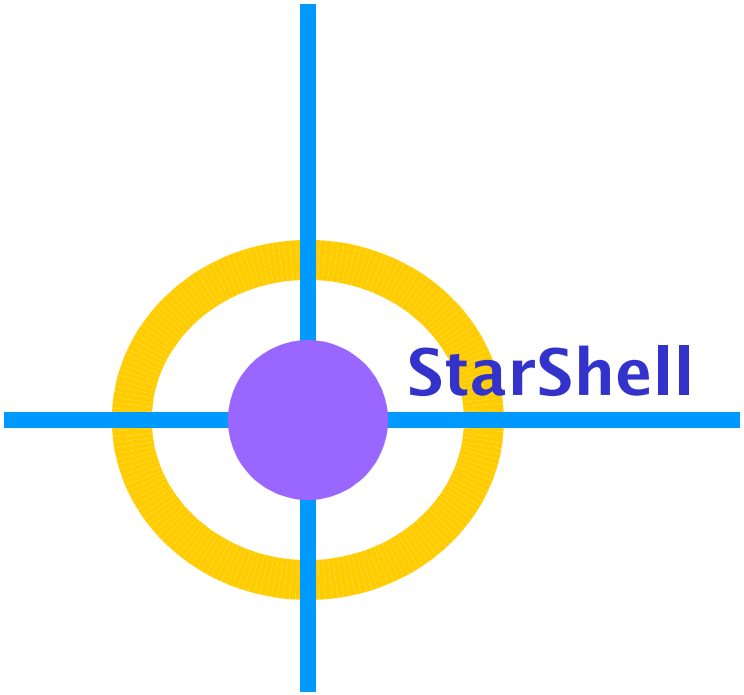
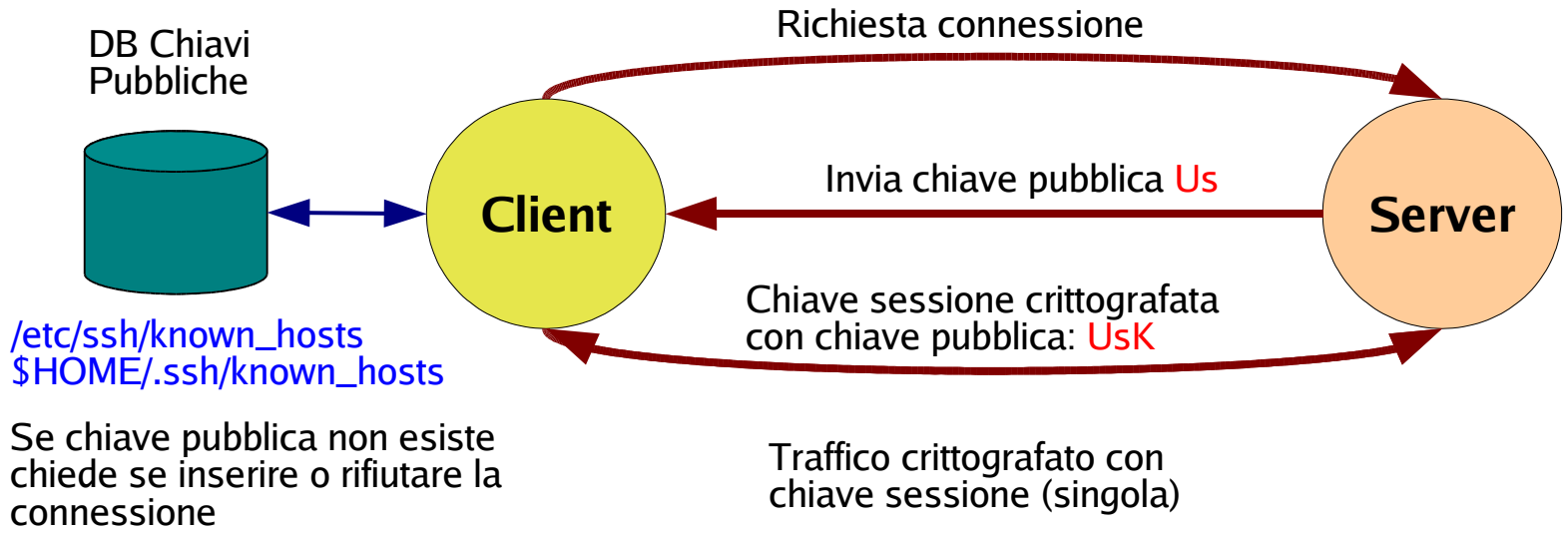


Ssh

Ssh

- Login remoto sicuro e altri servizi su canale insicuro
  - **Ssh, sftp, scp**
  - **Rimpiazza comandi Unix rlogin, rcp, rsh, ecc.**
- Fornisce:
  - **Crittografazione del canale**
  - **Autenticazione forte**
  - **Tunnel per altri protocolli su ssh**
- Contrasta:
  - **IP spoofing**
  - **DNS spoofing**
  - **Alterazioni di routing**

Ssh: Handshake



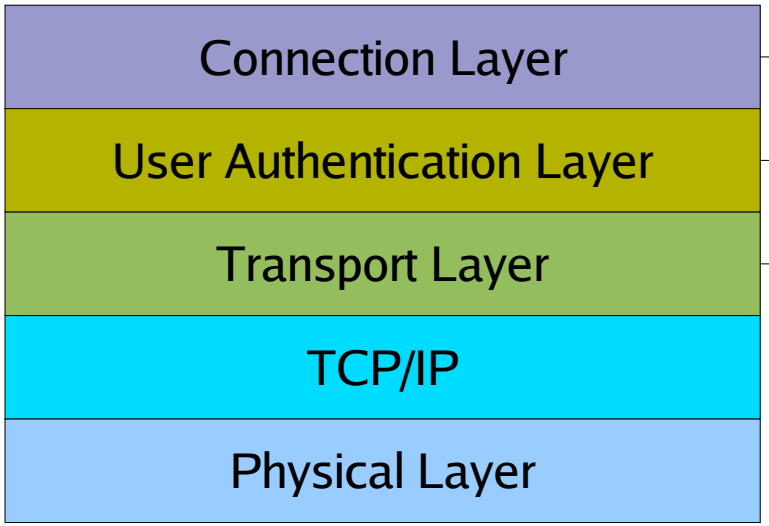

```
ssh -l utente server
```

- **Il server ha una coppia di chiavi doppie per ogni algoritmo supportato**
- **Segue l'autenticazione dell'utente (password), che transita già crittografata**

Ssh: antispoofing

- IP spoofing
  - Il server si autentica con chiave pubblica
    - **E' possibile preinstallare le chiavi pubbliche degli host conosciuti**
- DNS spoofing
  - Si può configurare l'autenticazione del client al server
    - **DB sul server delle chiavi pubbliche dei client conosciuti**
    - **Il client invia un pacchetto firmato con la propria chiave privata**

Ssh: Architettura

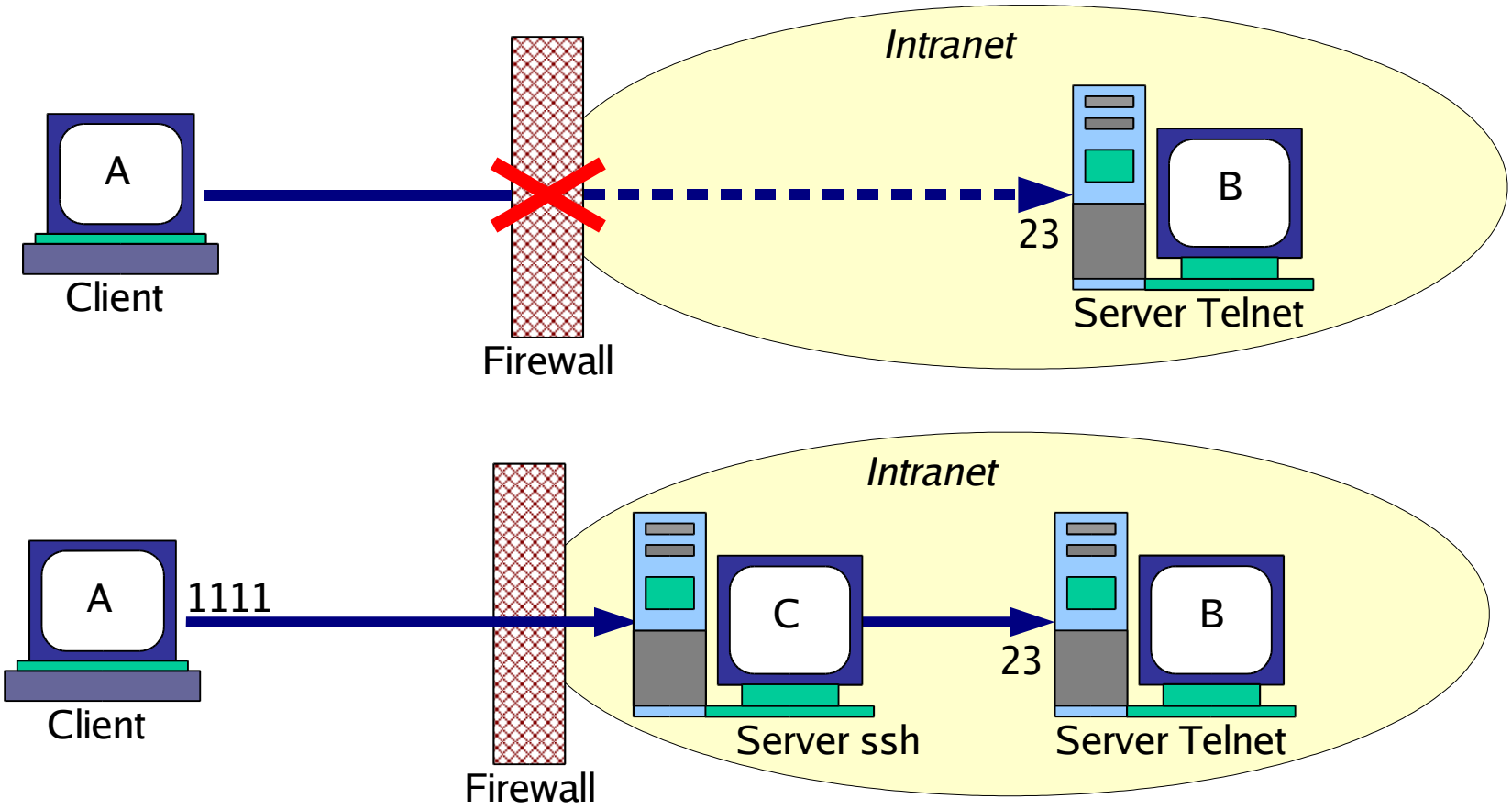


- Connessione divisa in canali logici multiplexati

- Identificazione del client
  - Chiave pubblica
  - Password
  - Basata sull'host (stile *rhosts*)

- Autenticazione del server
- Scambio chiavi
- Crittografazione
- Protezione dell'integrità
- Calcolo di un ID di sessione

Ssh: Port Forwarding




```
clientA> ssh -L 1111:serverB:23 serverC
```

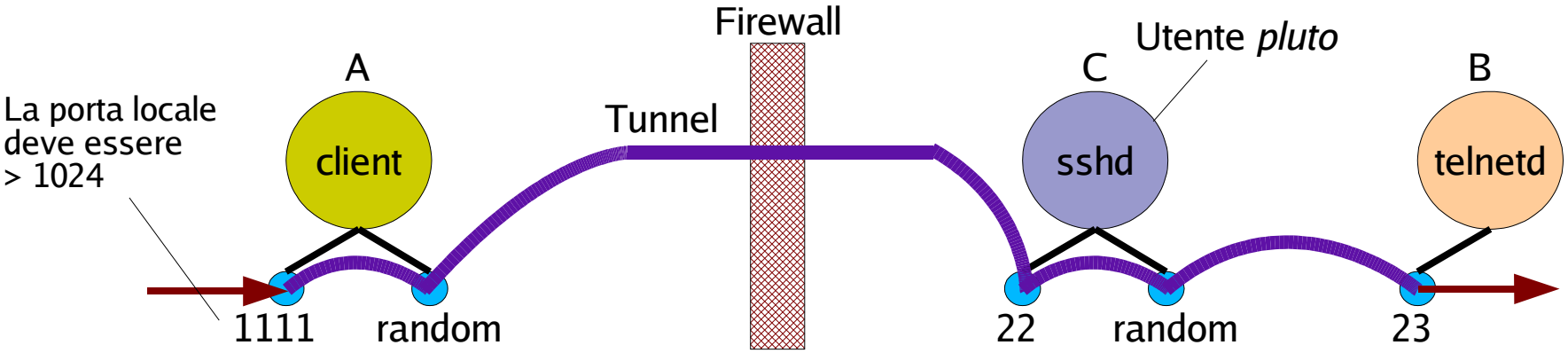
Setup del tunnel

```
clientA> telnet localhost 1111
```

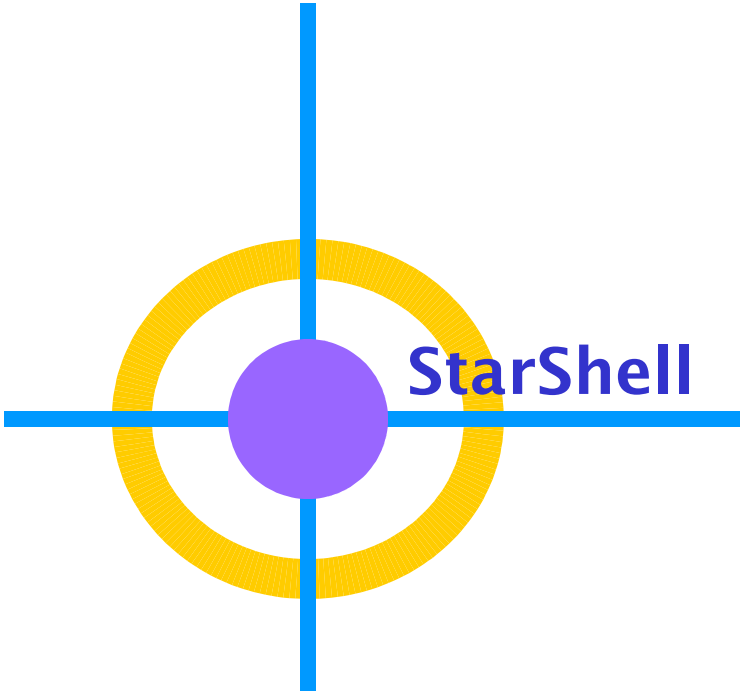
Uso del tunnel

Tunnel ssh: Pericoli

- Qualunque utente può stabilire un tunnel ssh
  - **Necessario un server ssh intranet e un utente noto su tale server**
  - **N.B.: Molti Linux installano e attivano ssh per default**
- I server ssh non devono avere utenti di comodo (guest)
- I server interni devono essere protetti da firewall personali
  - **Accettare connessioni solo dal server ssh ufficiale**




```
pippo@clientA> ssh -l pluto -L 1111:serverB:23 serverC
sam@clientA> telnet localhost 1111
```


StarShell