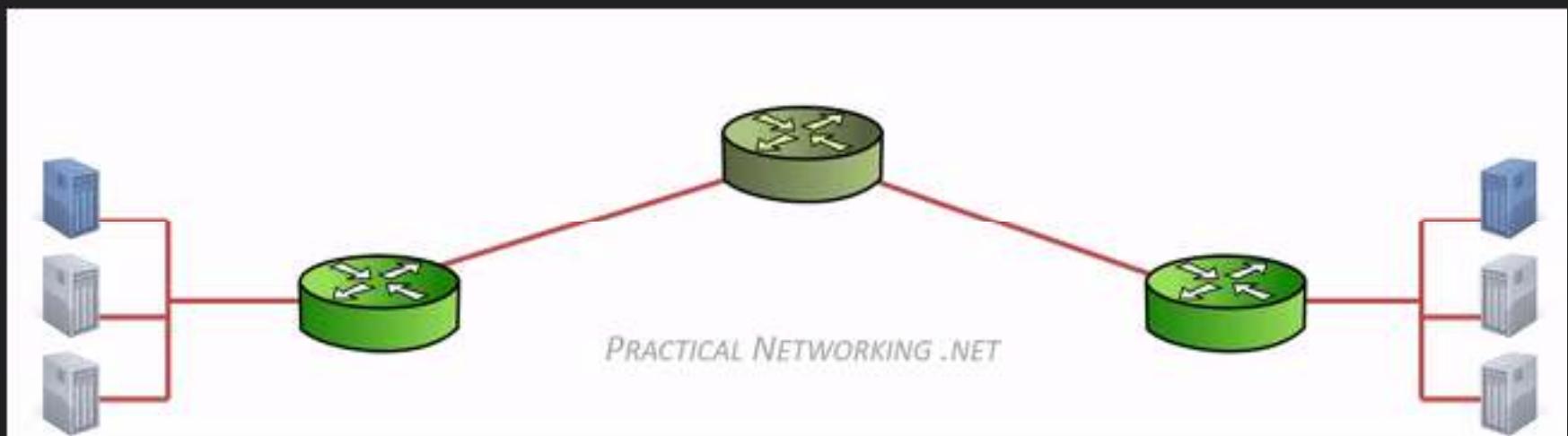




# IP Security Overview

- We have considered some application specific security mechanisms
  - e.g. 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



PRACTICAL NETWORKING .NET

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical



# Layers 7, 6, 5

- 7: Application layer
  - Provides different services to the applications
  - Uses the underlying layers to carry out work
    - e.g. SMTP (mail), HTTP (web), Telnet, FTP, DNS
- 6: Presentation layer
  - Converts data from applications into common format and vice versa
- 5: Session layer
  - organizes and synchronizes the exchange of data between application processes

# Layer 4

- 4: Transport layer
- Provides end to end transportation of segments
- E.g. TCP
  - encapsulates TCP segments in network layer packets
  - adds reliability by detecting and retransmitting lost packets
  - uses acknowledgements and sequence numbers to keep track of successful, out-of-order, and lost packets
  - timers help differentiate between loss and delay
- UDP is much simpler: no reliability features

# Layer 3

## ③ Network layer

- Routes the information in the network
- E.g. IP is a network layer implementation which defines addresses in such a way that route selection can be determined.
  - Single address space for the entire internetwork
  - adds an additional layer of addressing, e.g. IP address, which is different from MAC address.

# Layer 3

- 3: Network layer (e.g. IP)
  - Unreliable (best effort)
    - if packet gets lost, network layer doesn't care for higher layers can resend lost packets
  - Forwards packets hop by hop
    - encapsulates network layer packet inside data link layer frame
    - different framing on different underlying network types
    - receive from one link, forward to another link
    - There can be many hops from source to destination

# Layer 3

## ③ Network layer (e.g. IP)

- Makes routing decisions
  - how can the packet be sent closer to its destination?
  - forwarding and routing tables embody “knowledge” of network topology
  - routers can talk to each other to exchange information about network topology

# Layer 2

## ② Data Link layer

- Provides reliable transit of data across a physical network link
- bundles bits into frames and moves frames between hosts on the same link
- a frame has a definite start, end, size
- often also a definite source and destination link-layer address (e.g. Ethernet MAC address)
- some link layers detect corrupted frames while other layers re-send corrupted frames (NOT Ethernet)

# Layer 1

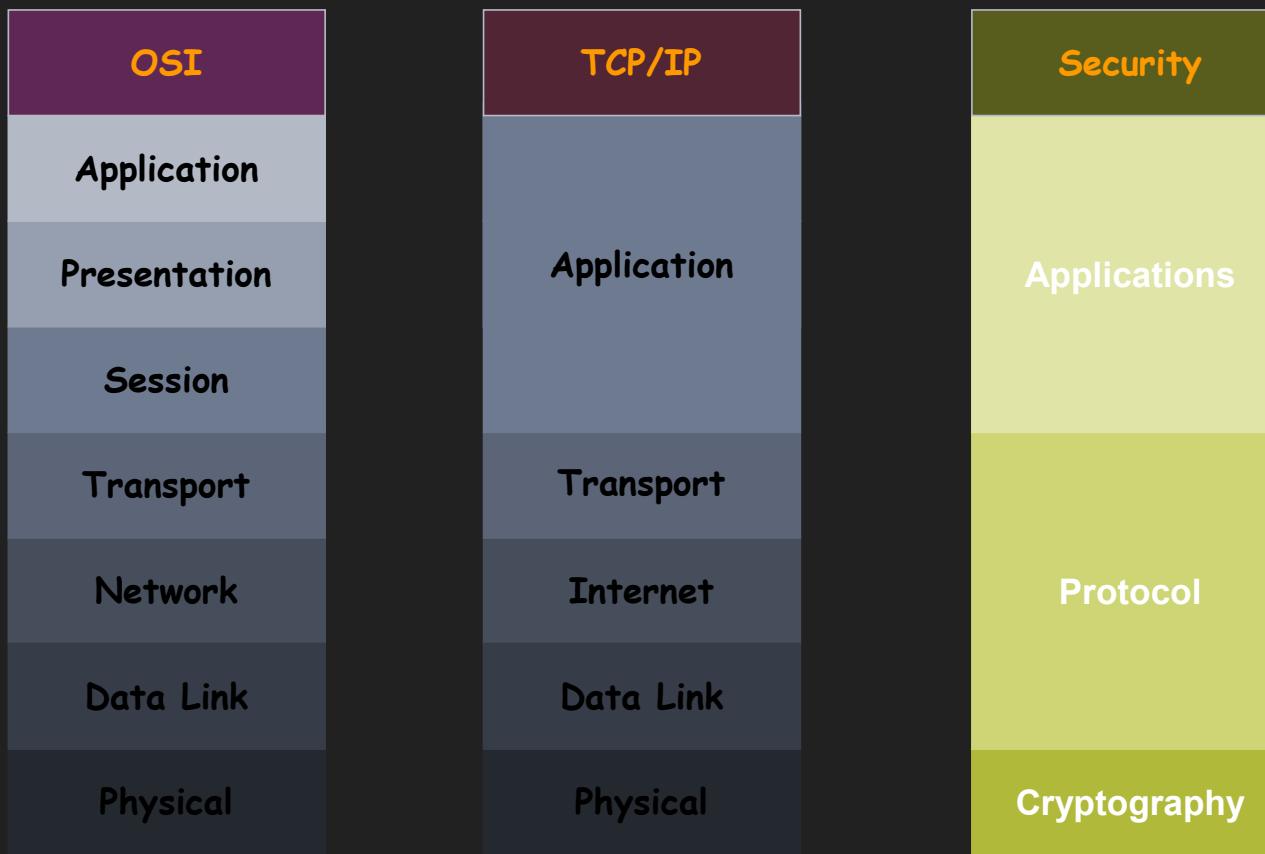
## ① Physical layer

- moves bits using voltage, light, radio, etc.
- no concept of bytes or frames
- bits are defined by voltage levels, or similar physical properties



1101001000

# Security versus OSI & TCP/IP Model



# Security Flows

Applications	<b>Applications:</b> Web, email, any application use security mechanism
Protocol	<b>Protocol:</b> SSL, TLS, IPSec*
Cryptography	<b>Algorithm:</b> Symmetric, Asymmetric (i.e.:Cipher, DES, AES)

# IP Security Overview

IPSec is not a single protocol. Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.

# What is IPSec?

- IP Security is a set of protocols and standards to support the securing of data at the IP layer. IPSec is a framework, not an implementation.
- Supports authentication and encryption of traffic.
  - Certifies the originator of the packet.
  - Protects the data from interception and tampering while in transit.

# IPSec

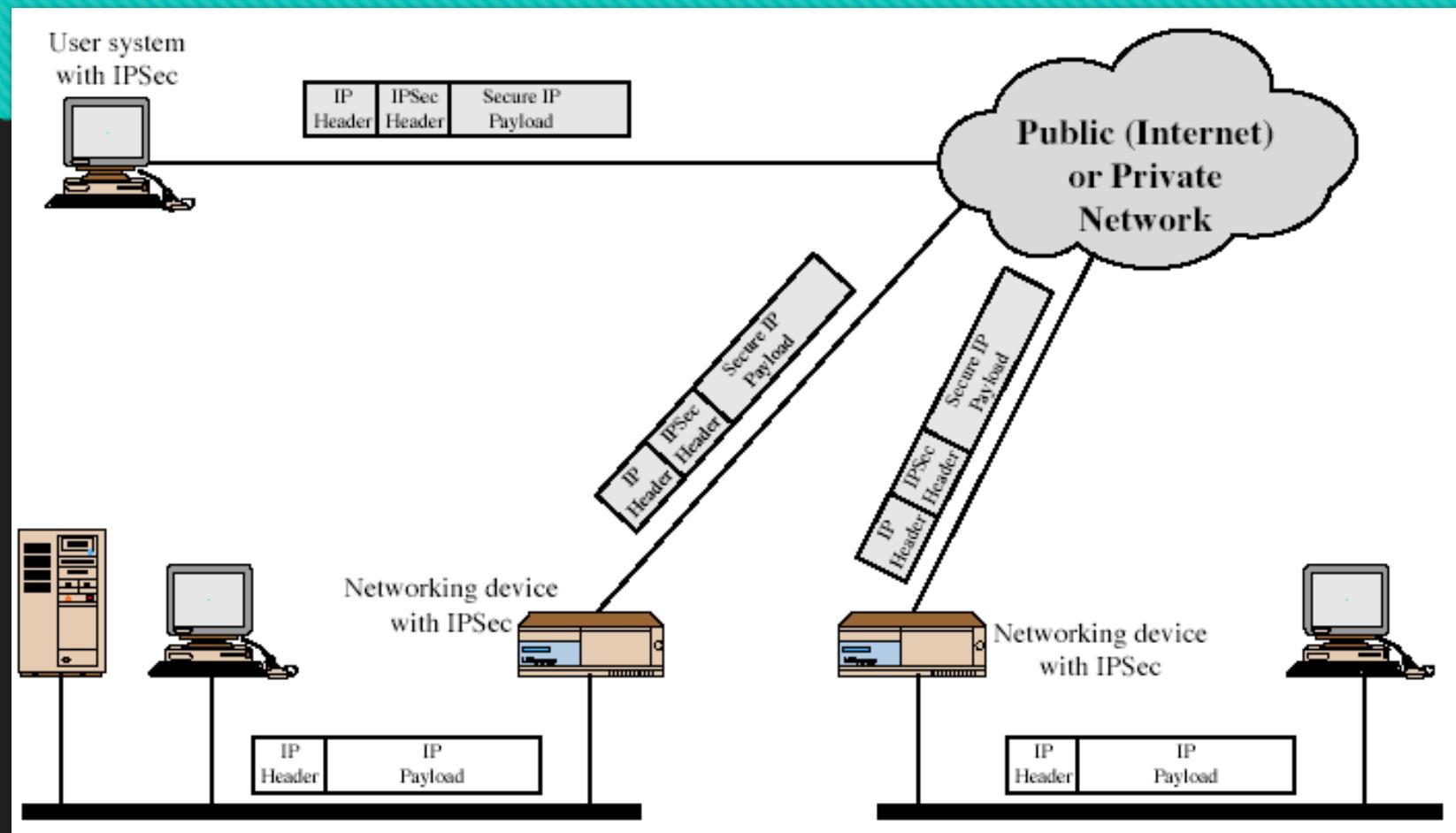
- general IP Security mechanisms provides
  - authentication
  - confidentiality
  - key management
- applicable to use over LANs, across public & private WANs, & for the Internet

# IP Security Overview

## Applications of IPSec

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

# IPSec Uses



## Benefits of IPSec

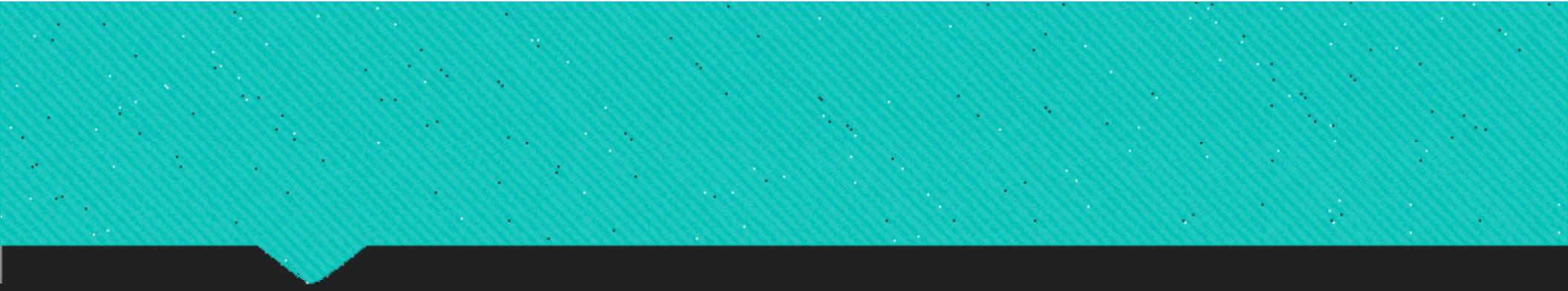
- in a firewall/router provides strong security to all traffic crossing the perimeter
- is resistant to bypass
- is below transport layer, hence transparent to applications
- can be transparent to end users
- can provide security for individual users if desired

# IP Security Architecture

- specification is quite complex
- defined in numerous RFC's
  - incl. RFC 2401/2402/2406/2408
  - many others, grouped by category
- mandatory in IPv6, optional in IPv4

# IPSec Services

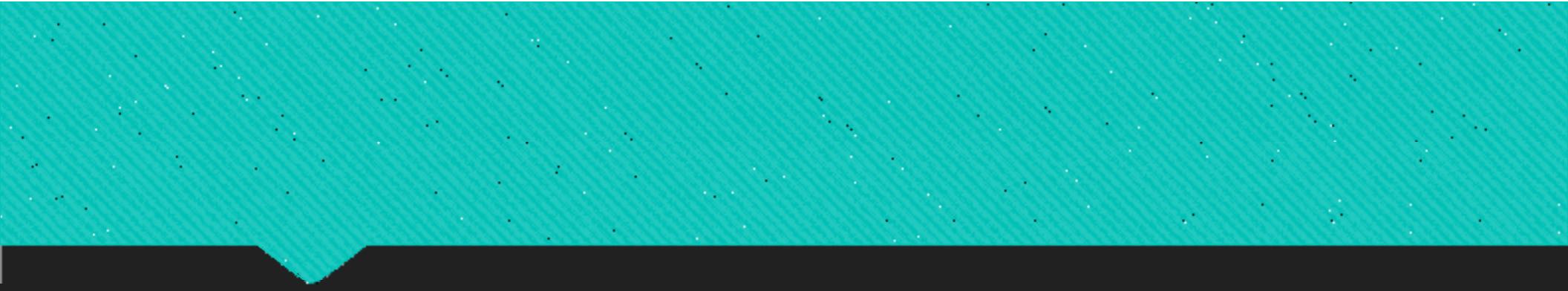
- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
  - a form of partial sequence integrity
- Confidentiality (encryption)
- Limited traffic flow confidentiality



Why do we want to use IPSec?

# Why do we want to use IPSec?

- **Secure our network**
- **Transparent operation**
  - IPSec allows us to secure any IP based protocol transparent to the application.
  - Support for legacy software which is inherently insecure (telnet,ftp).
  - An alternative mechanism to implementing application level security such as using SSL.
- **Widest industry support e.g. Cisco, Microsoft, Network Associates, CheckPoint Software, Bay Networks, etc.**
- **IETF standard – Will be mandatory in IPv6**

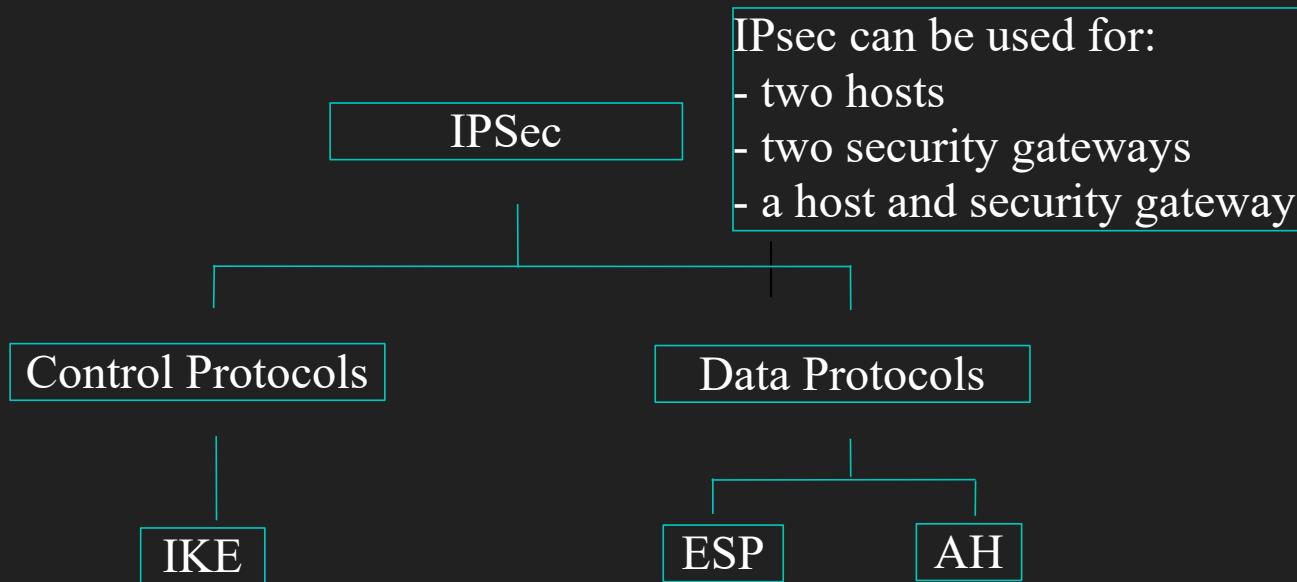


Why not to use IPsec?

## Why not to use IPSec?

- Processor overhead to encrypt & verify each packet can be great.
- Added complexity in network design.

# IPSec Diagram Structure

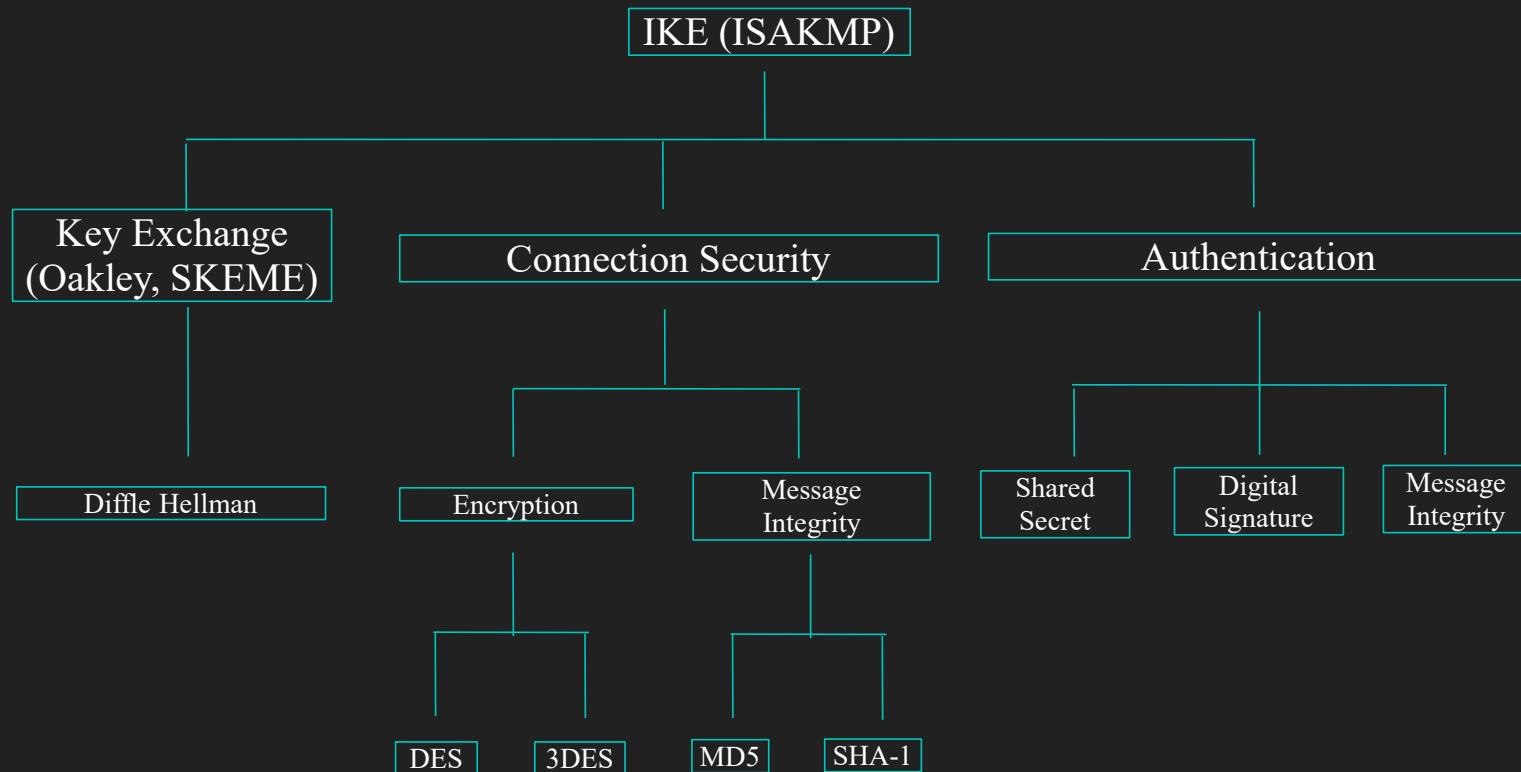


IKE – Internet Key Exchange

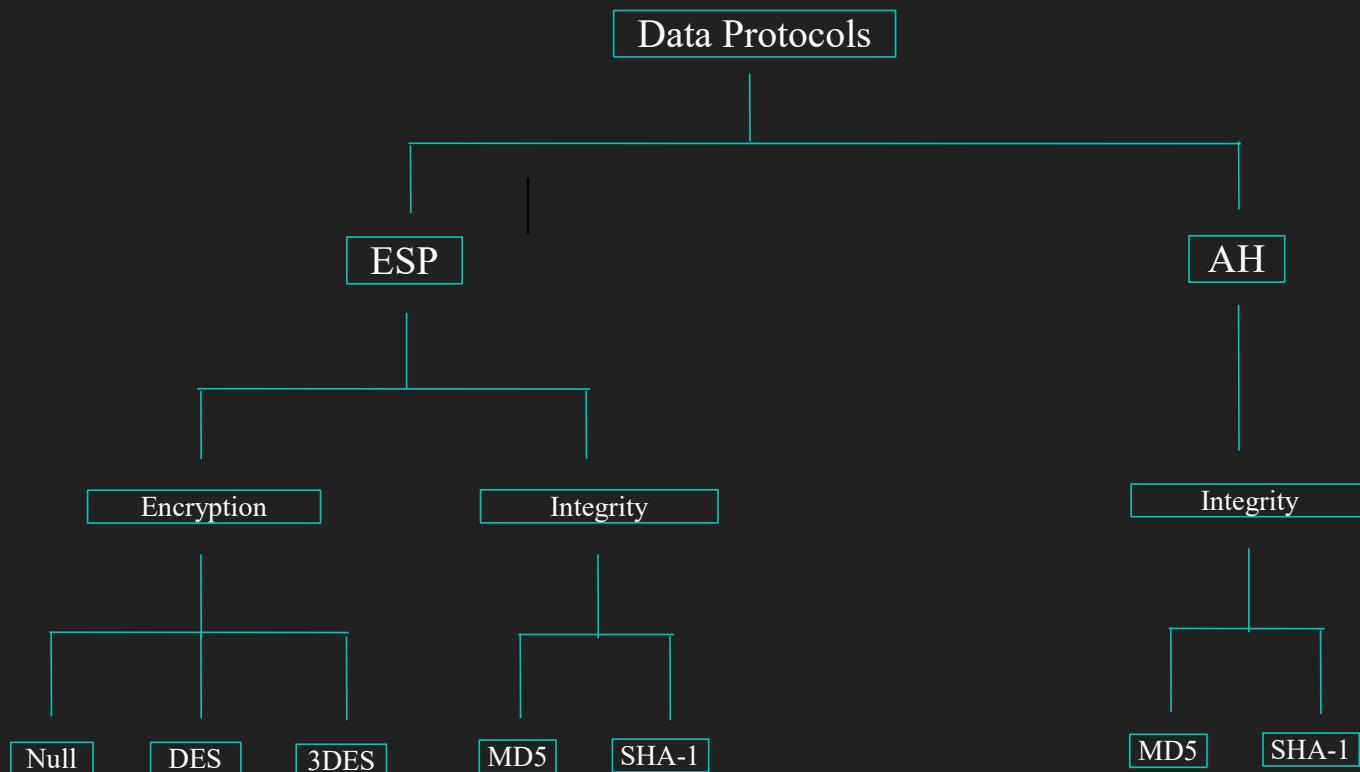
ESP – Encapsulating Security Payload

AH – Authentication Header

# IPSec Diagram Structure



# IPSec Diagram Structure





## IPSEC VPN Fundamentals



<https://learn.cantrill.io>



adriancantrill

- IPSEC is a group of protocols ...
- It sets up **secure tunnels** across **insecure networks**
- .. between **two peers** (**local** and **remote**)
- Provides **Authentication** ...
- .. and **encryption**



## Public Internet (Insecure) 😥

Created as required  
\*\* interesting traffic \*\*



IPSec Tunnels

## Public Internet (**Insecure**) 🤡

Created as required  
\*\* interesting traffic \*\*



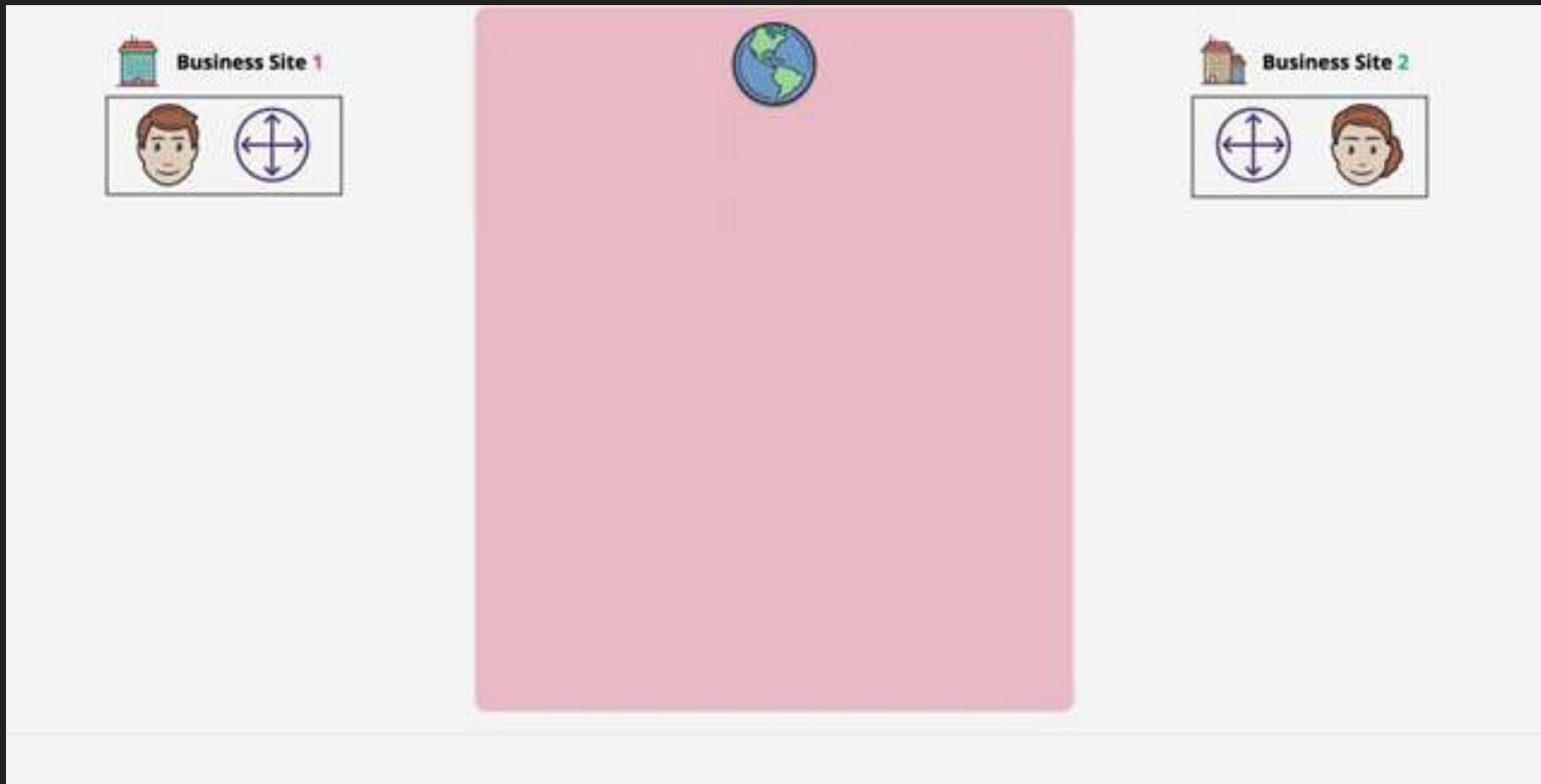
Data inside tunnels is  
**encrypted - secure connection**  
over an **insecure** network

IPSec Tunnels



- Remember - **Symmetric Encryption** is fast ... 
- ... but it's a challenge to exchange keys securely
- **Asymmetric Encryption** is slow ... 
- ... but you can easily exchange public keys

## Phase 1





Business Site 1



I'm Bob

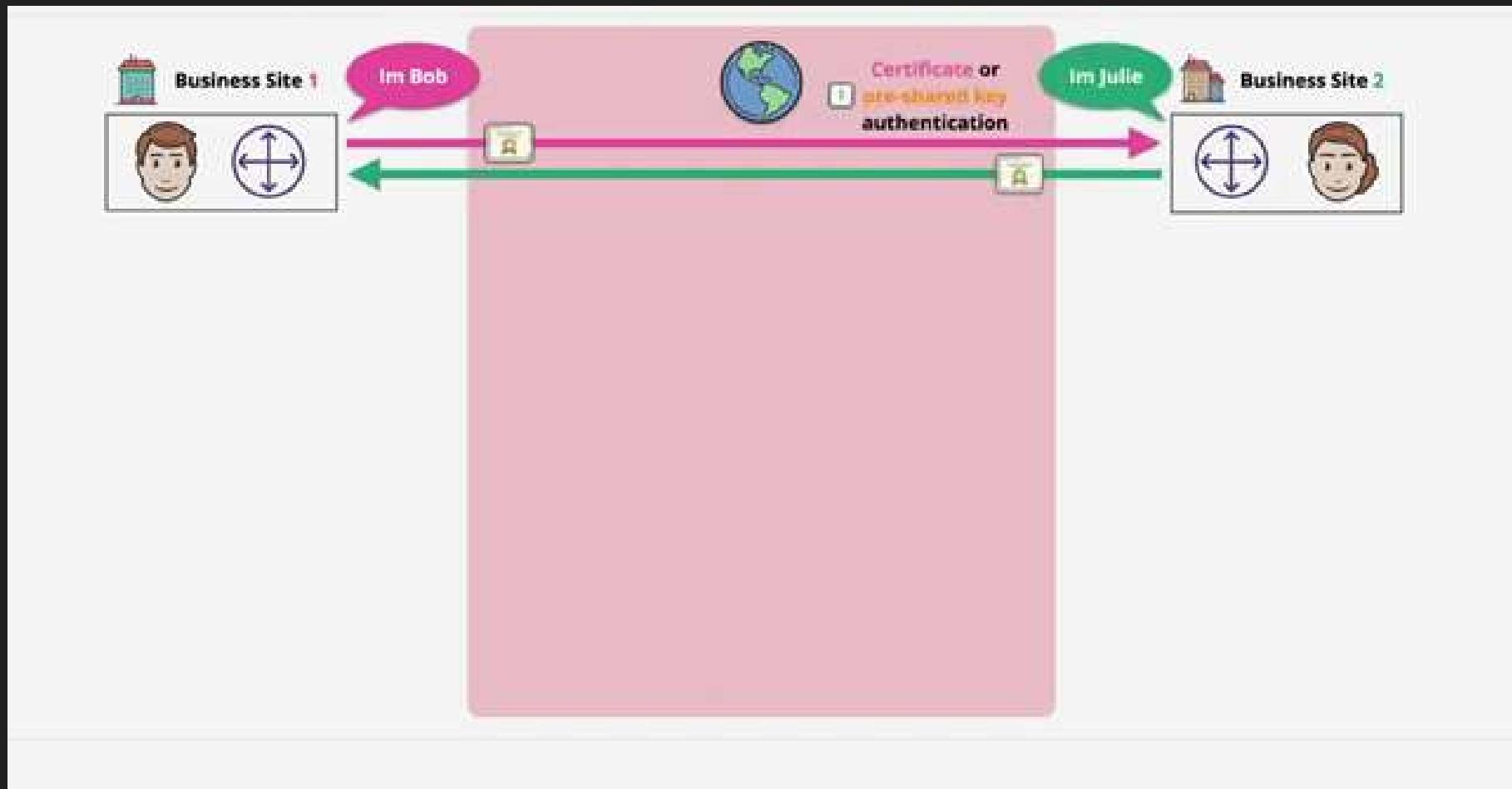


I'm Julie

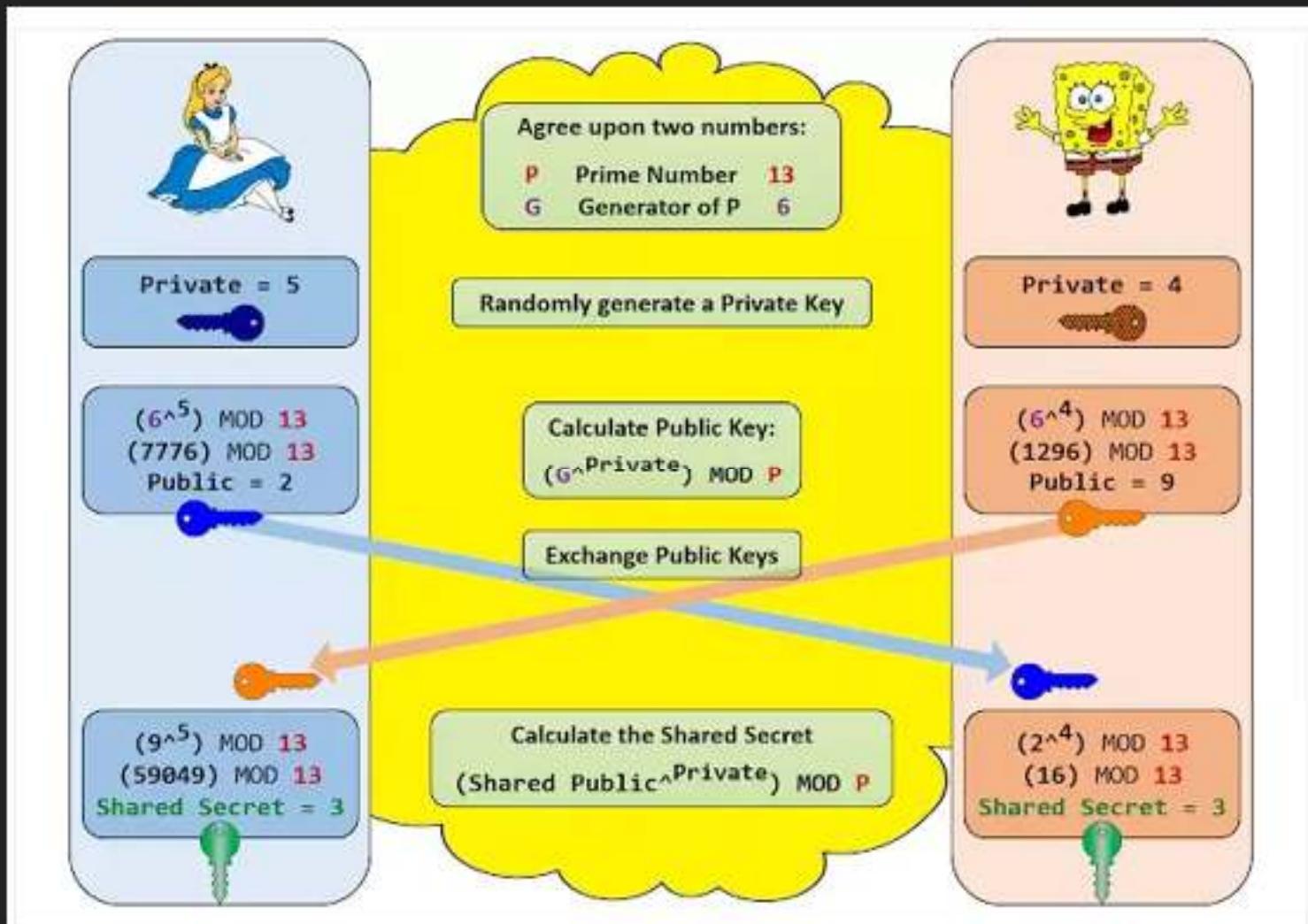


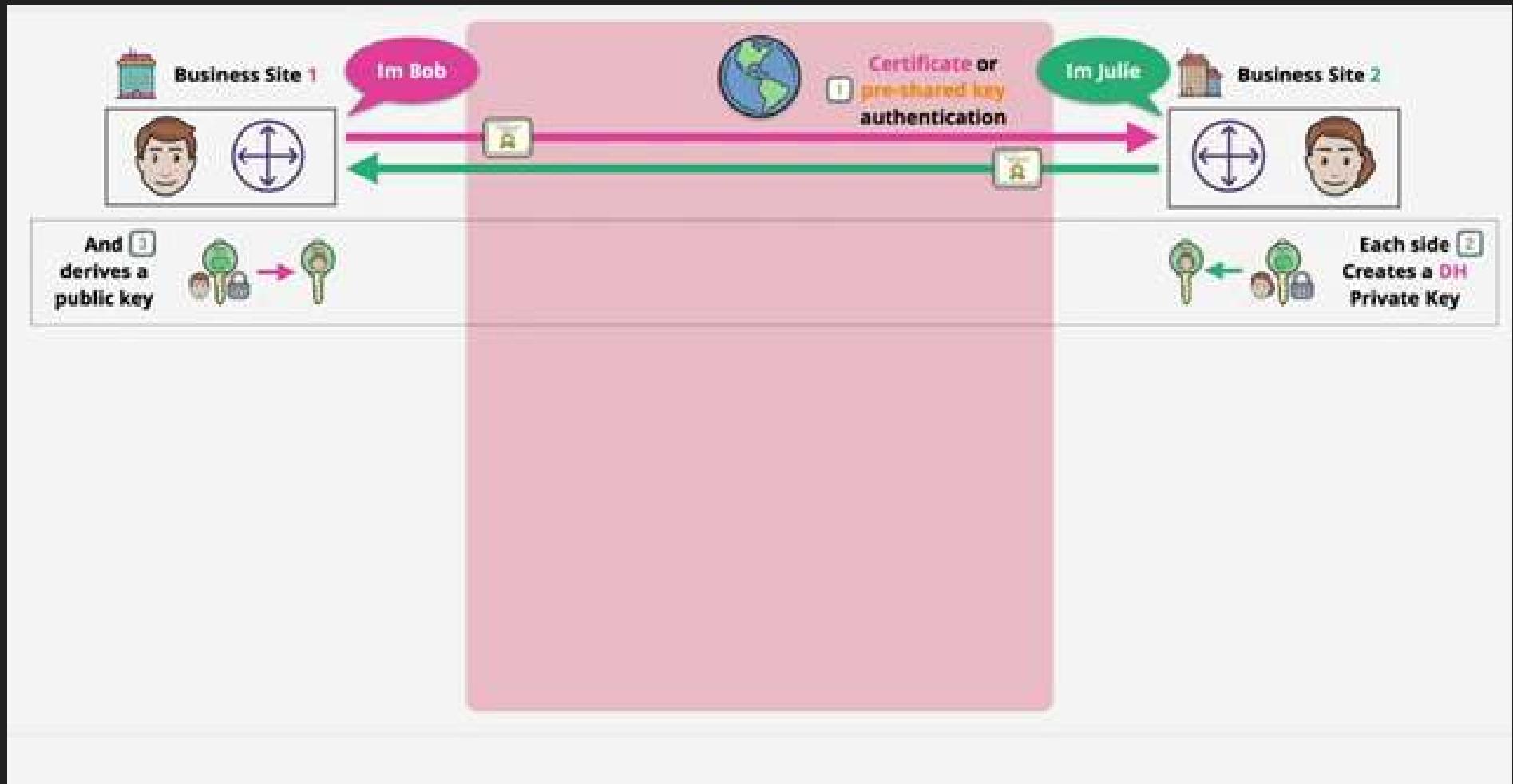
Business Site 2

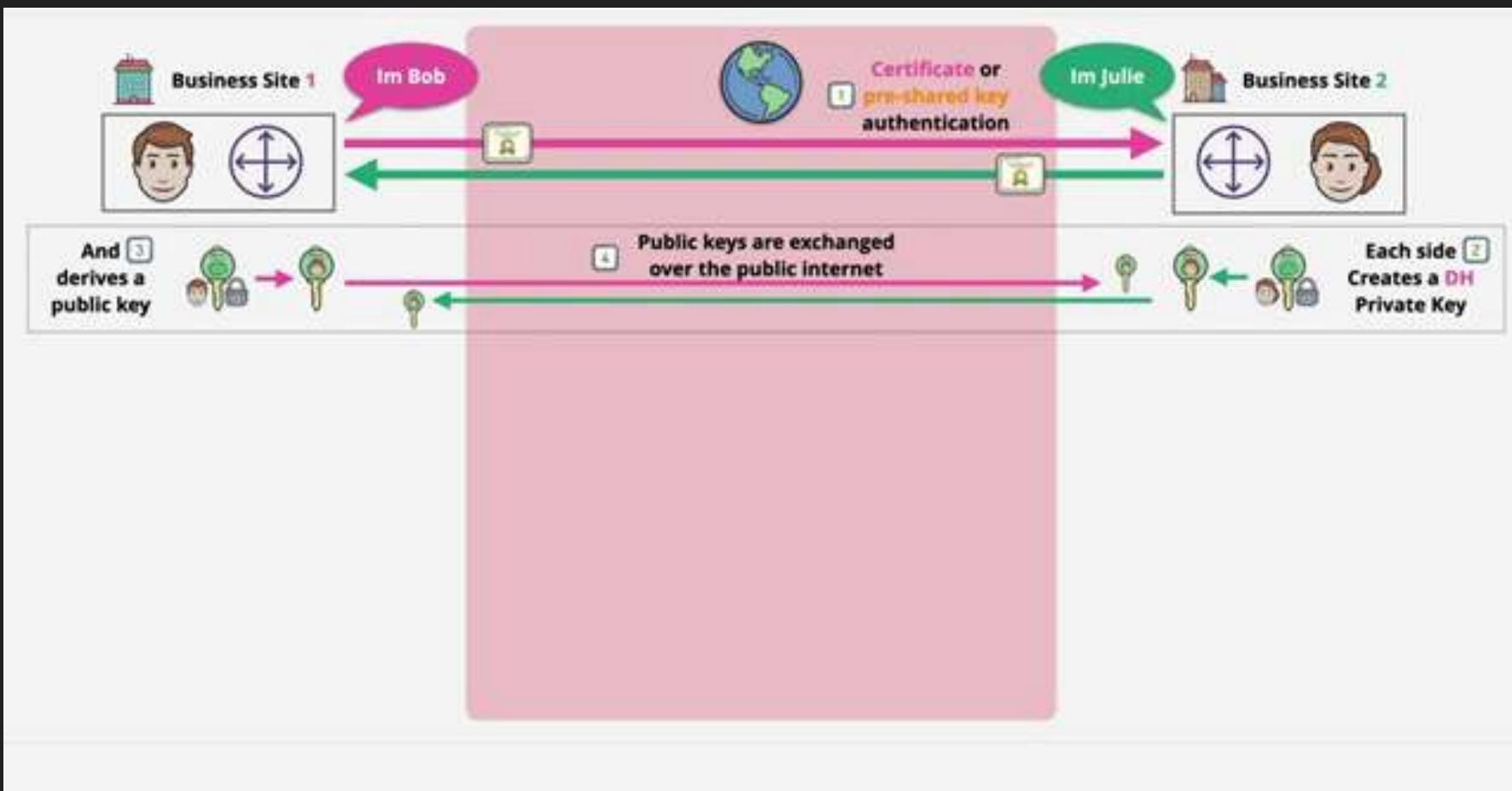


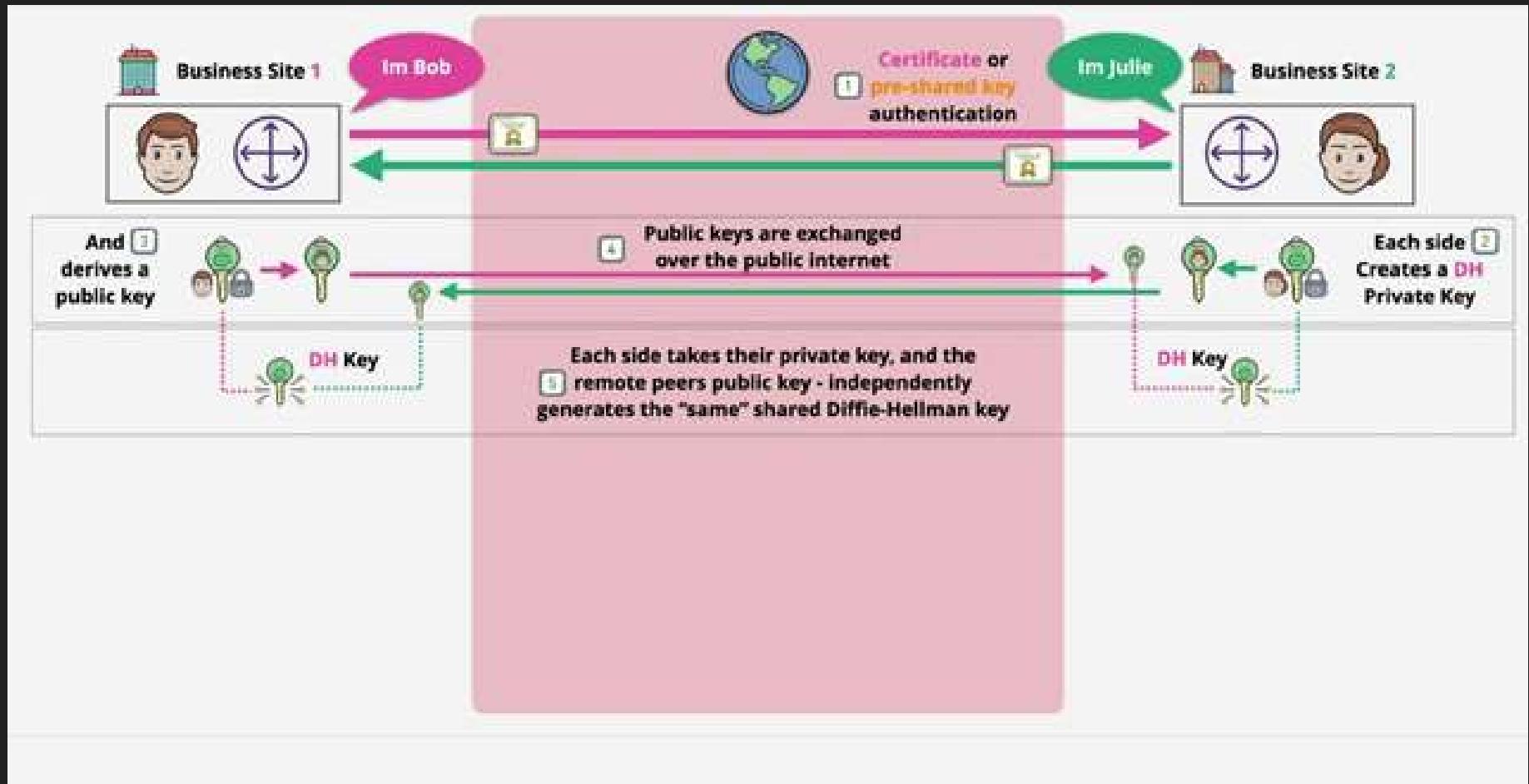


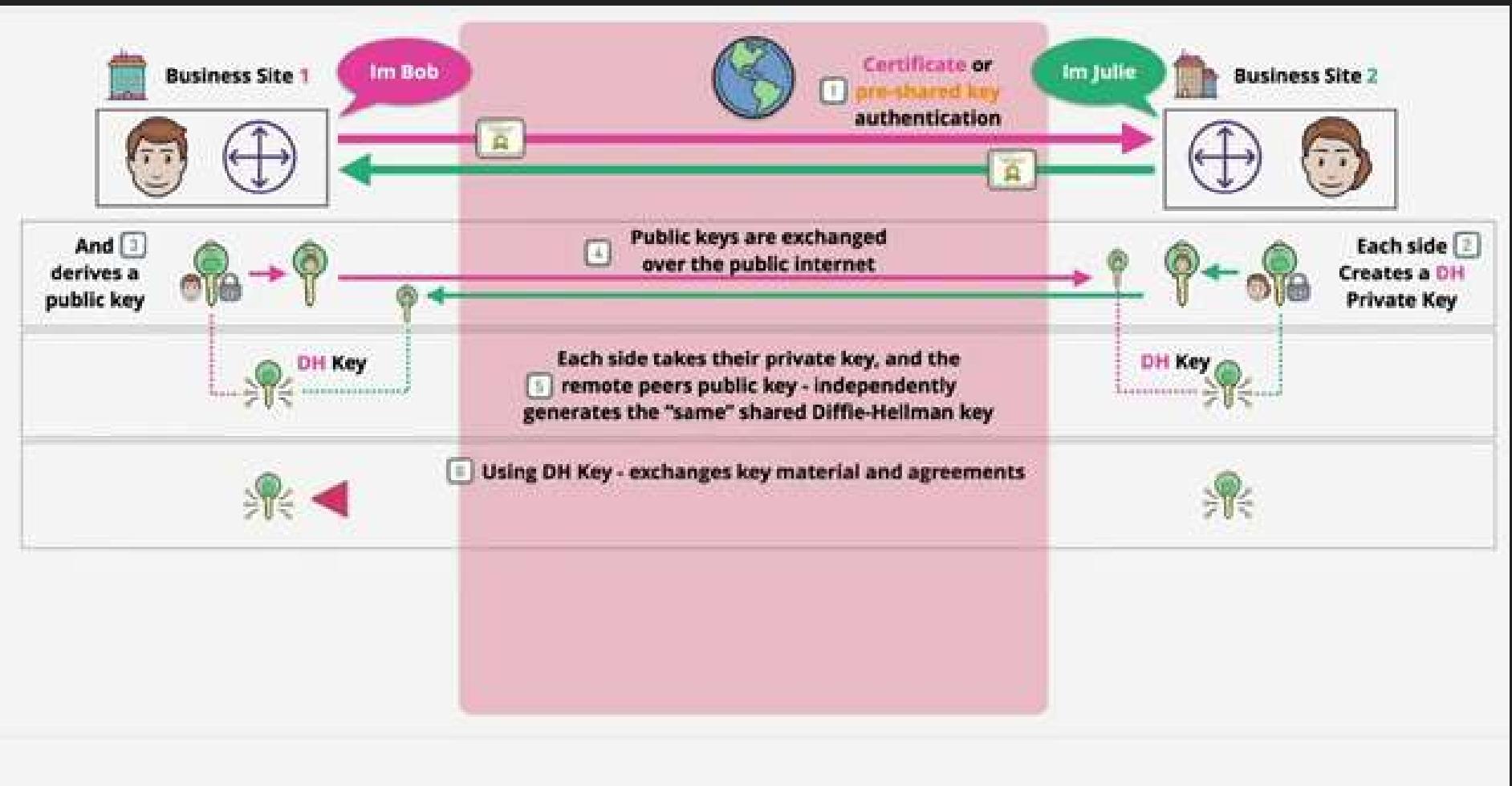
## Diffie Hellman Key Exchange Algorithm

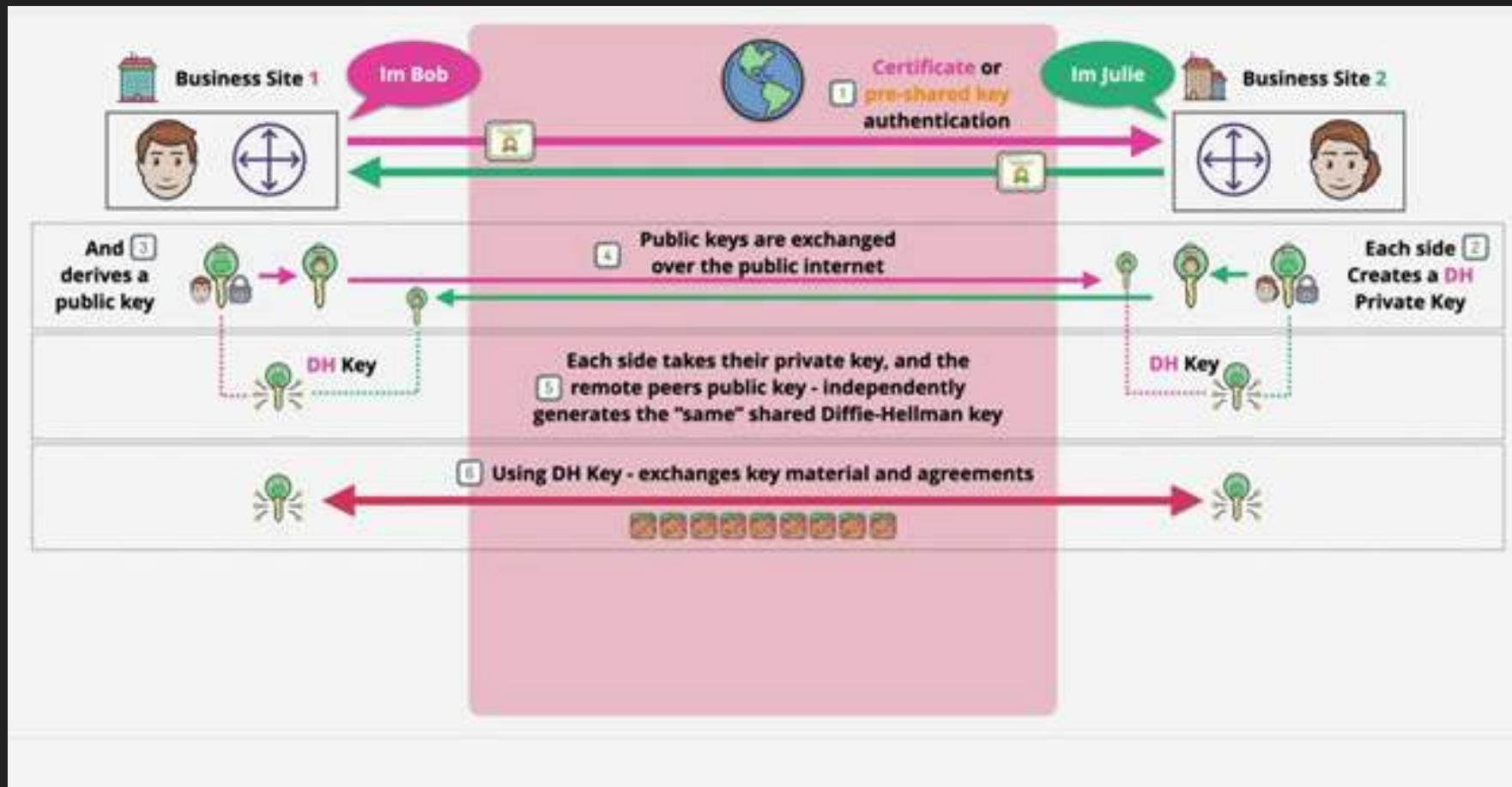


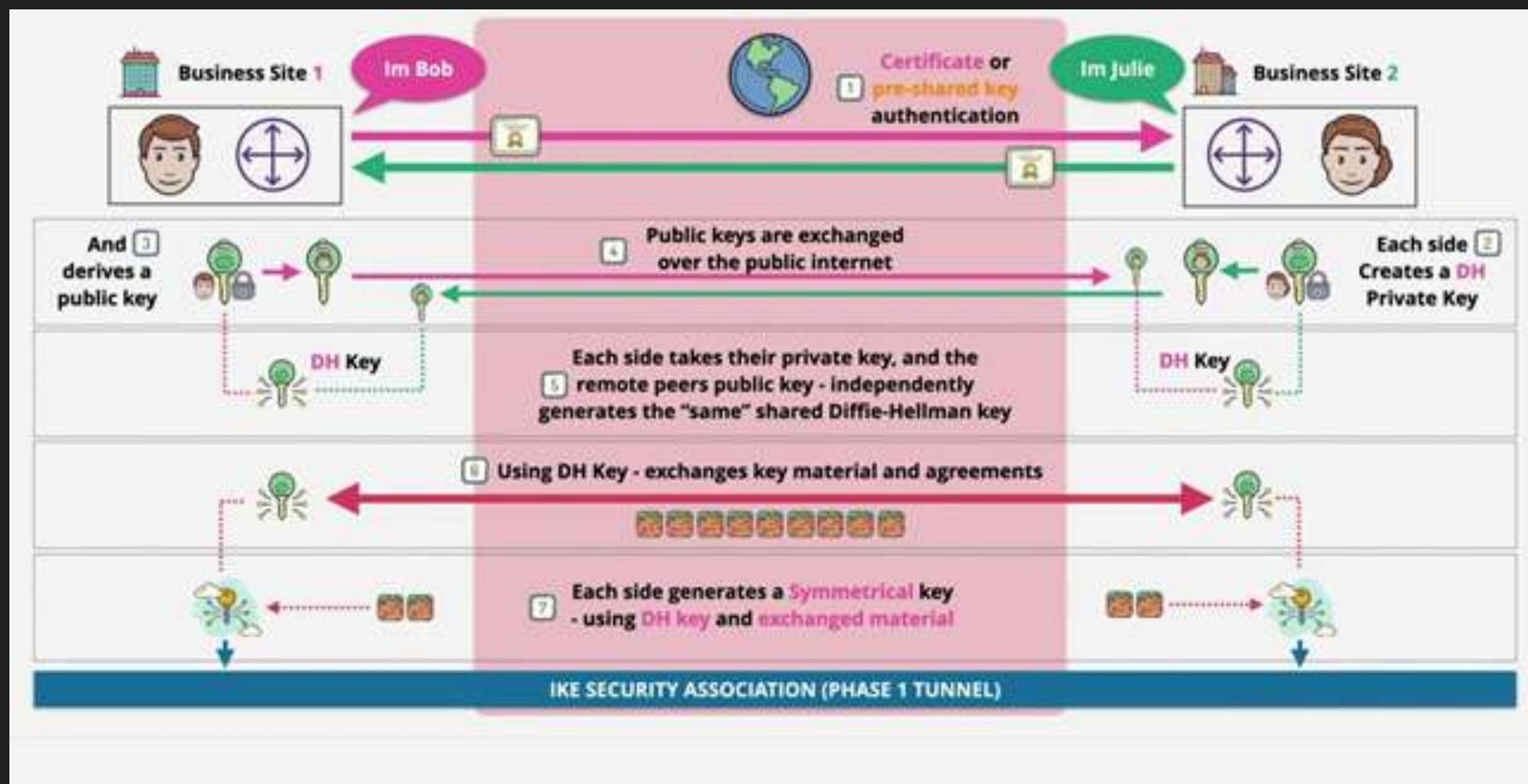












## Phase 2



**Business Site 1**

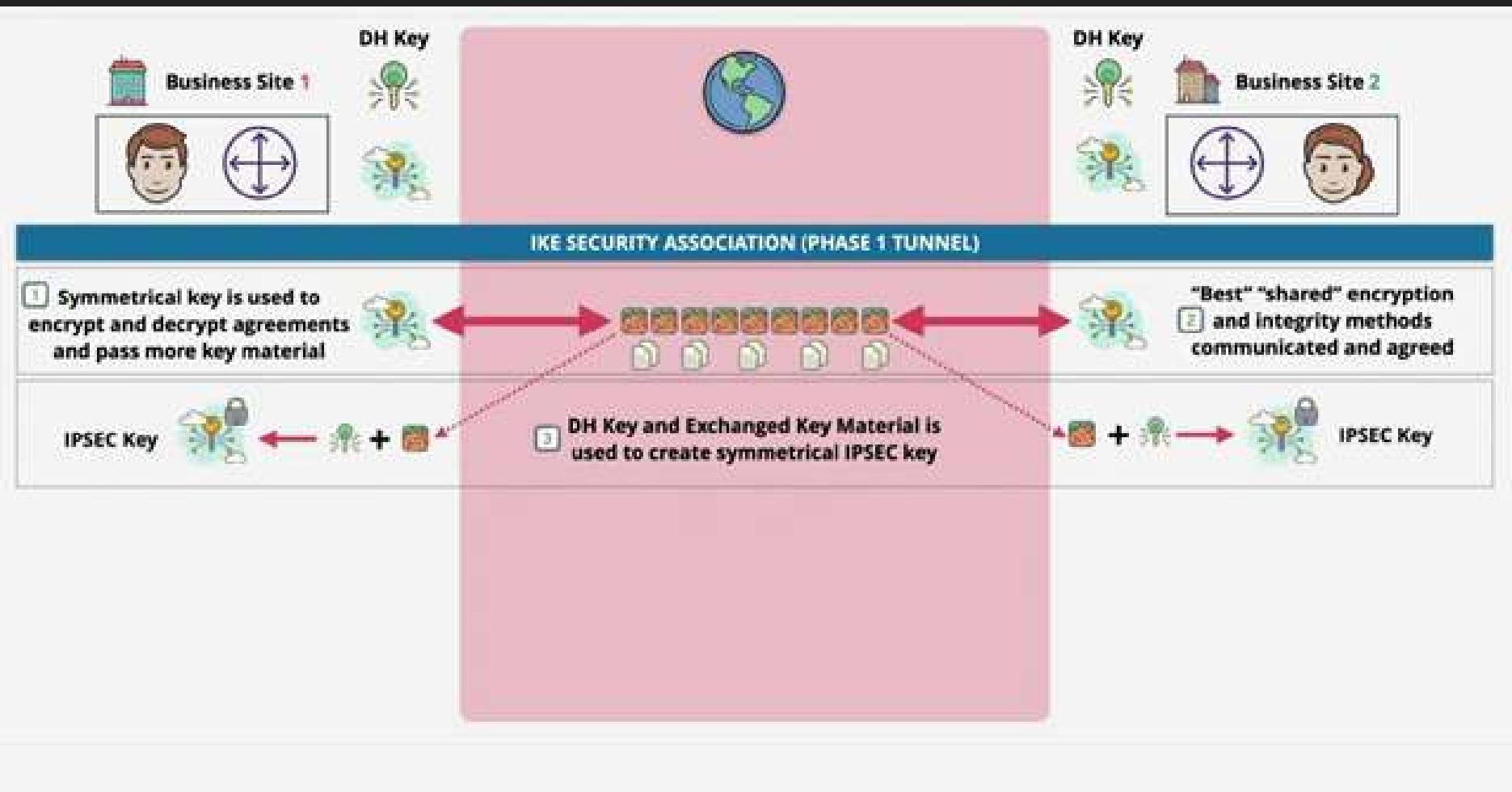


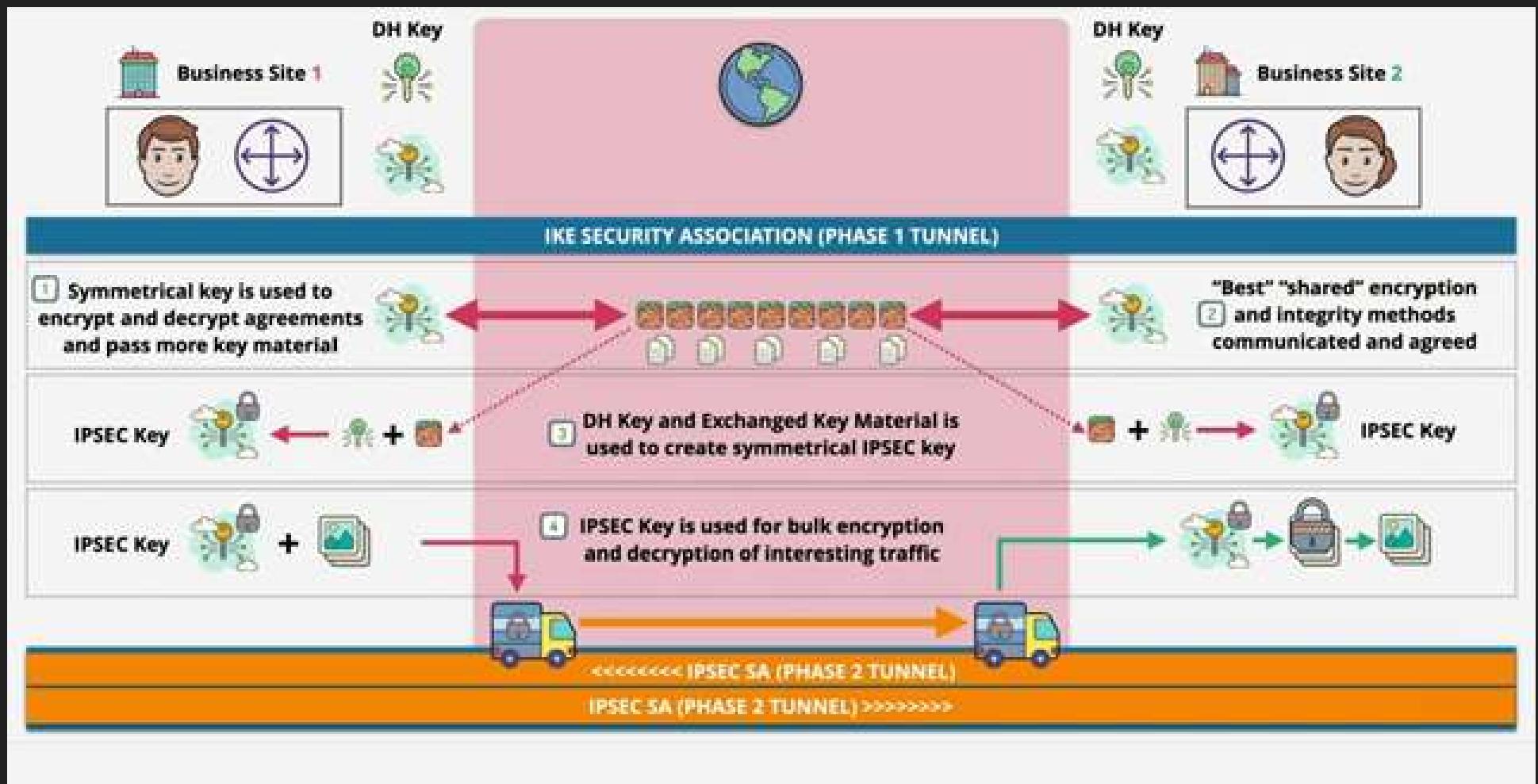
**Business Site 2**







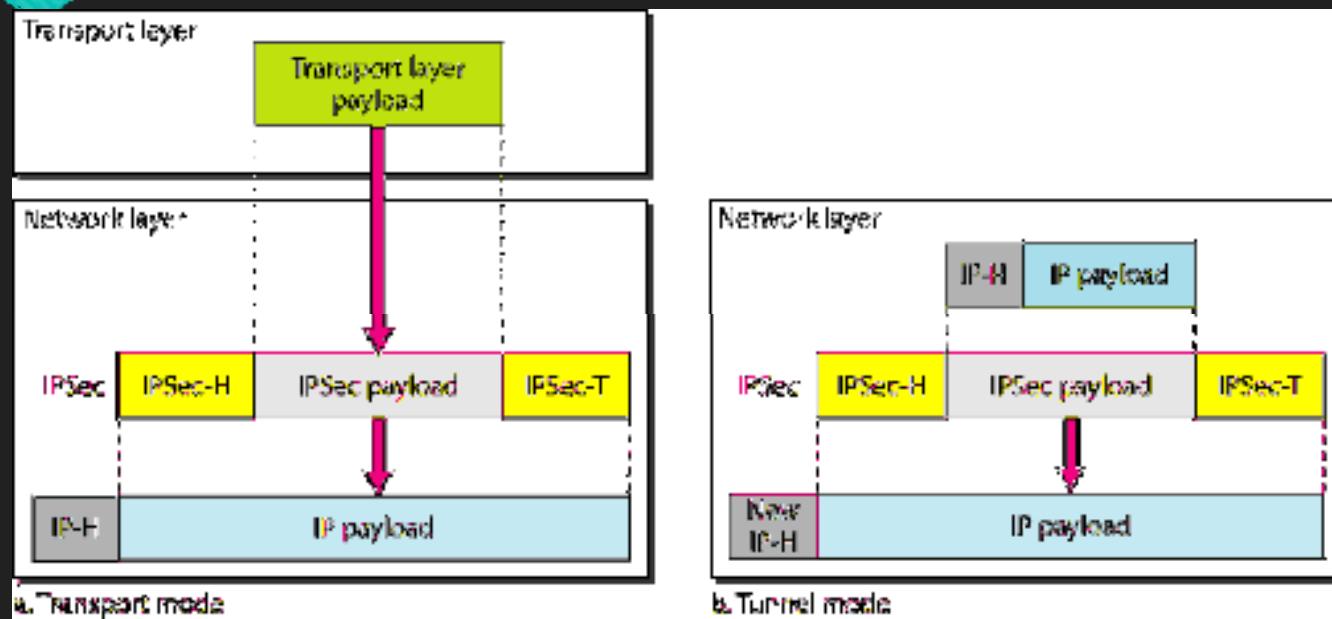




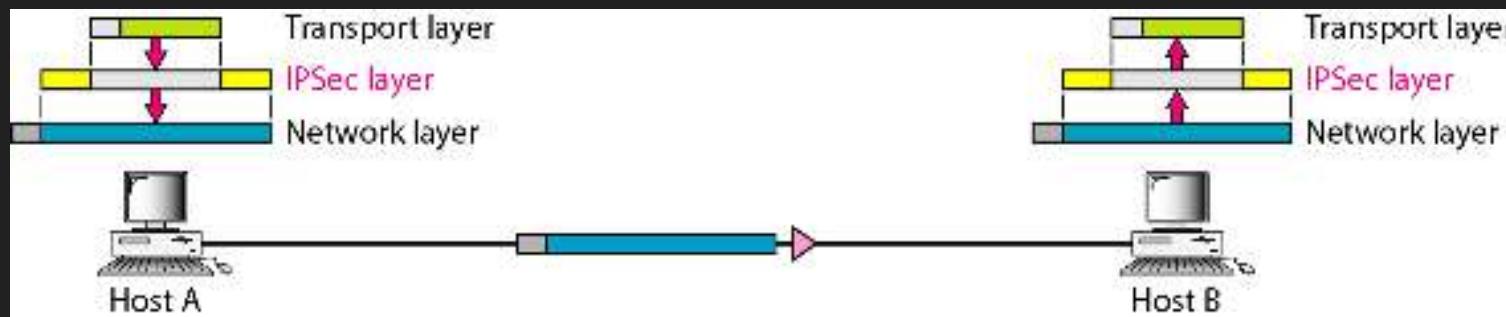
## IPSec Modes

- **Transport** – Secures the payload part of the IP packet, leaves the IP header unsecured. **Commonly used for securing traffic on a LAN.**
- **Tunnel** – Secures the entire IP packet and encapsulates it within a new IP packet. **Commonly used for creating a VPN.**

# IPSec Modes



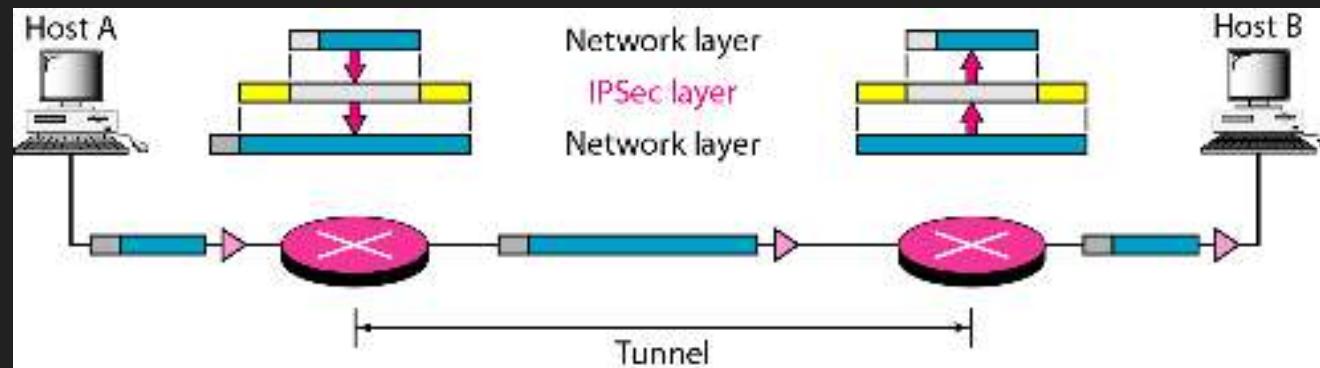
# Transport Modes



*Note*

**IPSec in the transport mode does not protect the IP header; it only protects the information coming from the transport layer.**

# Tunnel Modes



# Tunnel Modes

*Note*

IPSec in tunnel mode protects the original IP header.

# IPSec protocols – AH protocol

- AH - Authentication Header
- Defined in RFC 1826
- Integrity: Yes, including IP header
- Authentication: Yes
- Non-repudiation: Depends on cryptography algorithm.
- Encryption: No
- Replay Protection: Yes

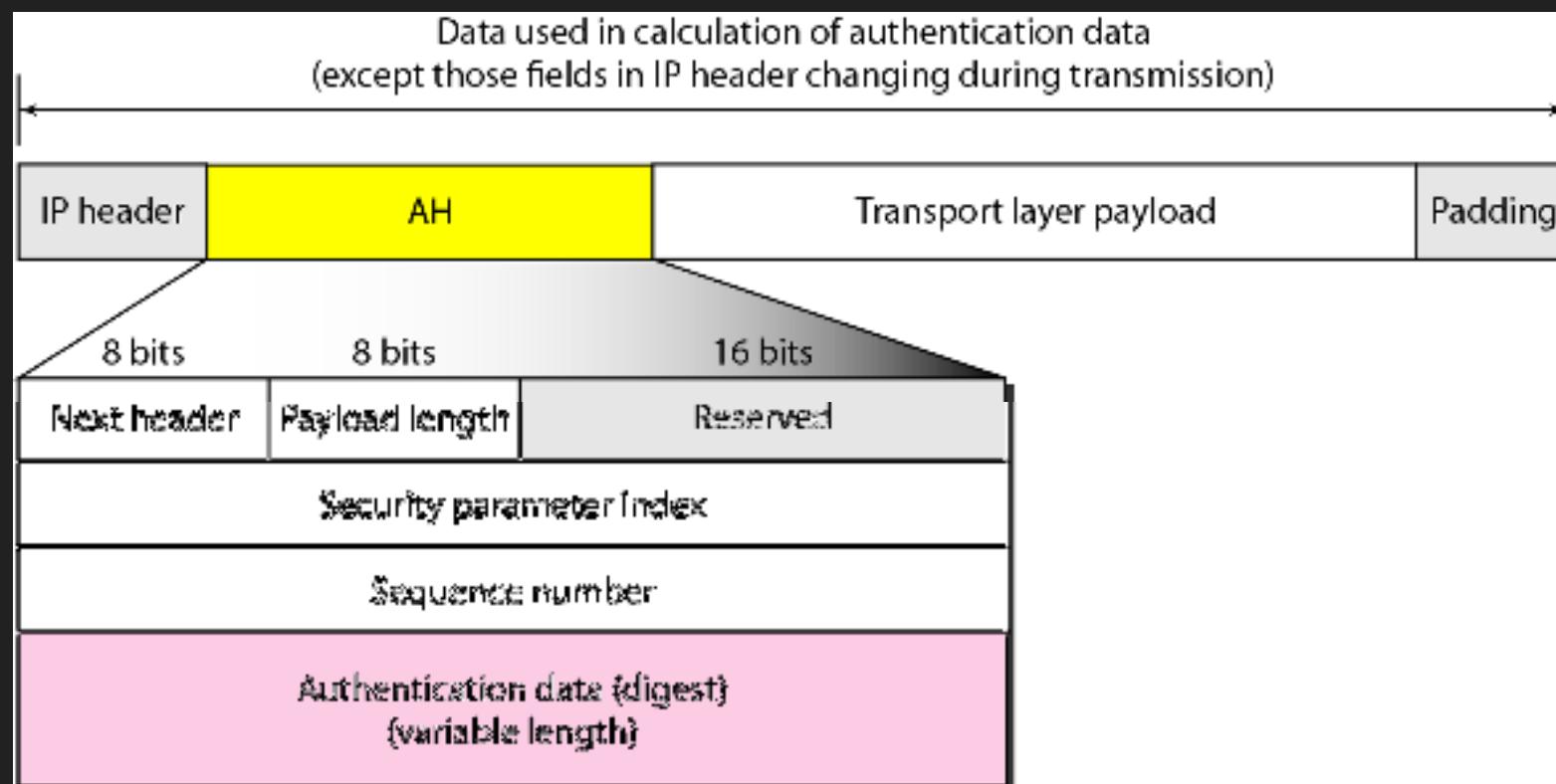
Transport Packet layout

IP Header	AH Header	Payload (TCP, UDP, etc)
-----------	-----------	-------------------------

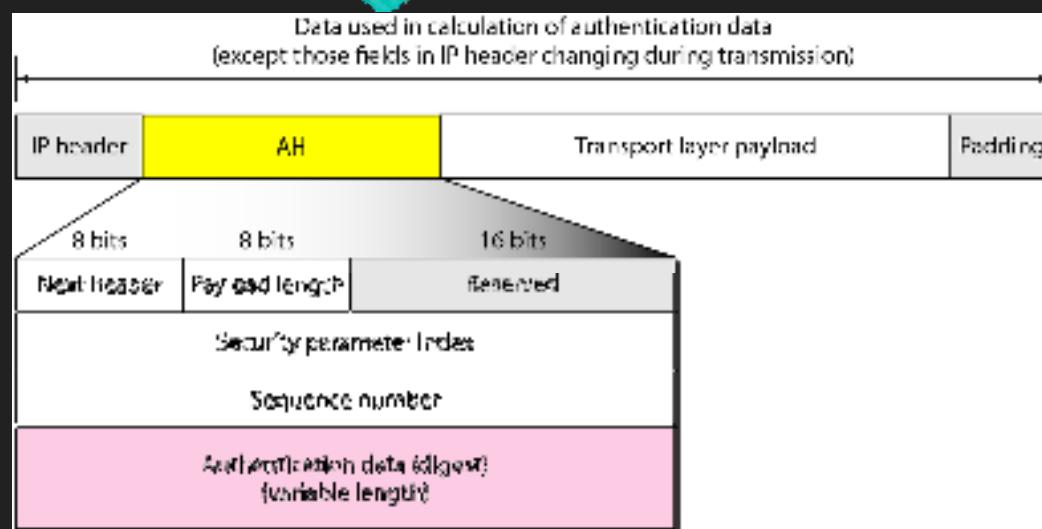
Tunnel Packet layout

IP Header	AH Header	IP Header	Payload (TCP, UDP,etc)
-----------	-----------	-----------	------------------------

## AH protocol in Transport Mode

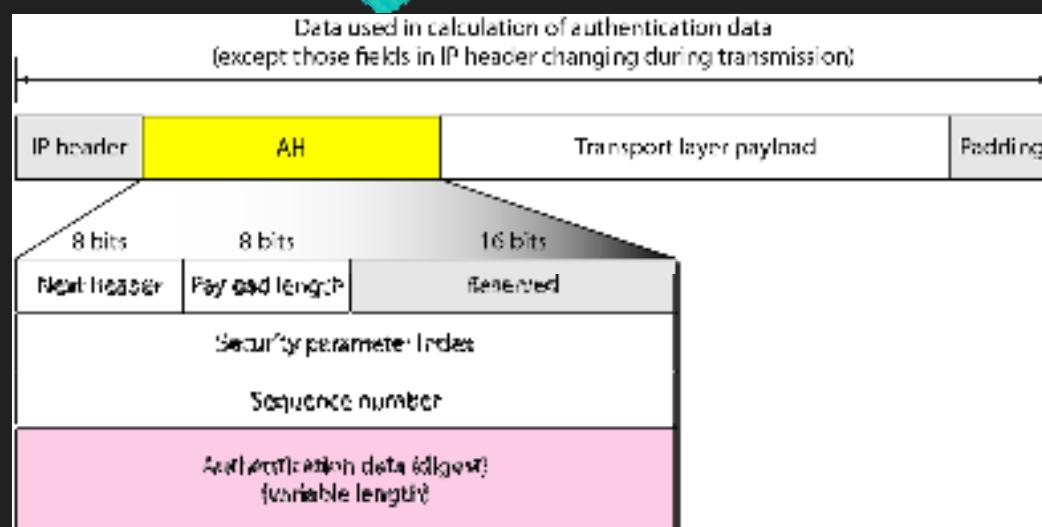


## AH protocol in Transport Mode



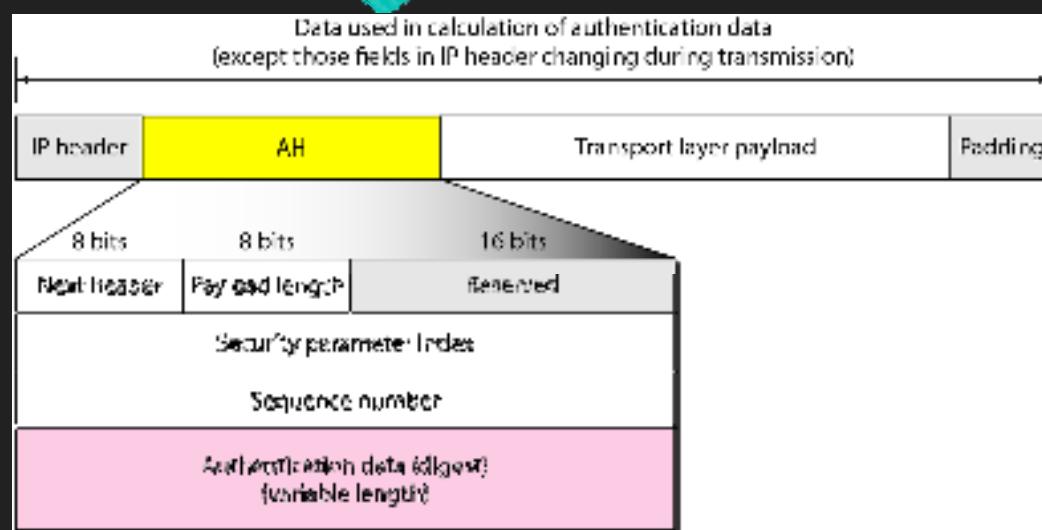
- **Next Header** – Next Header is 8-bit field that identifies type of header present after Authentication Header.
  - In case of TCP, UDP or destination header or some other extension header it will store correspondence IP protocol number .
  - Like, number 4 in this field will indicate IPv4, number 41 will indicate IPv6 and number 6 will indicate TCP.

## AH protocol in Transport Mode



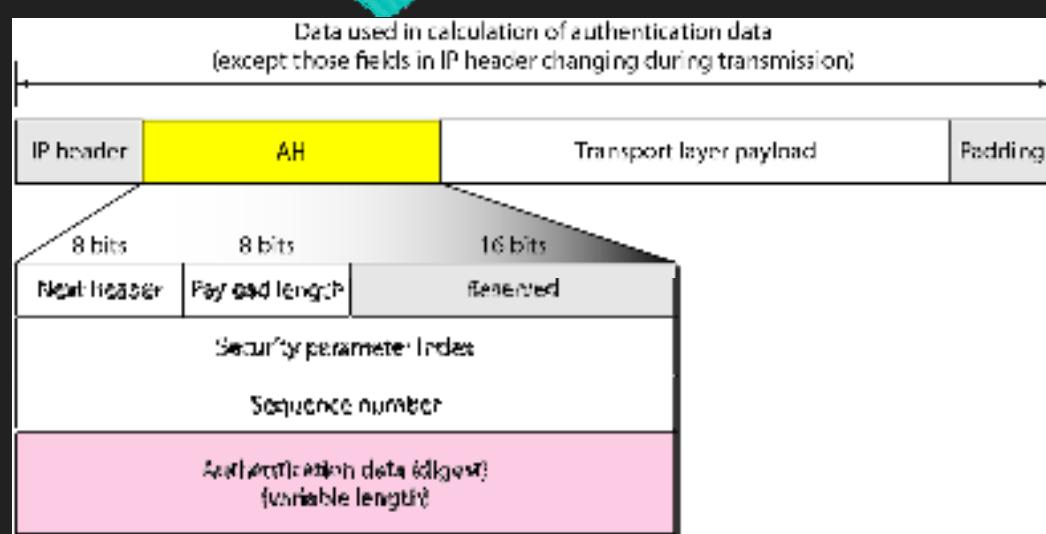
- **Payload Length** – Payload length is length of Authentication header and here we use scaling factor of 4.
  - Whatever be size of header, divide it by 4 and then subtract by 2.
  - We are subtracting by 2 because we're not counting first 8 bytes of Authentication header, which is first two row of picture given above.
  - It means we are not including Next Header, Payload length, Reserved and Security Parameter index in calculating payload length.
  - Like, say if payload length is given to be X. Then  $(X+2)*4$  will be original Authentication header length.

## AH protocol in Transport Mode



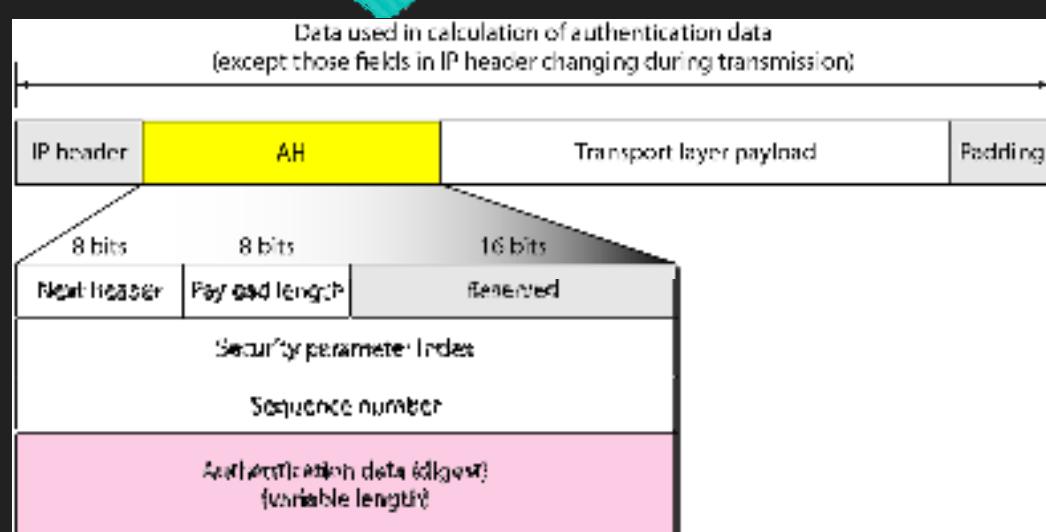
- This is 16-bit field which is set to “zero” by sender as this field is reserved for future use

## AH protocol in Transport Mode



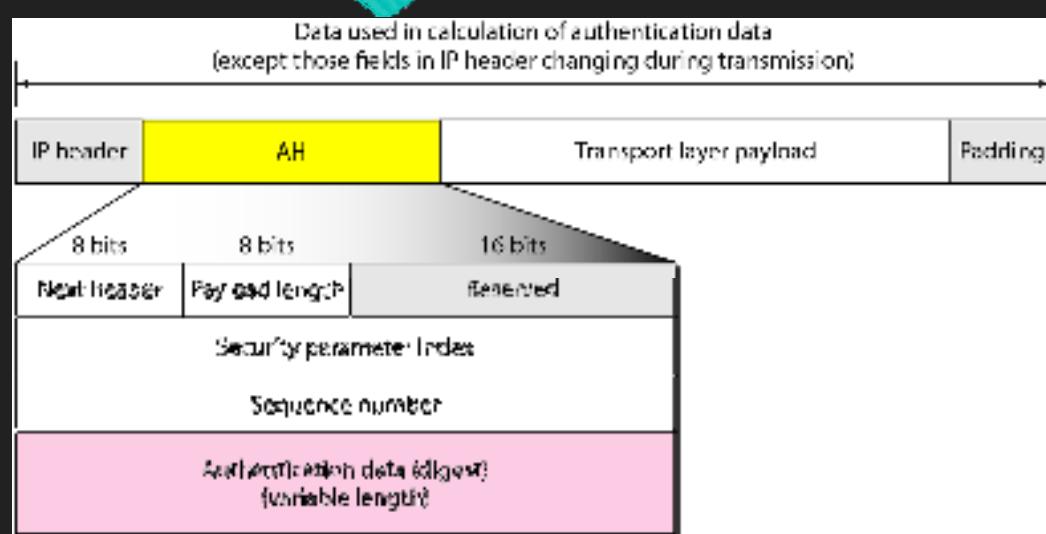
- If we're sending data from Source A to Destination B. Both A and B will already know algorithm and key they are going to use.
  - So for Authentication, hashing function and key will be required which only source and destination will know about.
  - Secret key between A and B is exchanged by method of Diffie Hellman algorithm. So Hashing algorithm and secret key for Security parameter index of connection will be fixed.
  - Before data transfer starts security association needs to be established.
  - In **Security Association**, both parties needs to communicate prior to data exchange. Security association tells what is security parameter index, hashing algorithm and secret key that are being 60 used.

## AH protocol in Transport Mode



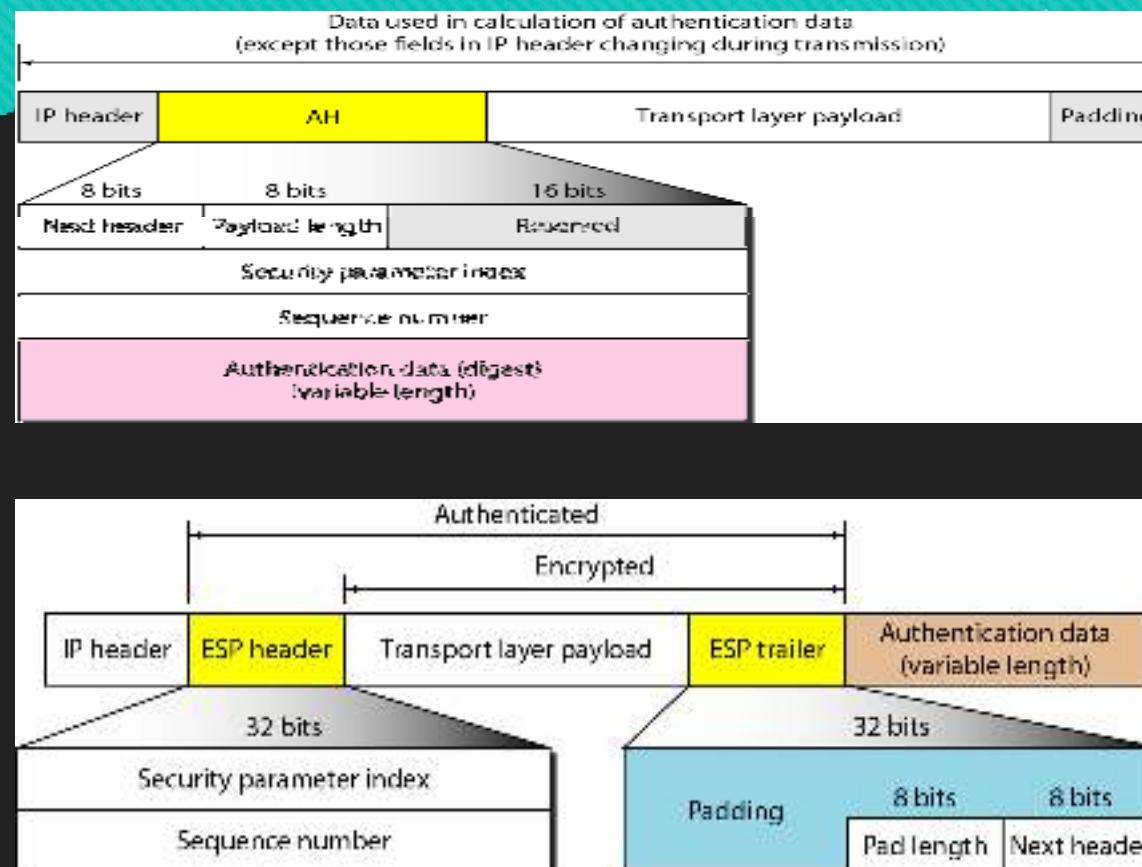
- This unsigned 32-bit field contains counter value that increases by one for each packet sent.
- Every packet will need sequence number. It will start from 0 and will go till  $2^{32} - 1$  and there will be no wrap around.
  - Say, if all sequence numbers are over and none of it is left but we cannot wrap around as it is not allowed.
- So, we will end connection and re-establish connection again to resume transfer of remaining data from sequence number 0.

## AH protocol in Transport Mode



- Authentication data is variable length field that contains Integrity Check Value (ICV) for packet.
- Using hashing algorithm and secret key, sender will create message digest which will be sent to receiver.
- Receiver on other hand will use same hashing algorithm and secret key. If both message digest matches then receiver will accept data.

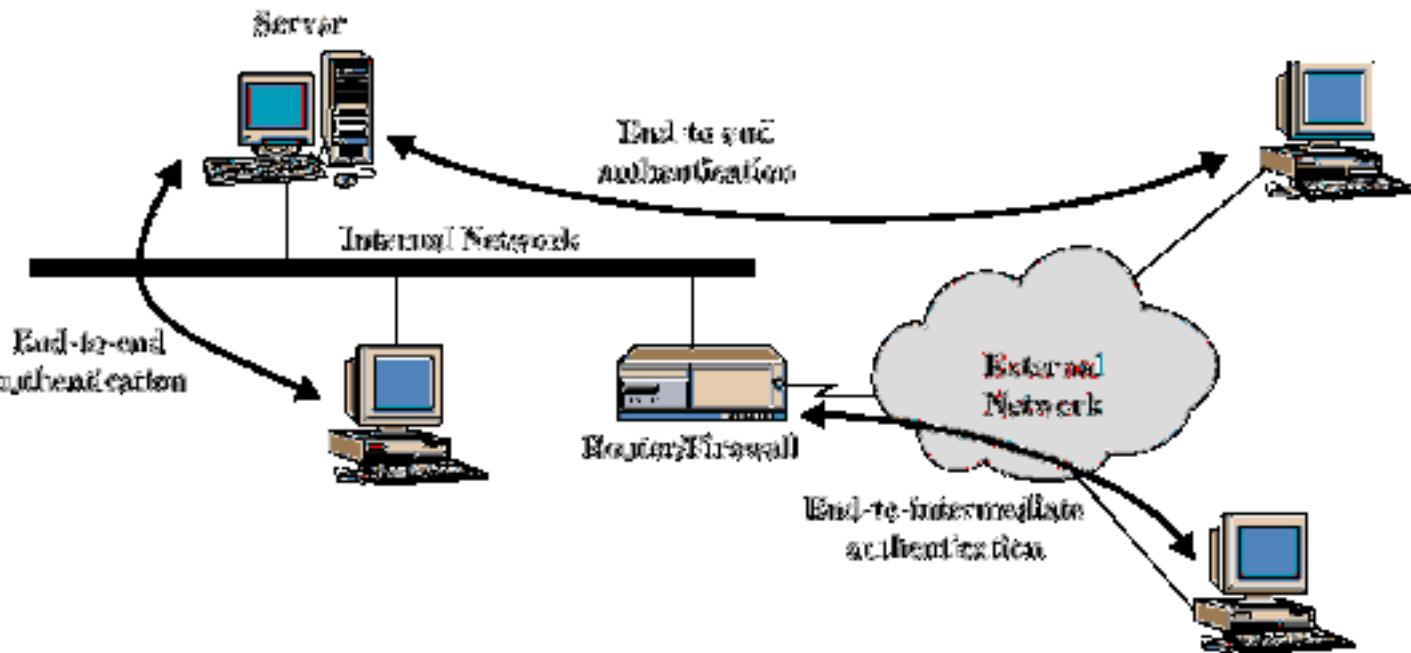
## AH & ESP



*Note*

**The AH Protocol provides source authentication and data integrity, but not privacy.**

# End-to-end versus End-to-Intermediate Authentication



# IPSec protocols – ESP protocol

- ESP – Encapsulating Security Payload
  - Defined in RFC 1827
  - Integrity: Yes
  - Authentication: Depends on cryptography algorithm.
  - Non-repudiation: No
  - Encryption: Yes
  - Replay Protection: Yes

Transport Packet layout

IP Header	ESP Header	Payload (TCP, UDP, etc)	
-----------	------------	-------------------------	--

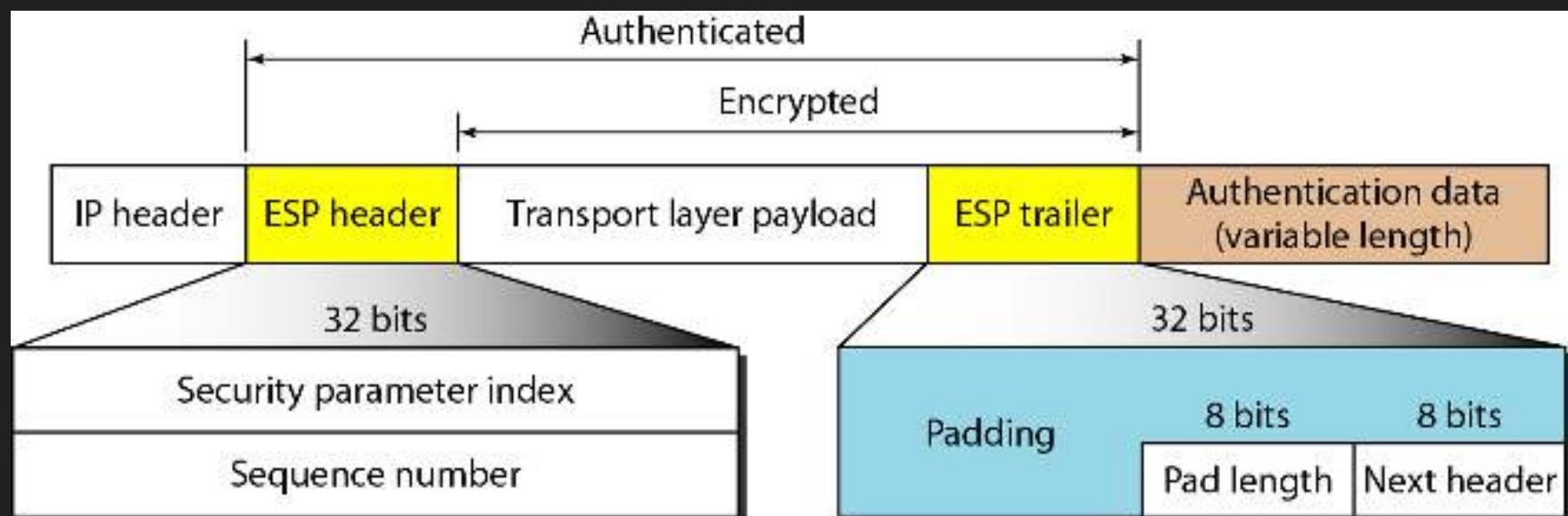
Tunnel Packet layout

IP Header	ESP Header	IP Header	Payload (TCP, UDP,etc)
-----------	------------	-----------	------------------------

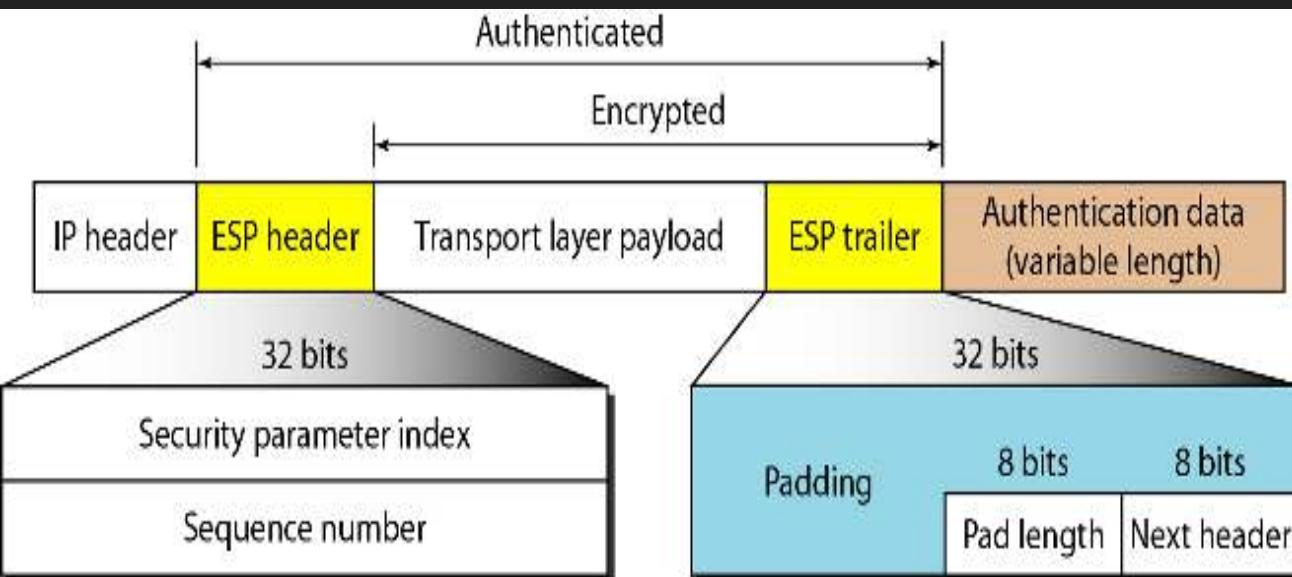
Unencrypted

Encrypted

## ESP protocol in Transport Mode



## ESP protocol in Transport Mode



- **Security Parameters Index (SPI):** this is used to identify the security association (SA) that is used to protect the packet.

- **Sequence Number:** this is used to provide anti-replay protection by ensuring that packets are received in the correct order and have not been duplicated or replayed.

- **Padding:** optional padding that is added to the packet to meet cryptographic requirements. 68

*Note*

**ESP provides source authentication,  
data integrity, and privacy.**

# What protocol to use?

- Differences between AH and ESP:
  - ESP provides encryption, AH does not.
  - AH provides integrity of the IP header, ESP does not.
  - AH can provide non-repudiation. ESP does not.
- However, we don't have to choose since both protocols can be used in together.
- Why have two protocols?
  - Some countries have strict laws on encryption. If you can't use encryption in those countries, AH still provides good security mechanisms. Two protocols ensures wide acceptance of IPSec on the Internet.

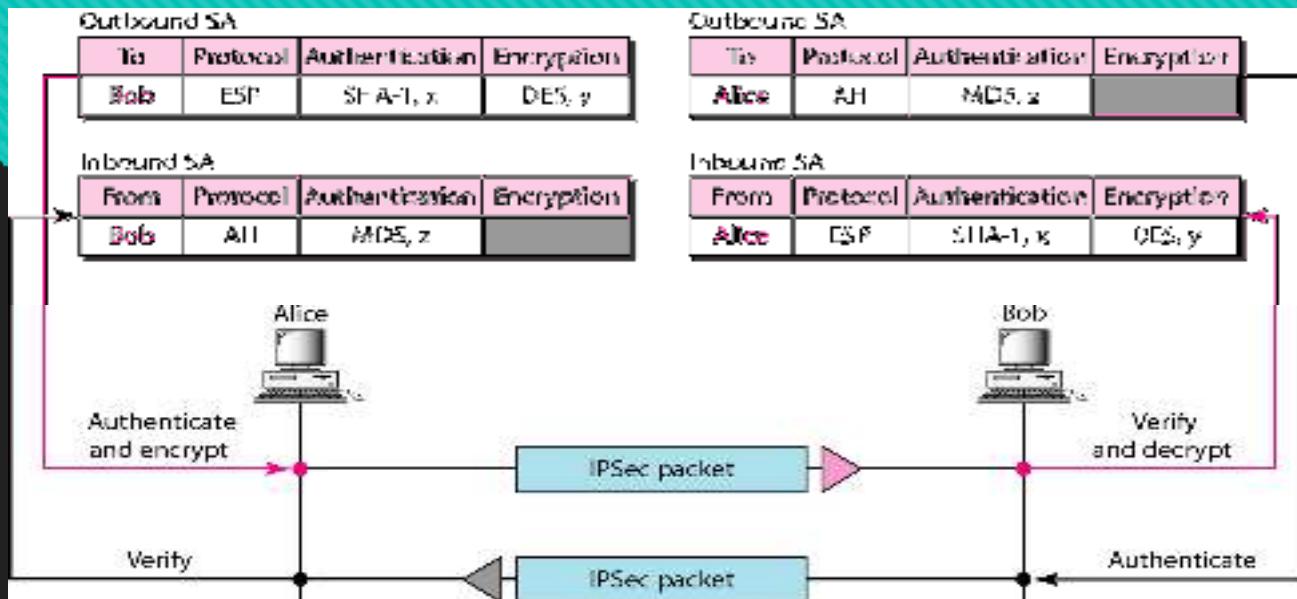
# Security Associations

- ◎ One of the most important concepts in IPSec is called a Security Association (SA). Defined in RFC 1825.
- ◎ SAs are the combination of a given Security Parameter Index (SPI) and Destination Address.
- ◎ SAs are one way. A minimum of two SAs are required for a single IPSec connection.
- SAs contain parameters including:
  - Authentication algorithm and algorithm mode
  - Encryption algorithm and algorithm mode
  - Key(s) used with the authentication/encryption algorithm(s)
  - Lifetime of the key
  - Lifetime of the SA
  - Source Address(es) of the SA
  - Sensitivity level (ie Secret or Unclassified)

## Example

- A security is a very complex set of pieces of information. However, we can show the simplest case in which Alice wants to have an association with Bob for use in a two-way communication.
- Alice can have an outbound association (for datagrams to Bob) and an inbound association (for datagrams from Bob). Bob can have the same. In this case, the security associations are reduced to two small tables for both Alice and Bob.

# Example



- The figure shows that when Alice needs to send a datagram to Bob, she uses the ESP Protocol of IPsec. Authentication is done by using SHA-1 with key X. The encryption is done by using DES with key Y. When Bob needs to send a datagram to Alice, he uses the AH Protocol of IPsec.
- Authentication is done by using MD5 with key z. Note that the inbound association for Bob is the same as the outbound association for Alice, and vice versa.

# How IPSec works: Phase 1

- Internet Key Exchange (IKE) is used to setup IPSec.
- IKE Phase 1:
  - Establishes a secure, authenticated channel between the two computers
  - Authenticates and protects the identities of the peers
  - Negotiates what SA policy to use
  - Performs an authenticated shared secret keys exchange
  - Sets up a secure tunnel for phase 2
  - Two modes: **Main mode** or **Aggressive mode**
- Main Mode IKE
  1. Negotiate algorithms & hashes.
  2. Generate shared secret keys using a Diffie-Hillman exchange.
  3. Verification of Identities.
- Aggressive Mode IKE
  - Squeezes all negotiation, key exchange, etc. into less packets.
  - Advantage: Less network traffic & faster than main mode.
  - Disadvantage: Information exchanged before a secure channel is created. Vulnerable to sniffing.

## How IPSec works: Phase 2

- An AH or ESP packet is then sent using the agreed upon “main” SA during the IKE phase 1.
- IKE Phase 2
  - Negotiates IPSec SA parameters
  - Establishes IPSec security associations for specific connections (like FTP, telnet, etc)
  - Renegotiates IPSec SAs periodically
  - Optionally performs an additional Diffie-Hellman exchange

## How IPSec works: Communication

- Once Phase 2 has established an SA for a particular connection, all traffic on that connection is communicated using the SA.
- IKE Phase 1 exchange uses UDP Port 500.
- AH uses IP protocol 51.
- ESP uses IP protocol 50.

## Question

Can IPSec using AH be used in transport mode if one of the machines is behind a NAT box? Explain your answer.

# Question

Can IPSec using AH be used in transport mode if one of the machines is behind a NAT box? Explain your answer.

No.

AH in transport mode includes the IP header in the checksum. The NAT box changes the source address, ruining the checksum. All packets will be perceived as having errors.

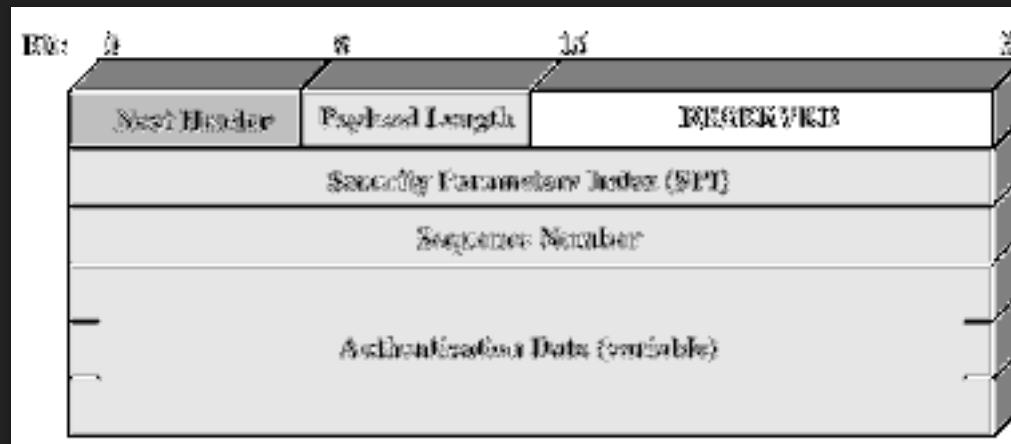
# Security Associations

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

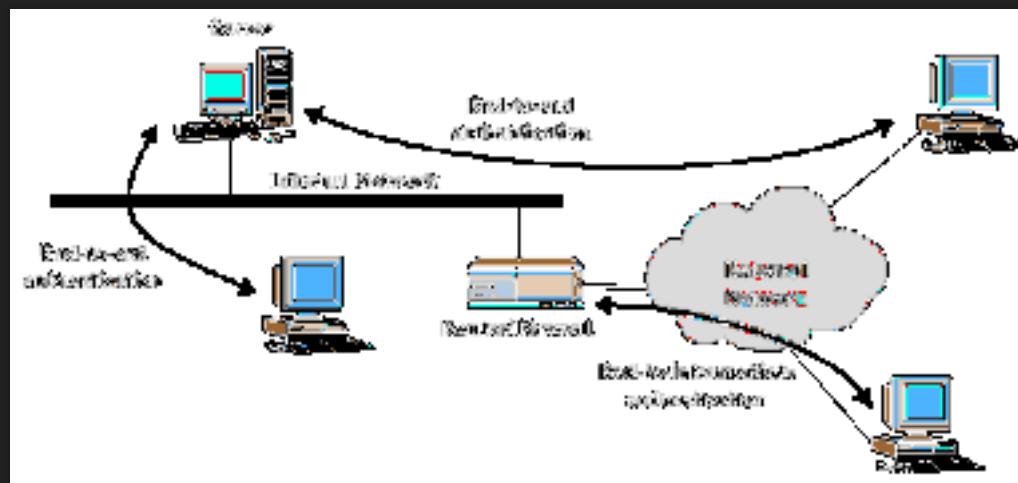
# Authentication Header (AH)

- provides support for data integrity & authentication of IP packets
  - end system/router can authenticate user/app
  - prevents address spoofing attacks by tracking sequence numbers
- based on use of a MAC
  - HMAC-MD5-96 or HMAC-SHA-1-96
- parties must share a secret key

# Authentication Header



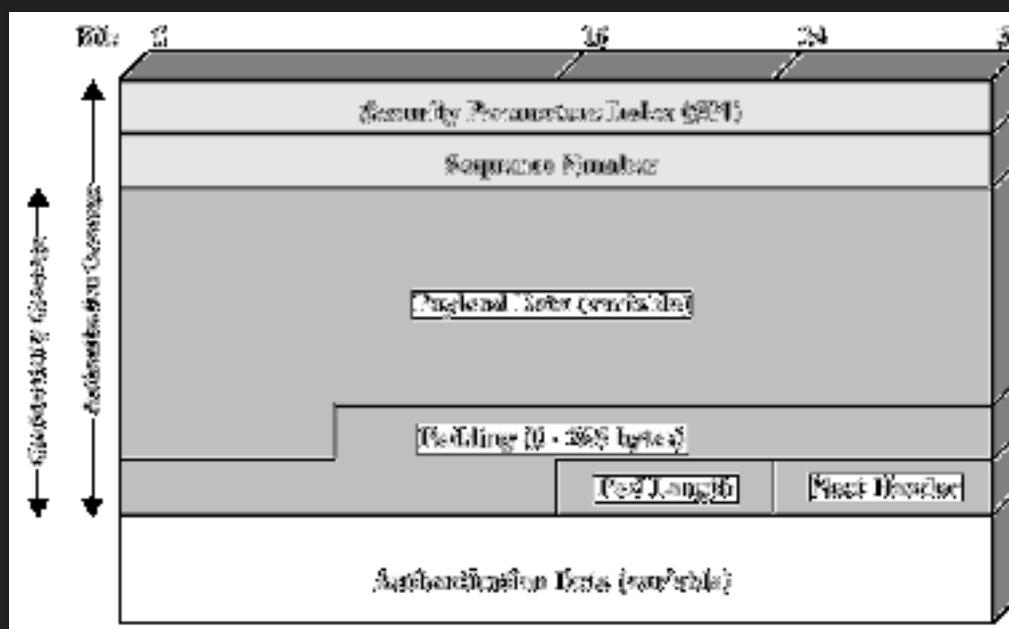
# Transport & Tunnel Modes



## Encapsulating Security Payload (ESP)

- provides message content confidentiality & limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- supports range of ciphers, modes, padding
  - incl. DES, Triple-DES, RC5, IDEA, CAST etc
  - CBC most common
  - pad to meet blocksize, for traffic flow

# Encapsulating Security Payload



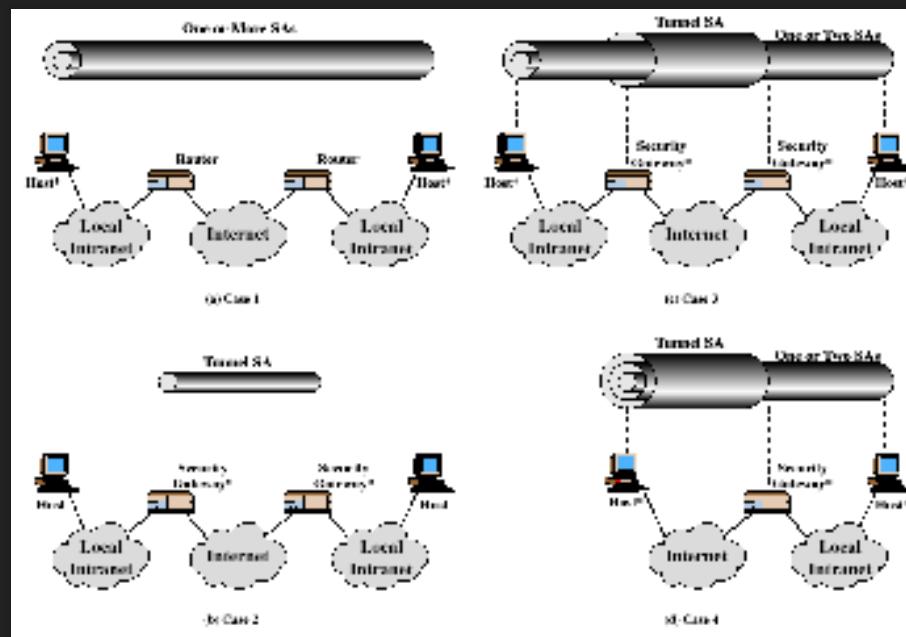
# Transport vs Tunnel Mode ESP

- transport mode is used to encrypt & optionally authenticate IP data.
  - data protected but header left in clear
  - can do traffic analysis but is efficient
  - good for ESP host to host traffic
- tunnel mode encrypts entire IP packet
  - add new header for next hop
  - good for VPNs, gateway to gateway security

# Combining Security Associations

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

# Combining Security Associations



## Question

- Why does IPSec need a security association?

# Key Management

- handles key generation & distribution
- typically need 2 pairs of keys
  - 2 per direction for AH & ESP
- manual key management
  - sysadmin manually configures every system
- automated key management
  - automated system for on demand creation of keys for SA's in large systems
  - has Oakley & ISAKMP elements

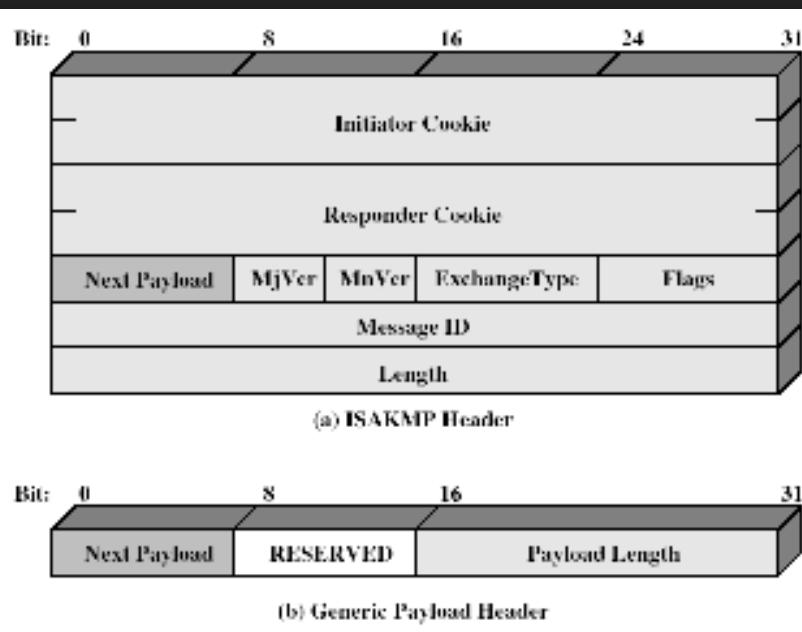
# Oakley

- ⌚ a key exchange protocol
- based on Diffie-Hellman key exchange
- adds features to address weaknesses
  - cookies, groups (global params), nonces, DH key exchange with authentication
- can use arithmetic in prime fields or elliptic curve fields

# ISAKMP

- Internet Security Association and Key Management Protocol
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify, & delete SAs
- independent of key exchange protocol, encryption alg, & authentication method

# ISAKMP



# Summary

• have considered:

- IPSec security framework
- AH
- ESP
- key management & Oakley/ISAKMP

---

# **THE IPSEC PROTOCOL SUITE**

# IPSEC

---

- ✖ IPsec is a suite of protocols. It consists of:
  - + Protocols that provide encryption-authenticity of the data stream (ESP, AH)
  - + Protocols that implement the *initial* key exchange to realize the encrypted stream (+ ISAKMP IKE).

# SET UP IPSEC (1)

<http://www.unixwiz.net/techtips/iguide-ipsec.html#flavors>

## ✖ AH vs ESP

### + AH (authenticate)

- ✖ provides authentication and message integrity, but it does not provide confidentiality

### + ESP (encrypt+authenticate)

- ✖ provides authentication, confidentiality and message integrity check

# **SET UP IPSEC (2)**

- ✖ Tunnel mode vs Transport mode

IPsec supports two modes of operation

- + Transport Mode

- ✖ provides a secure connection between two endpoints (host-to-host)
- ✖ Only the IP's payload is encrypted and not the header
- ✖ Computationally lighter

- + Tunnel Mode

- ✖ gateway-to-gateway connection
- ✖ the entire IP packet is encrypted
- ✖ computationally expensive
- ✖ only the gateway needs support of the Ipsec suite

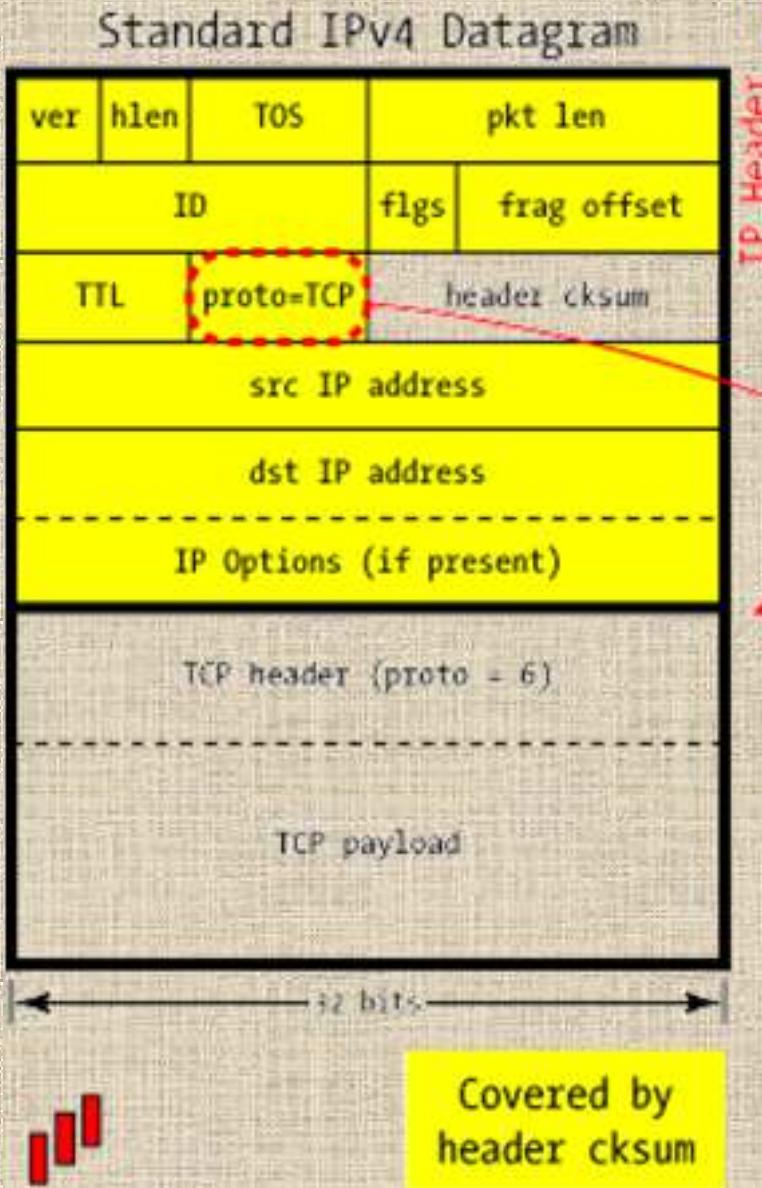
# SET UP IPSEC (3)

- ✖ MD5 vs SHA-1 vs DES vs 3DES vs AES vs blah blah blah
  - + Encryption methods:
    - ✖ *In Authentication mode*, ciphers are used to calculate an Integrity Check Value (ICV) over the packet's contents. ICV it's usually built on top of a cryptographic hash such as MD5 or SHA-1. It incorporates a secret key known to both ends, and this allows the recipient to compute and check the ICV in the same way.
    - ✖ *In Encryption mode*, ciphers are used with a secret key to encrypt the data before transmission (algorithms such as DES, 3DES, Blowfish, AES).

# SET UP IPSEC (4)

- ✖ IKE vs manual keys
  - + The Internet Key Exchange protocol is used to establish a *security association* (SA)
    - ✖ used to establish a *shared session secret*, that is, a shared key corresponding to the session to be established
    - ✖ from the shared secret are then derived encryption keys that will be used for the next communication.
  - + Manual keys require manual entry of the secret values for key exchange (occurs out-of-band)
- ✖ Main mode vs aggressive mode
  - + efficiency-versus-security tradeoff during the initial key exchange (IKE).
    - ✖ *Main mode* requires 6 packets back and forth, but affords complete security during the establishment of an IPsec connection
    - ✖ *Aggressive Mode* uses half the exchanges providing a bit less security because some information is transmitted in cleartext.

# STANDARD IP DATAGRAM (1)



<http://www.unixwiz.net/techtips/iguide-ipsec.html#ip>

**ver**

version of the protocol

**hlen**

IP Header length, as a four-bit quantity of 32-bit words. A standard IPv4 header is always 20 bytes long (5 words).

**TOS**

Type of Service. Specifies how the datagram should be handled (optimize for bandwidth? Latency? Low cost? Reliability?)

**pkt len**

Overall packet length in bytes (up to 65535). This count includes the bytes of the header.

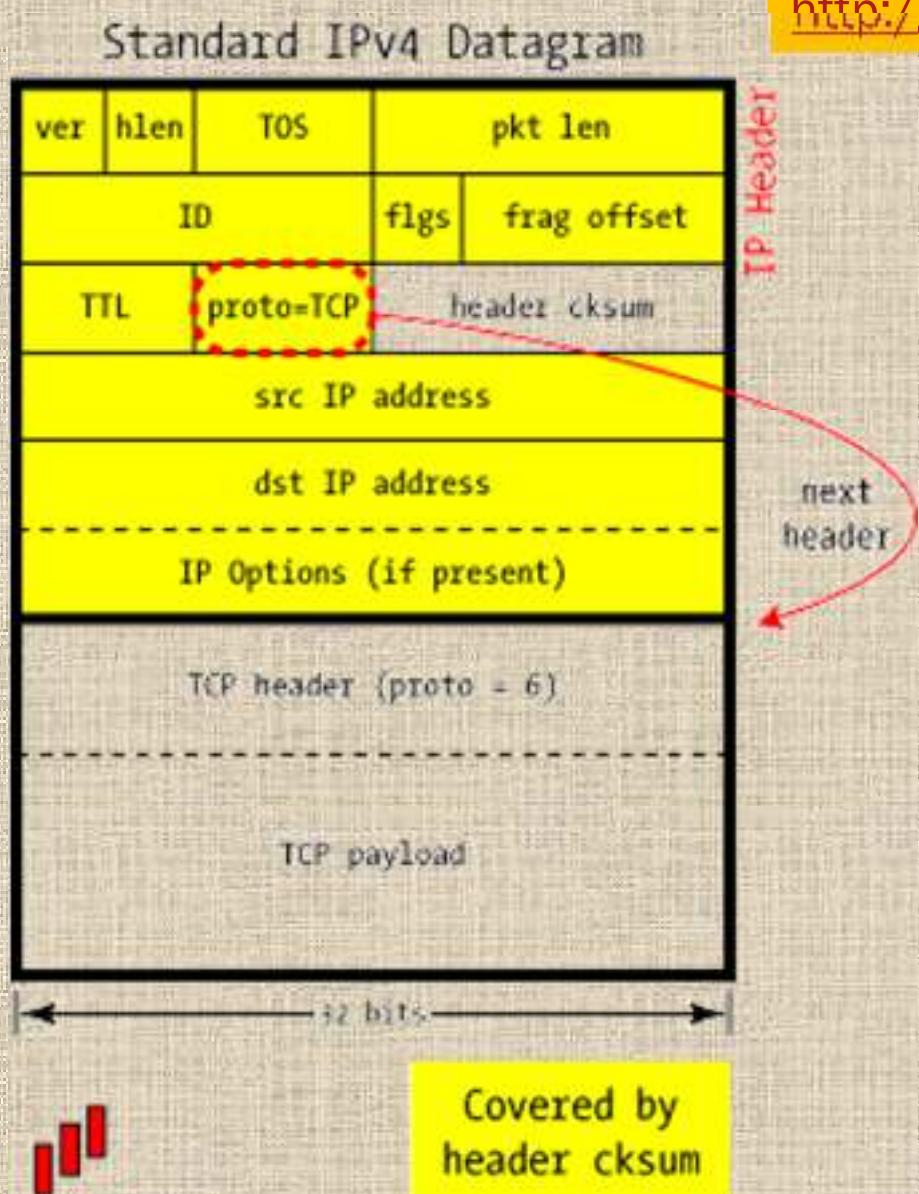
**ID**

Used to associate related packets that have been fragmented

**flgs**

Bits used for control and protocol datagram fragmentation

# STANDARD IP DATAGRAM (2)



<http://www.unixwiz.net/techtips/iguide-ipsec.html#ip>

## frag offset

tells the offset (measured in blocks of 8 bytes) of a particular fragment

## TTL

This is the *Time to Live* of the datagram.

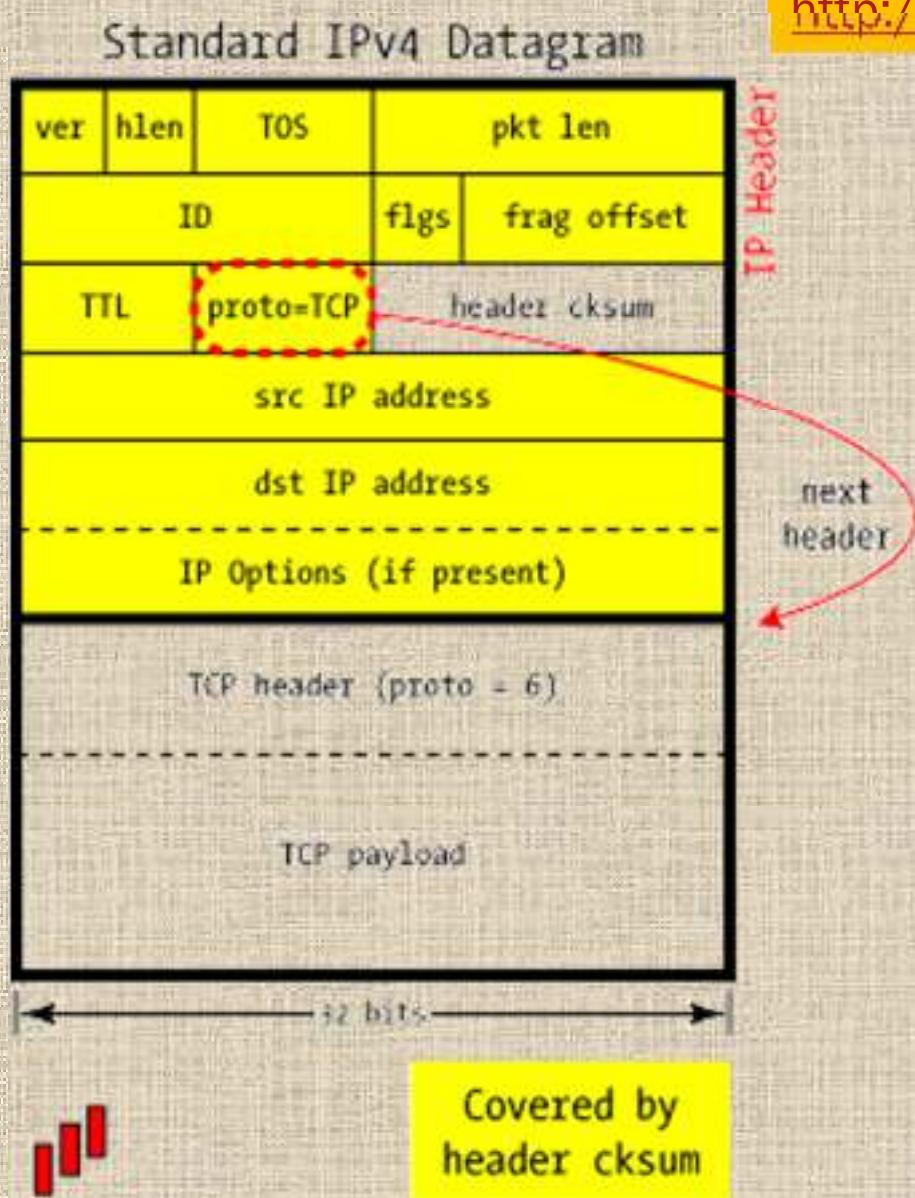
## proto

Shows the code associated with the protocol used in the data field of the IP datagram, for example the TCP protocol is associated with the code 6, for UDP code 17. Other protocols (47, GRE, 50, ESP, 51, AH)

## header checksum

it's designed to detect errors in transit. This is not a *cryptographic* checksum, and it doesn't cover any part of the datagram that follow the IP header.

# STANDARD IP DATAGRAM (3)



<http://www.unixwiz.net/techtips/iguide-ipsec.html#ip>

## src IP address

Shows the *IP address associated with the host of the sender of the datagram* (32-bit)

## dst IP address

Shows the *IP address associated with the host of the recipient of the datagram*

## IP Options

Options (optional and not used a lot) for more specific uses of the protocol.

## Payload

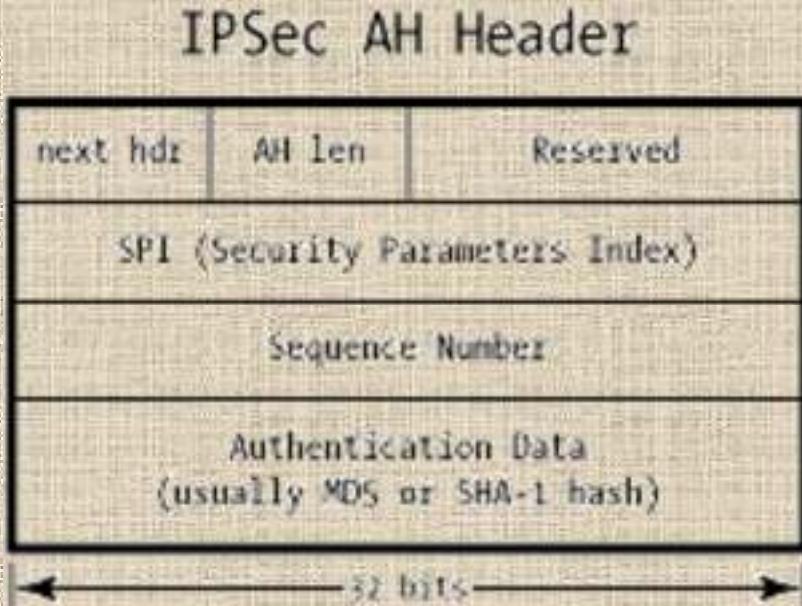
Data in transit.

# AH: AUTHENTICATION ONLY (1)

- ✖ AH is used to authenticate, but not encrypting, IP traffic
  - + serves the purpose of ensuring that we're really talking to who we think we are, detecting alteration of data while in transit, and (optionally) to guard against replay by attackers who capture data from the wire and attempt to re-inject that data back onto the wire at a later date
- ✖ Authentication...
  - + ...is performed by computing a cryptographic hash-based message authentication code over nearly all the fields of the IP packet (excluding those which might be modified in transit, such as TTL or the header checksum), and stores this in a newly-added AH header

# AH: AUTHENTICATION ONLY (2)

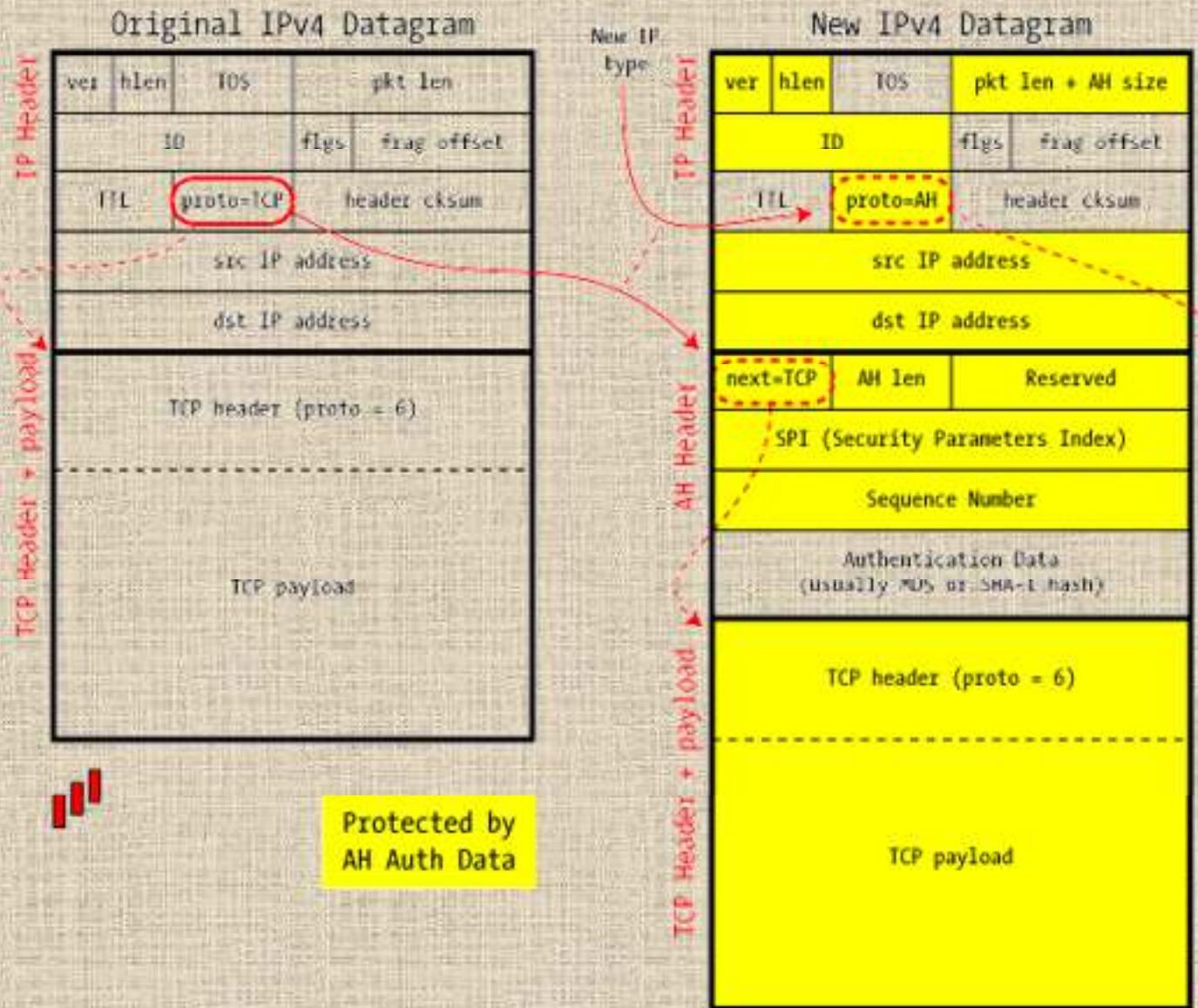
<http://www.unixwiz.net/techtips/iguide-ipsec.html#ah>



- ✖ next hdr
  - + This identifies the protocol type of the following payload.
- ✖ AH len
  - + Defines the length of the whole AH header
- ✖ Reserved
  - + This field is reserved for future use and must be zero.
- ✖ Security Parameters Index
  - + identifies the parameters of current security combined with the pair of IP addresses.
- ✖ Sequence Number
  - + This is a monotonically increasing identifier that's used to assist in anti-replay protection.
- ✖ Authentication Data
  - + Contains the Integrity Check Value (ICV)

# AH TRANSPORT MODE (1)

IPSec in AH Transport Mode



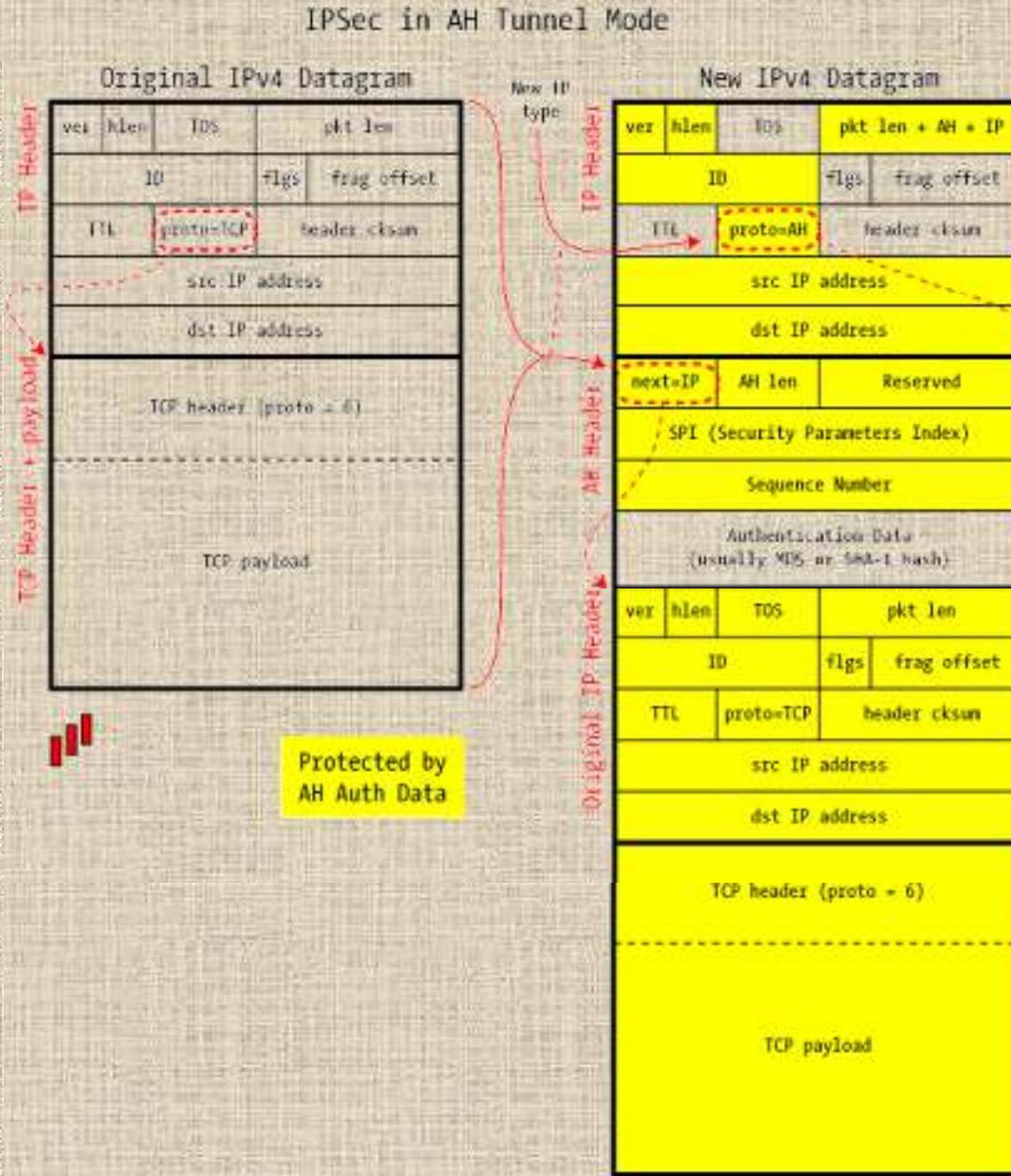
## AH TRANSPORT MODE (2)

- ✖ It's used to protect an end-to-end conversation between two hosts.
  - + This protection guarantees authentication only.
  - + Only the payload of the IP datagram is handled by IPsec, inserting an header between the IP header and the upper levels

# AH TRANSPORT MODE (3)

- ✖ When traffic is protected using AH in transport mode, AH is added as a new header between the IP header and the payload protocol (TCP, UDP, etc.).
- ✖ The IP header is changed to indicate that the next header to be treated is the AH protocol (next header field)
- ✖ Then the entire resulting IP packet, with the exception of some mutable IP header field, is authenticated by the hashing process and sent to the destination
- ✖ When the packet arrives at its destination and passes the authentication, the AH header is removed and the field Proto = AH header in the IP header is replaced with “Next Protocol”

# AH TUNNEL MODE (1)



## AH TUNNEL MODE (2)

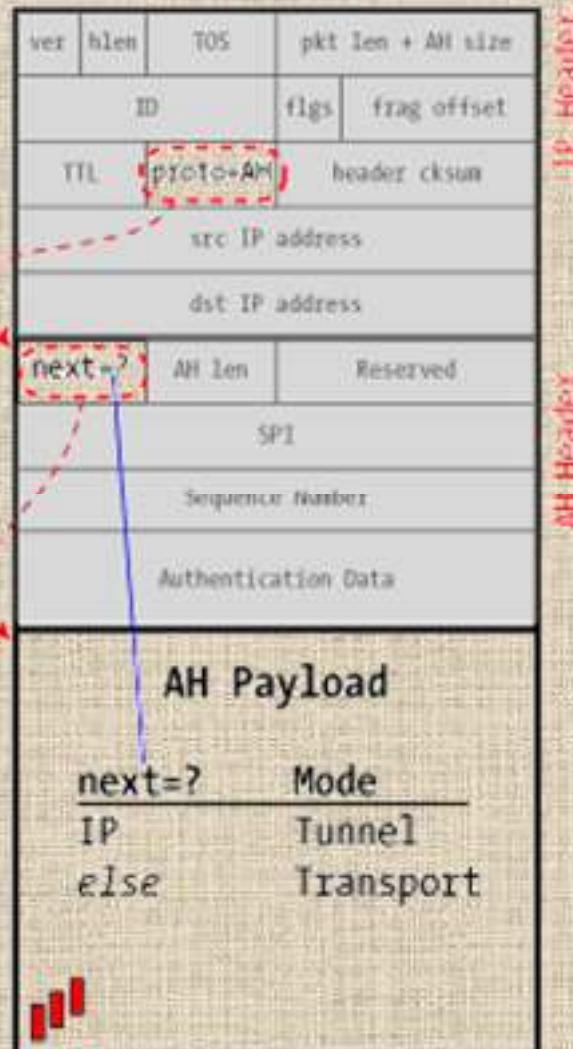
- ✖ In tunnel mode a IP datagram is fully encapsulated in a new IP datagram using IPSec.
  - + the packet is sealed with an Integrity Check Value to authenticate the sender and to prevent modification in transit
  - + it encapsulates the *full IP header* as well as the payload, and this allows the source and destination addresses to be different from those of the encompassing packet (this allows formation of a tunnel)

## AH TUNNEL MODE (3)

- ✖ When the packet arrives at its destination, after the authentication check, the entire IP header and AH are stripped off
  - + The reconstituted packet could be delivered to the local machine or routed elsewhere (according to the destination IP address found in the encapsulated packet)
- ✖ *Transport mode* is used strictly to secure an end-to-end connection between two computers
- ✖ *Tunnel mode* is more typically used between gateways (routers, firewalls, or standalone VPN devices) to provide a Virtual Private Network

# TRANSPORT OR TUNNEL? (1)

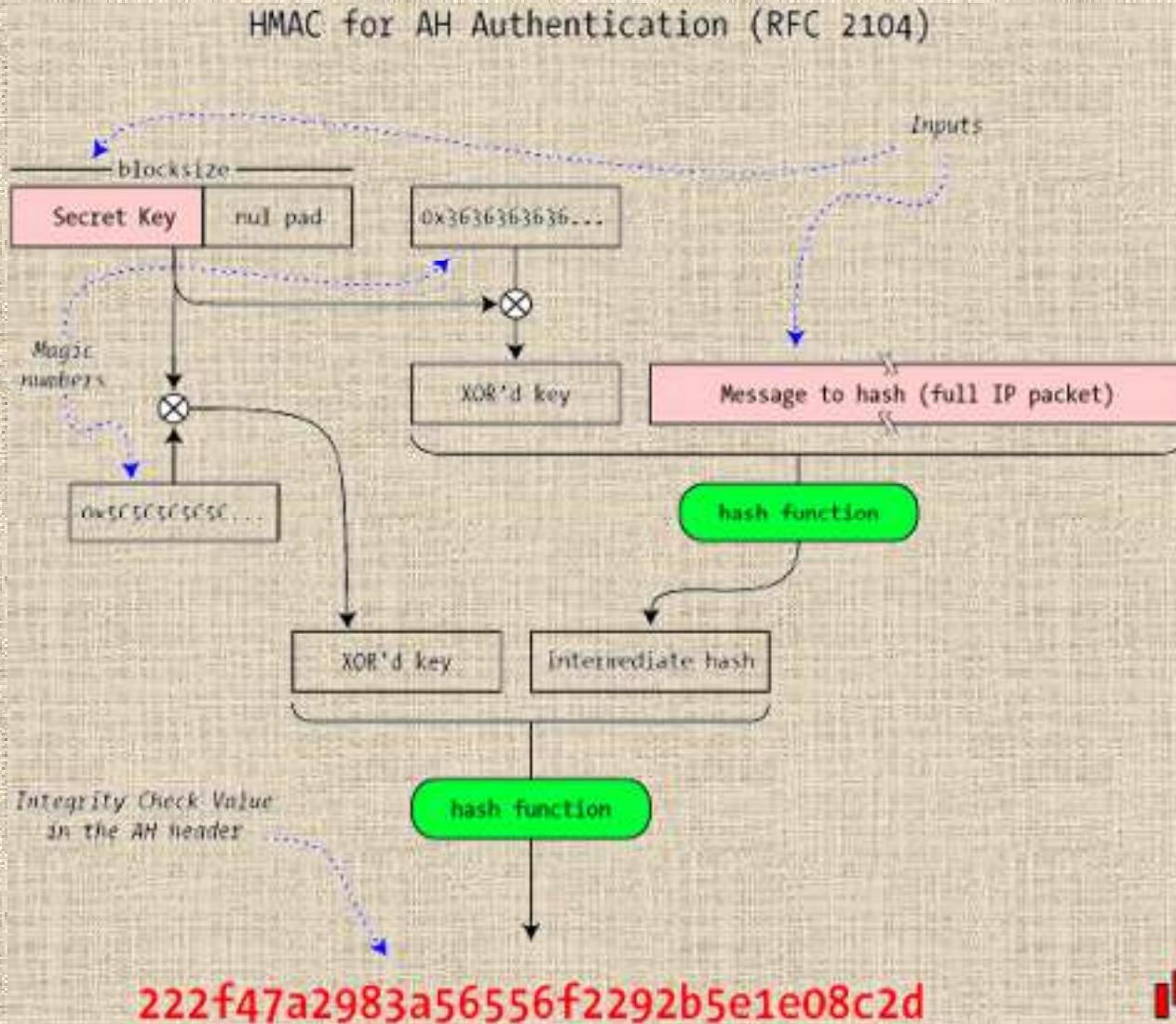
*Transport or Tunnel?*



## TRANSPORT OR TUNNEL? (2)

- ✖ There is no explicit "Mode" field in Ipsec... what distinguishes Transport mode from Tunnel mode?
  - + with the *next header* field in the AH header
    - ✖ When the next-header value is *IP*, it means that this packet encapsulates an entire IP datagram -> Tunnel mode.
    - ✖ Any other value (TCP, UDP, ICMP, etc.) ->Transport mode

# AUTHENTICATION ALGORITHMS (1)



## AUTHENTICATION ALGORITHMS (2)

- ✖ AH carries an Integrity Check Value in the Authentication Data portion of the header, built on top of standard cryptographic hash algorithms such as MD5 or SHA-1
  - + Rather than use a straight checksum, it uses a *Hashed Message Authentication Code* (HMAC) which incorporates a secret value while creating the ICV
  - + Though an attacker can easily recompute a hash, without the secret value he won't be able to recreate the proper ICV

# AH AND NAT

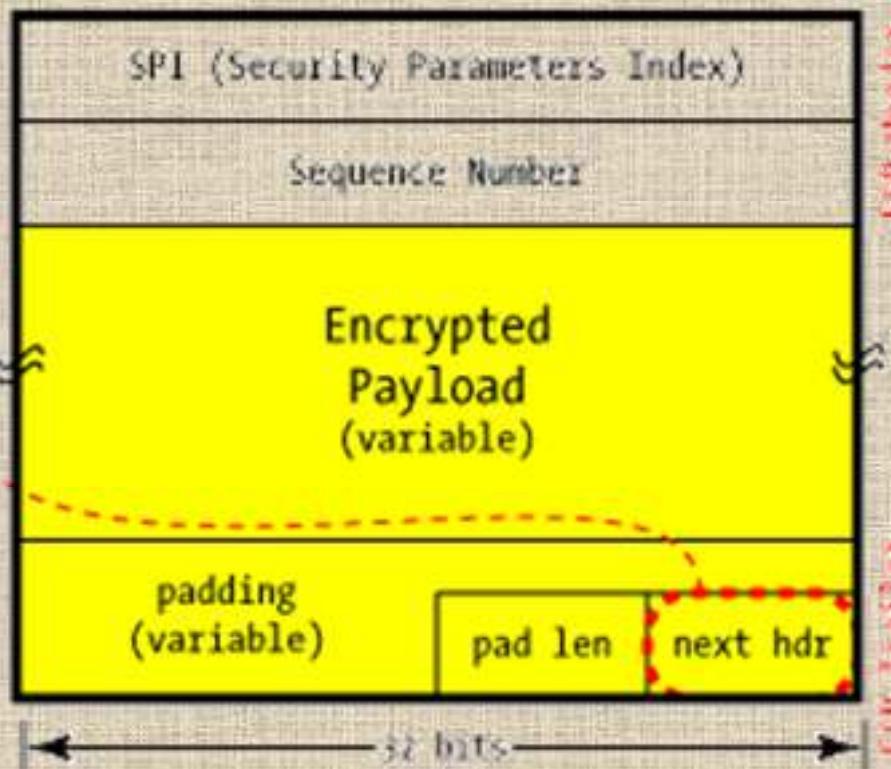
---

- ✖ AH covers the integrity of the entire IP packet
- ✖ ESP does not cover the IP header with controls of any kind neither in Tunnel mode nor in Transport mode
  - + Works better with NAT

# ESP – ENCAPSULATING SECURITY PAYLOAD

<http://www.unixwiz.net/techtips/iguide-ipsec.html#esp>

ESP w/o Authentication



# ESP – ENCAPSULATING SECURITY PAYLOAD

- ✖ Its goal is to provide confidentiality and integrity checking and authenticity to communication.
  - + Unlike AH, the IP header is not covered by integrity checks.
  - + As with AH, it also provides Tunnel and Transport modes .
- ✖ It's possible to use the service of confidentiality, or only authentication services and integrity (and possibly anti-replay), or both services together.

# **ESP –WITHOUT ENCRYPTION-**

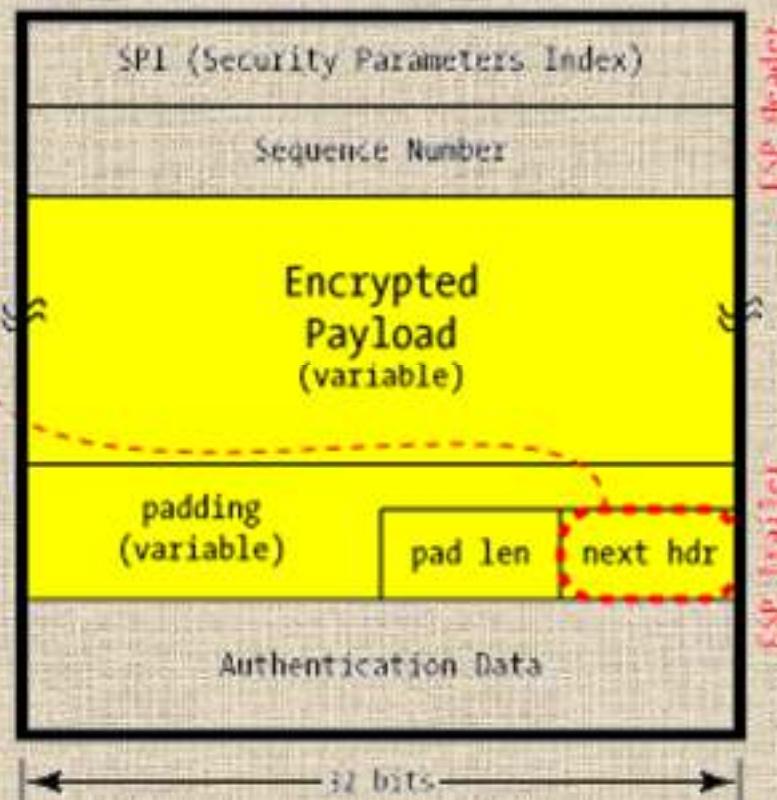
- ✖ use a NULL algorithm
  - + No confidentiality
  - + It only makes sense if combined with ESP authentication

## **ESP – WITH ENCRYPTION –**

- ✖ Adding encryption makes ESP a bit more complicated because the encapsulation surrounds the payload rather than preceding it as with AH
- ✖ ESP includes header and trailer fields to support the encryption and optional authentication
  - + DES, triple-DES, AES, and Blowfish are possible algorithms. Their use for a particular connection is specified by Security Associations (SA)

# ESP – WITH ENCRYPTION –

ESP with Authentication

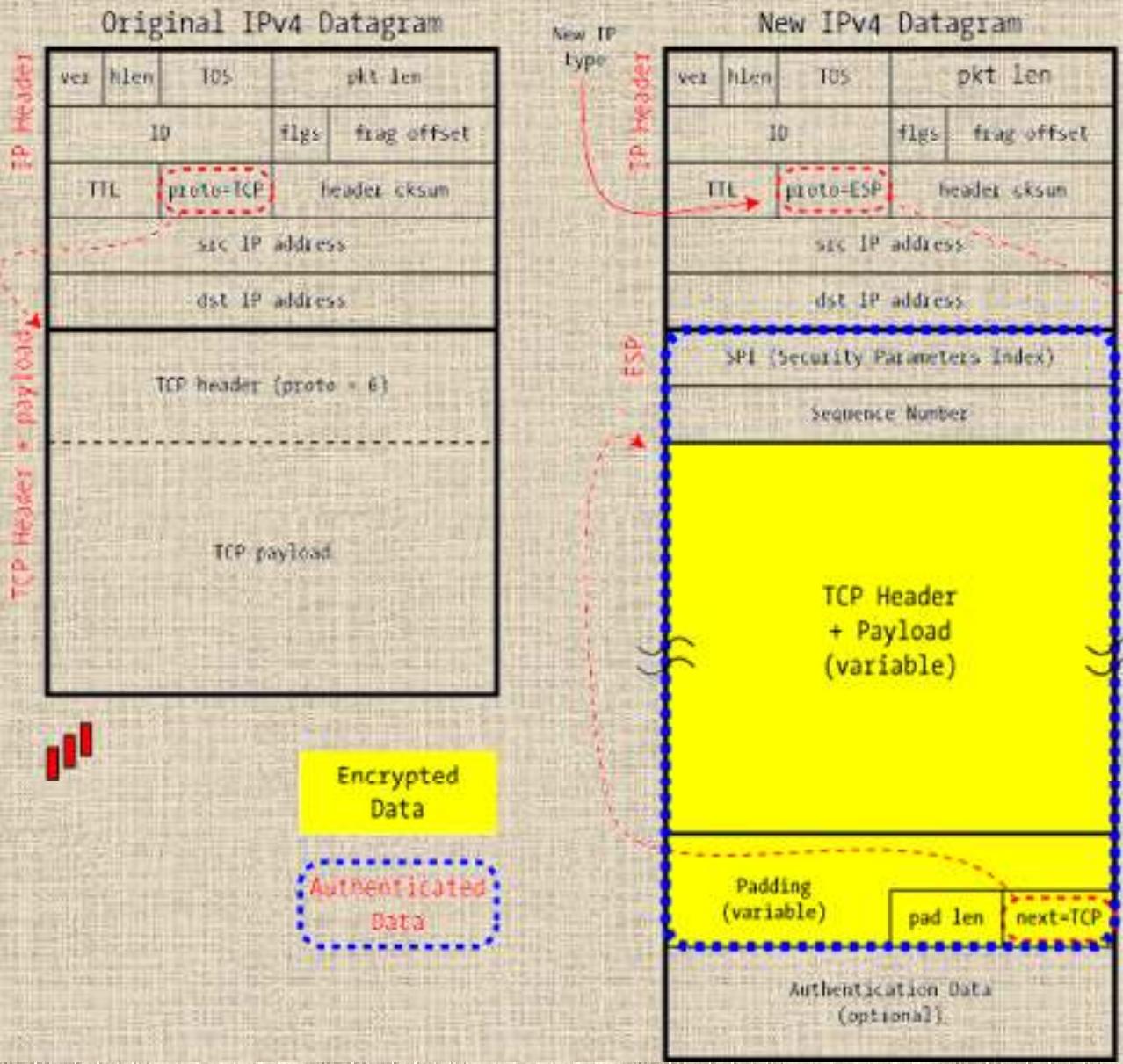


# ESP – WITH ENCRYPTION –

- ✖ HMAC as AH
  - + authentication is *only for the ESP header and encrypted payload* (the full IP packet isn't covered)
  - + When an outsider examines an IP packet containing ESP data, it's essentially impossible to make any real guesses about what's inside an ESP payload except for the usual data found in the IP header (particularly the source and destination IP addresses). It's only possible to know that it's ESP data

# ESP TRANSPORT MODE

IPSec in ESP Transport Mode

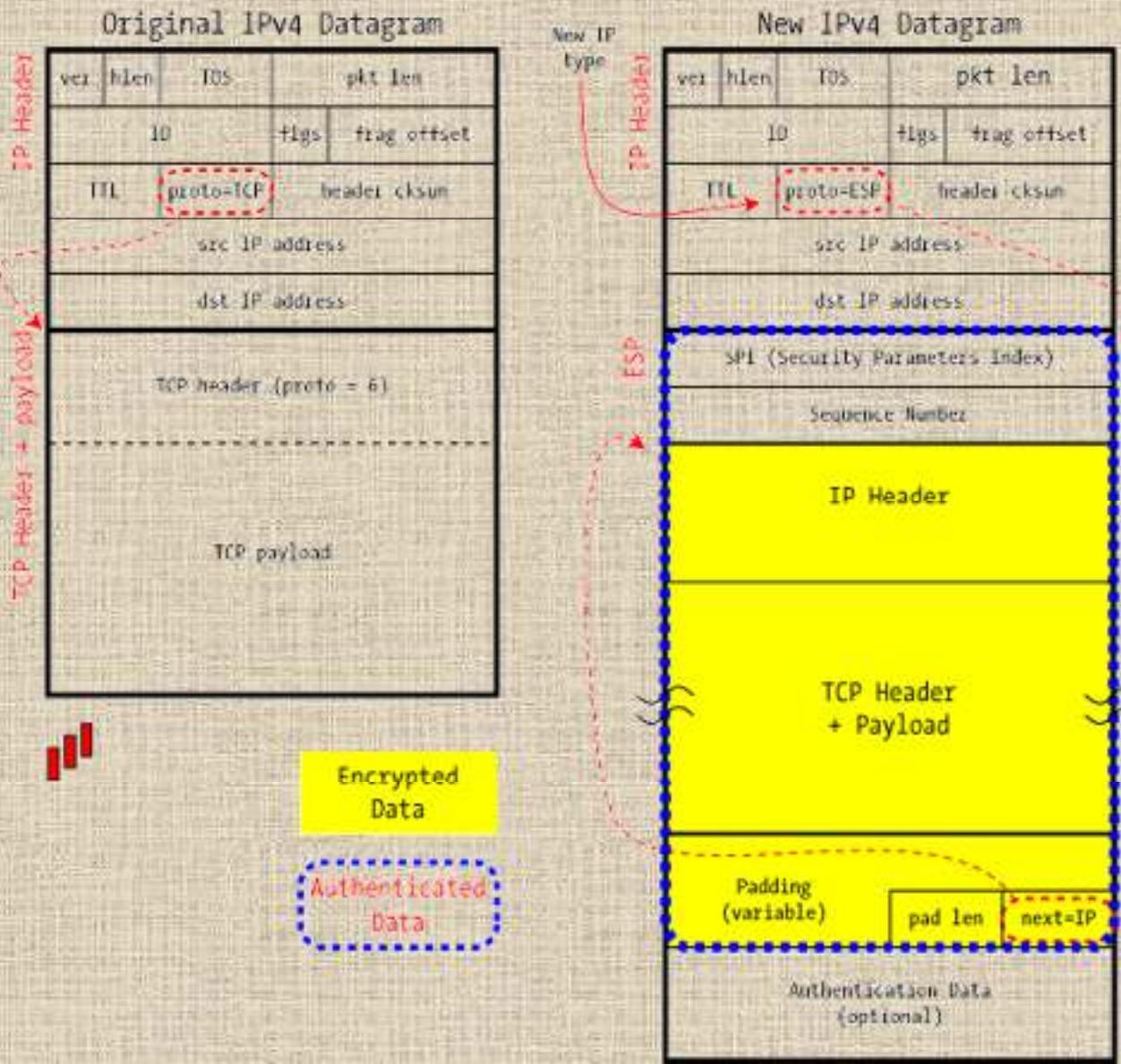


# ESP TRANSPORT MODE

- ✖ encapsulates just the datagram's payload and it is designed strictly for host-to-host communications
- ✖ The original IP header is left in place
  - + the source and destination IP addresses are unchanged

# ESP TUNNEL MODE

IPSec in ESP Tunnel Mode



# ESP TUNNEL MODE

---

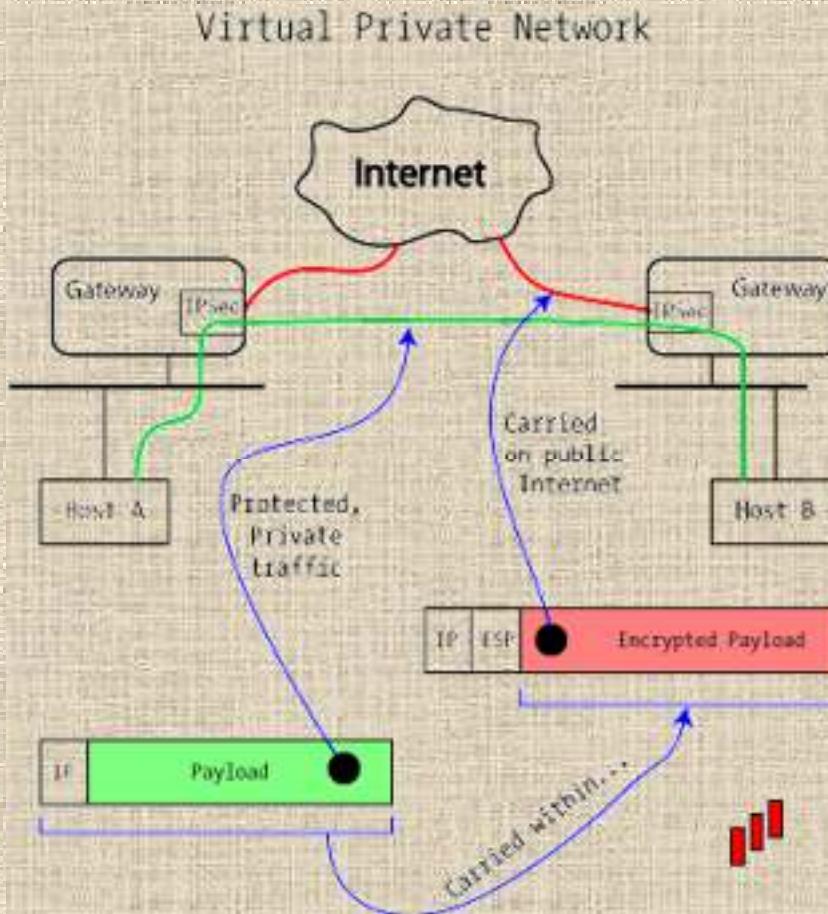
- ✖ encapsulates an entire IP datagram

# SUMMARY

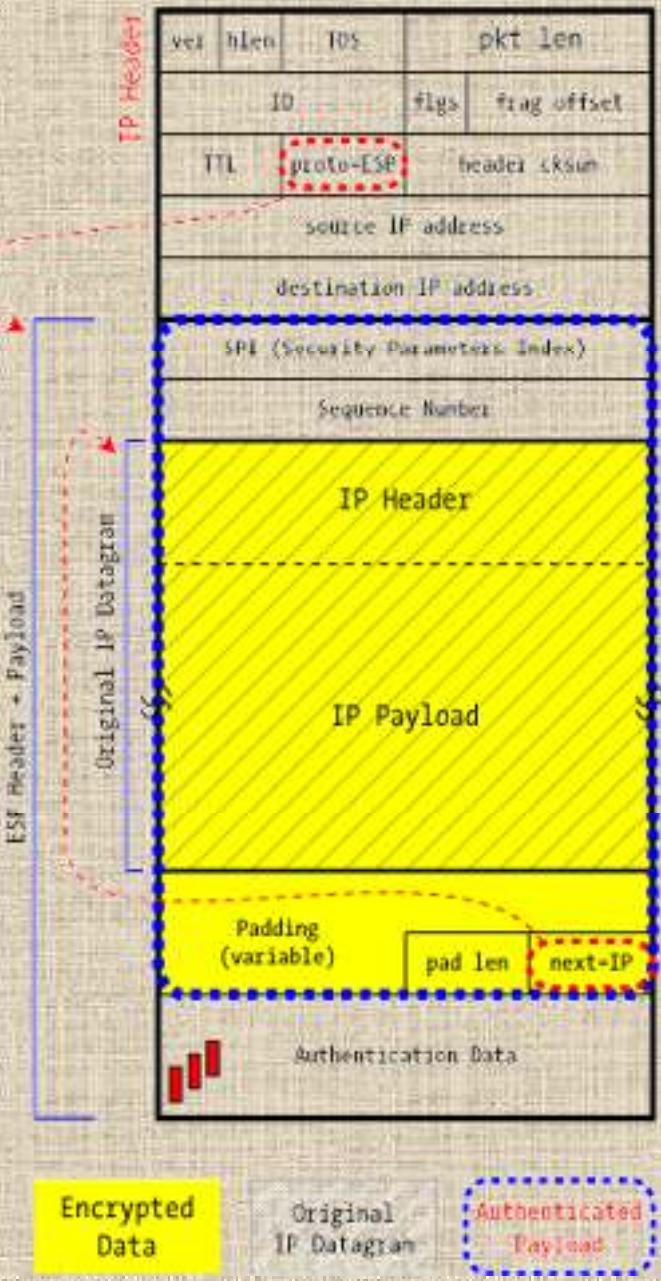
	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates the entire inner IP packet (inner header plus IP payload) plus selected portions of the outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

# BUILDING A REAL VPN

[http://www\\_unixwiz.net/techtips/iguide-ipsec.html#vpn](http://www_unixwiz.net/techtips/iguide-ipsec.html#vpn)



ESP+Auth+Tunnel Mode  
- Traditional VPN



# SECURITY ASSOCIATIONS AND THE SPI

<http://www.unixwiz.net/techtips/iguide-ipsec.html#other>

- + SA: a one way logical connection between the sender and the receiver
- + Identified by three parameters :
  - × Partner IP address
  - × Security Parameters Index (**SPI**)
  - × Identifier of the security protocol

# SECURITY ASSOCIATIONS AND THE SPI

- ✖ Security Association Database (SADB)
  - + A database containing some SAs, present on the hosts
- ✖ Security Parameter Index (SPI)
  - + Unique index associated with each entry of the SADB
  - + Identifies the SA associated with a packet
- ✖ Security Policy Database (SPD)
  - + Stores the policy used to determine the SA type (indicates preferences on what type of SA are acceptable)

---

# IPSEC

## ISAKMP + IKE

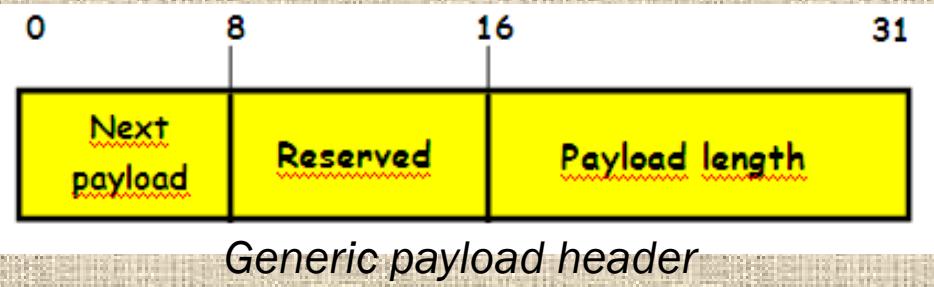
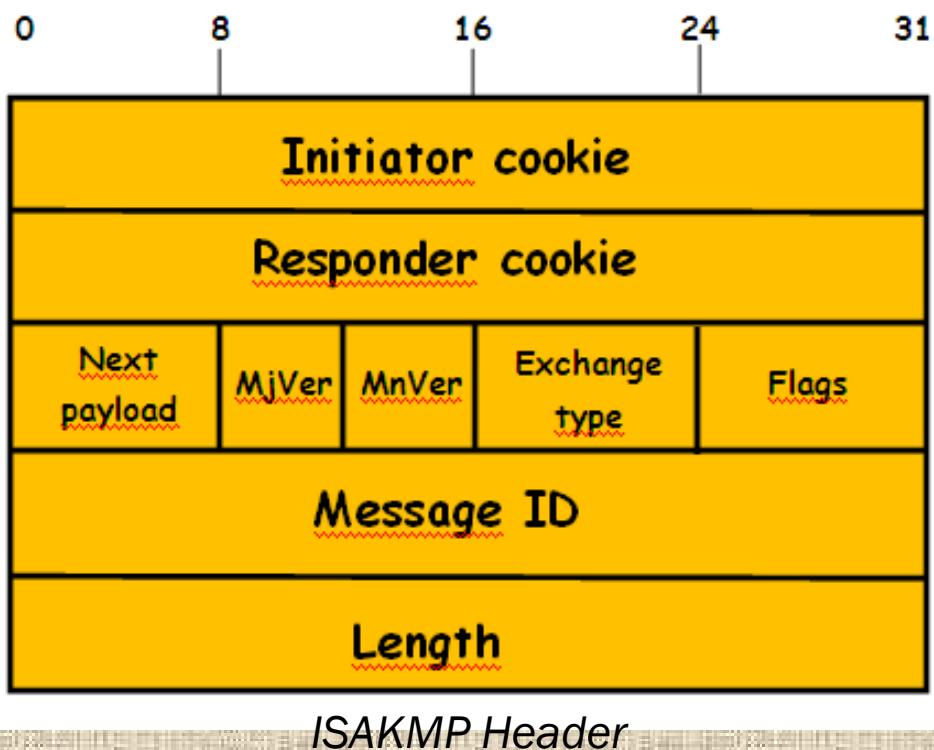
# INTERNET SECURITY ASSOCIATION AND KEY MANAGEMENT PROTOCOL

- ✖ ISAKMP protocol
  - + defines procedures and packet formats to
    - ✖ establish, negotiate, modify, delete the *security associations*
  - + defines payloads for exchanging key generation and authentication data
    - ✖ it's independent of the key generation technique, encryption algorithm and authentication mechanism

# ISAKMP MESSAGE

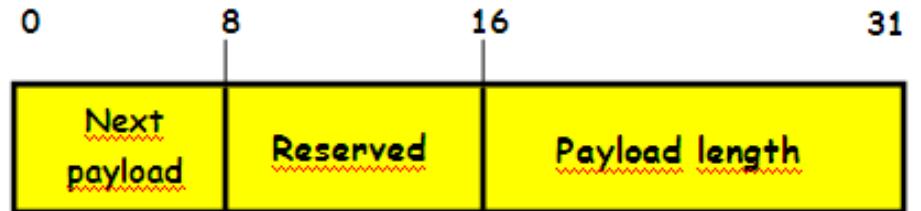
- ✖ An ISAKMP message consists of:
  - + Header + one or more payloads
- ✖ Transported in a transport protocol
  - + specifications require support for UDP

# HEADER ISAKMP



- ✖ **Initiator Cookie (64 bit)**: Cookie of entity that initiated SA establishment, SA notification, or SA deletion. (used to prevent DOS attacks)
- ✖ **Responder Cookie (64 bit)**: Cookie of responding entity; null in first message from initiator
- ✖ **Next Payload (8 bit)**: Indicates the type of the first payload in the message; payloads are discussed in the next subsection
- ✖ **MajorVersion (4 bit)**: Indicates major version of ISAKMP in use
- ✖ **MinorVersion (4 bit)**: Indicates minor ISAKMP version in use.
- ✖ **Exchange Type (8 bit)**: Indicates the type of exchange
- ✖ **Flag (8 bit)**: Indicates specific options set for this ISAKMP exchange
- ✖ **Message ID (32 bit)**: Unique ID for this message
- ✖ **Length (32 bit)**: Length of total message in octets

# PAYLOAD ISAKMP



- Next Payload (8 bit): has a value of 0 if this is the last payload in the message; otherwise its value is the type of the next payload
- Payload length (8 bit): indicates the length in octets of this payload

# SAKMP PAYLOAD TYPES (1)

Type	Parameters	Description
SA (Security Association)	Domain of interpretation, situation	Used to negotiate security attributes and indicate the Domain of interpretation and Situation under which negotiation is taking place.
P (Proposal)	Proposal #, Protocol-ID, SPI Size, # of Transforms, SPI	Used during SA negotiation; indicates protocol to be used and number of transforms. (transform = data processing algorithm, e.g. hmac-md5, etc...)
T (Transform)	Transform #, Transform-ID, SA Attributes	Used during SA negotiation; indicates transform and related SA attributes

# SAKMP PAYLOAD TYPES (2)

Type	Parameters	Description
KE (Key Exchange)	Key Exchange data	Supports a variety of key exchange techniques.
ID (Identification)	ID Type, ID Data	Used to exchange identification information
CERT (Certificate)	Cert Encoding, Certificater Data	Used to transport certificates and other certificate-related information
CR (Certificate Request)	# Cert Types, Certificate Types, # Certificate Auths, certificate Authorities	Used to request certificates; indicates the types of certificates requested and the acceptable certificate authorities
HASH (Hash)	Hash data	Contains data generated by a hash function
SIG (Signature)	Signature Data	Contains data generated by a digital signature function

# SAKMP PAYLOAD TYPES (3)

Type	Parameters	Description
NONCE(nonce)	Nonce Data	Contains a <i>nonce</i>
N(Notification)	DOI,Protocol-ID,SPI Size, Notify Message Type, SPI,Notification Data	Used to transmit notification data, such as an error condition
D (Delete)	DOI,Protocol-ID, SPI Size, # of SPIs, SPI (one or more)	Indicates an SA that is no longer valid

# PAYLOAD TYPES (1)

- ✖ The SA payload is used to begin the establishment of an security association
  - + the *Domain of Interpretation* parameter identifies the DOI under which negotiation is taking place
  - + The *Situation* parameter defines the security policy for this negotiation (the levels of security required)
- ✖ The **Proposal** payload contains information used during SA negotiation
  - + indicates the protocol for this SA (ESP or AH), includes the sending entity's SPI and the number of transforms.
- ✖ The **Transform** payload defines a security transform to be used to secure the communications channel for the designated protocol
  - + The *Transform #* parameter serves to identify this particular payload so that the responder may use it to indicate acceptance of this transform
  - + The *Transform-ID* and *Attributes* fields identify a specific transform (e.g., 3DES for ESP, HMAC-SHA-1-96 for AH) with its associated attributes

# PAYLOAD TYPES (2)

- ✖ The Key Exchange payload can be used for a variety of key exchange techniques(Oakley, Diffie-Hellman,...)
  - + The data field contains the data required to generate a session key and is dependent on the key exchange algorithm used
- ✖ The Identification payload is used to determine the identity of communicating peers and may be used for determining authenticity of information.
  - + Typically the ID Data field will contain an IPv4 or IPv6 address.
- ✖ The Certificate payload transfers a public-key certificate
  - + The *Certificate Encoding* field indicates the type of certificate
- ✖ The Certificate Request payload is used to request the certificate of the other communicating entity
  - + The payload may list more than one certificate type that is acceptable and more than one certificate authority that is acceptable

# PAYLOAD TYPES (3)

- ✖ The **Hash** payload contains data generated by a hash function over some part of the message and/or ISAKMP state.
  - + This payload may be used to verify the integrity of the data in a message or to authenticate negotiating entities
- ✖ The **Signature** payload contains data generated by a digital signature function over some part of the message and/or ISAKMP state.
  - + This payload is used to verify the integrity of the data in a message and may be used for nonrepudiation services
- ✖ The **Nonce** payload contains random data
  - + used to guarantee liveness during an exchange and protect against replay attack
- ✖ The **Notification** payload contains either error or status information associated with this SA or this SA negotiation
- ✖ The **Delete** payload indicates one or more SAs that the sender has deleted from its database and that therefore are no longer valid

# SAKMP: MESSAGE EXCHANGE

- ✖ Base
  - + allows key exchange and authentication material to be transmitted together.
  - + Minimizes the number of exchanges at the expense of not providing identity protection
- ✖ Identity Protection
  - + Expands the Base Exchange to protect the users' identities
- ✖ Authentication Only
  - + Used to perform mutual authentication, without a key exchange
- ✖ Aggressive
  - + Minimizes the number of exchanges at the expense of not providing identity protection
- ✖ Informational
  - + Used for one-way transmittal of information for SA management

(1) I → R : SA; NONCE	Begin ISAKMP-SA negotiation
(2) R → E : SA; NONCE	Basic SA agreed upon
(3) I → R : KE; ID <sub>I</sub> ; AUTH	Key generated; Initiator identity verified by responder
(4) R → E : KE; ID <sub>R</sub> ; AUTH	Responder identity verified by initiator; Key generated; SA established

**Notation :**

I = initiator

R = responder

\* = signifies payload encryption after the ISAKMP header

AUTH = authentication mechanism used

# BASE EXCHANGE

(1) I → R : SA; NONCE	Begin ISAKMP-SA negotiation
(2) R → E : SA; NONCE	Basic SA agreed upon
(3) I → R : KE; ID <sub>I</sub> ; AUTH	Key generated; Initiator identity verified by responder
(4) R → E : KE; ID <sub>R</sub> ; AUTH	Responder identity verified by initiator; Key generated; SA established

- The first two messages provide cookies and establish an SA with agreed protocol and transforms
- Both sides use a nonce to ensure against replay attacks
- The last two messages exchange the key material and user IDs, with an authentication mechanism used to authenticate keys, identities, and the nonces from the first two messages

# IDENTITY PROTECTION EXCHANGE

(1) I → R : SA	Begin ISAKMP-SA negotiation
(2) R → E : SA	Basic SA agreed upon
(3) I → R : KE; NONCE	Key generated
(4) R → E : KE; NONCE	Key generated
(5)* I → R : ID <sub>I</sub> ; AUTH	Initiator identity verified by responder
(6)* R → E : ID <sub>R</sub> ; AUTH	Responder identity verified by initiator; SA established

## Notation :

I = initiator

R = responder

\* = signifies payload encryption after the ISAKMP header

AUTH = authentication mechanism used

# IDENTITY PROTECTION EXCHANGE

(1) I → R : SA	Begin ISAKMP-SA negotiation
(2) R → E : SA	Basic SA agreed upon
(3) I → R : KE; NONCE	Key generated
(4) R → E : KE; NONCE	Key generated
(5)* I → R : ID <sub>I</sub> ; AUTH	Initiator identity verified by responder
(6)* R → E : ID <sub>R</sub> ; AUTH	Responder identity verified by initiator; SA established

- The first two messages establish the SA.
- The next two messages perform key exchange, with nonces for replay protection.
- Once the session key has been computed, the two parties exchange encrypted messages that contain authentication information, such as digital signatures and optionally certificates validating the public keys

(1) I → R : SA; NONCE	Begin ISAKMP-SA negotiation
(2) R → E : SA; NONCE; ID <sub>R</sub> ; AUTH	Basic SA agreed upon; Responder identity verified by initiator
(3) I → R : ID <sub>I</sub> ; AUTH	Initiator identity verified by responder; SA established

**Notation :**

I = initiator

R = responder

\* = signifies payload encryption after the ISAKMP header

AUTH = authentication mechanism used

# ONLY EXCHANGE

# AUTHENTICATION ONLY EXCHANGE

(1) I → R : SA; NONCE	Begin ISAKMP-SA negotiation
(2) R → E : SA; NONCE; ID <sub>R</sub> ; AUTH	Basic SA agreed upon; Responder identity verified by initiator
(3) I → R : ID <sub>I</sub> ; AUTH	Initiator identity verified by responder; SA established

- The first two messages establish the SA.
- In addition, the responder uses the second message to convey its ID and uses authentication to protect the message.
- The initiator sends the third message to transmit its authenticated ID

# AGGRESSIVE EXCHANGE

(1)  $I \rightarrow R : SA; KE; NONCE; ID_I;$

Begin ISAKMP-SA negotiation and key exchange

(2)  $R \rightarrow E : SA; KE; NONCE; ID_R;$   
AUTH

Initiator identity verified by responder; Key generated; Basic SA agreed upon

(3)\*  $I \rightarrow R : AUTH$

Responder identity verified by initiator; SA established

## Notation :

I = initiator

R = responder

\* = signifies payload encryption after the ISAKMP header

AUTH = authentication mechanism used

# AGGRESSIVE EXCHANGE

(1) I → R : SA; KE; NONCE; ID <sub>I</sub> ;	Begin ISAKMP-SA negotiation and key exchange
(2) R → E : SA; KE; NONCE; ID <sub>R</sub> ; AUTH	Initiator identity verified by responder; Key generated; Basic SA agreed upon
(3)* I → R : AUTH	Responder identity verified by initiator; SA established

- In the first message, the initiator proposes an SA with associated offered protocol and transform options. The initiator also begins the key exchange and provides its ID.
- In the second message, the responder indicates its acceptance of the SA with a particular protocol and transform, completes the key exchange, and authenticates the transmitted information.
- In the third message, the initiator transmits an authentication result that covers the previous information, encrypted using the shared secret session key

# INFORMATIONAL EXCHANGE

1)\* I → R : N/D

Error or status notification, or deletion

Used for one-way transmission of information for security association management

## Notation :

I = initiator

R = responder

\* = signifies payload encryption after the ISAKMP header

AUTH = authentication mechanism used

# **SECURITY ASSOCIATION**

---

- ✖ The concept of a *security association* (SA) is fundamental to IPSec, but neither AH or ESP are concerned with the SA management
- ✖ The security associations can be built manually or automatically
  - + their management manual is not always practicable
  - + IKE (Internet Key Exchange) protocol solves this problem

# IKE (INTERNET KEY EXCHANGE)

- Protocol for automatic key management necessary for all the operations of security provided by IPSec
  - ✖ Hybrid protocol
  - ✖ Works in the initial phases of a communication, allowing the creation of SA and archive management to these dedicated
  - ✖ ISAKMP based

# IKE (INTERNET KEY EXCHANGE)

- ✖ A Security Association is a contract established between two IPsec endpoints (hosts or security gateways)
  - + Automatic negotiation of parameters to be used for the IPsec connection.
  - + Separate SA required for each subnet or single host.
  - + Separate SA required for inbound and outbound connection.
  - + SAs are assigned a unique Security Parameters Index (SPI) and are maintained in a database

# IKE ELEMENTS

- ✖ Internet Security and Key Management Protocol (ISAKMP)
  - + The current implementation provides for the combined use of the features of two protocols
    - ✖ OAKLEY (a protocol by which two authenticated parties can reach an agreement about the key material to use and that will take advantage of the features for the IKE key exchange);
    - ✖ SKEME: a key exchange protocol similar to OAKLEY, but, IKE will use different features such as public-key encryption method and the fast renewal of the key

# IKE: THE PURPOSE

- ✖ The IKE negotiation occurs in two phases:
  - + The first phase sets up a *Internet Security Association Key Management Security Association* (ISAKMP SA)
  - + The second phase the ISAKMP SA is used for the negotiation and setup the IPSec SAs

# IKE: PHASE 1

---

- ✖ Establishes an ISAKMP SA to be used as a secure channel to the subsequent negotiation IPSec, in particular:
  - + Negotiates security parameters
  - + Generate a shared secret
  - + Authentic parts

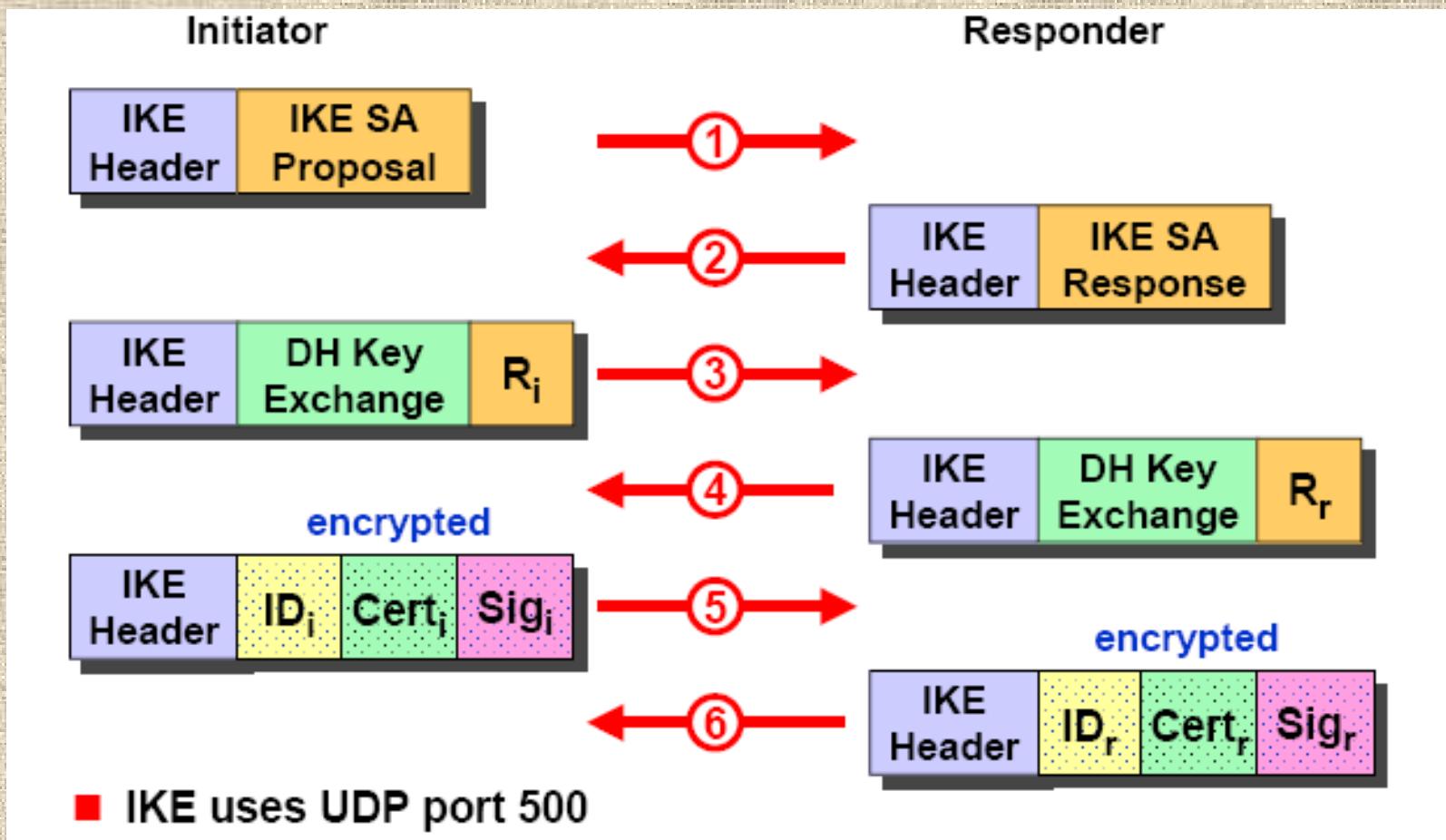
# IKE: PHASE 1

- ✖ IKE phase one occurs in two modes:
  - + Main mode: consists of six messages exchanged of which three are transmitted from the sender to the recipient and three response in the opposite direction
  - + Aggressive mode: uses only three messages. Two messages sent by the sender and one response.
- ✖ The main difference, in addition to the number of messages used, is that that the first mode, though slower, provides protection of identity
  - + Both modes authenticate the parties and establish an ISAKMP SA
  - + The aggressive mode can do so by using half of the messages
    - ✖ The price to pay, for greater speed, is the absence of support for the identification of the participants and therefore the possibility of attacks of man-in-the-middle in the case of using pre-shared keys

## IKE: PHASE 2

- ✖ Also called Quick mode
  - + Is used principally to negotiate the IPSec services of a general nature and regenerate the key material
  - + Is similar to a “Aggressive mode” negotiation but less complex because it exploits the communication already in place (see below ..)

# IKE PHASE 1 - MAIN MODE ESTABLISH A SECURE NEGOTIATION CHANNEL



# IKE PHASE 1 - MAIN MODE

## ESTABLISH A SECURE NEGOTIATION CHANNEL

6 messages exchanged between initiator and responder to establish a *IKE Security Association* (IKE SA)

- + IKE uses UDP port 500
- ✖ **Msg #1**
  - + The initiator sends an IKE SA Proposal listing all supported authentication methods, Diffie-Hellman groups, a choice of encryption and hash algorithms and the desired SA lifetime
- ✖ **Msg #2**
  - + The responder answers with an IKE SA Response indicating the preferred authentication method, Diffie-Hellman group, encryption and hash algorithm and acceptable SA lifetime

If the two parties were able to successfully negotiate a common set of methods the protocol is continued by establishing an encrypted communication channel using the Diffie-Hellman Key-Exchange algorithm

# IKE PHASE 1 - MAIN MODE

## ESTABLISH A SECURE NEGOTIATION CHANNEL

- ✖ Msg #3
  - + The initiator sends his part of the Diffie-Hellman secret plus a random value
- ✖ Msg #4
  - + The responder does the same by sending his part of the *Diffie-Hellman secret* plus a random value

Diffie-Hellman Key-Exchange can now be completed by both parties forming the common shared secret.

- + This shared secret is used to generate a symmetric session key with which the remaining messages of the IKE protocol are going to be encrypted

# IKE PHASE 1 - MAIN MODE

## ESTABLISH A SECURE NEGOTIATION CHANNEL

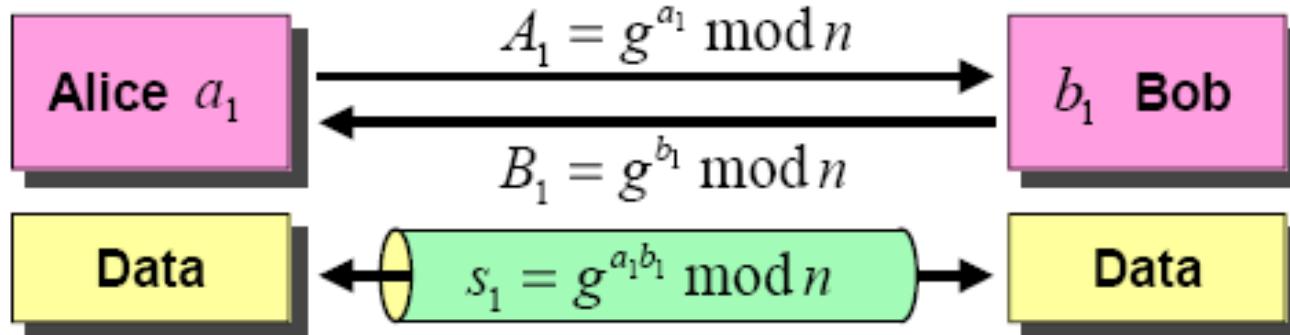
- ✖ Msg #5
  - + The initiator sends his identity optionally followed by a certificate linking the identity to a public key.
  - + This is followed by a hash over all message fields signed by a preshared secret or a private RSA key.
- ✖ Msg #6
  - + The same as Msg #5 but formed and sent by the responder

If the identity of both peers is successfully authenticated then an IKE SA has been established

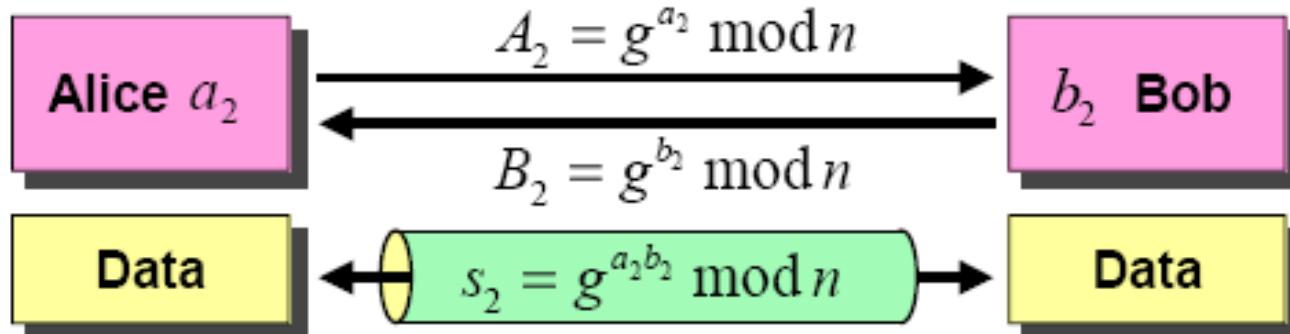
# THE DIFFIE-HELLMAN KEY-EXCHANGE ALGORITHM

## PERFECT FORWARD SECRECY

### ■ Session 1: January 26 2001



### ■ Session 2: February 2 2001



If key  $s_1$  gets compromised, then key  $s_2$  is still totally secure!

# IKE AGGRESSIVE MODE

- The aggressive mode obtains the same result as the main mode, but with a smaller number of messages (three instead of six) at a price, however, not to authenticate the identities of the two parties
  - given that payloads are exchanged before it is completed the Diffie-Hellman exchange, they are transmitted in clear and not encrypted as in the case of the main mode

## IKE: PHASE 2

- ✖ After completing phase 1, with the main mode, with the aggressive mode, the two parties have created a SA, and then can proceed to phase 2
  - + This negotiation takes place with the Quick Mode
  - + Contrary to what happens in the phase 1, here all the messages are encrypted because protected from the SA

# IKE PHASE 2 - QUICK MODE

## ESTABLISH OR RENEW AN IPSEC SA

- ✖ Encrypted Quick Mode Message Exchange
  - + All Quick Mode negotiations are encrypted with a shared secret.
  - + Key derived from a Diffie-Hellmann key-exchange plus additional parameters.
- ✖ Negotiation of IPsec Parameters
  - + Phase 2 Quick Mode establishes an IPsec SA using the secure channel created by the phase 1 IKE SA.
  - + The specific configuration parameters for the IPsec connection are negotiated (AH, ESP, authentication / encryption methods and parameters).
  - + Quick Mode can be used repeatedly to renew IPsec SAs about to expire.
- ✖ Optional Perfect Forward Secrecy
  - + If perfect forward secrecy is required, each consecutive Quick Modes will do a fresh Diffie-Hellmann key-exchange.

# INTRODUCTION TO SECURITY ASSOCIATION

- **Definition:** A Security Association (SA) is a relationship between two or more entities that describes how they will use security services to communicate securely.
- **Purpose:** Establishes parameters for secure communication, such as encryption algorithms, keys, and other security services.

# **COMPONENTS OF SECURITY ASSOCIATION**

- **Security Parameters Index (SPI):**
  - A unique identifier for a security association.
- **IPsec Protocol:**
  - Specifies the type of security protocol (e.g., ESP or AH).
- **Cryptographic Algorithms:**
  - Defines the encryption and hashing algorithms used.

# SECURITY ASSOCIATION DATABASE (SAD)

- **What is SAD?**
  - The **Security Association Database (SAD)** is a collection of all active Security Associations.
- **Functions:**
  - Stores information about each SA, including SPI, IPsec protocol, cryptographic keys, etc.
- **Location:**
  - Typically stored in the memory of networking devices like routers and firewalls.

# SECURITY POLICY DATABASE (SPD)

- **What is SPD?**
  - The **Security Policy Database (SPD)** defines the security policies that determine how and when IPsec is applied to packets.
- **Functions:**
  - Contains rules for processing incoming and outgoing traffic based on security requirements.
- **Location:**
  - Also stored in the memory of network devices, often alongside SAD.

# COMMUNICATION: 1. INITIAL SETUP

- Before communication begins, both the sender and receiver must establish a **Security Association (SA)**. This is typically done using a protocol like IKE (Internet Key Exchange).
- During this setup:
  - **SPI**: A unique identifier is generated for the SA. The SPI is used to index the Security Association in the SAD.
  - **SAD**: Both sender and receiver populate their SAD with the details of the Security Association, including the SPI, encryption/decryption keys, algorithms, and other parameters.
  - **SPD**: Security policies are defined in the SPD, which dictate which traffic should be secured and how.

# SENDING A SECURE PACKET

## •**Step 1: Packet Matching in SPD**

- The sender's system checks the SPD to determine if the outgoing packet should be secured (e.g., encrypted).
- The SPD contains rules that specify which types of traffic require security and how to handle them.
- If the packet matches a rule in the SPD that requires security, the system moves forward with securing the packet.

## •**Step 2: Finding the Security Association in SAD**

- The sender's system then looks up the appropriate Security Association in the SAD using the SPI associated with the packet.
- The SAD entry provides the necessary details, such as the encryption algorithm and the key to be used.

# SENDING A SECURE PACKET

- **Step 3: Packet Encryption**

- The packet is then processed according to the SA parameters found in the SAD. Typically, this involves encrypting the packet's payload and adding an IPsec header containing the SPI.

- The SPI in the IPsec header allows the receiver to identify the corresponding SA when the packet is received.

- **Step 4: Sending the Packet**

- The secured (encrypted) packet, along with the IPsec header (including the SPI), is sent over the network to the receiver.

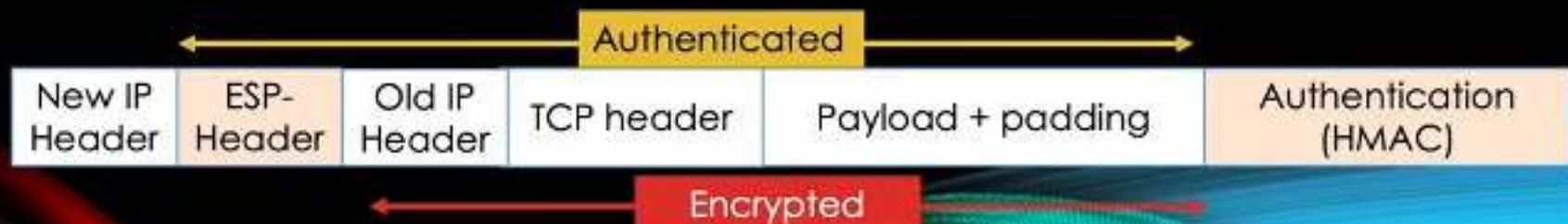
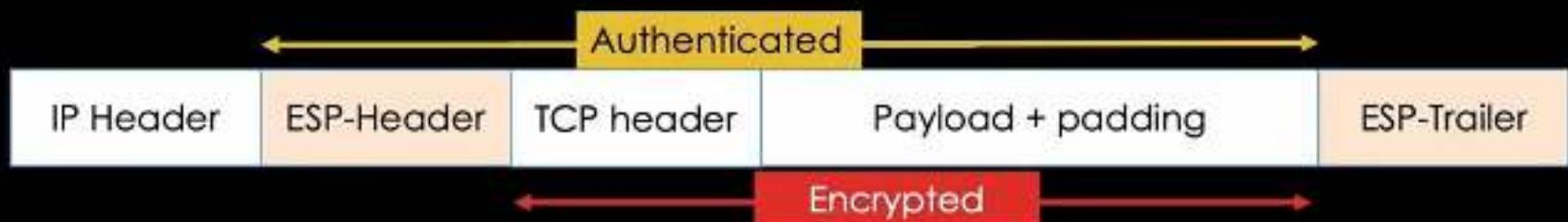
# RECEIVING THE SECURE PACKET

- **Step 1: SPI Lookup**
  - The receiver extracts the SPI from the IPsec header of the incoming packet.
  - The SPI is then used to look up the corresponding Security Association in the SAD.
- **Step 2: SAD Processing**
  - The SAD entry provides the receiver with the necessary decryption key and the algorithm required to process the packet.
  - The receiver decrypts the packet using the information in the SAD.
- **Step 3: SPD Verification**
  - The receiver checks the SPD to ensure that the packet conforms to the expected security policies.
  - This step verifies that the packet was received under the expected security conditions.
- **Step 4: Packet Decryption and Forwarding**
  - Once the packet is decrypted and verified, it is forwarded to the appropriate application or endpoint within the receiver's network.

# Encapsulating Security Payload Protocol (ESP)

Security and Privacy  
Academy

## Transport vs. tunnel mode



# Security Policies

Security and Privacy  
Academy



# Security Policy Database

Security and Privacy  
Academy



SPD

# Security Policies

Security and Privacy  
Academy

Protocol (AH/ESP)



Mode (Tunnel/Transport)

Destination / Source **IP**

Transport protocol (TCP/UDP)

Destination / Source **Port**

# Security Policies

Security and Privacy  
Academy

```
192.16.2.0/24[any] 192.16.1.0/24[any] any
    in prio def ipsec
    esp/tunnel/192.168.2.1-192.168.1.1/require
        created: Mar 10 08:12:24 2023 lastused:
        lifetime: 0(s) validtime: 0(s)
        spid=392 seq=8 pid=1752
        refcnt=1
192.16.1.0/24[any] 192.16.2.0/24[any] any
    out prio def ipsec
    esp/tunnel/192.168.1.1-192.168.2.1/require
        created: Mar 10 08:12:24 2023 lastused: Mar 10 08:12:16 2023
        lifetime: 0(s) validtime: 0(s)
        spid=385 seq=7 pid=1752
        refcnt=4
172.16.2.0/24[any] 172.16.1.0/24[any] any
    fwd prio def ipsec
    esp/tunnel/192.168.2.1-192.168.1.1/require
        created: Mar 10 08:12:24 2023 lastused: Mar 10 08:12:16 2023
        lifetime: 0(s) validtime: 0(s)
        spid=402 seq=6 pid=1752
        refcnt=4
```

# Security Association

Security and Privacy  
Academy

Key, authentication process, mode

Validity

Initializing Vector

IP addresses



# Security Association

Security and Privacy  
Academy

```
192.168.2.1 192.168.1.1
esp mode=tunnel spi=769(0x00000301) reqid=0(0x00000000)
E: 3des-cbc e1aae5c 795e8c56 e0a8a35d c8886a88 70f914a3 f367f01d
A: hmac-md5 0946d4a5 635f7ac6 22620c67 4c7adb4c
seq=0x00000000 replay=0 flags=0x00000000 state=mature
created: Mar 10 08:12:24 2023 current: Mar 10 08:44:54 2023
diff: 29(s) hard: 0(s) soft: 0(s)
last: Mar 10 08:34:54 2023 hard: 0(s) soft: 0(s)
current: 3525(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 23 hard: 0 soft: 0
sadb_seq=1 pid=1750 refcnt=0
```

# Security Association

Security and Privacy  
Academy

192.168.2.1 192.168.1.1

```
esp mode=tunnel spi=769(0x00000301) reqid=0(0x00000000)
E: 3des-cbc e1aae5c 795e8c56 e0a8a35d c8886a88 70f914a3 f367f01d
A: hmac-md5 0946d4a5 635f7ac6 22620c67 4c7adb4c
seq=0x00000000 replay=0 flags=0x00000000 state=mature
created: Mar 10 08:12:24 2023 current: Mar 10 08:44:54 2023
diff: 29(s) hard: 0(s) soft: 0(s)
last: Mar 10 08:34:54 2023 hard: 0(s) soft: 0(s)
current: 3525(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 23 hard: 0 soft: 0
sadb_seq=1 pid=1750 refcnt=0
```

# Security Association

Security and Privacy  
Academy

```
192.168.2.1 192.168.1.1
esp mode=tunnel spi=769(0x00000301) reqid=0 (0x00000000)
E: 3des-cbc e1aae5c 795e8c56 e0a8a35d c8886a88 70f914a3 f367f01d
A: hmac-md5 0946d4a5 635f7ac6 22620c67 4c7adb4c
seq=0x00000000 replay=0 flags=0x00000000 state=mature
created: Mar 10 08:12:24 2023 current: Mar 10 08:44:54 2023
diff: 29(s) hard: 0(s) soft: 0(s)
last: Mar 10 08:34:54 2023 hard: 0(s) soft: 0(s)
current: 3525(bytes) hard: 0(bytes) soft: 0(bytes)
allocated: 23 hard: 0 soft: 0
sadb_seq=1 pid=1750 refcnt=0
```

# Security Association

Security and Privacy  
Academy

```
192.168.2.1 192.168.1.1
    esp mode=tunnel spi=769(0x00000301) reqid=0(0x00000000)
    E: 3des-cbc e1aae5c 795e8c56 e0a8a35d c8886a88 70f914a3 f367f01d
    A: hmac-md5 0946d4a5 635f7ac6 22620c67 4c7adb4c
        seq=0x00000000 replay=0 flags=0x00000000 state=mature
    created: Mar 10 08:12:24 2023 current: Mar 10 08:44:54 2023
    diff: 29(s) hard: 0(s) soft: 0(s)
    last: Mar 10 08:34:54 2023 hard: 0(s) soft: 0(s)
    current: 3525(bytes) hard: 0(bytes) soft: 0(bytes)
    allocated: 23 hard: 0 soft: 0
    sadb_seq=1 pid=1750 refcnt=0
```

# Security Association

Security and Privacy  
Academy

```
192.168.2.1 192.168.1.1
    esp mode=tunnel spi=769(0x00000301) reqid=0(0x00000000)
    E: 3des-cbc e1aae5c 795e8c56 e0a8a35d c8886a88 70f914a3 f367f01d
    A: hmac-md5 0946d4a5 635f7ac6 22620c67 4c7adb4c
        seq=0x00000000 replay=0 flags=0x00000000 state=mature
        created: Mar 10 08:12:24 2023 current: Mar 10 08:44:54 2023
        diff: 29(s) hard: 0(s) soft: 0(s)
        last: Mar 10 08:34:54 2023 hard: 0(s) soft: 0(s)
        current: 3525(bytes) hard: 0(bytes) soft: 0(bytes)
        allocated: 23 hard: 0 soft: 0
        sadb_seq=1 pid=1750 refcnt=0
```

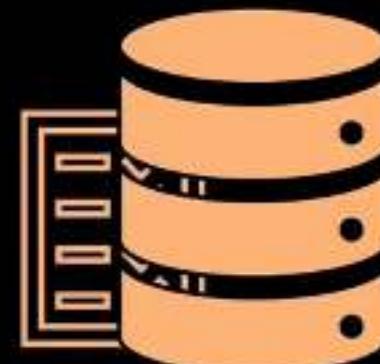
# Security Association

Security and Privacy  
Academy

```
192.168.2.1 192.168.1.1
    esp mode=tunnel spi=769(0x00000301) reqid=0(0x00000000)
    E: 3des-cbc e1aae5c 795e8c56 e0a8a35d c8886a88 70f914a3 f367f01d
    A: hmac-md5 0946d4a5 635f7ac6 22620c67 4c7adb4c
        seq=0x00000000 replay=0 flags=0x00000000 state=mature
        created: Mar 10 08:12:24 2023 current: Mar 10 08:12:53 2023
        diff: 29(s) hard: 0(s) soft: 0(s)
        last: Mar 10 08:12:40 2023 hard: 0(s) soft: 0(s)
        current: 3525(bytes) hard: 0(bytes) soft: 0(bytes)
        allocated: 23 hard: 0 soft: 0
        sadb_seq=1 pid=1750 refcnt=0
```

# Security Association Database

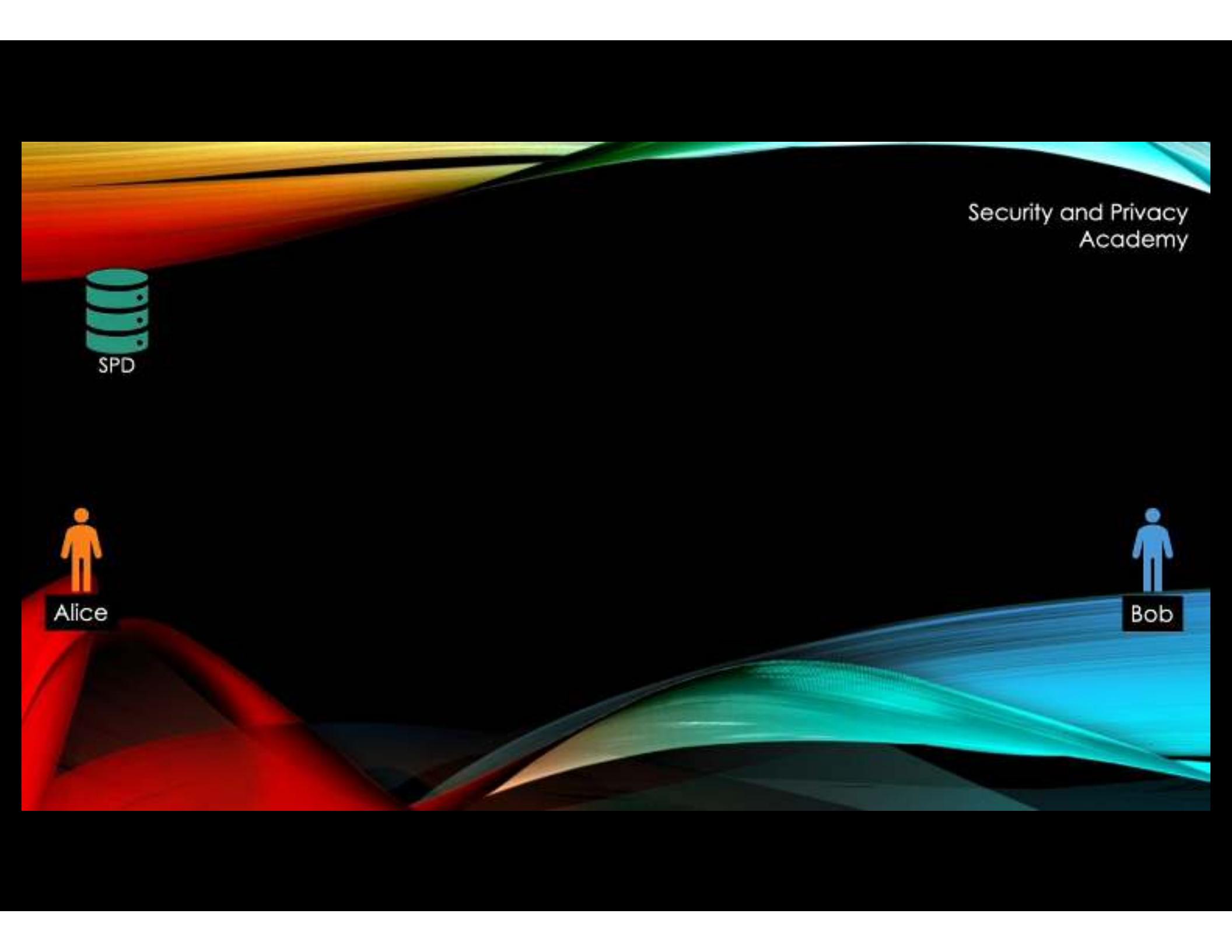
Security and Privacy  
Academy



SAD

## Internet Keyexchange Protocol (IKEv2)





Security and Privacy  
Academy



Alice



Bob



SPD



SAD



Alice



Bob



SPD



SAD



Alice



Bob

# Internet Keyexchange Protocol (IKEv2)

Security and Privacy  
Academy



SPD



SAD



Alice



Bob

# Internet Keyexchange Protocol (IKEv2)

Security and Privacy  
Academy



SPD



SAD



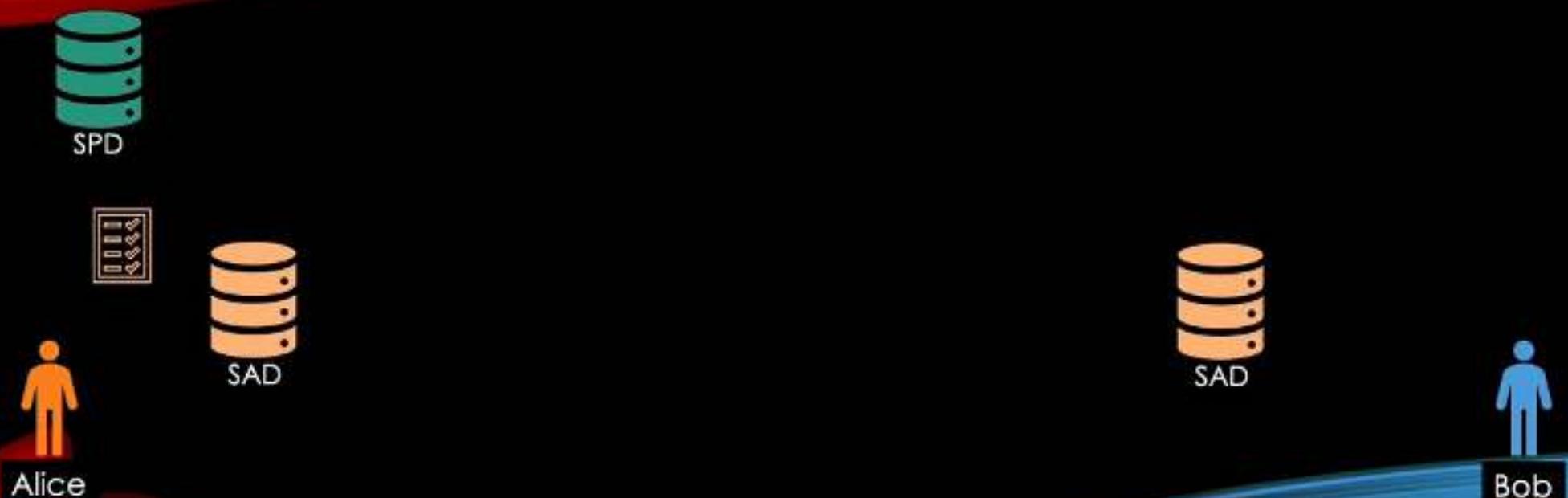
Alice



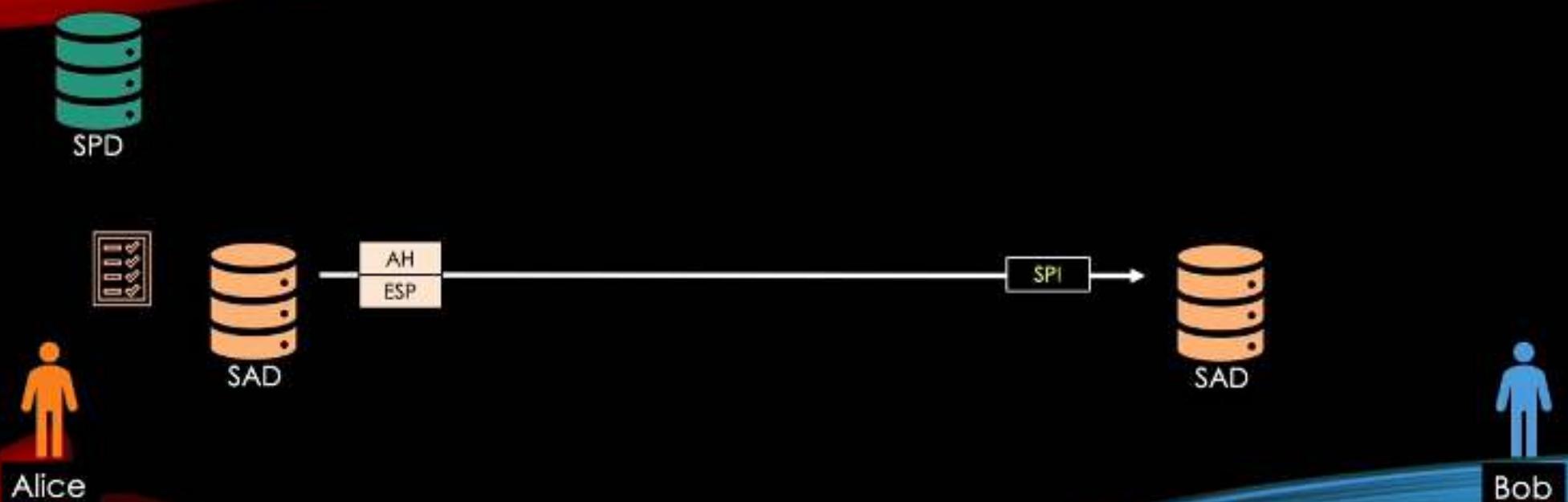
Bob

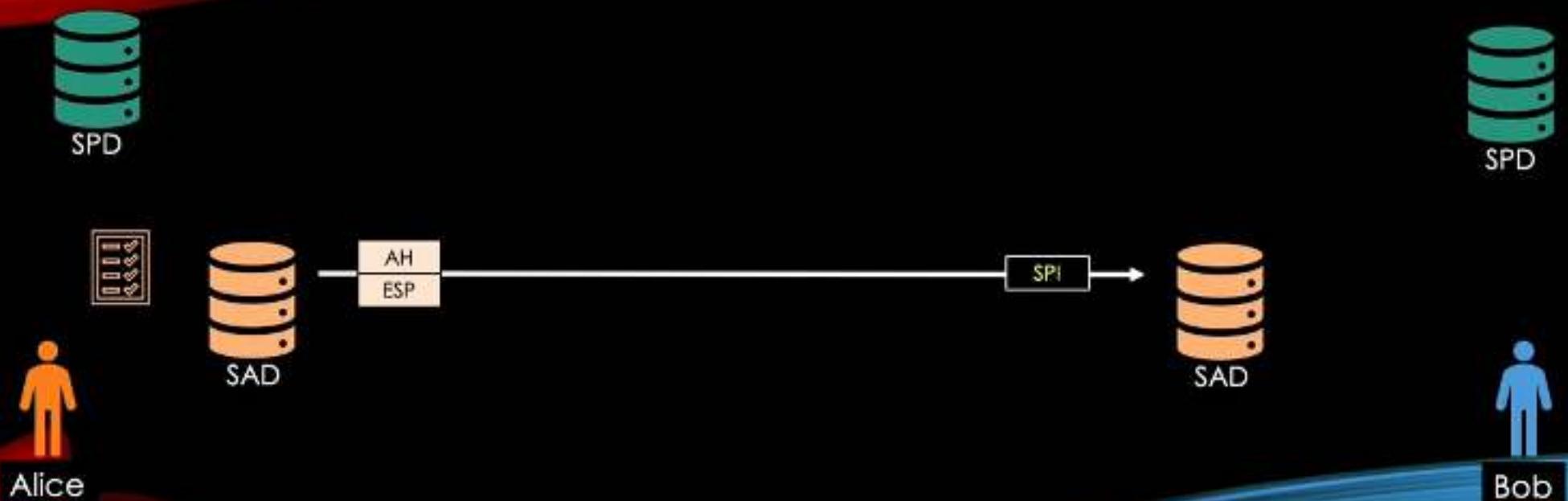
# Internet Keyexchange Protocol (IKEv2)

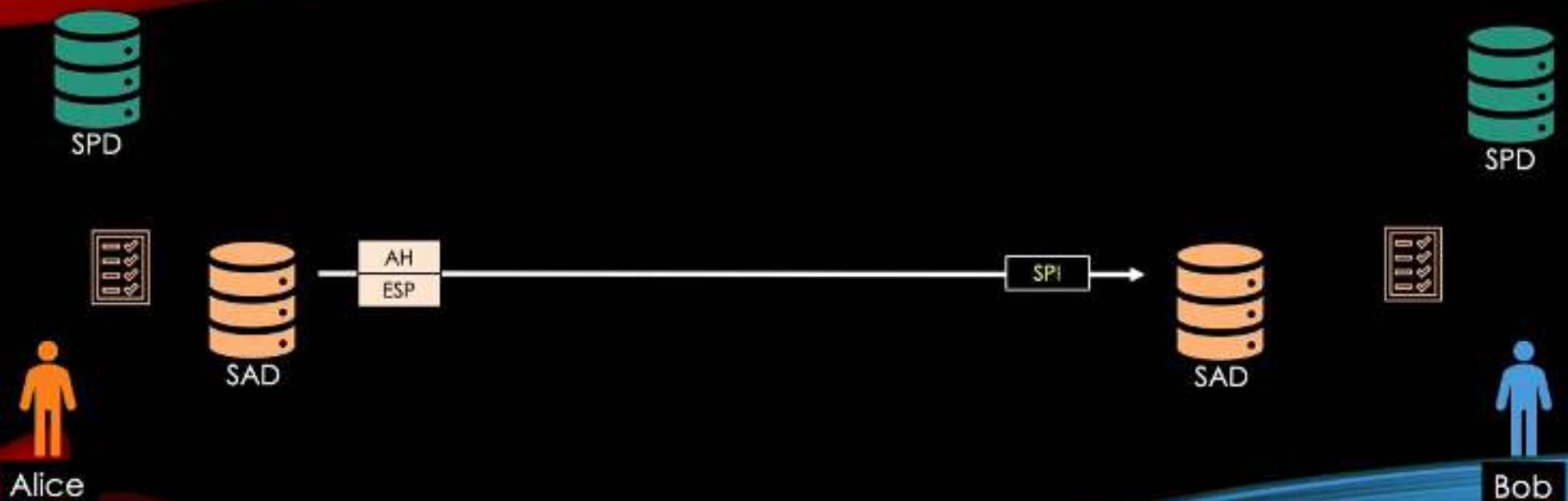
Security and Privacy  
Academy

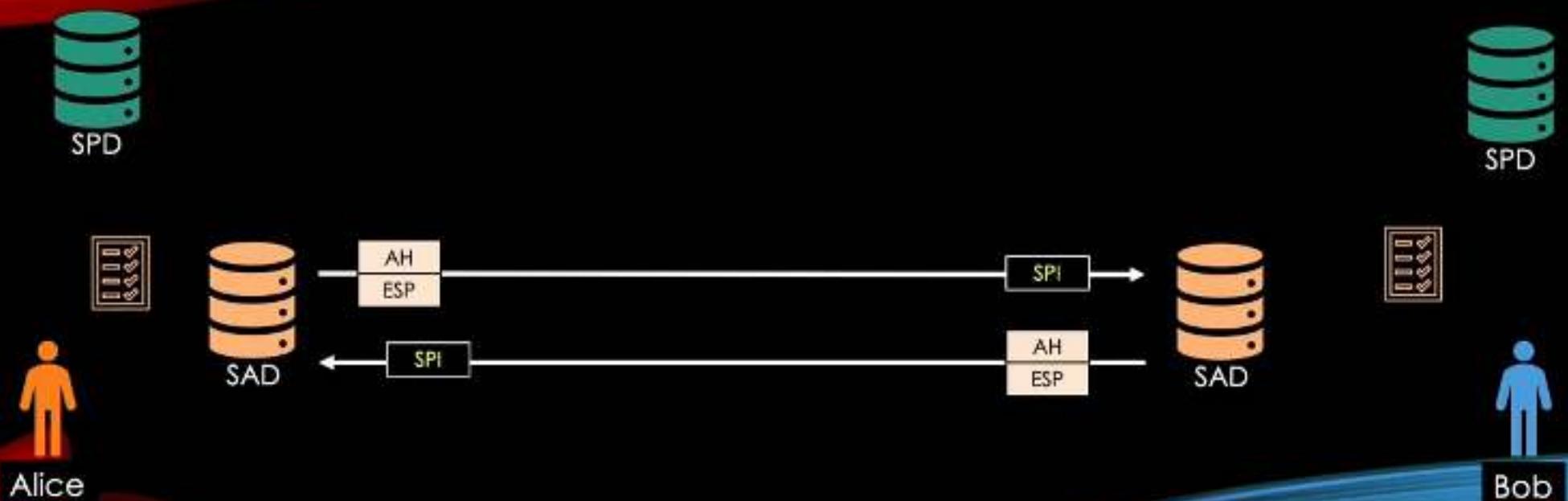












# MPLS Introduction

---

## **Multi-Protocol Label Switching**

# Motivation

---

## □ IP

- The first defined and used protocol
- De facto the only protocol for global Internet working

... but there are disadvantages

---

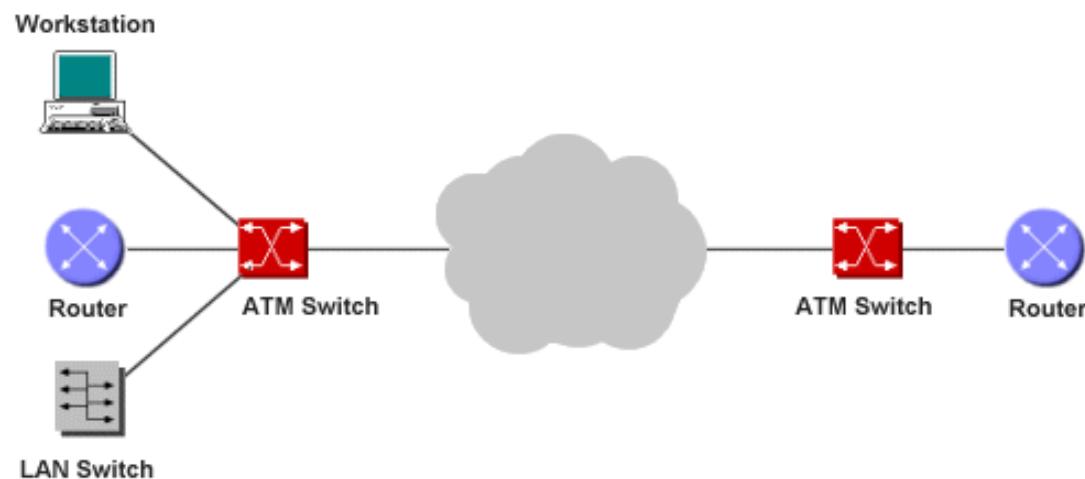
# Motivation (cont.)

---

- IP Routing disadvantages
  - Connectionless
    - e.g. no QoS
  - Each router has to make independent forwarding decisions based on the IP-address
  - Large IP Header
    - At least 20 bytes
  - Routing in Network Layer
    - Slower than Switching
  - Usually designed to obtain shortest path
    - Do not take into account additional metrics

# Motivation (cont.)

- Asynchronous Transfer Mode (ATM)
  - connection oriented
    - Supports QoS
  - fast packet switching with fixed length packets (cells)
  - integration of different traffic types (voice, data, video)



... but there are also disadvantages

# Motivation (cont.)

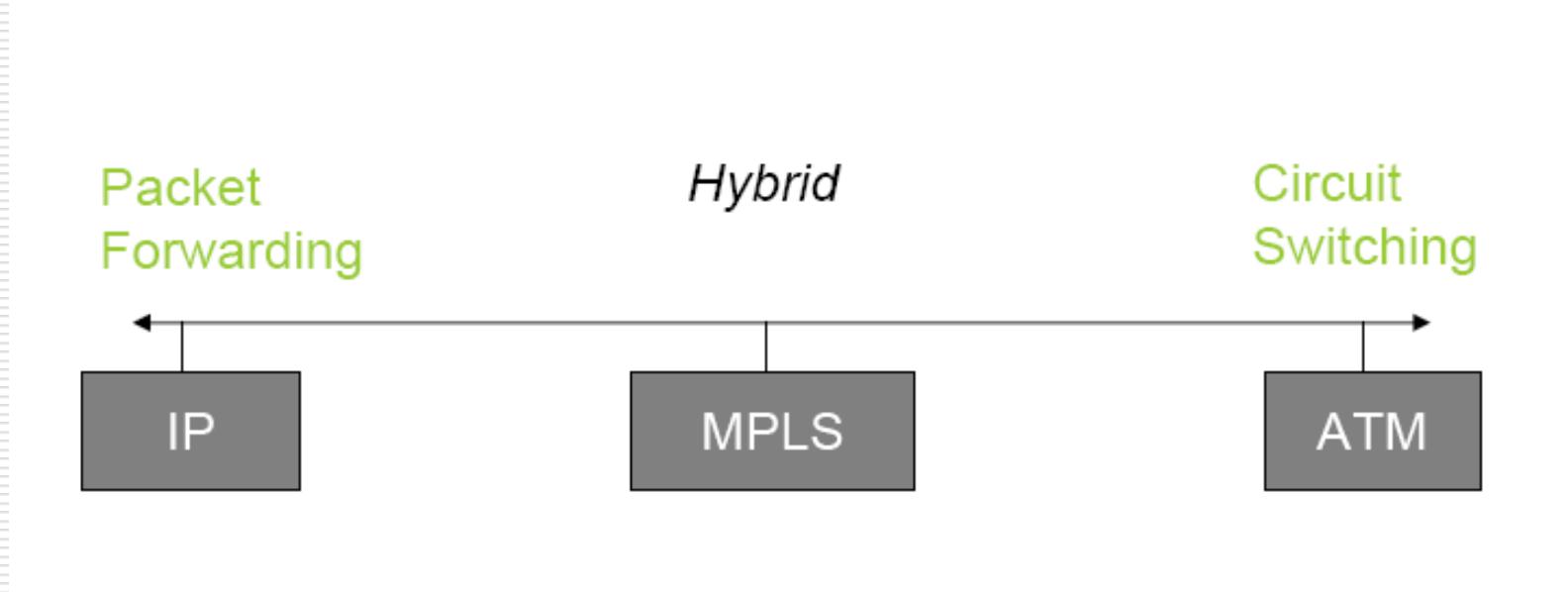
---

## □ ATM disadvantages

- Complex
- Expensive
- Not widely adopted

# Motivation (cont.)

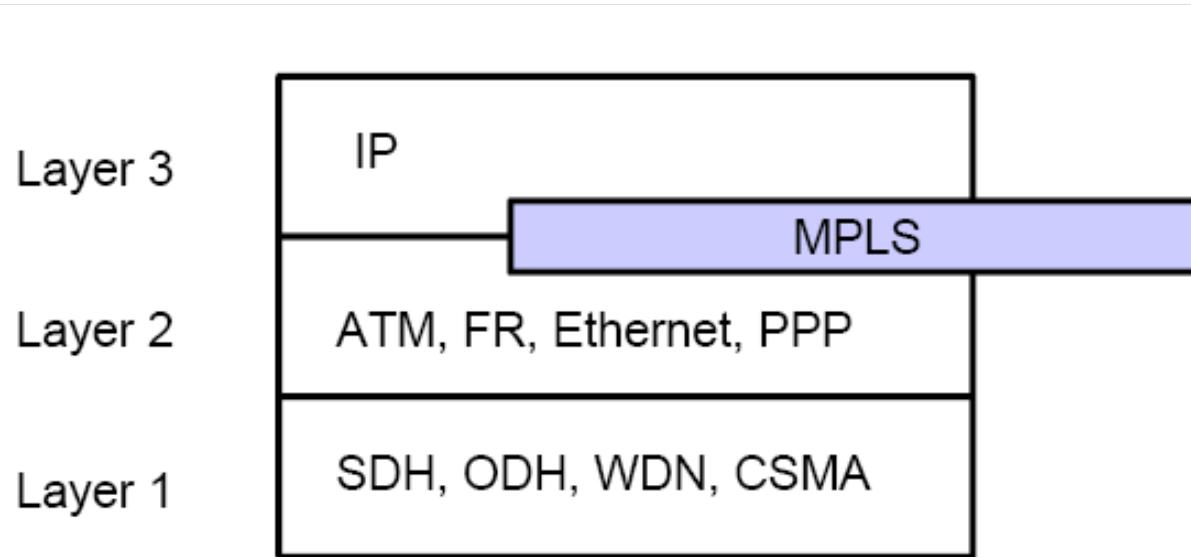
- Idea: Combine the forwarding algorithm used in ATM with IP.



# MPLS Basics

---

- Multi Protocol Label Switching is arranged between Layer 2 and Layer 3



# MPLS Basics (cont.)

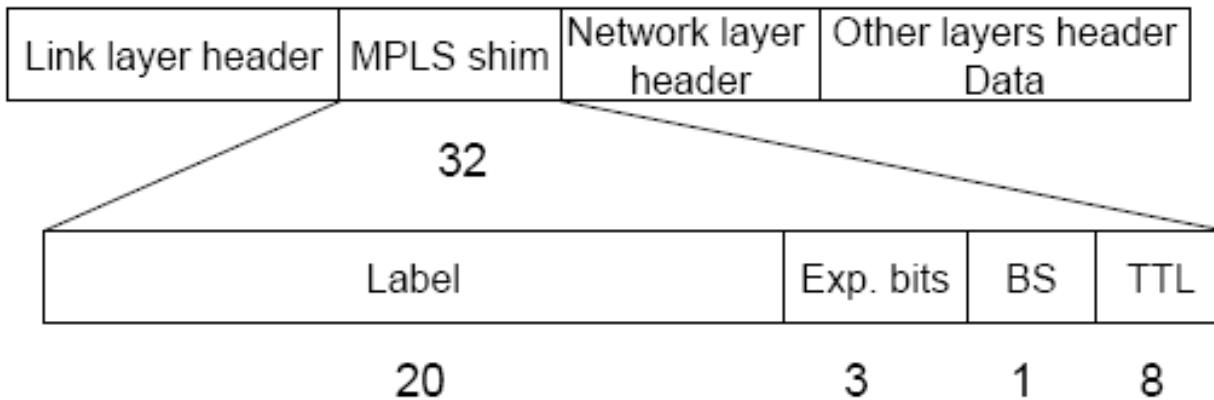
---

## □ MPLS Characteristics

- Mechanisms to manage traffic flows of various granularities (*Flow Management*)
- Is independent of Layer-2 and Layer-3 protocols
- Maps IP-addresses to fixed length labels
- Interfaces to existing routing protocols (RSVP, OSPF)
- Supports ATM, Frame-Relay and Ethernet

# Label

## □ Generic label format



Exp.bits: Experimental Bits, often used for Class of Service  
BS: Bottom of Stack bit, is set if no label follows

# Label Edge Router - LER

---

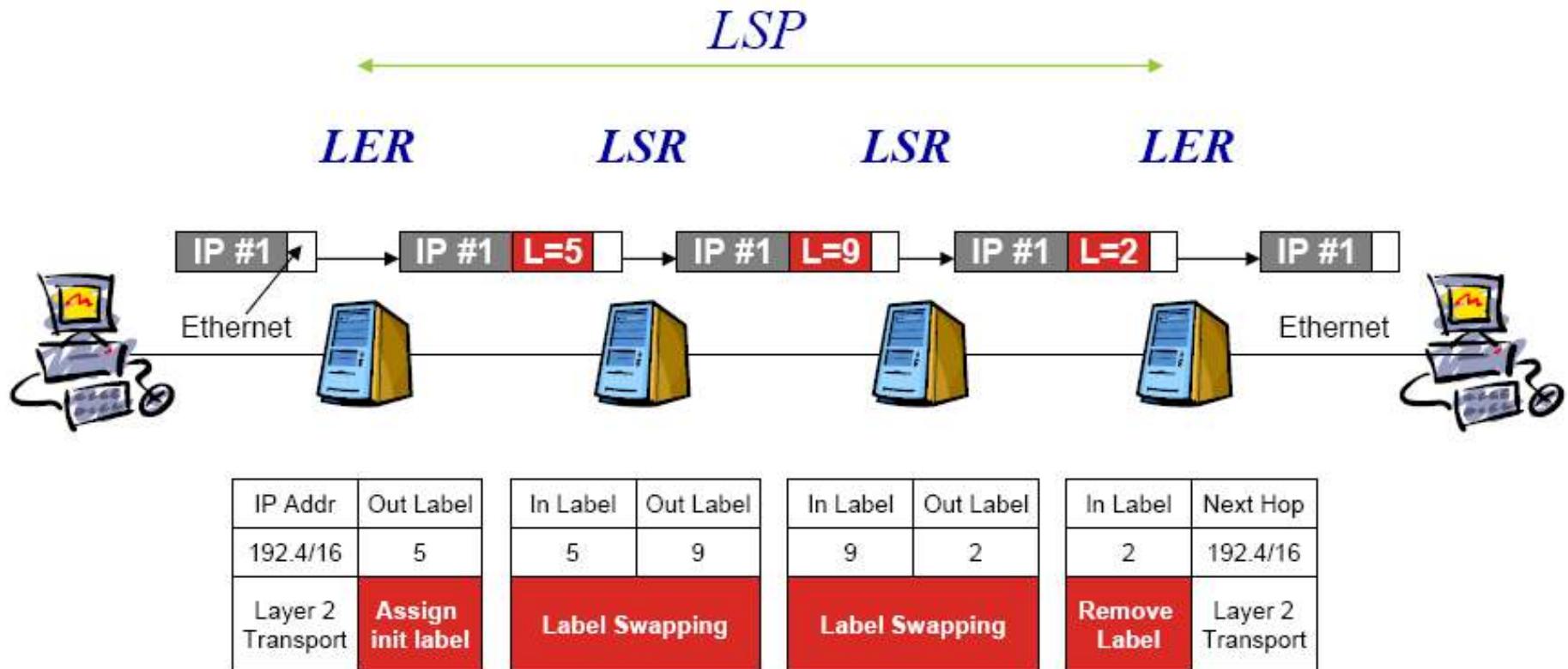
- Resides at the edge of an MPLS network and assigns and removes the labels from the packets.
  - Support multiple ports connected to dissimilar networks (such as frame relay, ATM, and Ethernet).
-

# Label Switching Router - LSR

---

- Is a high speed router in the core on an MPLS network.
  - ATM switches can be used as LSRs without changing their hardware. Label switching is equivalent to VP/VC switching.
-

# Positions of LERs & LSRs



“ROUTE AT EDGE, SWITCH IN CORE”

# Forward Equivalence Class - FEC

---

- Is a representation of a group of packets that share the same requirements for their transport.
  - The assignment of a particular packet to a particular FEC is done just once (when the packet enters the network).
-

# Label-Switched Paths - LSPs

---

- A path is established before the data transmission starts.
  - A path is a representation of a FEC.
-

# MPLS Operation

---

- The following steps must be taken for a data packet to travel through an MPLS domain.
  - label creation and distribution
  - table creation at each router
  - label-switched path creation
  - label insertion/table lookup
  - packet forwarding

# Step 1

---

- Label creation and label distribution
  - Before any traffic begins the routers make the decision to bind a label to a specific FEC and build their tables.
  - In LDP(Label Distribution Protocol), downstream routers initiate the distribution of labels and the label/FEC binding.
  - In addition, traffic-related characteristics and MPLS capabilities are negotiated using LDP.
  - A reliable and ordered transport protocol should be used for the signaling protocol.

# Step 2

---

## ❑ Table creation

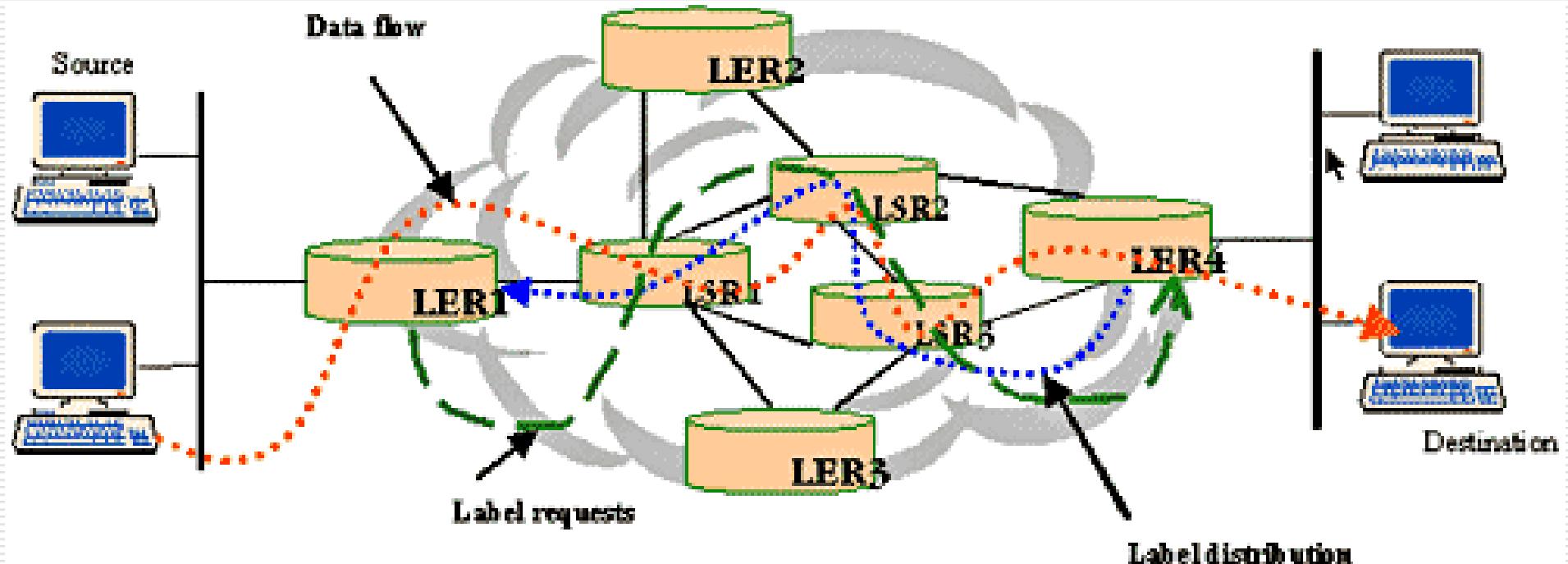
- On receipt of label bindings each LSR creates entries in the label information base (LIB).
- The contents of the table will specify the mapping between a label and an FEC.
  - ❑ mapping between the input port and input label table to the output port and output label table.
  - ❑ The entries are updated whenever renegotiation of the label bindings occurs.

# Example of LIB Table

---

Input Port	Incoming Port Label	Output Port	Outgoing Port Label
1	3	3	6
2	9	1	7

# MPLS Operation Example

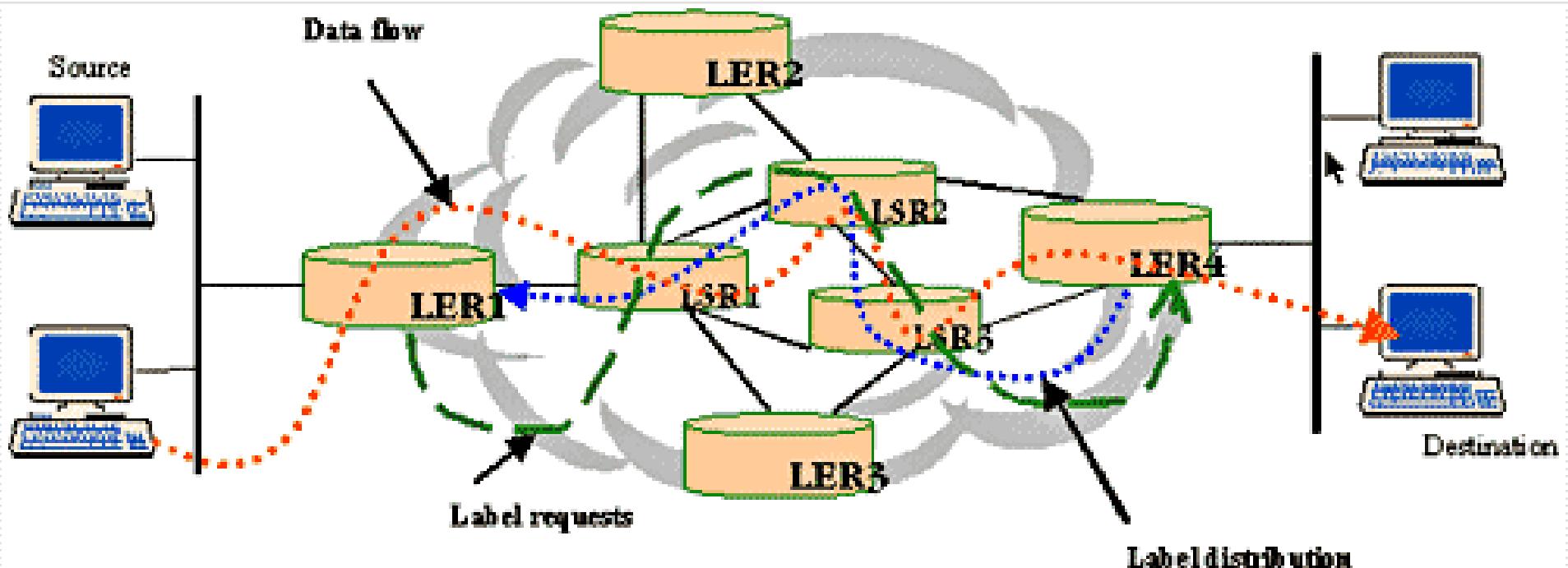


# Step 3

---

- Label switched path creation
  - The LSPs are created in the reverse direction to the creation of entries in the LIBs(label information bases).

# MPLS Operation Example



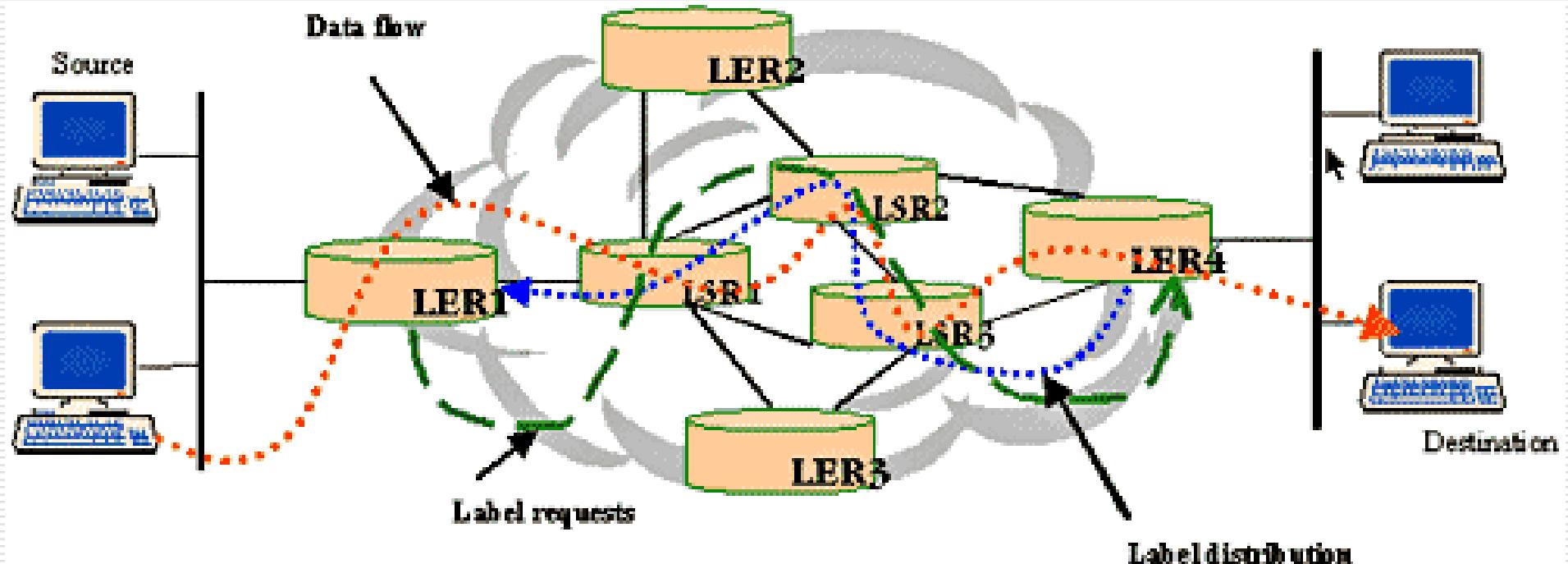
# Step 4

---

## □ Label insertion/table-lookup

- The first router (LER1) uses the LIB table to find the next hop and request a label for the specific FEC.
- Subsequent routers just use the label to find the next hop.
- Once the packet reaches the egress LSR (LER4), the label is removed and the packet is supplied to the destination.

# MPLS Operation Example



# Step 5

---

## □ Packet forwarding

- LER1 may not have any labels for this packet as it is the first occurrence of this request. In an IP network, it will find the longest address match to find the next hop. Let LSR1 be the next hop for LER1.
- LER1 will initiate a label request toward LSR1.
- This request will propagate through the network as indicated by the broken green lines.

# Step 5 (cont.)

---

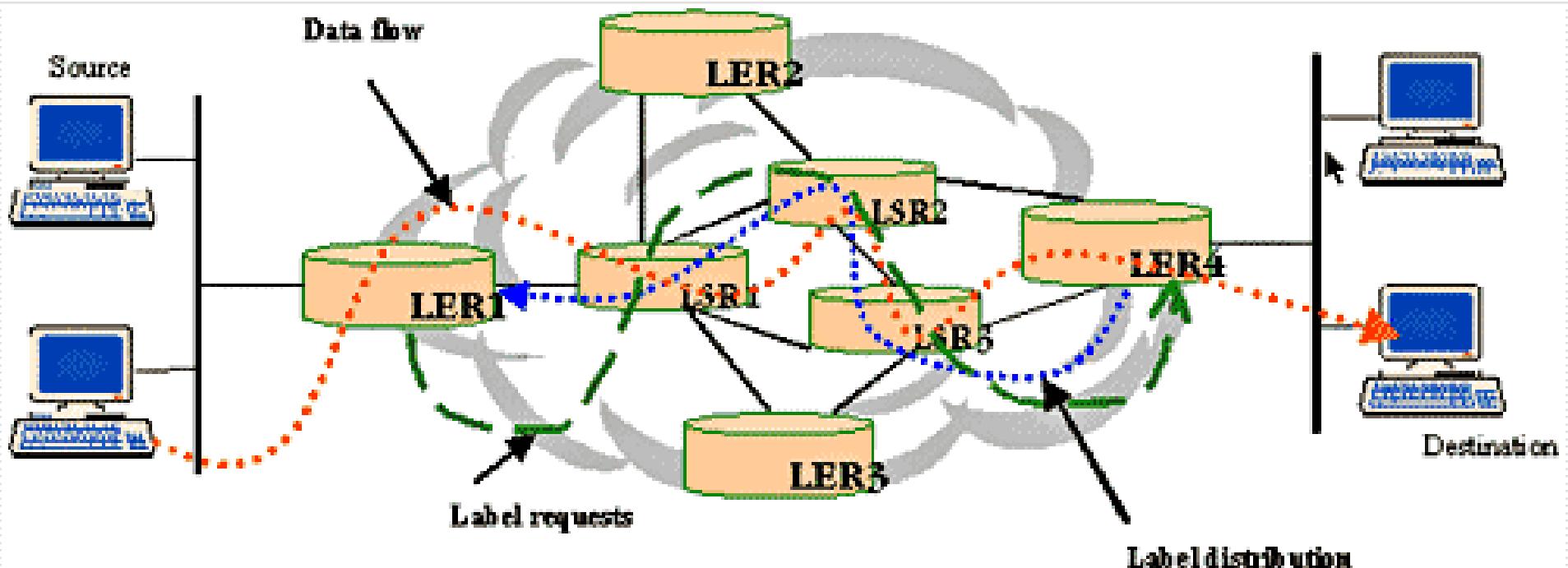
- Each intermediary router will receive a label from its downstream router starting from LER2 and going upstream till LER1. The LSP setup is indicated by the broken blue lines using LDP or any other signaling protocol. If traffic engineering is required, CR-LDP will be used in determining the actual path setup to ensure the QoS/CoS requirements are complied with.
- LER1 will insert the label and forward the packet to LSR1.

# Step 5 (cont.)

---

- Each subsequent LSR, i.e., LSR2 and LSR3, will examine the label in the received packet, replace it with the outgoing label and forward it.
  - When the packet reaches LER4, it will remove the label because the packet is departing from an MPLS domain and deliver it to the destination.
  - The actual data path followed by the packet is indicated by the broken red lines.
-

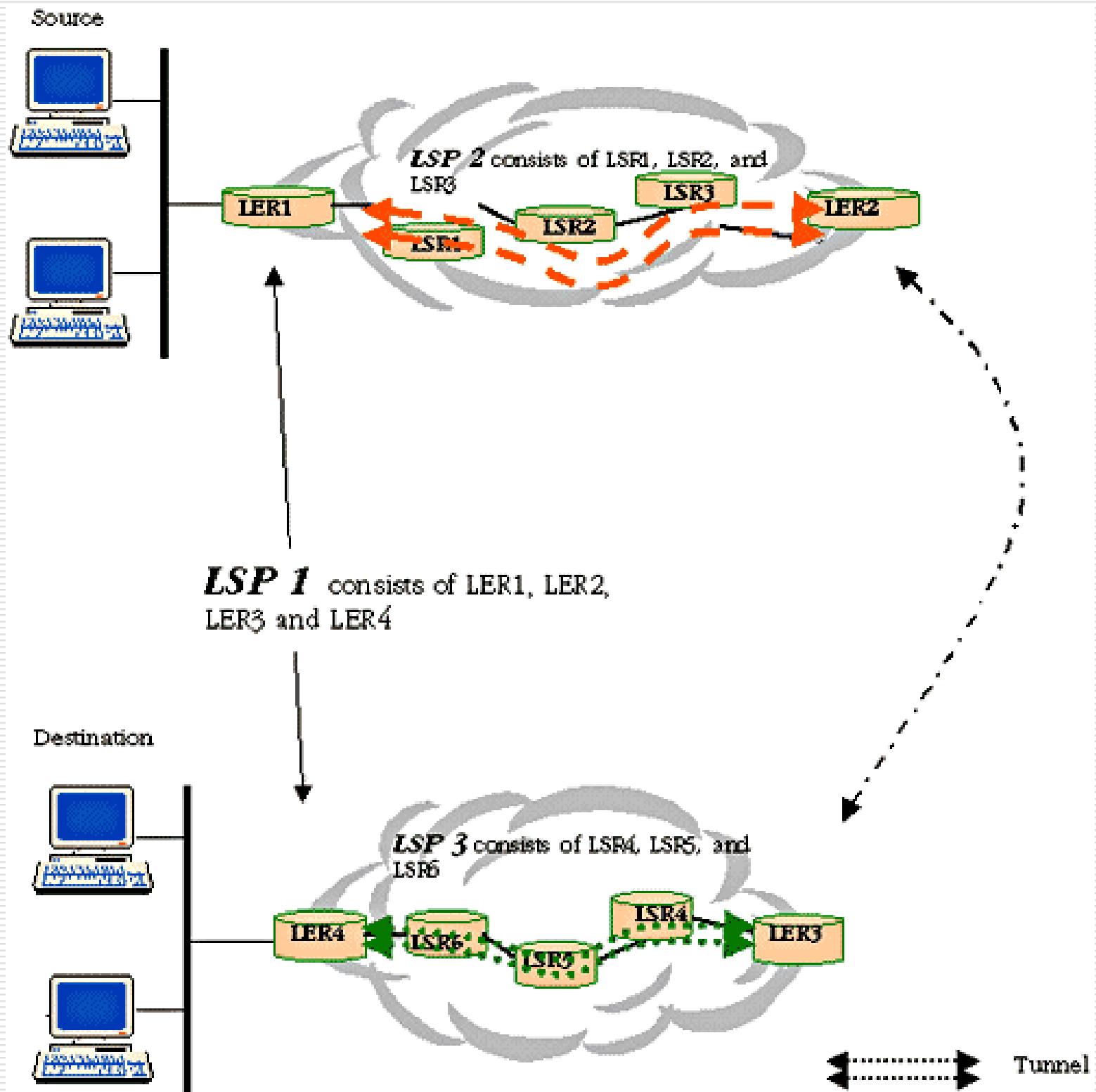
# MPLS Operation Example



# Tunneling in MPLS

---

- Control the entire path of a packet without explicitly specifying the intermediate routers.
    - Creating tunnels through the intermediary routers that can span multiple segments.
  - MPLS based VPNs.
-



# Cellular Phone Security from GSM, LTE, 4G, 5G

Understanding the Evolution of Cellular  
Network Security

Dr. Faraz Masood

# GSM (Global System for Mobile Communications)

Introduction to GSM:

- First widely adopted digital cellular network, launched in 1991.
- Used 2G technology, offering voice and limited data services.

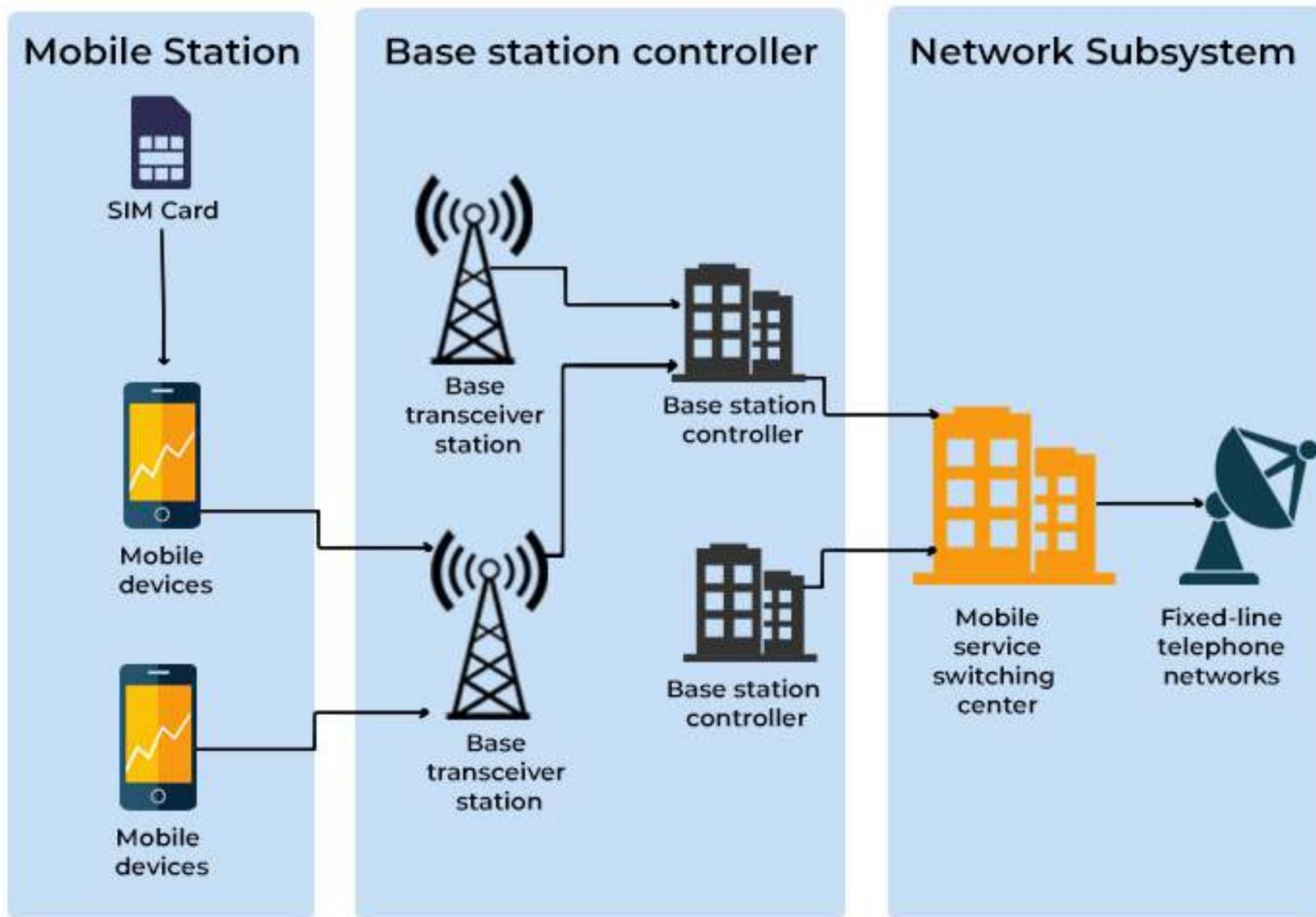
Security Features in GSM:

- A5 encryption algorithm for data protection.
- SIM-based authentication using Ki and IMSI.

Security Flaws in GSM:

- Weak encryption easily broken (e.g., A5/1).
- Vulnerable to IMSI catchers (Stingrays).
- Lack of mutual authentication.

# WORKING OF A GSM NETWORK



# 3G Security Enhancements

Introduction to 3G Networks:

- Launched in the early 2000s, offering higher data rates.
- Based on UMTS (Universal Mobile Telecommunications System).

Security Improvements over GSM:

- Stronger encryption (KASUMI algorithm).
- Mutual authentication between the device and the network.
- Improved data confidentiality and integrity.

Remaining Concerns:

- Vulnerabilities in the air interface.
- Complex key management.

# LTE (Long-Term Evolution)

## Introduction to LTE:

- Launched in 2009, marked the beginning of 4G networks.
- Significant improvements in data speed and capacity.

## Security Enhancements in LTE:

- AES-based encryption for robust security.
- Enhanced key management and mutual authentication.
- Security mechanisms for both user and control planes.

## Challenges in LTE Security:

- Vulnerabilities to IMSI catching and rogue base stations.
- Potential risks from legacy systems fallback.

# 4G (Fourth Generation)

Introduction to 4G:

- 4G is synonymous with LTE, providing high-speed data access.
- Enhanced mobile broadband with improved security over 3G.

4G Security Features:

- Evolved Packet System (EPS) with integrated security protocols.
- End-to-end encryption for both voice and data.
- Stronger protection against man-in-the-middle attacks.

Security Concerns:

- Still susceptible to certain advanced threats like SS7 attacks.
- Interoperability with older networks poses risks.

# 5G (Fifth Generation)

Introduction to 5G:

- Launched in 2019, 5G offers ultra-fast data speeds and low latency.
- Supports IoT, critical communications, and enhanced mobile broadband.

Security Enhancements in 5G:

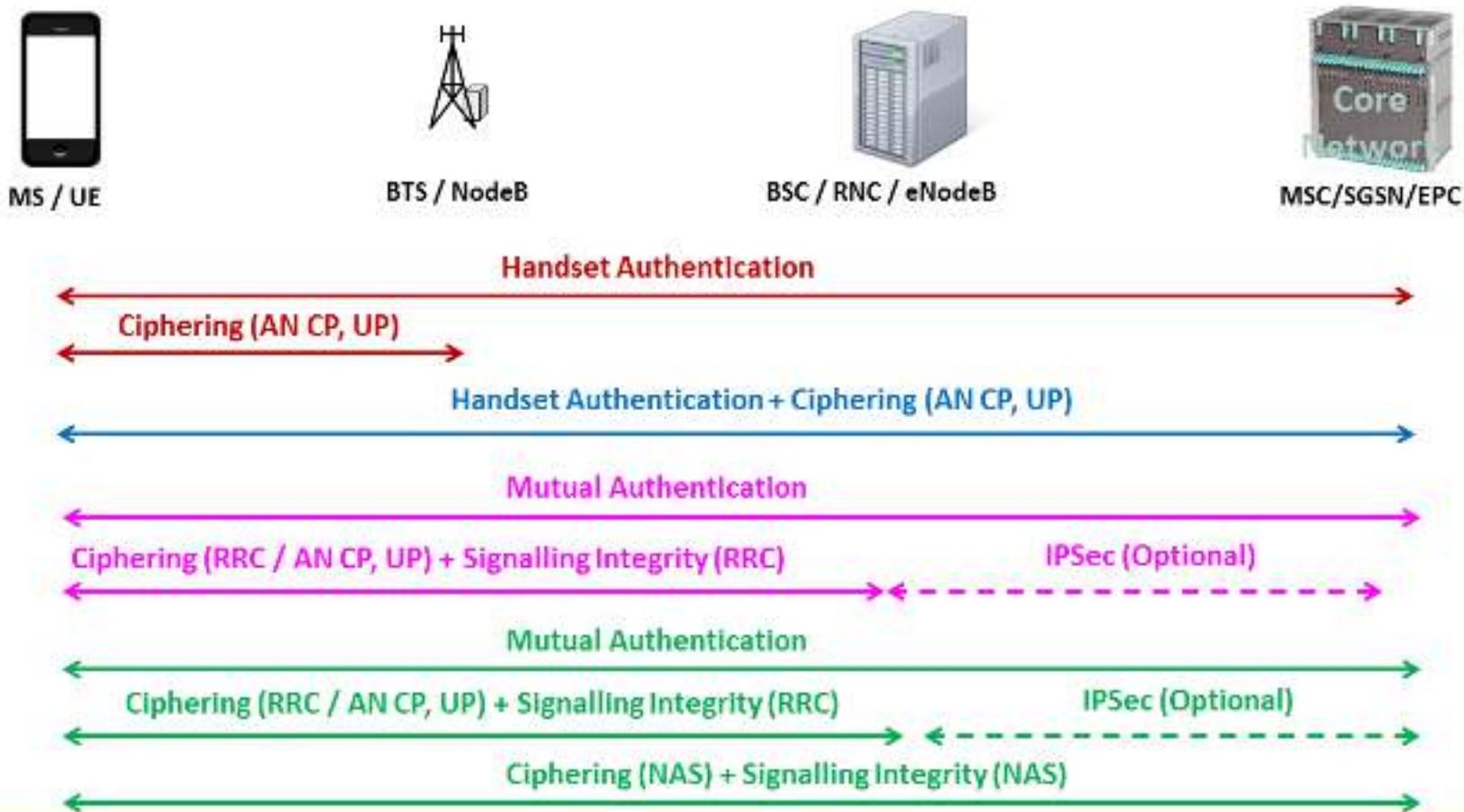
- Unified Authentication Framework (UAF) for robust security.
- Improved encryption with enhanced algorithms.
- Privacy features to protect user identity.
- Network slicing security for isolated virtual networks.

5G Security Challenges:

- Increased attack surface due to more connected devices.
- New vulnerabilities related to software-defined networking (SDN) and network function virtualization (NFV).
- Challenges in securing the supply chain and infrastructure.

# Security Architecture Evolution

AN – Access Network  
AS – Access Stratum  
RRC – Radio Resource Control  
NAS – Non-Access Stratum  
CP – Control Plane  
UP – User Plane



# Comparison of Cellular Network Security

Generation	Key Security Features	Vulnerabilities	Status
GSM (2G)	A5 encryption, SIM-based	Weak encryption, no mutual auth	Deprecated
3G	KASUMI, mutual auth	Air interface vulnerabilities	Still in use
LTE (4G)	AES encryption, EPS	IMSI catching, legacy fallback	Widely used
5G	UAF, advanced encryption	Increased attack surface, SDN/NFV	Emerging standard

# Best Practices for Cellular Security

Tips for Securing Cellular Devices:

Always update device software to the latest version.

Use strong, unique passwords and biometric authentication.

Be cautious with public Wi-Fi and use a VPN when necessary.

Disable legacy network fallback if possible.

Monitor for unusual activity and use security apps.

# Conclusion

Summary:

Cellular network security has evolved significantly from GSM to 5G.

Each generation brought improvements, but new challenges emerged.

5G offers the most robust security features, but vigilance is required to address emerging threats.

# Q&A

## Questions and Answers

Open the floor for questions. Clarify any doubts and provide additional insights where necessary.

# References

3GPP documentation on cellular security.

Various white papers and research articles on GSM, LTE, and 5G security.

Industry reports from organizations like GSMA and NIST.

# WiFi (Wireless) Password Security - WEP, WPA, WPA2, WPA3, WPS Explained

Understanding WiFi Security Protocols

Dr. Faraz Masood

26<sup>th</sup> Aug 2024

# Introduction

WiFi networks are essential for connectivity but are vulnerable to various attacks.

Proper security measures are crucial to protect sensitive information.

This presentation will explore the evolution of WiFi security protocols: WEP, WPA, WPA2, WPA3, and WPS.

# WEP (Wired Equivalent Privacy)

What is WEP?

WEP was the first security protocol designed for WiFi networks, introduced in 1997.

It uses RC4 encryption with 40-bit and later 104-bit keys.

Security Flaws in WEP:

The encryption key is static, making it vulnerable to cracking.

Tools like Aircrack-ng can break WEP encryption within minutes.

WEP is deprecated and should not be used for securing networks.

# WEP (Wired Equivalent Privacy)

- Wired Equivalent Privacy (WEP)
  - Semitic Encryption Keys
  - Small Key Size
    - Initially 64 Bits
    - Later 128 Bits
  - Initialization Vector (IV) Added to Protect Encryption Key
    - 24 Bits (Part of Key)
    - $64 - 24 = 40$
    - $128 - 24 = 104$
-

# WEP (Wired Equivalent Privacy)



Alice

Symmetric Key



WEP Key: Tuna-Can



Bob



Charlie

---

# WEP (Wired Equivalent Privacy)



Alice

WEP Key: Tuna-Can

Symmetric Key



WEP Key: Tuna-Can



Bob

WEP Key: Tuna-Can



Charlie

# WEP (Wired Equivalent Privacy)



Alice

WEP Key: Tuna-Can

Symmetric Key



WEP Key: Tuna-Can



Bob  
WEP Key: Tuna-Can



Charlie  
WEP Key: Tuna-Can

# WEP (Wired Equivalent Privacy)



Alice



# WEP (Wired Equivalent Privacy)



Alice

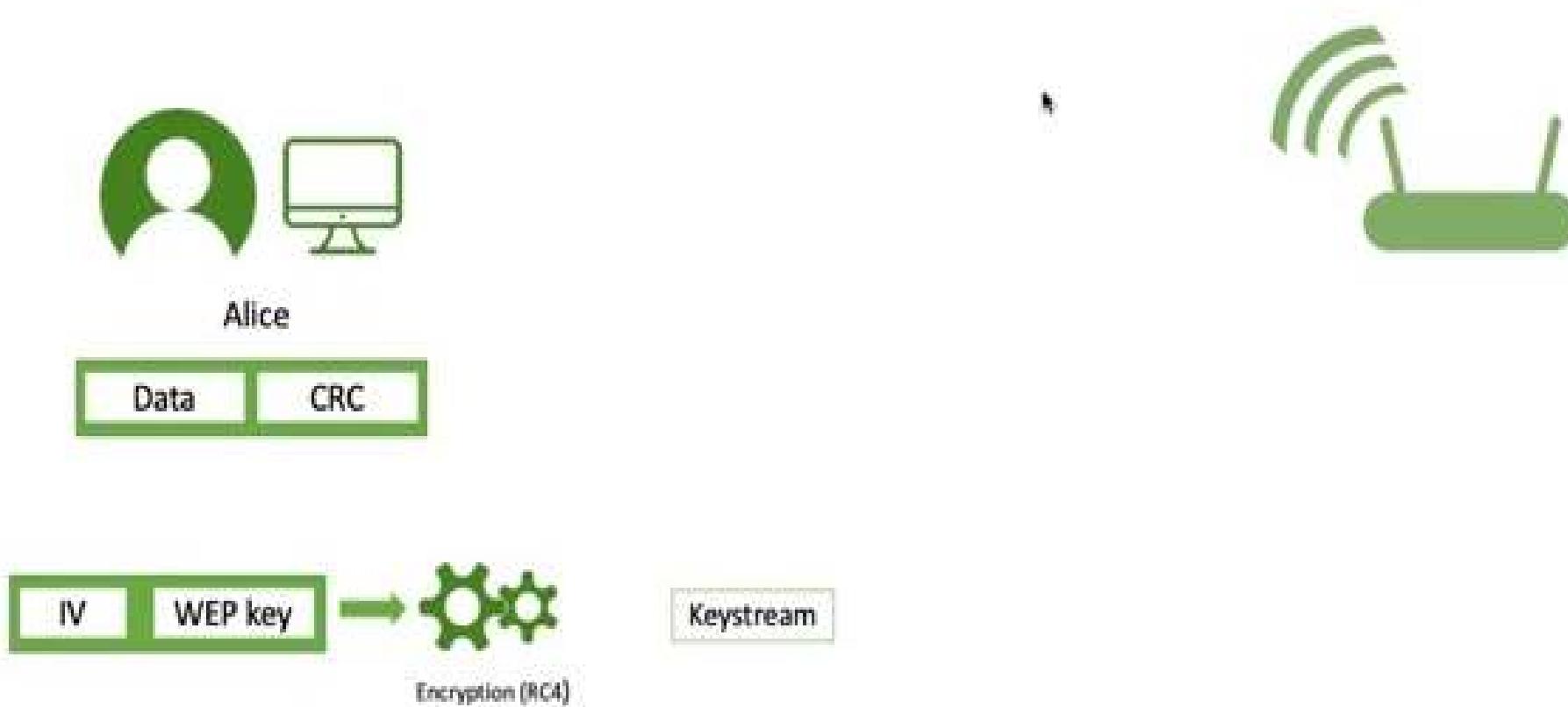


---

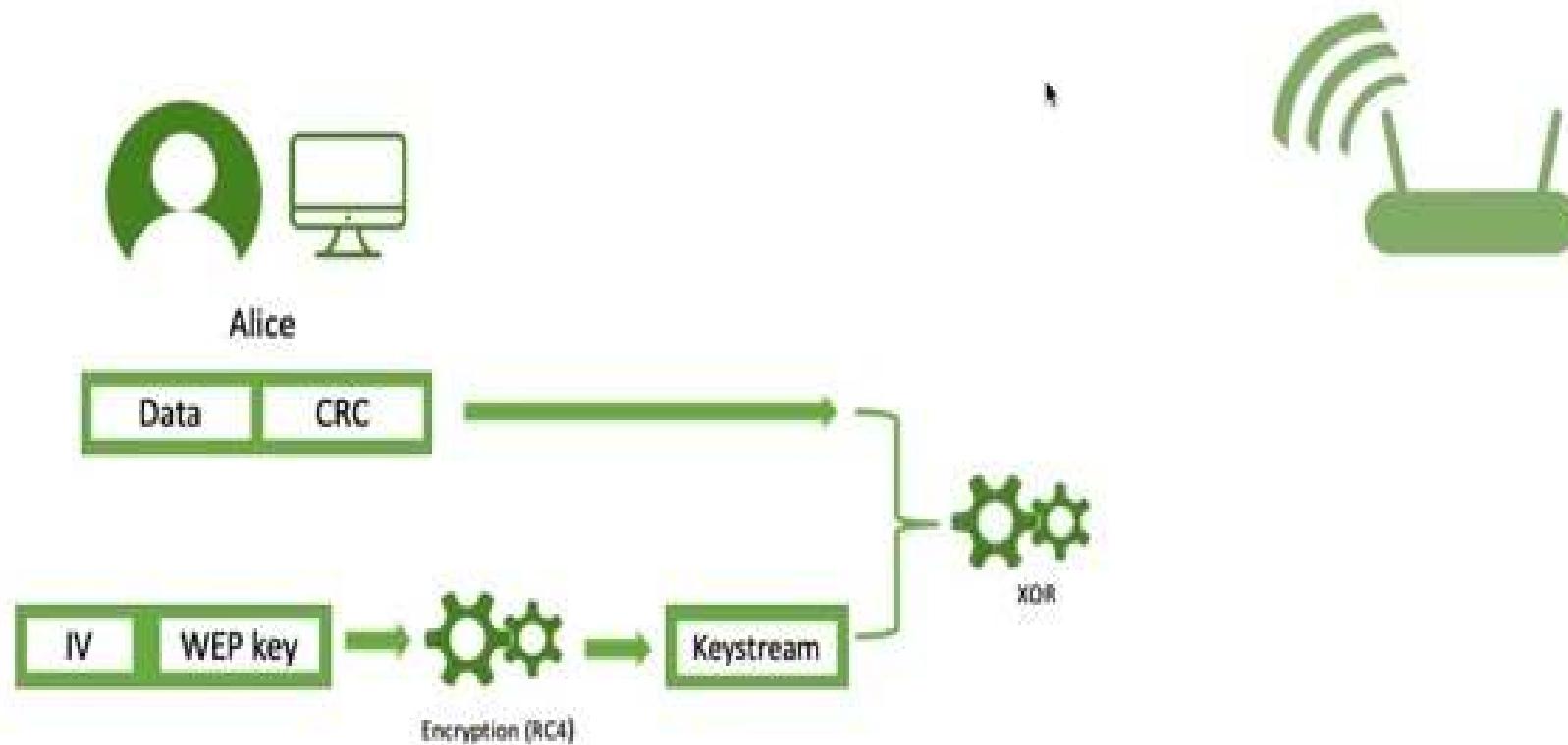
# WEP (Wired Equivalent Privacy)



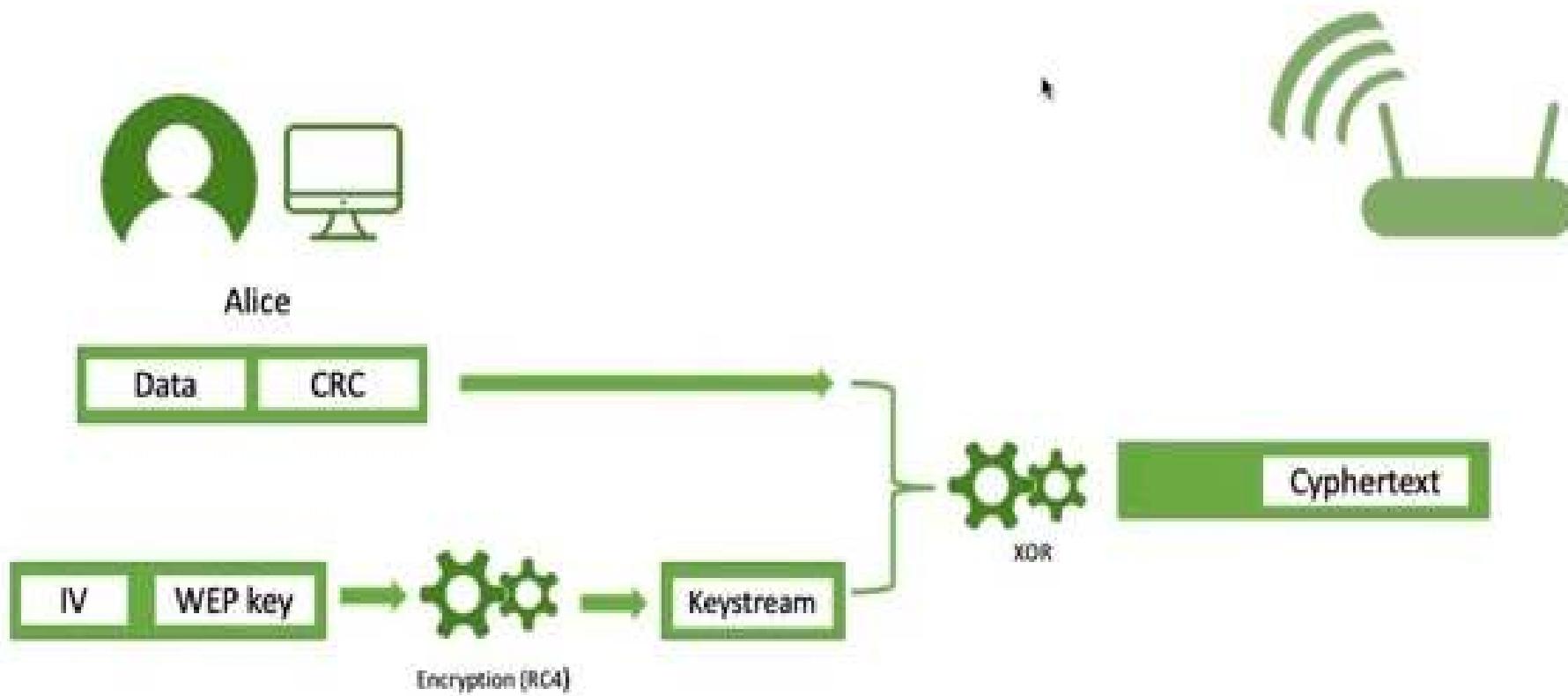
# WEP (Wired Equivalent Privacy)



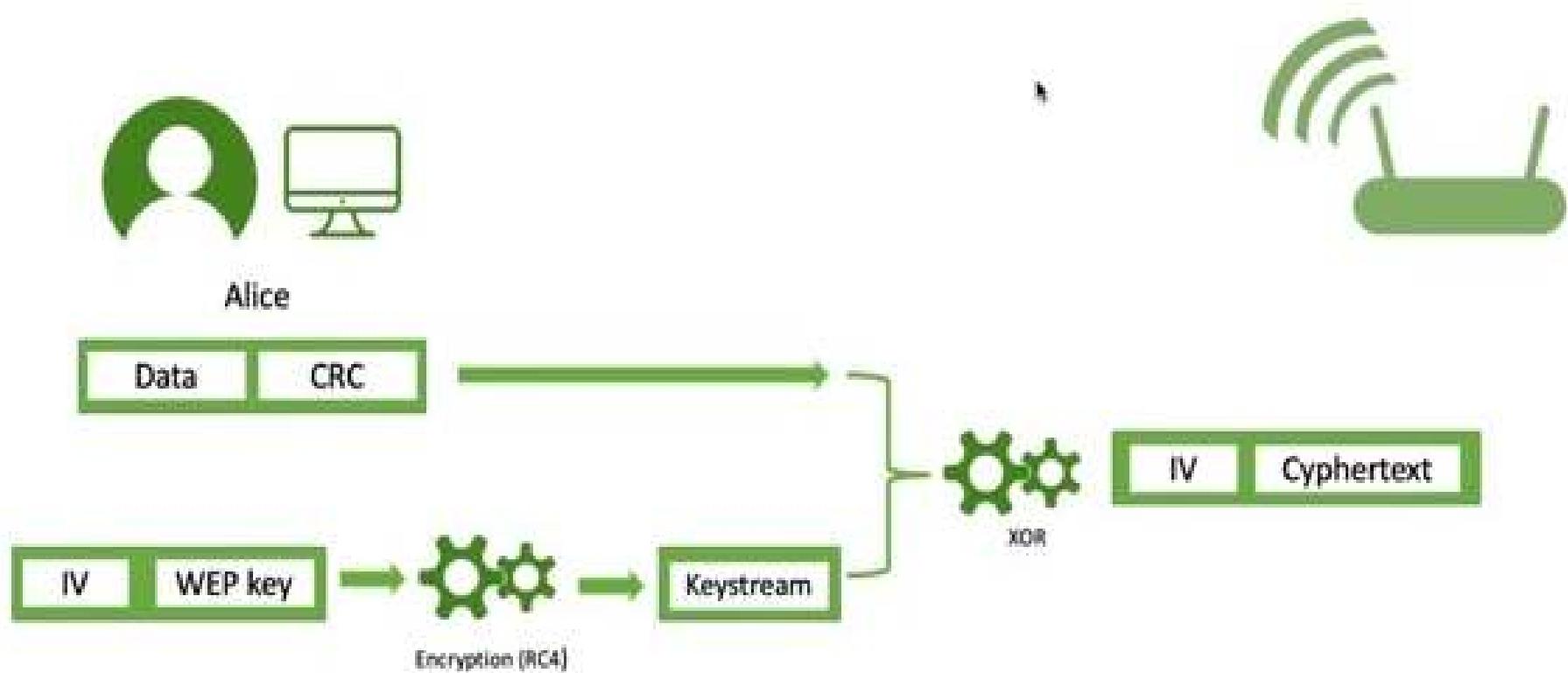
# WEP (Wired Equivalent Privacy)



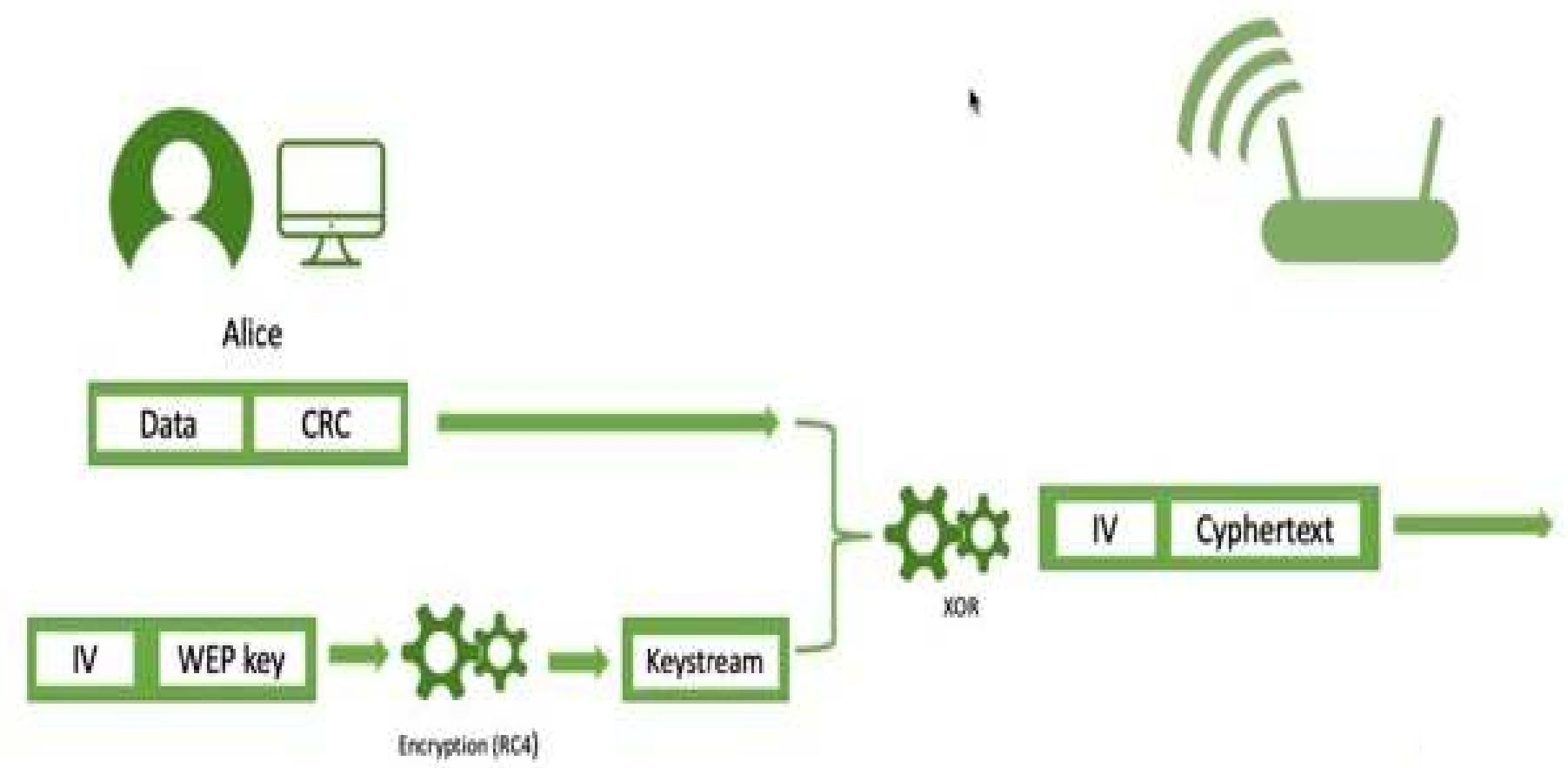
# WEP (Wired Equivalent Privacy)



# WEP (Wired Equivalent Privacy)



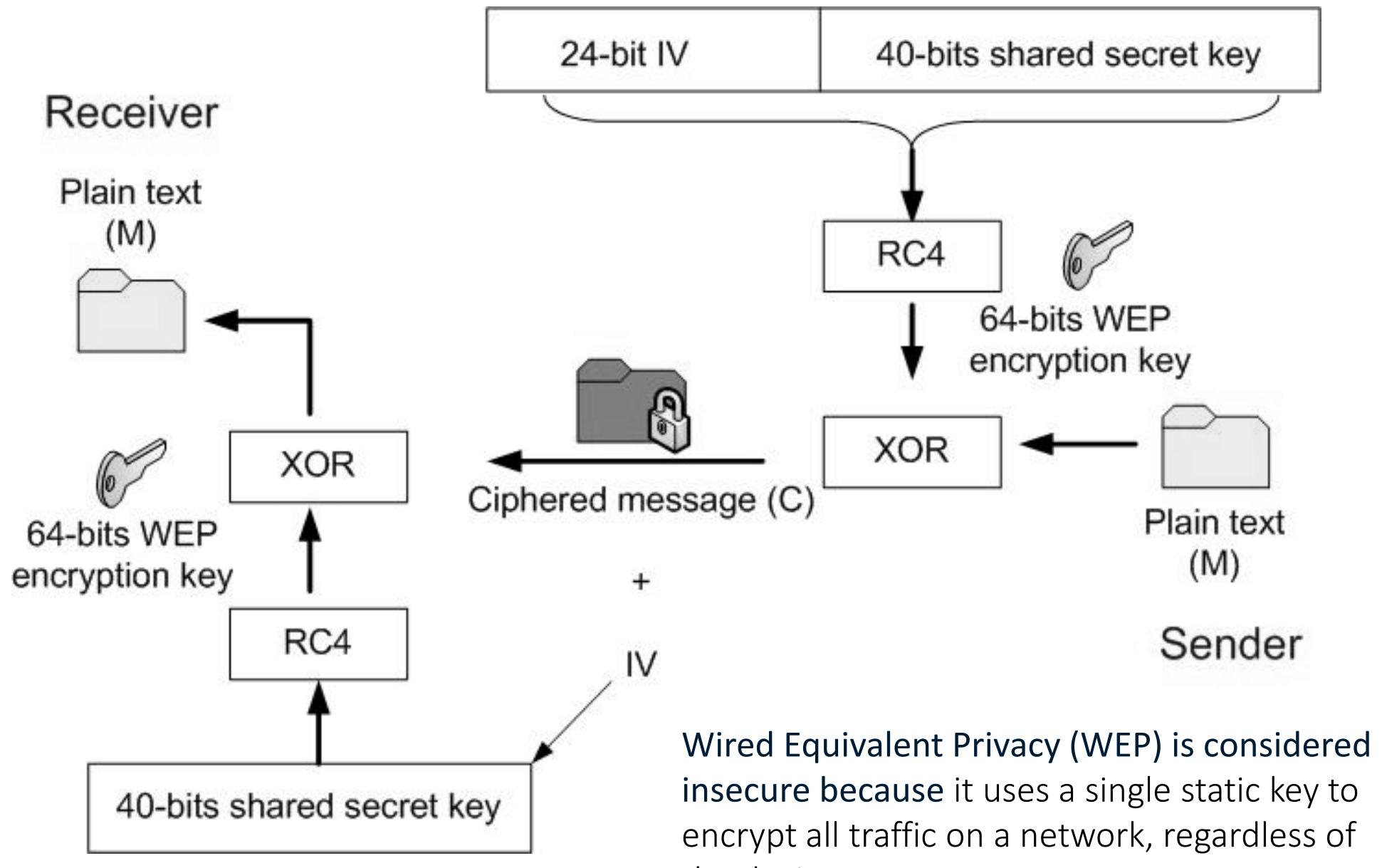
# WEP (Wired Equivalent Privacy)



# WEP (Wired Equivalent Privacy)

- Small IV size (24 bits)
  - 16,777,216 different IV possibilities
  - Then IV Values Will Be Repeated
  - Some IV values Were Weak
    - Math Process Could Reverse This to Determine Encryption Key
    - Create a Large Volume of Traffic to Get the Needed Packets
      - Automated Tools Make This Relatively Quick

---



# WPA (WiFi Protected Access)

## Introduction to WPA

WPA was introduced in 2003 as an interim solution to replace WEP.

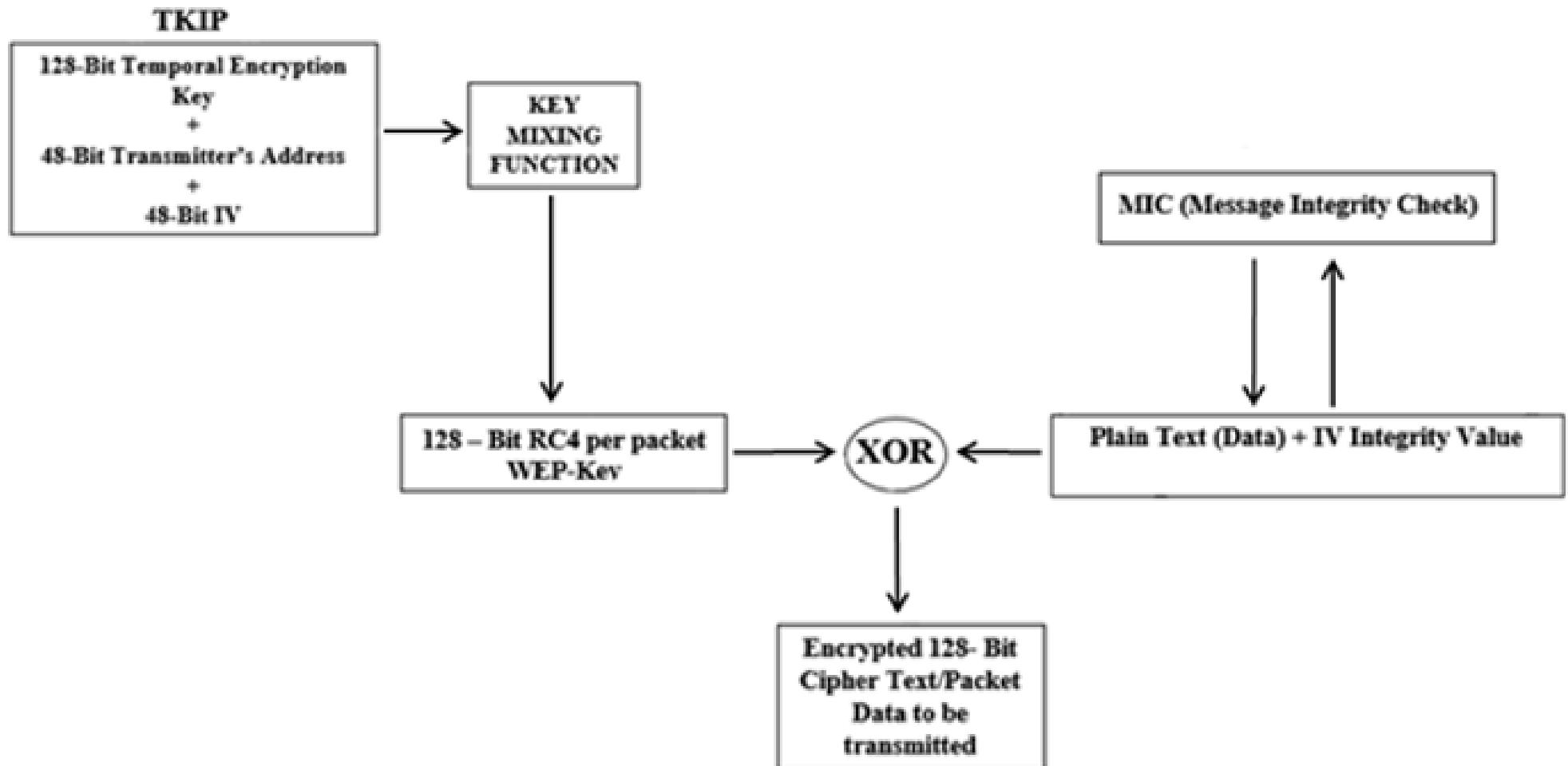
It employs TKIP (Temporal Key Integrity Protocol) for better encryption.

## Security Enhancements:

Dynamic key generation adds complexity to encryption.

WPA provides better security than WEP but is still susceptible to attacks like dictionary attacks on pre-shared keys.

## WPA



# WPA2 (WiFi Protected Access II)

## Introduction to WPA2

Introduced in 2004, WPA2 became the industry standard for WiFi security.

It uses AES (Advanced Encryption Standard) for encryption, replacing TKIP.

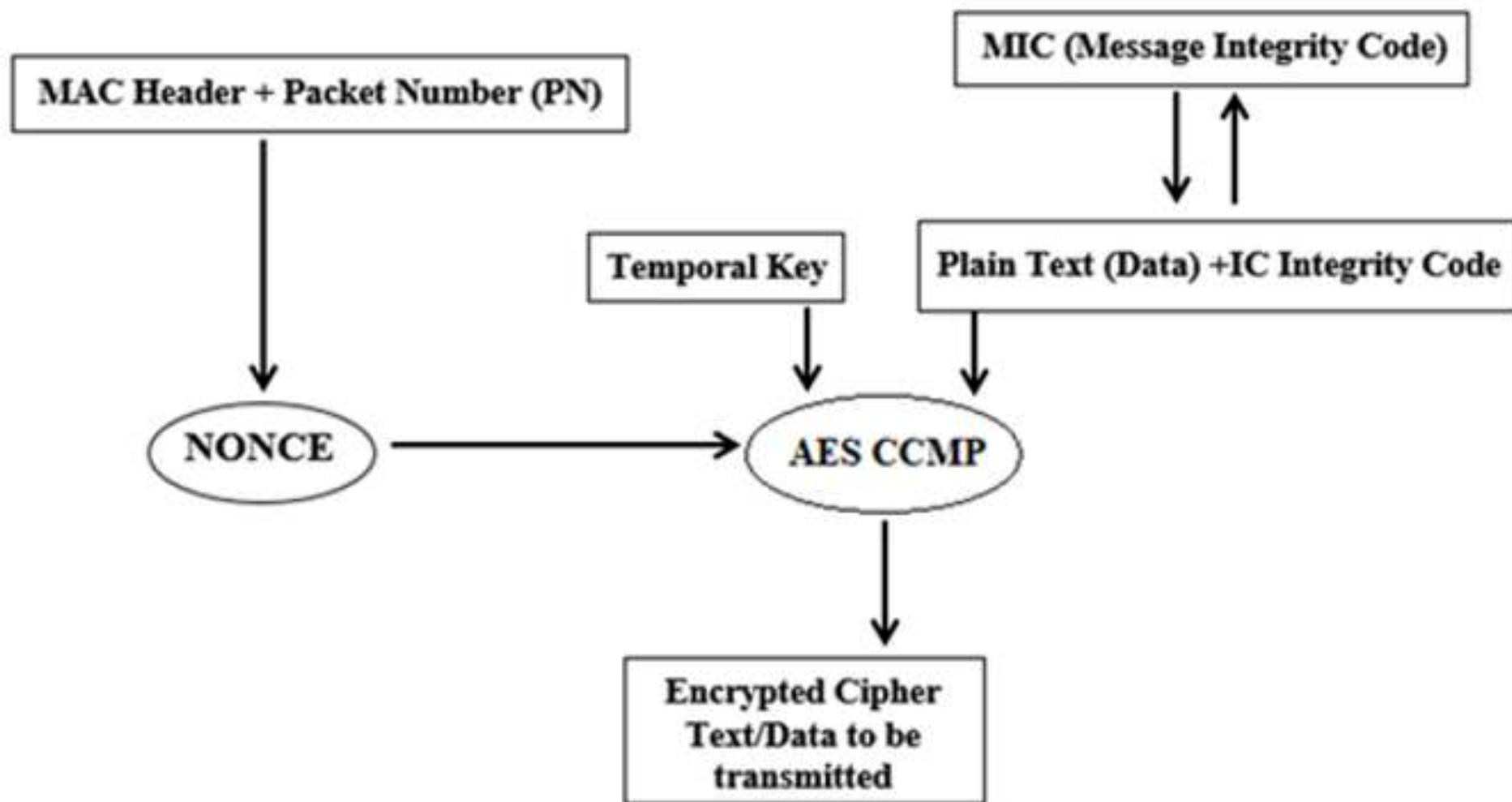
## Key Features of WPA2:

Offers robust encryption with 128-bit keys.

Mandatory for WiFi CERTIFIED™ devices since 2006.

Vulnerabilities like the KRACK attack (Key Reinstallation Attack) exposed some weaknesses, but it remains widely used.

## WPA-2



# WPA3 (WiFi Protected Access III)

What is WPA3?

Launched in 2018, WPA3 is the latest WiFi security standard.

It addresses vulnerabilities found in WPA2 and introduces stronger protections.

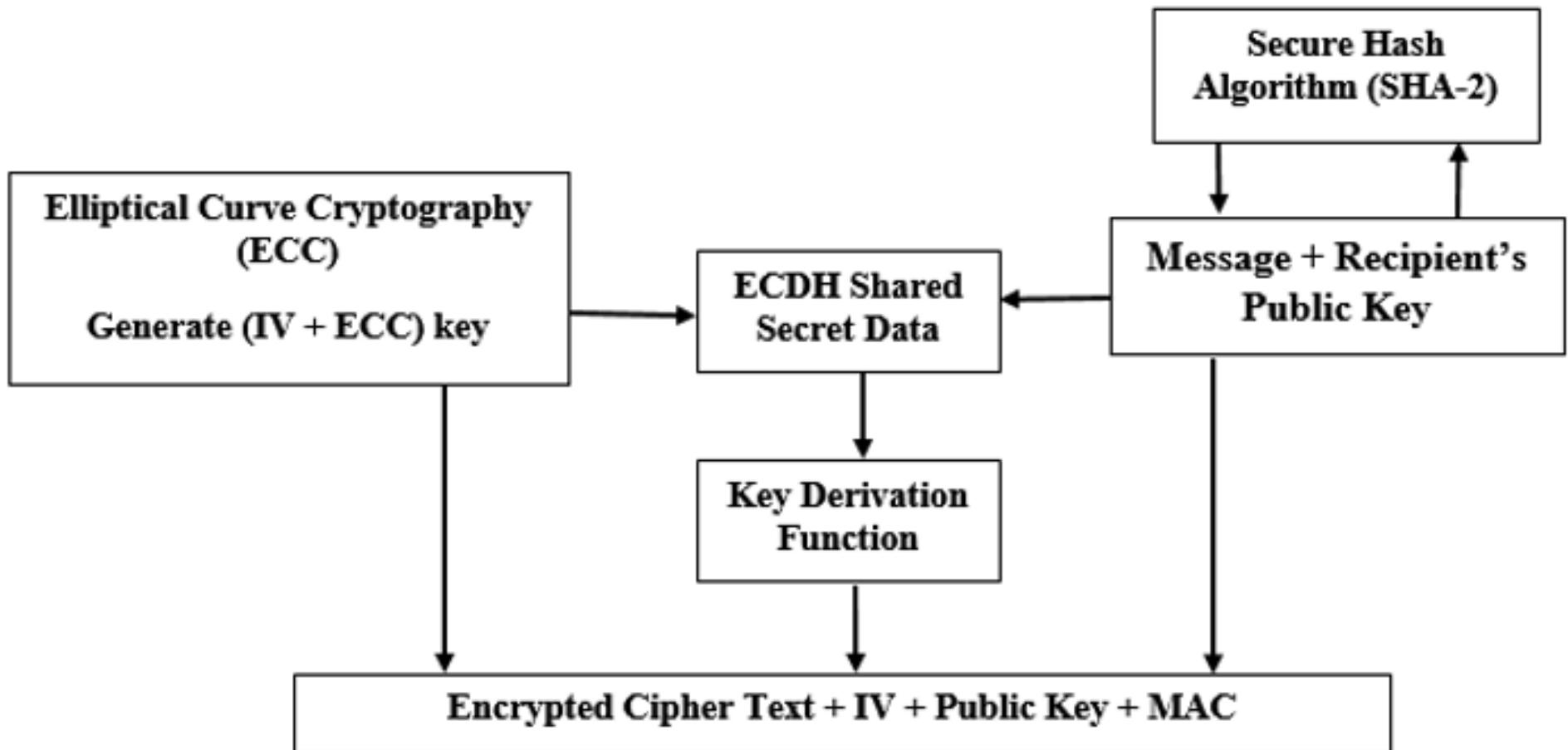
Security Enhancements in WPA3:

Protects against brute-force attacks with Simultaneous Authentication of Equals (SAE).

Provides forward secrecy, ensuring that past sessions cannot be decrypted even if the password is compromised later.

Improves security in open networks through individualized data encryption.

## WPA-3



# WPS (WiFi Protected Setup)

What is WPS?

WPS was designed to simplify the process of connecting devices to a WiFi network, introduced in 2006.

Methods include using a PIN, push-button configuration, or NFC.

Security Concerns with WPS:

The PIN method is highly vulnerable to brute-force attacks.

Once the WPS PIN is cracked, the network's WPA/WPA2 key can be easily retrieved.

Disabling WPS is recommended to prevent unauthorized access.



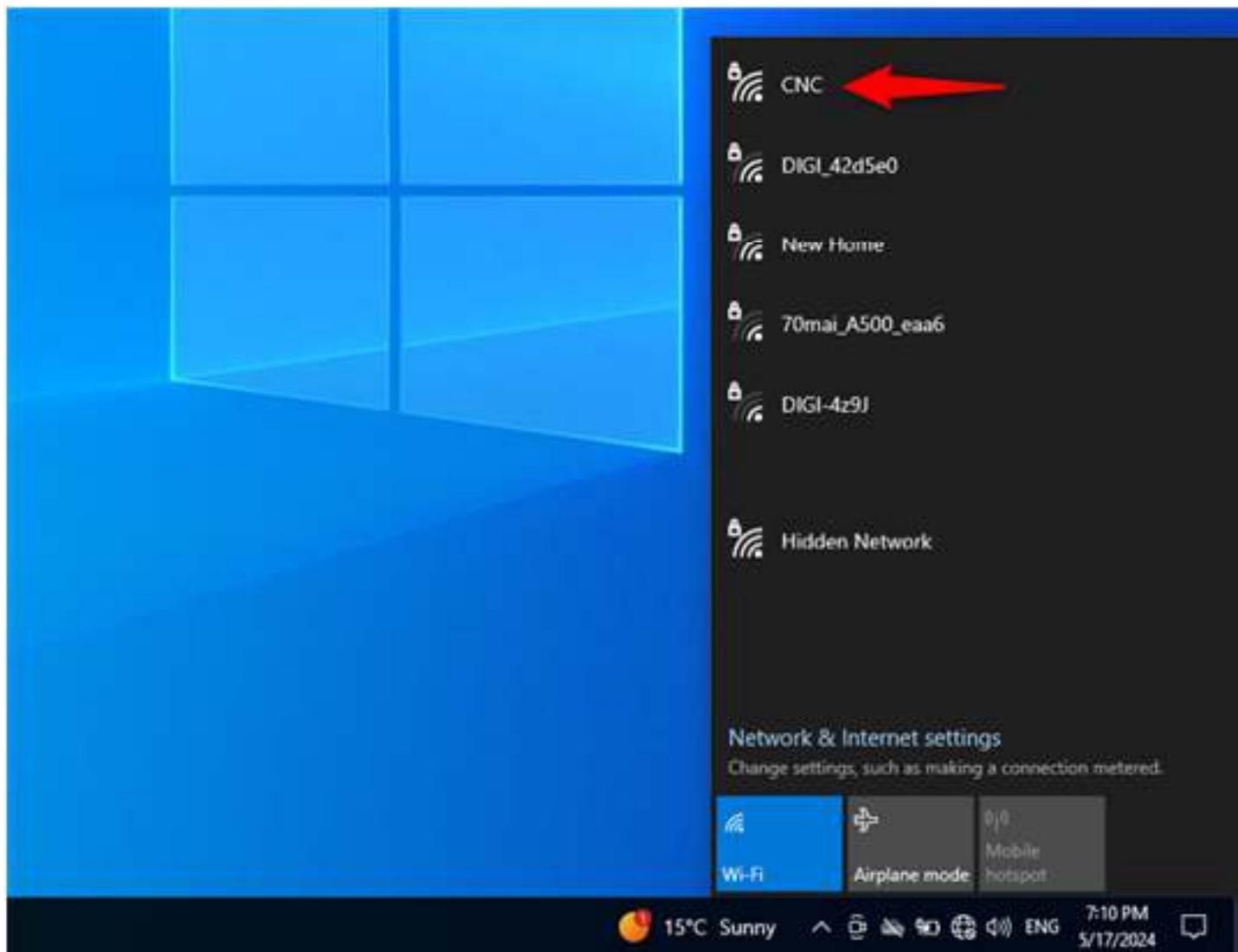
15°C Sunny

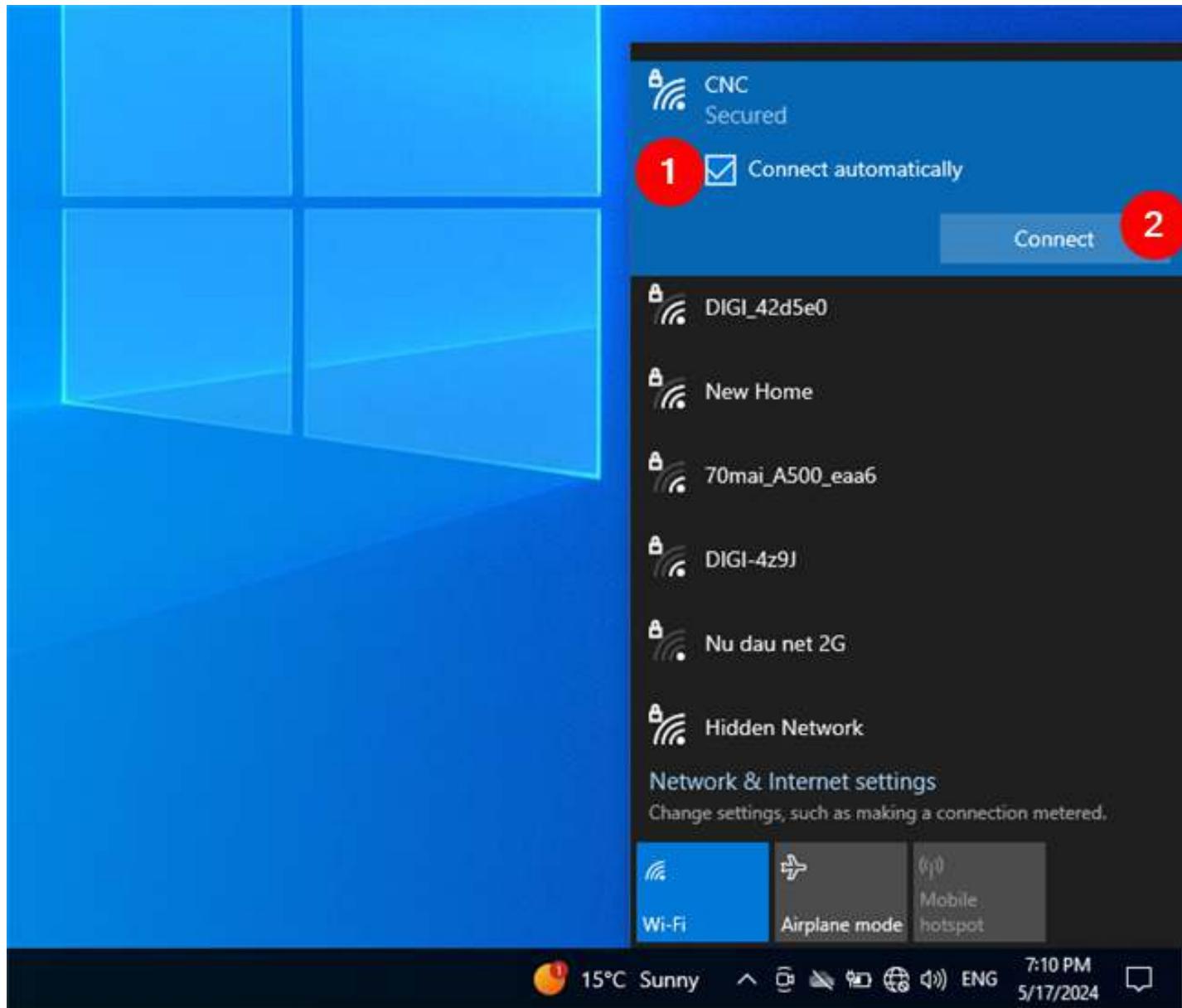


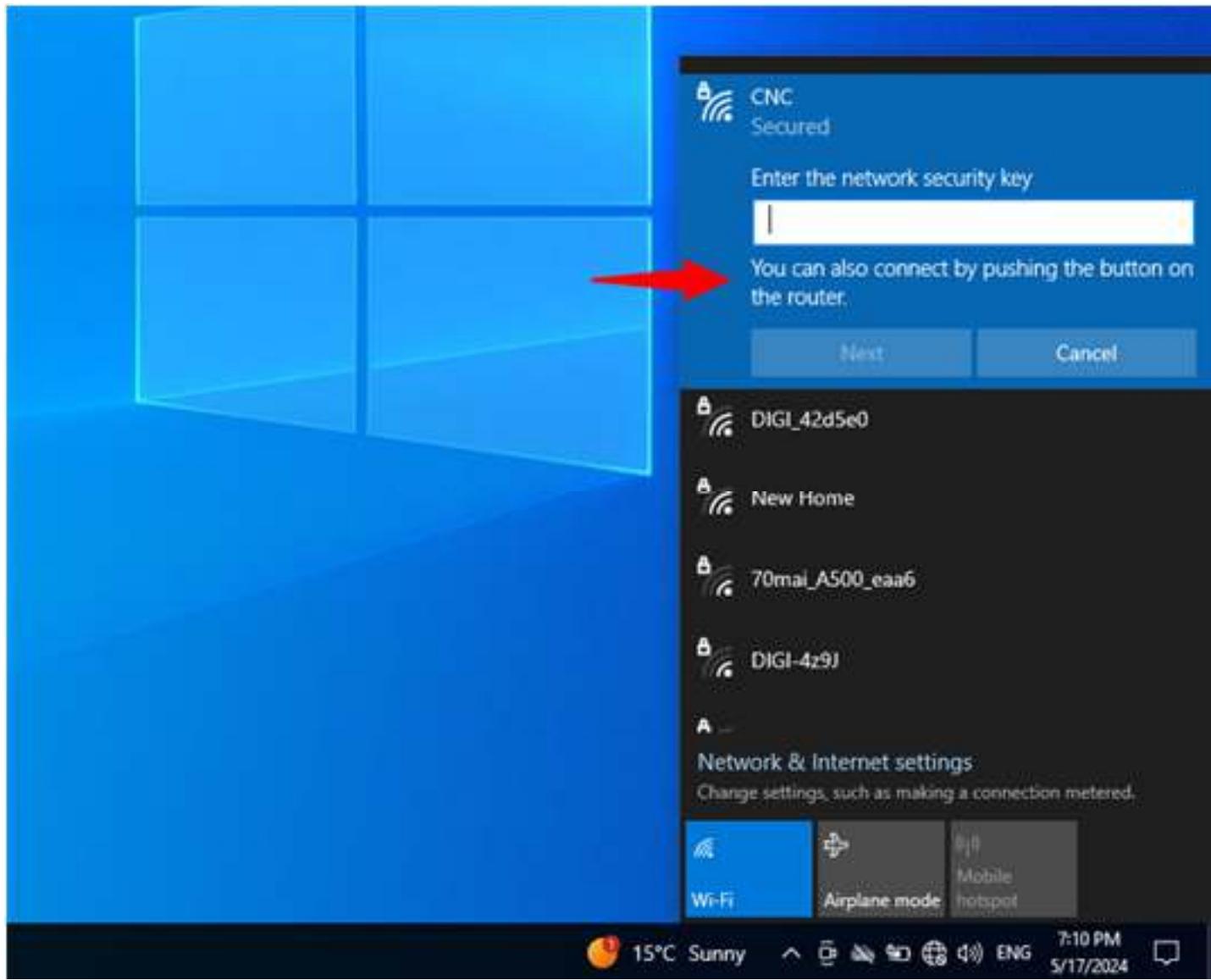
ENG

7:10 PM  
5/17/2024



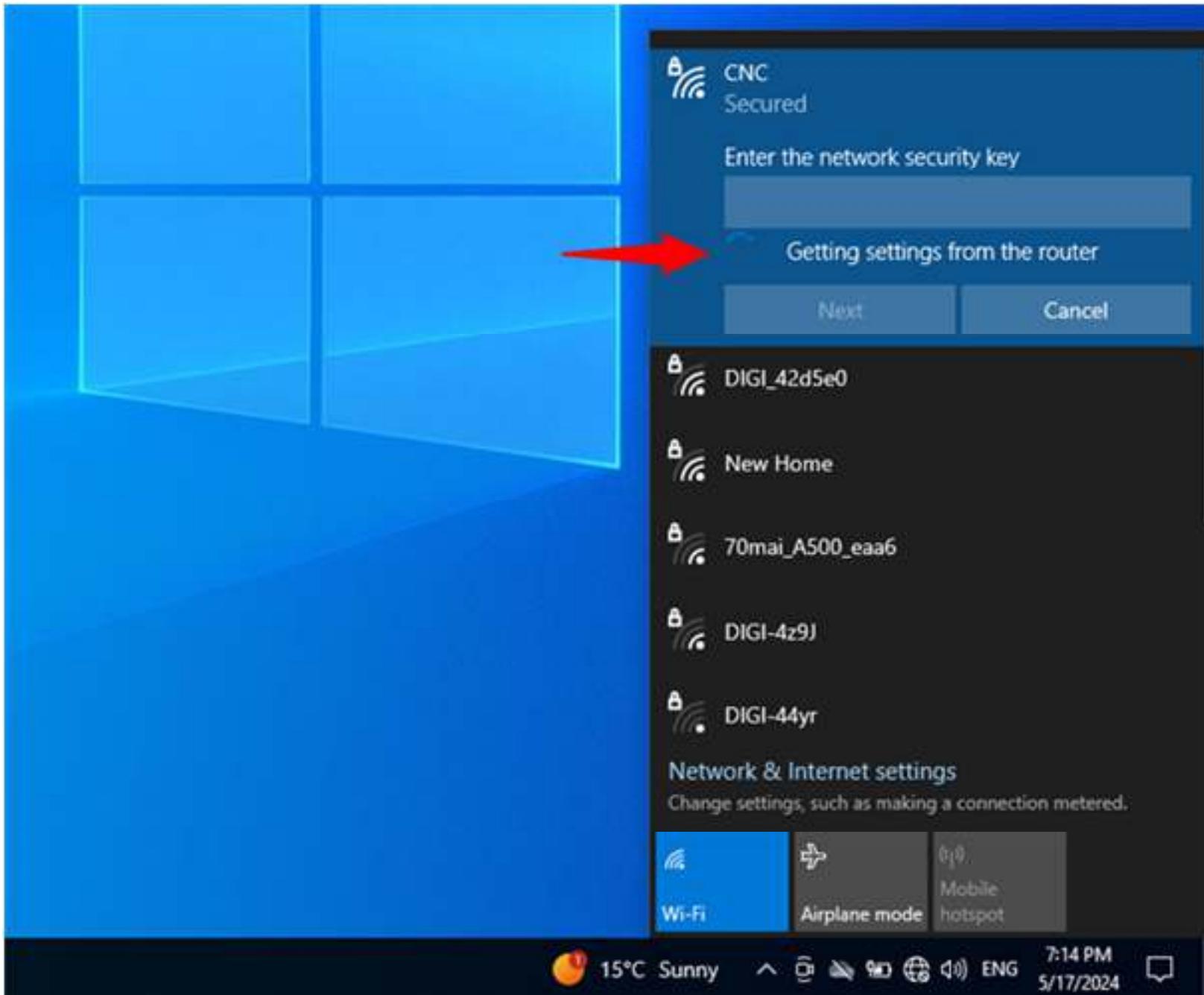


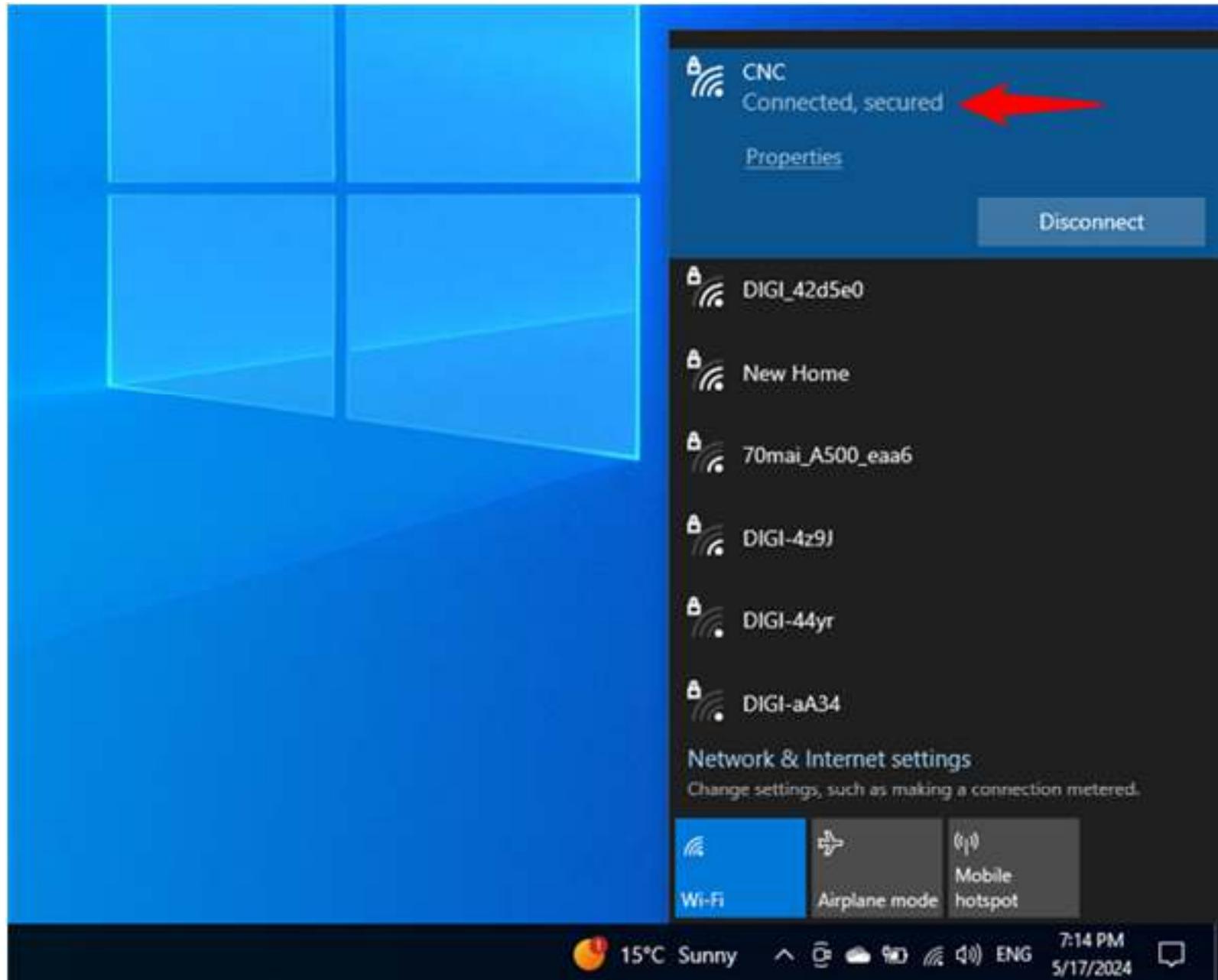




In order to connect your Windows 10 PC or laptop via WPS, instead of typing the Wi-Fi password, walk to your wireless router or access point. Push the WPS button on it for a couple of seconds. This button is usually found on the back of the router or one of its sides.







# Comparison of WiFi Security Protocols

Comparison of Security Protocols:

WEP: RC4 (40/104-bit), Static key, Very Weak, Deprecated

WPA: TKIP/RC4, Dynamic key, Improved, Still vulnerable

WPA2: AES-CCMP, Pre-shared key (PSK), Strong, Widely used

WPA3: AES-GCMP, SAE, Very Strong, Current standard

WPS: No encryption, PIN/Push-button, Weak, Not recommended

# Best Practices for WiFi Security

Securing Your WiFi Network:

Always use WPA3 if your devices support it.

Regularly update your router's firmware to patch any security vulnerabilities.

Disable WPS to prevent brute-force attacks.

Use strong, unique passwords with a mix of letters, numbers, and symbols.

Consider setting up a guest network for visitors to keep your primary network secure.

# Conclusion

Summary:

WiFi security has evolved from WEP to WPA3, each improving on the shortcomings of its predecessor.

WPA3 is currently the best option for securing wireless networks.

Continuous vigilance, such as updating firmware and using strong passwords, is necessary to maintain security.

# References

- Wi-Fi Alliance. 'Wi-Fi Security Technologies.' Wi-Fi Alliance.
- Aircrack-ng documentation. 'Understanding WEP and WPA Encryption.'
- WPA3 specification from IEEE 802.11.
- Various online articles and books on WiFi security.

# WIRELESS NETWORK AND SECURITY

- 1. Components Of wireless networks
- 2. Security issues in wireless

- Wireless Technology overview
- The IEEE 802.11 WLAN Standards
- Secure Wireless LANs
- Migrating to Wireless LANs (Cutting the cord)

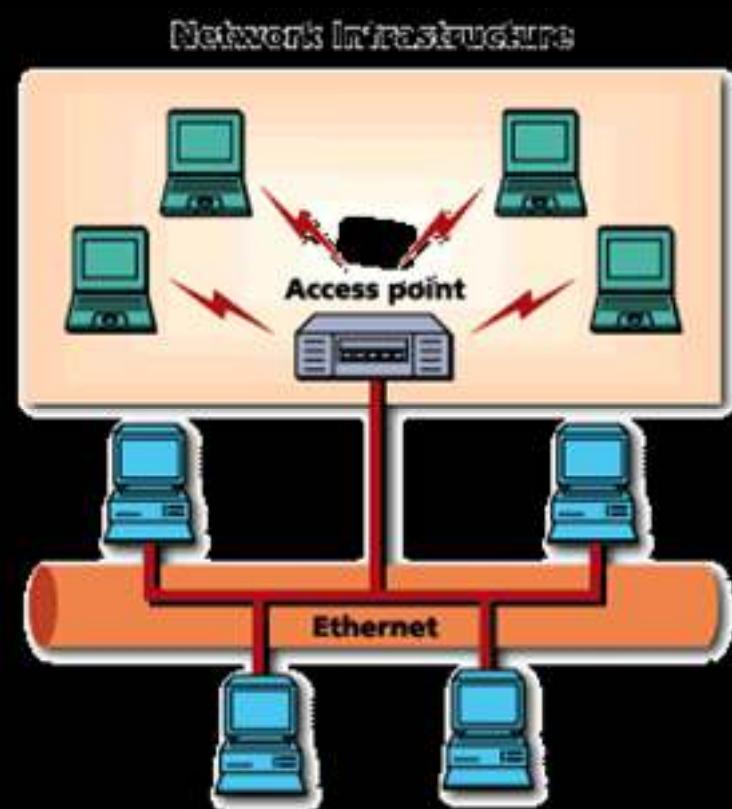
# WIRELESS?

- A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier.
- The last link with the users is wireless, to give a network connection to all users in a building or campus.
- The backbone network usually uses cables

# COMMON TOPOLOGIES

The wireless LAN connects to a wired LAN

- There is a need of an access point that bridges wireless LAN traffic into the wired LAN.
- The access point (AP) can also act as a repeater for wireless nodes, effectively doubling the maximum possible distance between nodes.



# COMMON TOPOLOGIES

## Complete Wireless Networks

- The physical size of the network is determined by the maximum reliable propagation range of the radio signals.
- Referred to as **ad hoc** networks
- Are self-organizing networks without any centralized control
- Suited for temporary situations such as meetings and conferences.



# HOW DO WIRELESS LANS WORK?

Wireless LANs operate in almost the same way as wired LANs, using the same networking protocols and supporting the most of the same applications.

# HOW ARE WLANS DIFFERENT?

- They use specialized **physical and data link** protocols
- They integrate into existing networks through **access points** which provide a bridging function
- They let you stay connected as you **roam** from one coverage area to another
- They have unique **security** considerations
- They have specific **interoperability** requirements
- They require **different hardware**
- They offer **performance** that differs from wired LANs.

# PHYSICAL AND DATA LINK LAYERS

## Physical Layer:

- The wireless **NIC** takes **frames** of data from the link layer, scrambles the data in a predetermined way, then uses the modified data stream to modulate a **radio carrier signal**.

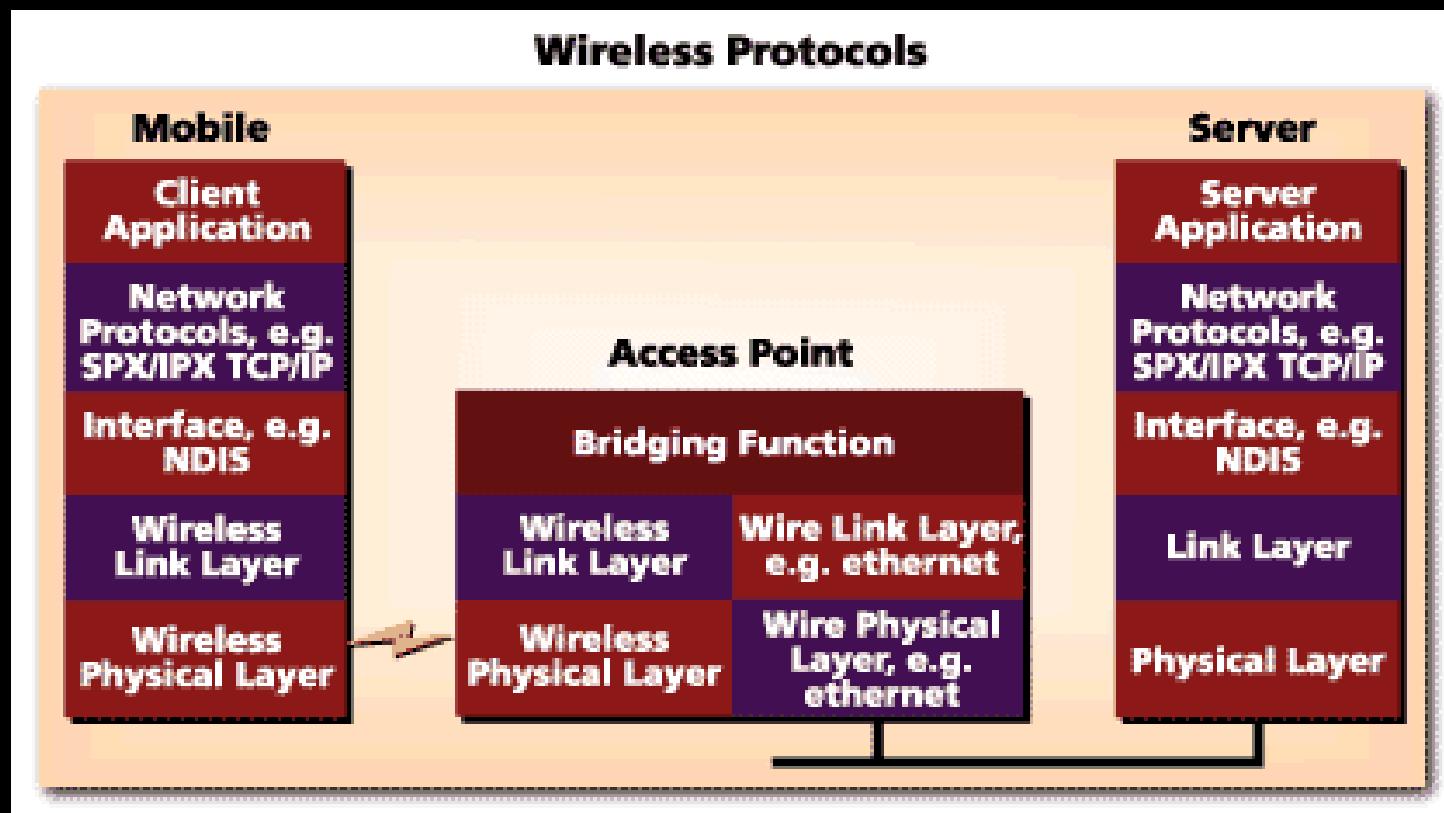
## Data Link Layer:

- Uses **Carriers-Sense-Multiple-Access with Collision Avoidance** (CSMA/CA).

# INTEGRATION WITH EXISTING NETWORKS

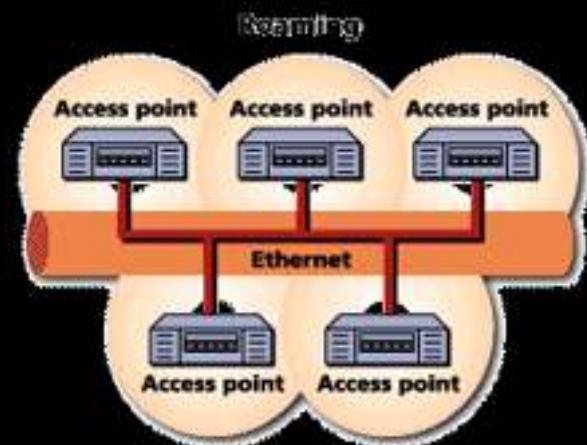
- Wireless Access Points (APs) - a small device that bridges wireless traffic to your network.
- Most access points bridge wireless LANs into Ethernet networks, but Token-Ring options are available as well.

# INTEGRATION WITH EXISTING NETWORKS



# ROAMING

- Users maintain a continuous connection as they roam from one physical area to another
- Mobile nodes automatically register with the new access point.
- Methods: DHCP(Dynamic Host Configuration Protocol ), Mobile IP
- IEEE 802.11 standard does not address roaming, you may need to purchase equipment from one vendor if your users need to roam from one access point to another.



# WHAT IS 802.11?

- A family of wireless LAN (WLAN) specifications developed by a working group at the Institute of Electrical and Electronic Engineers (IEEE)
- Defines standard for WLANs using the following four technologies
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
  - Infrared (IR)
  - Orthogonal Frequency Division Multiplexing (OFDM)
- Versions: 802.11a, 802.11b, 802.11g, 802.11e, 802.11f, 802.11i

# SECURITY

- In theory, spread spectrum radio signals are inherently difficult to decipher without knowing the exact hopping sequences or direct sequence codes used
- The IEEE 802.11 standard specifies optional security called "**W**ired **E**quivalent **P**rivacy" whose goal is that a wireless LAN offer privacy equivalent to that offered by a wired LAN. The standard also specifies optional authentication measures.

# INTEROPERABILITY

- Before the IEEE 802.11 interoperability was based on cooperation between vendors.
- IEEE 802.11 only standardizes the physical and medium access control layers.
- Vendors must still work with each other to ensure their IEEE 802.11 implementations interoperate
- Wireless Ethernet Compatibility Alliance (WECA) introduces the Wi-Fi Certification to ensure cross-vendor interoperability of 802.11b solutions

# HARDWARE

- PC Card, either with integral antenna or with external antenna/RF module.
- ISA Card with external antenna connected by cable.
- Handheld terminals
- Access points

# PERFORMANCE

- **802.11a** offers speeds with a theoretically maximum rate of 54Mbps in the 5 GHz band
- **802.11b** offers speeds with a theoretically maximum rate of 11Mbps at in the 2.4 GHz spectrum band
- **802.11g** is a new standard for data rates of up to a theoretical maximum of 54 Mbps at 2.4 GHz.

# 802.11 - TRANSMISSION

- Most wireless LAN products operate in unlicensed radio bands
  - 2.4 GHz is most popular
  - Available in most parts of the world
  - No need for user licensing
- Most wireless LANs use spread-spectrum radio
  - Resistant to interference, secure
  - Two popular methods
    - Frequency Hopping (FH)
    - Direct Sequence (DS)



# Issues In Wireless Security

# CURRENT 802.11 SECURITY

- (as per the 1999 spec)
- Authentication
  - Tied to association (session between station and AP)
  - Open system - all stations may associate
  - Shared key - stations must know secret
- Integrity
- Privacy

# CURRENT 802.11 SECURITY

- (as per the 1999 spec)
- Authentication
- Integrity - Integrity Check (IC) field
  - 32 bit CRC in encrypted payload
  - Not separately keyed
  - Vulnerable to bit-flipping attacks
- Privacy

# CURRENT 802.11 SECURITY

- (as per the 1999 spec)
- Authentication
- Integrity
- Privacy - Wired Equivalent Privacy (WEP)
  - RC4 cipher (relies on XOR)
  - Up to 4 keys per station (40 bit or 104 bit)
  - Initialization Vector (IV)
    - 24 bit extension to key
    - Provides some randomization to key
    - Unfortunately, keyspace is small!

# BIG WEP ATTACK - WEAK IV

- Say an AP constantly sends 1500 byte frames at 11 Mbps
  - Keyspace is exhausted in 5 hours
  - Will be quicker if packets are smaller
- Original IV algorithms made things much worse
  - Some cards used same IV for multiple packets  
Some cards reset IV to 0 after initialization
  - Some cards increment IV by 1 after each packet
- WEP+ fixed these “Weak IV” issues

# IMPROVING SECURITY

- Improve authentication
  - System wide common login
- Improve integrity
  - Separate integrity key
  - Stronger integrity algorithm
- Improve privacy
  - Increase keyspace size (make cracker analyze more data in order to recover key)
    - Per -user keys
    - Key rollover
  - Stronger privacy algorithm

# 802.11I AND WPA

- IEEE 802.11i - IEEE 802.11 task group “MAC enhancement for wireless security”
- Wi-Fi Alliance WPA - subset of 802.11i
  - Compatible with earlier draft
  - Defined for Basic Service Set only
  - Defined for current hardware
- WPA has two major components
  - Authentication
  - TKIP encryption

# WPA

- Authentication
  - 802.1x (not 802.11x) - defined for both wired and wireless session establishment
    - EAP (Extensible Authentication Protocol) - generic wrapper for authentication traffic
    - EAP impact
      - Authentication is between laptop and server - AP is pretty clueless
      - Different auth methods, updating auth methods do not require upgrades on AP
  - Pre-Shared Key (PSK) - for SOHO networks

# WPA

- Temporal Key Integrity Protocol (TKIP)
  - Stronger privacy
    - Still uses RC-4 encryption
    - Key rollover (temporal key)
  - Stronger integrity
    - Message Integrity Code (MIC) - computed with own integrity algorithm (MICHAEL)
    - Separate integrity key
    - Integrity counter measures

# 802.11

- Additions over WPA
  - IBSS (ad-hoc mode) authentication - what does a security context mean without a trusted third party? Is PSK enough?
  - Counter-Mode/CBC-MAC Protocol (CCMP)
    - Privacy: AES-CCM (128 bit key)
    - Integrity: CBC-MAC

# 802.11I CRITICISMS

- Does not secure 802.11 management control and action frames
  - Disassociate, output power, etc.
- Fundamental dilemma: does 802.11i secure
  - 1. Traffic carried by the network?
  - 2. Network elements themselves?

# Kerberos Authentication Protocol

A Secure Network Authentication Protocol

# Kerberos

Network authentication protocol



Provides strong authentication for client/server applications, using secret-key cryptography

A user types in a password and logs into a workstation. On behalf of the user, the workstation authenticates and accesses resources seamlessly

Developed at MIT

Kerberos V4 and V5 are widely deployed

KDC: a database of <principal, key> and a library of subroutines

# Key Features of Kerberos

- Mutual Authentication: Both the user and the server verify each other's identity.
- Single Sign-On: Users authenticate once and gain access to multiple services.
- Strong Security: Utilizes secret-key cryptography and timestamps to prevent replay attacks.
- Scalability: Suitable for large networks with many users and services.

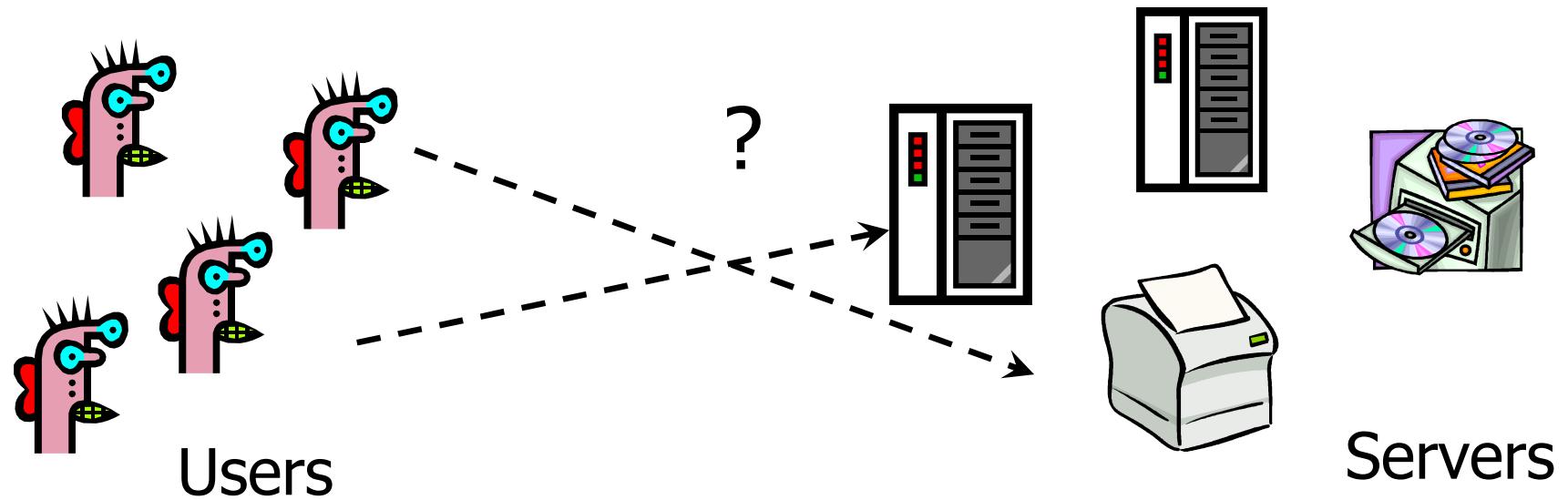
# How Kerberos Works

1. Authentication: The client sends a request to the Authentication Server (AS) to prove its identity.
2. Ticket Granting: The AS sends a Ticket Granting Ticket (TGT) back to the client.
3. Service Request: The client presents the TGT to the Ticket Granting Server (TGS) to request access to a service.
4. Access Granted: The TGS sends a service ticket to the client, allowing access to the requested service.

# Components of Kerberos

- Authentication Server (AS): Verifies the client's identity and provides the Ticket Granting Ticket (TGT).
- Ticket Granting Server (TGS): Issues service tickets based on the TGT.
- Key Distribution Center (KDC): Combines the AS and TGS, centralizing authentication and ticket distribution.
- Client: Requests access to services on behalf of the user.
- Service Server: Hosts the services the client wants to access.

# Many-to-Many Authentication

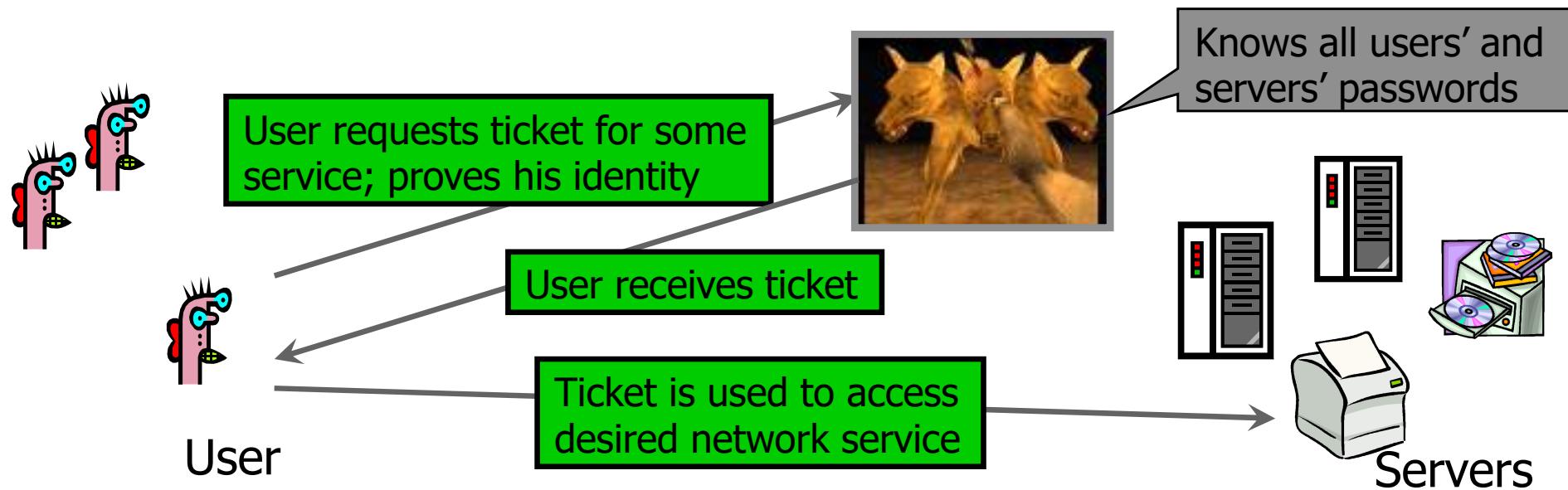


How do users prove their identities when requesting services from servers on the network?

Naïve solution: every server knows every user's password:

- insecure: compromise of any server will compromise all users
- inefficient: a user must contact every server to change password

# Using Trusted Third Party



Trusted authentication service on the network:  
knows all passwords, can grant access to any server  
convenient, but also the single point of failure  
requires high level of physical security

# Configuration

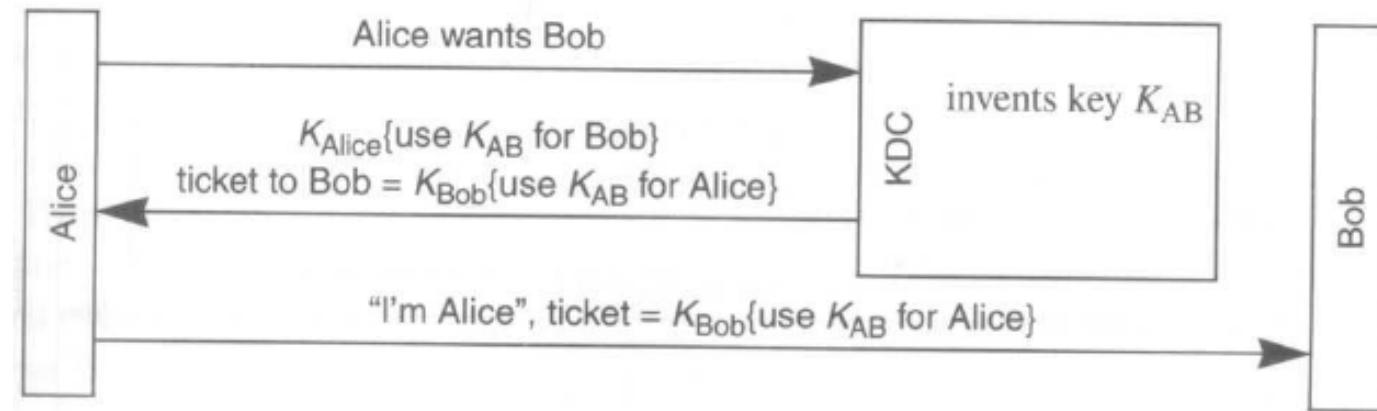
- Kerberos server: KDC
- Each principal has its master key,  $K_{\text{Alice}}$ , shared with KDC
  - human user: key is derived from password
  - machine: key is pre-configured
- KDC has a master key,  $K_{\text{KDC}}$ , known only by itself, to encrypt user master keys and ticket-granting tickets
- KDC keeps a database of <principal, key>, where “key” for each user is encrypted by  $K_{\text{KDC}}$
- Based on secret-key cryptography: DES, V5 theoretically can use other encryption algorithms

# Session Keys

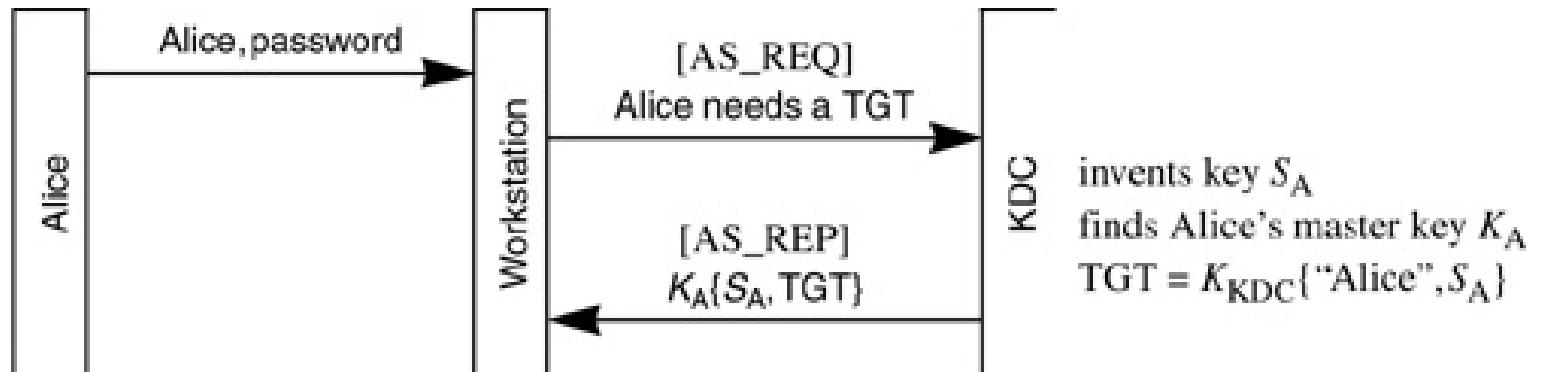
- For login sessions
- Should we use the master key  $K_{Alice}$  (long-term key)?
- Use  $K_{Alice}$  at the beginning of each session to negotiate a session key  $S_A$ 
  - eavesdropping
  - database reading
  - password guessing: online, offline (dictionary attack)

# Ticket-Granting Ticket (TGT)

- Recall: ticket



- TGT:  $K_{KDC}\{Alice, S_A, \text{expiration time}, \dots\}$ , for assigning the session key

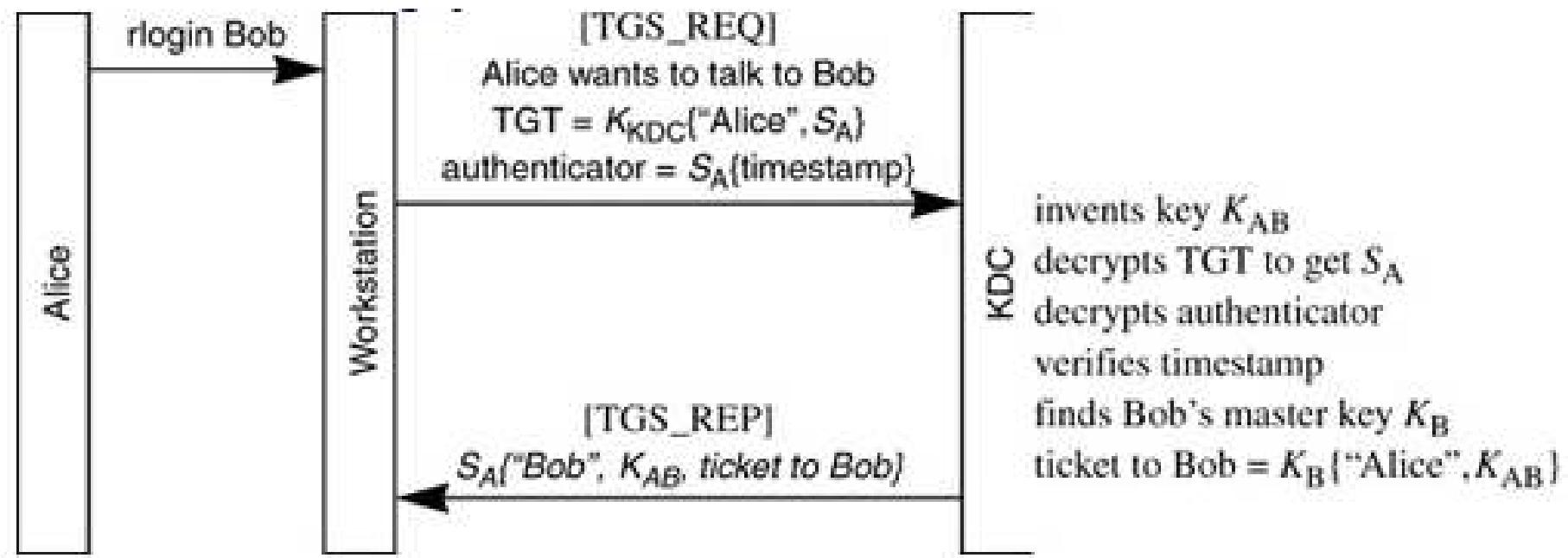


Obtaining a TGT

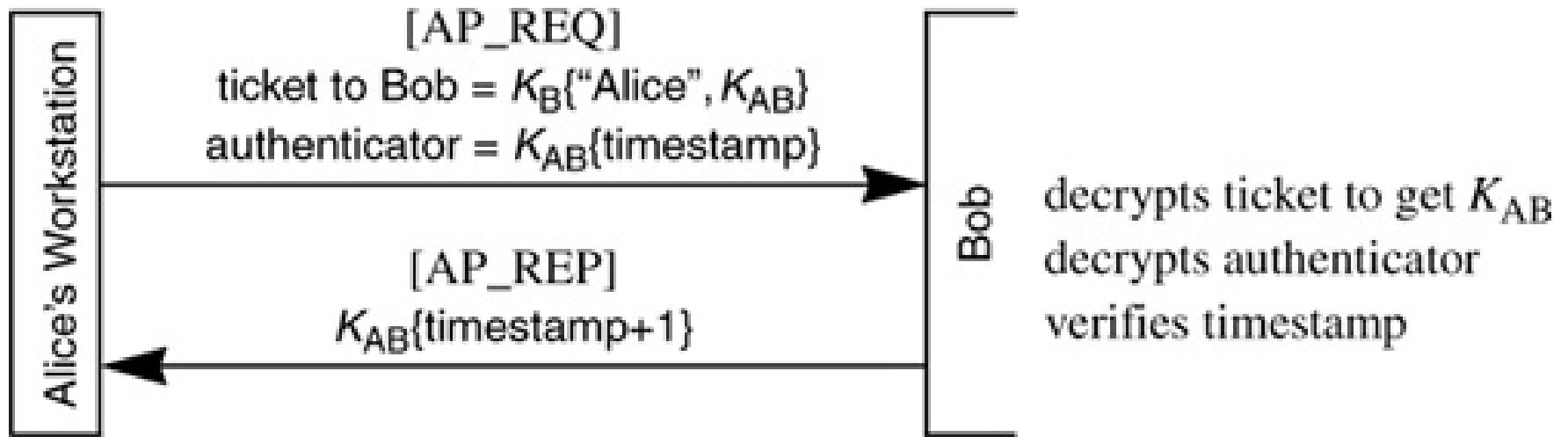
# Obtaining Services from A Remote Node

- After obtaining TGT, the credential for Alice...
- Step 1: Alice uses TGT to obtain a ticket
- Step 2: Alice uses ticket to log into remote node

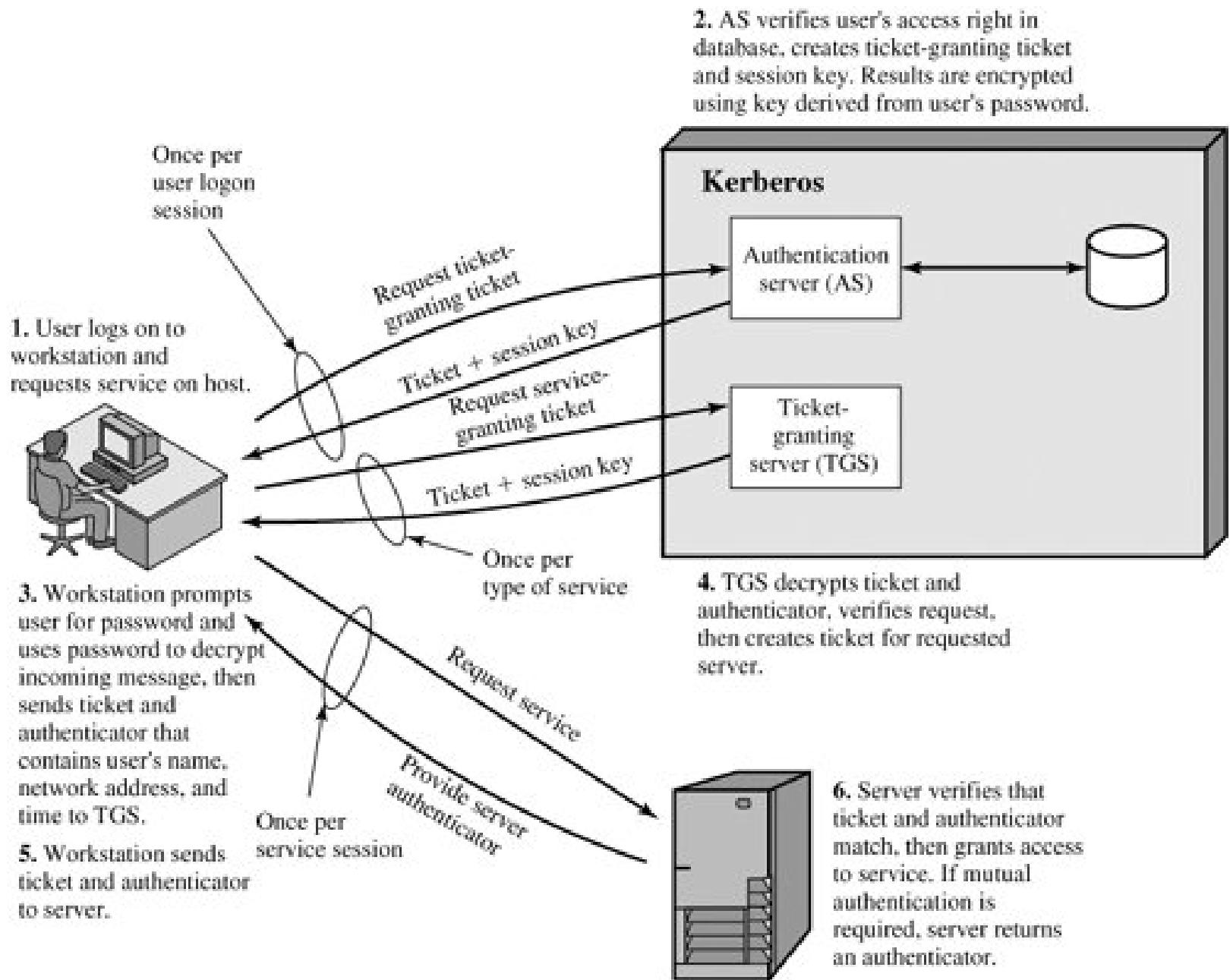
# Step 1: Obtaining A Ticket to Bob



## Step 2: Accessing Bob



# Overview of Kerberos



# Step 1: Authentication Request

The client sends a request to the Authentication Server (AS) with the user's credentials (username and encrypted password).

The AS verifies the credentials against its database and generates a Ticket Granting Ticket (TGT) and a session key, encrypted with the user's secret key.

# Step 2: Ticket Granting Ticket (TGT)

The Authentication Server (AS) sends the TGT and session key back to the client.

The TGT contains the client's ID, the TGS's ID, a timestamp, and a validity period, all encrypted with the TGS's secret key.

The client cannot read the TGT but stores it for future use when requesting services.

# Step 3: Service Request to TGS

The client sends a request to the Ticket Granting Server (TGS) for access to a specific service.

The request includes the TGT, an authenticator (a timestamp encrypted with the session key), and the ID of the requested service.

The TGS verifies the TGT and the authenticator to ensure the client's identity and request validity.

# Step 4: Service Ticket Issuance

Once the TGS verifies the client, it generates a service ticket for the requested service.

The service ticket contains the client's ID, the service's ID, a new session key, and a validity period, all encrypted with the service server's secret key.

The TGS sends the service ticket and the new session key (encrypted with the client's key) back to the client.

# Step 5: Accessing the Service

The client sends the service ticket and a new authenticator (encrypted with the new session key) to the service server.

The service server decrypts the service ticket with its secret key and uses the session key to verify the authenticator.

If verification is successful, the client is granted access to the service.

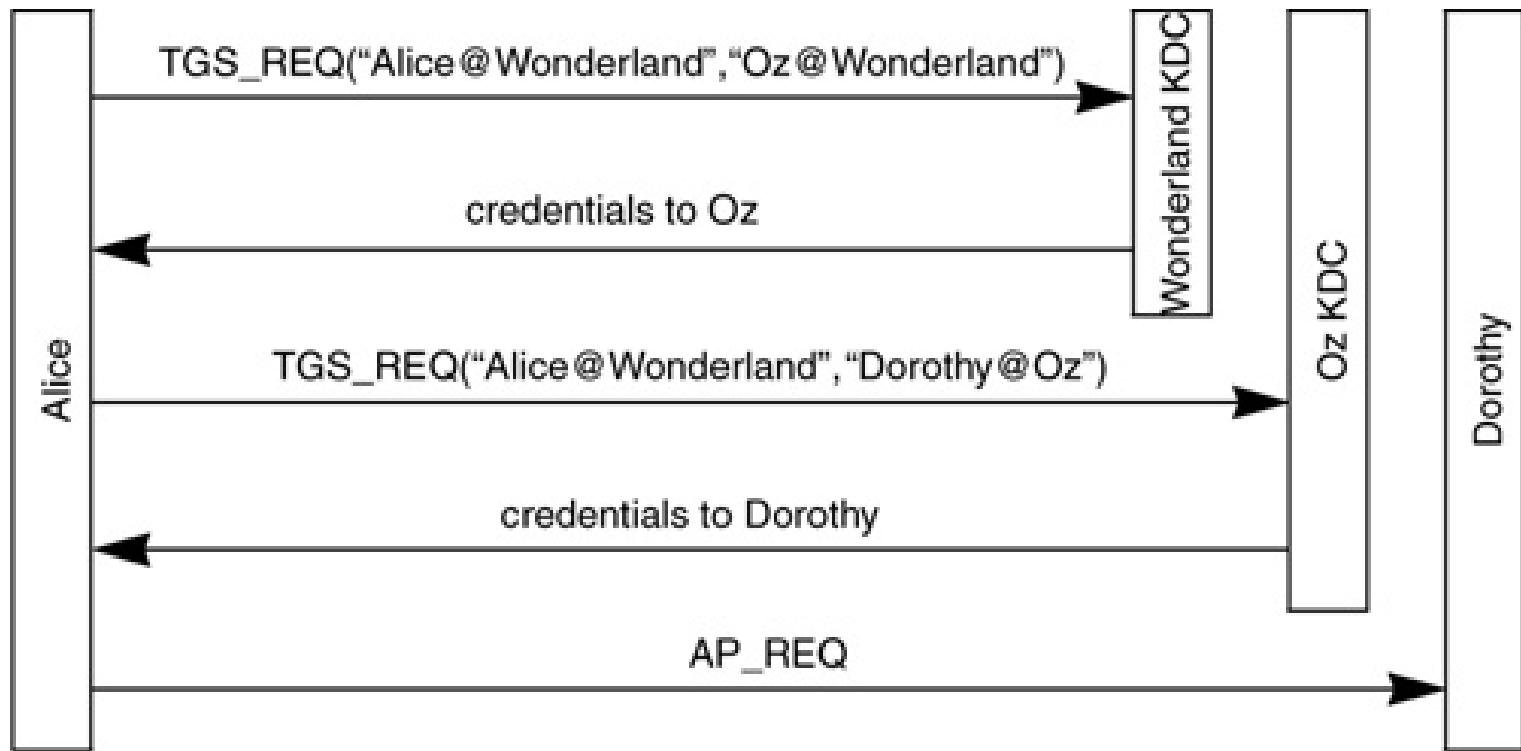
# Replicated KDCs

- Purposes:
  - Prevent single point failure
  - Prevent performance bottleneck
- Multiple KDCs
  - One master copy for read/write
  - Multiple replicas for read only
  - All having the same database and the same master key
- Updating KDC database
  - KDC's database is transferred in clear
  - Privacy: keys are stored as ciphertext encrypted by  $K_{KDC}$
  - Integrity: a cryptographic hash of the database file and a timestamp

# Realms

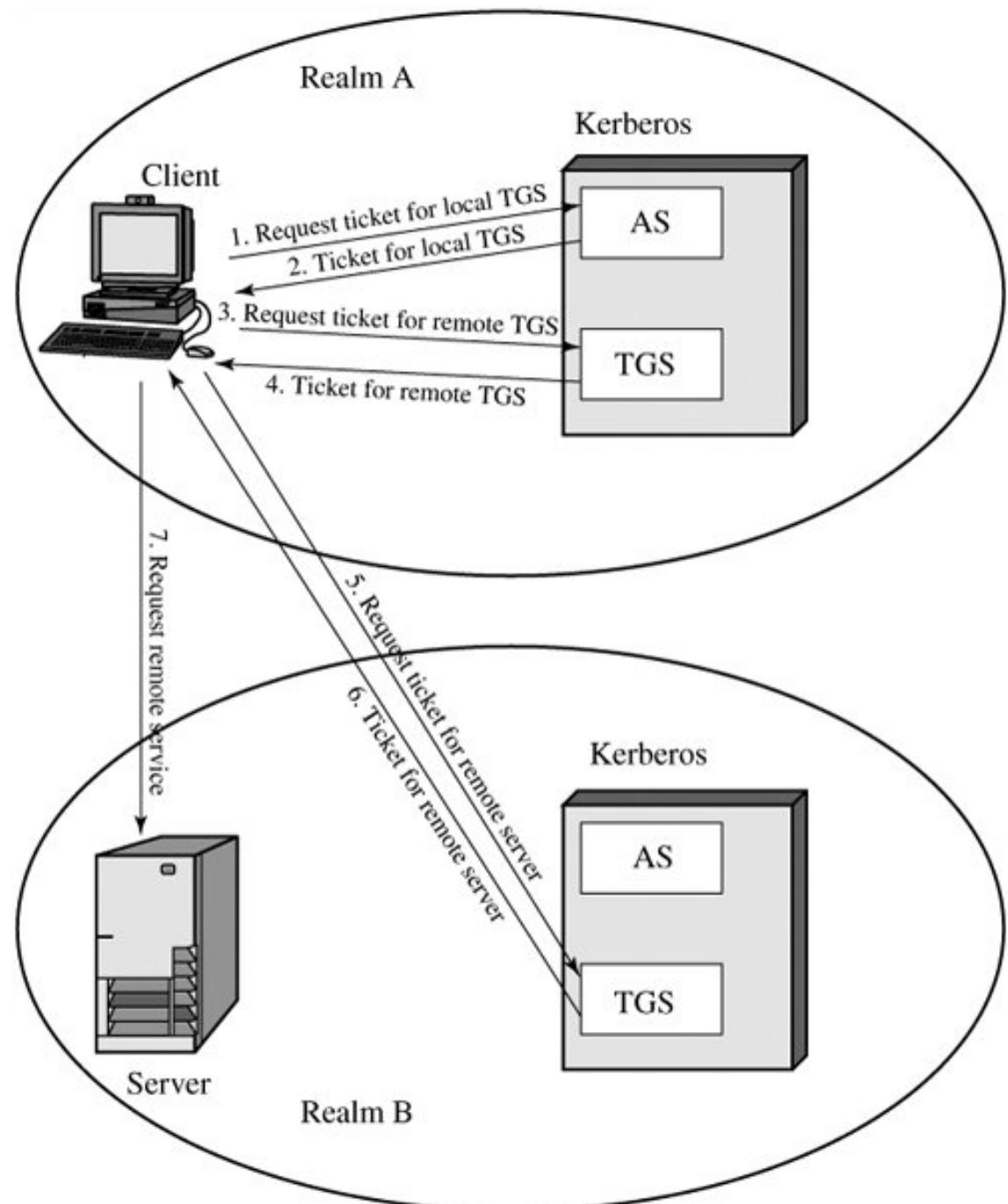
- To scale to a large network including multiple administrations, the principals are divided into realms. Each realm has its own KDC.
- The KDCs of other realms are treated as resources (principals) of a local realm.

# Interrealm Authentication



- Kerberos V4 does not allow authentication through a chain of KDCs: a rogue KDC can impersonate other realms
- Kerberos V5 does: hierarchy of realms

# Interrealm Authentication (2)



# Benefits of Using Kerberos

- Enhanced Security: Prevents eavesdropping and replay attacks.
- Efficiency: Single sign-on reduces repeated authentication steps.
- Compatibility: Works across various platforms and applications.
- Centralized Management: Simplifies the administration of user credentials.

# Challenges and Limitations

- Single Point of Failure: The Key Distribution Center (KDC) is a critical component.
- Time Sensitivity: Requires synchronized clocks between clients and servers.
- Complex Setup: Requires careful configuration and management.
- Network Dependency: Requires network connectivity for authentication processes.

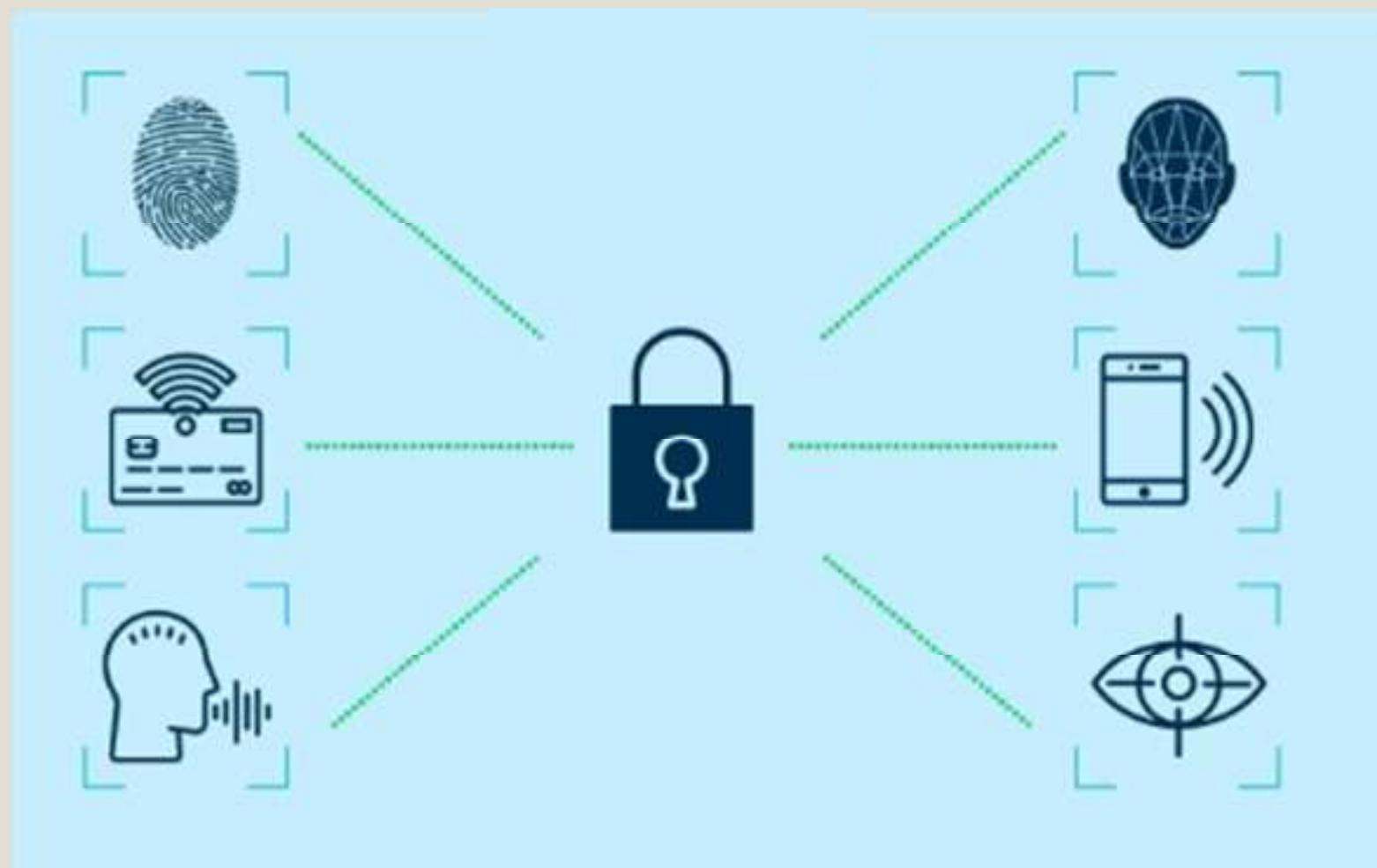
# UNDERSTANDING KEY SECURITY CONCEPTS

Authentication, Authorization, Auditing, Privacy,  
Integrity, Availability, Non-repudiation

## WHAT IS AUTHENTICATION?

- Definition: Proving who you are.
- Examples: Passwords, Fingerprints, Face ID
- Why It Matters: Keeps intruders out!

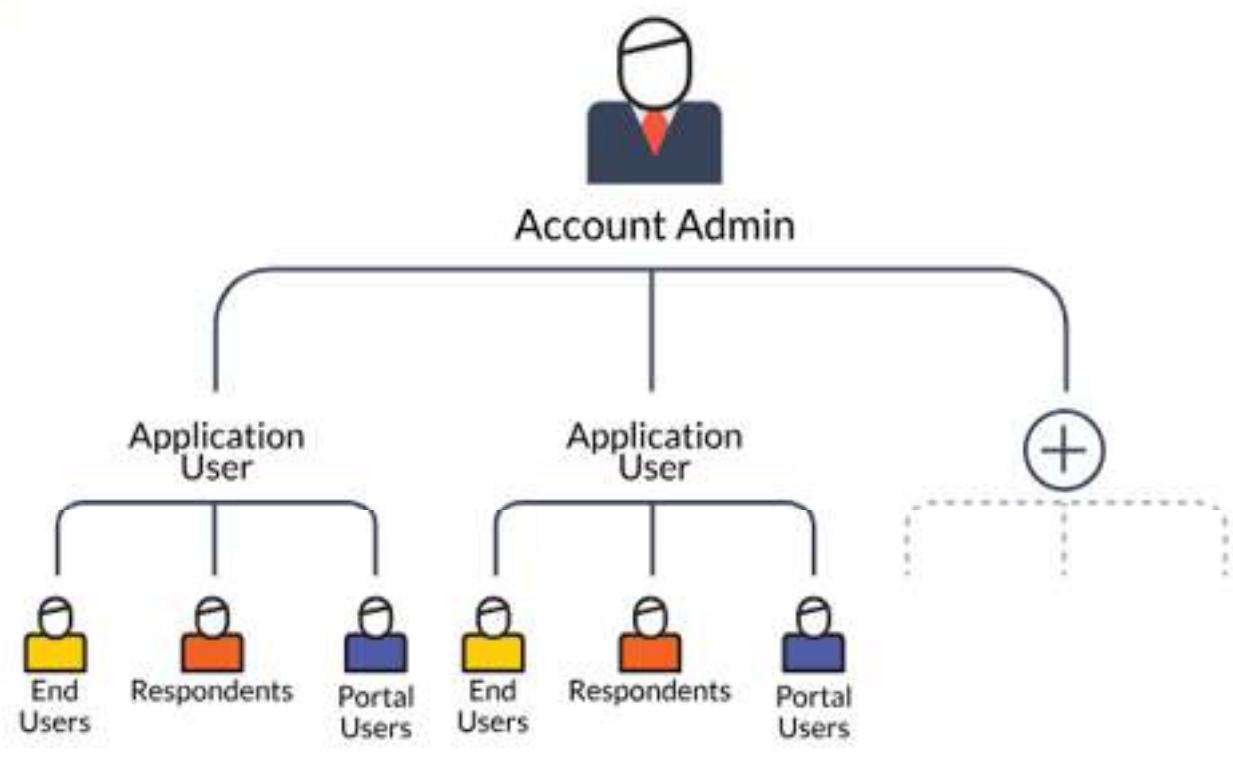
# WHAT IS AUTHENTICATION?



# WHAT IS AUTHORIZATION?

- Definition: Deciding what you can do.
- Examples: Access to files, permissions on apps
- Why It Matters: Prevents unauthorized actions!

# WHAT IS AUTHORIZATION?



# WHAT IS AUDITING?

- Definition: Tracking what happens in the system.
- Examples: Logs of who accessed what and when
- Why It Matters: Helps find problems and keep people accountable.

# WHAT IS AUDITING?

Detailed View of Recorded Audit Events (Filter 1)

Audit Class	Event Class	Recording	Message ID	System log message text (before setting variables)
During Logout	Critical		AU2	Login failed (reason=8A, type=8A, method=8C)
			AU3	User 8A locked in client 8A after errors in password checks.
			AU5	User 8A unlocked in client 8A after entering wrong password.
			B01	WS: Delayed login failed (type=8B, WF=8C). Refer to Web service log 8A.
			B02	SPIpings replay attack detected (IPN=8A)
			CU4	OAuth 2.0: Logged-on client user 8A not same as parameter client ID 8D
			CU5	OAuth 2.0: Client ID 8A in SAPB assertion not same as client ID 8D in request
			D03	Invalid SAP (03) data
			AU1	Login successful (type=8A, method=8C)
			AU0	Login failed (reason = 8B, type = 8A)
			CU2	OAuth 2.0: Invalid access token received (reason=8A)
			CU3	OAuth 2.0: Insufficient OAuth 2.0 scope for requested resource (user=8A)
			CU5	OAuth 2.0: Client 8A requested invalid access grant type 8D
			CU7	OAuth 2.0: Scope 8B not permitted for client 8C, user 8D (cause=8A)
			CU8	Rejected Assertion
			CU9	8A: 8B
			OK	8A
			CU0	Name ID of a subject
			CU1	Attribute
			CUF	Authentication Assertion
			CU6	Signed LogonRequest rejected
			CUH	Unsigned LogonRequest rejected
			AUC	User Logoff
			B02	WS: Delayed login successful (type=8B, WF=8C). Refer to Web service log 8A.
			B04	8A insertion used
			B05	8A: 8B
			B06	Name ID of a subject
			B07	Attribute
			B10	Authentication assertion
			B12	8A
			B13	Signed LogonRequest accepted
			B14	Unsigned LogonRequest accepted
			CU8	OAuth 2.0: Access token issued (client=8A, user=8B, grant type=8C)
			CU9	OAuth 2.0: Valid access token increased for user 8A

## WHAT IS PRIVACY?

- Definition: Keeping your personal info safe.
- Examples: Encrypting emails, secure messaging apps
- Why It Matters: Protects against identity theft and data misuse.

# WHAT IS PRIVACY?



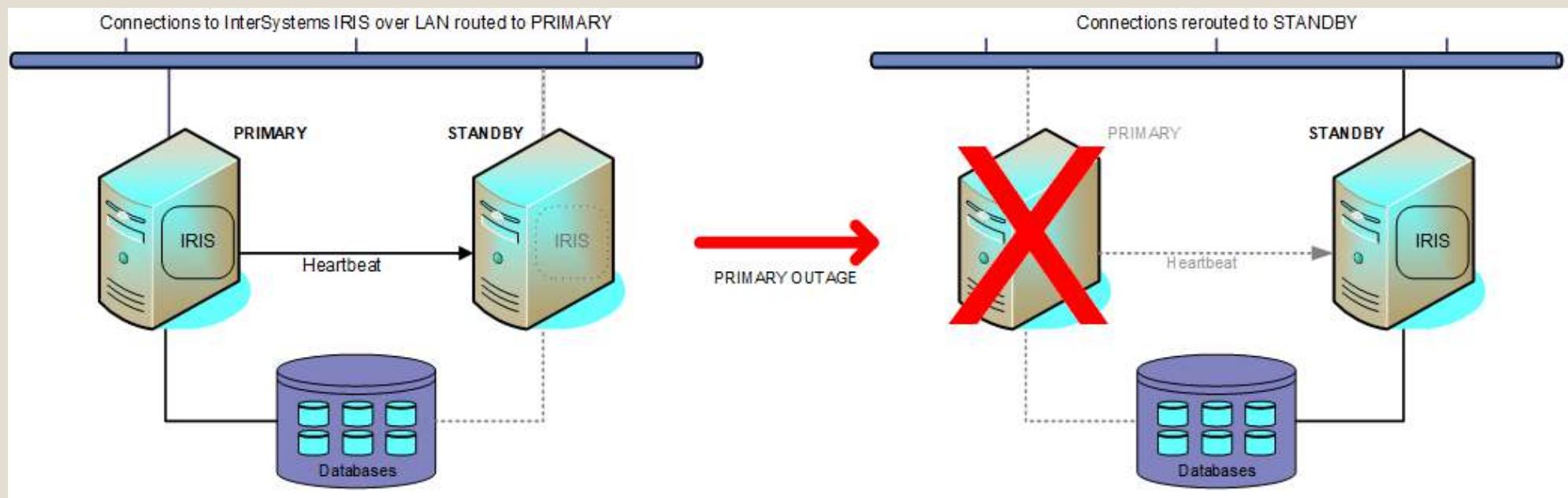
# WHAT IS INTEGRITY?

- Definition: Making sure data is correct and unchanged.
- Examples: Checksums, Digital signatures
- Why It Matters: Ensures trust in data and transactions.

# WHAT IS AVAILABILITY?

- Definition: Ensuring access to services and data when needed.
- Examples: Backup servers, Load balancing
- Why It Matters: Keeps systems running smoothly.

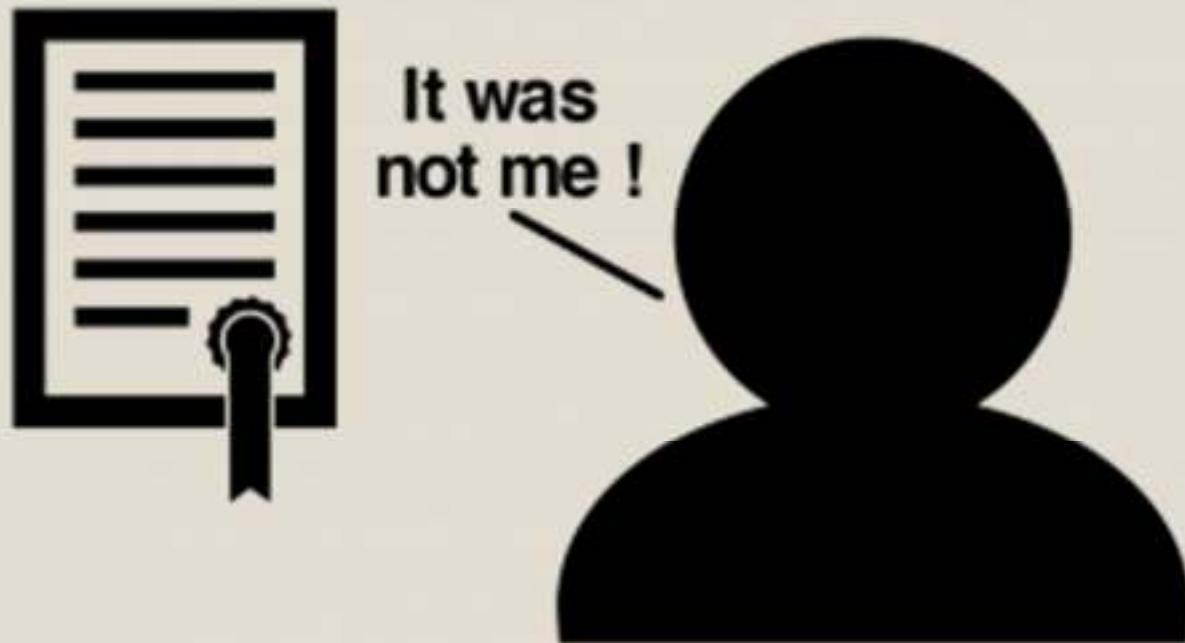
# WHAT IS AVAILABILITY?



# WHAT IS NON-REPUDIATION?

- Definition: Ensuring that actions can't be denied later.
- Examples: Signed digital contracts, Email receipts
- Why It Matters: Provides proof of actions for accountability.

# WHAT IS NON-REPUDIATION?



## RECAP OF KEY POINTS

- **Authentication:** Proving who you are
- **Authorization:** Deciding what you can do
- **Auditing:** Tracking what happens
- **Privacy:** Keeping personal info safe
- **Integrity:** Ensuring data is correct
- **Availability:** Ensuring access
- **Non-repudiation:** Ensuring actions can't be denied
- **Final Thought:** A strong security system uses all these concepts together!

# UNDERSTANDING SECURITY THREATS IN INTERNAL APPLICATIONS

Spoofing, Tampering, Repudiability, Information Disclosure, Denial of Service, Elevation of Privilege

# SPOOFING

- Definition: Pretending to be someone else to gain access.
- Examples: Phishing attacks, Credential theft.
- Impact: Unauthorized access to sensitive data and systems.

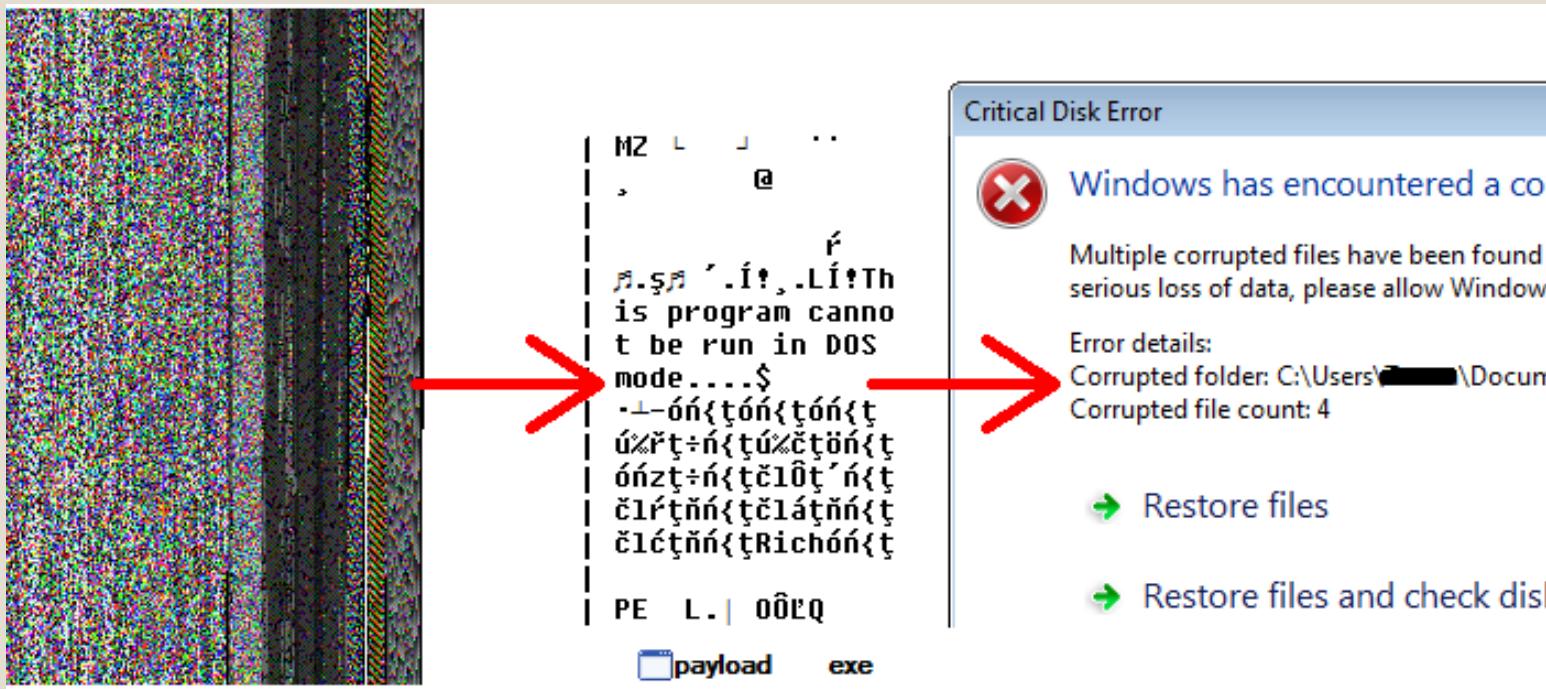
# SPOOFING



# TAMPERING WITH DATA

- Definition: Modifying data without permission.
- Examples: Altering database records, Man-in-the-middle attacks.
- Impact: Loss of data integrity, Corruption of information.

# TAMPERING WITH DATA



# REPUDIABILITY

- Definition: Denying actions after they have been performed.
- Examples: Deleting transaction logs, Disabling audit trails.
- Impact: Difficulty in proving actions for accountability.

# REPUDIABILITY

	Results	Messages					
	database_name	backup_start_date	backup_type	backup_size MB	physical_device_name	is_copy_only	user_name
1	L	2018-02-24 20:00:07.000	DIFF	2.38281250000	E:\SQLBackups\	2018...	0
2	L	2018-02-24 16:00:20.000	DIFF	2.38281250000	E:\SQLBackups\	2018...	0
3	L	2018-02-24 12:05:22.000	Full	7191.06347656250	{AC964911-C0C9}	1	NT AUTHORITY\SYSTEM
4	L	2018-02-24 12:00:12.000	DIFF	2.38281250000	E:\SQLBackups\	2018...	0
5	L	2018-02-24 09:35:00.000	Full	7191.06982421875	{95C67D04-1128}	0	NT AUTHORITY\SYSTEM
6	L	2018-02-24 08:00:20.000	DIFF	9.25781250000	E:\SQLBackups\	2018...	0
7	L	2018-02-24 04:00:13.000	DIFF	1.00781250000	E:\SQLBackups\	2018...	0
8	L	2018-02-24 00:04:58.000	Full	7190.88232421875	{CF704E4A-CEE1}	1	NT AUTHORITY\SYSTEM
9	L	2018-02-24 00:00:36.000	Full	7191.57031250000	E:\SQLBackups\	201...	0
10	L	2018-02-24 00:00:20.000	DIFF	174.25781250000	E:\SQLBackups\	2018...	0
11	L	2018-02-23 20:00:13.000	DIFF	174.25781250000	E:\SQLBackups\	2018...	0
12	L	2018-02-23 18:04:23.000	Full	7190.90869140625	{2897BB92-A91E}	1	NT AUTHORITY\SYSTEM
13	L	2018-02-23 16:00:05.000	DIFF	170.82031250000	E:\SQLBackups\	2018...	0
14	L	2018-02-23 12:00:13.000	DIFF	113.75781250000	E:\SQLBackups\	2018...	0
15	L	2018-02-23 08:00:06.000	DIFF	21.69531250000	E:\SQLBackups\	2018...	0
16	L	2018-02-23 04:00:19.000	DIFF	1.00781250000	E:\SQLBackups\	2018...	0
17	L	2018-02-23 00:04:56.000	Full	7189.87597656250	{6B3D7085-6318}	1	NT AUTHORITY\SYSTEM
18	L	2018-02-23 00:02:07.000	DIFF	1.00781250000	E:\SQLBackups\	2018...	0
19	L	2018-02-23 00:00:06.000	Full	7190.19531250000	E:\SQLBackups\	201...	0
20	L	2018-02-22 20:00:18.000	DIFF	192.13281250000	E:\SQLBackups\	2018...	0
21	L	2018-02-22 18:03:49.000	Full	7189.88867187500	{F39EDD90-68E	1	NT AUTHORITY\SYSTEM
22	L	2018-02-22 16:00:11.000	DIFF	165.32031250000	E:\SQLBackups\	2018...	0

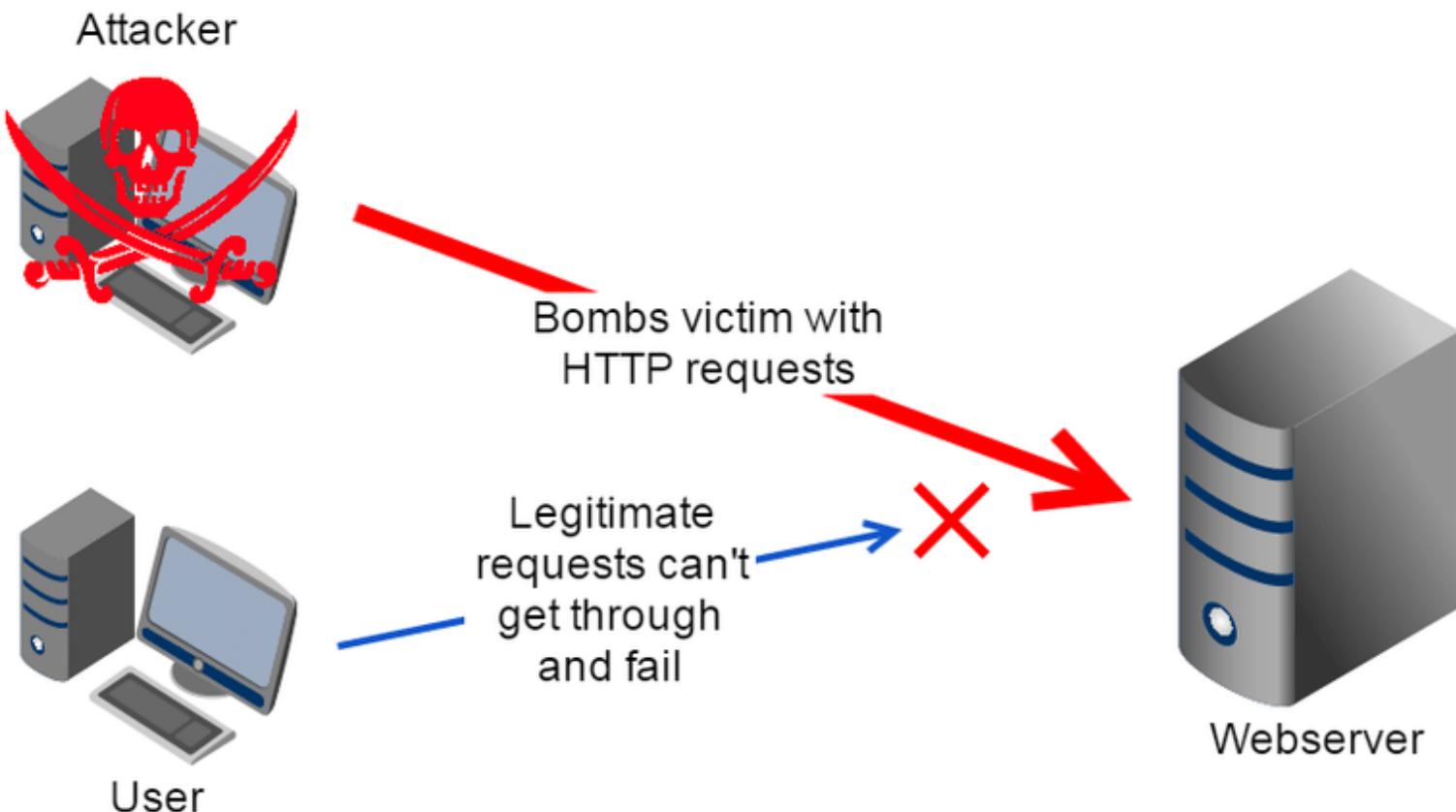
# INFORMATION DISCLOSURE

- Definition: Exposing confidential information to unauthorized parties.
- Examples: Data breaches, Insecure data storage.
- Impact: Loss of privacy, Legal consequences, Financial losses.

# DENIAL OF SERVICE (DOS)

- Definition: Disrupting the availability of services.
- Examples: DDoS attacks, Resource exhaustion.
- Impact: Service downtime, Loss of revenue, Poor user experience.

# DENIAL OF SERVICE (DOS)



# ELEVATION OF PRIVILEGE

- Definition: Gaining higher access rights than permitted.
- Examples: Exploiting software bugs, Privilege escalation attacks.
- Impact: Full control over systems, Access to all data and services.

# ELEVATION OF PRIVILEGE



## RECAP OF KEY THREATS

- **Spoofing:** Impersonation to gain access
  - **Tampering:** Altering data maliciously
  - **Repudiability:** Denying actions to evade accountability
  - **Information Disclosure:** Exposing sensitive data
  - **Denial of Service:** Disrupting service availability
  - **Elevation of Privilege:** Unauthorized escalation of access
- 
- **Final Thought:** A comprehensive security strategy should address all these threats!

# Firewalls and VPNs

Firewalls and Virtual Private Networks

Overview of Security Mechanisms in Remote  
Access Networks

Presented by: Dr. Faraz Masood

# Introduction

## Overview:

Remote access networks require robust security mechanisms to prevent unauthorized access and data breaches.

Firewalls act as barriers between internal corporate networks and external, untrusted networks (e.g., the Internet).

**Virtual Private Networks (VPNs)** create secure, encrypted connections over public networks, allowing safe remote access to corporate resources.

## Example:

Imagine a company with employees working remotely. To protect sensitive data when employees connect from home, the company uses a VPN to encrypt the data transmitted over the Internet.

# Firewall Protection

## Definition:

A firewall is a security device or software that monitors and controls incoming and outgoing network traffic based on predefined security rules.

## Purpose:

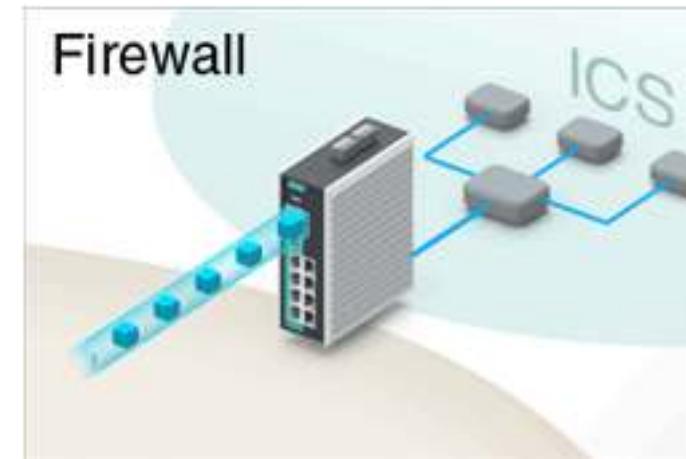
Protects private networks (like a company's internal network) from unauthorized access and malicious attacks.

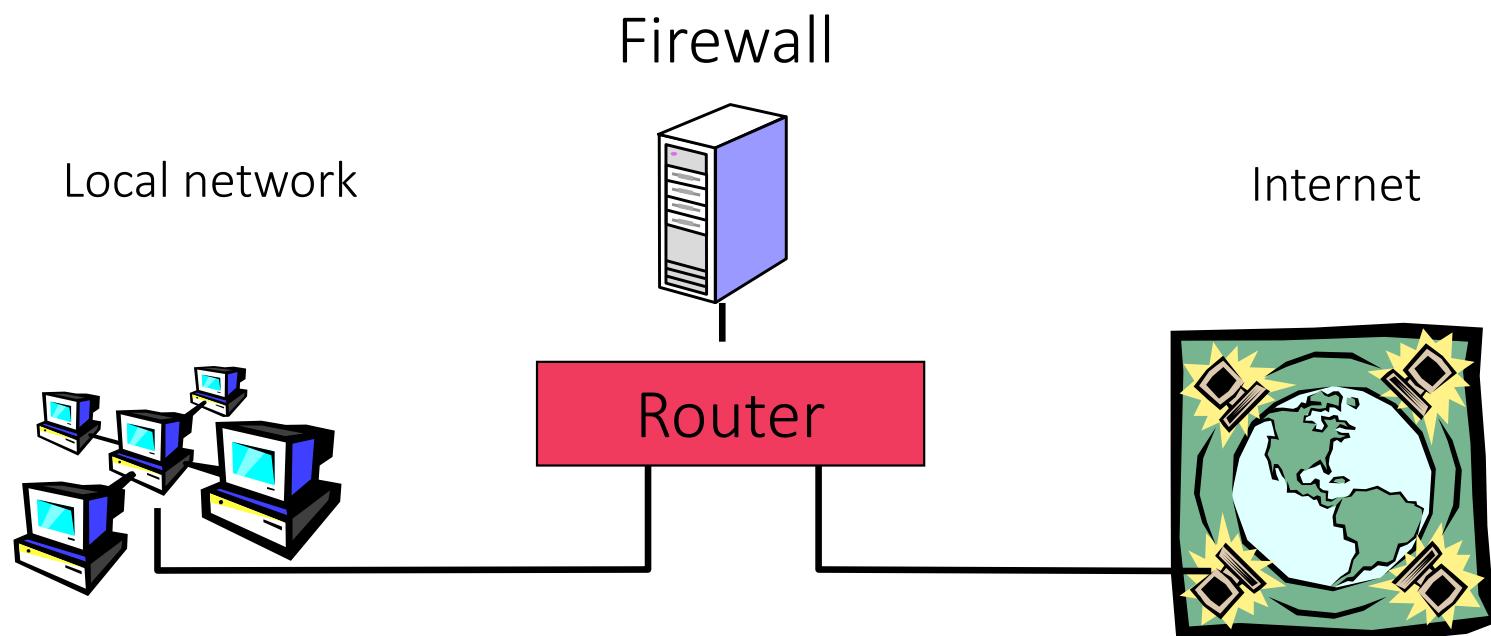
## Function:

Acts as a gatekeeper that filters traffic based on rules (e.g., only allowing traffic from trusted sources).

## Example:

A firewall might block all incoming traffic except for web traffic (HTTP/HTTPS) from specific IP addresses to prevent unauthorized access.





# Network Security Policy

Definition:

A network security policy is a set of rules that define how network resources are protected and used.

Elements of a Security Policy:

Resources to Protect: Servers, databases, sensitive information.

Threats Identified: Hackers, malware, unauthorized access.

Usage Rules: Who can access the network, what data they can access, and how it can be used.

Actions for Violations: Block access, log attempts, notify administrators.

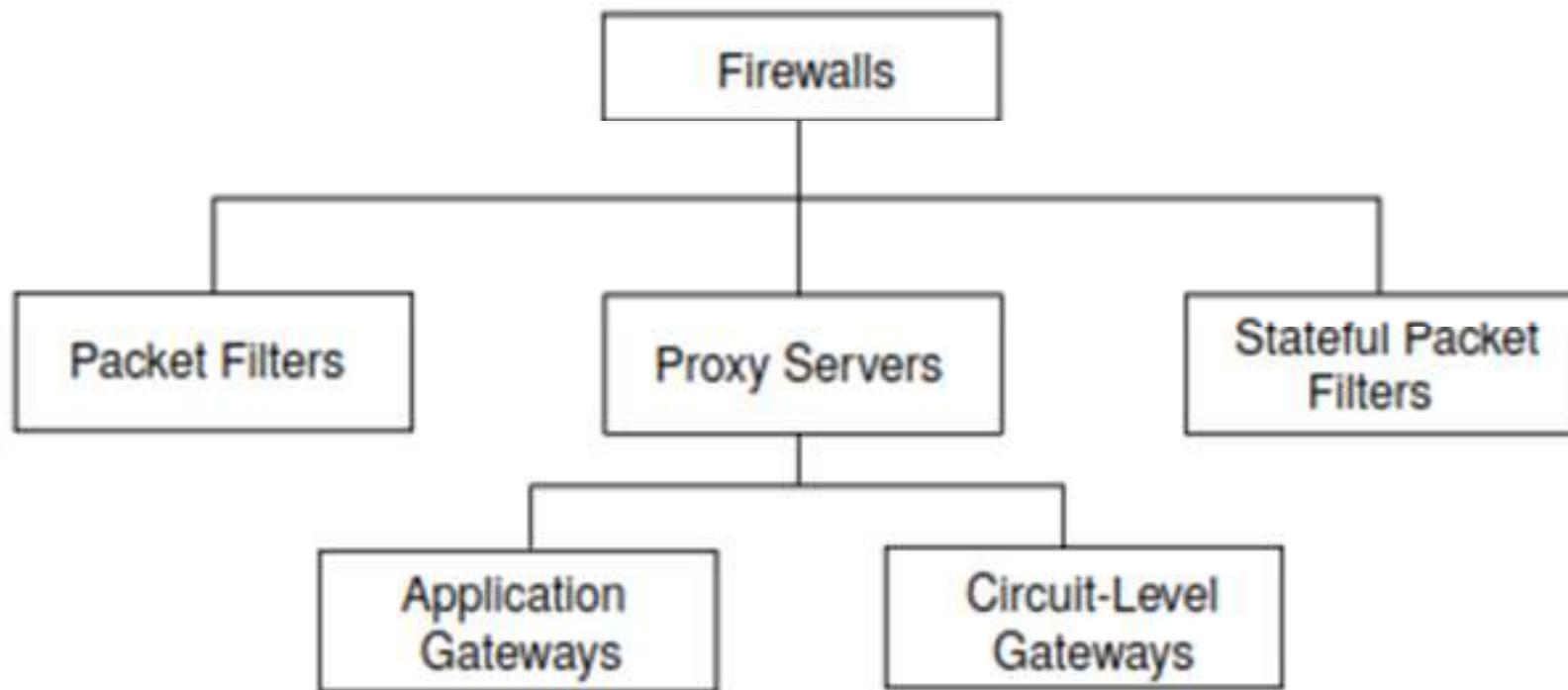
Example Policy Rules:

Block all incoming traffic except from IP addresses within a trusted range.

Allow only secure HTTPS connections (port 443).

Deny all attempts to access the internal network from outside the company's VPN.

# Types of Firewalls



# Types of Firewalls

## Packet Filters:

Inspects packets based on rules like IP addresses and port numbers.

Example: A packet filter might allow web traffic (port 80) but block FTP traffic (port 21).

## Proxy Servers:

Intermediary servers that handle requests from clients and forward them to actual servers.

- **Application Gateways:** Examines traffic at the application layer, such as filtering out certain types of data (e.g., blocking all email attachments).
- **Circuit-Level Gateways:** Controls traffic at the session level, like validating TCP or UDP sessions.

## Stateful Packet Filters:

Monitors the state of active connections and makes filtering decisions based on the state.

Example: Allows incoming traffic only if it matches an existing, approved connection.

## Hybrid Firewalls:

Combines two or more types of firewalls for enhanced security (e.g., packet filtering with a proxy server).

# Packet Filters

## Definition:

A packet filter is a firewall that inspects each packet against a set of user-defined rules to determine whether it should be allowed or blocked.

## Function:

Decides to allow or block packets based on criteria like source/destination IP address, protocol type (TCP/UDP), and port numbers.

## Advantages:

Fast, cost-effective, easy to implement in existing network routers.

## Disadvantages:

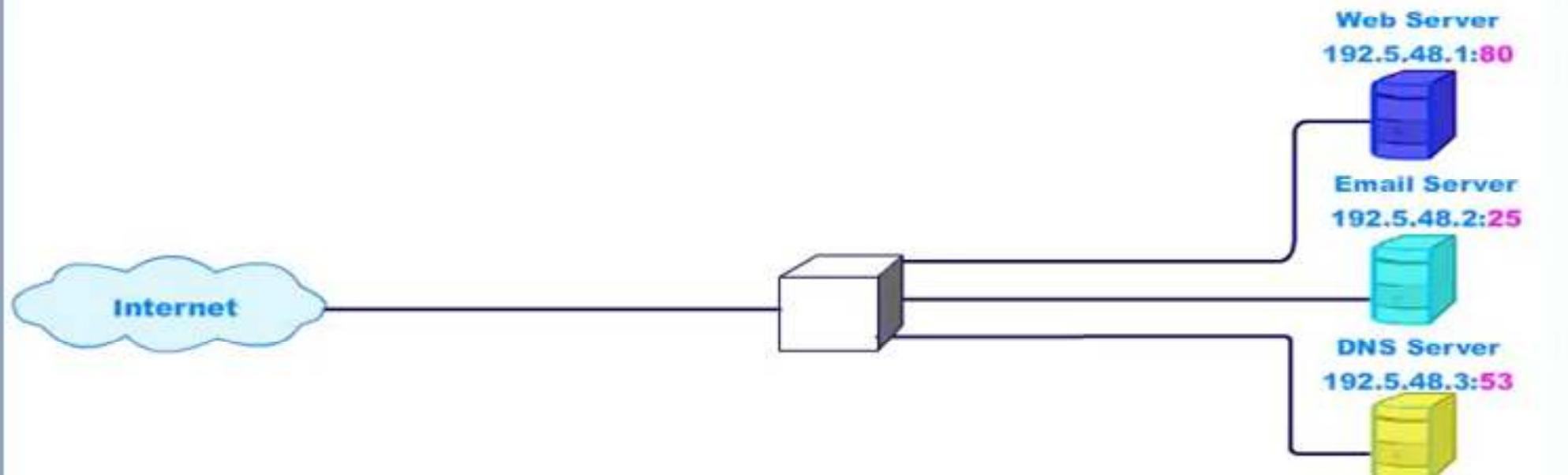
Least secure type of firewall; susceptible to IP spoofing (where attackers disguise their identity by falsifying their IP address).

## Example:

A network administrator sets up a packet filter to block all Telnet requests (port 23) to prevent remote login attempts by unauthorized users.

# Packet Filters

Firewall: Packet Filtering



# Proxy Servers

## Definition:

An intermediary that receives user requests and forwards them to the actual servers.

## Types:

**Application Gateways:** Operate at the application layer, inspecting traffic in detail (e.g., HTTP, FTP).

**Example:** A company may use an application gateway to block all incoming FTP traffic while allowing only HTTP traffic.

**Circuit-Level Gateways:** Operate at the transport layer (TCP/UDP); validate sessions before allowing data transmission.

**Example:** Ensures that all TCP sessions are authenticated before allowing any traffic.

## Advantages:

High security (especially application gateways) and ability to perform detailed traffic inspection.

## Disadvantages:

Can become a bottleneck due to intensive processing requirements.

# Stateful Packet Filters

Definition:

A firewall that monitors the state of active connections and makes filtering decisions based on the context of traffic.

Function:

Keeps track of the state of network connections (e.g., established, in-progress).

Filters packets based on the state table to allow only legitimate traffic.

Benefits:

Tighter security with reduced processing overhead compared to application gateways.

Example:

Only allows incoming traffic for connections that were initiated from within the network (e.g., returning data from a website that an internal user requested).

# Firewall Architectures

Definition:

Refers to how firewall components are arranged in a network to provide protection.

Types of Firewall Architectures:

**Dual-Homed Host Firewall:** A host with two network interfaces, one for the internal network and one for the external network.

**Screened Host Firewall:** Uses a combination of a bastion host and a packet-filtering router.

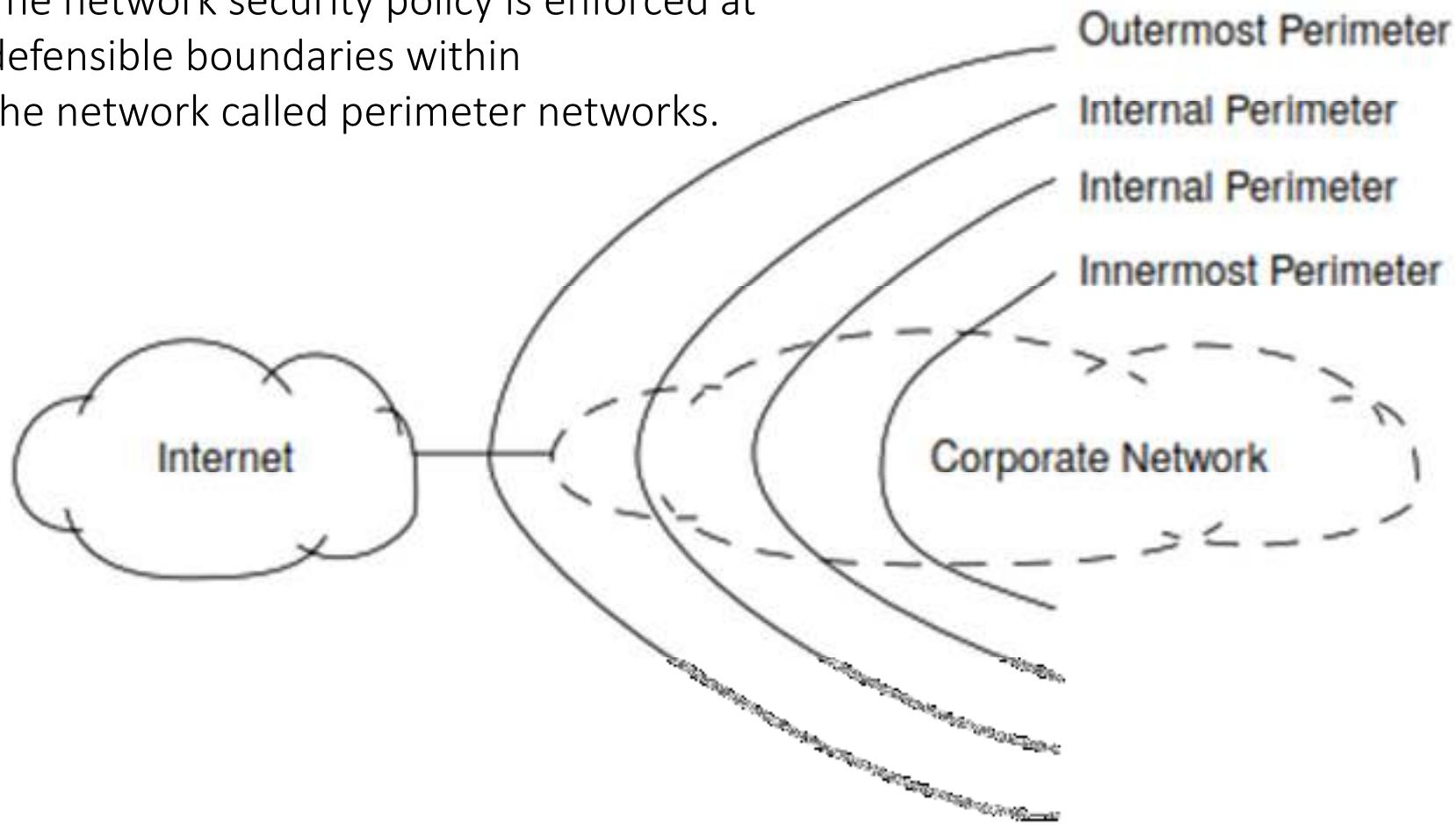
**Screened Subnet Firewall (DMZ):** Adds an extra layer of security between the internal and external networks.

Example:

A company might use a screened subnet firewall to protect its public-facing web server while keeping its internal network isolated.

# Firewall Architectures

The network security policy is enforced at defensible boundaries within the network called perimeter networks.



# Dual-Homed Host Firewall

## Definition:

A firewall setup where a single host (firewall) has two network interfaces to separate the internal and external networks.

## Characteristics:

Prevents direct communication between internal and external networks.

IP forwarding is disabled, ensuring no packets are directly routed between the networks.

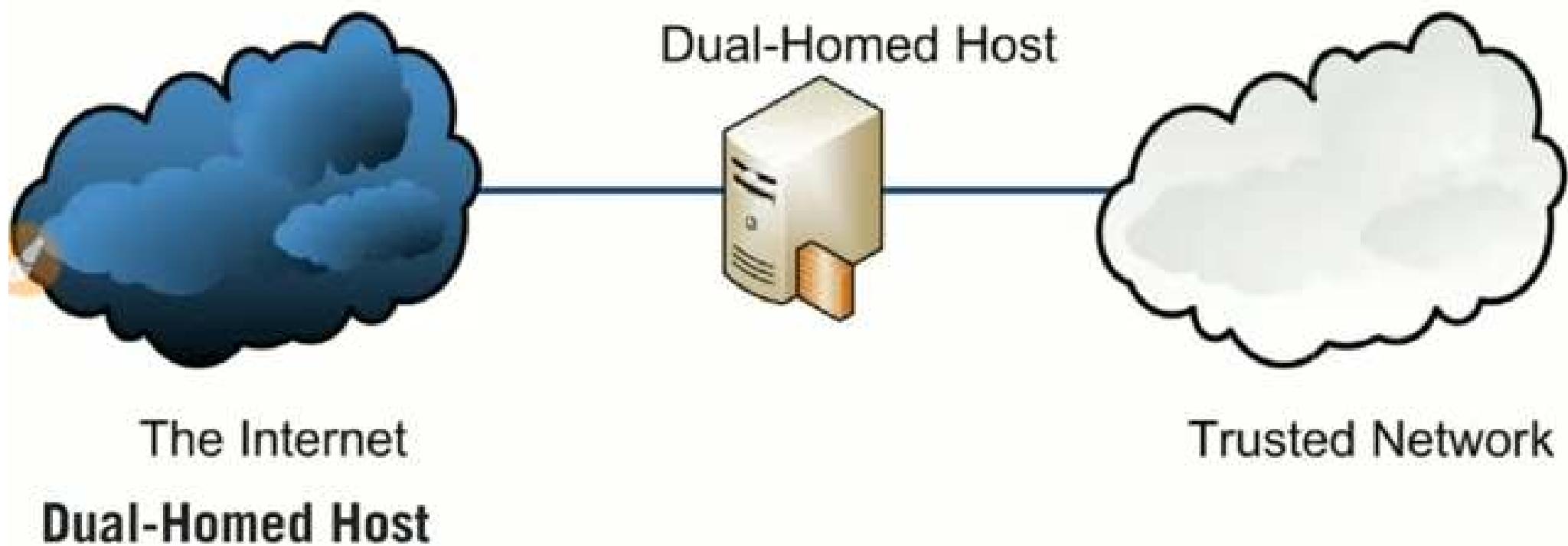
## Advantages:

Provides strong isolation; traffic is controlled by application proxies.

## Example:

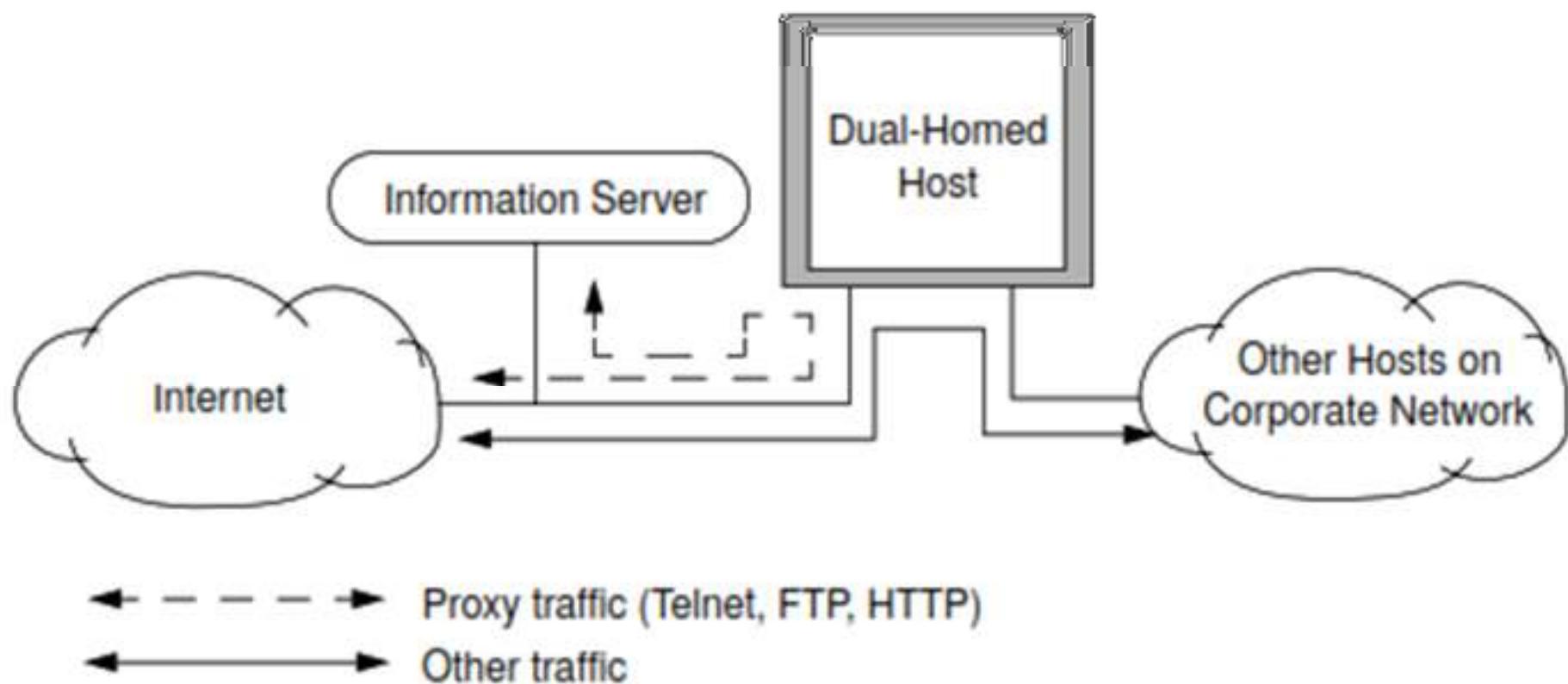
Used in environments where high security is needed, such as financial institutions or government agencies.

# Dual-Homed Host Firewall

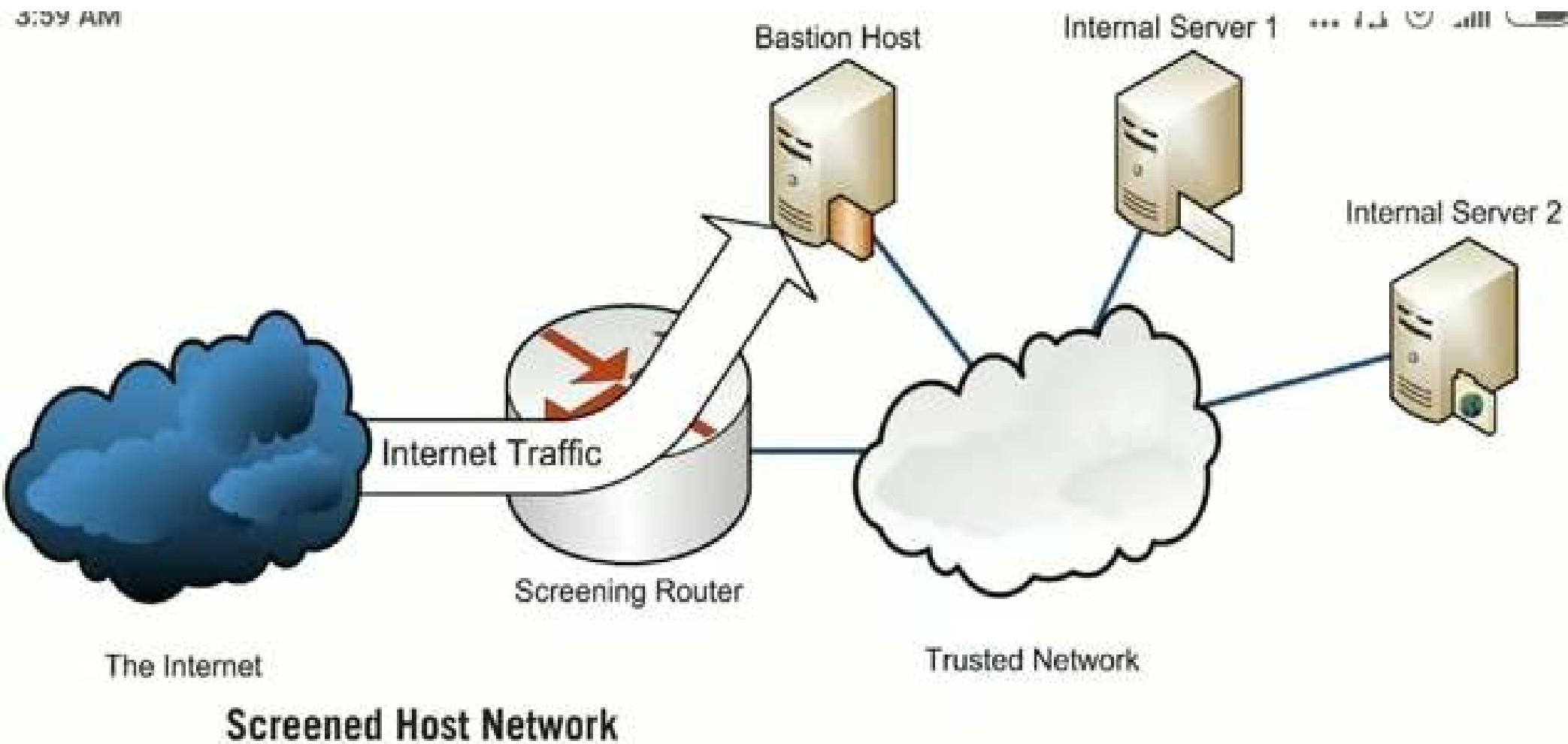


**Dual-Homed Host**

# Dual-Homed Host Firewall



# Screened Host Firewall



# Screened Host Firewall

## **Definition:**

- A firewall architecture with a bastion host and a packet-filtering router.

## **Characteristics:**

- All traffic from the external network must pass through the screening router before reaching the bastion host.

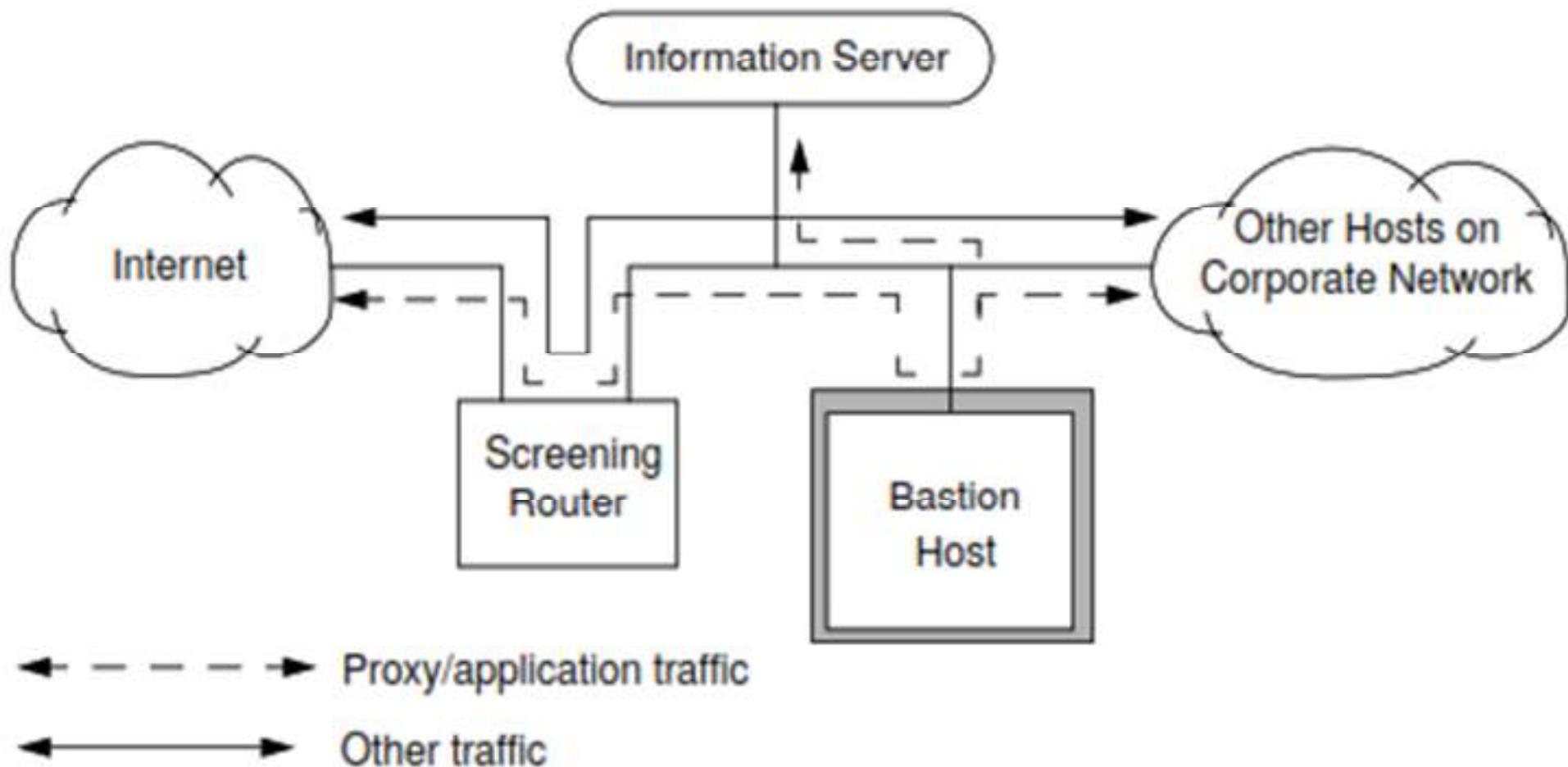
## **Advantages:**

- Provides an extra layer of security by placing the bastion host between the internal network and the Internet.

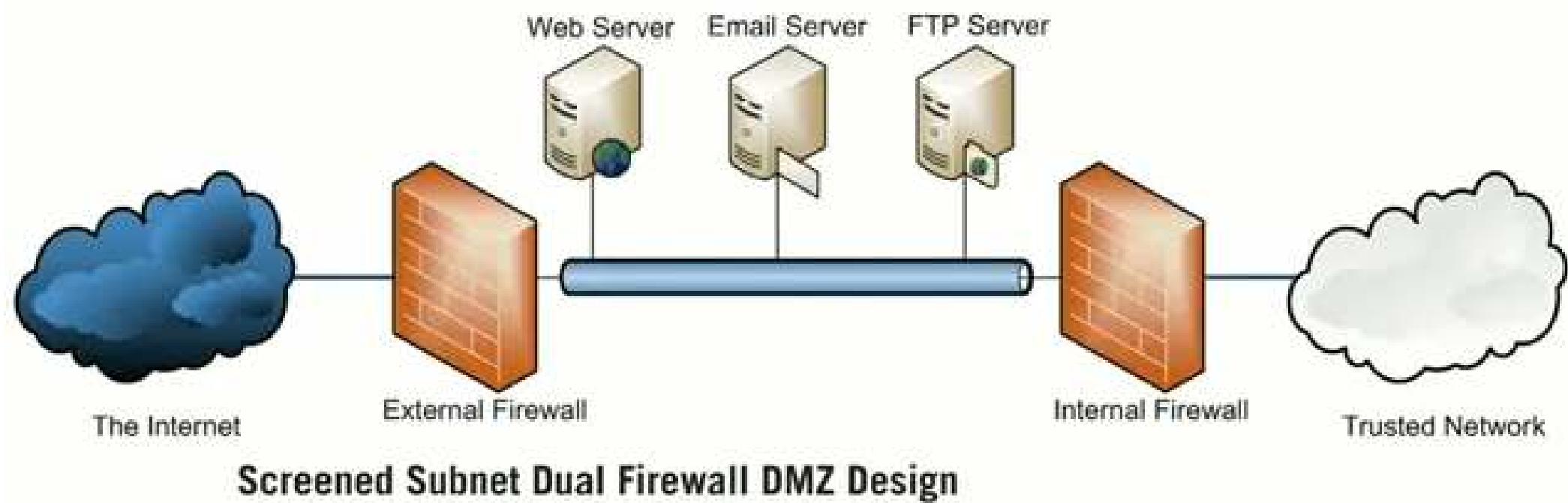
## **Example:**

- Ideal for protecting email servers that need to communicate with both internal users and external networks.

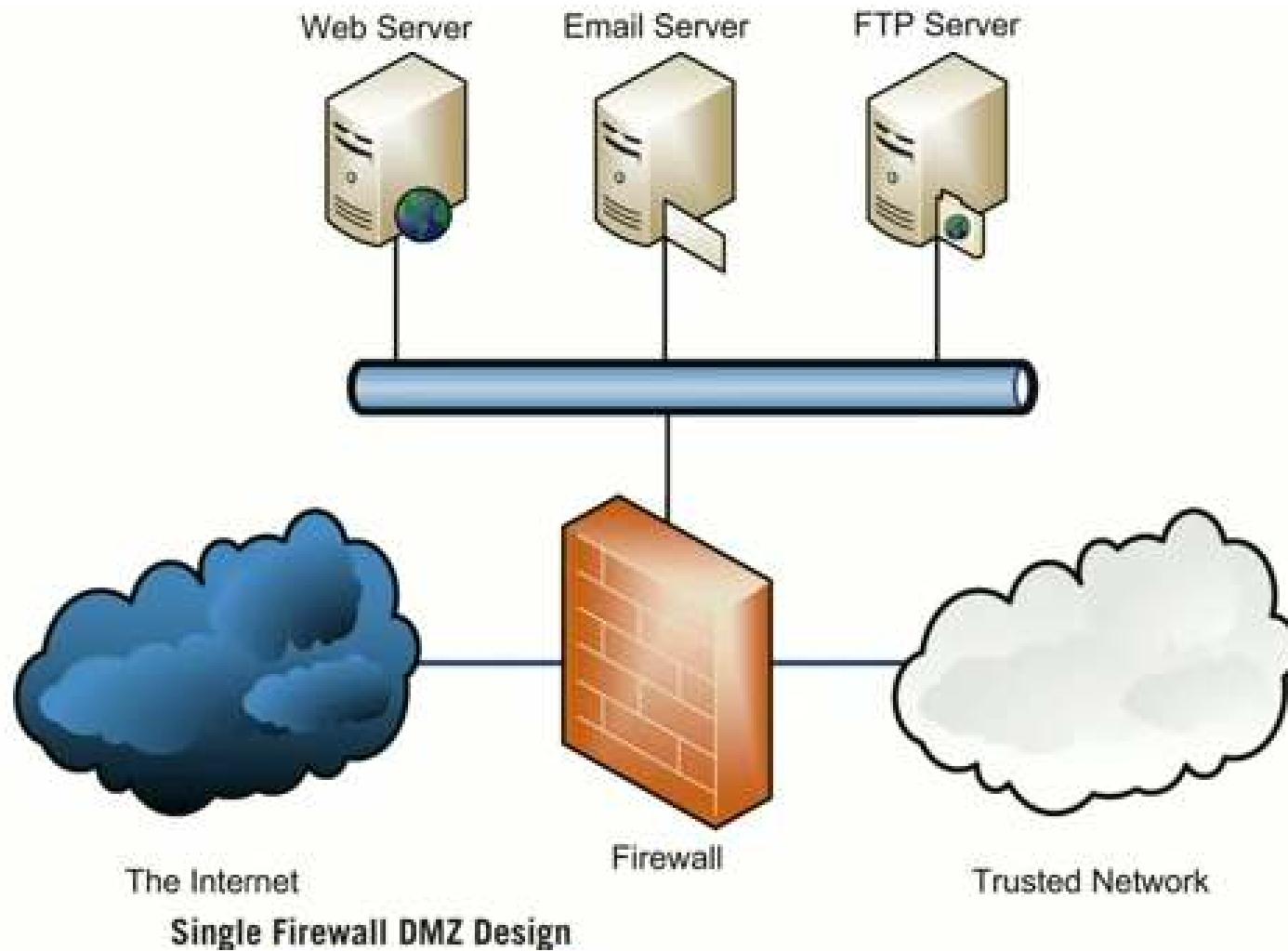
# Screened Host Firewall



# Screened Subnet Firewall (DMZ)



# Screened Subnet Firewall (DMZ)



# Screened Subnet Firewall (DMZ)

## **Definition:**

- An architecture that creates a **Demilitarized Zone (DMZ)** between the internal and external networks.

## **Characteristics:**

- Utilizes two routers (external and internal) to add a perimeter network (DMZ) between the corporate network and the Internet.

## **Advantages:**

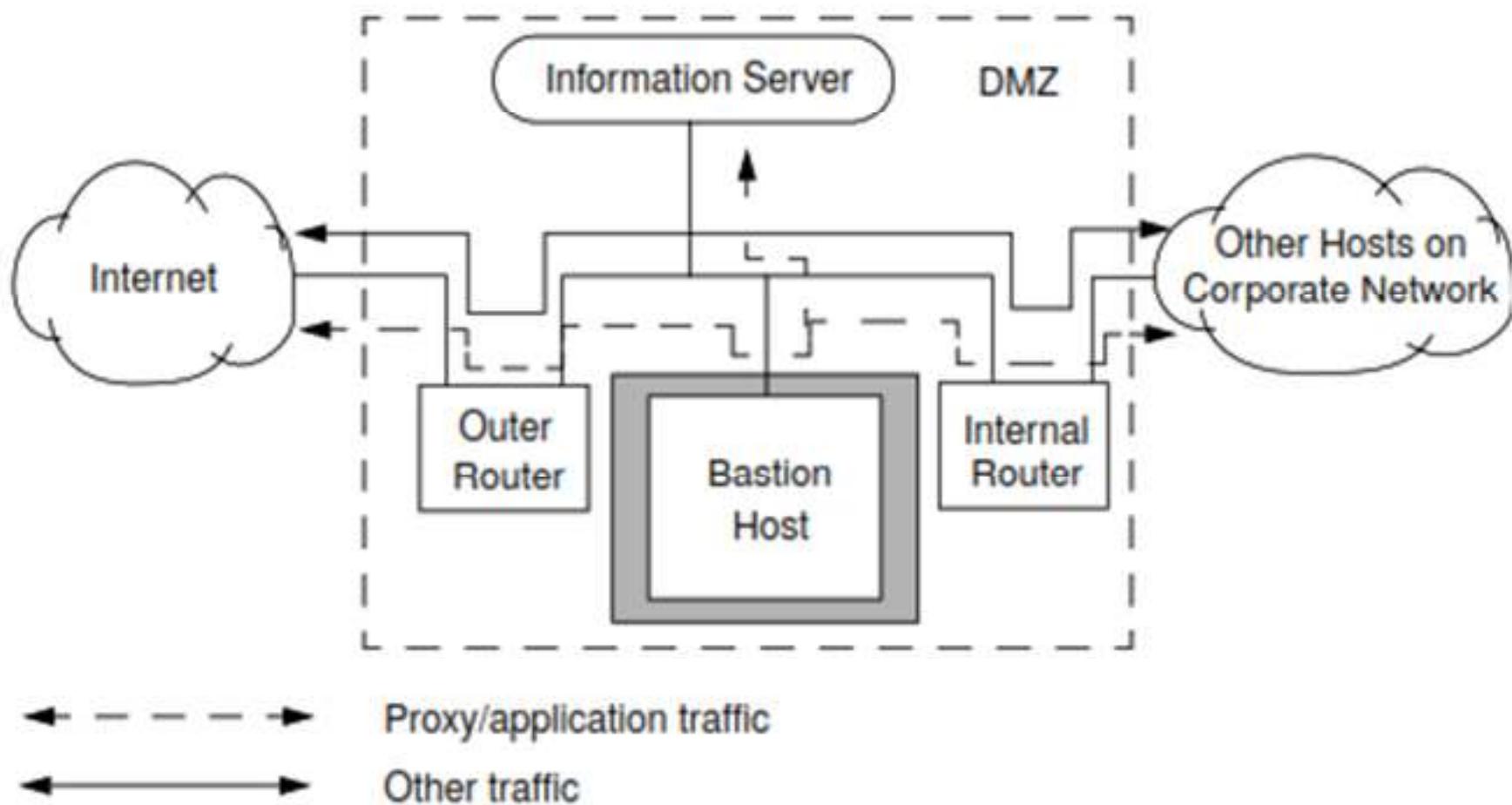
- Enhances security by isolating the DMZ network from both the internal network and the Internet.

## **Example:**

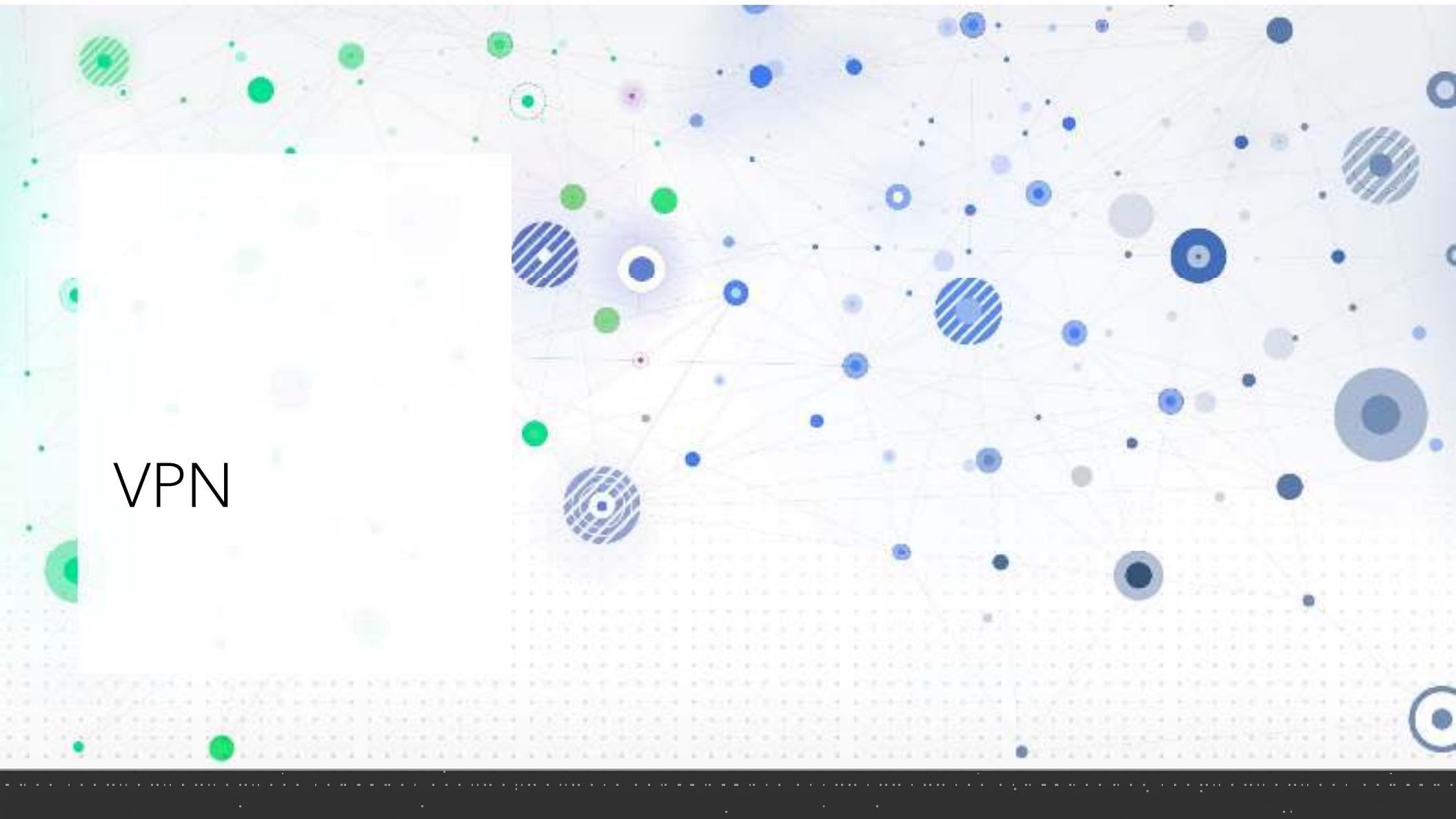
- Used by e-commerce companies to place web servers in the DMZ, while keeping sensitive databases in the internal network.

**Diagram:** Illustrate the DMZ setup with an outer and inner router, and the placement of a web server in the DMZ.

# Screened Subnet Firewall (DMZ)



VPN



# Virtual Private Networks (VPNs)

A **Virtual Private Network (VPN)** provides a secure communication channel over a public network like the Internet.

## Purpose:

- Enables remote and branch offices to securely connect to the corporate network.
- Converts a public network into a private, secure network using encryption.

## Advantages:

- Cost-effective alternative to private leased lines.
- Allows remote access and communication with high security.

## Example:

- A remote worker connects to the company's internal network using a VPN client, allowing them to access internal resources securely.

# Types of VPNs

## **Access VPNs:**

Provides secure access for remote users such as telecommuters and mobile employees.

**Example:** A sales manager accesses the company's CRM system from a hotel using an access VPN.

## **Intranet VPNs:**

Connects multiple branch offices securely to the corporate headquarters.

**Example:** A company with offices in different cities uses an intranet VPN to maintain secure internal communications.

## **Extranet VPNs:**

Allows external partners, customers, or suppliers to access certain parts of the corporate network securely.

**Example:** A supplier accesses inventory data from a retailer's database through an extranet VPN.

# VPN Architectures

**VPN Client:** Device initiating the connection (e.g., laptop, mobile).

**Network Access Server (NAS):** Terminates dial-up calls and initiates a VPN connection. The NAS is owned by the ISP.

**VPN Server:** Recovers the packet from the tunnel the VPN tunnel and decrypts data. Reside in ISP's.

**VPN Protocol:** Manages how the data is encrypted and transmitted.

## Tunneling Protocols:

- **Layer 2 Protocols:** PPTP, L2F, L2TP.
- **Layer 3 Protocols:** IPSec.

## Example:

- A remote employee's laptop acts as a VPN client connecting through a NAS provided by their ISP to a corporate VPN server.

# VPN Architectures

**VPN Client:** The VPN client is the software or device that connects to the VPN server

**Remote Network:** This is the local network to which the VPN client is connected

**PSTN (Public Switched Telephone Network):** This network provides a communication channel between the VPN client and the internet through traditional telecommunication infrastructure

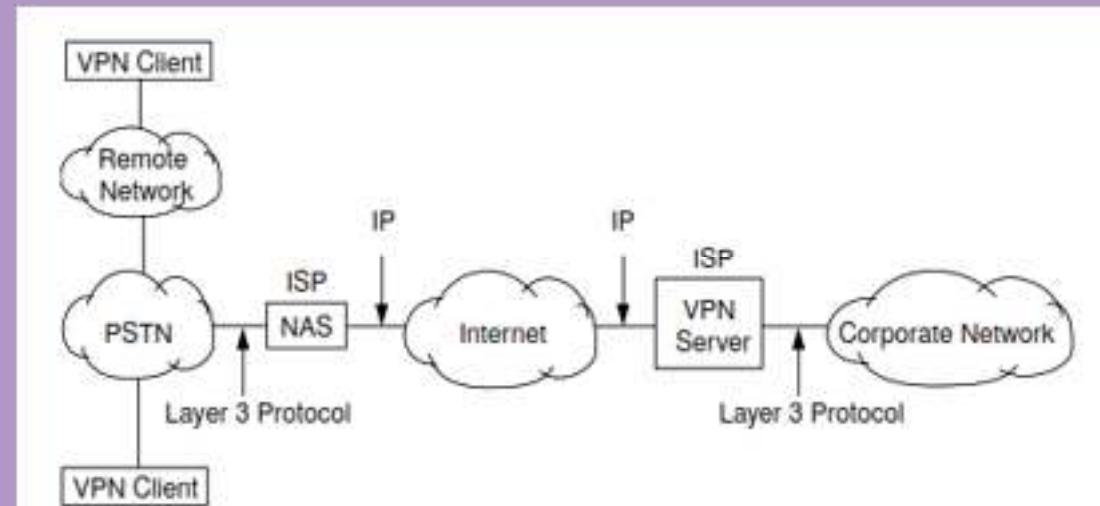
**NAS :** The NAS is a device that provides a point of entry to a secure network

**Internet:** The internet acts as a public network that the VPN traffic must traverse

**ISP :** The ISP provides internet connectivity for the VPN client and the VPN server

**VPN Server:** The VPN server is the endpoint of the VPN tunnel on the corporate network side

**Corporate Network:** This is the private network that the VPN client wants to access securely



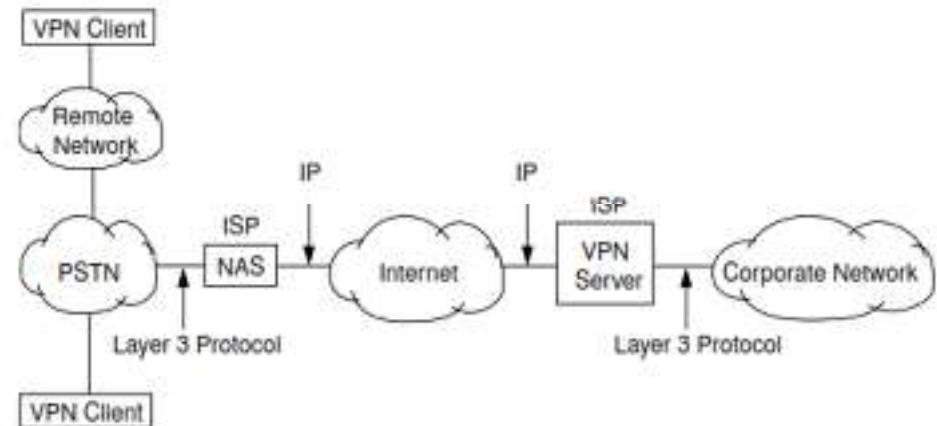
# Protocols and Communication Flow

---

Layer 3 Protocol:  
Refers to network layer protocols used to transport data between networks

IP : IP is used for routing the encrypted packets over the internet.

# Working of the VPN



The VPN client initiates a connection to the VPN server, establishing a secure tunnel over the internet

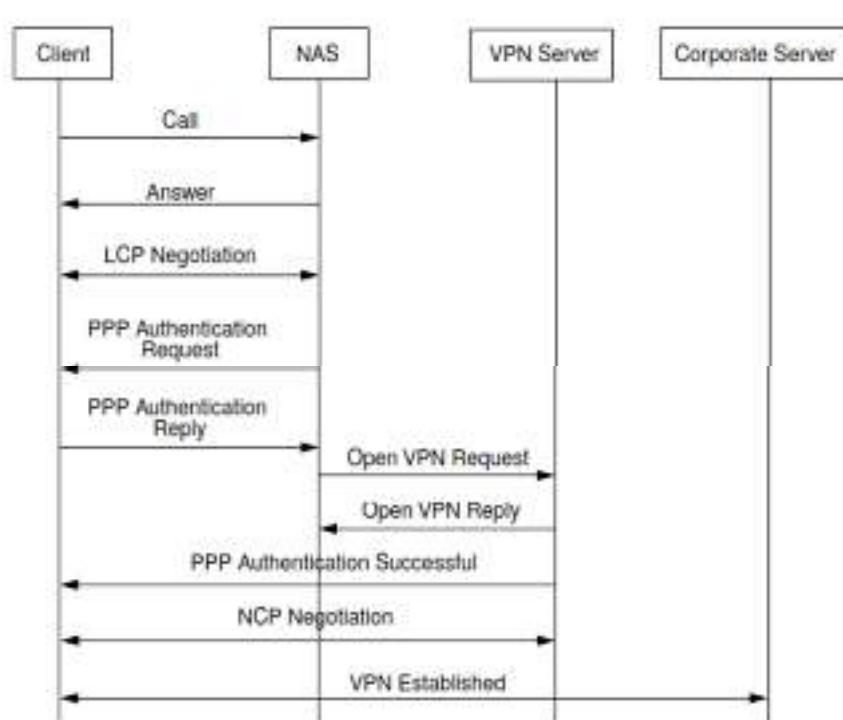
The client communicates with the Network Access Server, typically through an ISP

Once authenticated, an encrypted IP tunnel is created between the VPN client and the VPN server

Data flows through the PSTN, NAS, internet, and VPN server securely, and the VPN server connects the client to the corporate network

The corporate network is now accessible to the remote user as if they were directly connected to it

# Layer 2 Tunneling Protocols



## Call

- The client initiates a connection by making a call to the NAS

## Answer

- The NAS responds to the client's call

## logical control protocol Negotiation

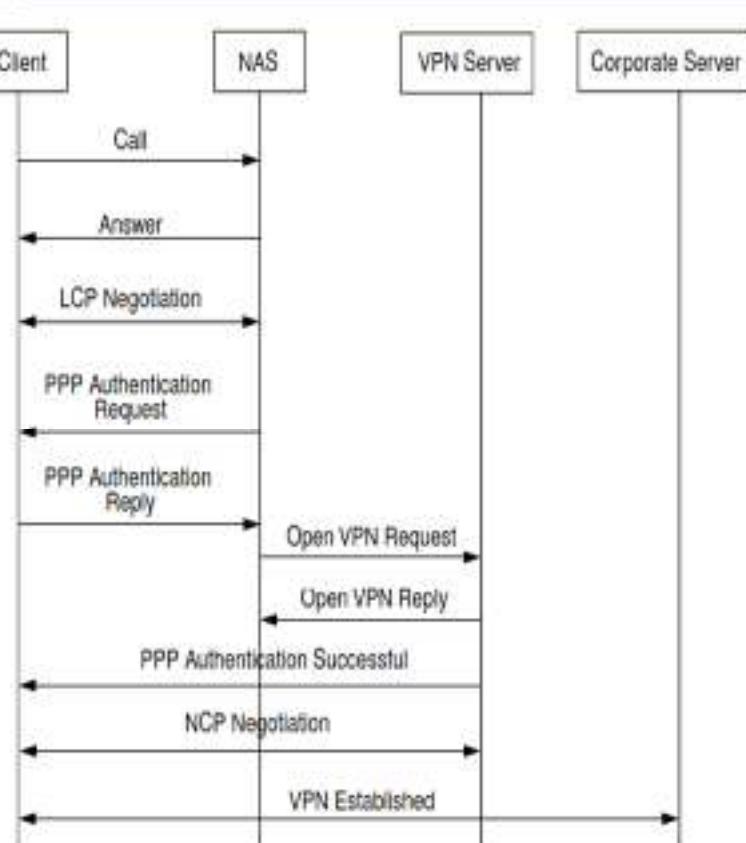
- The client and NAS perform LCP negotiation, which is a part of the Point-to-Point Protocol

## PPP Authentication Request

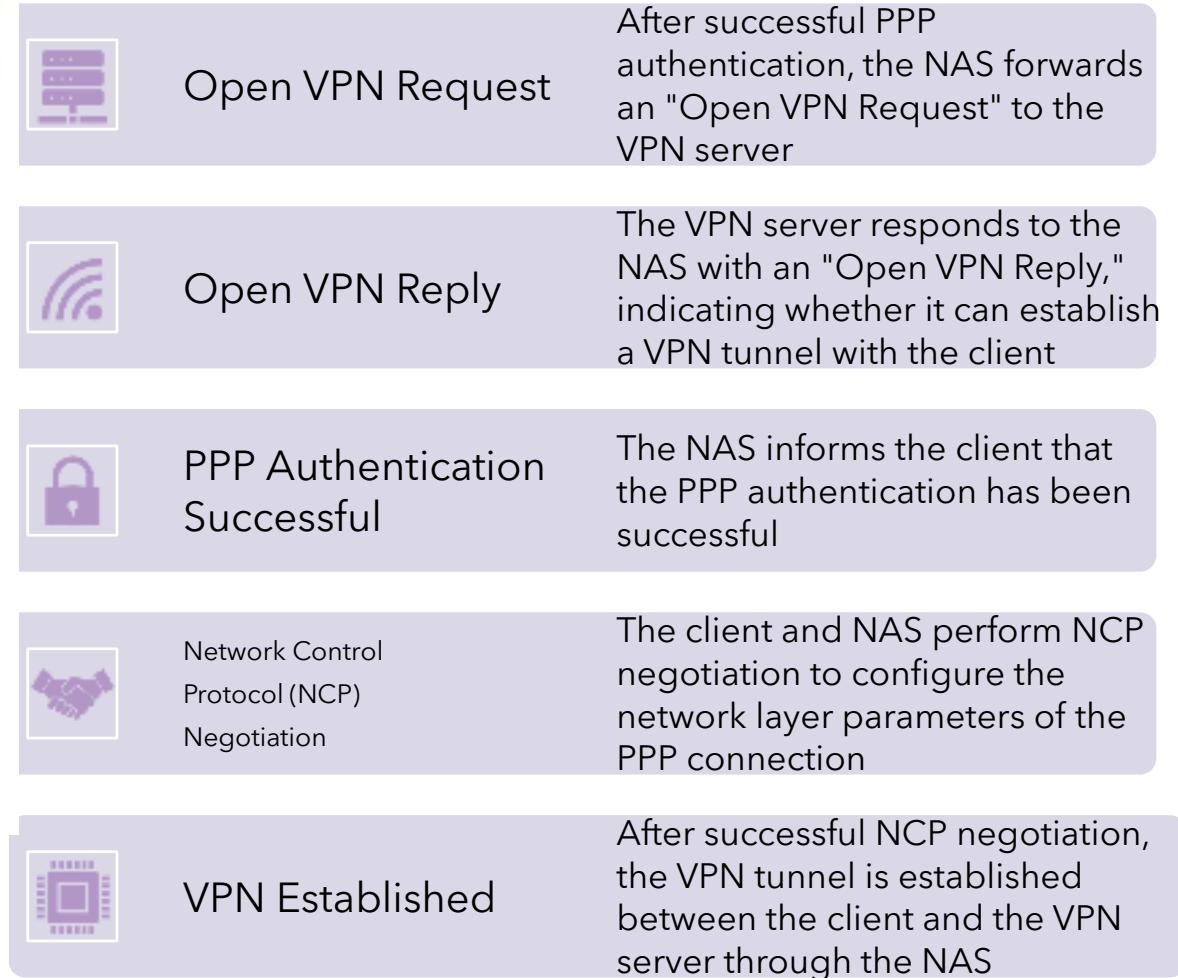
- The NAS requests authentication from the client using the chosen PPP authentication protocol

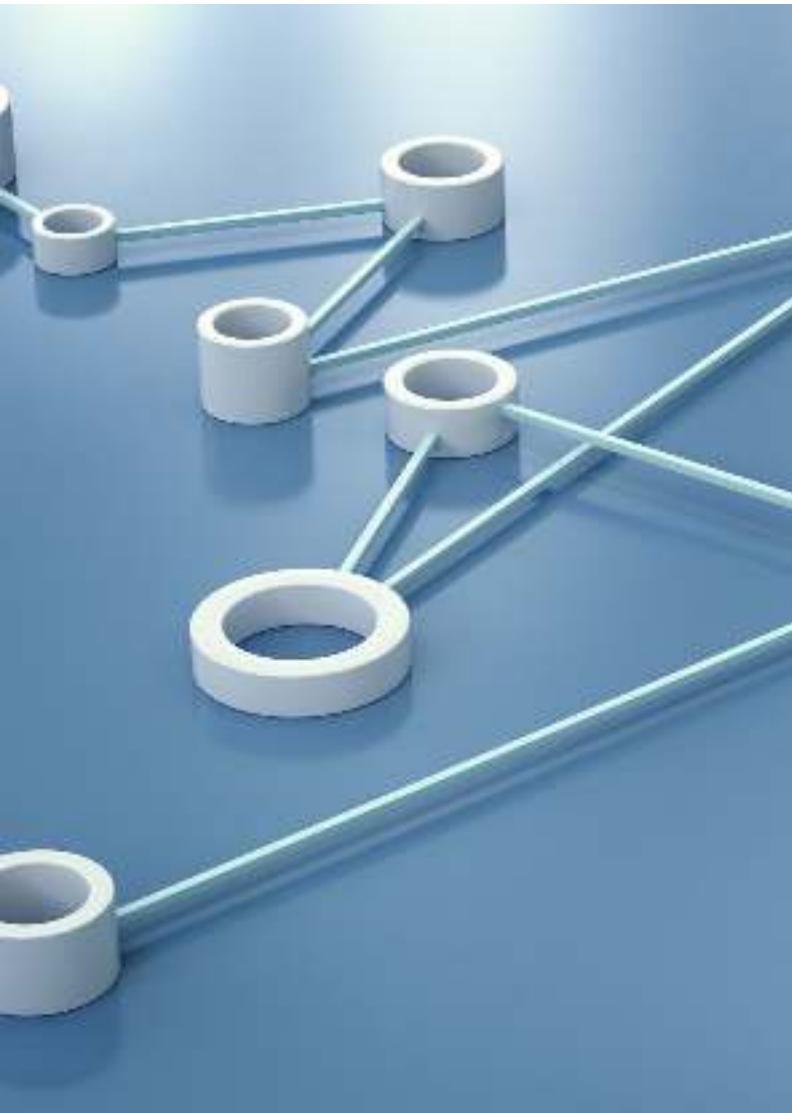
## PPP Authentication Reply

- The client sends an authentication reply back to the NAS



## Layer 2 Tunneling Protocols





# Key Takeaways

---

**Authentication and Negotiation:** The process involves several layers of authentication and negotiation to ensure a secure connection

- **LCP and NCP Negotiations:** These are essential steps in setting up the connection parameters for data transmission
- **PPP Authentication:** Ensures that only legitimate users can access the corporate network

**VPN Tunnel Establishment:** The ultimate goal is to create a secure tunnel that allows the client to communicate with the corporate network as if directly connected

# Layer 2 Tunneling Protocols

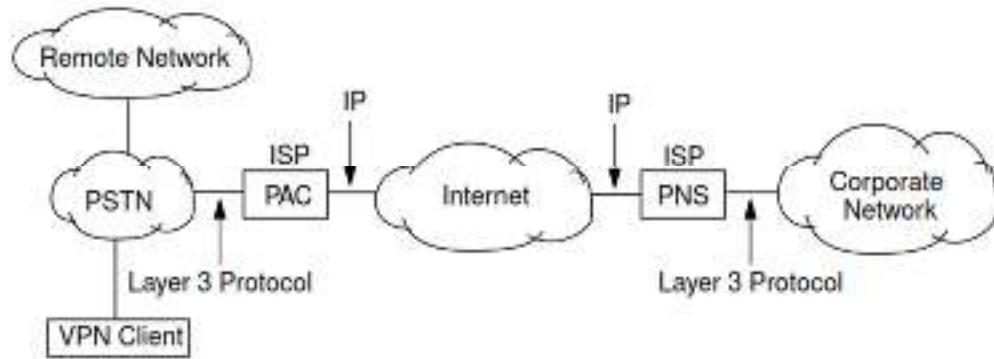
## Overview:

- Operate at the data link layer (Layer 2) to encapsulate data packets for secure transmission.

## Protocols:

- **PPTP (Point-to-Point Tunneling Protocol):** Allows different types of network traffic to be encrypted and transmitted over the Internet.
  - **Example:** Encapsulates IPX or NetBEUI packets inside IP packets.
- **L2F (Layer 2 Forwarding):** Protocol-independent, works over X.25, Frame Relay, and ATM.
  - **Example:** Used by ISPs to connect customers securely over various networks.
- **L2TP (Layer 2 Tunneling Protocol):** Combines PPTP and L2F; more firewall-friendly due to its use of UDP.
  - **Example:** Allows secure connections for remote offices over different ISPs.

# PPTP Architecture



## PPTP access concentrator (PAC)

- The PAC is a network device that establishes the connection between the VPN client and the internet
- The PAC acts as a gateway that receives encrypted packets from the VPN client and encapsulates them in PPTP for transmission over the internet to the PNS

## PPTP network server

- The PNS is the server-side component of the PPTP architecture that terminates the PPTP tunnels initiated by the PAC
- The PNS also handles the authentication, authorization, and accounting services required for client access
- The PNS essentially serves as the VPN server in a PPTP environment, managing the secure communication between the VPN client and the corporate network

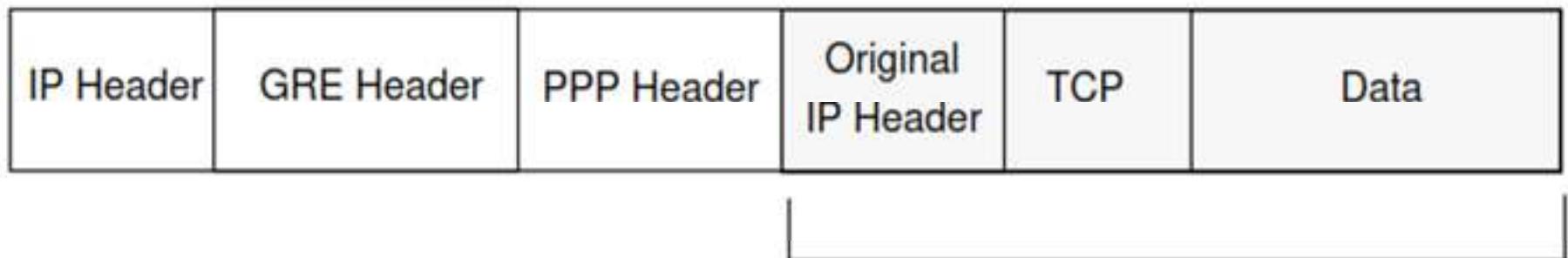
# Summary of Their Roles in PPTP

---

The PAC is responsible for establishing the initial connection with the VPN client and creating a secure tunnel over the internet

The PNS receives the tunneled traffic from the PAC, performs necessary security checks, and provides access to the corporate network

# PPTP packet format.



## **PPTP Encryption:**

PPTP does not offer direct packet-by-packet encryption.

Relies on PPP's native encryption.

## **PPP Payload**

## **Packet Encapsulation:**

PPTP Packet is encapsulated using Generic Routing Encapsulation (GRE).

Carried over IP networks.

## **Separation of Control and Data Channels:**

Control Channel: Runs over TCP.

Data Channel: Runs over GRE.

**PPP Payload:** Includes data with its TCP and IP headers.

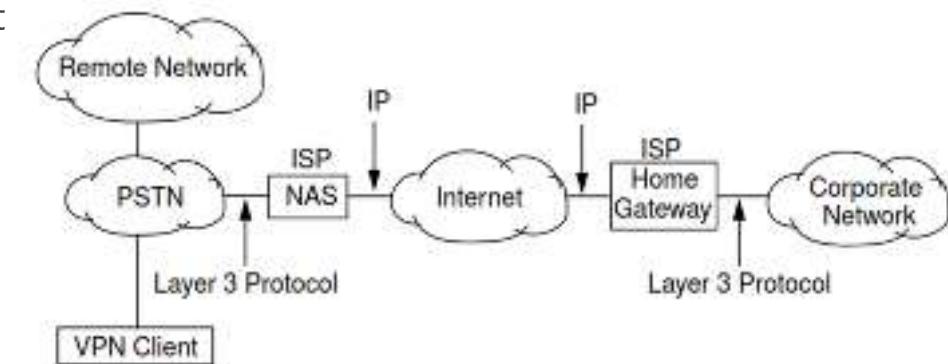
# Key Components of L2F

## Network Access Server(NAS)

- The NAS is a critical component in the L2F architecture
- In the L2F setup, the NAS receives Layer 3 protocol data from the VPN client over the PSTN and forwards it to the Home Gateway

## Home Gateway

- The Home Gateway, in the context of L2F, is the endpoint at the corporate network side
- This gateway receives encrypted data sent from the NAS over the public internet, decrypts it, and forwards it to the appropriate resources within the corporate network
- The Home Gateway also plays a role in ensuring that only authenticated and authorized VPN clients are allowed to access the corporate network



# Working of L2F Protocol

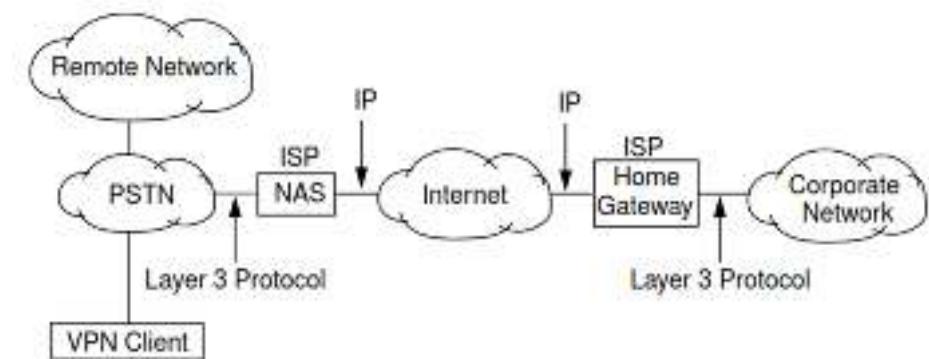
**VPN Client:** Initiates a connection from the remote network over the PSTN to the NAS using a Layer 3 protocol

**NAS:** Acts as an intermediary that accepts the connection from the VPN client, performs the necessary authentication, and then encapsulates the client data into an L2F tunnel

**Internet:** Functions as the public network through which the L2F tunnel securely carries the client data from the NAS to the Home Gateway

**Home Gateway:** Terminates the L2F tunnel, decapsulates the client data, and forwards it to the corporate network for processing

**Corporate Network:** The destination network that the VPN client wants to securely access



# L2F packet format.

L2F Header	SLIP/PPP Payload	L2F Checksum (Optional)
------------	------------------	----------------------------

## **L2F Encapsulation:**

L2F (Layer 2 Forwarding) uses its own encapsulation header. Unlike PPTP, it does not rely on IP and GRE headers.

## **Network Compatibility:**

L2F's unique header allows it to operate across various types of networks, enhancing flexibility.  
Packet Structure:

**SLIP/PPP Payload:** Encapsulated within an L2F packet.

**L2F Header:** Custom header specific to L2F.

**Optional L2F Checksum:** Serves as a trailer for additional integrity verification.



# Summary of L2F Protocol

---

**Layer 2 Forwarding:** Provides a secure method for connecting remote users to a corporate network by creating a virtual private tunnel over the internet

**Role of NAS and Home Gateway:** The NAS acts as the tunnel initiator, while the Home Gateway serves as the tunnel terminator, enabling secure access to the corporate network

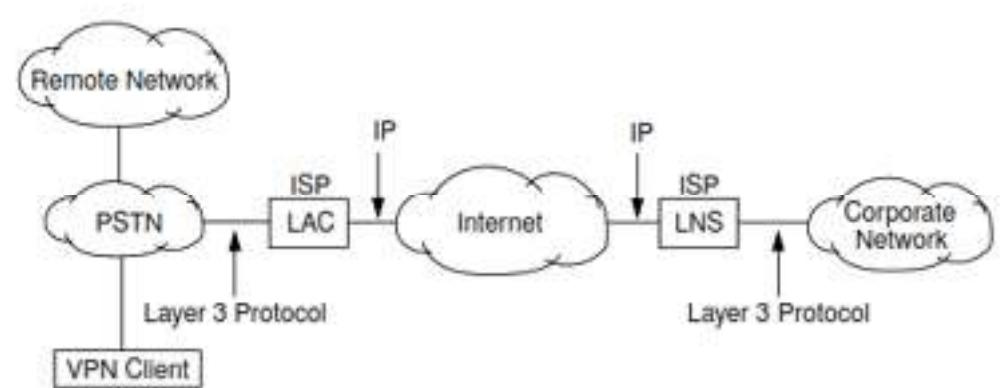
**Security and Authentication:** The L2F protocol relies on secure tunneling techniques and user authentication to protect data integrity and privacy while traversing public networks

## LAC(L2TP access concentrator (LAC))

- The LAC is a device located at the client's end that acts as the starting point for the L2TP tunnel
- The LAC receives Layer 3 protocol data from the VPN client through the PSTN and encapsulates these packets into L2TP frames
- The LAC is responsible for establishing and maintaining the L2TP tunnel between itself and the LNS, ensuring that the data is correctly tunneled over the public network

## Key Components Specific to L2TP Architecture

---

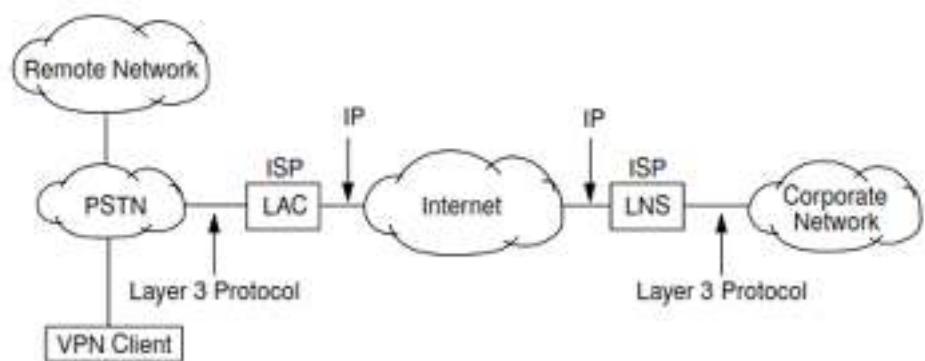


## LNS

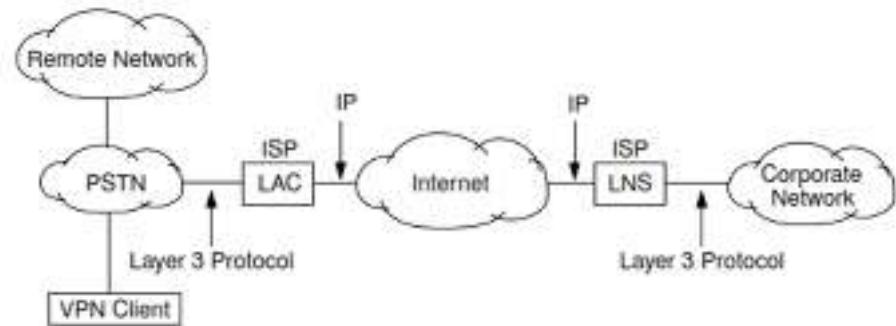
- The LNS is the endpoint of the L2TP tunnel on the corporate network side
- The LNS authenticates the VPN client, manages the sessions, and forwards the client's data to the appropriate resources within the corporate network
- It acts as the server-side gateway that terminates the L2TP tunnel, ensuring secure communication between the VPN client and the corporate network

## Key Components Specific to L2TP Architecture

---



# Working of the L2TP Protocol



VPN Client	LAC	Internet	LNS	Corporate Network
<ul style="list-style-type: none"><li>The VPN client initiates a connection from a remote network over the PSTN using a Layer 3 protocol to communicate with the LAC</li></ul>	<ul style="list-style-type: none"><li>The LAC acts as the client's gateway to the VPN</li><li>The LAC sends these encapsulated packets over the public internet to the LNS, providing a secure path for data transmission</li></ul>	<ul style="list-style-type: none"><li>The internet acts as the medium over which the L2TP tunnel carries the client's data securely from the LAC to the LNS</li></ul>	<ul style="list-style-type: none"><li>The LNS receives the L2TP-encapsulated packets from the LAC, decapsulates them, and authenticates the user</li><li>After successful authentication, the LNS forwards the decapsulated packets to the corporate network, allowing the client to access internal resources securely</li></ul>	<ul style="list-style-type: none"><li>The corporate network is the end destination for the client's data, consisting of servers, applications, databases, and other resources that are not directly accessible from the public internet</li></ul>

# Summary of L2TP Protocol

---



## Layer 2 Tunneling Protocol

L2TP is used to tunnel data across public networks securely, but it relies on another protocol for encryption



## Role of LAC and LNS

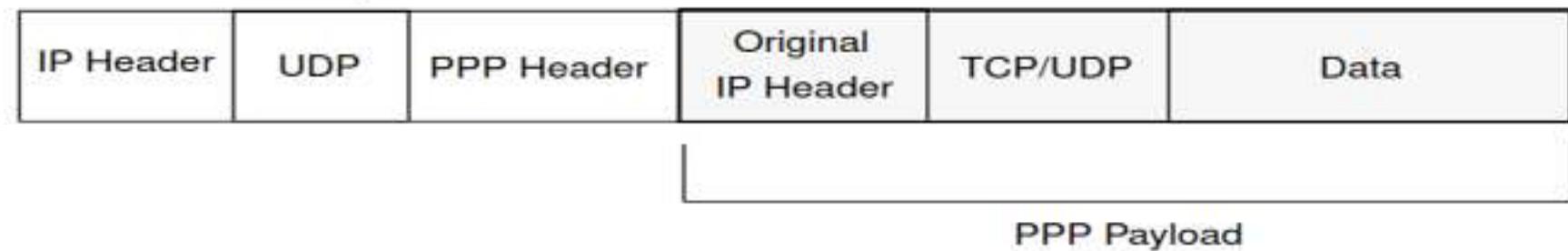
The LAC serves as the client-side device that initiates the L2TP tunnel, while the LNS is the server-side device that terminates the tunnel, handles authentication, and forwards data to the corporate network



## Security and Functionality

L2TP provides a flexible, protocol-independent method for tunneling, which is often paired with IPsec to ensure strong encryption and secure data transmission over potentially insecure public networks

# Summary of L2TP Protocol



## **L2TP Features:**

Combines features of PPTP and L2F.

Runs over UDP instead of TCP and does not use GRE.

## **Firewall Compatibility:**

More firewall-friendly as many firewalls do not support GRE used by PPTP.

Key Components:

**LAC (L2TP Access Concentrator):** Acts as the NAS (Network Access Server).

**LNS (L2TP Network Server):** The VPN server endpoint.

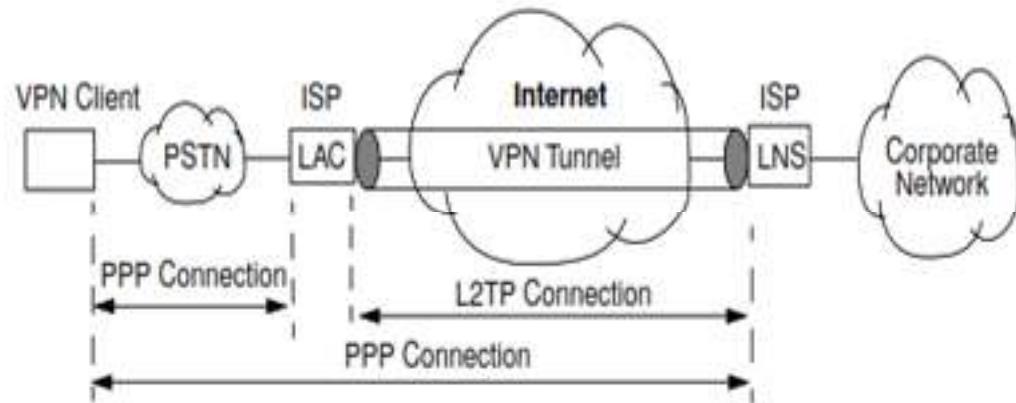
# VPN Models

## NAS-Initiated VPN:

- VPN connection initiated by the NAS, which handles user authentication and creates the tunnel.
- **Advantages:** Reduces overhead by supporting multiple user connections.
- **Example:** Used by organizations outsourcing their VPN management to ISPs.

## Client-Initiated VPN:

- VPN connection initiated directly by the client device.
- **Advantages:** Greater control over security and encryption.
- **Example:** A remote worker uses a VPN client software to connect directly to the company's VPN server.
- **Diagram:** Compare NAS-initiated and client-initiated VPN models.



# NAS-Initiated VPN Model

---



## VPN Client

The VPN Client is a remote user or device that needs to connect securely to a corporate network



## PSTN

The PSTN provides the initial physical layer connection between the VPN client and the NAS



## LAC

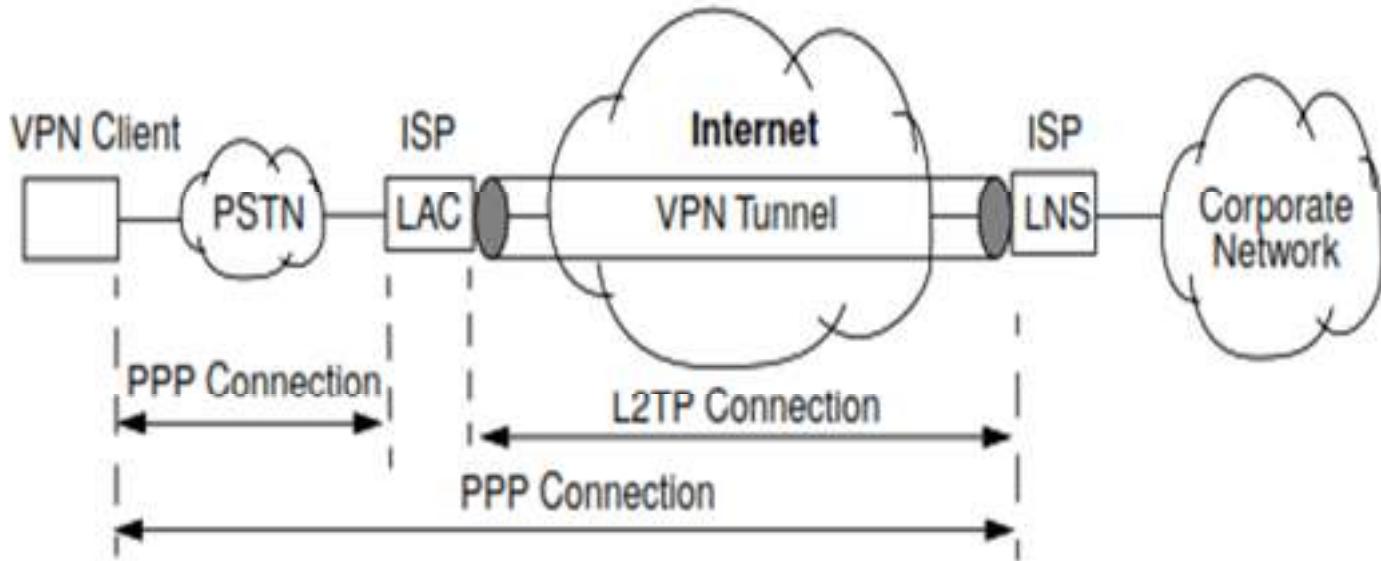
The LAC is the network access server that receives the PPP connection from the VPN client



## Internet

The Internet acts as the public network over which the L2TP VPN tunnel is established

In this NAS-Initiated model, the LAC is responsible for establishing and managing the VPN tunnel to the LNS on behalf of the client



#### VPN Tunnel

- The VPN Tunnel represents the L2TP tunnel established between the LAC and the LNS

#### LNS

- The LNS is the server at the corporate network side that terminates the L2TP tunnel initiated by the LAC
- The LNS also handles client authentication, session management, and access control

#### Corporate Network

- The corporate network consists of internal resources such as servers, applications, and databases that the VPN client wishes to access securely

## NAS-Initiated VPN Model

# Connections

## PPP Connection

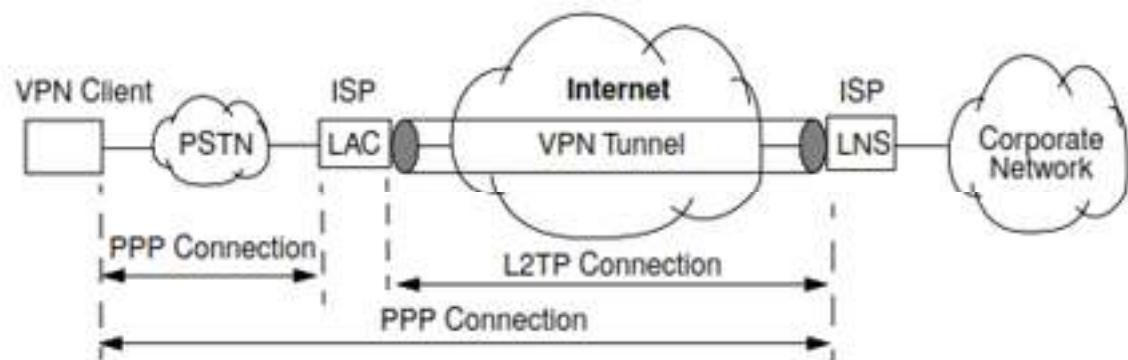
- The initial connection from the VPN client to the NAS is a standard PPP connection over the PSTN

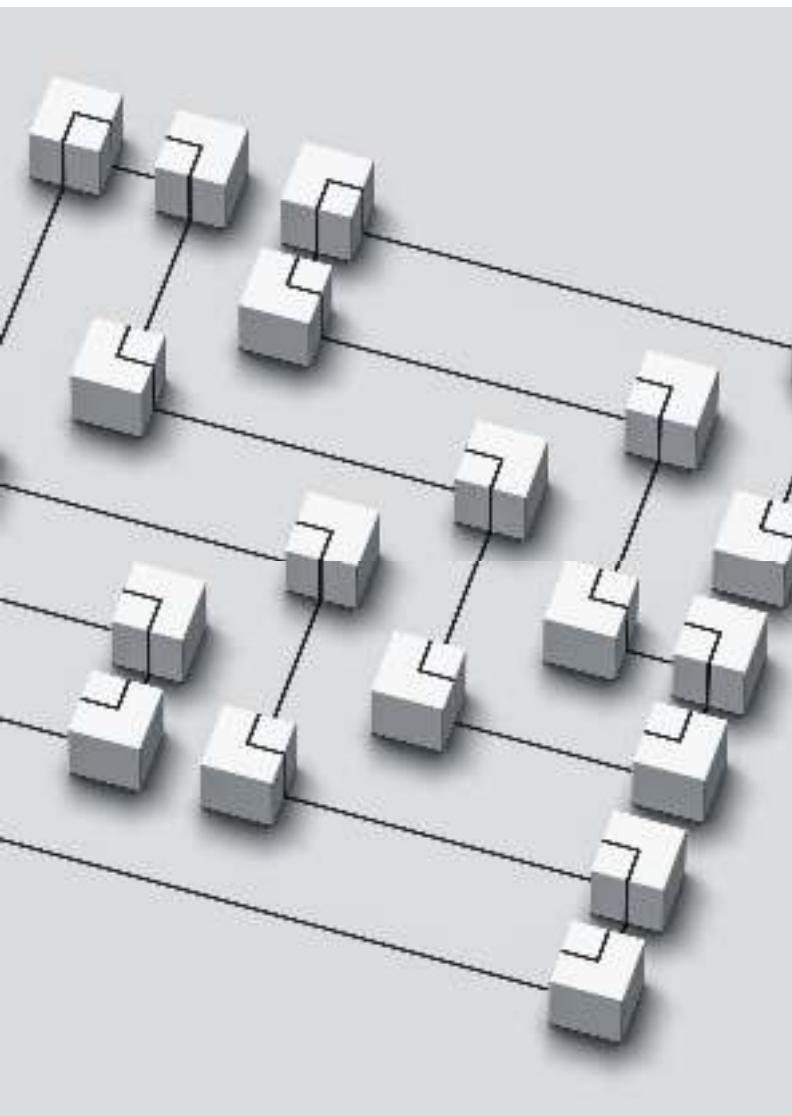
## L2TP Connection

- The LAC initiates an L2TP connection over the internet to the LNS

## PPP Connection

- Once the L2TP tunnel is established, the PPP connection effectively extends from the VPN client to the LNS across the L2TP tunnel





## Key Features of the NAS-Initiated VPN Model

---

**NAS-Initiated Tunnel:** In this model, the NAS is responsible for initiating the L2TP tunnel to the corporate network, reducing the complexity required on the client side

**Centralized Authentication:** The LNS at the corporate network side handles all authentication, ensuring that only legitimate users are allowed access

**Secure Data Transmission:** The model ensures that all data transmitted between the client and the corporate network is securely encapsulated and protected from interception or tampering over the public internet

# Use Cases

---

This model is particularly useful for ISPs or enterprises that want to provide secure remote access services to multiple users without requiring complex VPN client configurations

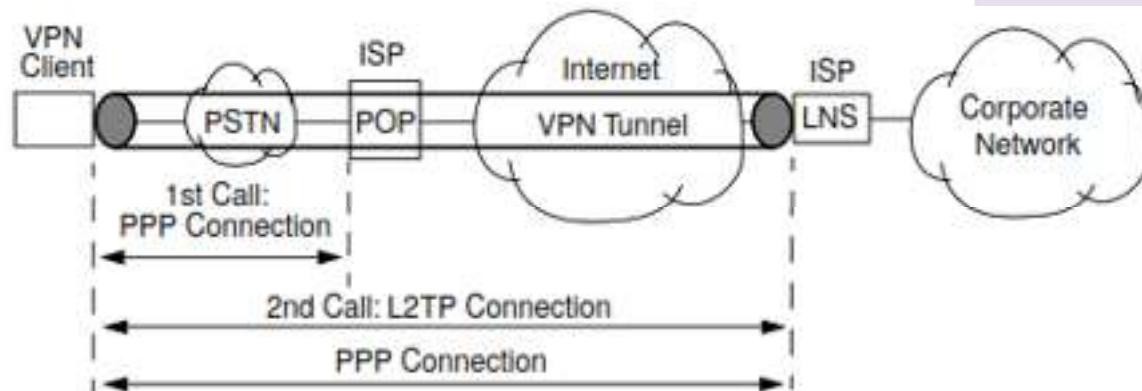
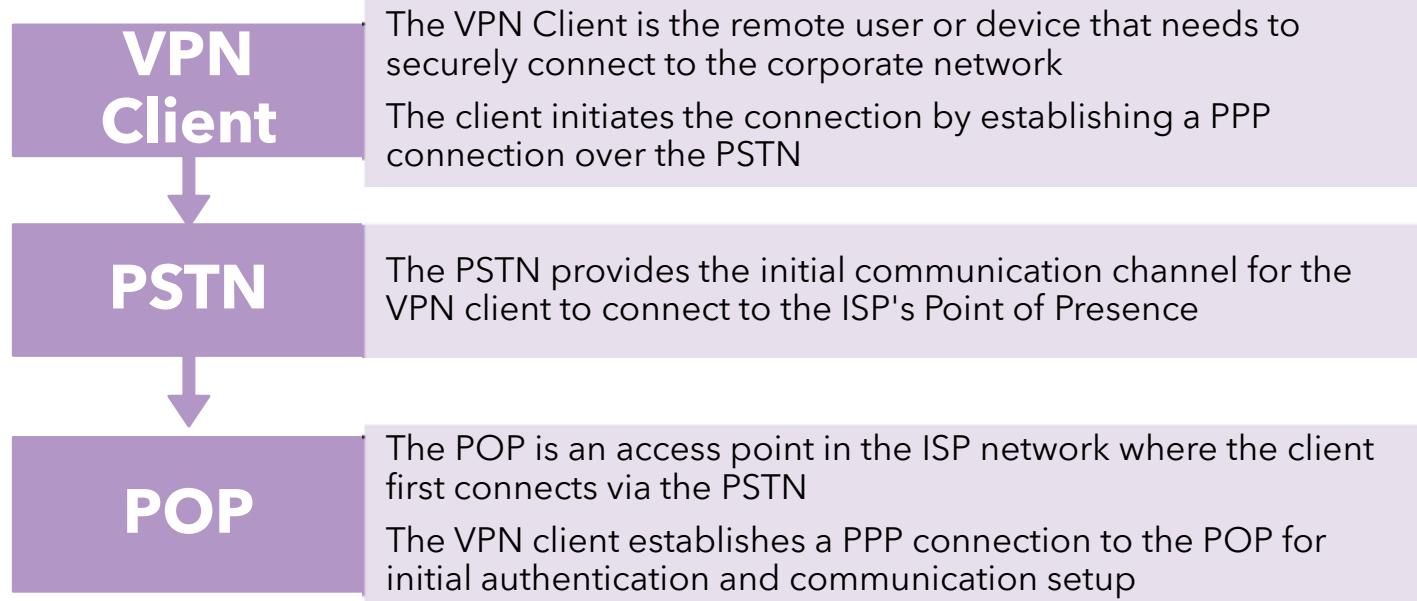
It allows for centralized management of VPN connections, authentication, and policies by the network administrators at the corporate network



# Client-Initiated VPN

---

# Client-Initiated VPN



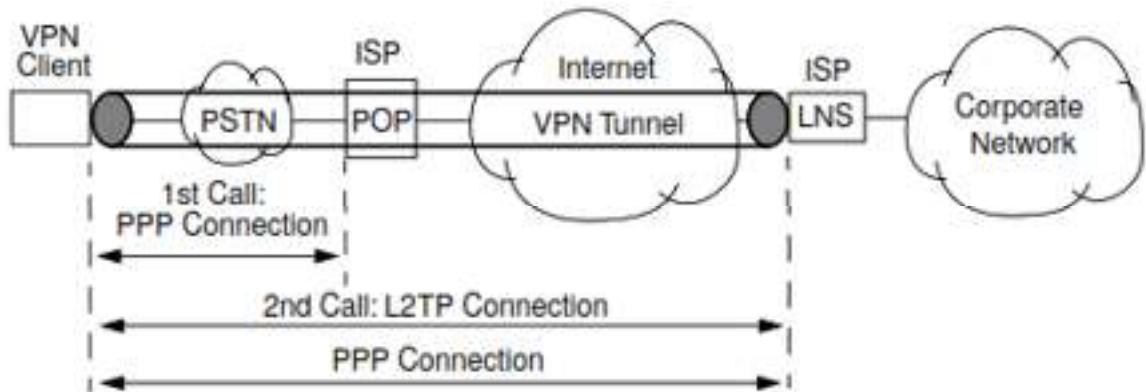
# Client-Initiated VPN

## LNS

- The LNS is located within the ISP network
- The LNS authenticates the client and establishes the VPN tunnel, securely forwarding client traffic to the corporate network
- The LNS serves as the endpoint for the L2TP tunnel, managing the secure transmission of data between the VPN client and the corporate network

## Corporate Network

- The destination network that the VPN client aims to access securely

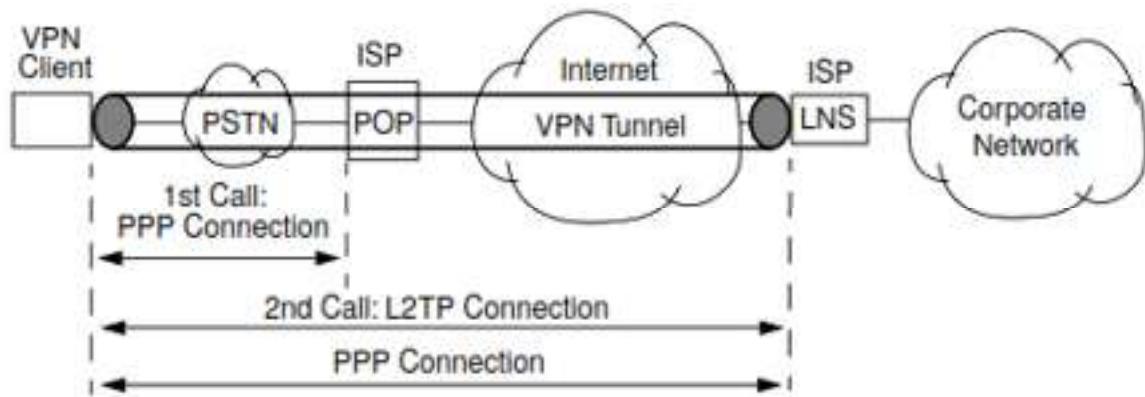


# Key Features of Setup

**VPN Server in ISP Network:** This configuration places the VPN server within the ISP network

**Two-Step Connection:** The client establishes a PPP connection to the ISP's POP and then a secondary L2TP connection to the LNS to set up a VPN tunnel

**Flexible and Managed by ISP:** The ISP controls both the internet access and the VPN service, which can simplify management and provide better service integration



# Summary of Client- Initiated VPN

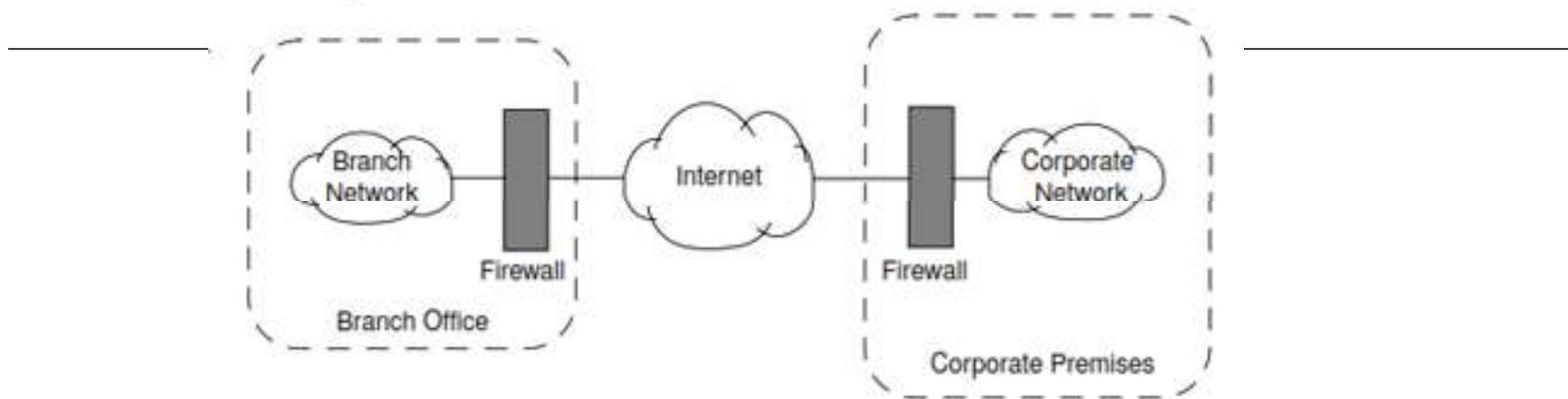
**Client-Initiated VPN Model:** The VPN client is responsible for initiating and managing the VPN connection

## Two Variants

- **VPN Server in ISP Network:** Managed by the ISP, this variant can offer simplified management for clients but provides less control for the corporate network
- **VPN Server in Corporate Network:** Offers enhanced security and direct control by the corporate network but requires the organization to manage the VPN infrastructure

**Two-Step Process:** Both variants involve the client first establishing a PPP connection to the ISP's POP and then a secondary L2TP connection to the VPN server

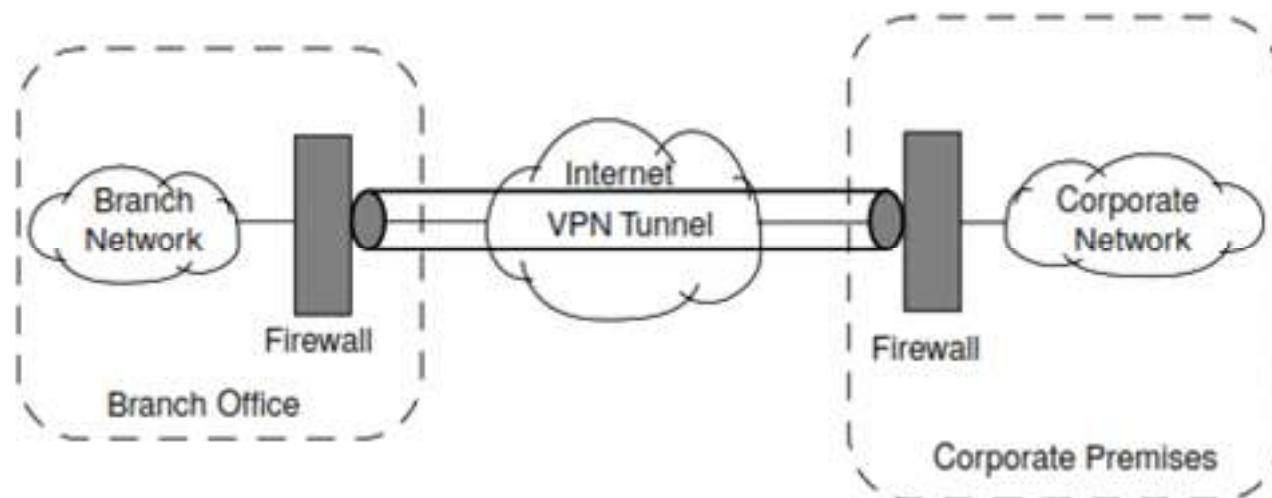
# Firewalls and VPNs: Integration



**Firewalls providing authorized access to two networks.**

# Firewalls and VPNs: Integration

---



**VPN tunnel between two firewalls.**

# Firewalls and VPNs: Integration

---

## **Relationship:**

- **Firewalls** control access to networks, while **VPNs** provide secure data transmission.
- **Benefits of Integration:**
  - Combining both ensures comprehensive protection by filtering unwanted traffic and encrypting sensitive data.

## **Example:**

- A company sets up firewalls at multiple sites and establishes encrypted VPN tunnels between them to secure data transmission.
- **Diagram:** Show a VPN tunnel between two firewalls, illustrating protected communication.

# Conclusion

---

- **Summary:**

- Firewalls protect networks by controlling access and filtering traffic.
- VPNs secure communication over public networks by encrypting data.
- Combining both technologies provides robust security for organizations against external threats.

- **Key Takeaway:**

- Organizations need both firewalls and VPNs to ensure comprehensive network security and data protection.