24/9/2019

Key Management of PGP :-

PGP uses 4 keys :-

i) one-time session symmetric keys
ii) Public keys
iii) private keys
iv) passphrase based symmetric keys

- Public-key consists of its own id :- atleast 64 bits (least significant) acts as id.

Key Rings :-

- It is table format to kept all private keys. → private key ring

fields in private key ring :-

Timestamp - when it is created (Date & time)

key ID - least significant 64 bits ($KU_i \bmod 2^{64}$)

Encrypted private key is stored.

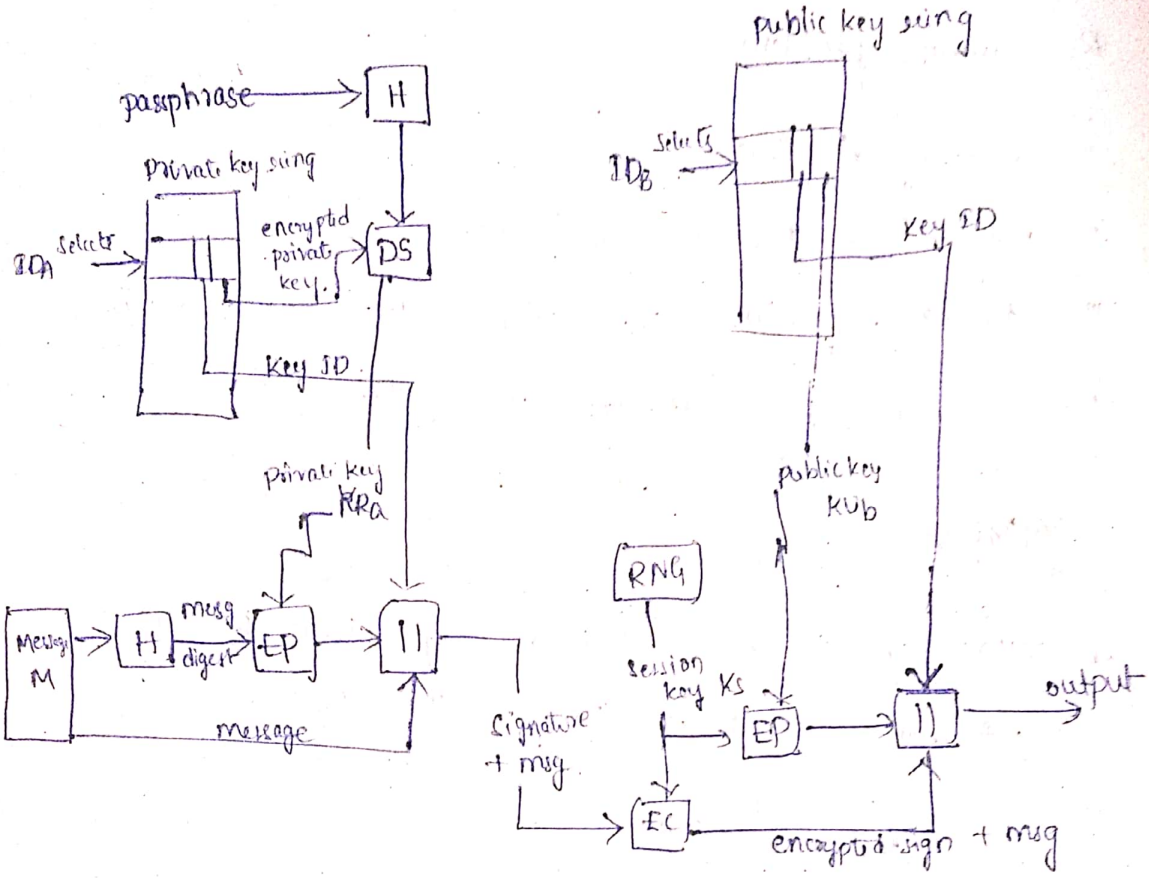
↳ to decrypt, passphrase (private key) key is used.

- fields in public key ring :-

timestamp
key ID
Public key
owner Trust
User ID
key legitimacy
key signature
signature trust

* * * In public key ring there is ~~(none)~~ No private key.

* As every user have more than one key pairs concept of key rings came into picture.



25/9/2019

S/MIME [Secure / multipurpose internet mail extension) :-

* To prevent limitations and drawbacks of SMTP S/MIME came

Limitation of SMTP (RFC 5322):

* SMTP cannot transmit binary files.
* SMTP cannot :-
  i) transmit executable files
  ii) transmit text data that contains unicode characters or National language characters.

iii) transfer cannot a over limit

iv) It cannot handle non-textual data included in X-404 message.

* Common problems :-

i) wrapping of lines

ii) removal of trialing white space

iii) padding of lines in a msg to the same length

iv) conversation of tap into space characters.

MIME :-

* MIME consists of 5 new messages that provide information about the body of the msg.

- content - type
- content - Transfer encoding
- content - ID
- content - Discription
- content - Disposition

MIME-Version :- MIME version is 1.0.

i) content-type :- Text, image, audio, binary, video

ii) content - Transfer encoding :-

- Text — unformatted data
  — enriched (formatted data)

* 8bit :-

Short lines of ASCII

Usage :- SMTP message transfer.

* 7bit :- short but can have non-ASCII characters.

Usage :- other mail transfer context

binary :- ASCII, Non-ASCII and not necessarily short per SMTP transfer

* Usage :- other mail transfer context

base 64 :- It is mapping of 6 bit block to 8 bit block.

* Usage :- used in PGP.

quoted-printable :- Human understandable form

* Usage :- Introduce non-safe characters and reversible. line break also provided.

X-token :- Named non-standard encoding mechanism

* Usage :- Vendor specific / Application specific.

iii) Content-ID :- It is used for Identification of MIME content.

iv) content-Discription :- discription of the object with the body when you have audio kind of thing then this discription is useful to know body content indetails.

* functions of S/MIME :-

* It has 4 kinds of functions :-

i) Enveloped Data :- Encrypted content & encrypted key

ii) Signed data :- It consists of encoded msg along with signed digest data

iii) Clear-signed data :- consists of clear-text msg along with encoded signed data

iv) Signed and enveloped data :- nesting of signed and encrypted entities.

26/9/17

- Message digest generated by using SHA & Md3 Algorithm

  must – SHA

  should – Md3

- for digital signature provided algorithms: DSS, RSA

  must – DSS

  should – RSA

- Message Encryption – Algorithms:

  must – 3 DES

  should – RC 2/40

S/MIME :- Applications Table

UNIT-4

Ip Security

- Security provided at network layer level.
- Security provided to Ip packet

- First level of security :-

Here Ip Security provided security in the Internet level

- Second level of Security :-

Implementing higher level security mechanisms depending on the requirements.

Eg :- PGP, Kerboros, SSH.

- Security at application and transport layer (TLS)

In network layer, Ip security is provided. It is implemented at 1st level of security.

- Ip level security encomphasis 3 functional areas :

i) authentication
ii) confidentiality
iii) key management

Applications of Ip Security :-

- Secure the branch office over the Internet.

- secure remote access over the internet
- establishing extranet and intranet connectivity with partners.
- Enhancing electronic commerce networking. security.

Eg:- protecting credit card numbers.

Benefits of ip security :-

- provides strong security when implemented in a firewall or router that can be applied to all traffic crossing the perimeter.
- IP security is resistent to bypass if all traffic from the outside must use IP and the firewall is the only way of entrance from the internet into the organisation.
- IS is below transport layer hence, transparent to application layers.
- can be transparent to ~~app~~ end users.
- can provide security to individual users if needed.

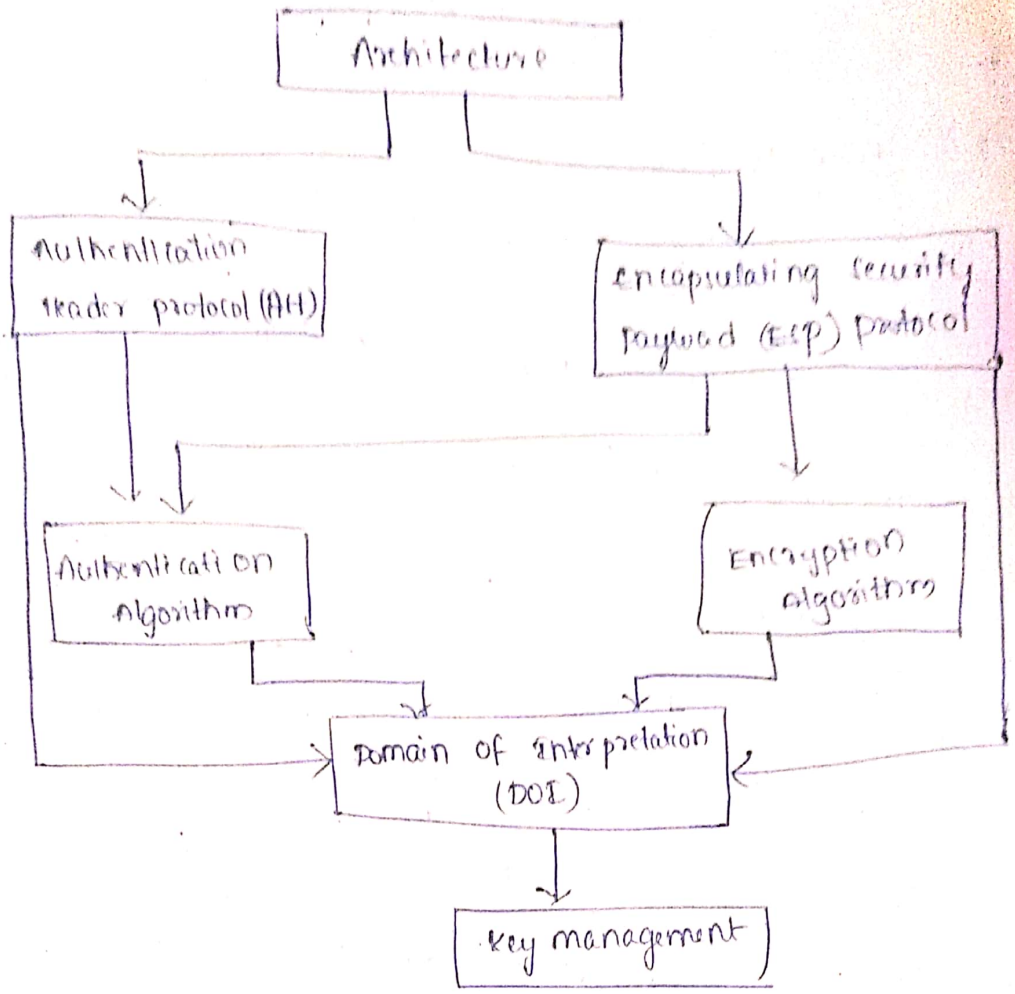
Ip Security Architecture :-

- Explain ip security protocol. (Or) Architecture of Ip security

AH → Authentication header

ESP → Encapsulating security payload

- only authentication use AH
- confidentiality and confidentiality | → ESP



27/9/2019

Authentication ~~Headers~~

This block covers the gender concepts the security ~~re~~ceivement the mechanism defining the IP security.

ESP:-

Esp header is included in the IP packet. the ESP packet is used for packet encryption and optionally for Authentication.

- The ESP uses the encryption alg then IP security provides

3> Access control

2> Rejection of replayed packets

3> confidentiality

4> Limited traffic for confidentiality.

- ESP uses encrypted alg with Authentication alg then ip security provides

  i> Access control

  ii> Rejection of replayed packet

  iii> Confidentiality

  iv> Limited traffic for confidentiality

  v> Connection less Intigrity

  vi> Data origin Authentication

Authentication Header:-

Mainly attached to ip packet for Authentication

→ AH provides

  i> Access control

  ii> connection less ontigrity

  iii> Data origin Authentictn

  iv> Rejection of replayed packet-

Encryption Alg:-

It is having set of documents that describe how various alg are used for ESP

Authentication Alg :-

→ This block is having set of documents that describe how various alg are used authentication Header optionally for ESP.

Domain of Interpretation

connected to all Documents :-

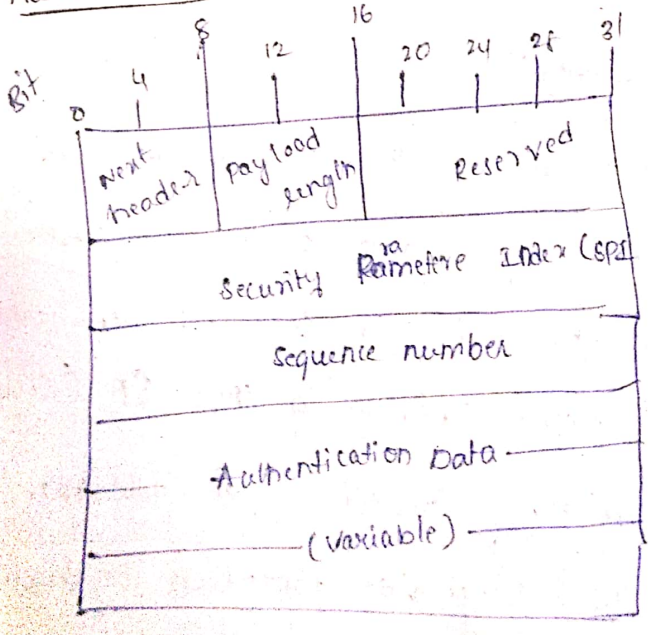
DOI consists of values which are needed to relate one document with other document these values includes the identifiers used for approving the encrypt -on and Authentication alg as well as it also includes the values representing key lifetime.

key management :-

This block describe the IKE generati keys for

21/9/19

Authentication Header :-



format of IPsec AH

Next header :- size is 8 bits. contains the protocol number of the next header after AH. used to link headers together.

Payload length :- size is 8 bits. This field measures the length of the Authentication header itself not the upper data layer (payload) length.

- It is measured in 32 bite units with 2 substracted for consistency with how header lengths are normally calculated in IPV6.
- The default length of the Authentication data field is 96 bits or three 32-bit words.

Reserved :- size is 16 bits. Reserved for further use.

Security parameter Index (SPI) :-

- SPI length is 32 bits. A 32-bit value that when combined with the destination address and security protocol type and identifies the security associations to be used for this diagram.

Sequence number :-

- length is 32 bit. This is a counter field that is initialized to '0', when a security association is formed between two devices and then incremented for each datagram sent using that SA (Security Assoc^{n}) This uniquely identifies each datagram on an SA and it used to provide protection against replay attack by preventing the retransmission of captured datagram.

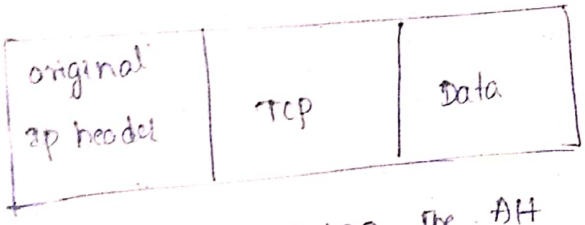
* protocol

Authentication Data :-

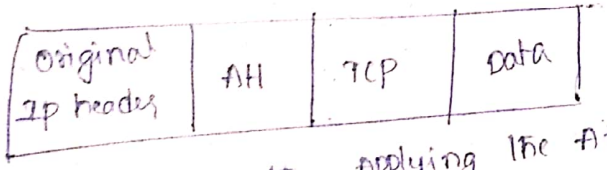
- Size is variable.
- This field contains the result of the hashing algorithm performed by AH algorithm. The integrity check value (i.e. authenticated code for the trusted version of the code).

* Transport and Tunnel modes of AH protocol :-

1) AH with transport mode :-



Before applying the AH

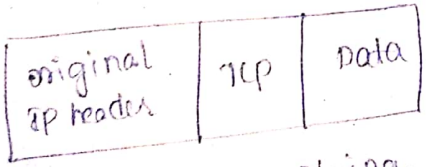


After applying the AH.

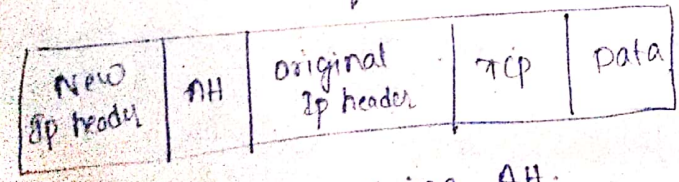
- AH is presents after ip header and before TCP.

2) AH with tunnel mode :-

- AH is added before the entire packet - so, to identify the packet, new IP header field added extra.



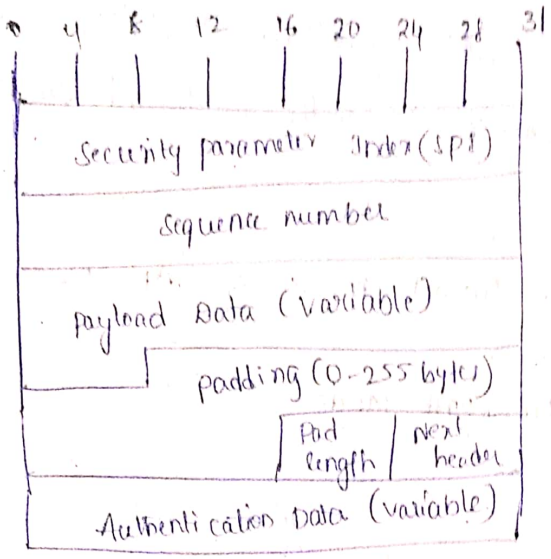
Before applying the AH



After applying AH.

9/10/2019

ESP Packet format :-



* Security parameter Index (SPI) :-
  - 32 - bit length
  - It combines destination address & IP security protocol to identify the security association.

* Sequence number :-
  - length - 32 - bit
  - main purpose - provide anti-replay attack.
  - It is a counter value. Initially '0'.

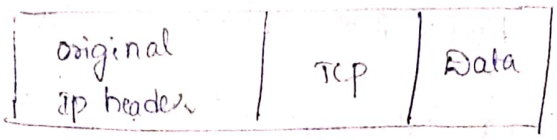
* payload Data :-
  - It is variables. minimum size 255 bytes. If it is less than this then append nbr of bytes

Next header :-
- Next header is used to build the connectivity from one header to another.

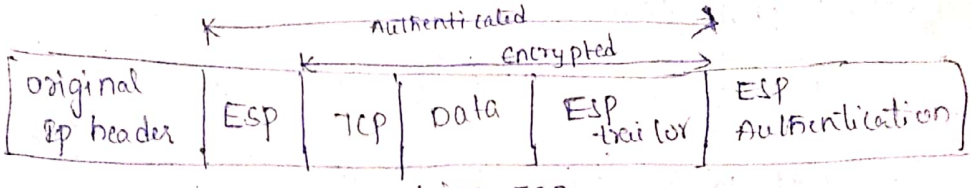
i) ESP
ii) Esp trailer
iii) Esp Authentication } these will be added at end of IP data packet

* Transport and tunnel modes of ESP protocol :-

Esp Transport mode :-

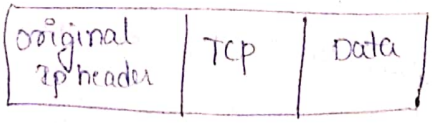


Before applying ESP

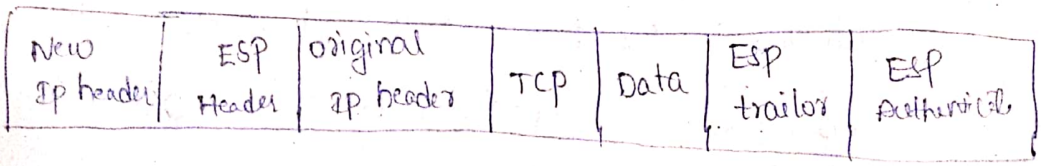


After applying ESP

Esp with tunnel mode :-



Before applying ESP



After applying ESP

Security Association selectors :-

The selectors are extracted from the network and transport layer headers. The database (SPD - security policy database) is indexed by selectors and contains the information on the security services offered to an IP packet.

* The selectors are used to filter the outgoing traffic inorder to map into a particular selector association.

* Destination ip address :-

The Destination address can be a whild card address and adress range, a network prefix or a specific host. The first 3 are used for host behind secure gateways. These are required to support more than one system sharing the same security association. The destination address field used as a selector is different from the destination address used to look up SA's (security association) in the case of tunnel ip packets.

* The Destination ip address of the outer header ~~packet~~ can be different from that of the inner header when the packets are tunneled. However, the policy in the gateway is set based on the actual destination and this address is used to index into SPD.

* User ID :-

* It is an used identifier from the operating system. This field is available if IP Security is running on the same operating system as user.

* Data sensitivity level :-

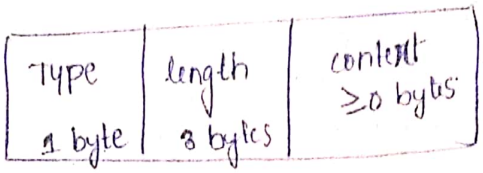
* This is used for system providing

Transport layer protocol :-

The protocol field specifies the transport protocol whenever the transport protocol is accessible. In many cases, when ESP is used the transport protocol is not accessible. Under these circumstances a wildcard is used. Transport layer protocol is obtained from IPV4 protocol or IPV6 next header field. This may be an individual number, a list of numbers.

23/10/2019

Handshake protocol



- Total 10 types of messages are there.

S.NO	TYPE	parameters
1.	Hello_request	Null
2.	client_hello	version, random session id, cipher suit compression method regarding to client
3.	Server_hello	version, random session id, cipher suit compression method
4.	Certificate	Chain of X.509 V3 certificate
5.	Server_key_exchange	parameters, signature
6.	Certificate_request	type authorities
7.	Server_done	Null
8.	certificate_verify	signature
9.	Client_key_exchange	parameters, signature
10.	finished_hash value	

Client hello:- Parameters

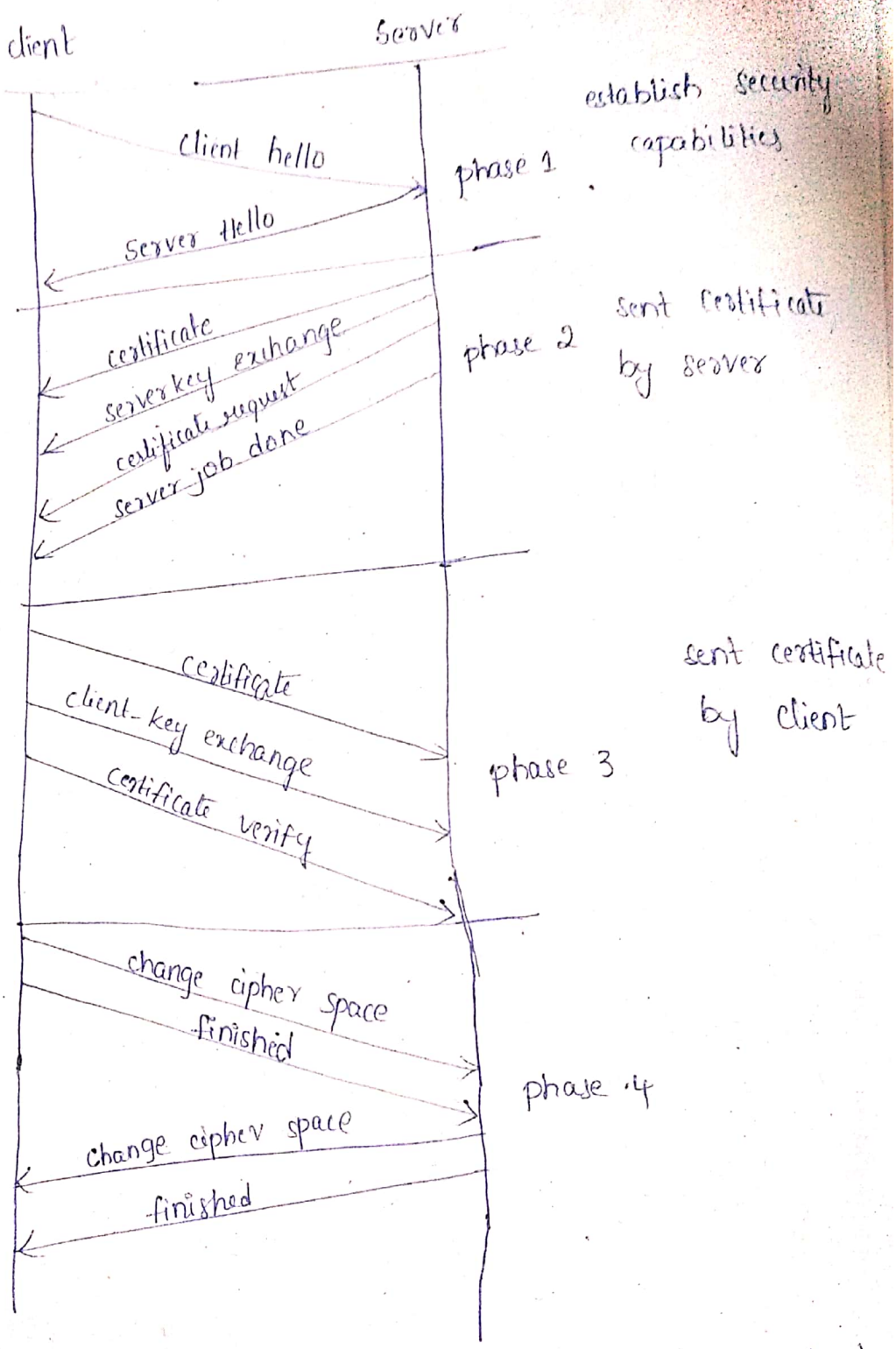
phase1:

version - define ssl → to avoid replay attack

random sessioid - 0 - indicates new connection establishment

cipher suit - what are the cipher alg are supported

- what are suitable encryption algo are supported



Phase-2:- server may send certificate (x.509 v3 certi) to client

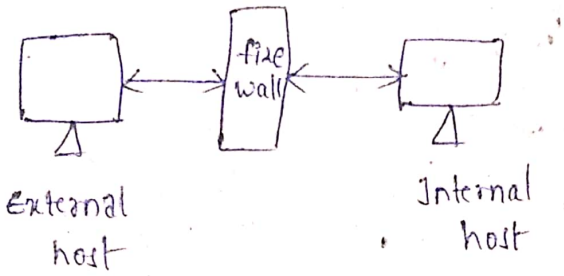
phase-3:- client send its certificate to server

phase-4:- connection is established.

30/10/2015

Firewall

- It is a Network device
- It is a software / hardware or combination of both
- It forwards / block the data



- 3 types of firewall

i) Packet filtering :-

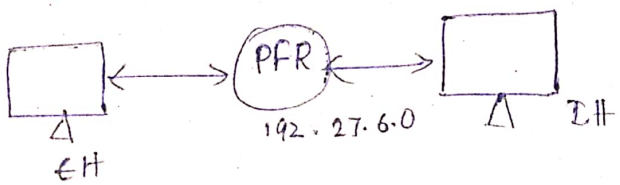
- set of rules
- rules can be framed based on SA, DA, port no, protocols.

Advantages :-

- simple

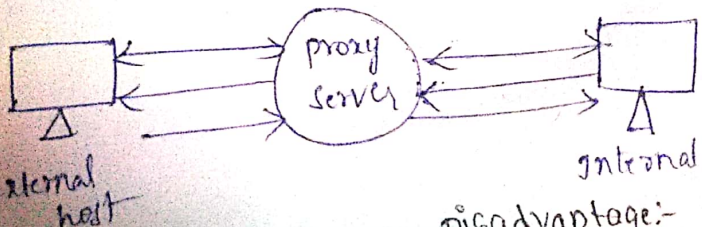
Disadvantages :-

- formation of rules is difficult
- less secure.



ii) Application level - gateway :-

- proxy server



Advantage:-

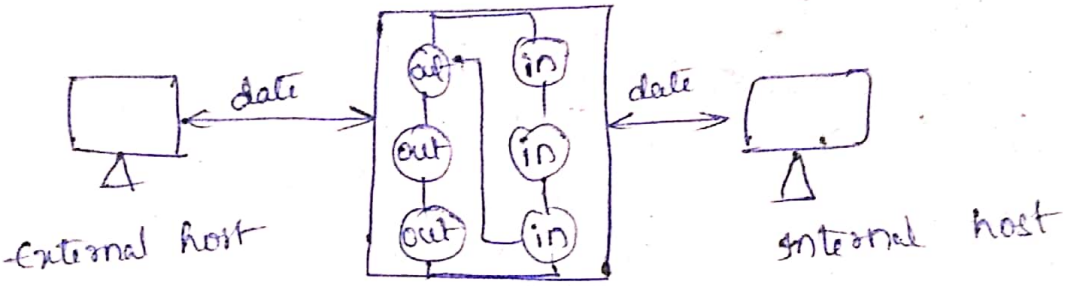
secure

Disadvantage:-

- processing is overhead.

iii) Circuit-level gateway :-

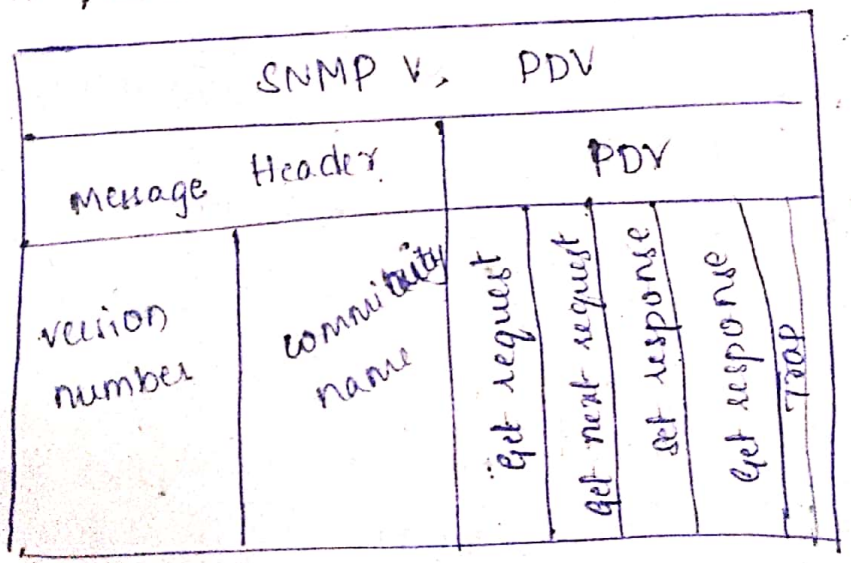
- Do not filter individual packet
- Do not permit ~~end~~ end-to-end Tcp connection
- Two Tcp connection.



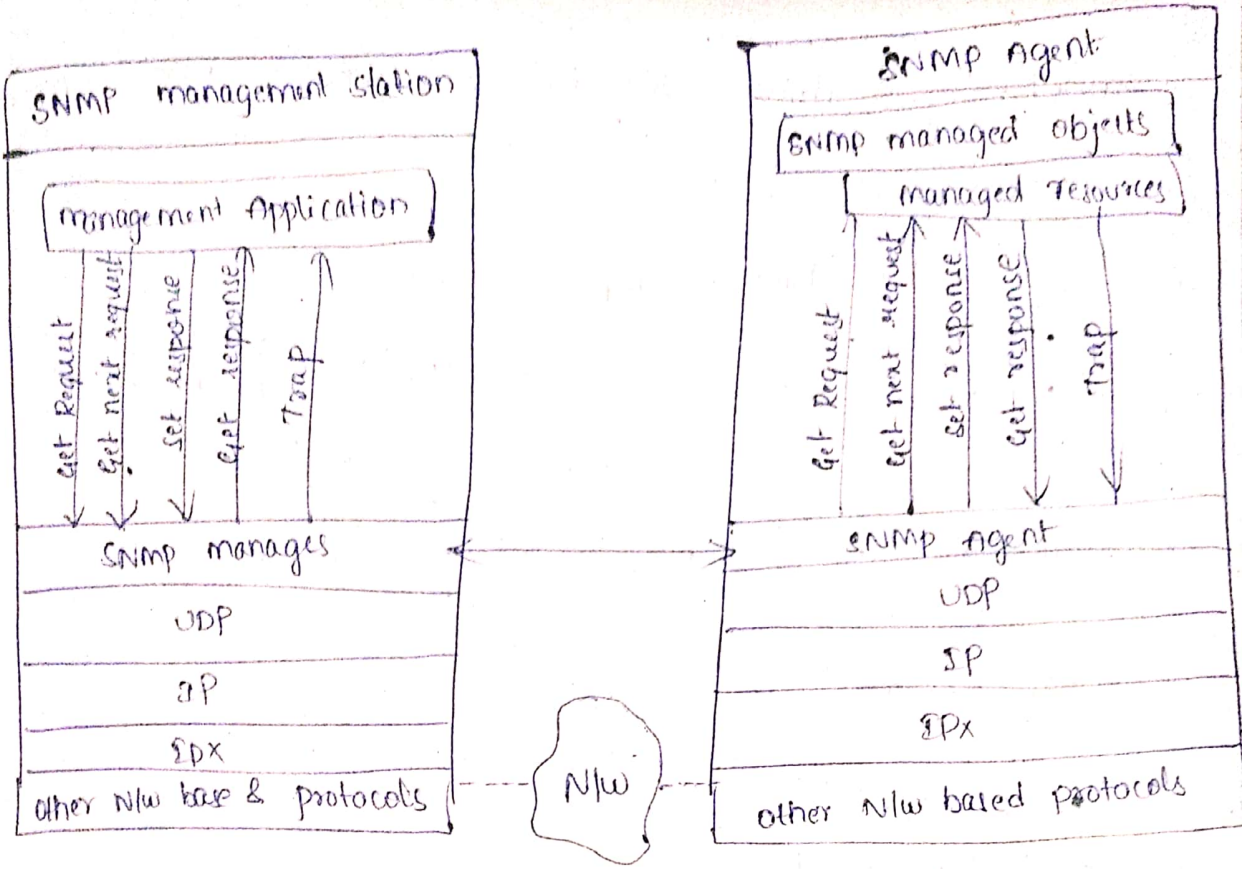
21/10/2019

SNMP protocol :-

SNMP V1 Header's-



* Community names are unique values.



- Get request — 0 (PDU type)
- Get next request — 1 (")
- Set response — 2 (")
- Get response — 3 (PDU type)
- Trap — 4 (PDU type)

SNMP V1 PDU format :-

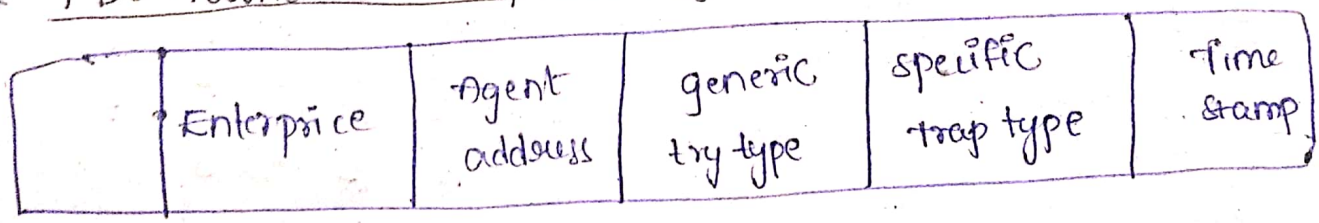
PDU Type	Request ID	Error status	Error Index	object 1 value 1	object 2 value 2	....	object n value n
0/1/2/3							

Variable binding

- Request IDs:- SNMP request with responses
- Error status: It specify no. of errors and their types.
- Error index: It is associate an error with a specific object instance

Variable bindings: It defines data fields of SNMP V1 PDU which is of variable length.

* PDU format of trap message:-



Enterprise: It is responsible for trap generation.

PDU 2 format

- Get request
- Get bulk request
- Get response
-