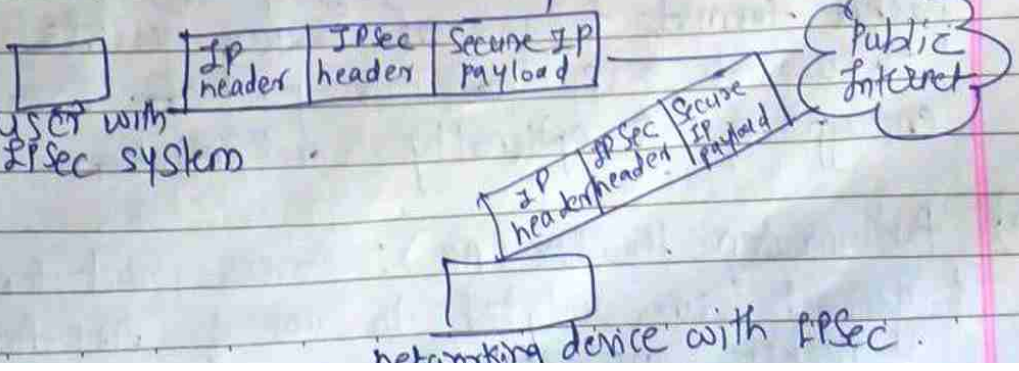
5. IP And Web Security

* IP Security (IPSec) is an IETF (Internet Engineering Task force) standard suite of protocols betn communication points across the IP network.
  - Provides data authentication, integrity & confidentiality
  - IPSec protects one or more paths betn pair of hosts, pair of security gateways or sec gateway & host

TCP
- connection oriented services.
- guarantees delivery of packets.
- Packet identification through seq. numbers.
- If packet not in seq, but in range of specified window, is accepted.

IP
- Connectionless protocol.
- cannot ensure delivery of packets.
- IP is mainly responsible for routing the packets over the n/w.
- Packet can take diff routes to reach destination in diff sequence.
- fragmentation → breaking down large IP packet into small pieces.



Defn of IPSec :- set of protocols used to secure internet communications by authenticating & encrypting each IP packet in a data stream.

* Benefits of IPSec :-
- In a firewall/router provides strong security to all traffic crossing the perimeter.
- 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 :-

Defined in numerous RFC's :-
1. RFC 2401: Overview of security architecture
2. RFC 2402: Description of packet authentication extension to IPv4 & IPv6.
3. RFC 2406: Description of packet encryption extension to IPv4 & IPv6
4. RFC 2408: Specification of key management capabilities.

Additional 4 documents are also published by IP Security Protocol working Group

1. Architecture → covers general concepts security requirements, definations & mechanisms
2. ESP (Encapsulating Security Payload) Covers packet format & general issues related to use of ESP for packet encryption, & optionally authentication.
3. Authentication Header (AH): covers packet format & general issues related to use of AH for packet authentication.

4) Encryption Algo :— Set of documents that describes how various encryption algos are used for ESP

5) Authentication Algo :— A set of documents that describe how auth algos are used for AH.

6) Key Management : describes key manage. schemes.

7) Domain of Interpretation (DOI) : Contains values needed for other documents to relate each other.

* IP Mac Address → Physical address → Media access control / MAC address.
— identifies a device to other devices on same local n/w.
— Internet addresses / IP → identifies device globally. N/w packet needs both addresses

MAC is unique identifier assigned to a NIC card.
IP address helps you to identify N/w connection

IPSec Services :—

	AH	ESP (encryp)	ESP (encryp + auth)
1) Access control	✓	✓	✓
2) Connectionless integrity	✓		✓
3) Data origin auth.	✓		✓
4) Rejection of replayed packets	✓	✓	✓
5) Confidentiality		✓	✓
6) limited traffic flow confidentiality.		✓	✓

* Security Association (SA) :—

They are like agreements betn devices to communicate securely. SA is a one-way relationship betn sender & Receiver that ensures secure communication

- SA is defined by 3 main elements:—
  1] Security Parameters Index (SPI) :—
  A unique identifier for each SA
  2] IP destn address → IP of receiver
  3] Security Protocol Identifier :— Indicates whether SA uses Auth. Header (AH) or Encapsulating Sec. Payload (ESP) protocol.

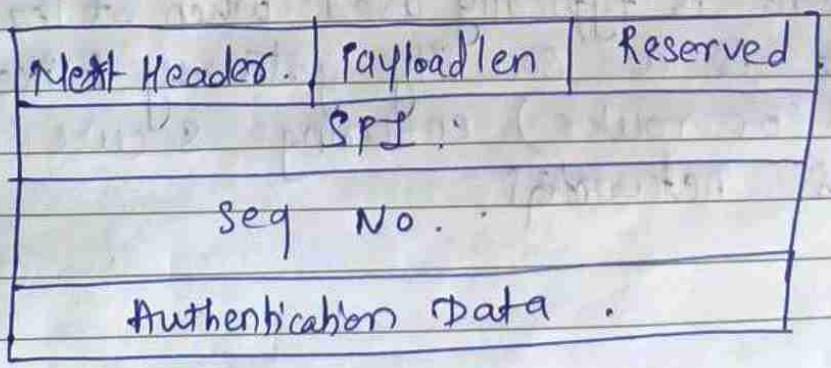
Apart from this SA also has parameters like seq numbers, lifetimes, & details about AH & ESP protocols.

only for understanding

Example Scenario of SA to understand :—
Company A & B want to set up secure VPN tunnel betn N/w
1. Establishing SAs : Company A's firewall establishes an SA with B's firewall. They agree on which encryption & authentication methods to use, & each assigns an SPI to identify aggreement.
2. Data transfer : When company A sends data to B, it uses agreed SA to encrypt & protect data. B's firewall, on receiving data, uses SPI to look up correct SA & decrypt data.

* AH (Authentication Header) :- is a protocol in IPSec designed to provide data integrity, authentication & protection against replay attacks for IP packets.
- It does not provide encryption, i.e. does not hide contents of data, instead, it ensures that data has not been tampered with during transit & confirms identity of sender.
- prevents ~~data~~ IP address spoofing attacks by tracking seq. numbers
- parties must share a secret key.

Imp fields in this header :-
1. Next header → type of protocol (TCP, UDP) following AH.
2. Payload length : length of AH header
3. Security Parameters Index (SPI) : Identifier for SA
4. Seq. number : Prevents replay attacks by ensuring each packet has a unique number
5. Authentication data : cryptographic hash (checksum) of packet.



* Transport AND Tunnel Modes:- these are 2 modes of operation supported by IPSec.

1) Transport Mode:
- It secures only the data (payload) of an IP packet, not the header
- Typically used for direct, end to end communi between 2 devices. (like client & server).
- ESP in transport Mode: Encrypts & optionally auth. just payload, not header
- AH in transport mode: authenticates payload and parts of IP header. (selected portions)

2) Tunnel Mode:
- It protects entire IP packet, including both header and payload.
- The original packet is encapsulated inside a new IP packet, creating a secure "tunnel" that hides original contents from any routers along the way.
- This mode is typically used when at least one endpoint is a security gateway (like a firewall or router) ensuring secure communications across networks.

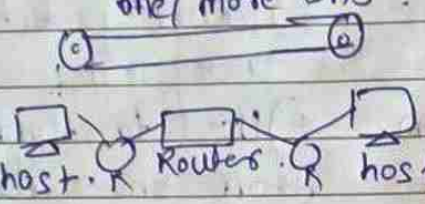
Transport Mode	Tunnel Mode
1) End hosts do IPsec encapsulation of their own data. Hence IPsec needs to implement on each end-hosts.	1) IPsec gateways provide service to other hosts in peer-to-peer tunnels, hence end hosts don't need IPsec.
2) lower overhead	2) More overhead
3) No edits in IP header	3) Entire packet is hashed & encrypted
4) Used in securing communication from one device to another	4) Used to tunnel traffic from one site to another
5) Good for ESP host-to-host.	5) Good for VPNs, gateway-to-gateway security
6) Provides protection to upper layer protocols.	6) Provides protection to entire IP packet
7) AH in transport mode auth. IP payload & some header.	7) Auth. entire inner IP packet & selected portions of outer IP header
8) ESP in transp mode encrypts & optionally auth. IP payload	8) entire inner IP pack, including IP header.

* Combining Both ESP & AH :-
- A single SA can only implement AH / ESP but not both simultaneously.
- By combining SAs into a bundle, we can get benefits of both protocols.
- A Security Association (SA) bundle is a collection or sequence of multiple SAs that works together to provide various IPsec security services.

↗ just for inf. refer ppt bases → mentioned below ↘

4 cases of Combining SAs :—

1) Transport mode SA applied End to end :
- Both AH & ESP are applied betn 2 devices (host-to-host). first SA uses ESP to encrypt payload, then second SA uses AH to authenticate encrypted payload.



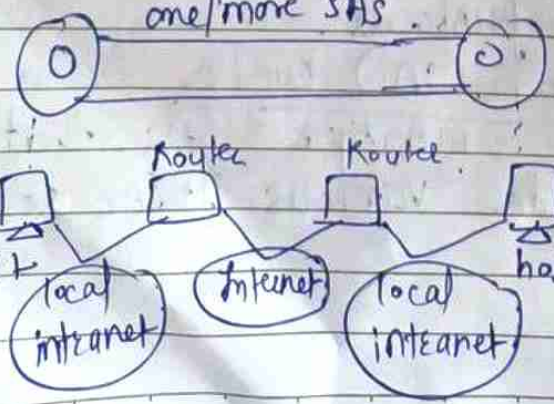
2) Transport Mode SA + Tunnel mode SA :—
Data is secured using both transport mode and tunnel mode.
Eg: 1st ESP in transport mode SA then ESP in tunnel mode SA.

3) Dual transport Mode SAs :— applying 2 transport mode SAs sequentially betn 2 devices.

4) Dual tunnel mode SAs :— involves applying 2 tunnel mode SAs betn 2 networks. ESP in tunnel mode, AH in tunnel mode.

imp

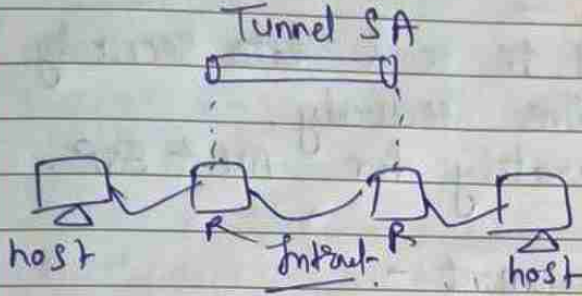
Cases in PPT :—



End-to-End Security betn Hosts.

Both hosts should have IPSec Configured.
Can use AH / ESP in transport mode.
Ex: Secure comm^n betn 2 internal hosts on a private N/w.

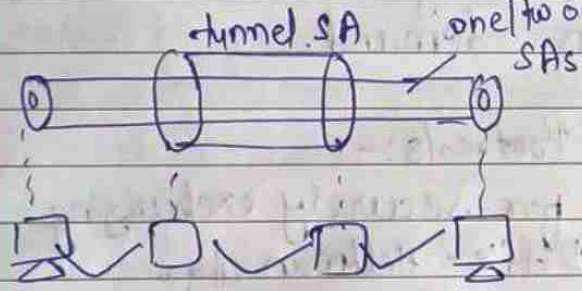
(2)



Security implemented betn 2 security gateways. End hosts do not need to be aware of IPSec.

Ex: Suitable for corporate networks that need to connect branch offices securely.

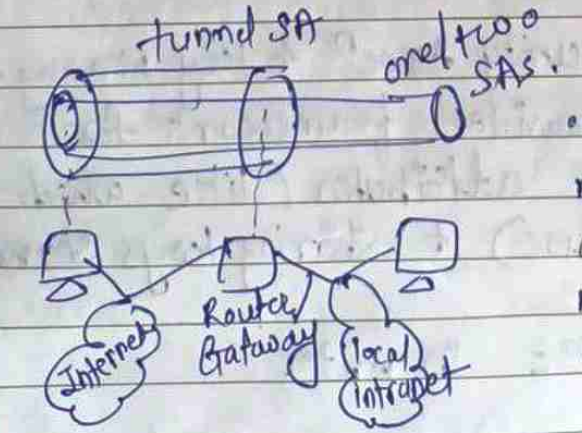
(3)



- Builds on case 2 by adding an additional layer of end-to-end security.
- tunnel betn gateways + one / ~~more~~ two SAs betn end hosts

Ex: Protecting sensitive data exchanged betn specific devices within 2 secure n/w

(4)



- for remote hosts that need to securely connect to an organization's internal network. Commonly used for remote access VPNs, where employees connect to corporate n/w from home or a remote location using a secure tunnel.

* Key management :-

- handles key generation & distribution of secret keys.
- 2 pairs of keys :-
  - Transmit key → Used to send data securely.
  - Receive key → Receive securely.

  This is done seperately for AH & ESP.

- Types of Key management :-

1. Manual key manage :- System administrator sets up keys manually for each device.
2. Automated :- Uses auto systems to create and distribute keys on demand.

- Key management Protocols :-

1) Oakley Protocol :- for securely exchanging keys based on Diffie-Hellman algo. Improves Diffie-Hellman by adding extra security features like protection against certain types of attacks.

2) ISAKMP (Internet Security Assoc^n & Key Manag. Protocol) :- It provides framework for negotiating security attributes (like which encryp^n method to use) & sharing keys securely.

See SSL Vs IPsec in ppt.

Web Security

- Need of web security due to foll. threats
1) Integrity: Modification of user data, causes loss of int, vulnerability to all other threats.
2) Confidentiality: loss of info, loss of privacy.
3) Denial of Service: Prevent user from getting work done → killing of user threads, flooding machine with bogus requests, isolating mac by DNS attacks, etc.
4) Authentication: Misrepresentation of user, belief that false info is valid.

Due to all this, web security is needed.

* Web traffic Security approaches:-

1] IPSec: Provides security at N/w layer. Encrypts & authenticates each IP packet to secure data. transparent to end users & applications.

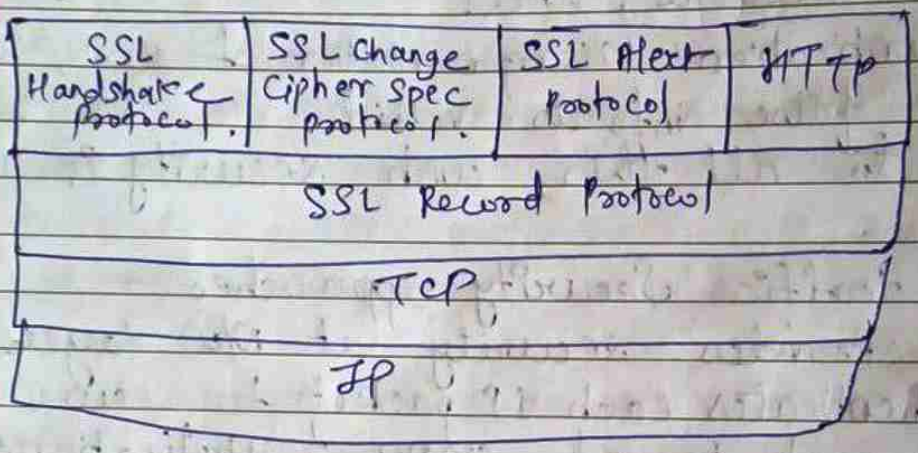
2] Transport level Security (SSL/TLS): Secures data at transport layer, commonly used for encrypting web traffic (like HTTPS). These can be integrated into underlying protocols (like HTTPS) to auto encrypt traffic b/w a web ~~server~~ browser & server.

3] Application Specific Security: Security measures that are built directly into specific applications. Eg: SET (Secure Electronic transaction) is protocol specifically designed to secure online credit card transactions.

* SSL :— Secure Socket Layer

- SSL is a cryptographic protocol used to provide secure communication over comp. N/w.
- Uses TCP to provide a reliable end-to-end service.

o SSL Architecture :→



o SSL session : an association betn client & server
- created by handshake protocol.

o SSL connection :— a transient, peer-to-peer, communications link.
- associated with one SSL session.

Session state is defined by foll. parameters:
- Session identifier.
- Peer certificate : X509.v3 certificate.
- Compression method : algo used to compress data prior to encryption.
- Cipher spec : Specifies bulk data encryption algo & hash algo.
- master secret : 48-byte secret shared betn client & server.
- Is resumable : flag indicating whether session can be used to initiate new connections.

- Connection state is defined by foll parameters:-
  - Client & Server random: Byte sequences that are chosen by server & client for each connection
  - Server write MAC secret: secret key used in MAC operations on data sent by server.
  - Client write MAC secret: secret key used in MAC oper^n on data sent by client.
  - Server write key: encryp key for data enc by server & decryp by client.
  - Client write key: encryp key for data encryp by client & decryp by server.
  - Initialization vectors: in block ciphers.
  - Seq. numbers → for messages.

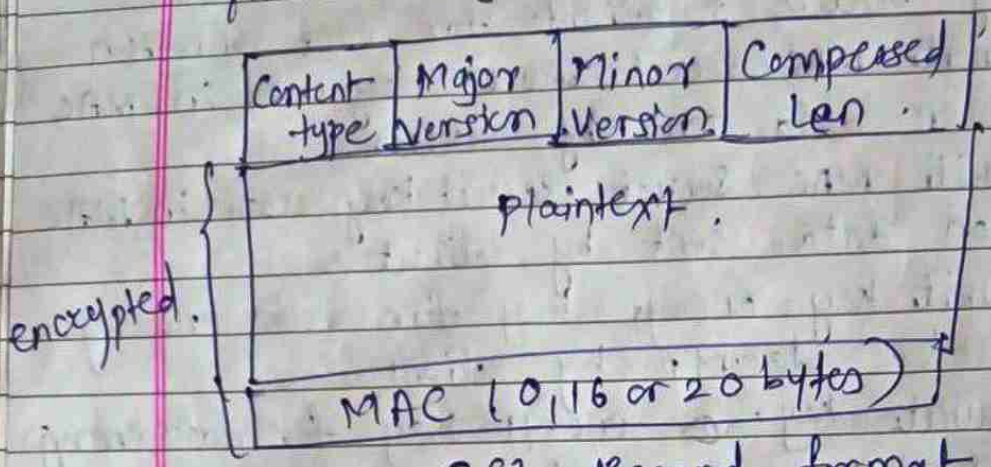
SSL Record Protocol.

- SSL R.P is responsible for ensuring the confidentiality and integrity of data. Steps:—

(1) Fragmentation: data is divided into small blocks
(2) Compression: ~~data~~ fragmented data is optionally compressed.
(3) MAC: add mac to ensure data integrity.
(4) Encryption: Data is encrypted using negotiated encryp algos and keys (DES-40, 3DES, etc) Fortezza
(5) Transmission: encrypted data, along with MAC is sent over N/w.

final step is to append a header, consisting of foll fields:— (1) Content type (8 bits): higher layer protocol used to process enclosed fragment
(2) Major Version (8 bits): Major version of SSL. SSLV3 → value is 3
(3) Minor version (8 bits): minor version for SSLV3 value is 0.

④ Compressed length (16 bits) : length in bytes of plaintext fragment (or compressed fragment)



SSL: Record format

* SSL Change Cipher Spec Protocol :— It is used to signal that sender will begin using a new set of cryptographic parameters, including cipher suit (encryp. t hash algos & keys that were established during handshake. Consists of single message which consists of single byte with value 1.

* SSL Alert Protocol :— used to send alert messages betn client and server. This messages indicate either a warning or an error that has occured during session. Categories are :—
  - Warning : non-fatal message that indicate a potential problem (Eg closed connection)
  - fatal : critical issues that result in termination of connection. (Eg handshake failure)

→ An alert message contains → level → severity of alert (warning or fatal)
Description → numeric code describing specific issue.

Eg:- unexpected_message,
bad_record_mac,
decompression_failure,
handshake_failure.

Remainder of alerts are the following:
- close_notify: Sender will not send any more msg.
- no_certificate: if no appr. cert is available
- bad_certificate: if cert is corrupt
- unsupported_certificate
- certificate_revoked
- " _ expired
- " _ unknown, etc.

* SSL HandShake Protocol:— Process thr. which client & server establish a secure comm^n channel.

1) Phase 1:- Establish Security capabilities.
Client hello: client sends a message to server indicating supported SSL versions, cipher suits & other parameters
Server hello: Server responds with selected SSL version, cipher suit & its own random value
Client hello contains:- version, random (client generated random structure), session ID, Cipher suit (list of cryp. algos supported by client in dec. order of preference), compression method → list of comp methods that client supports.
Eg: RSA, fixed Diffie-Hellman, Fortezza, etc.

Server auth & key exchange

2) Phase 2: Server sends its SSL cert to authenticate itself. Server may send cert, key exchange; and request cert. Server signals end of hello msg phase.

3) Phase 3: Client Auth & key exchange: Client sends cert if req. sends key exchange. Client may send cert verification.

Key exchange can be done using Diffie-Hellman, RSA, etc.

4) Phase 4: finish. (Change cipher suit & finish handshake protocol)
Both parties verify handshake & send a final msg confirming that handshake is complete.

Then SSL session begins.

- TLS (Transport Layer Security) is a successor to SSL.
with minor differences
- in record format version number
- uses HMAC for MAC (HMAC → hash based MAC) based on cryp. hash funcn & secret key.
- a pseudo-random function expands seeds
- has additional alert codes
- some changes in supported ciphers
- changes in certificate negotiations
- changes in use of padding.

* SET (Secure Electronic Transactions):—
- Set is a security standard designed to make credit card transactions safe over the internet. Open encryption & security specification to protect Internet credit card transactions.
- Provides privacy by restricting sensitive information access.

• Set Requirements:—
- Confidentiality of payment & order info.
- Integrity of transmitted data
- Authentication of cardholders & merchants.
- Ensure best security practices and sys design
- Create protocols that do not depends on transport security mechanisms and are compatible with it.
- Promotes interoperability among software and network providers.

* Key features of SET:—
1] Confidentiality: It encrypts your credit card details so no one else, not even merchant, can see your card no. only bank gets your credit card info.
2] Data integrity: - Ensures the info you send (like payment & order details) isn't changed on its way to merchant or bank. Uses digital signatures to confirm everything is as it should be.
3] cardholder Authentication: Checks that person using the card is actually cardholder. Uses digital certificates (like digital ID card) to verify identities.

4] Merchant Authentication: verifies that merchant you're bying from is legitimate & authorized to accept credit cards.

* Main players in SET:—
Cardholder, Merchant, Issuer (bank), Acquirer (bank that handles merchant's credit card transactions), Payment Gateway, Certificate Authority (CA) :- Issues digital certificates to prove identities of cardholders, merchants & banks.

SET transaction:—
(1) customer opens account (2) receives a certificate
(3) merchants have their own certificates.
(4) customer places an order (5) merchant is verified
(6) order & payment are sent (7) merchant req. payment authorization
(8) merchant confirms order (9) merchant provides goods or service (10) merchant req. payment.

Imp * What is Dual Signature?
Customer creates dual messages:—
— order Info (OI): for merchant.
:- Payment Info (PI) for bank.
To keep these two pieces of info seperate but linked, SET uses a dual signature
(1) merchant has received OI & verified the signature.
(2) Bank has received PI & verified signature
(3) Customer has linked the OI and PI and can prove the linkage.

* Types of SET transactions :—

1) Purchase request:
a) Initiate req : customer req. certificates in Initiate Req. message, sent to merchant.
b) merchant generates a response & signs it with its private key. signature key
c) Purchase request :- cardholder sends the actual purchase details to merchant. OI, PI. cardholder uses a dual signature to link OI & PI together but keeps them seperate. whole message is encrypted.
d) Purchase response : Reply from merchant back to cardholder to confirm order.

2) Payment authorization :- i) verifies all certificates
ii) decrypts digital envelop of auth. block to obtain sym key & decrypts auth block.
iii) verifies merchants signature
iv) decrypts digital envelop of payment block to obtain sym key & decrypt payment block
v) verifies dual signature on payment block.
vi) verifies transaction ID received from merchant matches that in PI received from customer.
vii) Req & receives an authorization from issuer
viii) sends auth. response back to merchant.

3) Payment Capture :- merchant sends payment gateway → payment capture req. gateway checks request, then causes funds to be transferred to merchants account notifies merchant using capture response.

SSL	TLS
1. Secure socket layer	1. Transport layer Sec.
2. Supports fortezza algo.	2. Doesn't support fortezza algo
3. Common in 3.0 version	3. Common in 1.0 version
4. Message digest is used to create a master secret	4. Pseudo-random funcn is used to create master secret
5. MAC based protocol is used.	5. HMAC based protocol is used
6. more complex than TLS	6. Simple
7. less secure as compared to TLS.	7. Provides high security.
8. less reliable & slower	8. Highly reliable & upgraded. less latency
9. has been depreciated	9. TLS is widely used
10. Uses port to set up explicit connection	10. Uses protocol to set up implicit connection