QUEEN'S UNIVERSITY BELFAST

ESTD 1845

Tunneling and VPNs – Part 2

Dr. Sandra Scott-Hayward

CSC3064 Lecture 10

School of Electronics, Electrical Engineering and Computer Science

Session Overview

- IPSec

References:
Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.
Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.
Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2007.

QUEEN'S UNIVERSITY BELFAST

IPSec - Overview

- Security problems of IP and objectives of IPsec
- The IPsec architecture:
  - IPsec security protocol modes:
    - Transport mode
    - Tunnel mode
  - IP Security Policy Database (SPD)
  - Security associations (SA) and the SA Database (SADB)
- IPsec security protocols:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Entity Authentication and the Internet Key Exchange (IKE)

QUEEN'S UNIVERSITY BELFAST

Recap – Security Problems of the Internet Protocol

When an entity receives an IP packet, it has no assurance of:

- *Data origin authentication / data integrity:*
  - The packet has actually been sent by the entity which is referenced by the source address of the packet
  - The packet contains the original content the sender placed into it, so that it has not been modified during transport
  - The receiving entity is in fact the entity to which the sender wanted to send the packet
- *Confidentiality:*
  - The original data was not inspected by a third party while the packet was sent from the sender to the receiver

QUEEN'S UNIVERSITY BELFAST

Security objectives of IPSec

IPsec aims to ensure the following security objectives:

- *Data origin authentication / connectionless data integrity:*
  - It is not possible to send an IP datagram with either a masqueraded IP source or destination address without the receiver being able to detect this
  - It is not possible to modify an IP datagram in transit, without the receiver being able to detect the modification
  - *Replay protection:* it is not possible to later replay a recorded IP packet without the receiver being able to detect this
- *Confidentiality:*
  - It is not possible to eavesdrop on the content of IP datagrams

Security objectives of IPSec

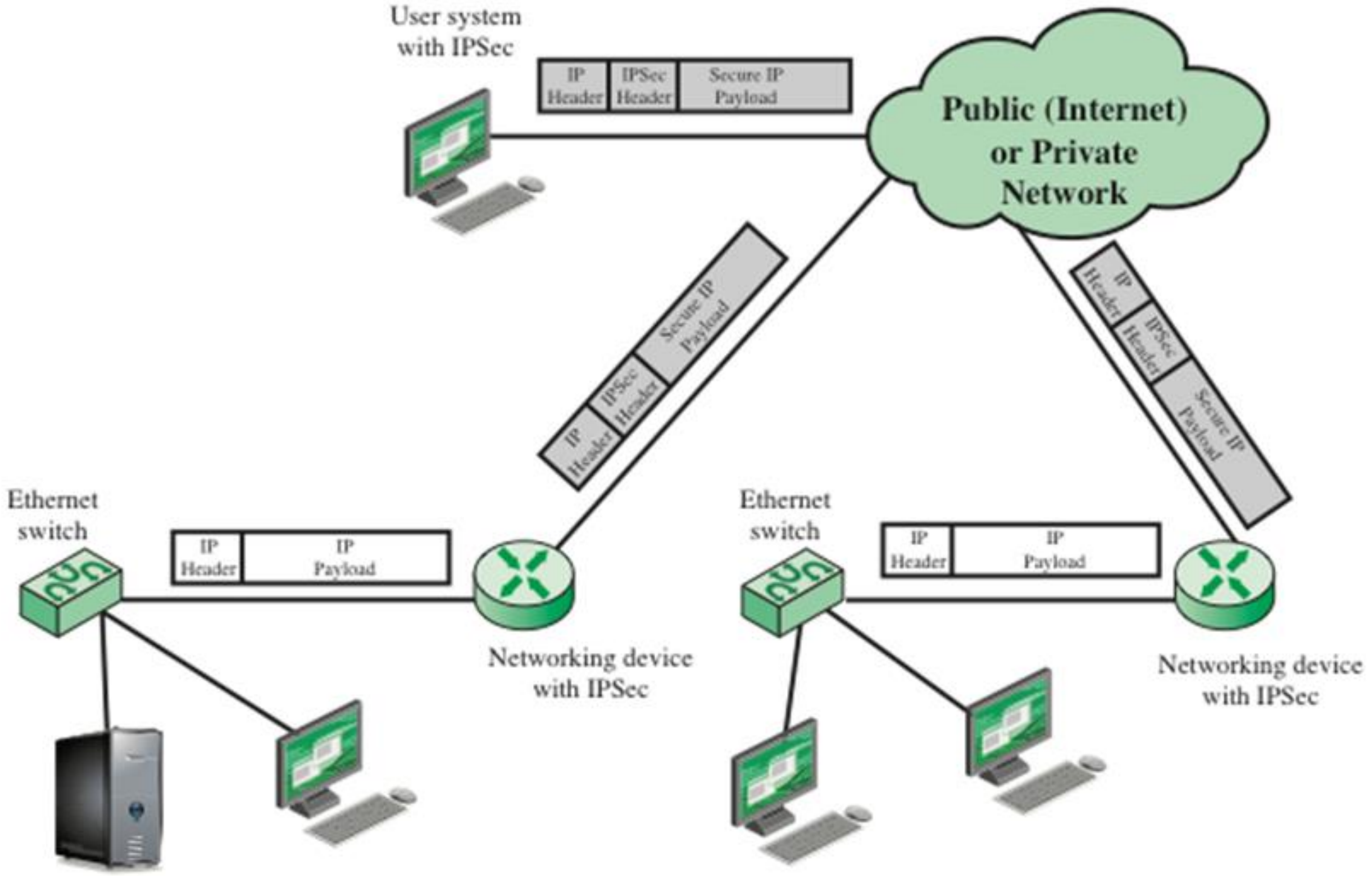
Security policy:

- Sender, receiver and intermediate nodes can determine the required protection for an IP packet according to a local security policy
- Intermediate nodes and the receiver will drop IP packets that do not meet these requirements

IPSec

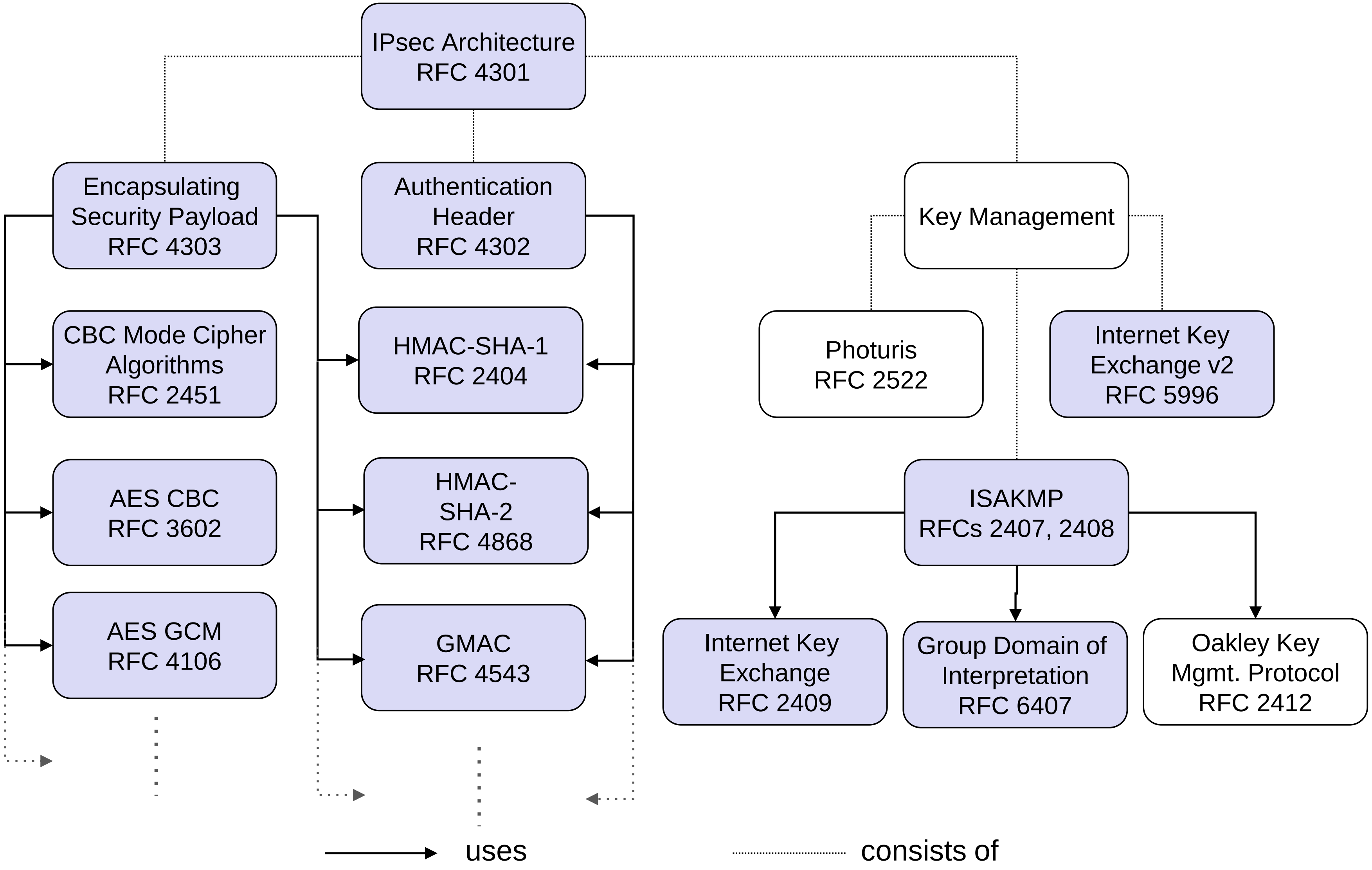
- Security extensions for IPv4 and IPv6
- IP Authentication Header (AH)
    - Authentication and integrity of payload and header
- IP Encapsulating Security Protocol (ESP)
    - Confidentiality of payload
- ESP with optional ICV (integrity check value)
    - Confidentiality, authentication and integrity of payload

IPSec Scenario



Overview of IPSec Standardization

Background



QUEEN'S UNIVERSITY BELFAST

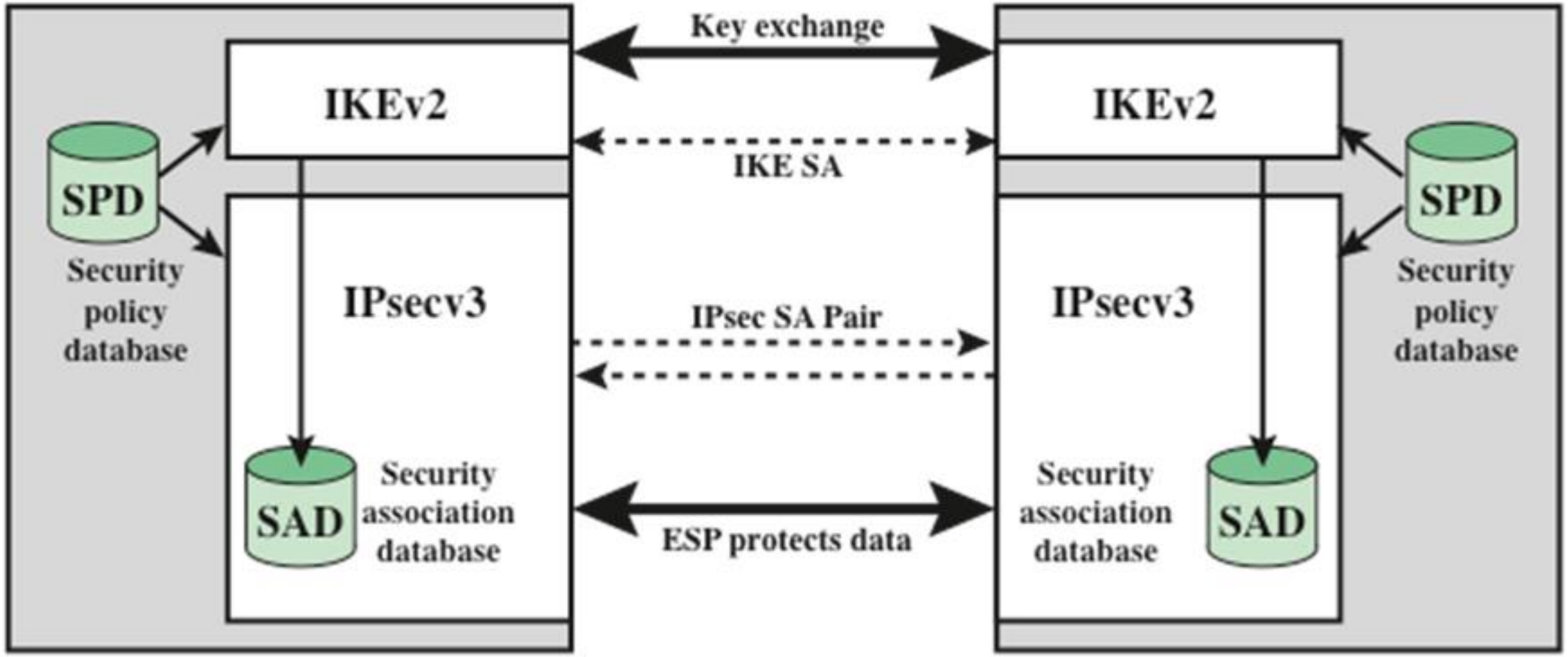
Overview of the IPSec architecture (1)

RFC 4301 defines the basic architecture of IPsec:

- Concepts:
  - Security association (SA), security association database (SADB)
  - Security policy, security policy database (SPD)
- Fundamental IPsec Protocols:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Protocol Modes:
  - Transport Mode
  - Tunnel Mode
- Key Management Procedures:
  - IKE & IKEv2

QUEEN'S UNIVERSITY BELFAST

Overview of the IPSec architecture (2)



Overview of the IPSec architecture (3)

A *security association (SA)* is a simplex "connection" that provides security services to the traffic carried by it

- Security services are provided to one SA by the use of either AH or ESP, but not both
- For bi-directional communication two security associations are needed
- An SA is uniquely identified by a triple consisting of a *security parameter index (SPI)*, an IP destination address, and a security protocol identifier (AH / ESP)
- An SA can be set up between the following peers:
  - Host ↔ Host
  - Host ↔ Gateway (or vice versa)
  - Gateway ↔ Gateway
- There are two conceptual databases associated with SAs:
  - The security policy database (SPD) specifies what security services are to be provided to which IP packets and in what fashion
  - The security association database (SADB)

IPSec Security Policy Selection

The following selectors to be extracted from the network and transport layer headers allow to select a specific policy in the SPD:

- *IP source address:*
  - Specific host, network prefix, address range, or wildcard
- *IP destination address:*
  - Specific host, network prefix, address range, or wildcard
- *Protocol:*
  - The protocol identifier of the transport protocol for this packet
- *Upper layer ports:*
  - If accessible, the upper layer ports for session oriented policy selection

IPSec Security Policy Definition

Example: Protect the Post Office Protocol v3 (POP3) traffic between a mail client node A and a mail server node B. Encrypt the traffic to protect private email exchange.

SP Entries Node A

Direction	**Outbound**	**Inbound**
Source Address	Node A	POP Server B
Destination Address	POP server B	Node A
Upper Layer Protocol	TCP	TCP
Upper Layer Source Port	Any	POP3
Upper Layer Destination Port	POP3	Any
IPsec Protocol	ESP	ESP
Mode	Transport	Transport

SP Entries Node B

Direction	**Outbound**	**Inbound**
Source Address	POP Server B	Node A
Destination Address	Node A	POP server B
Upper Layer Protocol	TCP	TCP
Upper Layer Source Port	POP3	Any
Upper Layer Destination Port	Any	POP3
IPsec Protocol	ESP	ESP
Mode	Transport	Transport

QUEEN'S UNIVERSITY BELFAST

IPSec Security Association

Example: Protect the Post Office Protocol v3 (POP3) traffic between a mail client node A and a mail server node B. Encrypt the traffic to protect private email exchange.

SA Entries Node A

Direction	**Outbound**	**Inbound**
SPI	1000	1001
Destination Address	POP Server B	Node A
IPsec Protocol	ESP	ESP
Algorithm	3DES-CBC	3DES-CBC
Key	The secret key from A to B	The secret key from B to A
Mode	Transport	Transport

SA Entries Node B

Direction	**Outbound**	**Inbound**
SPI	1001	1000
Destination Address	Node A	POP Server B
IPsec Protocol	ESP	ESP
Algorithm	3DES-CBC	3DES-CBC
Key	The secret key from B to A	The secret key from A to B
Mode	Transport	Transport

Overview of the IPSec architecture (4)

Protocol modes – A SA is always of one of the following types:

- *Transport mode* can only be used between end-points of a communication:
  - host $\leftrightarrow$ host, or
  - host $\leftrightarrow$ gateway, if the gateway is a communication end-point (e.g. for network management)
- *Tunnel mode* can be used with arbitrary peers

Overview of the IPSec architecture (5)

The difference between the two modes is that:

- Transport mode just adds a security specific header (+ eventual trailer):

IP header	IPsec header	protected data

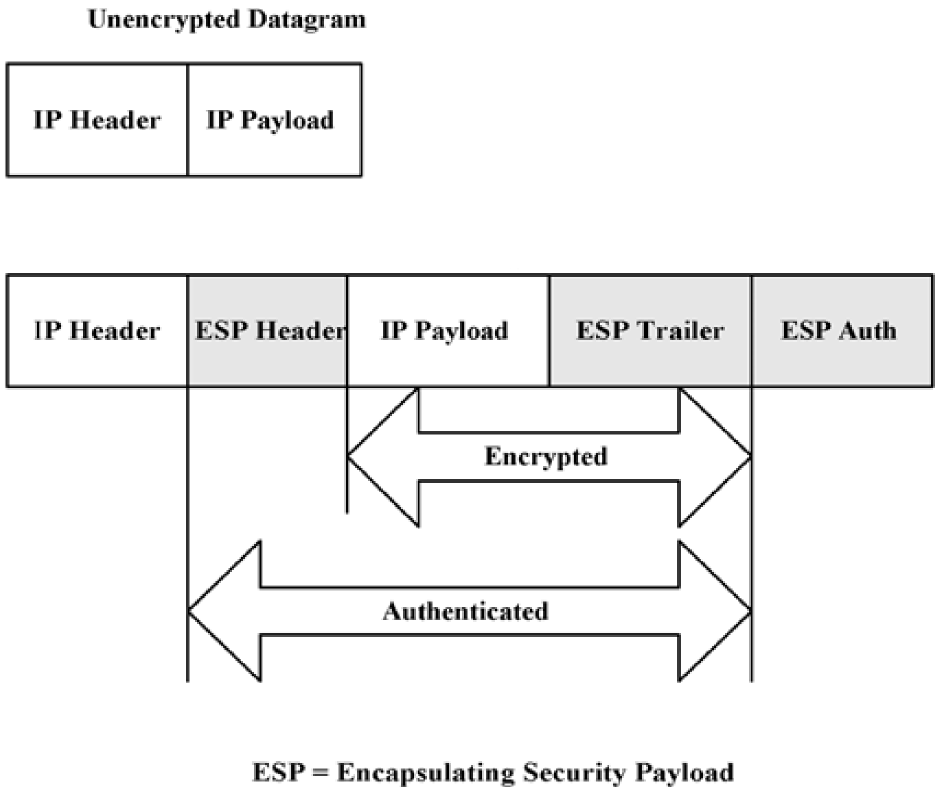
- Tunnel mode encapsulates IP packets:

IP header	IPsec header	IP header	protected data

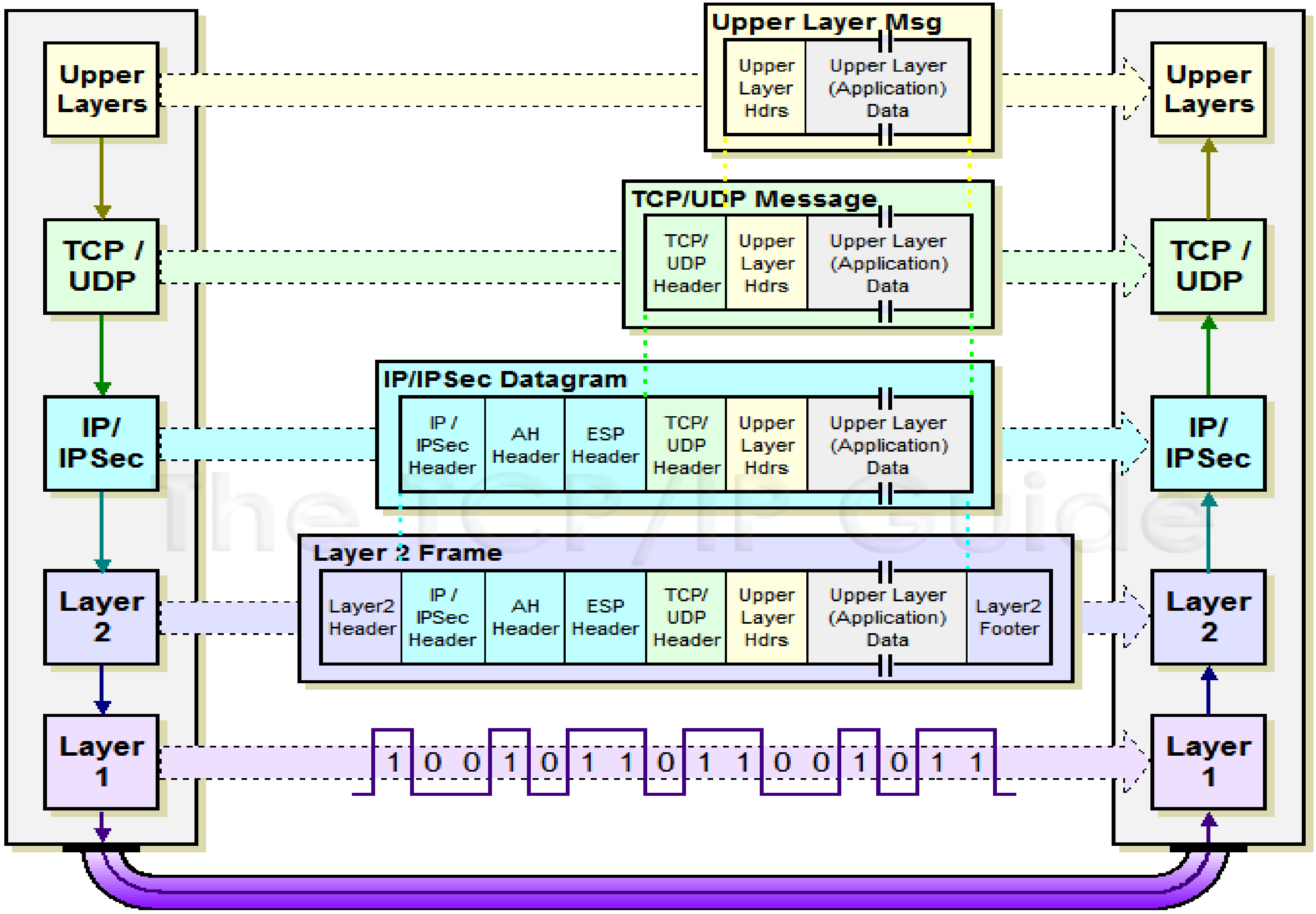
- Encapsulation of IP packets allows for a gateway protecting traffic on behalf of other entities (e.g. hosts of a subnetwork, etc.)

What IPSec mode is shown in the figure?

A. Tunnel mode
✓B. Transport mode

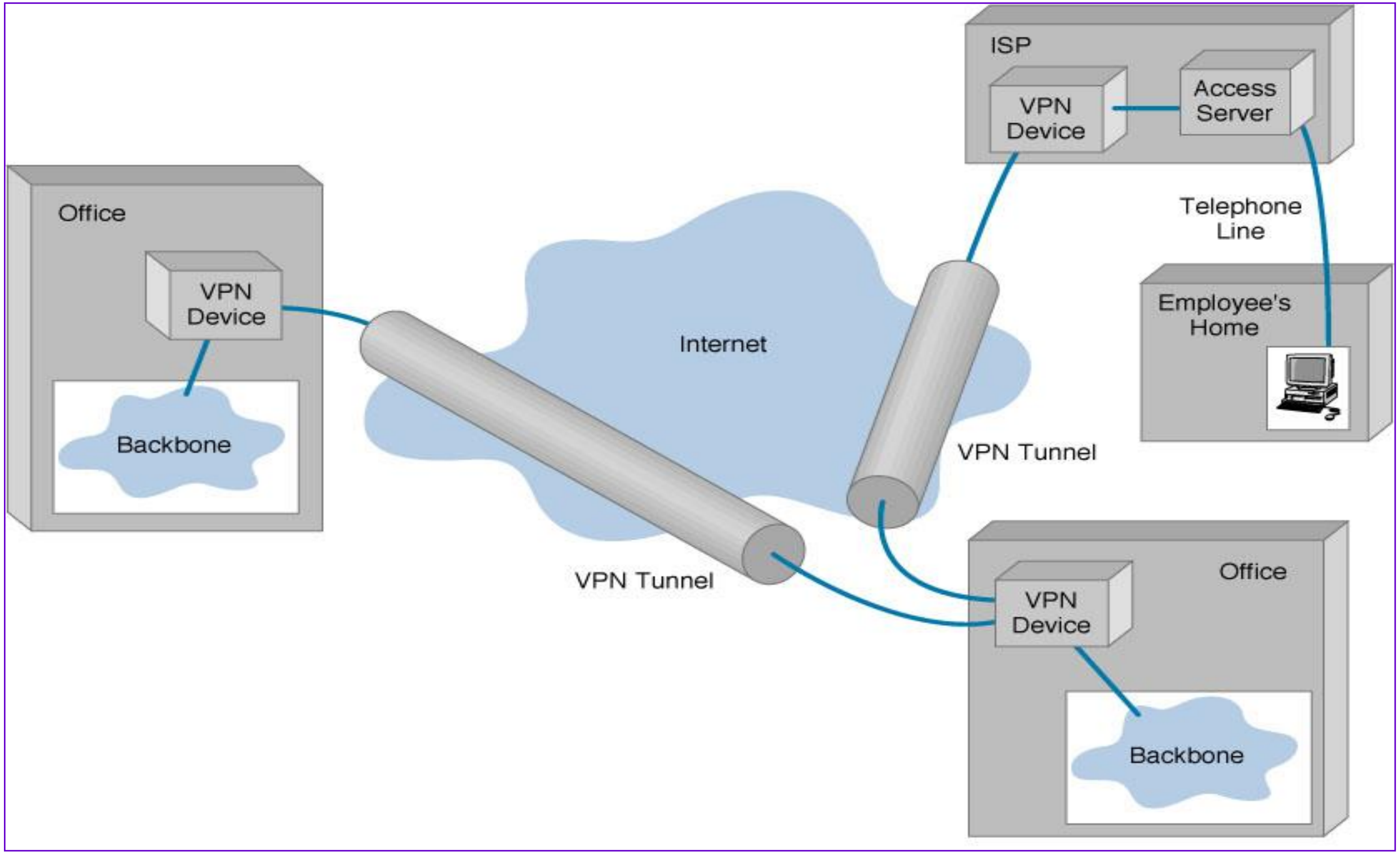


IPSec Transport Mode: IPSec instead of IP header

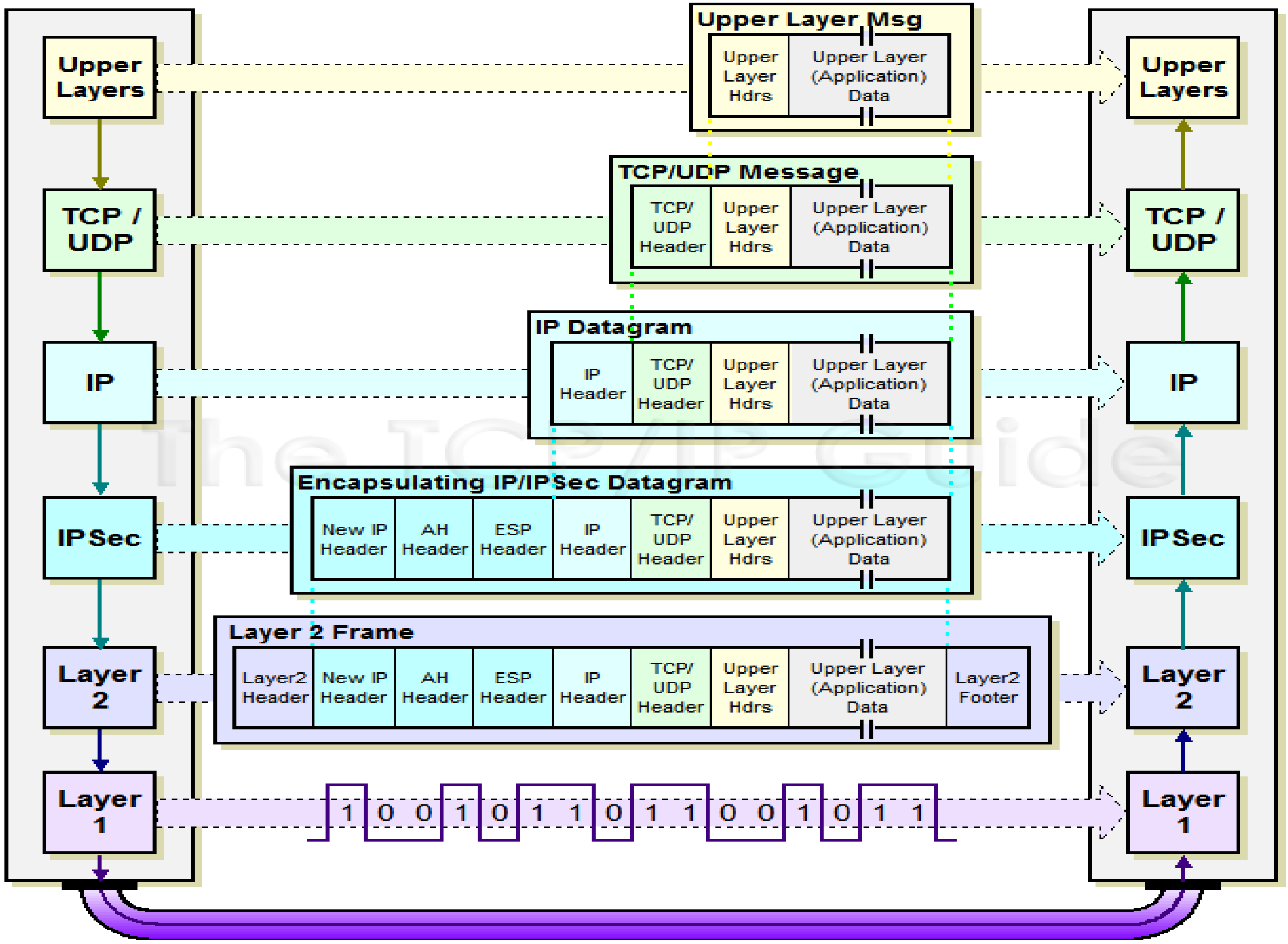


http://www.tcpipguide.com/free/t_IPSecModesTransportandTunnel.htm

IPSec Tunnel Mode



IPSec Tunnel Mode: IPSec header + IP header



http://www.tcpipguide.com/free/t_IPSecModesTransportandTunnel.htm

Transport mode and Tunnel Mode Functionality

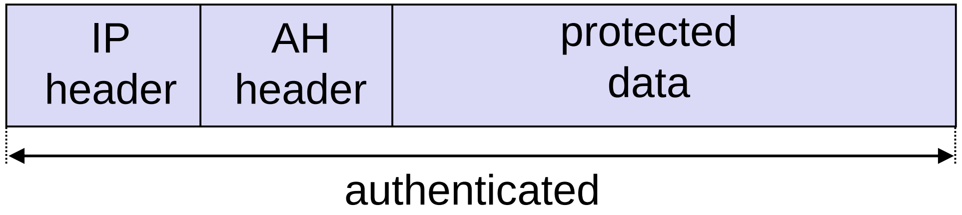
Transport Mode	Tunnel Mode
• Provides protection primarily for upper-layer protocols • Examples include a TCP or UDP segment or an ICMP packet • Typically used for end-to-end communication between two hosts • ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header • AH in transport mode authenticates the IP payload and selected portions of the IP header	• Provides protection to the entire IP packet • Used when one or both ends of a security association (SA) are a security gateway • A number of hosts on networks behind firewalls may engage in secure communications without implementing IPsec • ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet, including the inner IP header • AH in tunnel mode authenticates the entire inner IP packet and selected portions of the outer IP header

QUEEN'S UNIVERSITY BELFAST

Overview of the IPSec architecture (6)

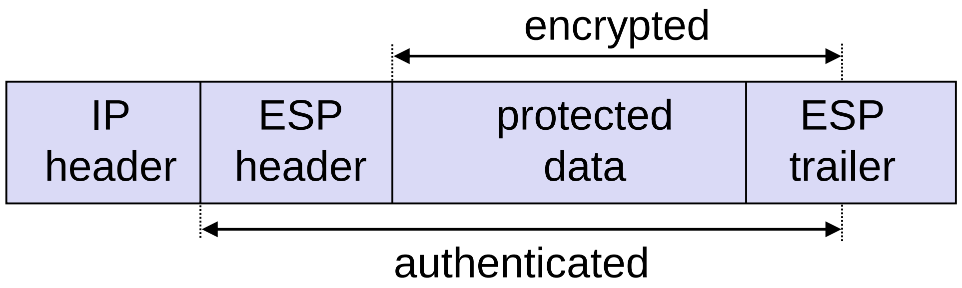
The authentication header (AH):

- Provides data origin authentication and replay protection
- Is realized as a header which is inserted between the IP header and the data to be protected



The encapsulating security payload (ESP):

- Provides data origin authentication, confidentiality and replay protection
- Is realized with a header and a trailer encapsulating the data to be protected



QUEEN'S UNIVERSITY BELFAST

Overview of the IPSec architecture (7)

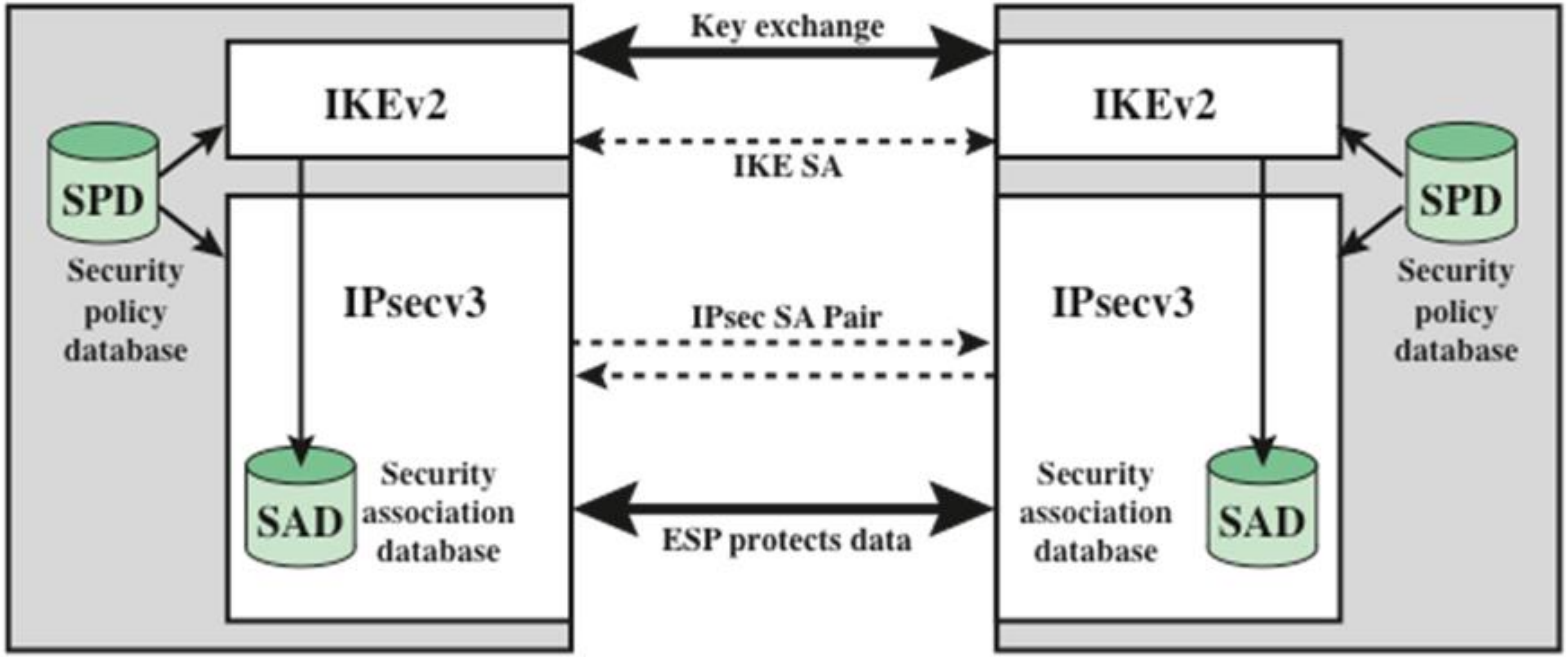
Prior to any packet being protected by IPsec, an SA has to be established between the two "cryptographic endpoints" providing the protection

Setup of security associations is realized with:

- Internet Security Association Key Management Protocol (ISAKMP):
  - Defines generic framework for key authentication, key exchange and negotiation of security association parameters
- Internet Key Exchange (IKE):
  - Defines an authentication and key exchange protocol
  - Is conformant to ISAKMP and may be used for different applications
  - Setup of IPsec SAs between two entities is realized in two phases:
    - Establishment of an IKE SA (defines how to setup IPsec SAs)
    - Setup of IPsec SAs

QUEEN'S UNIVERSITY BELFAST

Overview of the IPSec architecture (8)

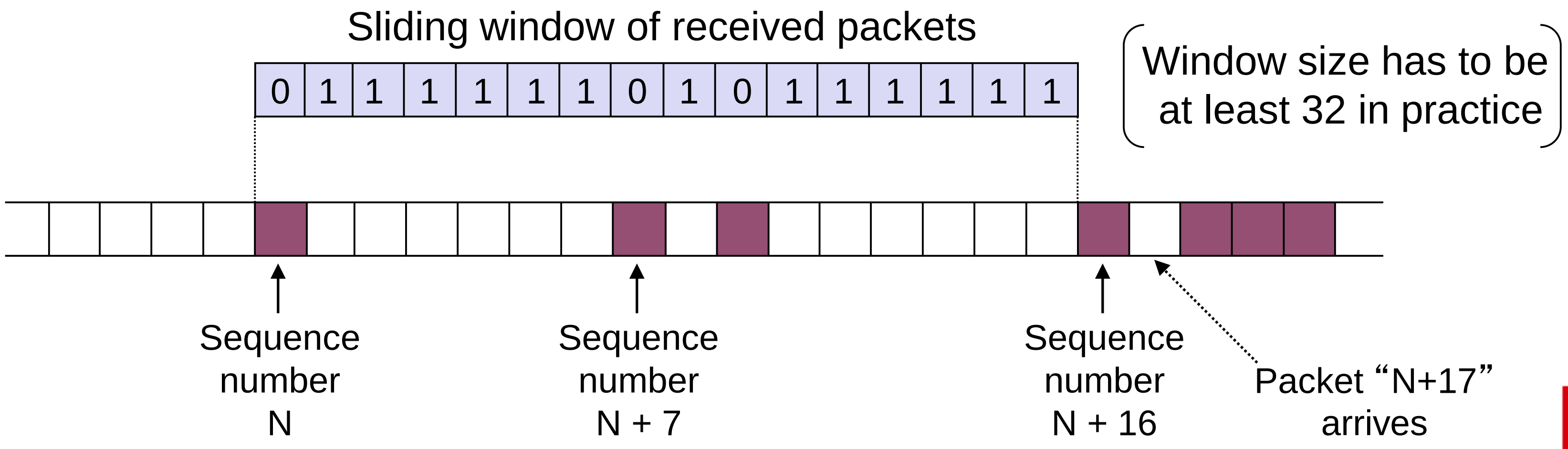


QUEEN'S UNIVERSITY BELFAST

IPSec Replay Protection (1)

Both AH- and ESP-protected IP packets carry a sequence number which realizes a replay protection:

- When setting up an SA this sequence number is initialized to zero
- The sequence number is increased with every IP packet sent
- The sequence number is 32 bits long, a new session key is needed before a wrap-around occurs
- The receiver of an IP packet checks if the sequence number is contained in a window of acceptable numbers



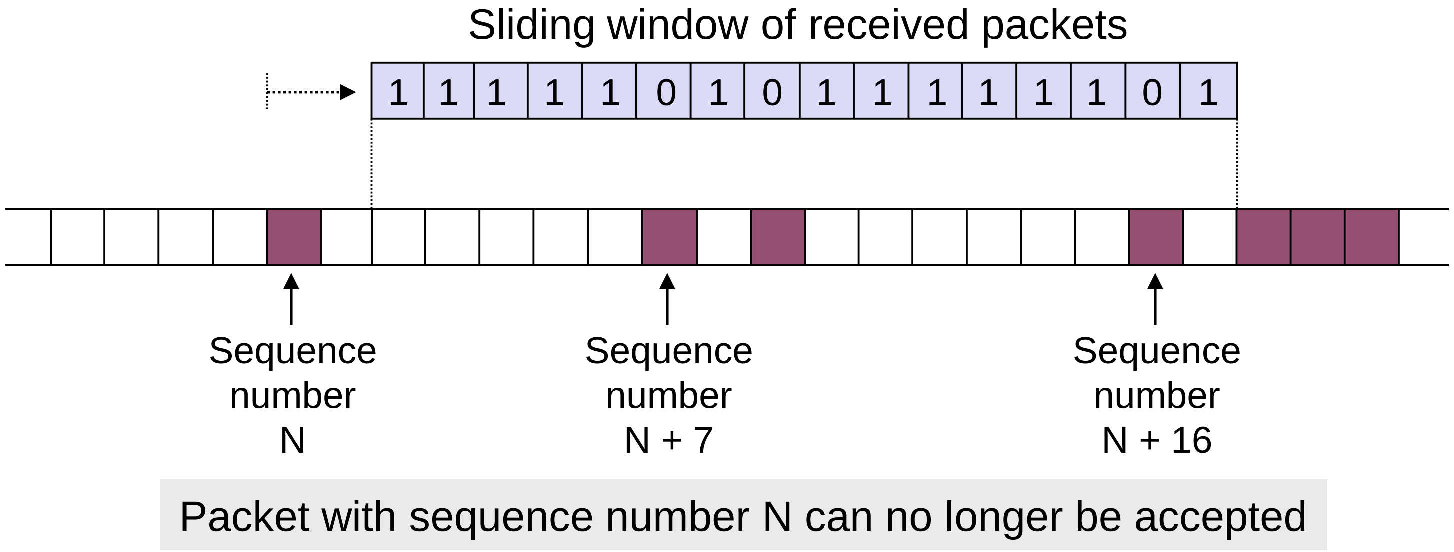
Packet with sequence number N can still be accepted

IPSec Replay Protection (2)

If a received packet has a sequence number which:

- is to the left of the current window $\Rightarrow$ the receiver rejects the packet
- is inside the current window $\Rightarrow$ the receiver accepts the packet
- is to the right of the current window $\Rightarrow$ the receiver accepts the packet and advances the window
- Of course IP packets are only accepted if they pass the authentication verification and the window is never advanced before this verification

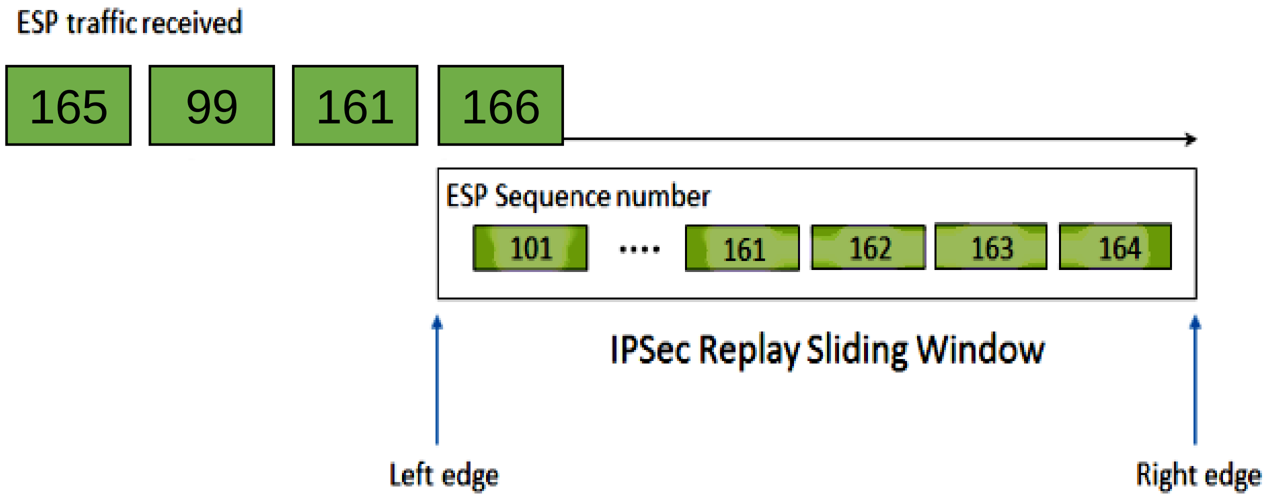
The minimum window size is 32 packets (64 packets is recommended)



QUEEN'S UNIVERSITY BELFAST

Which packets will be rejected for replay protection?

A. All
B. 99 and 161
C. None
D. 99 and 165



IPSec Implementation Alternatives: Host Impl.

- Advantages of IPsec implementation in end systems:
  - Provision of end-to-end security services
  - Provision of security services on a per-flow basis
  - Ability to implement all modes of IPsec
- Two main integration alternatives:

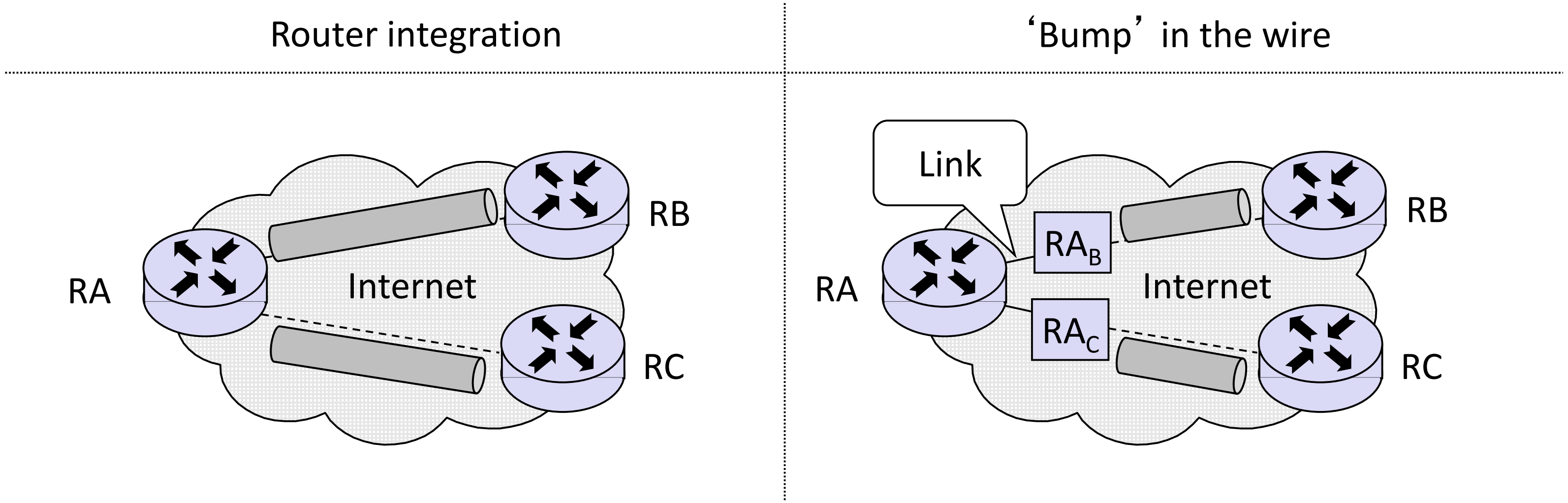
OS integrated	"Bump" in the stack
	Application
Application	Transport
Transport	Network
Network + IPsec	IPsec
Data Link	Data Link

True OS integration is the method of choice, as it avoids duplication of functionality

If the OS can not be modified, IPsec is inserted above the data link driver

IPSec Implementation Alternatives: Router Impl.

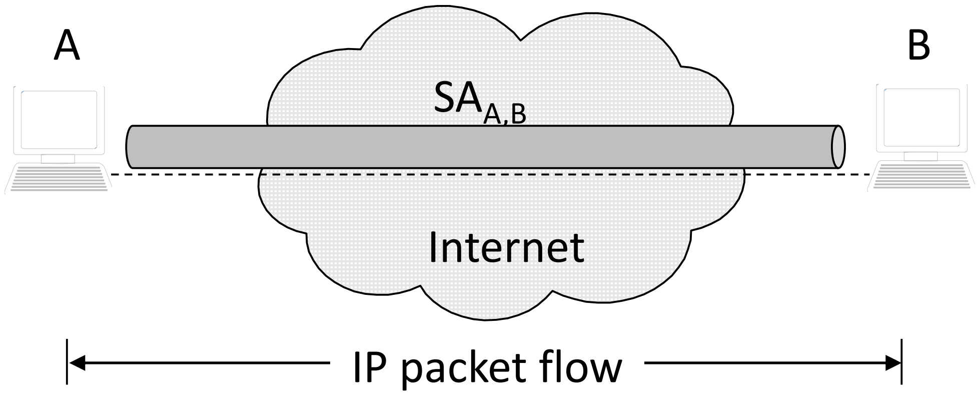
- Advantages of IPsec implementation in routers:
  - Ability to secure IP packets flowing between two networks over a public network such as the Internet:
    - Allows to create *virtual private networks (VPNs)*
    - No need to integrate IPsec in every end system
  - Ability to authenticate and authorize IP traffic coming in from remote users
- Two main implementation alternatives:



QUEEN'S UNIVERSITY BELFAST

When to use which IPSEC mode? (1)

- Transport mode is used when the "cryptographic endpoints" are also the "communication endpoints" of the secured IP packets
  - Cryptographic endpoints: the entities that generate / process an IPsec header (AH or ESP)
  - Communication endpoints: source and destination of an IP packet

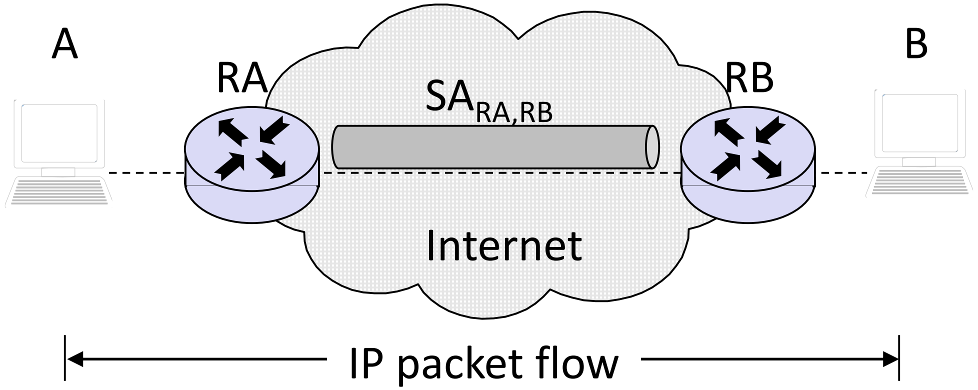


- In most cases, communication endpoints are hosts (workstations, servers)

When to use which IPSEC mode? (2)

Tunnel mode is used when at least one "cryptographic endpoint" is not a "communication endpoint" of the secured IP packets

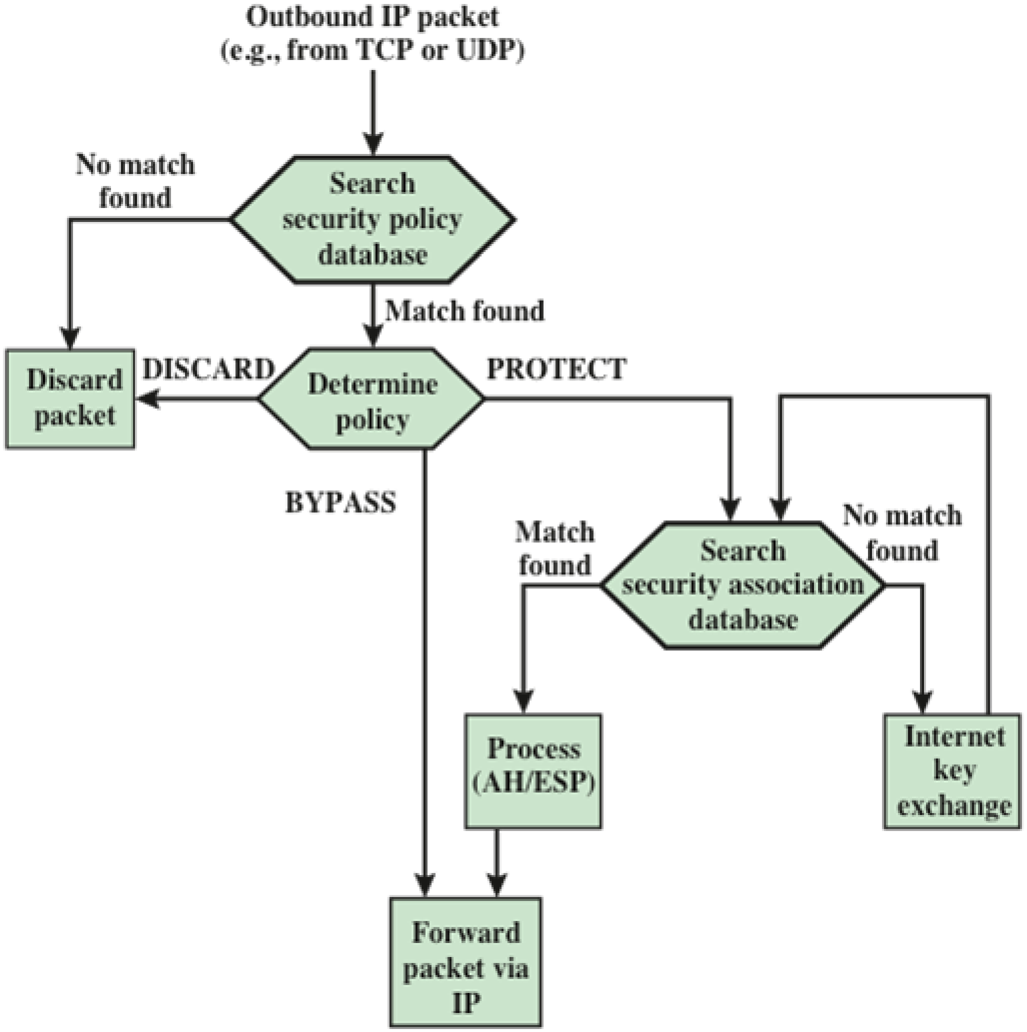
- This allows for gateways securing IP traffic on behalf of other entities



Packet structure

IP Header	IPsec Header	IP Header	Protected Data
Src = RA Dst = RB		Src = A Dst = B	

Basic scheme of IPSec Processing: Outgoing Packets



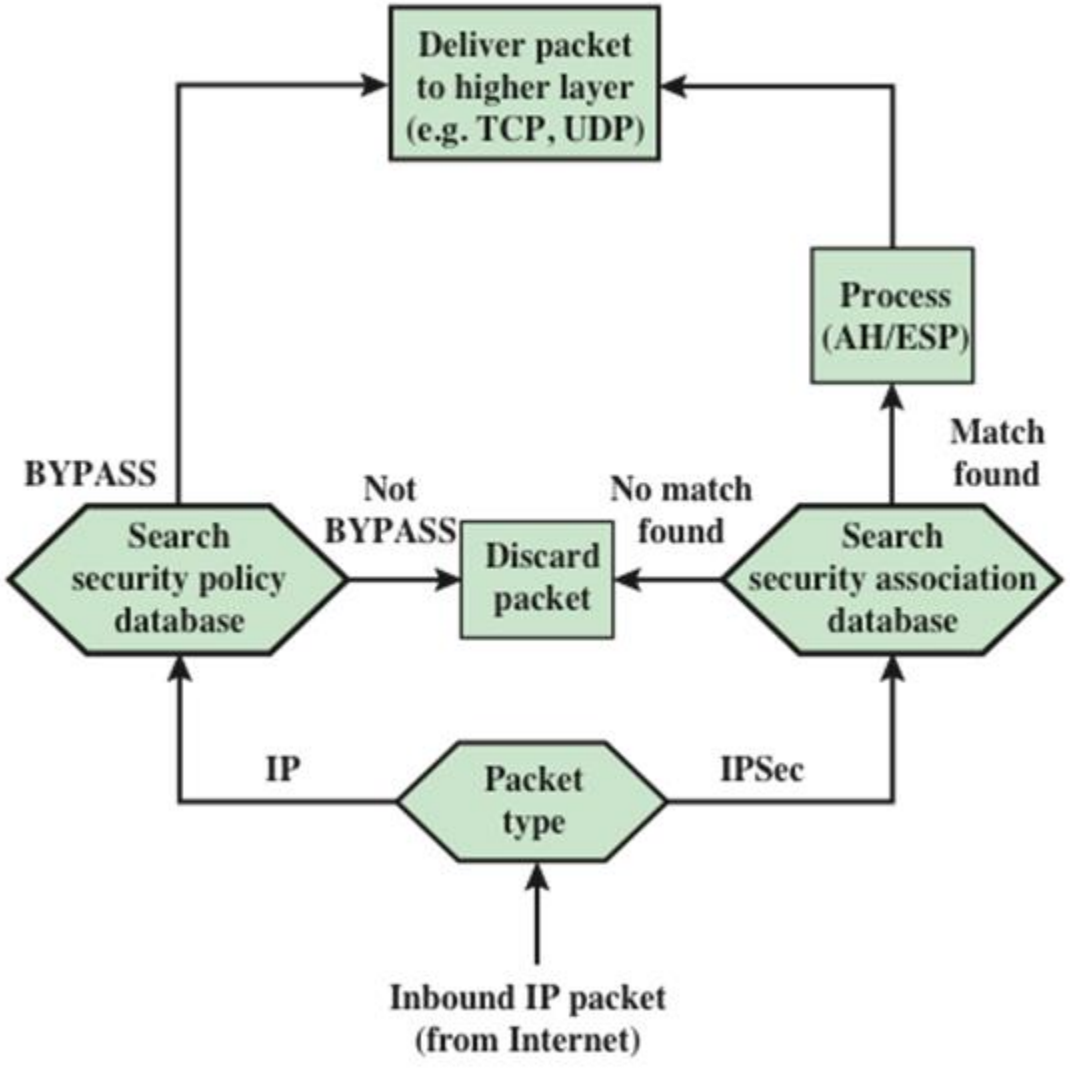
Background

Basic scheme of IPSec Processing: Outgoing Packets

- Consider, the IP layer of one node (host / gateway) is told to send an IP packet to another node (host / gateway)
- In order to support IPsec it has to perform the following steps:
  1. Determine if and how the outgoing packet needs to be secured:
     - This is realized by performing a lookup in the SPD
     - If the policy specifies "discard" then drop the packet $\Rightarrow$ done
     - If the packet does not need to be secured, then send it $\Rightarrow$ done
  2. Determine which SA should be applied to the packet:
     - If there is not yet an appropriate SA established with the corresponding node, then ask the key management demon to perform an IKE
  3. Look up the determined (and eventually freshly created) SA in the SADB
  4. Perform the security transform determined by the SA by using the algorithm, its' parameters and the key as specified in the SA
     - This results in the construction of an AH or an ESP header
     - Eventually also a new (outer) IP header will be created (tunnel mode)
  5. Send the resulting IP packet $\Rightarrow$ done

QUEEN'S UNIVERSITY BELFAST

Basic scheme of IPSec Processing: Incoming Packets



Background

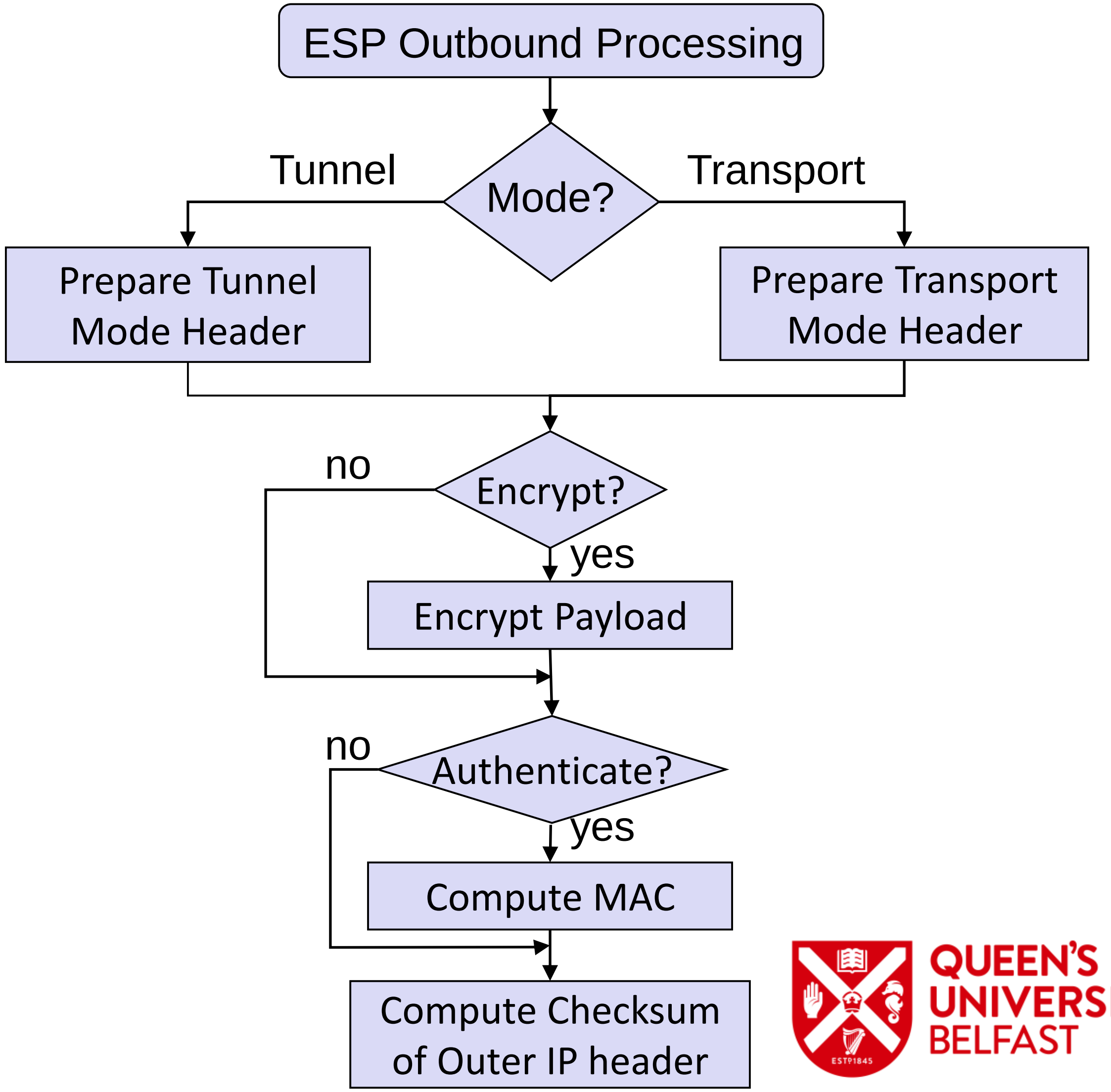
Basic scheme of IPSec Processing: Incoming Packets

- Consider now, the IP layer of one node (host / gateway) receives an IP packet from another node (host / gateway)
- In order to support IPsec it has to perform the following steps:
  1. Determine if the packet contains an IPsec header this entity is supposed to process:
     - If there is such an IPsec header then look up the SA in the SADB which is specified by the SPI of the IPsec header and perform the appropriate IPsec processing
     - If the SA referenced by the SPI does not (yet) exist, drop the packet
  2. Determine if and how the packet should have been protected:
     - This is again realized by performing a lookup in the SPD, with the lookup being performed by evaluating the inner IP header in case of tunneled packets
     - If the policy specifies "discard" then drop the packet
     - If the protection of the packet did not match the policy, drop the packet
     - If the packet had been properly secured, then deliver it to the appropriate protocol entity (network / transport layer)

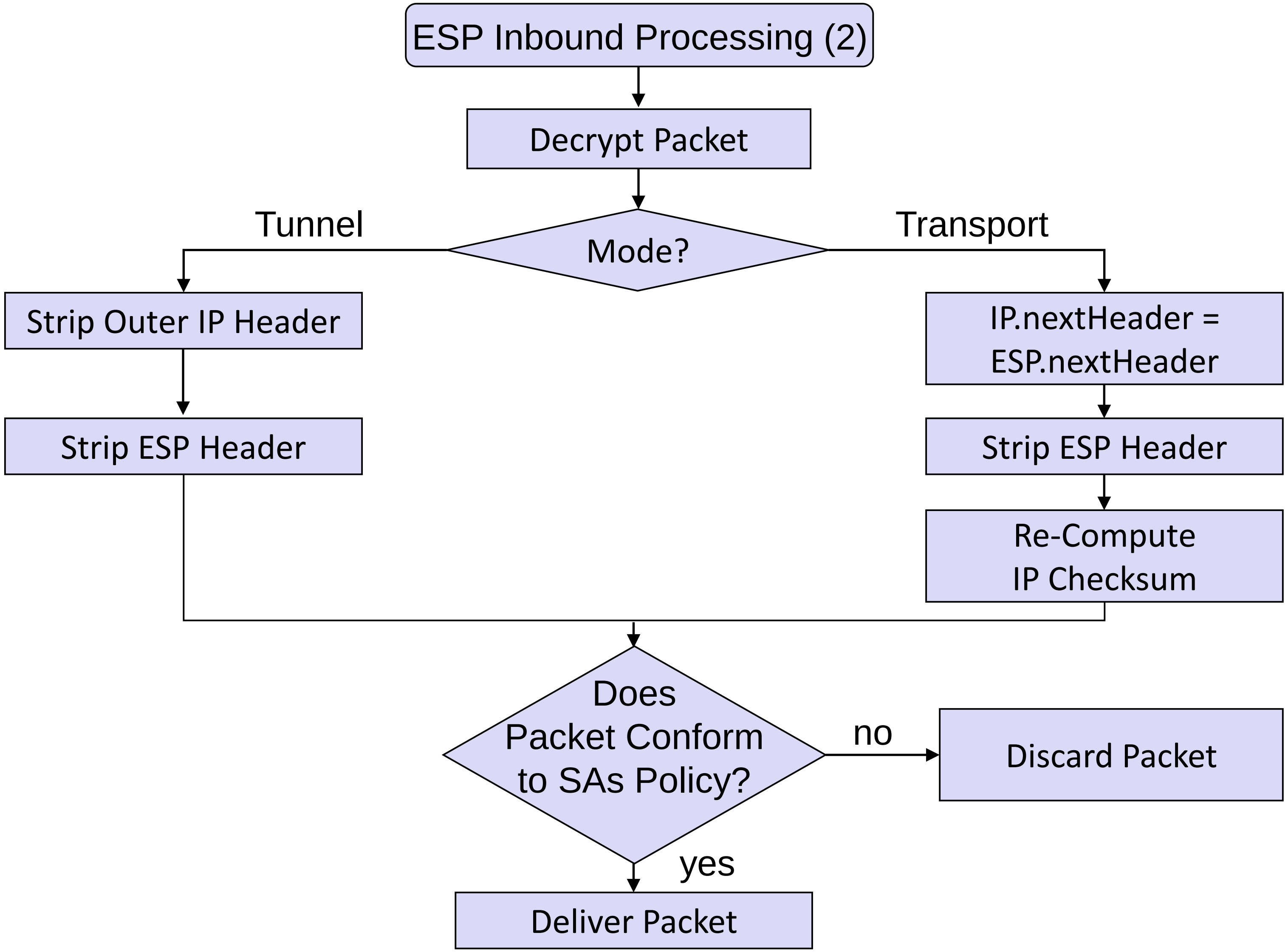
QUEEN'S UNIVERSITY BELFAST

The Encapsulating Security Payload (1)

- ESP constitutes a generic security protocol that provides to IP packets replay protection and one or both of the following security services:
  - Confidentiality, by encrypting encapsulated packets or just their payload
  - Data origin authentication, by creating and adding MACs to packets



The Encapsulating Security Payload (2)

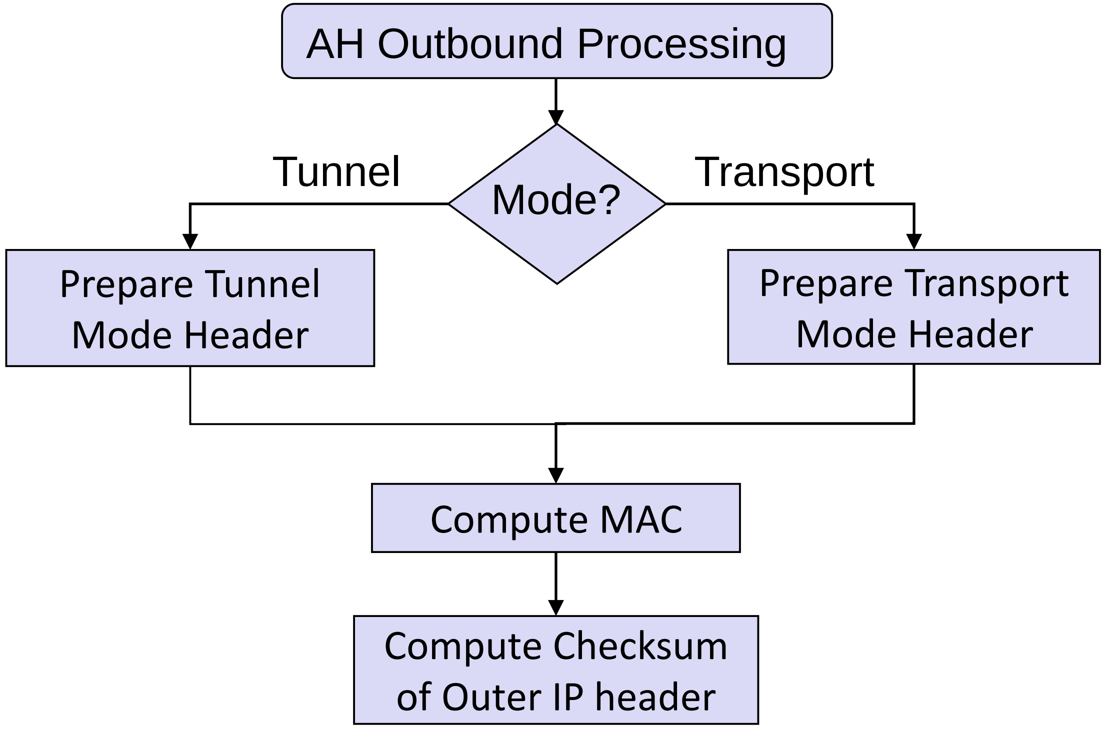


QUEEN'S UNIVERSITY BELFAST

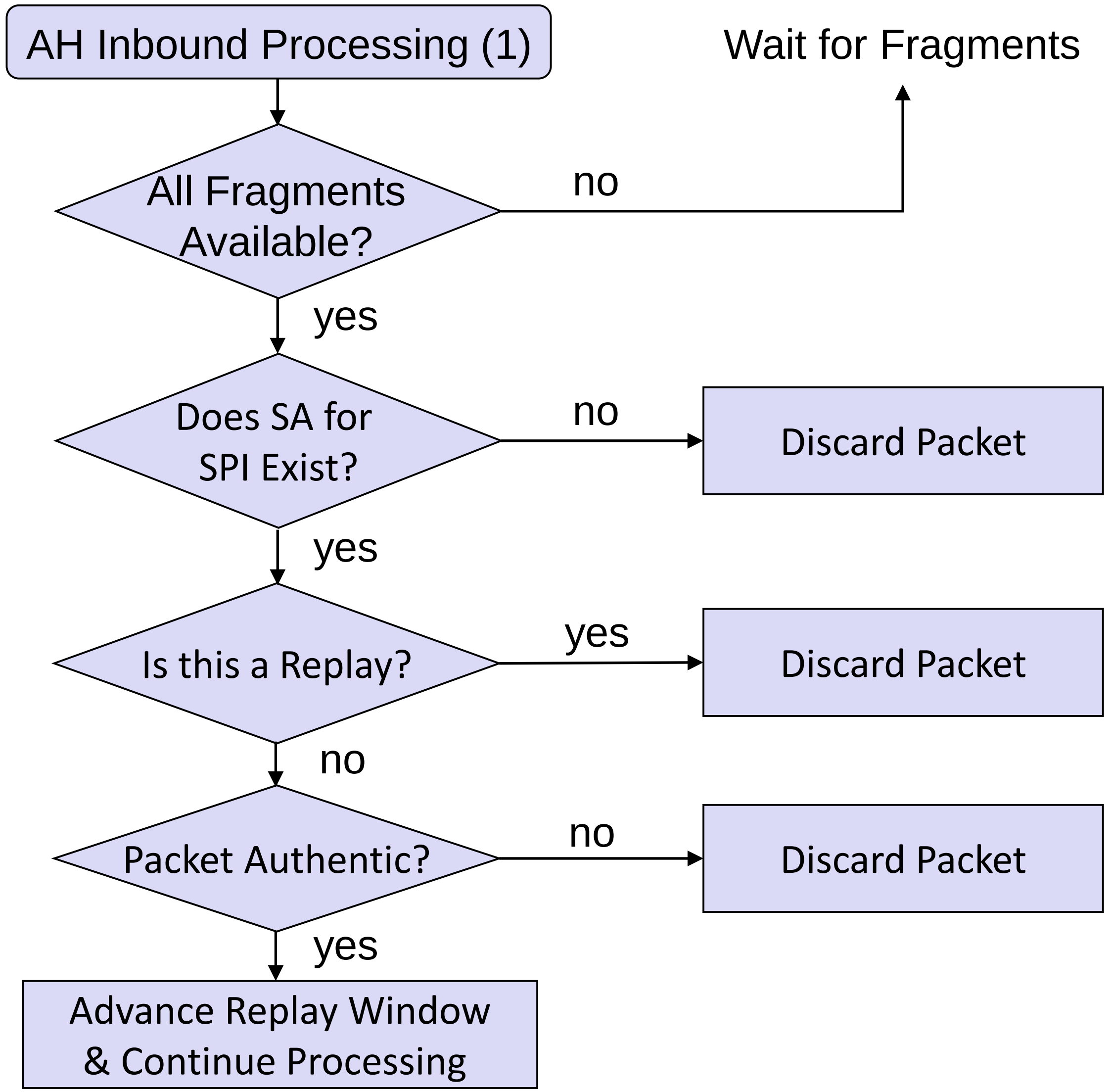
The Authentication Header (1)

AH constitutes a generic security protocol that provides to IP packets:

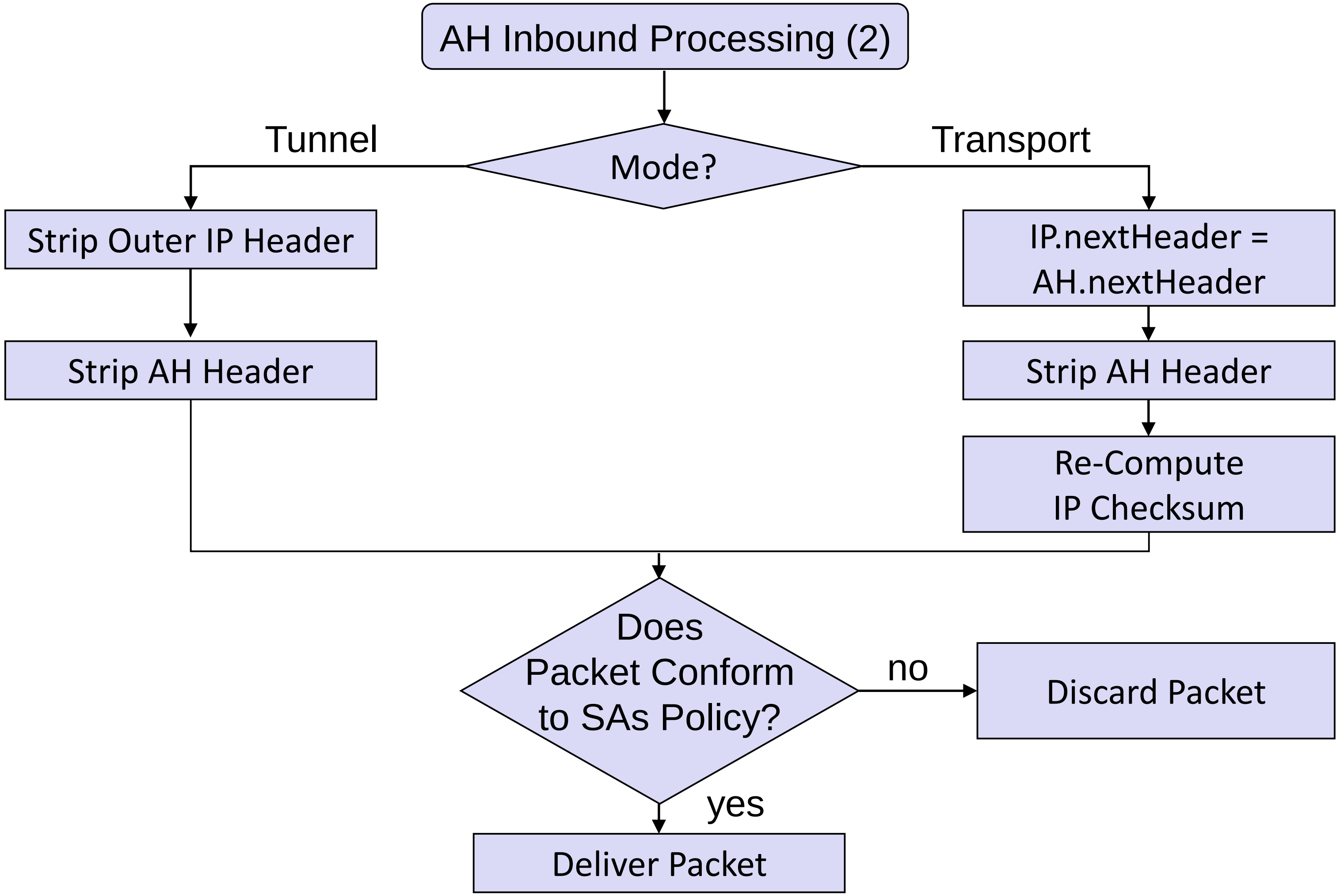
- Replay protection
- Data origin authentication, by creating and adding MACs to packets



The Authentication Header (2)



The Authentication Header (3)



Issues with IPSec

Compression:

- If encryption is used, then the resulting IP packets can not be compressed in the link layer, e.g. when connecting to an ISP via Modem
- Therefore, the *IP payload compression protocol (PCP)* has been defined
- PCP can be used with IPsec:
    - IPsec policy definition allows to specify PCP
    - IKE SA negotiation allows to include PCP in proposals

Interoperability problems of end-to-end security with header processing in intermediate nodes:

- Interoperability with firewalls:
    - End-to-end encryption conflicts with the firewalls' need to inspect upper layer protocol headers in IP packets
- Interoperability with network address translation (NAT):
    - Encrypted packets neither permit analysis nor change of addresses
    - Authenticated packets will be discarded if source or destination address is changed

Summary

- IPsec is IETF' s security architecture for the Internet Protocol
- It provides the following security services to IP packets:
    - Data origin authentication
    - Replay protection
    - Confidentiality
- It can be realized in end systems or intermediate systems:
    - End system implementation: OS integrated or "bump in the stack"
    - Gateway implementation: Router integrated or "bump in the wire"
- Two fundamental security protocols have been defined:
    - Authentication header (AH)
    - Encapsulating security payload (ESP)
- SA negotiation and key management is realized with:
    - Internet security association key management protocol (ISAKMP)
    - Internet key exchange (IKE)

QUEEN'S UNIVERSITY BELFAST

Summary

- IPSec
  - Security Objectives
  - Security Association, Security Policy Definition, SA Database
  - Transport/Tunnel Mode
  - Authentication Header/Encapsulating Security Payload
  - Issues with IPSec

Questions?

Next Session: Thursday, 21 February 2019
AAA/Firewalls

QUEEN'S UNIVERSITY BELFAST