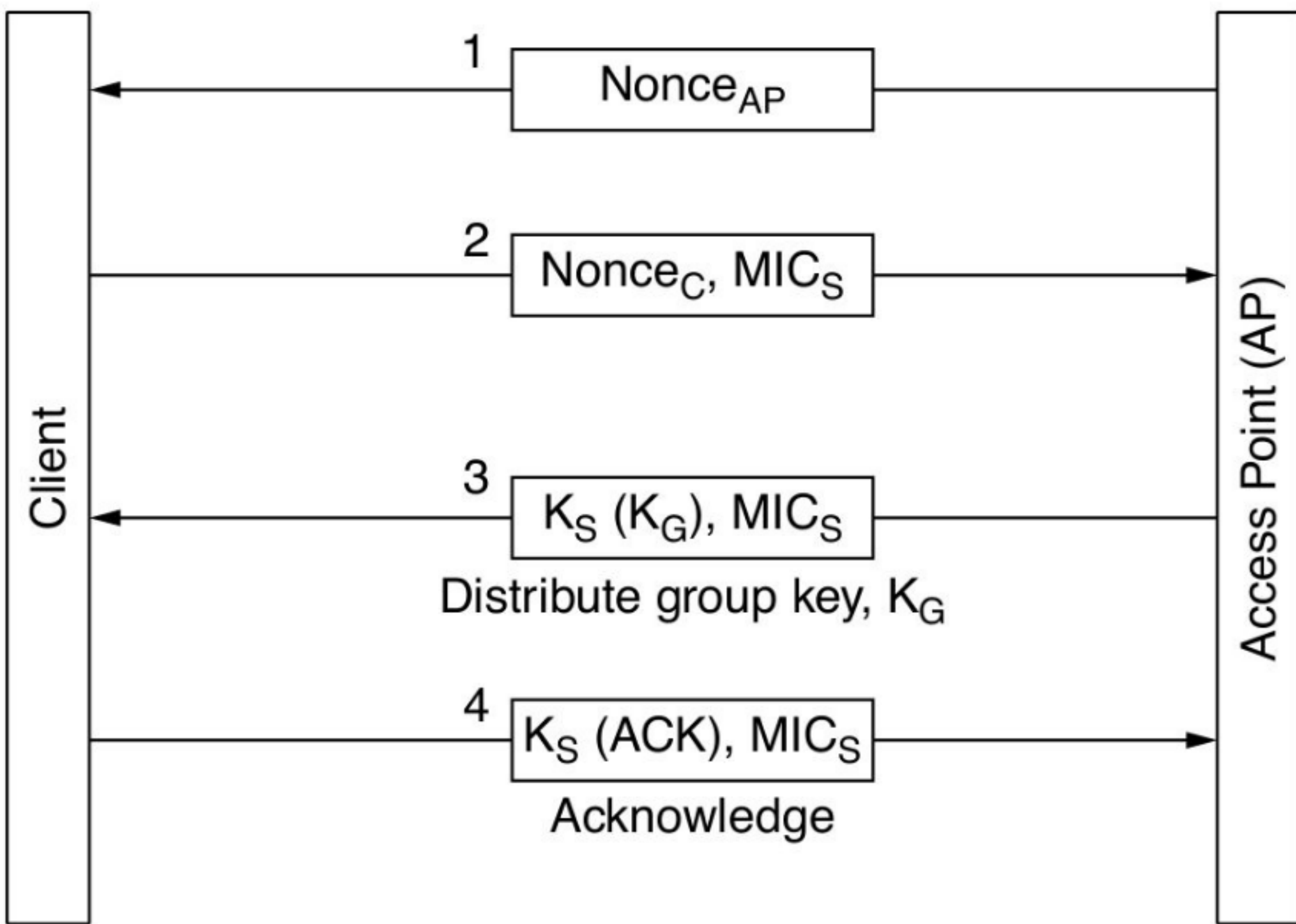


Compute session keys  $K_S$  from MAC addresses, nonces, and master key

Verify AP has  $K_S$



**$K_S$**  = Session Key specifica tra Client e AP  
 **$K_G$**  = Group Key usata per broadcast

Compute session keys  $K_S$ , same as the client

Verify client has  $K_S$