1. Accés remot i funcionament de SSH

El model client-servidor

En una connexió remota intervenen un **client**, que inicia la comunicació, i un **servidor**, que escolta peticions i oferix accés a un servei. Els dos equips han de disposar de connectivitat i el tallafocs ha de permetre el trànsit corresponent.

El servidor SSH sol escoltar en **TCP 22**. El client utilitza un port d'origen temporal. Conéixer una IP no és suficient: cal que el servei estiga actiu, siga accessible i accepte el compte indicat.

Necessitat	Solució habitual
Executar ordres i administrar un servidor sense escriptori	SSH
Treballar amb un escriptori remot de Windows	RDP
Visualitzar o controlar un escriptori amb una solució multiplataforma	VNC

Què aporta SSH?

SSH significa *Secure Shell*. Es va crear com a alternativa a eines com Telnet, que no protegixen el contingut de la comunicació. Cal distingir el **protocol SSH** de **OpenSSH**, una implementació que proporciona el client `ssh` i el servidor `sshd`.

SSH-1 és la primera versió i està obsoleta. En esta unitat es treballa amb **SSH-2**.

La connexió proporciona confidencialitat i integritat, autentica el servidor i permet autenticar l'usuari. La contrasenya, si s'utilitza, viatja dins del canal xifrat. L'autenticació amb clau pública és una altra opció; SSH no obliga a utilitzar-la.

Què passa quan es connecta?

1. El client establix la connexió TCP amb el servidor.

2. Es negocien els mecanismes criptogràfics i les claus de sessió.
3. El servidor acredita la seua identitat amb una clau de host. En una primera connexió, cal contrastar-ne l'empremta amb una font fiable.
4. L'usuari s'autentica, per exemple amb contrasenya o clau pública.
5. S'obri una sessió per a executar ordres o transportar altres comunicacions.

La clau de host identifica **l'equip servidor**. La clau de l'usuari identifica **qui intenta entrar**. Tenen funcions diferents.

Primera connexió

```
ssh alumne@192.168.0.1
hostname
whoami
exit
```

`hostname` i `whoami` s'executen al servidor després d'entrar. `exit` tanca la sessió remota. El client conserva les claus de host conegudes en `~/.ssh/known_hosts`; un canvi inesperat s'ha d'investigar abans d'acceptar-lo.

Referències

- Arquitectura del protocol SSH — RFC 4251.
- Manual del client OpenSSH.