單向認證簡介

單向認證 (One-way Authentication)

- 只能確認某一方的身份：
  - 主機登入系統：只有主機能確認登入者的身份
- 『盤問/回應』(Challenge/Response) 協定

- 認證協定：
  - 單向共享密鑰認證

    確認對方所持有的『共享密鑰』(Shared Secret)
  - 單向公開鑰匙認證

    確認登入者鑰匙配對(私鑰或公鑰)