# SSH

SECURE SHELL

# SSH MŰKÖDÉSE

- Sávon belüli interaktív távoli hozzáférés protokollja
- Titkosítja a teljes kommunikációt
- TCP-re épül
- 22-es szerverportot használja üzenetküldésre

# SSH BEÁLLÍTÁSÁHOZ SZÜKSÉGES ELŐZETES KONFIGURÁCIÓ

- Hostnév

```
Router(config)# hostname R1
```

- DNS tartománynév

```
R1(config)# ip domain name m013.local
```

- Enable jelszó (minden távoli hozzáféréshez kell)

```
R1(config)# enable secret class
```

# SSH BEÁLLÍTÁSÁHOZ SZÜKSÉGES ELŐZETES KONFIGURÁCIÓ

- Felhasználószintű hitelesítés

Létre kell hozzá hozni a felhasználót (itt felhasználó: user1 és jelszó: cisco):

```
R1(config)# username user1 password cisco
```

Lehet létrehozni adminisztrátor felhasználót is (ekkor rögtön privilegizált exec módba kerül a felhasználó és így az enable jelszó megspórolható):

```
R1(config)# username admin privilege 15 secret class
```

A `privilege 15` jelenti a privilegizált exec módot (0 lenne a user exec mód)

# SSH BEÁLLÍTÁSÁHOZ SZÜKSÉGES ELŐZETES KONFIGURÁCIÓ

- Be kell még állítani, hogy a helyi felhasználó adatbázist használja a távoli elérésnél hitelesítéshez:

```
R1(config)# line vty 0 4
R1(config-line)# login local
```

# SSH BEÁLLÍTÁSA

- Először az asszimetrikus titkosító kulcsot kell létrehozni (ez a kulcs nagy és csak lassú titkosítást tesz lehetővé és ezért csak arra használja az ssh, hogy a gyorsan működő szimmetrikus titkosítás titkosító kulcsát biztonságosan lehessen átküldeni a két gép között).

```
R1(config)# crypto key generate rsa
```

- Ekkor megkérdezi, hogy mekkora kulcsra van szükségünk (360-2048). Alapértelmezetten 512 biteset ad. Mindig a legnagyobbat érdemes állítani: 2048
- Vagy meg lehet adni egyben is:

```
R1(config)# crypto key generate rsa general-keys modulus 2048
```

# SSH BEÁLLÍTÁSA

Innen tulajdonképpen már működik is az ssh szerver a routeren. A további beállítások:

- SSH2 bekapcsolása (legalább 768 bites kulcs kell hozzá):

```
R1(config)# ip ssh version 2
```

- Hányszor próbálkozhass újra, ha elrontod a jelszót (itt öt próbálkozás lesz):

```
R1(config)# ip ssh authentication-retries 5
```

- Mennyi  idő van a jelszó beírására (másodpercben):

```
R1(config)# ip ssh time-out 60
```

# SSH BEÁLLÍTÁSA

- Annak beállítása, hogy csak ssh segítségével lehessen belépni:

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

- Minkettő: `transport input all` (ez eltűnik)
- Csak telnet: `transport input telnet`
- Mindkettő tiltása: `transport input none`

- A kapcsolón az ssh beállítása ugyanez.