KEY DISTRIBUTION

- For symmetric encryption to work, the two parties to an exchange must share the samekey, and that key must be protected from access by others.
- Key distribution can be achieved in a number of ways. For parties A and

  B:A key could be selected by A and physically delivered to B.
- A third party could select the key and physically deliver it to A and B.
- If A and B have previously used a key, one party could transmit the new key to theother, encrypted using the old key.
- If A and B each have an encrypted connection to a third party C, C could deliver a keyon the encrypted links to A and B.
    - Options 1 and 2 call for manual delivery of a key. But, delivering a key manually is not always possible.
    - Option 3 is a possibility for either link or end-to-end encryption, but if an attackerever succeeds in gaining access tone key, then all subsequent keys are revealed.
    - To provide keys for end- to- end encryption, option 4 is preferable. Figure 2.9 shows an implementation which satisfies option 4. For this scheme two kinds of keys are identified:

Session key:

Data encrypted with a one-time session key. At the conclusion of the sessionthe key is destroyed

1Permanent key:

Used between entities for the purpose of distributing session keys.

The Configuration consists of the following elements:

Key distribution center: the key distribution center (KDC) determines which systems are allowed to communicate with each other. When permission is granted for two systems to establish a connection, the distribution center provides a one-time session key for that connection.

Security service module(SSM): This module, which may consist of functionality at one protocol layer, performs end-to-end encryption and obtains session keys on behalf of users.

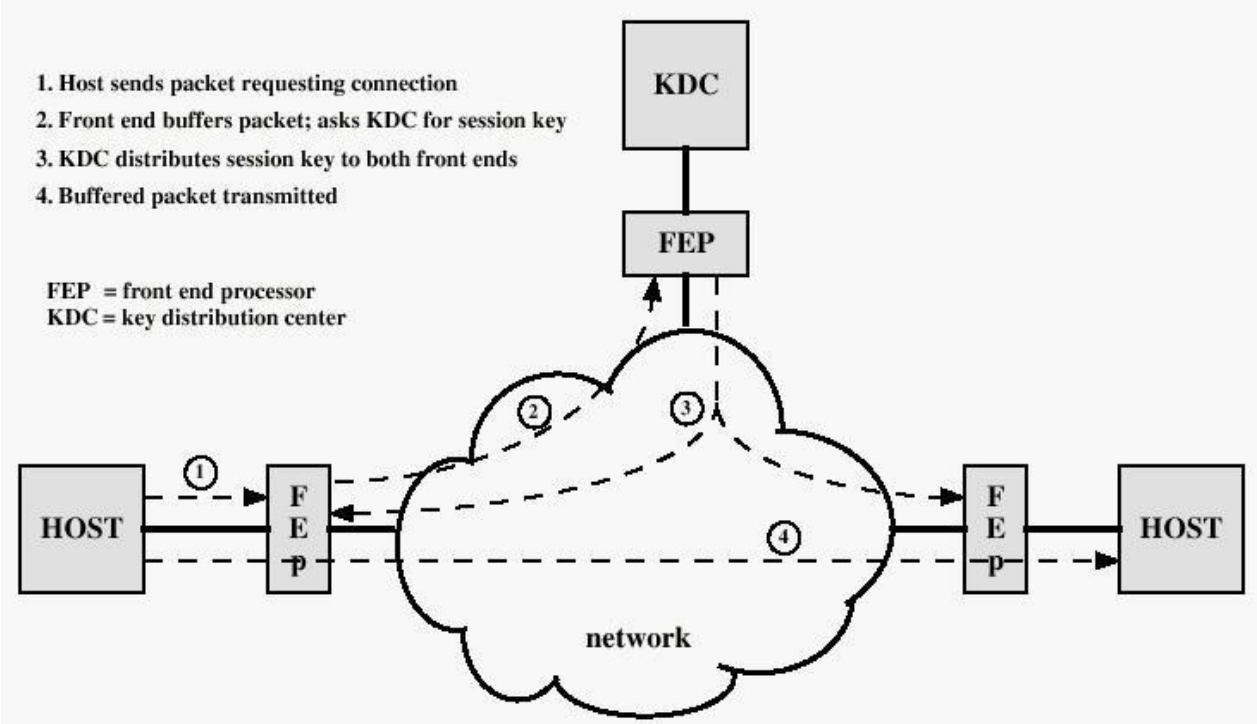

Figure 2.10 Automatic Key Distribution for Connection-Oriented Protocol

The steps involved in establishing a connection are shown in fig above.