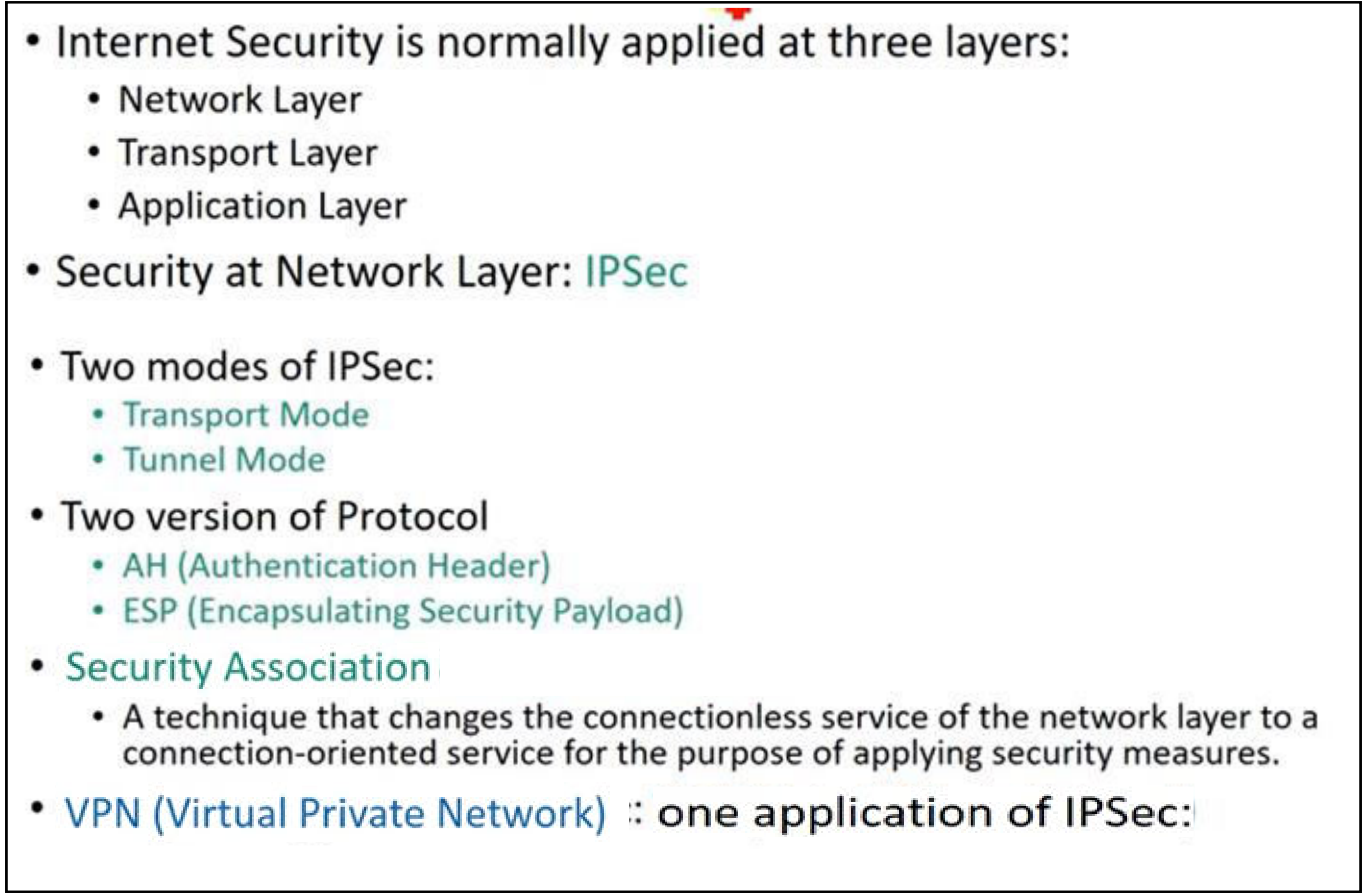
CSE 4215

Chapter 4

Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec)

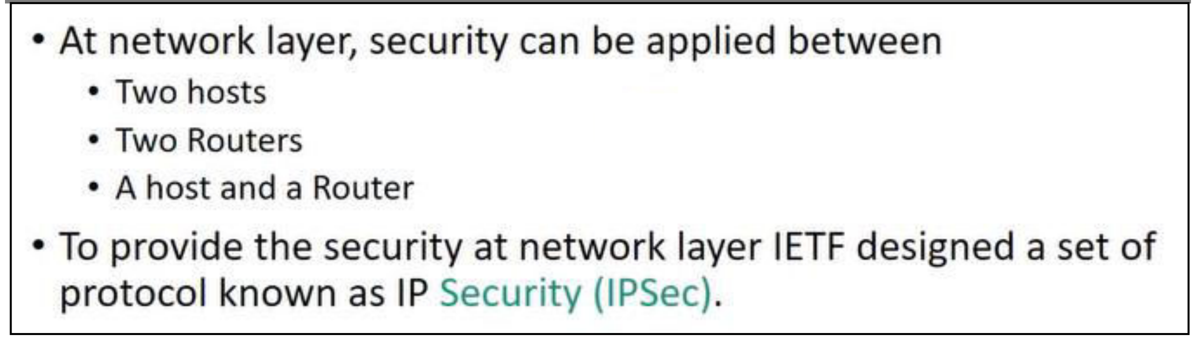
Introduction



- Internet Security is normally applied at three layers:
  - Network Layer
  - Transport Layer
  - Application Layer
- Security at Network Layer: IPSec
- Two modes of IPSec:
  - Transport Mode
  - Tunnel Mode
- Two version of Protocol
  - AH (Authentication Header)
  - ESP (Encapsulating Security Payload)
- Security Association
  - A technique that changes the connectionless service of the network layer to a connection-oriented service for the purpose of applying security measures.
- VPN (Virtual Private Network) : one application of IPSec:

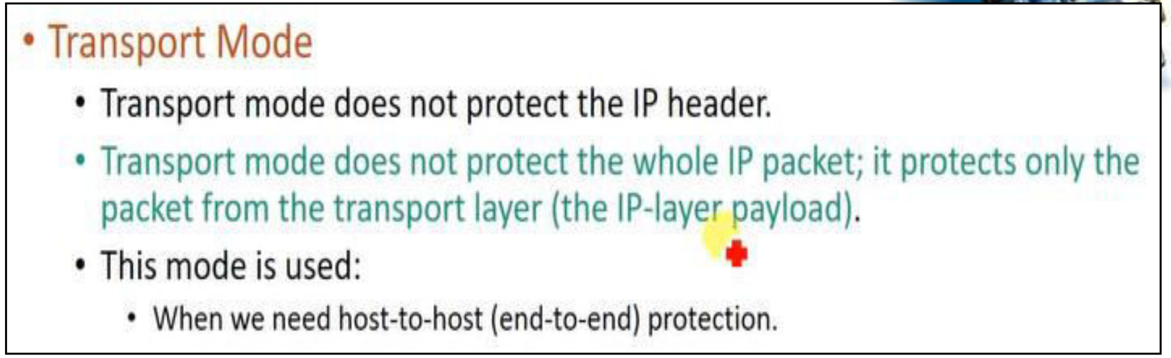
Internet Protocol Security (IPSec)

Network Security Layer

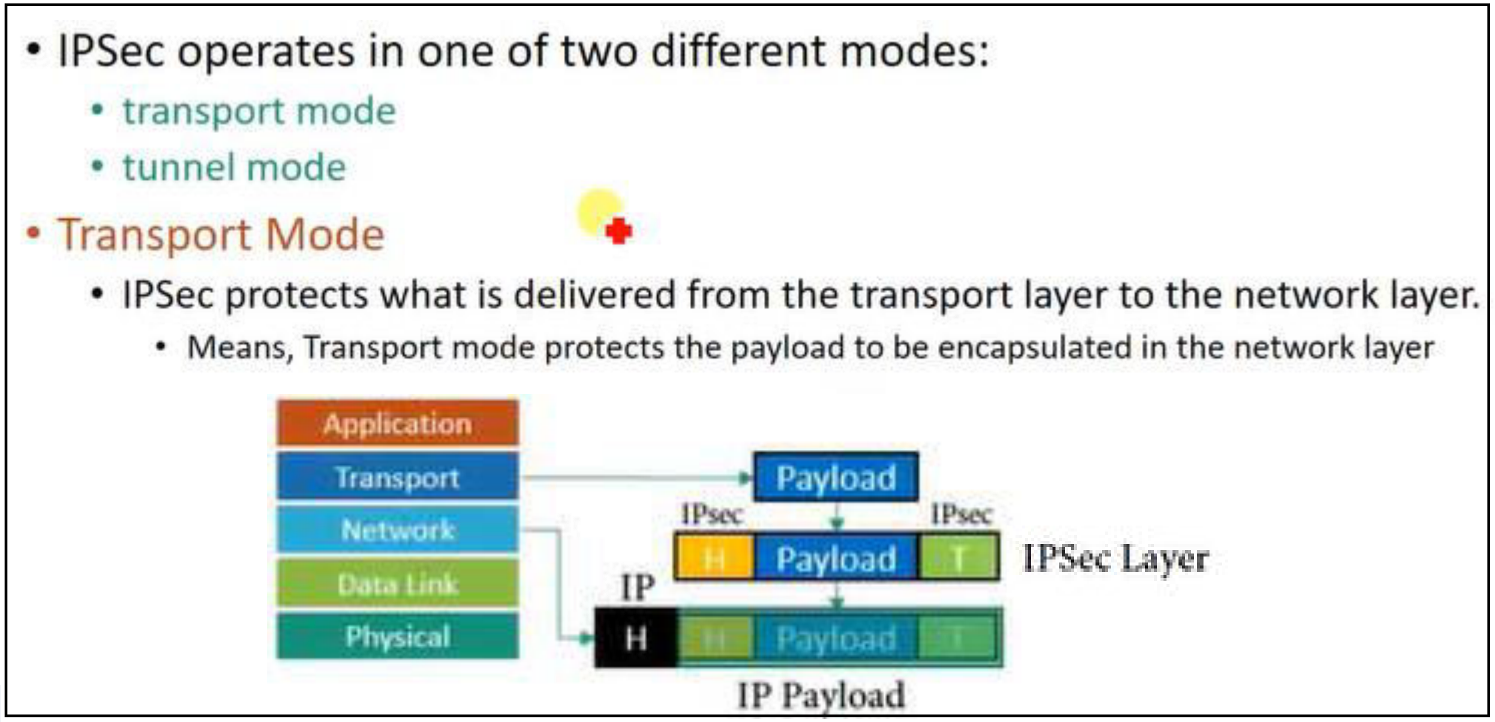


- At network layer, security can be applied between
  - Two hosts
  - Two Routers
  - A host and a Router
- To provide the security at network layer IETF designed a set of protocol known as IP Security (IPSec).

* **IETF**: Internet Engineering Task Force



- Transport Mode
  - Transport mode does not protect the IP header.
  - Transport mode does not protect the whole IP packet; it protects only the packet from the transport layer (the IP-layer payload).
  - This mode is used:
    - When we need host-to-host (end-to-end) protection.

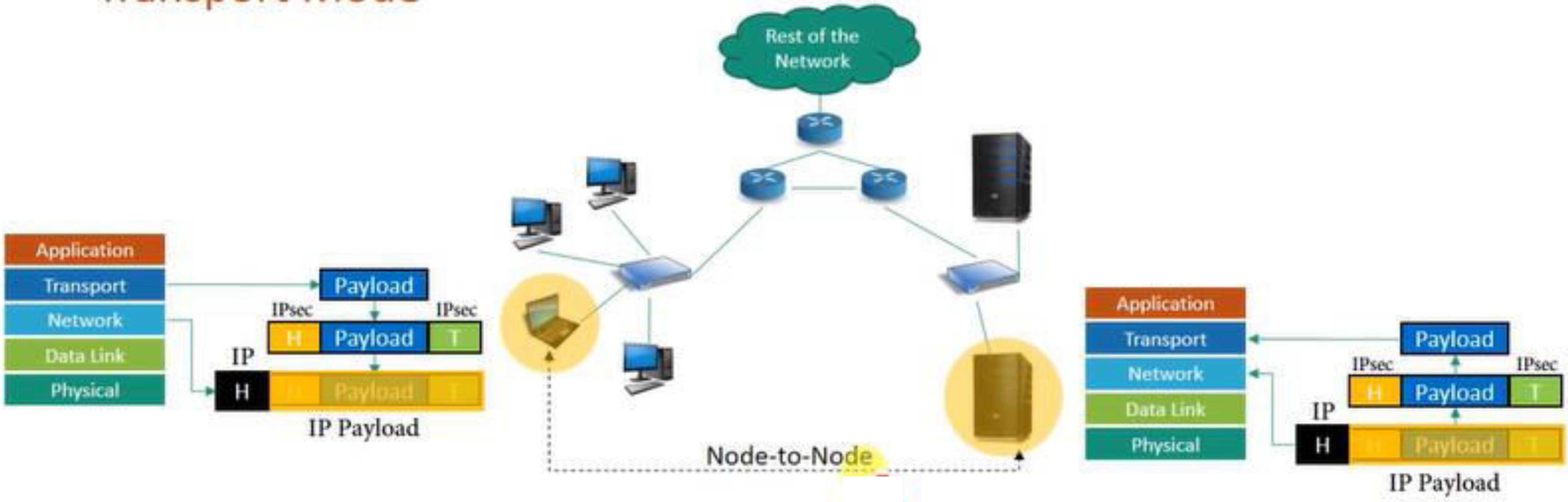


- IPSec operates in one of two different modes:
  - transport mode
  - tunnel mode
- Transport Mode
  - IPSec protects what is delivered from the transport layer to the network layer.
    - Means, Transport mode protects the payload to be encapsulated in the network layer

Internet Protocol Security (IPSec)

Example

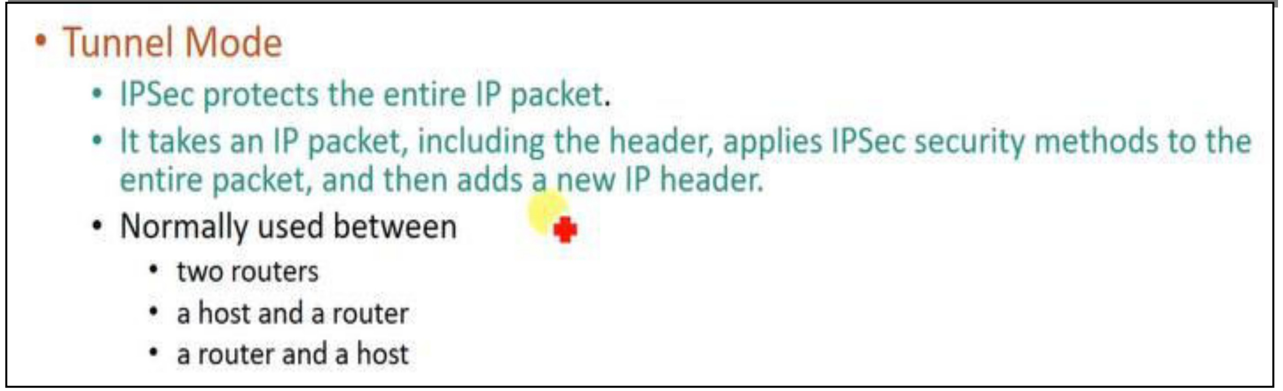
- Transport Mode



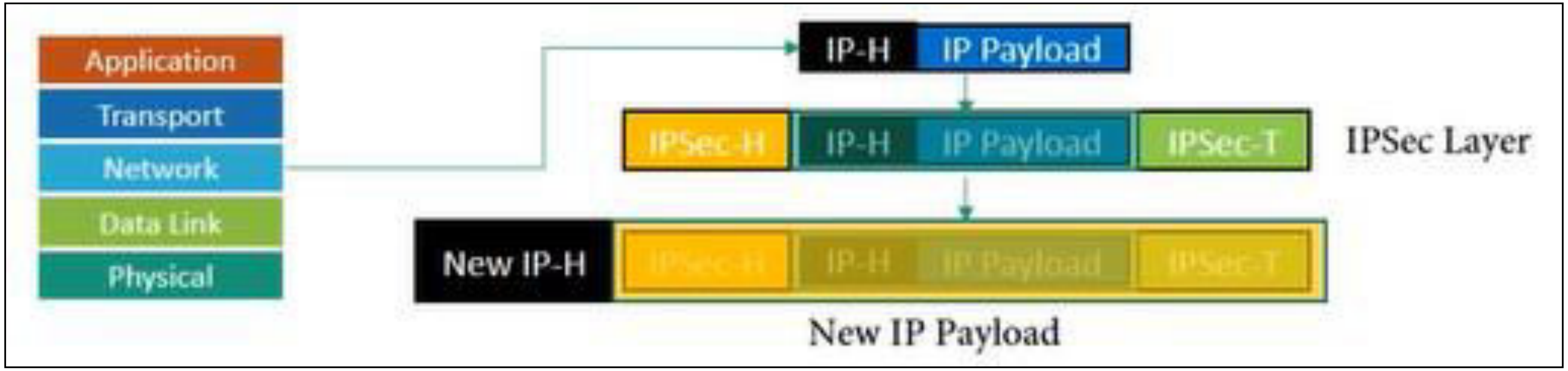
Here two nodes wants to communicate, whatever the route of data transfer, there is a logical connection between these two nodes. The IPSec layer exists between Transport and Network layer.

Internet Protocol Security (IPSec)

Tunnel Mode



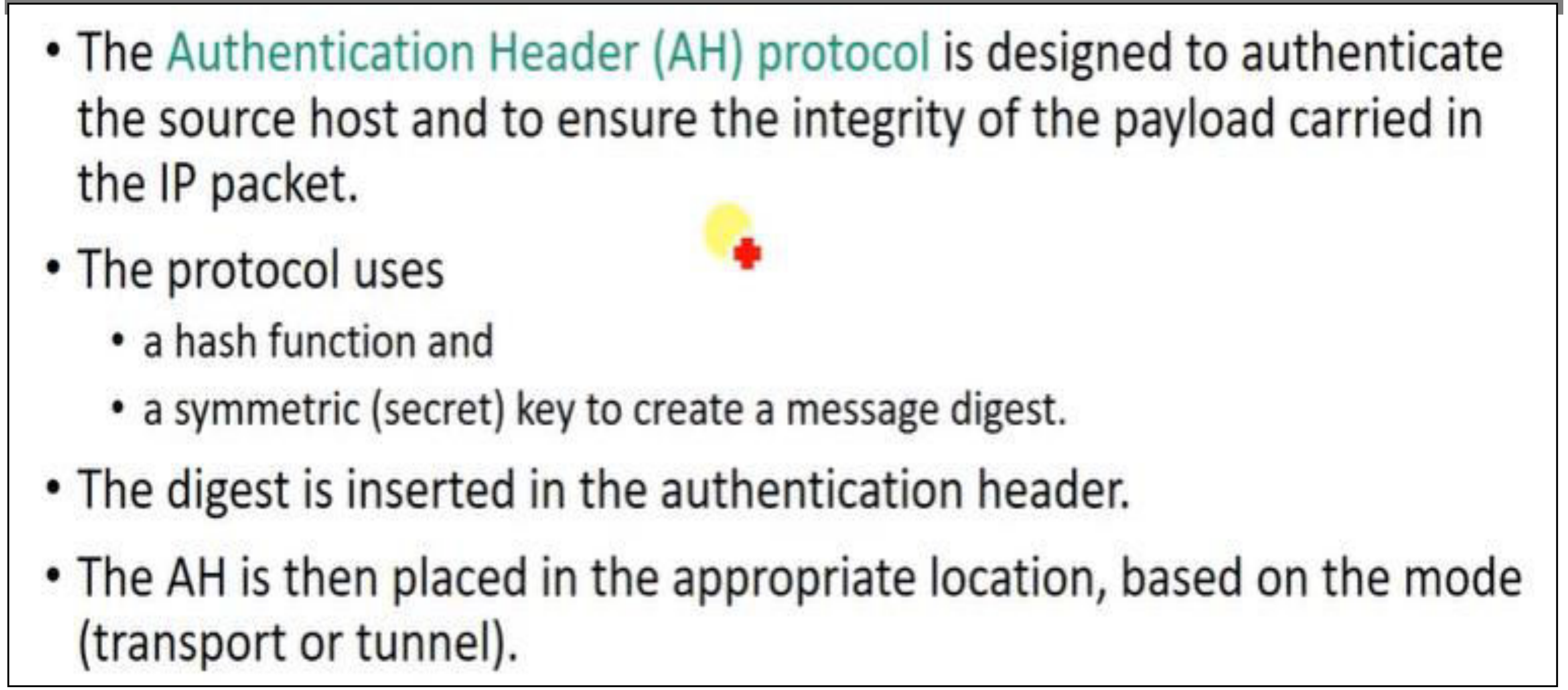
- Tunnel Mode
  - IPSec protects the entire IP packet.
  - It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header.
  - Normally used between
    - two routers
    - a host and a router
    - a router and a host



Here IPSec layer is the part of Network layer

Internet Protocol Security (IPSec)

Authentication Header Protocol

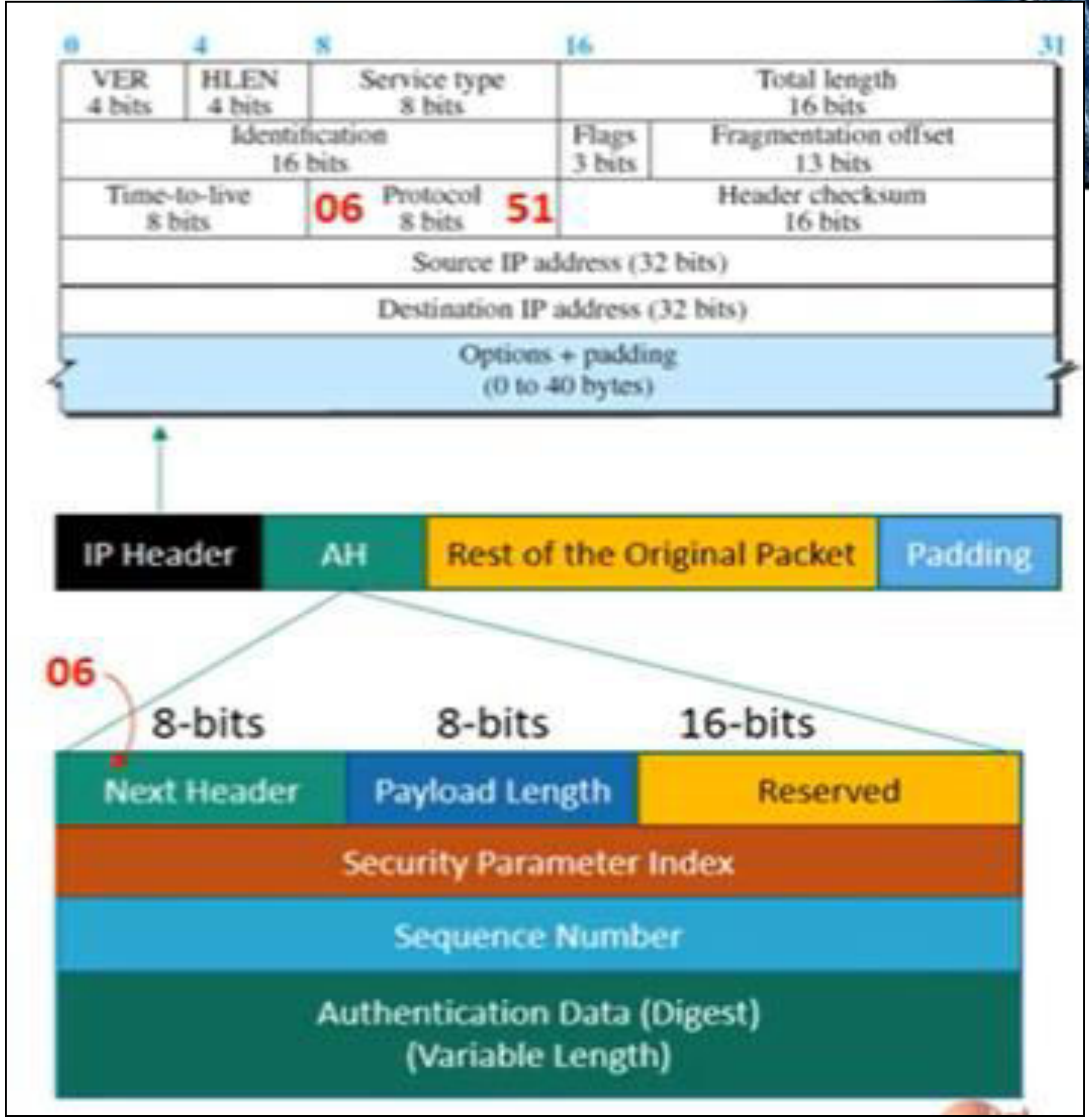


- The Authentication Header (AH) protocol is designed to authenticate the source host and to ensure the integrity of the payload carried in the IP packet.
- The protocol uses
  - a hash function and
  - a symmetric (secret) key to create a message digest.
- The digest is inserted in the authentication header.
- The AH is then placed in the appropriate location, based on the mode (transport or tunnel).

Internet Protocol Security (IPSec)

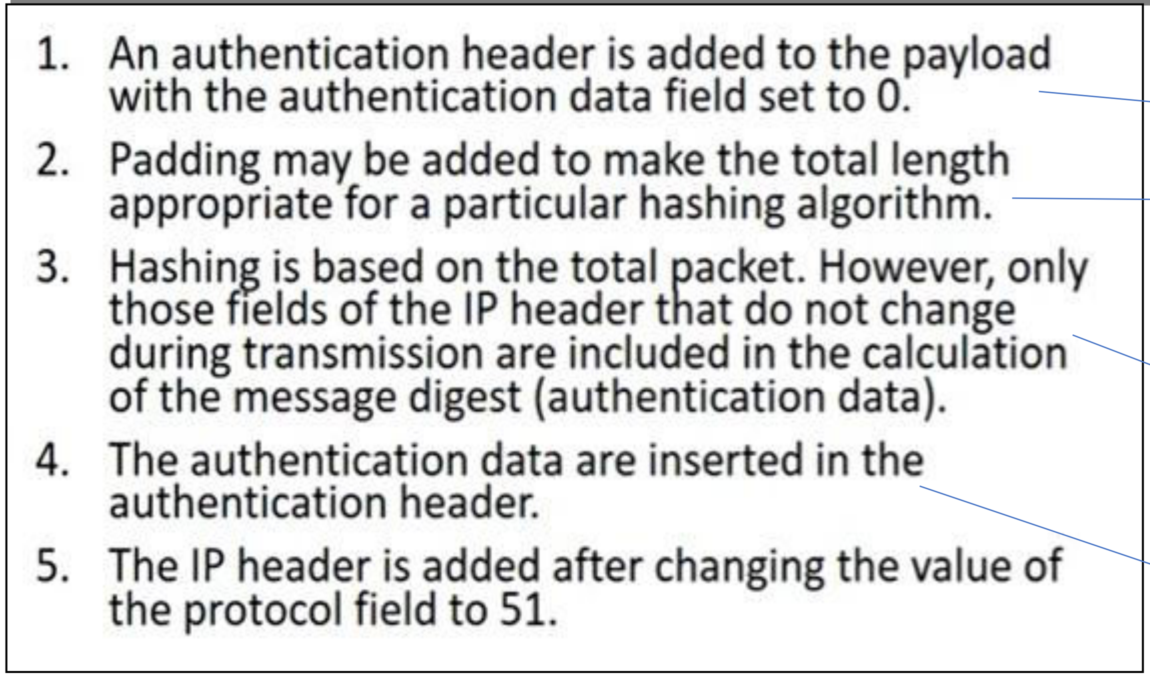
Authentication Header Protocol

- Figure shows the fields and the position of the authentication header in transport mode.
    - Next Header. The 8-bit next header field defines the type of payload carried by the IP datagram (such as TCP, UDP, ICMP, or OSPF).
    - Payload Length. It defines the length of the authentication header in 4-byte multiples.
    - Security Parameter Index. The 32-bit SPI field plays the role of a virtual circuit identifier and is the same for all packets sent during a connection called a *Security Association* (discussed later).
    - Sequence Number. A 32-bit sequence number provides ordering information for a sequence of datagrams.
    - Authentication Data. Finally, the authentication data field is the result of applying a hash function to the entire IP datagram except for the fields that are changed during transit (e.g., time-to-live).
- The AH protocol provides source authentication and data integrity, but not privacy.

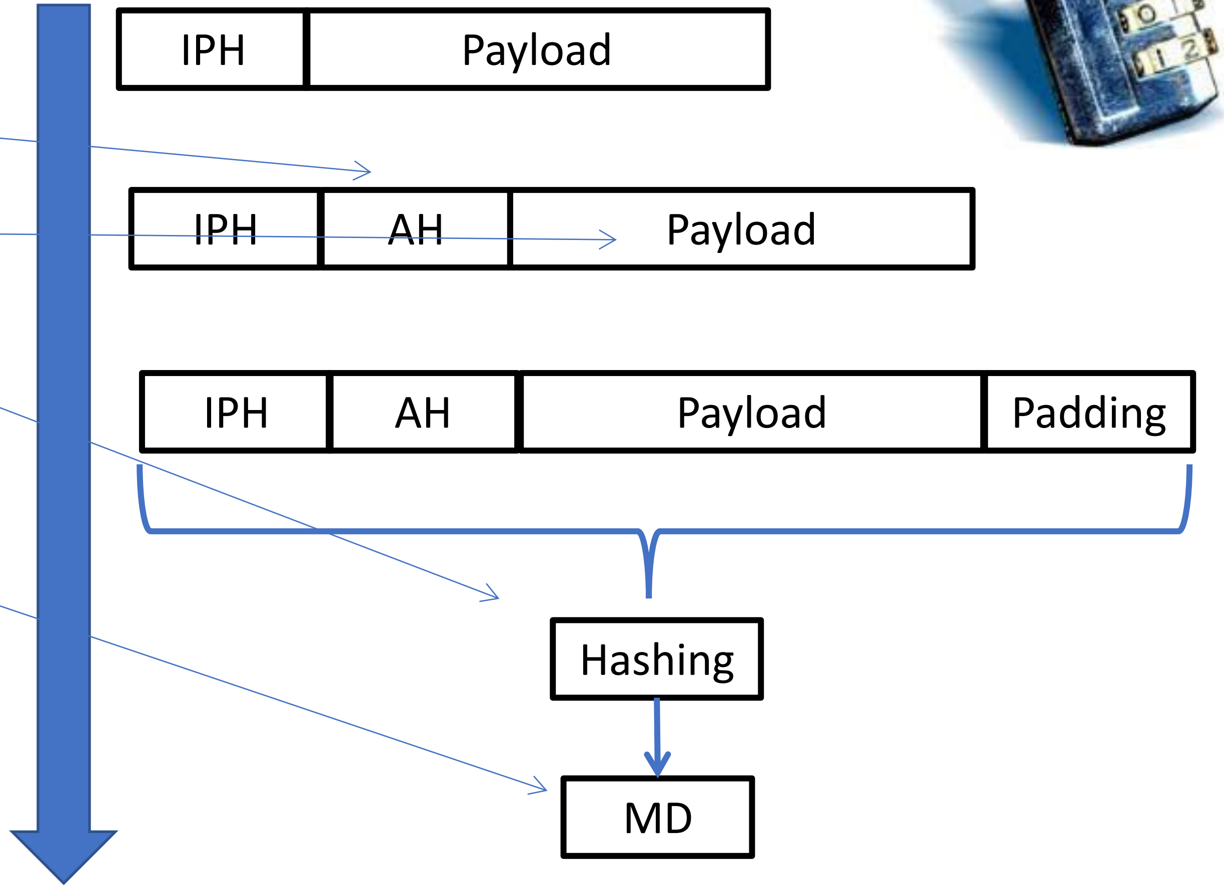


Internet Protocol Security (IPSec)

Authentication Header Protocol



1. An authentication header is added to the payload with the authentication data field set to 0.
2. Padding may be added to make the total length appropriate for a particular hashing algorithm.
3. Hashing is based on the total packet. However, only those fields of the IP header that do not change during transmission are included in the calculation of the message digest (authentication data).
4. The authentication data are inserted in the authentication header.
5. The IP header is added after changing the value of the protocol field to 51.

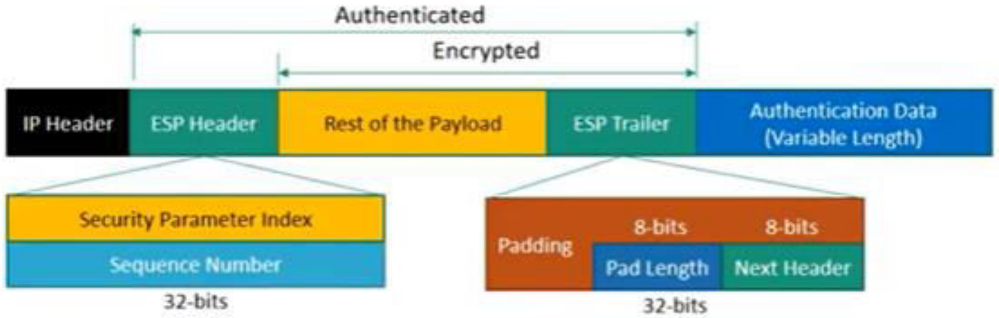


Internet Protocol Security (IPSec)

Encapsulating Security Payload (ESP)

- The AH protocol does not provide confidentiality, only source authentication and data integrity.
- Encapsulating Security Payload (ESP) provides
  - source authentication
  - Integrity
  - Confidentiality
- ESP adds a header and trailer.

- When an IP datagram carries an ESP header and trailer, the value of the protocol field in the IP header is 50.
- A field inside the ESP trailer (the next-header field) holds the original value of the protocol field (the type of payload being carried by the IP datagram, such as TCP or UDP).

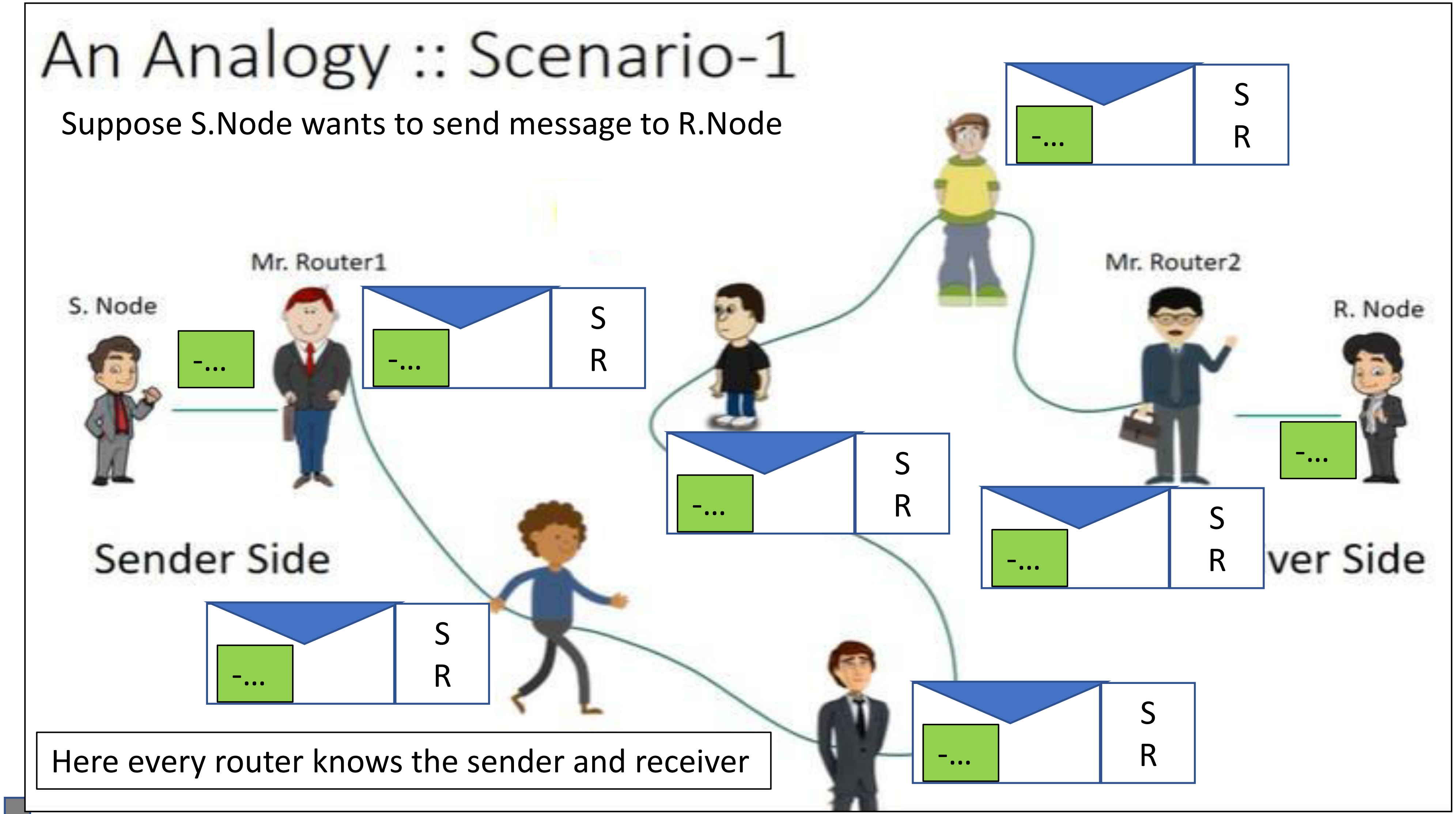


The ESP procedure follows these steps:

1. An ESP trailer is added to the payload.
2. The payload and the trailer are encrypted.
3. The ESP header is added.
4. The ESP header, payload, and ESP trailer are used to create the authentication data.
5. The authentication data are added to the end of the ESP trailer.
6. The IP header is added after changing the protocol value to 50.

Internet Protocol Security (IPSec)

Security Association (SA)



An Analogy :: Scenario-1

Suppose S.Node wants to send message to R.Node

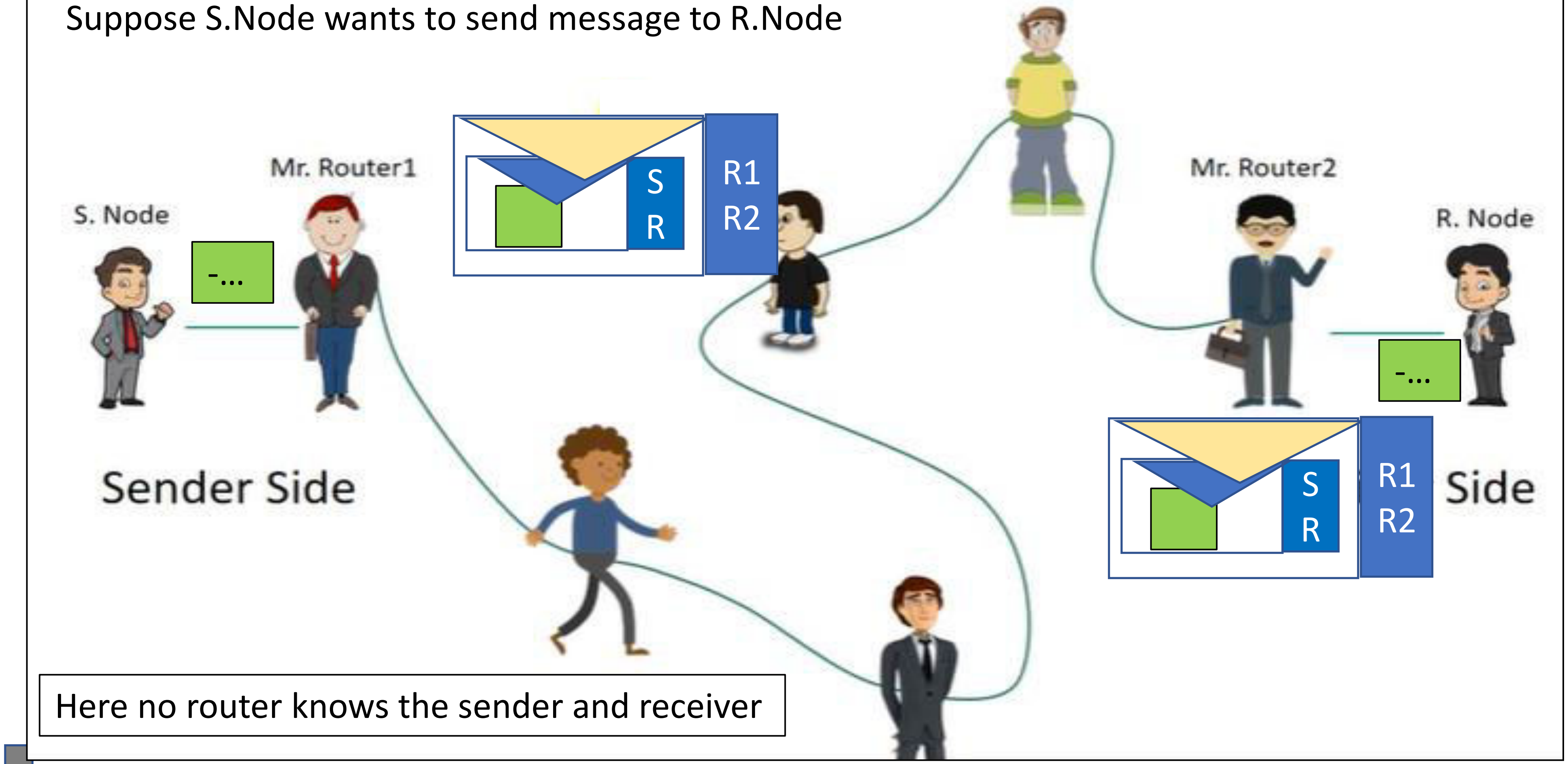
Here every router knows the sender and receiver

Internet Protocol Security (IPSec)

Security Association (SA)

An Analogy :: Scenario- 2

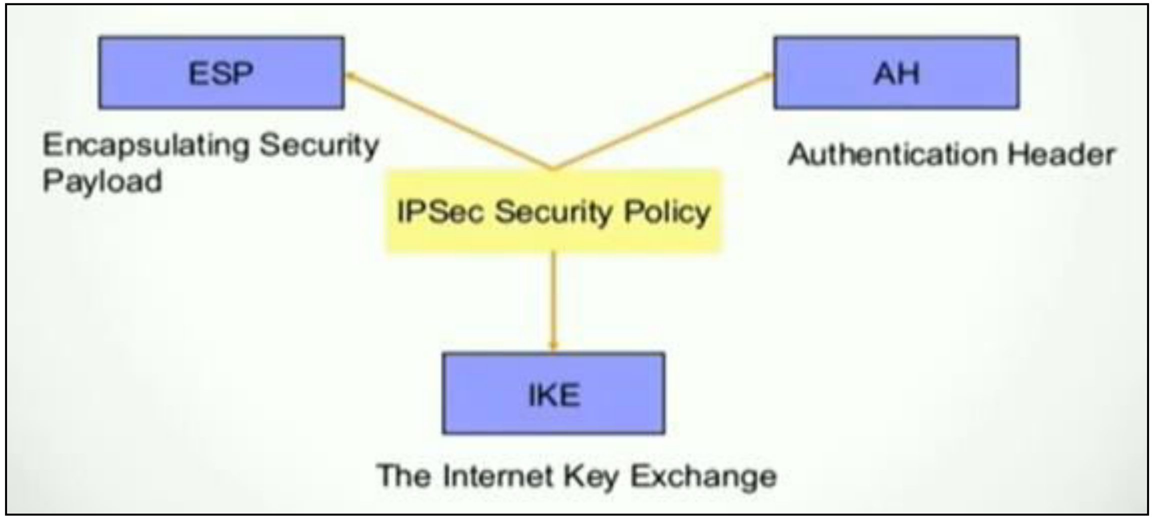
Suppose S.Node wants to send message to R.Node



Here no router knows the sender and receiver

Internet Protocol Security (IPSec) Protocols

IPSec is the combinations of protocols (ESP, AH, IKE)



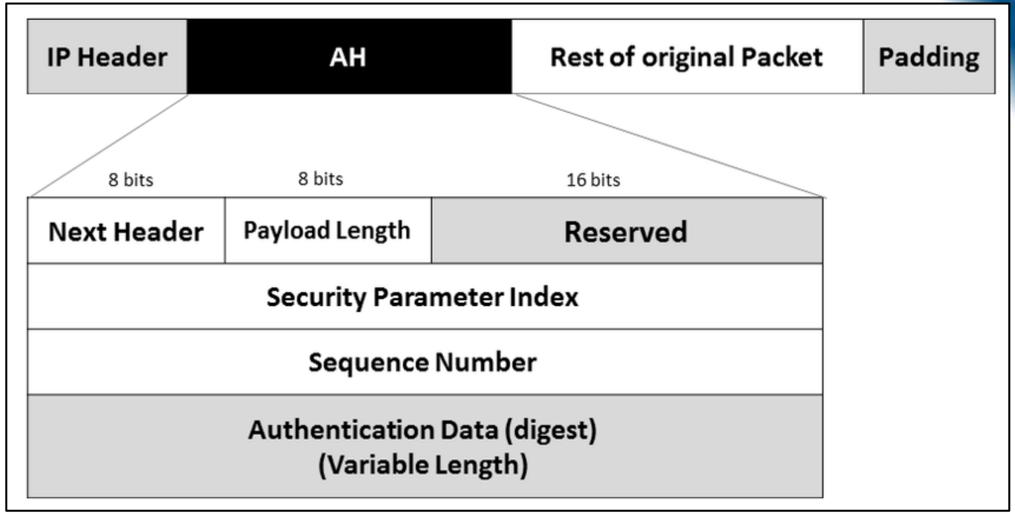
Service Provided

i) **ESP: Confidentiality, Authenticity & Integrity**

ii) **AH: Authenticity & Integrity**

iii) **IKE: Key related**

Authentication Header (AH)



IP Header	AH	Rest of original Packet	Padding

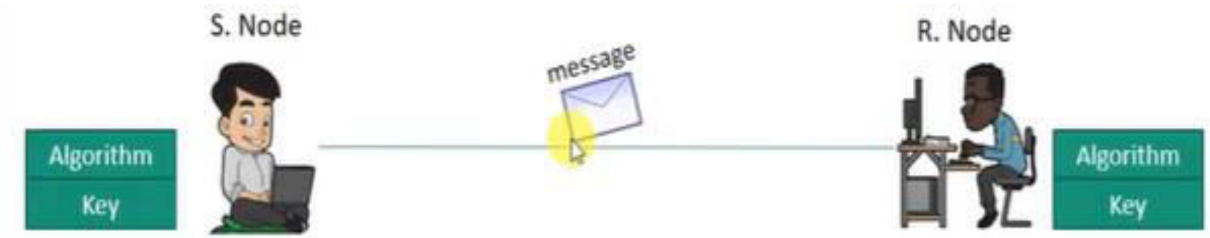
8 bits	8 bits	16 bits
Next Header	Payload Length	Reserved
Security Parameter Index		
Sequence Number		
Authentication Data (digest) (Variable Length)		

- **Security Parameter Index**: Client Service Code
- **Sequence Number**: Data Packet Number
- **Authentication Data**: Authentication Algo implemented

Internet Protocol Security (IPSec) Protocols

Security Association

- A Security Association is a contract between two parties; it creates a secure channel between them.

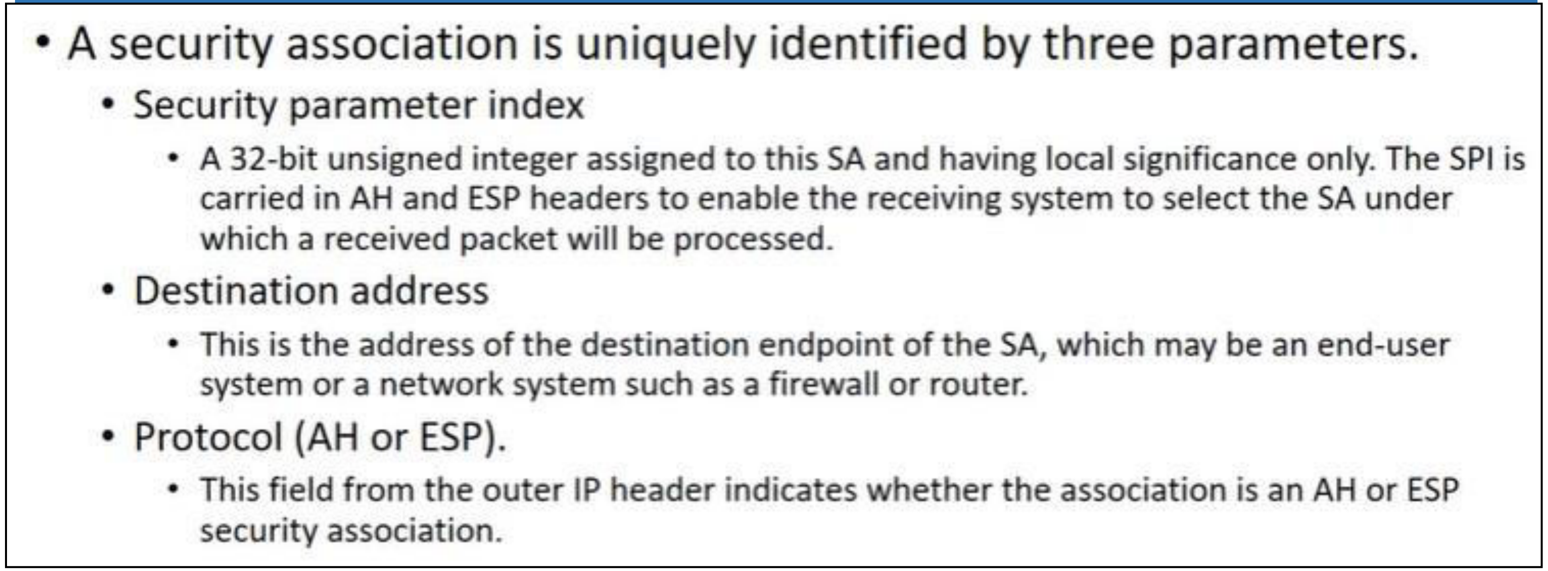


- If a peer relationship is needed for two-way secure exchange, then two security associations are required.
  - one outbound SA
  - one inbound SA.

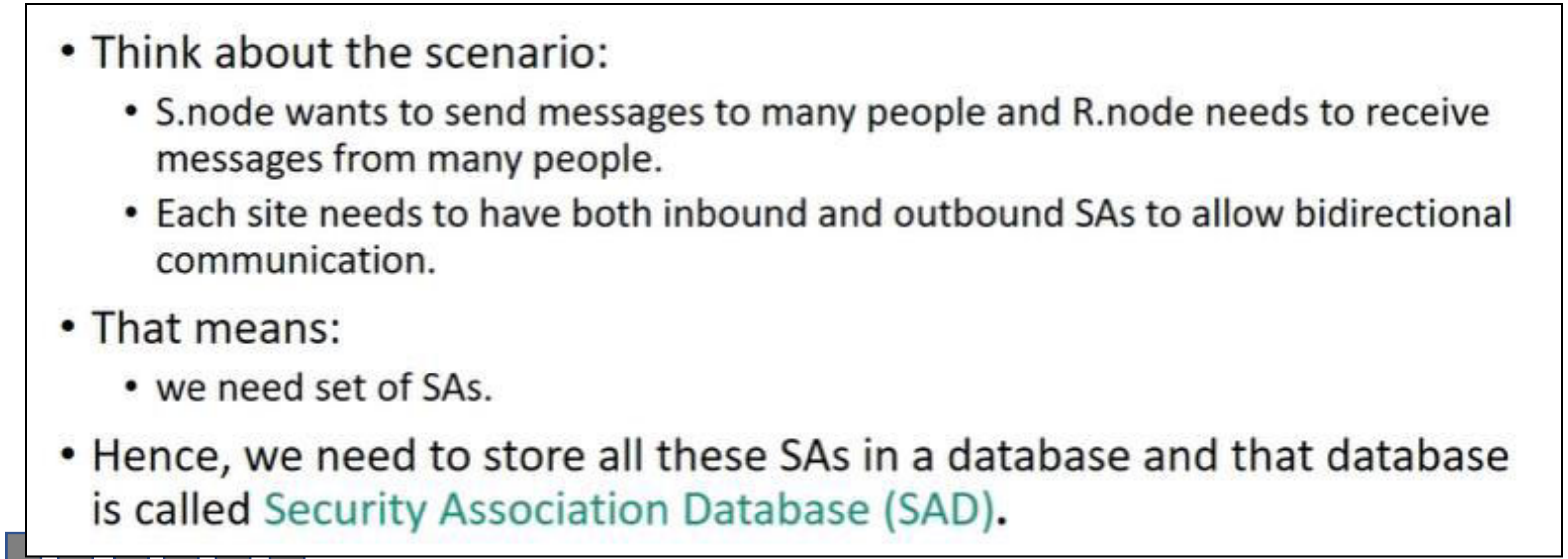
- The Security Association can be more involved if the two parties need message integrity and authentication.
- Each association needs other data such as the algorithm for message integrity, the key, and other parameters.

Internet Protocol Security (IPSec) Protocols

Security Association



- A security association is uniquely identified by three parameters.
  - Security parameter index
    - A 32-bit unsigned integer assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.
  - Destination address
    - This is the address of the destination endpoint of the SA, which may be an end-user system or a network system such as a firewall or router.
  - Protocol (AH or ESP).
    - This field from the outer IP header indicates whether the association is an AH or ESP security association.



- Think about the scenario:
  - S.node wants to send messages to many people and R.node needs to receive messages from many people.
  - Each site needs to have both inbound and outbound SAs to allow bidirectional communication.
- That means:
  - we need set of SAs.
- Hence, we need to store all these SAs in a database and that database is called Security Association Database (SAD).

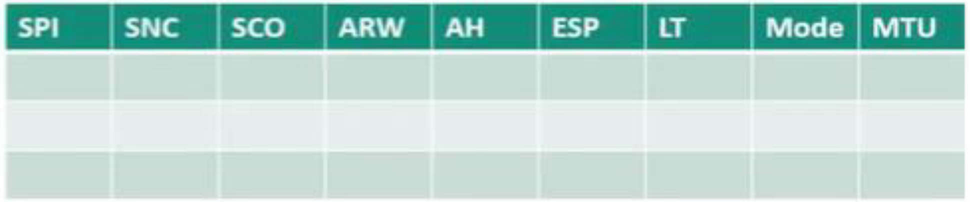
Internet Protocol Security (IPSec) Protocols

Security Association Database

- It is a two dimensional table.
- Each row defining a single SA.
- Normally, there are two SADs, one inbound and one outbound.
- When a host needs to send a packet that must carry an IPSec header, the host needs to find the corresponding entry in the outbound SAD to find the information for applying security to the packet.
- Similarly, when a host receives a packet that carries an IPSec header, the host needs to find the corresponding entry in the inbound SAD to find the information for checking the security of the packet.

- SAD contains the following entry:
  - Security Parameter Index:
  - Sequence Number Counter:
  - Sequence Counter Overflow:
  - Anti-Replay Window:
  - AH Information:
  - ESP Information:
  - Lifetime of this Security Association:
  - IPsec Protocol Mode:
  - Path MTU:

Security Association Database



SPI	SNC	SCO	ARW	AH	ESP	LT	Mode	MTU

William Stallings - Cryptography and Network Security Principles and Practice, 7th Edition-Pearson (2017) Chapter-20

Internet Protocol Security (IPSec) Protocols

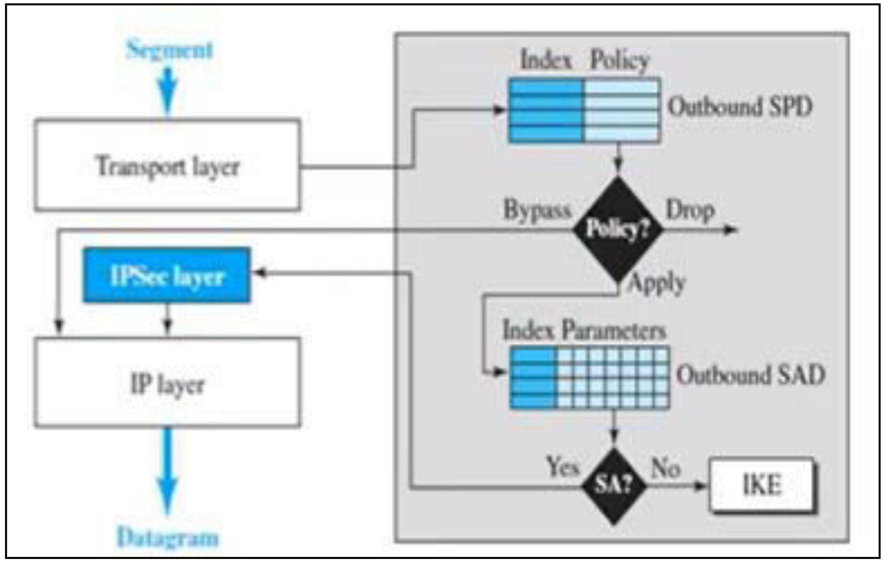
Security Policy Database

- Another important aspect of IPSec is the Security Policy (SP), which defines the type of security applied to a packet when it is to be sent or when it has arrived.
- Each host that is using the IPSec protocol needs to keep a Security Policy Database (SPD).
- Here also there is a need for an inbound SPD and an outbound SPD.

- Outbound SPD
  - When a packet is to be sent out, the outbound SPD is consulted.
  - The input to the outbound SPD is the six tuple index
  - The output is one of the three following cases:
    - drop (packet cannot be sent),
    - bypass (bypassing security header),
    - apply (applying the security according to the SAD; if no SAD, creating one).

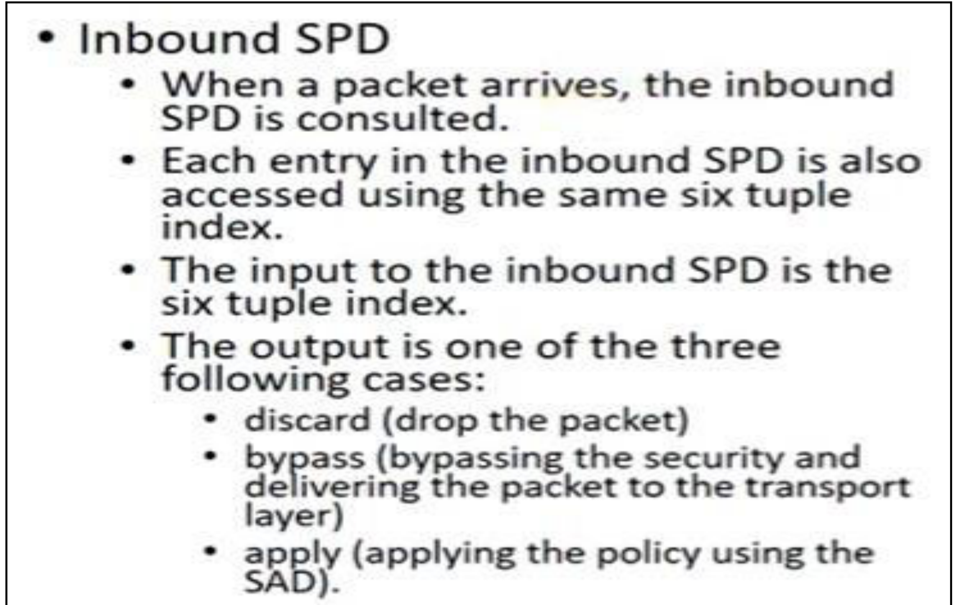
- Each entry in the SPD can be accessed using a six tuple index:
  - source address
  - destination address
  - Name
  - Protocol
  - source port
  - destination port

SA	DA	Name	Protocol	SP	DP	Policy
						Drop
						Bypass
						Apply

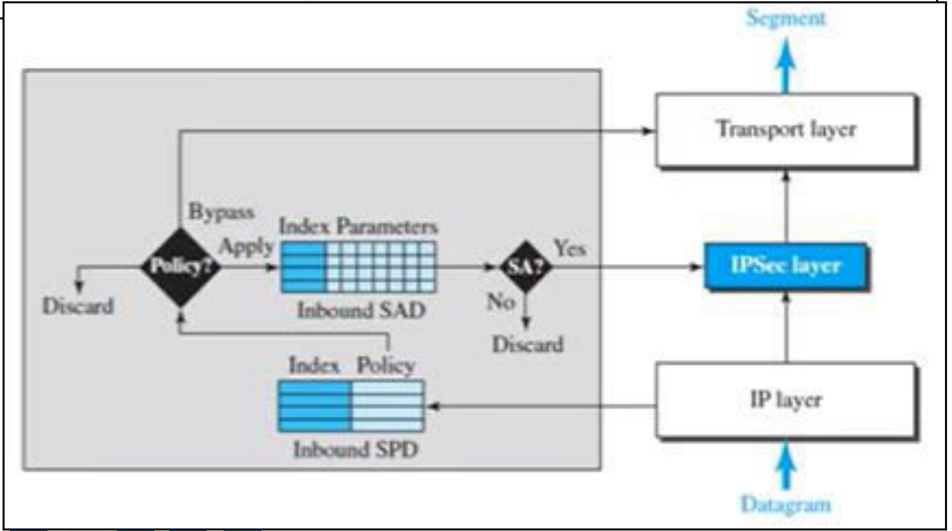


Internet Protocol Security (IPSec) Protocols

Security Policy Database

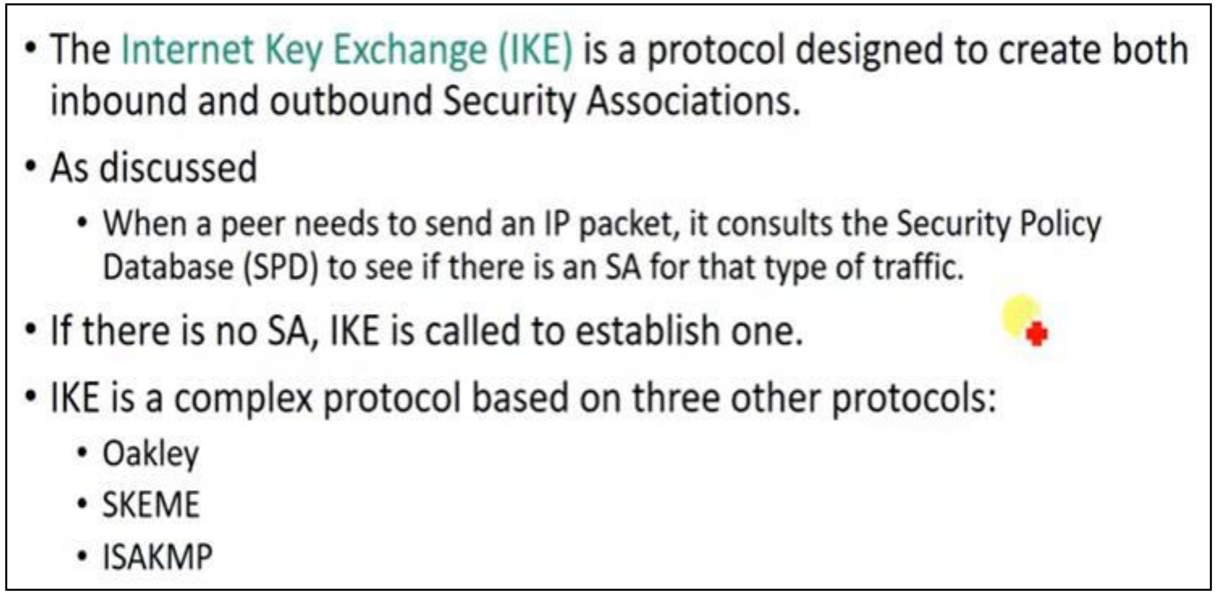


- Inbound SPD
  - When a packet arrives, the inbound SPD is consulted.
  - Each entry in the inbound SPD is also accessed using the same six tuple index.
  - The input to the inbound SPD is the six tuple index.
  - The output is one of the three following cases:
    - discard (drop the packet)
    - bypass (bypassing the security and delivering the packet to the transport layer)
    - apply (applying the policy using the SAD).



Internet Key Exchange (IKE)

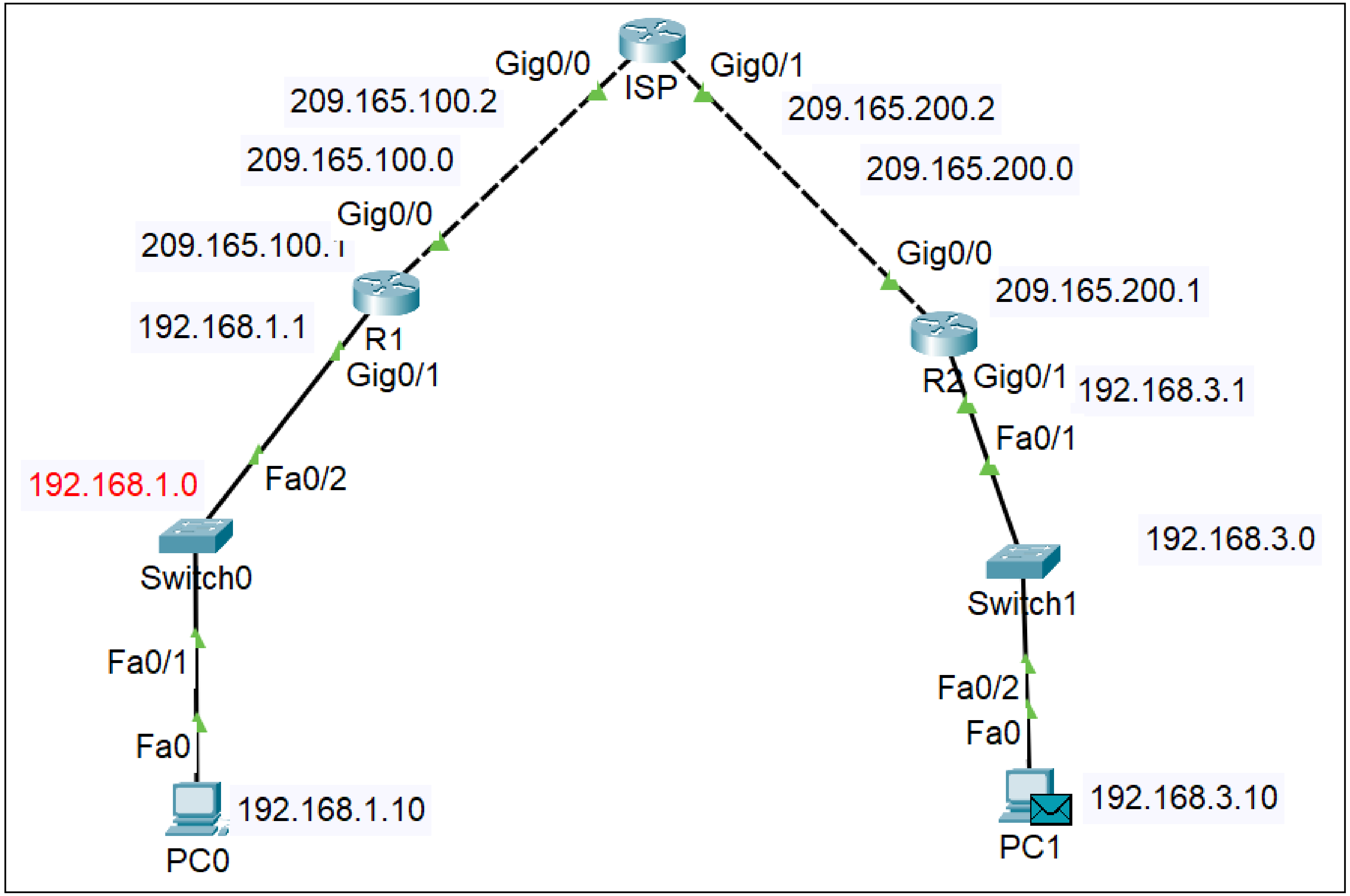
- It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.
- IKE provides message content protection and also an open frame for implementing standard algorithms.



- The Internet Key Exchange (IKE) is a protocol designed to create both inbound and outbound Security Associations.
- As discussed
  - When a peer needs to send an IP packet, it consults the Security Policy Database (SPD) to see if there is an SA for that type of traffic.
- If there is no SA, IKE is called to establish one.
- IKE is a complex protocol based on three other protocols:
  - Oakley
  - SKEME
  - ISAKMP

Internet Protocol Security (IPSec) Protocols

Packet Tracer Application



Ipsec is implemented between R1 and R2.
For configuration follow the file con_ipsec_PT.txt