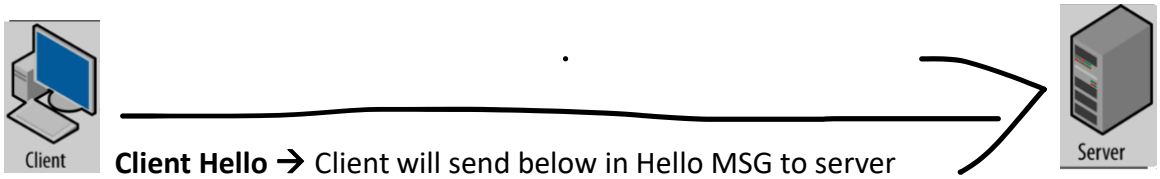
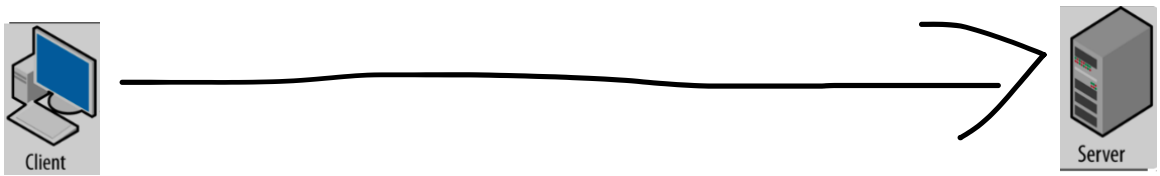
SSL/TLS Handshake

SSL/TLS handshake before. TLS 1.3.

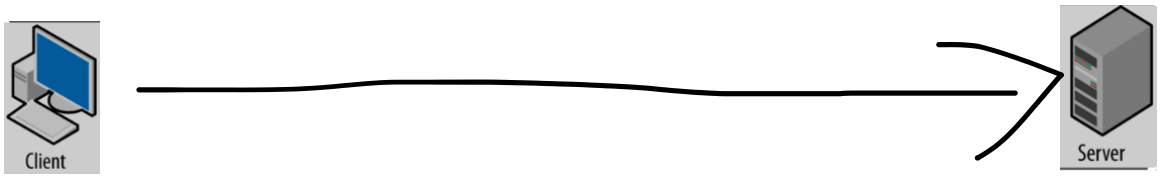


Client Hello → Client will send below in Hello MSG to server
TLS/SSL version
Supported Cipher Suits
Client will generate string of random bytes [Called Client Random]

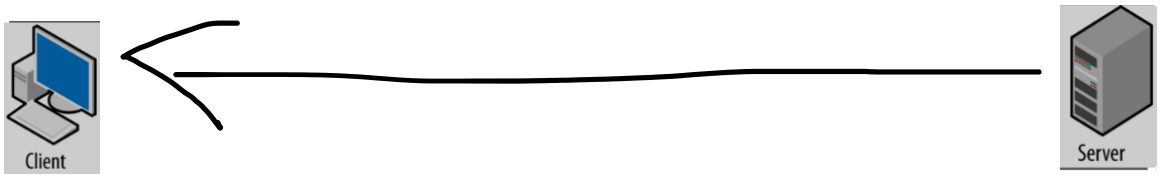
Server Hello → Server will send below in Hello MSG to Client:
Server's SSL Certificate [It will have server's public key]
TLS/SSL version [which should be one of from client msg]
Supported Cipher suit [anyone of from the list shared by client]
Server will generate string of random bytes [Called Server Random]



Server Authentication → Client will check Server's SSL certificate and certificate authority. Here it will be checked if server is the same which it is claiming to be.

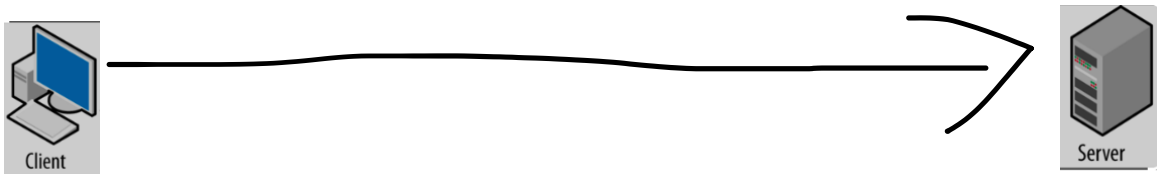


Pre – Master Secret → Client will generate another random string, encrypt the string using Server's public key and send to server.

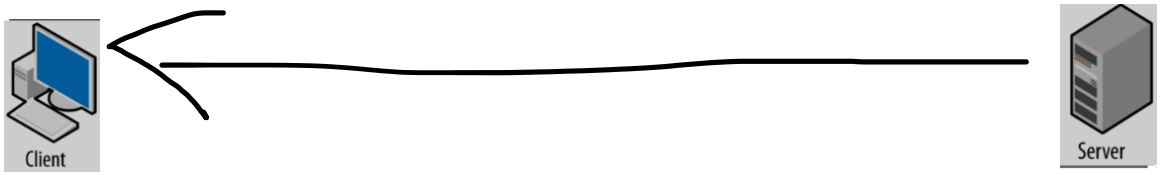


Server will decrypt the pre-master key using it's private key.

Session Key/Master Key → Both server and client will create the session key by using below:
Client Random
Server Random
Pre – Master secrete



Client Finish MSG → Client will send finished msg and this msg will be encrypted by session key.



Server Finish MSG → Server will send finished msg and this msg will be encrypted by session key.

Symmetric encryption is established now session key will be used for rest of the communication.