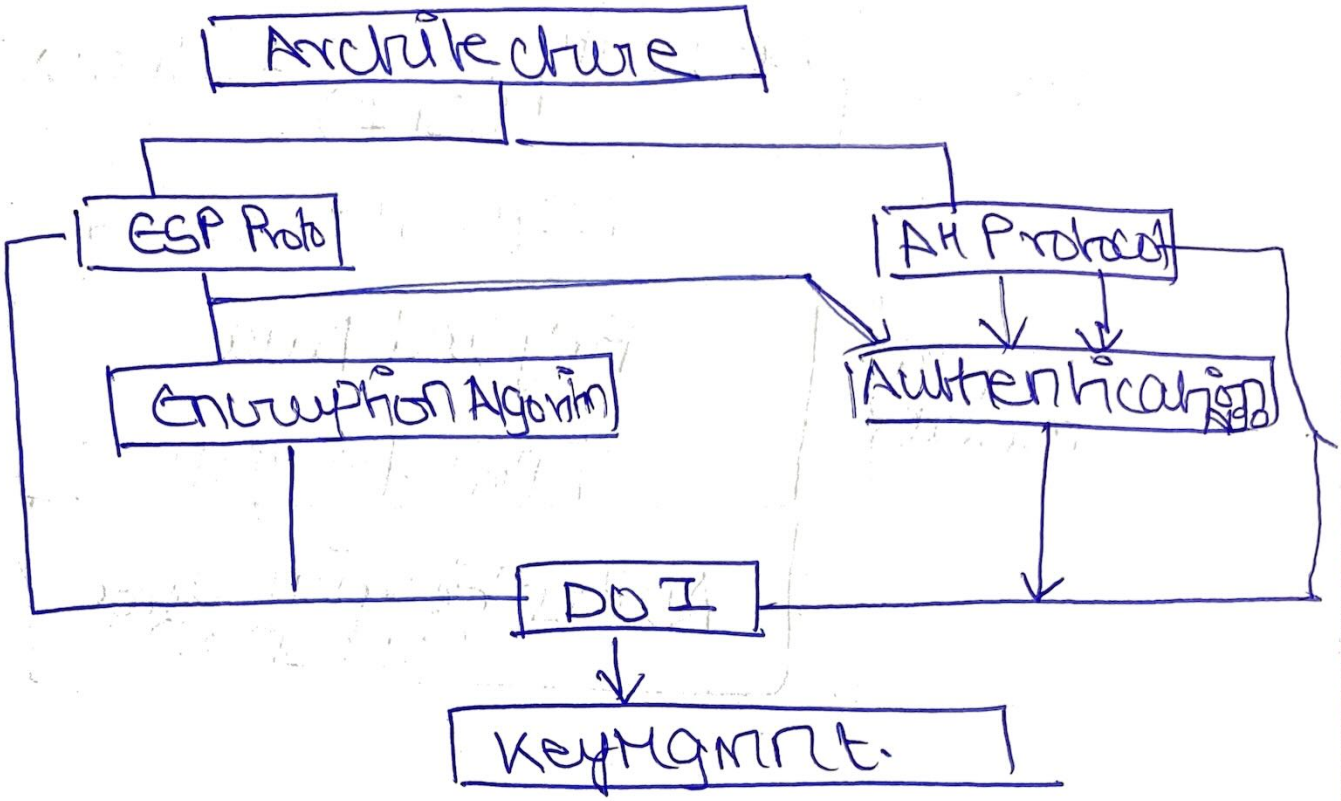
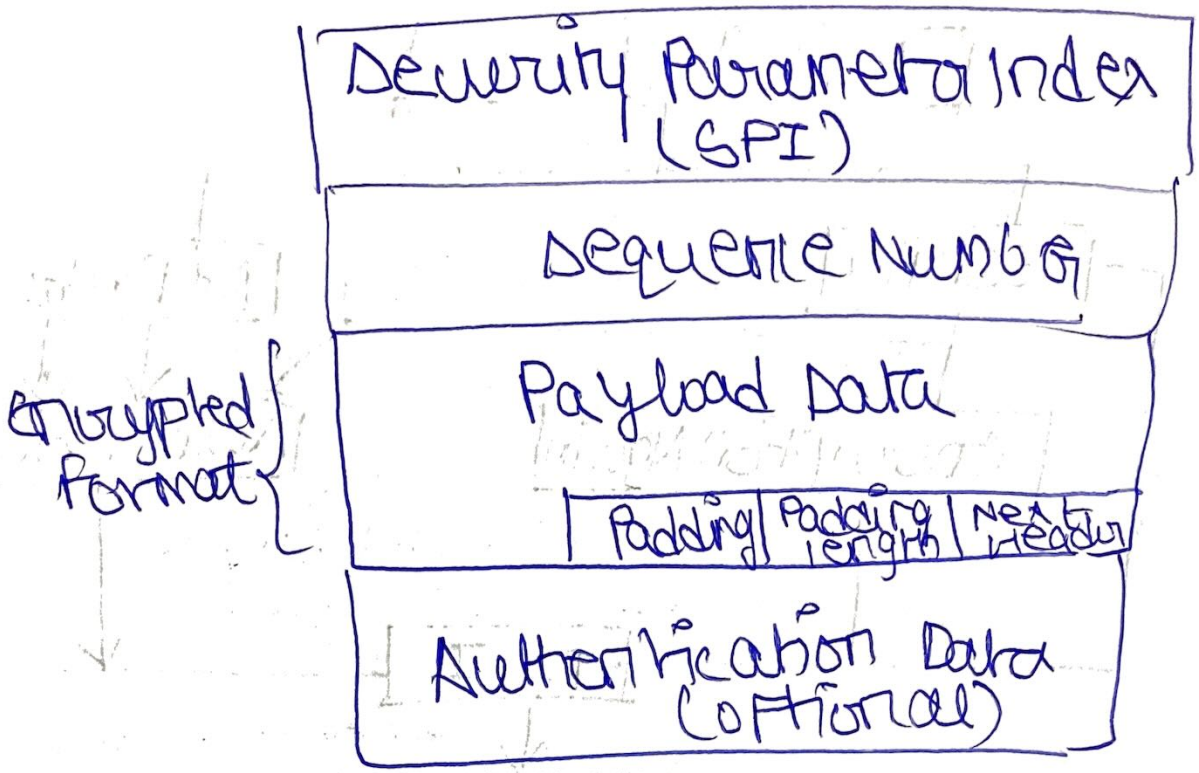
IP Security Architecture



→ It covers the general concept protocols, definitions, algorithms & sec requirments of IP technology

→ ESP Protocol.
These are ~~the~~ implemented in two ways.
1) ESP with optional authentication
2) ESP with Authentication.


Security Parameter Index (SPI)
Sequence Number
Payload Data
Padding
Padding length
Next Header
Encrypted Format
Authentication Data (optional)

Network Security (Unit -II)

Syllabus

- → IP sec. , Protocols of IP sec.
- → SA and its Parameter (Transport and Tunnel Mode)
- → IPV4 and IPV6 header
- → AH and ESP
- → IKE

→ **IP Sec** :- The communication between two entities over on IP network (sender and a receiver) is protected by this Internet Protocol security.

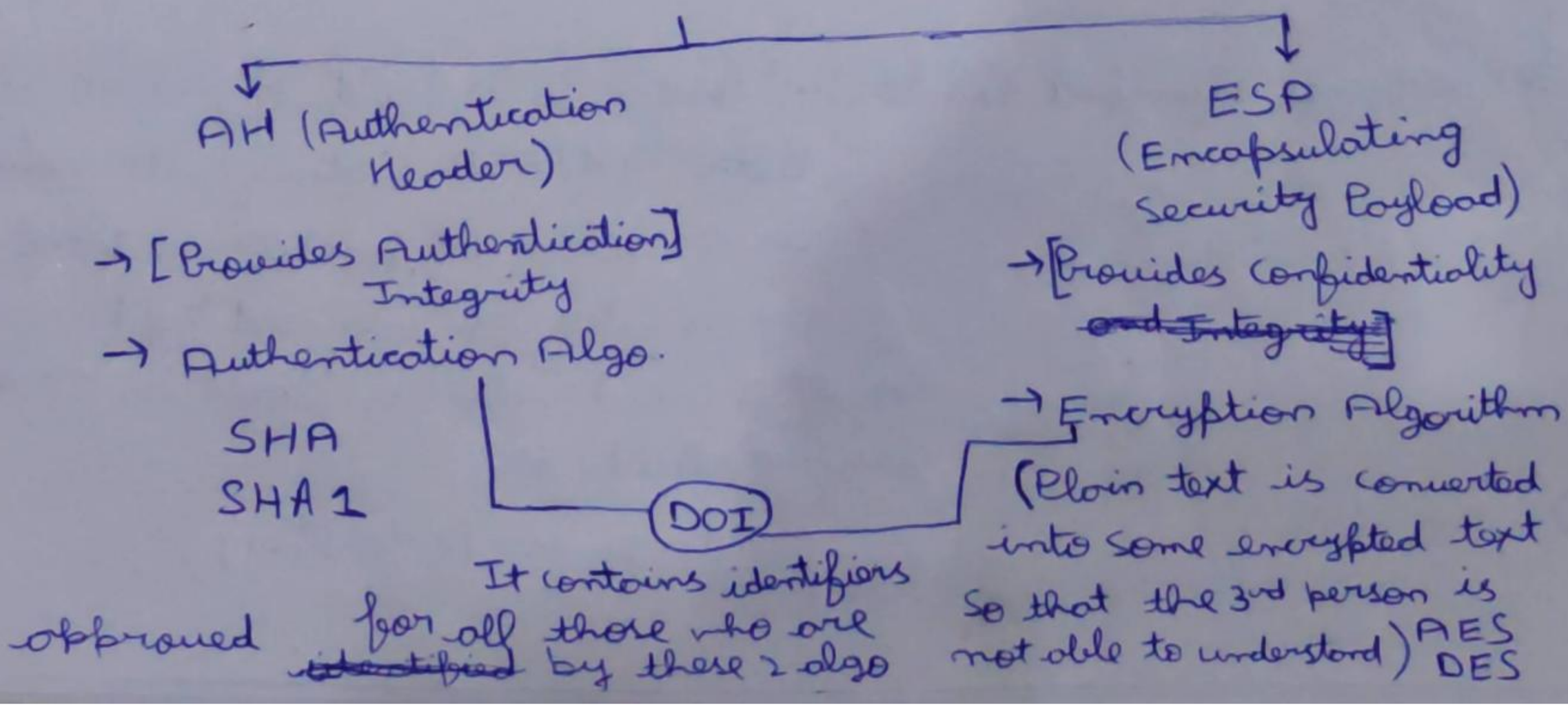
It provides security in three terms

1.) Authenticity 2.) Confedendiatility

3.) Integrity

Structure and Protocols of IP sec.

IP sec. basically has two protocols



Key Management

IP sec. (Manual)

IKE Protocol (Automated)

→ SA :- Security Association, it is a kind of relationship or (contract which is shared with every entities (Sender and receiver) and they have to be agree on this to start the communication.

→ The relationship describes that there is a Secure connection / communication between Sender and receiver

→ It has 3 parameters

1.) Security Parameter Index -: It is an identification parameter for SA. In between many SA's, we can uniquely identify a particular SA by using SPI

2.) Security Protocol Identifier -: To identify which protocol (AH/ESP) is implemented in the considered SA

3.) Sequence Number Counter -: There is a field of Seq. no. in both AH/ESP, initially its value is 0., when 1st packet is transferred the counter is increased by 1 and the increased value is stored in the Seq. no. field, ~~its~~

→ Range is (0 to $2^{32}-1$)

4.) AH Information 5.) ESP information

Every information related to the Authentication implementation and ESP implementation can be found in both these fields respectively (like Algorithm used, lifetime of, Size of the keys etc)
keys

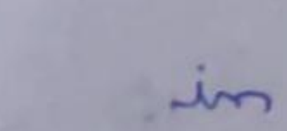
6.) Lifetime of SA :. There is a certain lifetime followed by a SA (Initiation, Generation and Termination)

→ Whenever a new SA is generated, the corresponding SPI is also generated

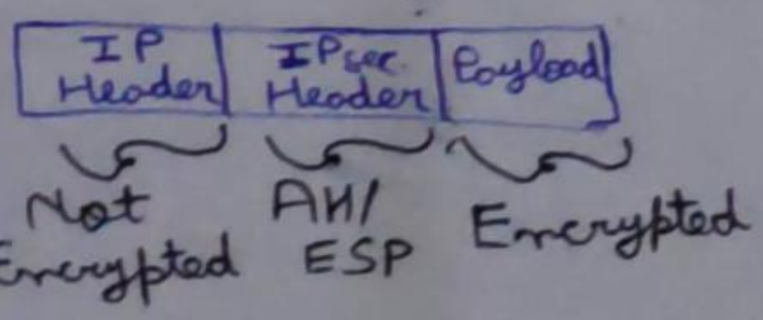
7.) IPsec. Protocol mode — Transport mode, Tunnel mode } Both IPsec protocols can be implemented in these modes

⇒ # Transport and Tunnel Mode

Transport Mode :. → only the payload is encrypted (cypher text) and not the header



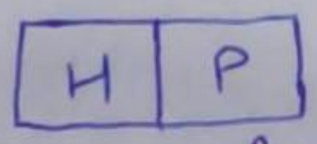
Data Packet (original)



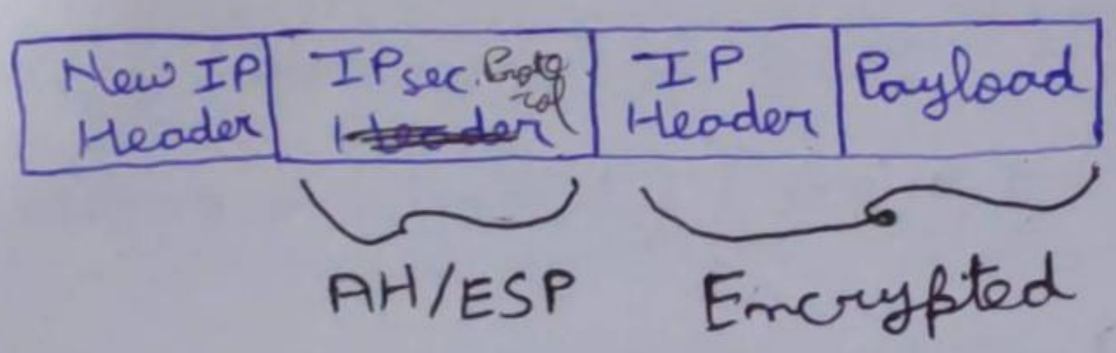
Data Packet in Transport Mode

Tunnel Mode :- → Payload as well as the IP header is encrypted

It Encrypts the IP header and inserts a New IP header for the data packet.

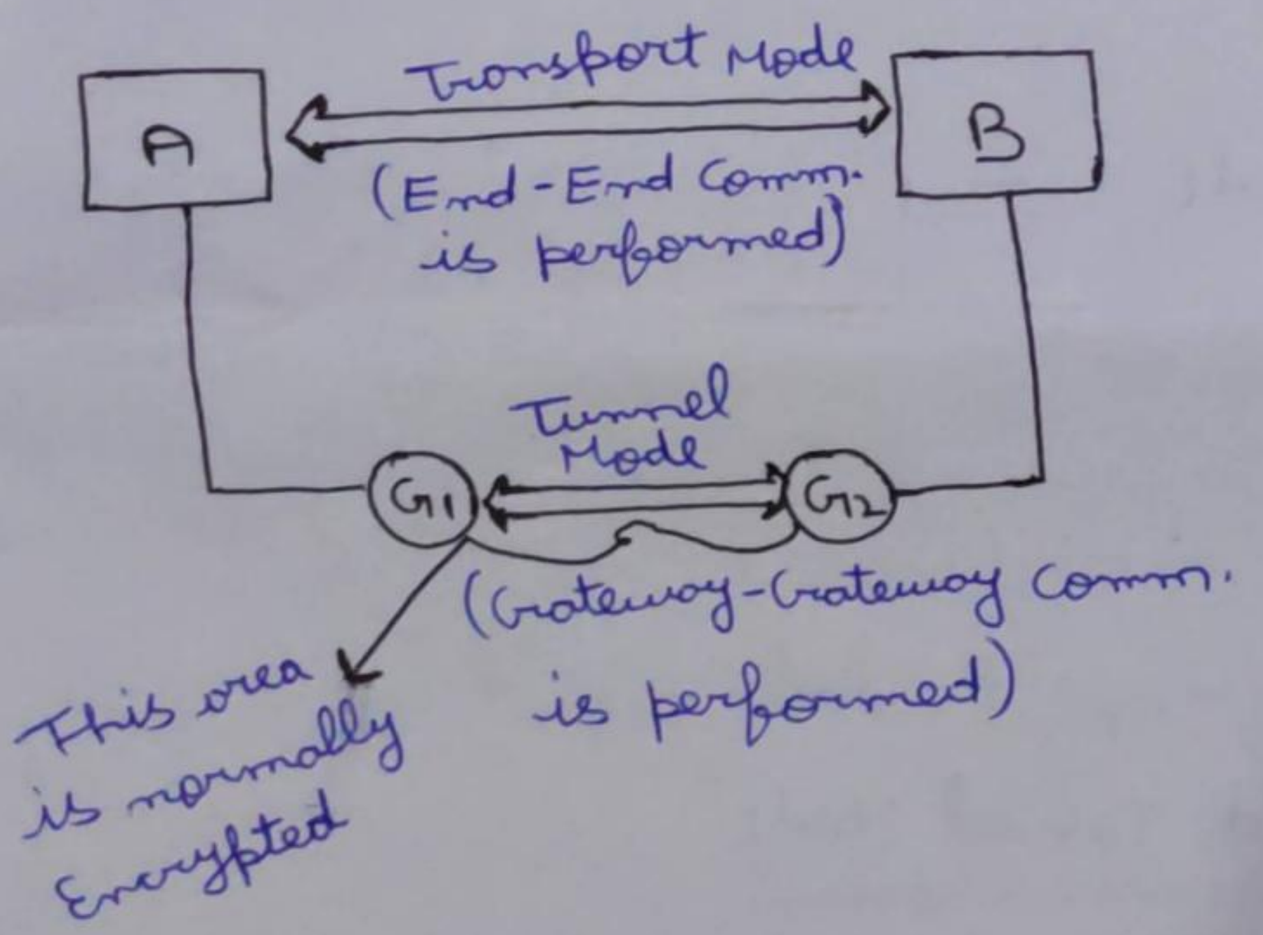


original Data Packet



Data Packet in Tunnel Mode

⇒



⇒ Transport mode is less complex than Tunnel mode.

IPv4

IP address -: A unique number which is provided to each and every devices

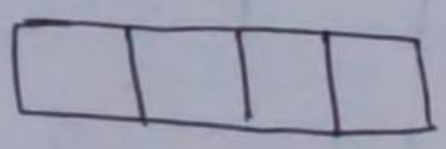
→ length of IPv4 is 32 bit

→ Around (2^{32}) unique addresses are generated

→ Range of IPv4 is 0-255

192.255.108.253

→ It has 4 octets, each of 8 bit



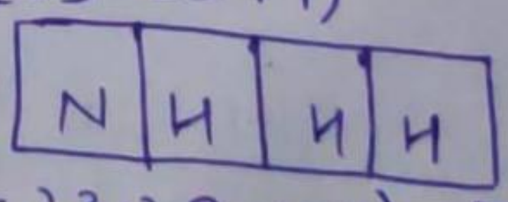
It is a

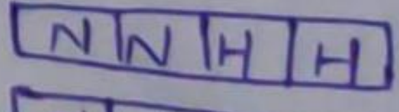
→ Numeric address seperated by (.) dot

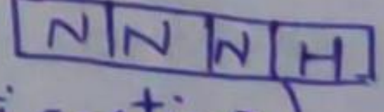
→ It has total 5 classes

Range of Classes

127.0.0.1 ← local server	Class A	0-126	(125.255.23.17)
NID → 1	Class B	128-191	(191.23.28.144)
HID → 0	Class C	192-222	(192.204.18.114)
NID → (1)	Class D	223-239	(Used For Multicasting)
HID → (0)	Class E	240-255	(Used for Research)







[To find the class, we always check at the first octet]

→ IPv6

→ length of IPv6 is 128 bit

→ Around (2^{128}) unique addresses are generated

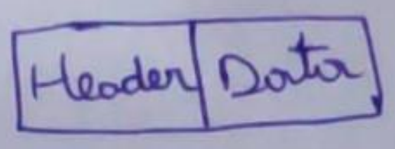
(This is the reason why IPv6 come because the no of unique IP addresses generated in IPv4 is less)

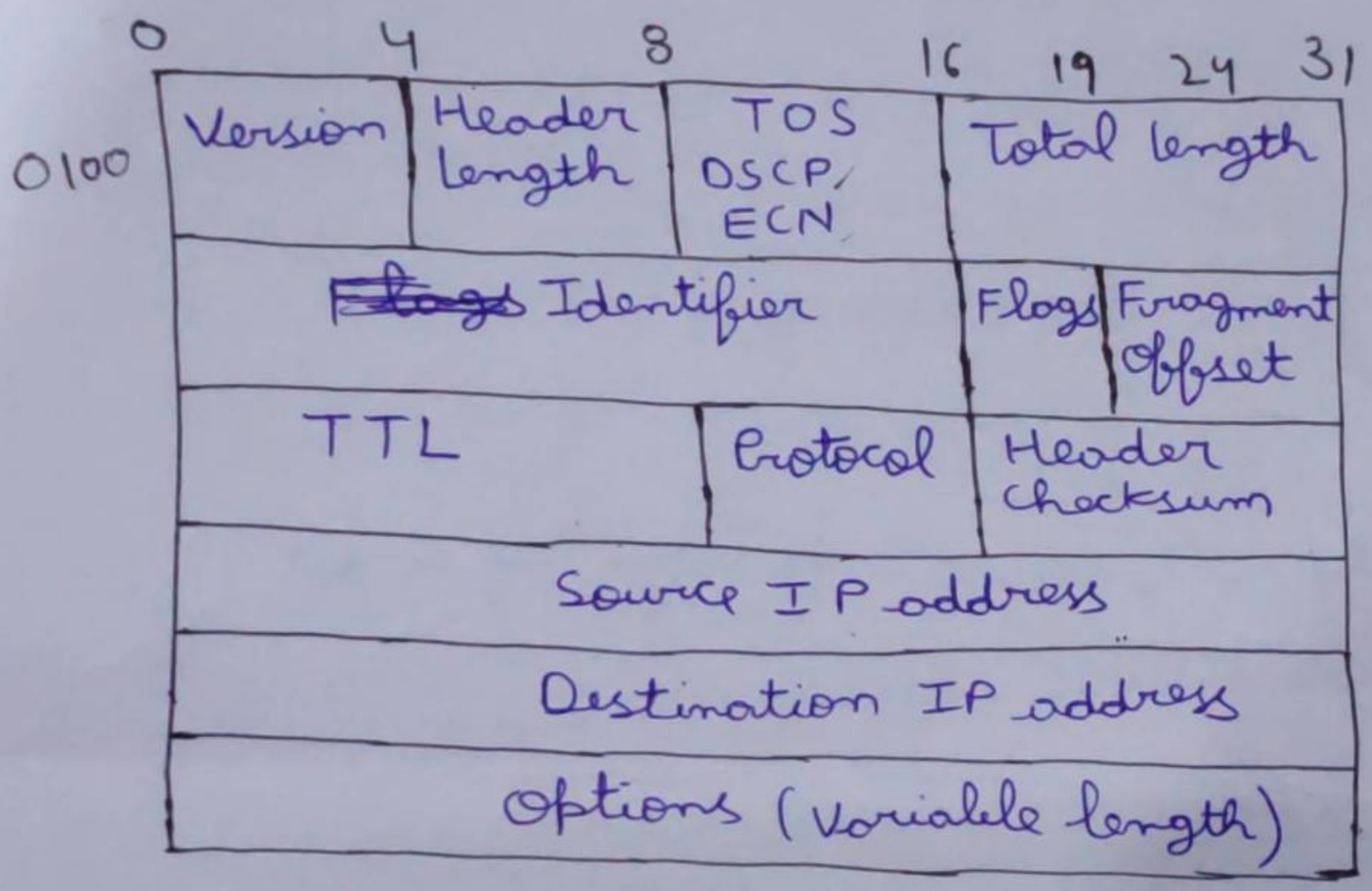
→ Range of IPv6 is 0-FFFF (65535)

→ It is a alphanumeric number seperated by colon (Both number and Hexadecimal)

→ It does not have any class

=> IPv4 Header





: Version - This 4 bit field defines the version of IP used (IPv4 or IPv6), so whenever the receiver receives a packet first thing they know is the version

: Header length - This 4 bit field defines the length of entire IP header and once the packet is received succesfully, the header is removed

: TOS :- This is a 8 bit field in which first 3 bit is called Precedence and next 4 is called TOS bits, last bit is not used. Divided into two types:

DSCP, Differentiated Services Code Point, is a type of service

ECN, Explicit Congestion Notification, Carries info about congestion seen in the route, it doesn't drop the packet, just sends notification to sender for control

: Total length - This 16 bit field defines the total length (IP Header + Payload) of the IPv4 datagram in bytes

: Identifier - This 16 bit field is used to break the packet (fragmentation)

: Flags - This is a 3 bit field. 1st bit is reserved, 2nd bit is called DF (Don't fragment), 3rd bit is MF (More Fragment)
If Data packet is too large, these flags tells if they can be fragmented or not

: Fragment Offset - This 13 bit field compares both sender and receiver, tells exact position of the broke packet and checks that it is original packet or not.

: TTL (Time to live) - This 8 bit field avoids looping in the network.

This 8 bit field
: Protocol - Tells the network layer and the destination host to which packet protocol does the packet belongs to.

: Header Checksum - This 16 bit field maintains header integrity, used for error detection in packet

: Source IP address - This 32 bit field tells the IP address of the source

: Destination IP address - This 32 bit field tells the IP address of the destination

: Optional (Padding) - This field is used to send the extra data with header other than original packet.

⇒ IPv6 Header format (More refined than IPv4 header)

Version (4)	Priority (8)	Flow label (20)
Payload length (16)	Next Header (8)	Hop limit (8)
Source Address (128)		
Destination Address (128)		

Base Header = 40 Bytes (Fixed)

1 Byte = 8 bits

Extension Headers:
i) Routing Header (43)
ii) Hop by Hop option (0)
iii) Fragment Header (44)
iv) Authentication Header (51)
v) Dest options (60)
vi) ESP (50)

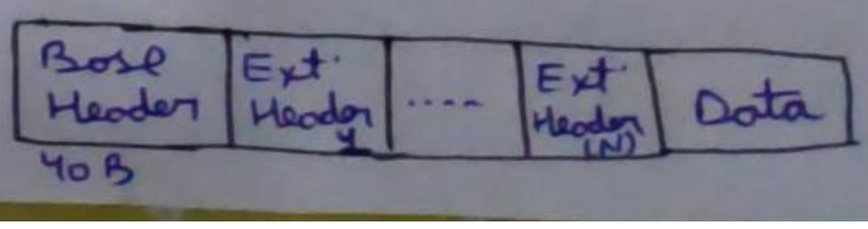
: Version - The value of this 4 bit field is 0110 (hence it will used, to know that packet is of IPv6)

: Priority - This 8 bit field is also known as Traffic Class, controls the congestion when congestion occurs; Sender can set a priority for the packet [lower priority packet can be dropped and Higher priority can be send forward]

: Flow label - This 20 bit field is used for Real time data processing (no delay and min. loss of data), so to achieve this at this field converts datagram services into virtual circuits which means all the packets (having flow label bits) will follow only a single path.

: Payload length - This 16 bit field is used to send ~~extra~~ Jumbo data -grams (upto 4GB) with the help of ext. header [HOP by HOP opt.]

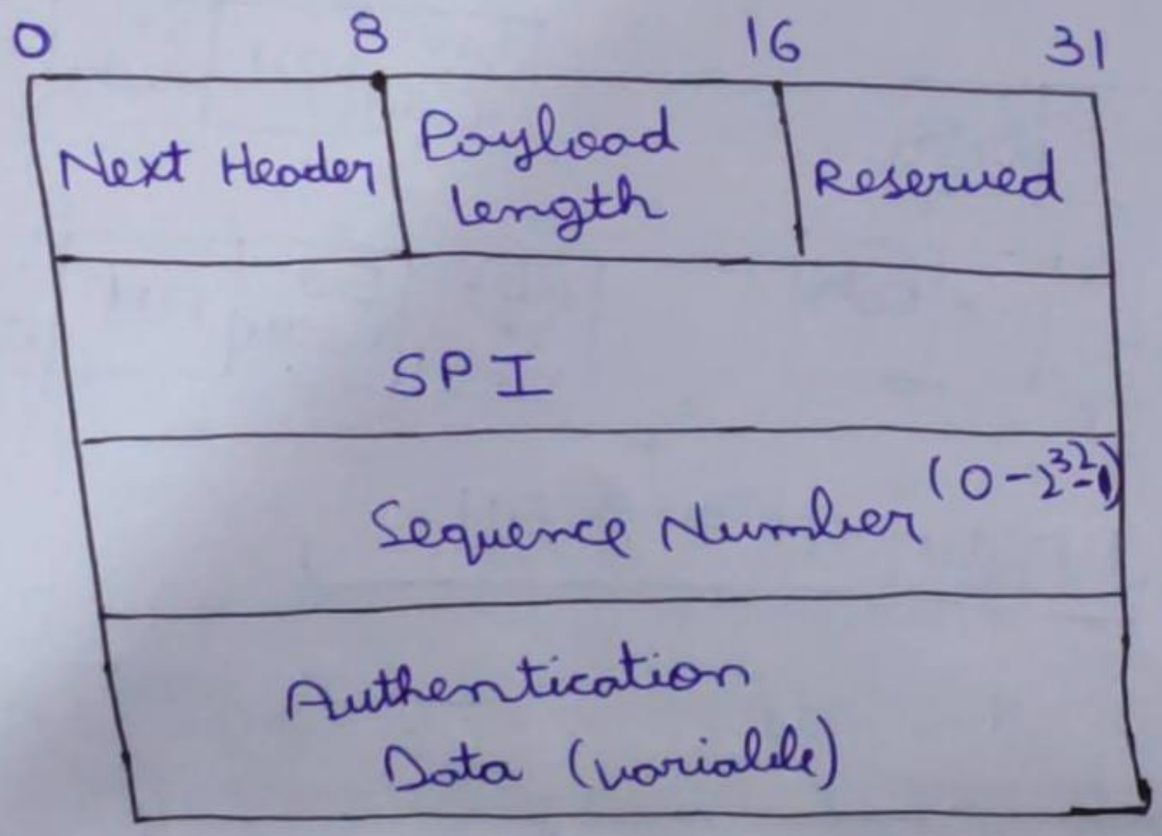
: Next header - This 8 bit field basically contains all the extension headers



: Hop limit - This 8 bit field is same as TTL, maintains Congestion

: Source Address, Dest Address - IP addresses of the source and destination (both are of 32 bit)

⇒ AH :



: Next Header - This 8 bit field tells about the type of header immediately following the current header

: Payload length - This 8 bit field tells the length of original data

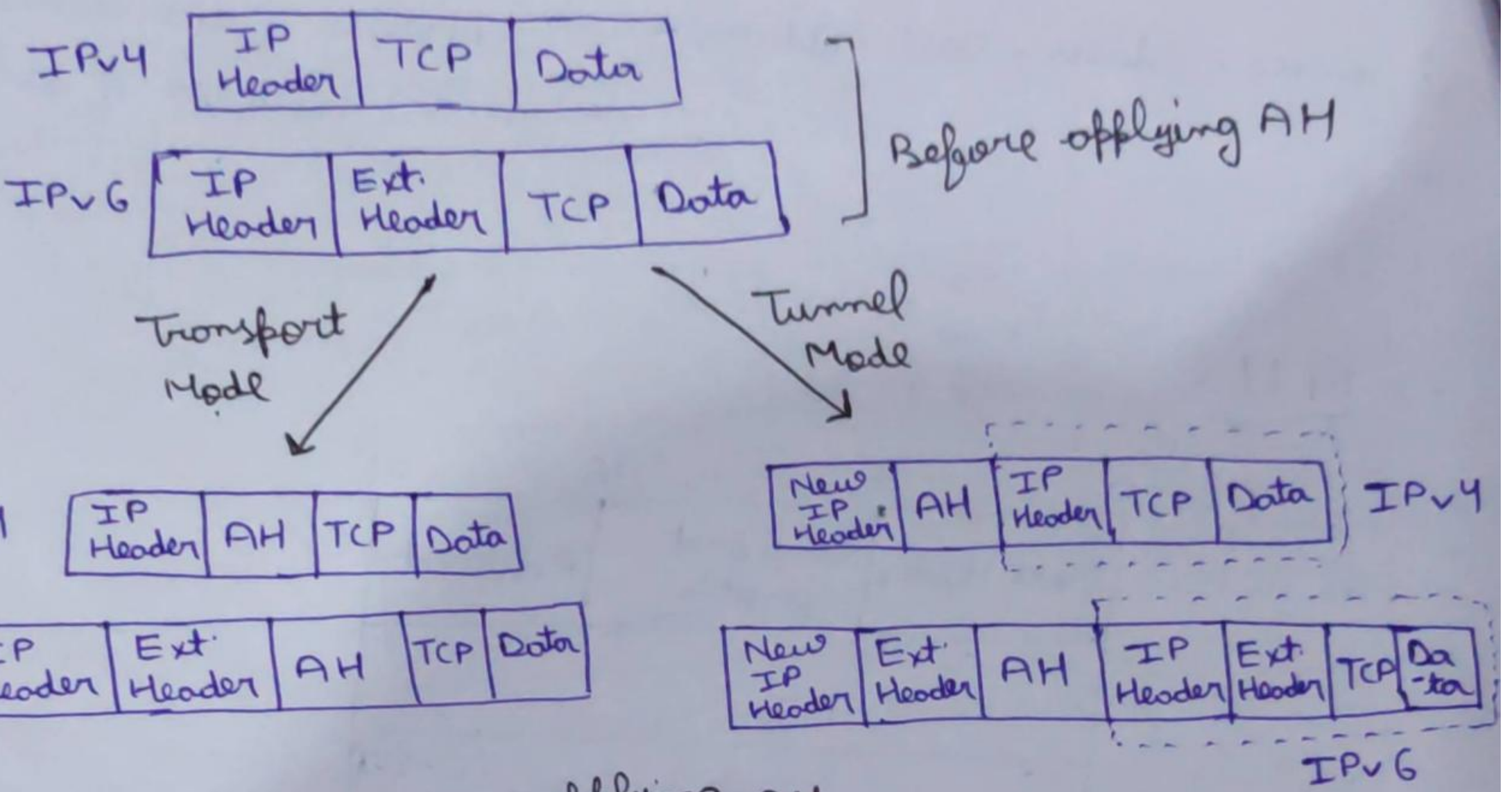
: Reserved - It is for the future use (contains reserved fields)

: SPI - To identify that particular SA to which the packet belongs

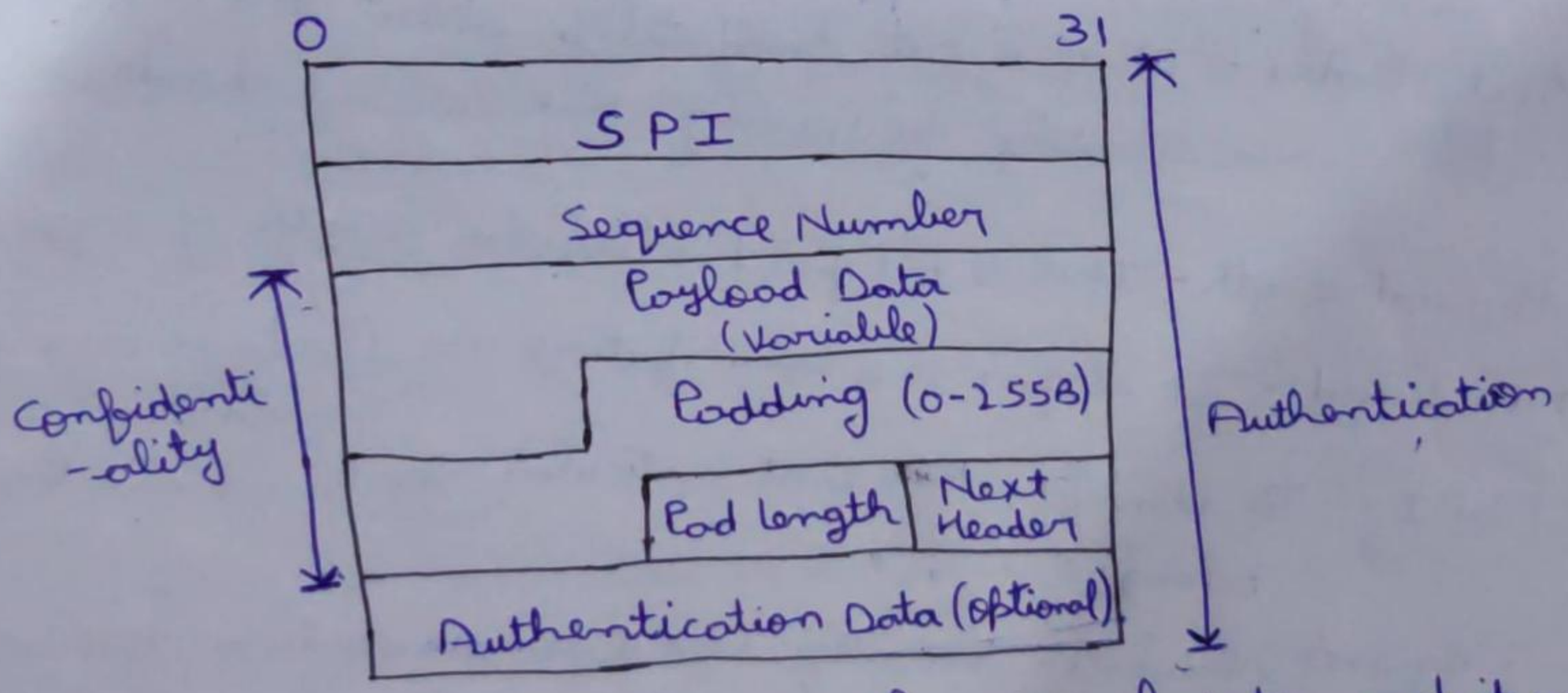
: Sequence Number - Initially before communication, the value of the field is 0, as the comm. starts counter increases the value of field by 1.

: Authentication Data - It contains ICV (Integrity Check value) It is a variable length field, determines whether undesirable modifications to our data is made or not

⇒ Mode of operation in AH :



→ ESP -:



: Payload data - It the normal original data and it will be encrypted before sending

: Padding - This field provides extra bytes (if necessary) to the plain text so that it can be encrypted further

Ex:- Plain Text 62 B

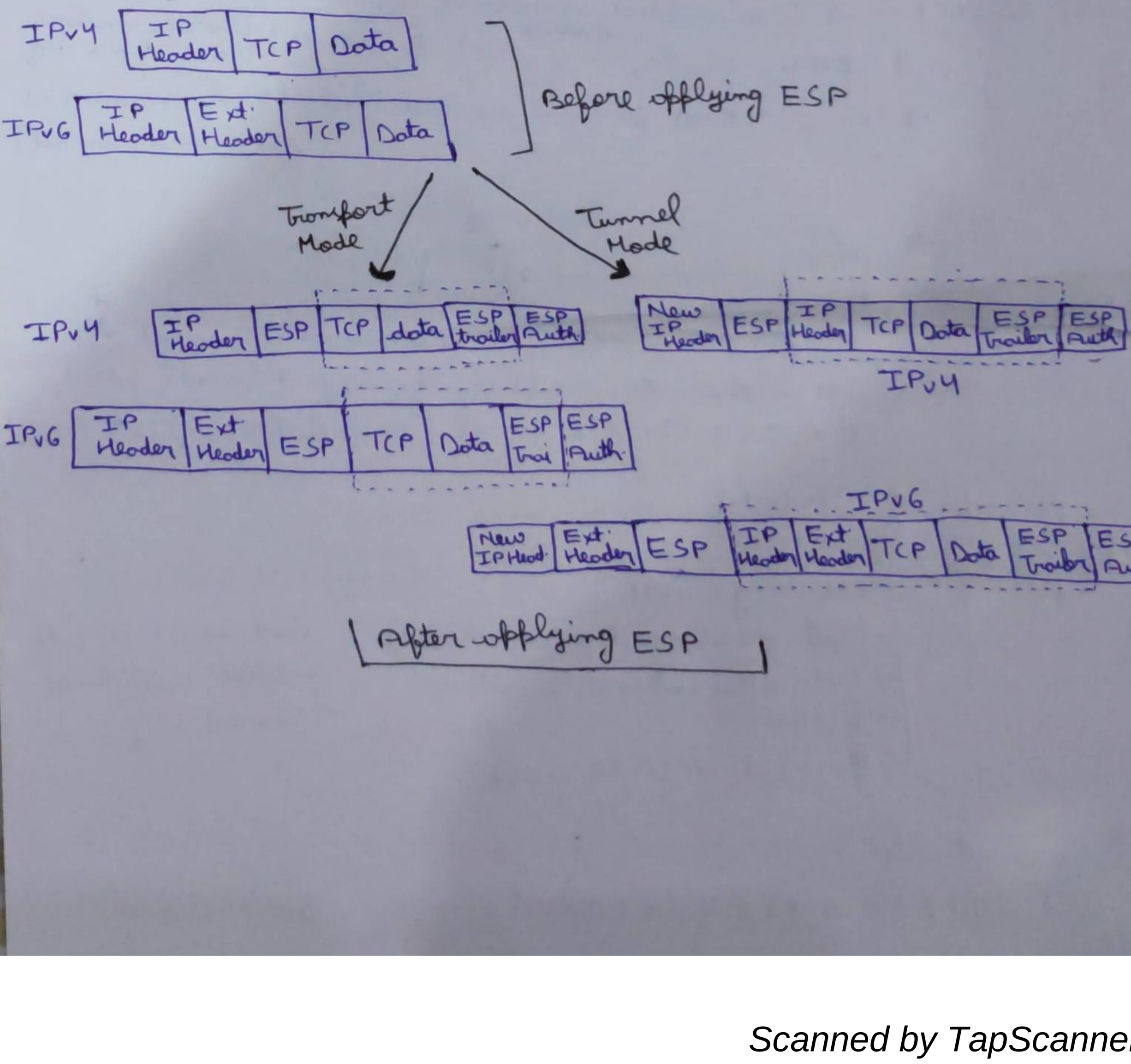
(But we need 64 byte for the algo. so the extra 2B will be padded from that

: Pad length - It tells how much bytes is used for the padding purpose

: Next header - This field is used to identify the type of data in the payload data field

: Authentication Data - Some as AH, just the difference is that this field ~~is~~ is optional in ESP

=> Mode of operation in ESP :



IKE :- . Internet Key Exchange is a secure key management protocol

- Keys ensures security and are managed by IKE
- Before protecting any IP packets, we need to build an IPsec tunnel which can be established using a protocol IKE

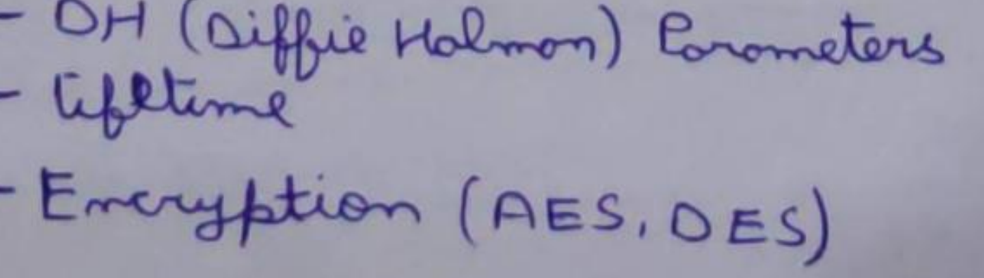
- It has two phases

  Phase 1 (Main Mode / Aggressive Mode)

  Phase 2 (Quick Mode)

⇒ Phase 1 : → Two entities negotiate about the encryption and other protocols ~~and other~~ they want to use and other parameters (SA) that are req.

→ An ISAKMP session is established (also known as IKE Phase 1 tunnel)



→ This tunnel is used ~~as~~ as a secure method to establish the second tunnel called the IKE Phase 2 tunnel [Main Purpose of IKE Phase 1]

3 steps of Phase 1.

① Negotiation
- Hashing (SHA)
- Authentication (Pre-shared Keys)
- DH (Diffie Hellman) Parameters
- Lifetime
- Encryption (AES, DES)

② DH Exchange

End result is both entities will have a shared key

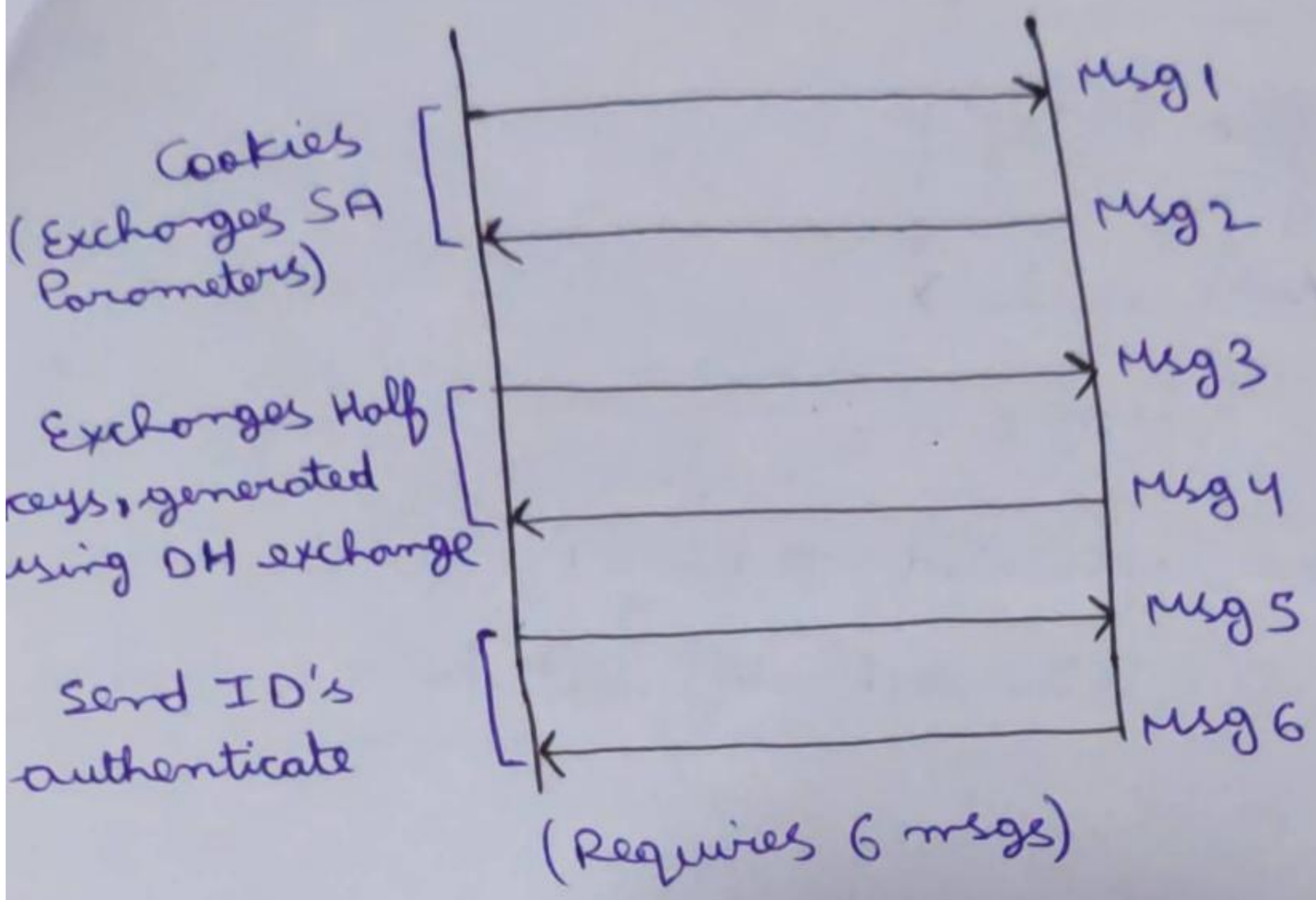
③ Authentication

End result is a IKE Phase 1 tunnel which is bidirectional

→ Uses two modes

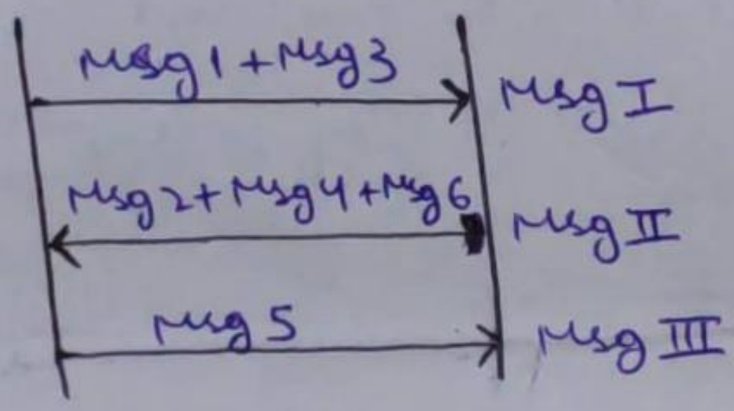
Main Mode (More Secure) | Aggressive Mode

=> Main Mode



(Requires 6 msgs)

Aggressive Mode



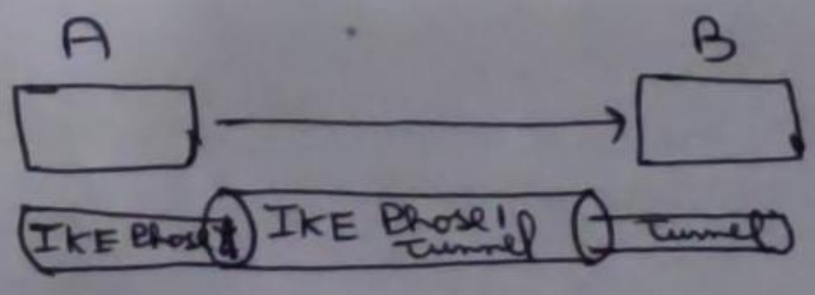
(Requires 3 msgs), Comprissed ver. of Main Mode

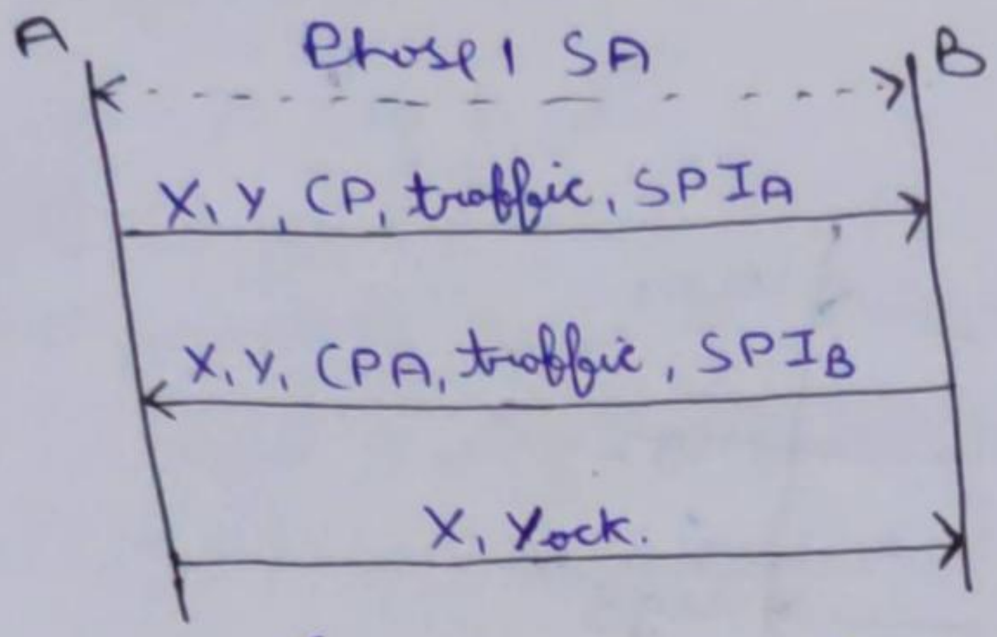
Whatever mode & Phase 1 use, they use for different Auth. Methods

- Original Public key Encryption
- Revised " " "
- Public key Signature
- Pre-stored keys

4 Methods X 2 Modes = 8 Variants of Phase 1

=> Phase 2: → Once IKE phase 1 is completed, we have an IKE Phase 2 tunnel that we can use to protect our data





(Requires 3 Msgs)

X = Pair of cookies generated in Phase 1

Y = 32 bit no. to distinguish different phase 2 sessions

CP = Crypto Proposal

CPA = Crypto Proposal accepted

"X and Y are in clear rest of phase 2, messages are encrypted and integrity protected"

ack = Acknowledgement of prev. msg.