or neighbour 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
- **secure branch office connectivity over the Internet**
- **secure remote access over the Internet**
- **establishing extranet and intranet connectivity with partners**
- **enhancing electronic commerce security**

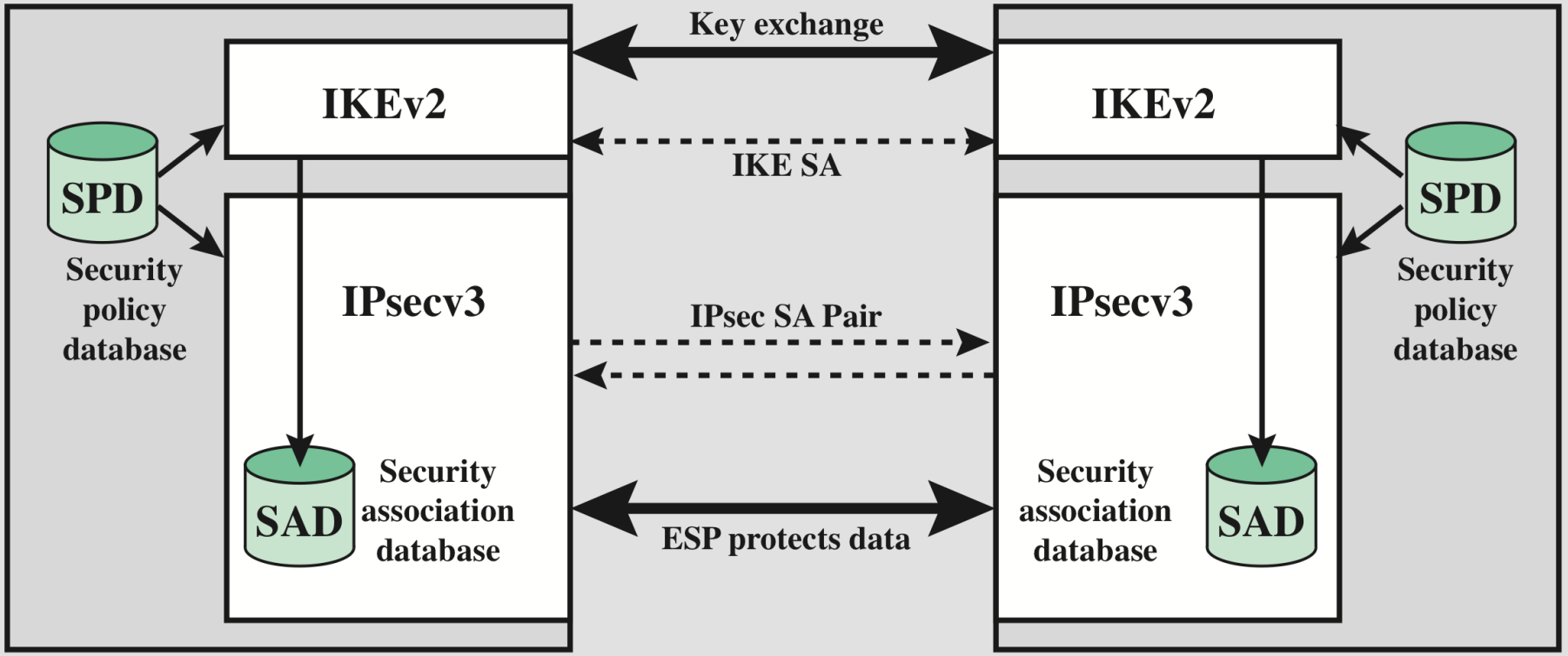
IP Security Architecture

- **specification is quite complex, with groups:**
  - **Architecture**
    > RFC4301 Security Architecture for Internet Protocol
  - **Authentication Header (AH)**
    > RFC4302 IP Authentication Header
  - **Encapsulating Security Payload (ESP)**
    > RFC4303 IP Encapsulating Security Payload (ESP)
  - **Internet Key Exchange (IKE)**
    > RFC4306 Internet Key Exchange (IKEv2) Protocol
  - **Cryptographic algorithms**
  - Other

IPSec Services

1. **Access control**
2. **Connectionless integrity**
3. **Data origin authentication**
4. **Rejection of replayed packets**
   – a form of partial sequence integrity
5. **Confidentiality (encryption)**
6. **Limited traffic flow confidentiality**

IP Security Policy



Security Associations (SA)

- **SA is a one-way relationship between sender & receiver that affords security for traffic flow**
- **SA is defined by 3 parameters:**
  1. Security Parameters Index (SPI)
  2. IP Destination Address
  3. Security Protocol Identifier AH or ESP
- **SA has a number of other parameters**
  - seq no, AH & ESP info, lifetime etc.
- **SA have a database of Security Associations SAD & SPD**

Security Association Database (SAD)

A SAD is normally defined by the following parameters in an SAD entry.

1. **Security Parameter Index: A 32-bit value selected by the receiving end of an SA to uniquely identify the SA.**
2. **Sequence Number Counter: A 32-bit value used to generate the Sequence Number field in AH or ESP headers.**
3. **Sequence Counter Overflow: A flag indicating whether overflow of the Sequence Number Counter to prevent further transmission of packets on this SA.**
4. **Anti-Replay Window: Used to determine whether an inbound AH or ESP packet is a replay.**
5. **AH Information: Authentication algorithm, keys, key lifetimes, and related parameters being used with AH.**
6. **ESP Information: Encryption and authentication algorithm, keys, initialization values, key lifetimes, and related parameters being used with ESP.**
7. **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).**
8. **IPsec Protocol Mode: Tunnel or transport.**
9. **Path MTU: Maximum size of a packet that can be transmitted without fragmentation.**

Security Policy Database (SPD)

The following selectors determine an SPD entry:

1. **Remote IP Address: This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address. The latter two are required to support more than one destination system sharing the same SA (e.g., behind a firewall).**
2. **Local IP Address: This may be a single IP address, an enumerated list or range of addresses, or a wildcard (mask) address. The latter two are required to support more than one source system sharing the same SA (e.g., behind a firewall).**
3. **Next Layer Protocol: The IP protocol header (IPv4, IPv6, or IPv6 Extension) includes a field (Protocol for IPv4, Next Header for IPv6 or IPv6 Extension) that designates the protocol operating over IP. This is an individual protocol number, ANY, or for IPv6 only. If AH or ESP is used, then this IP protocol header immediately precedes the AH or ESP header in the packet.**

Security Policy Database (Host SPD example)

- **relates IP traffic to specific SAs**
  - **match subset of IP traffic to relevant SA**
  - **use selectors to filter outgoing traffic to map**
  - **based on: local & remote IP addresses, next layer protocol, name, local & remote ports**

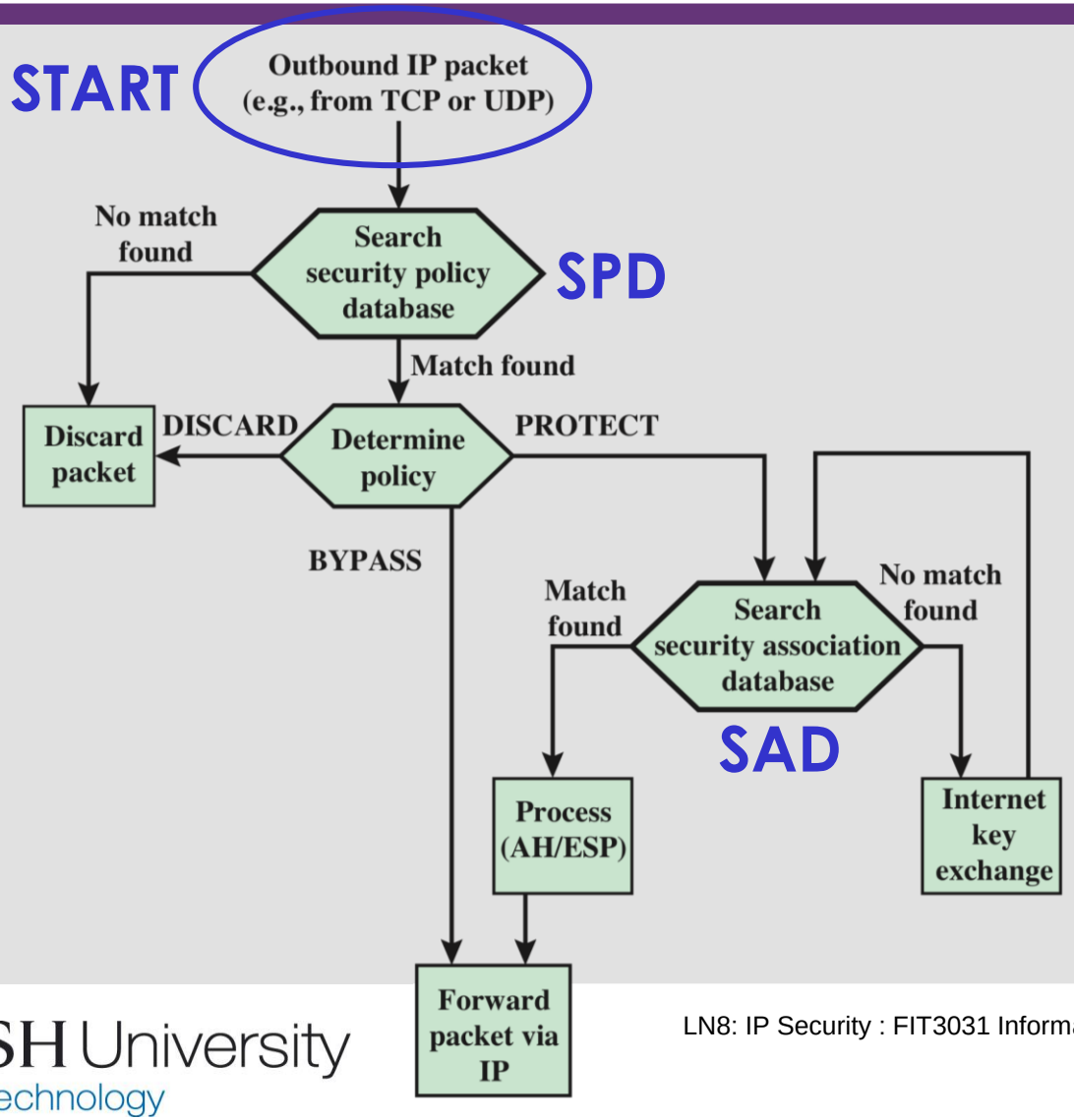
Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	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

Local LAN 1.2.3.0/24

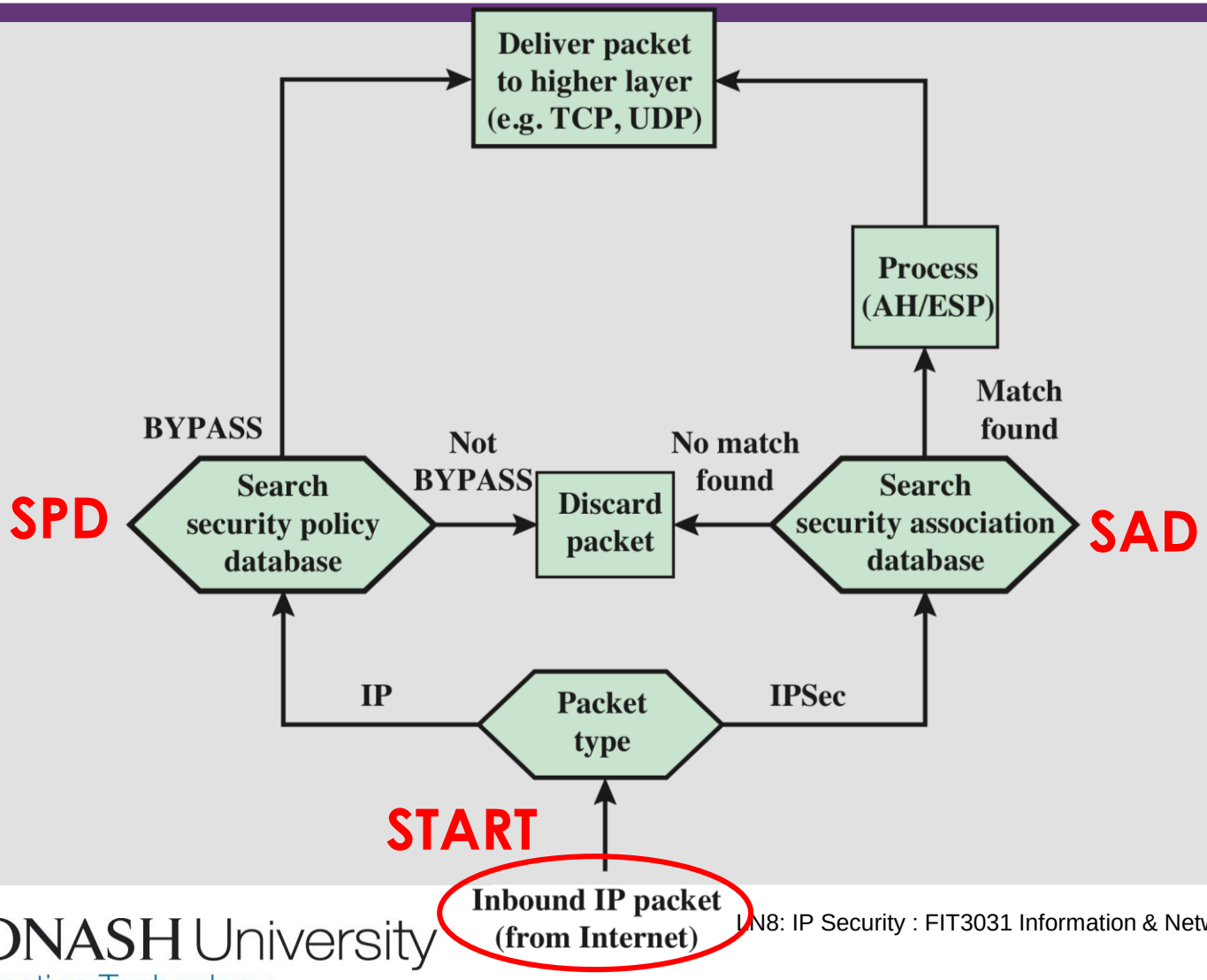
Local Host: 1.2.3.101

Server: 1.2.4.10

IP Traffic Processing : Outbound Packets



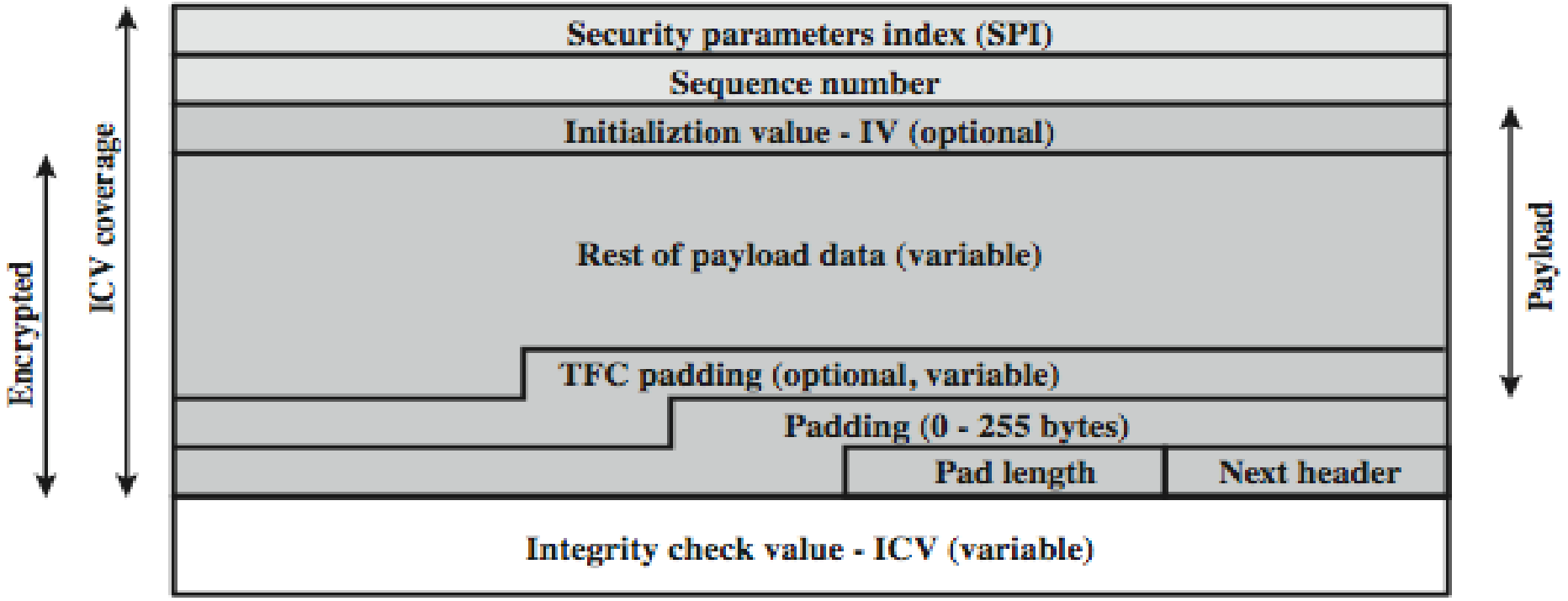
IP Traffic Processing : **Inbound Packets**



Encapsulating Security Payload (ESP)

- **provides message content confidentiality, data origin authentication, connectionless integrity, an anti-replay service, limited traffic flow confidentiality**
- **services depend on options selected when establish Security Association (SA), net location**
- **can use a variety of encryption & authentication algorithms**

Encapsulating Security Payload (ESP)



Encryption & Authentication Algorithms & Padding

- **ESP can encrypt payload data, padding, pad length, and next header fields**
  - if needed have IV at start of payload data
- **ESP can have optional ICV (Integrity check value) for integrity**
  - is computed after encryption is performed
- **ESP uses padding**
  - to expand plaintext to required length
  - to align pad length and next header fields
  - to provide partial traffic flow confidentiality

Anti-Replay Service

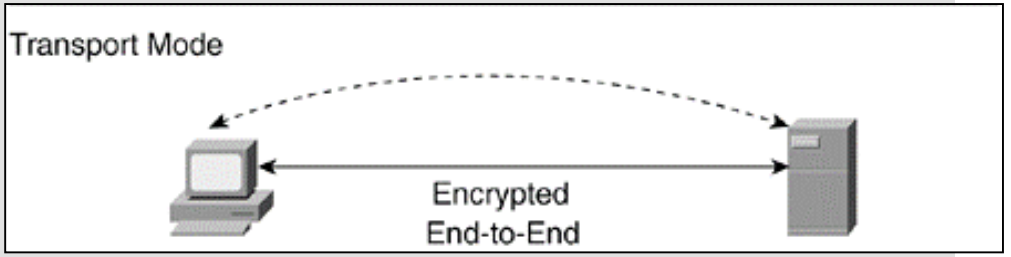
Replay is when attacker resends a copy of an authenticated packet

- **use sequence number (32 bits) to thwart this attack**
- **sender initializes sequence number to 0 when a new SA is established**
  - increment for each packet
  - must not exceed the limit of $2^{32} - 1$
  - If this limit is reached, the sender **terminates** SA and renegotiate a new SA with a **new key**
- **receiver then accepts packets with sequence numbers within the window range of (N –W+1) to N**
  - **where W=window size; N = 2^{32}**

Transport and Tunnel Modes

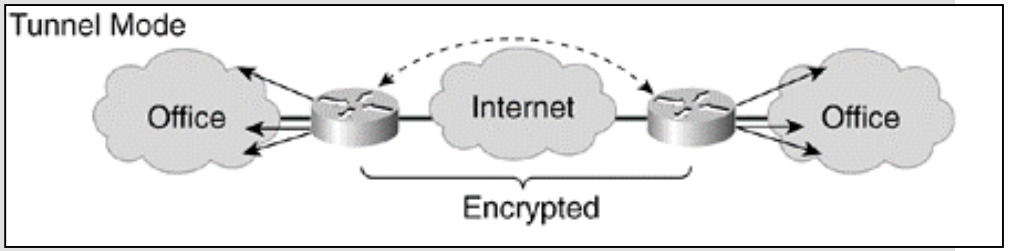
Transport Mode

- to encrypt & optionally authenticate IP data
- can do traffic analysis but is efficient
- good for ESP of **host to host** traffic

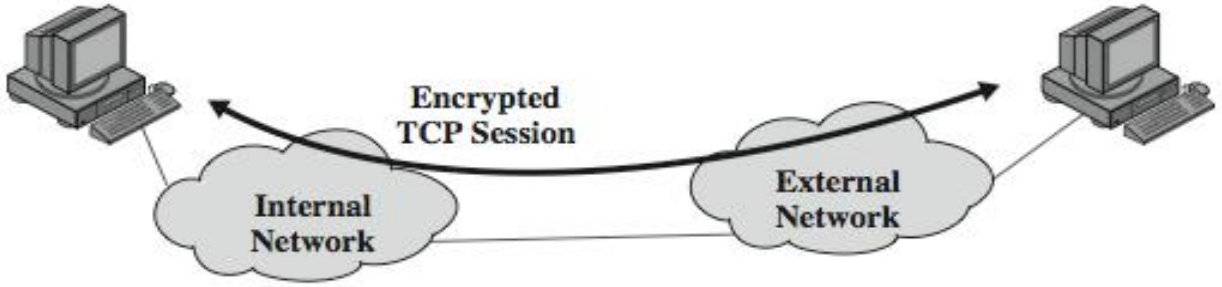


Tunnel Mode

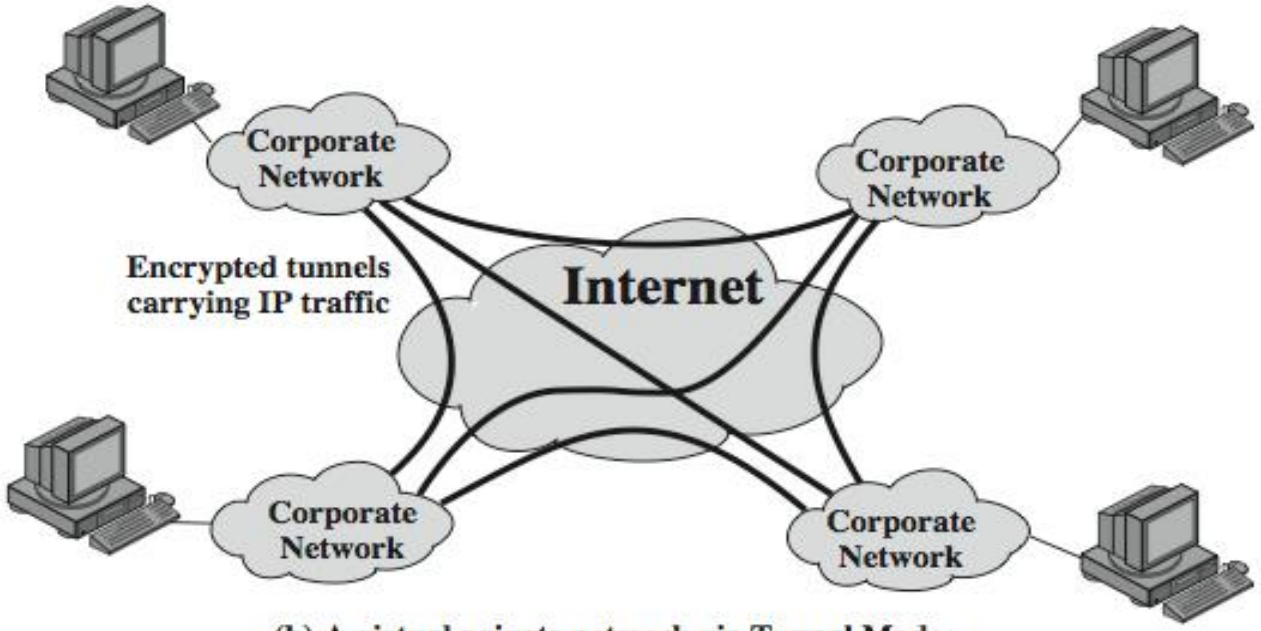
- encrypts entire IP packet
- add new header for next hop
- no routers on way can examine inner IP header
- good for VPNs, **gateway to gateway** security



Transport and Tunnel Modes

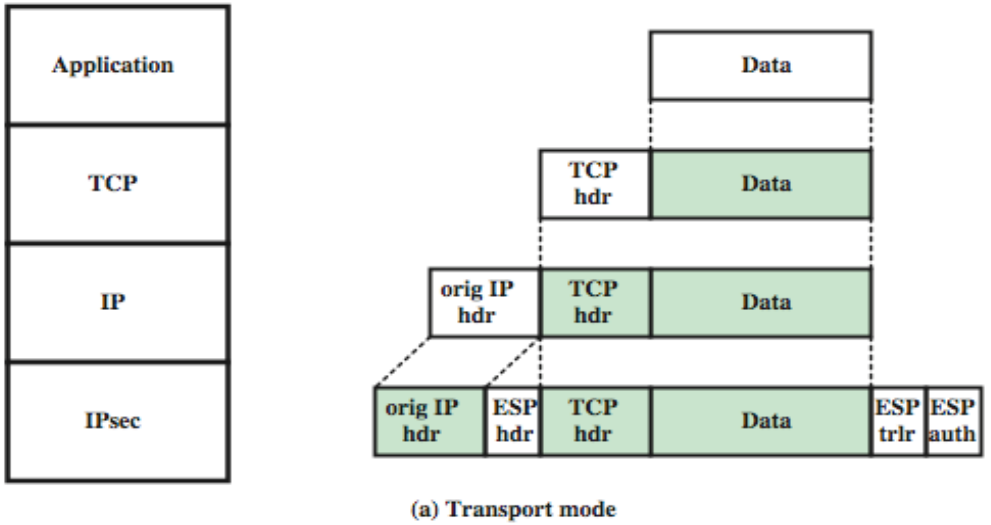


(a) Transport-level security



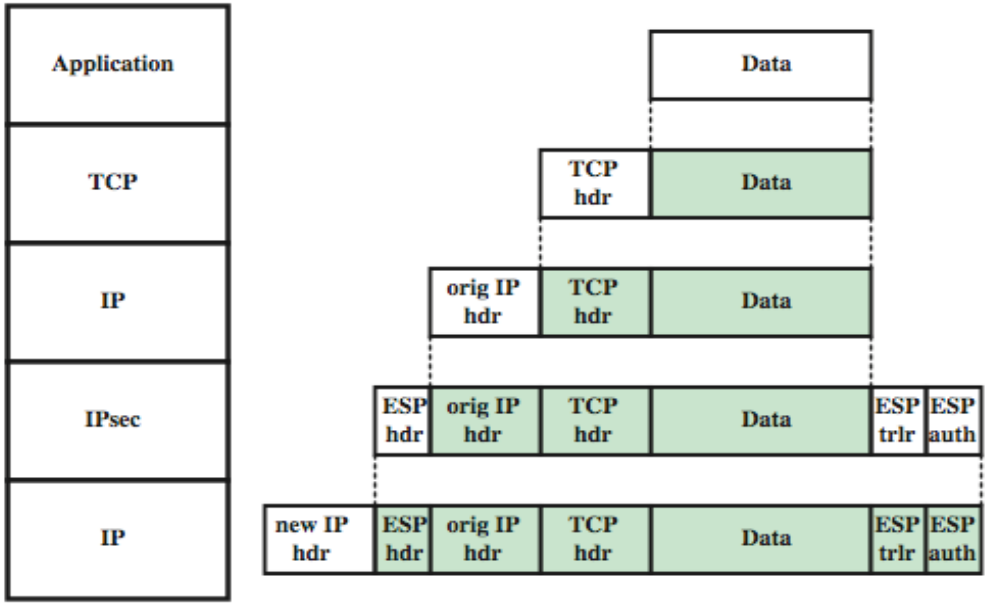
(b) A virtual private network via Tunnel Mode

Transport Mode Protocols with the use of ESP



(a) Transport mode

Tunnel Mode Protocols with the use of ESP



(b) Tunnel mode

Security association bundle

- **Traffic flow between hosts may require IPSec but separate services between security gateways**
- **In all cases, multiple SAs need to be employed for the same traffic flow to achieve IPSec**
- **Security association bundle refers to a sequence of SAs through which traffic must be processed to provide desired set of IPSec services.**

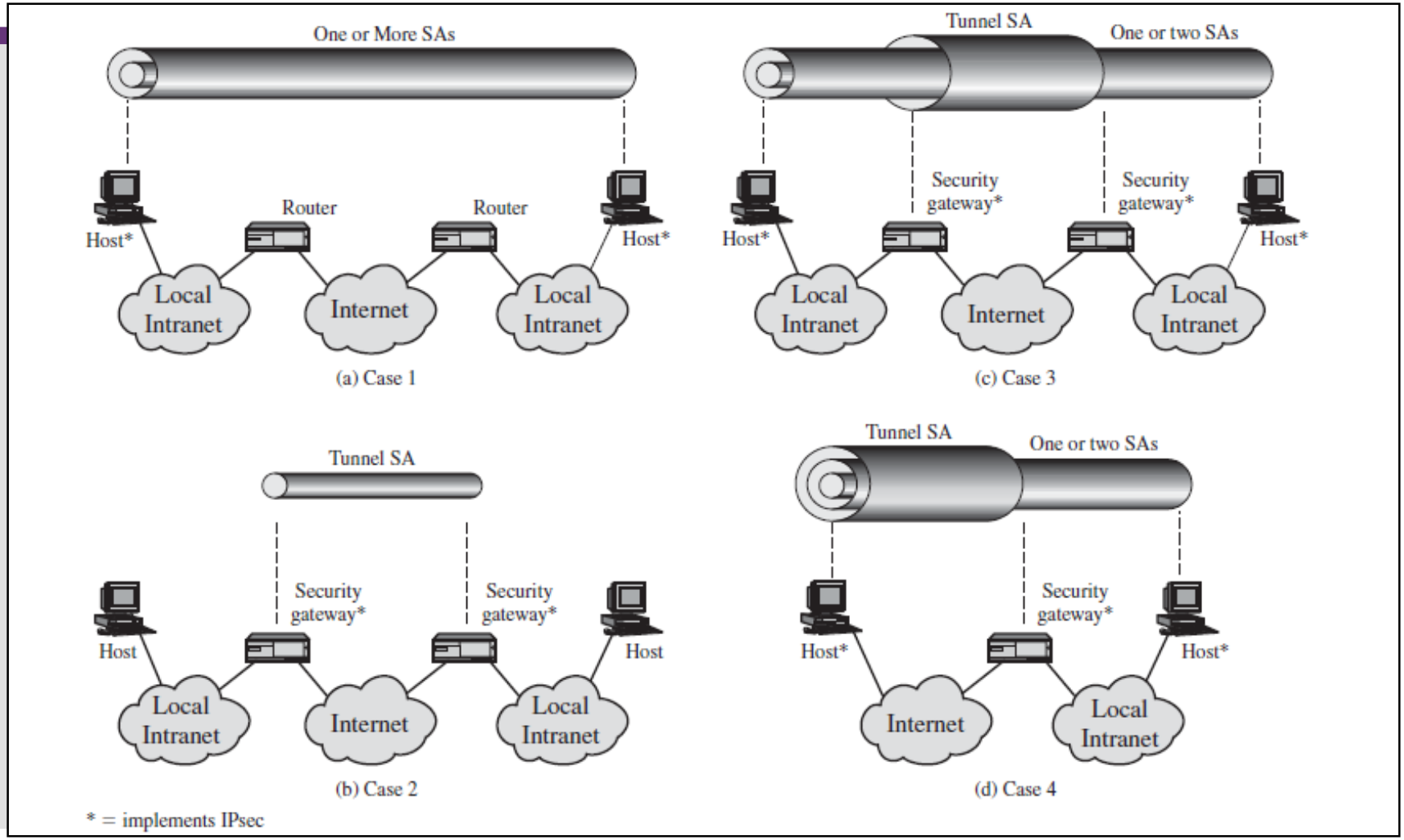
SA bundles

- **Transport adjacency**
  - Applying more than one security protocol (AH, ESP) to the **same IP packet without invoking tunneling**
- **Iterated tunneling**
  - Application of multiple layers of security protocols (AH, ESP) **effected through IP tunneling**
- **The two above approaches can be combined**
  - Example: **transport** SA **between hosts** travel part of the way through a **tunnel** SA between security **gateways**

Authentication Plus Confidentiality

- **ESP with authentication option**
  - **Option-1**:- ESP to data followed by → authentication data(AH) on ciphertext
  - **Option-2**:-Transport Adjacency
    - > Use 2 bundles of SAs
  - **Option-3**:- Transport-Tunnel Bundle
    - > Authentication prior to encryption
    - > Inner AH transport SA and an outer ESP tunnel SA

Combining Security Associations



IPSec Key Management

- **handles key generation & distribution**
- **typically need 2 pairs of keys**
  - 1 pair of keys for both directions for AH
  - 1 pair of keys for both directions for ESP

A. manual key management

- Use sysadmin to manually configures every system

B. automated key management

- automated system for on demand creation of keys for SA's in large systems
- ***has Oakley & ISAKMP elements***

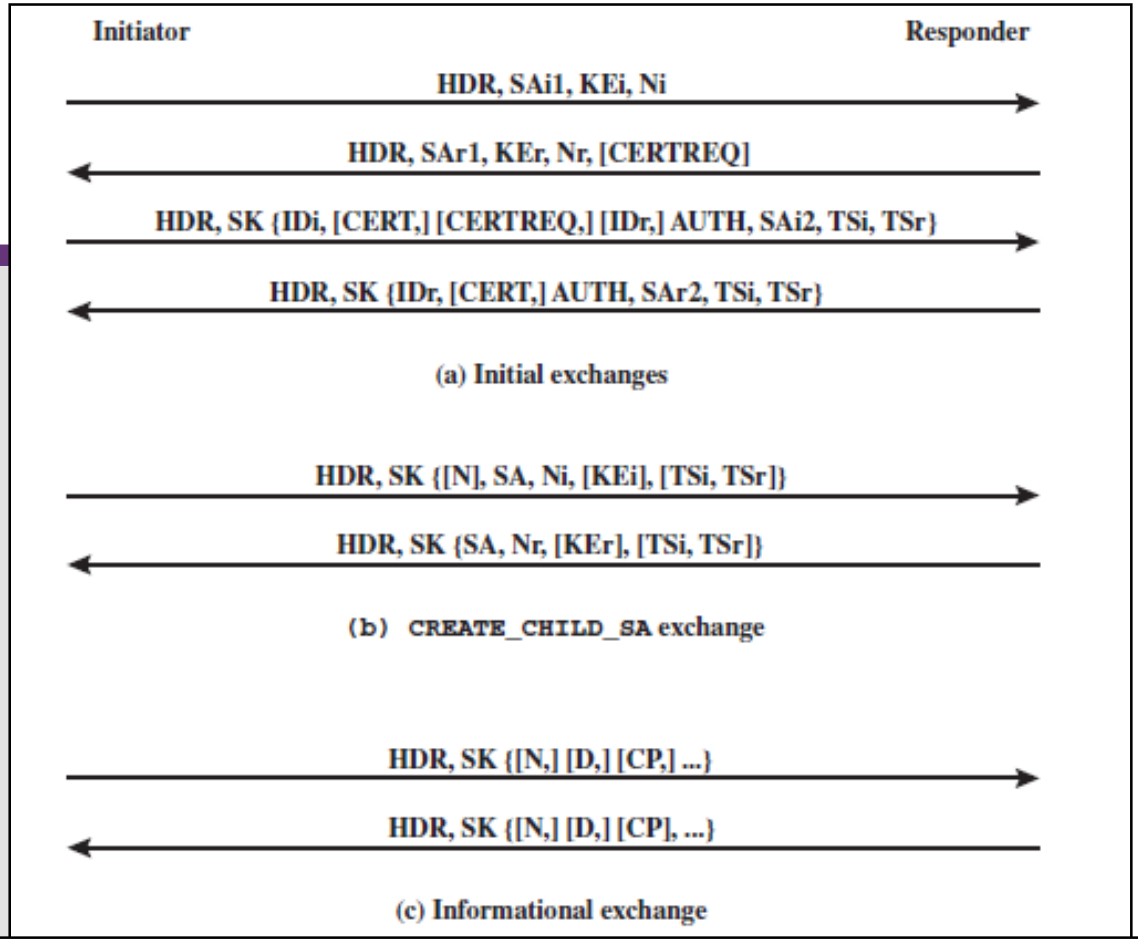
Oakley –automated key management

- **a key exchange protocol**
- **based on Diffie-Hellman key exchange**
- **adds features to address weaknesses**
  - no info on parties, man-in-middle attack, cost
  - so adds cookies, groups (global params), nonces, DH key exchange with authentication
- **can use arithmetic in prime fields or elliptic curve fields**

ISAKMP –automated key management

- **Internet Security Association and Key Management Protocol (ISAKMP)**
- **provides framework for key management**
- **defines procedures and packet formats to establish, negotiate, modify, & delete SAs**
- **independent of key exchange protocol, encryption algorithm, & authentication method**
- **IKEv2 no longer uses Oakley & ISAKMP in IKEv1 terms, but basic functionality is same**

IKEV2 Exchanges



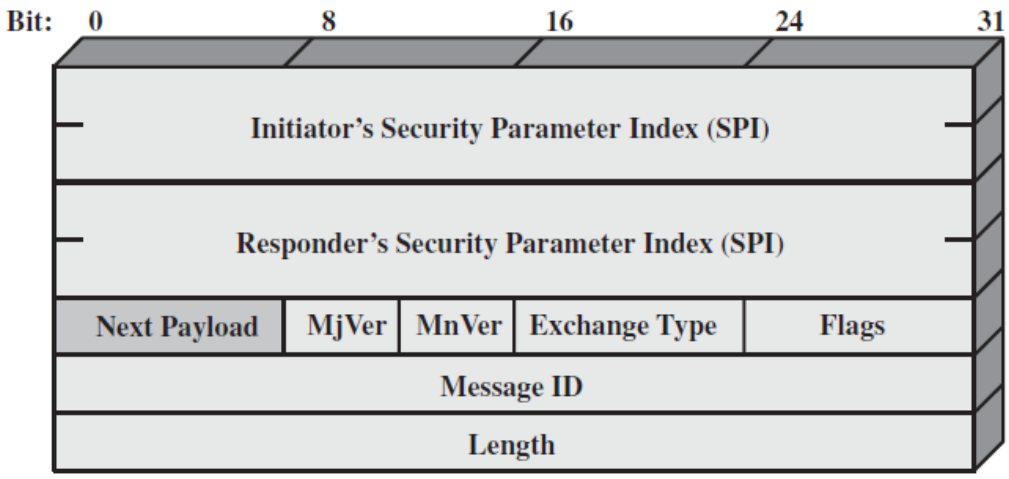
HDR = IKE header
SAx1 = offered and chosen algorithms, DH group
KEx = Diffie-Hellman public key
Nx= nonces
CERTREQ = Certificate request
IDx = identity
CERT = certificate

SK {...} = MAC and encrypt
AUTH = Authentication
SAx2 = algorithms, parameters for IPsec SA
TSx = traffic selectors for IPsec SA
N = Notify
D = Delete
CP = Configuration

ISAKMP: IKE Format

The header format for an ISAKMP message, which includes the fields:

- ✓ Initiator SPI (64 bits): chosen by the initiator to identify a unique SA
- ✓ Responder Cookie (64 bits): chosen by responder to identify unique IKE SA
- ✓ Next Payload (8 bits): type of the first payload in the message.
- ✓ Major/Minor **Version** (4 bits): Indicates major/minor version of IKE in use (v1, v2)
- ✓ Exchange Type (8 bits): type of exchange.
- ✓ Flags (8 bits): specific options IKE exchg.
- ✓ Message ID (32 bits): control retransmission, matching of reqs/resps.
- ✓ Length (32 bits): Total message (header plus all payloads) in octets



IKE Payloads & Exchanges

- **have a number of ISAKMP payload types:**
  - Security Association, Key Exchange, Identification, Certificate, Certificate Request, Authentication, Nonce, Notify, Delete, Vendor ID, Traffic Selector, Encrypted, Configuration, Extensible Authentication Protocol
- **payload has complex hierarchical structure**
- **may contain multiple proposals, with multiple protocols & multiple transforms**

Cryptographic Suites

- **variety of cryptographic algorithm types**
- **to promote interoperability have**
  - RFC4308 defines VPN cryptographic suites
    - > VPN-A matches common corporate VPN security using 3DES & HMAC
    - > VPN-B has stronger security for new VPNs implementing IPsecv3 and IKEv2 using AES
  - RFC4869 defines four cryptographic suites compatible with US NSA specs
    - > provide choices for ESP & IKE
    - > AES-GCM, AES-CBC, HMAC-SHA, ECP, ECDSA

Summary

- **have considered:**
  - IPSec security framework
  - IPSec security policy
  - ESP
  - combining security associations
  - internet key exchange
  - cryptographic suites used

Further Reading

- **Study Guide 8**
- **Chapter 8 & Appendix D (TCP-IP) of the textbook: Network Security Essentials-Application & Standards" by William Stallings 5th Edition, Prentice Hall, 2013**

- **Acknowledgement: part of the materials presented in the slides was developed with the help of Instructor's Manual and other resources made available by the author of the textbook.**