Message authentication:

A message authentication code (MAC) is a cryptographic checksum on data that uses a session key to detect both accidental and intentional modifications of the data.

A MAC requires two inputs: a message and a secret key known only to the originator of the message and its intended recipient(s). This allows the recipient of the message to verify the integrity of the message and authenticate that the message's sender has the shared secret key. If a sender doesn't know the secret key, the hash value would then be different, which would tell the recipient that the message was not from the original sender. There are four types of MACs: unconditionally secure, hash function-based, stream cipher-based and block cipher-based In the past, the most common approach to creating a MAC was to use block ciphers like Data Encryption Standard (DES), but hash-based MACs (HMACs) which use a secret key in conjunction with a cryptographic hash function to produce a hash, have become more widely used.

Type of Authentication:-

Offline authentication: An offline authentication policy defines the way users authenticate when they are not connected to the network.

Mutual authentication: Mutual authentication or two-way authentication refers to two parties authenticating each other at the same time, being a default mode of authentication in some protocols SSH and optional in others (TLS).

Mutual authentication is of two types:

1) Certificate based

2) User name-password based