

5. alkalom – Távoli elérés: Telnet és SSH: elmélet

Hálózatok I. · 11. évfolyam · 9–10. óra

A távoli elérés

- Ha a kapcsolónak már van **felügyeleti IP-címe** (SVI) és átjárója, nem kell konzolkábelrel odamenni: a saját gépünkről, a hálózaton keresztül is beléphetünk. Ez a **sávon belüli** elérés.
- A távoli belépések a **VTY-vonalakon** (virtuális vonalakon) érkeznek. A kapcsolón 16 van belőlük (line vty 0 15), sok routeren 5 (line vty 0 4).
- VTY-jelszó nélkül** a távoli belépést az eszköz el is utasítja. **enable secret nélkül** távolról nem lehet a # módba lépni (% No password set).

Telnet és SSH

	Telnet	SSH (Secure Shell)
Port	TCP 23	TCP 22
Titkosítás	nincs	van
Belépéskor	vonali jelszó	felhasználónév + jelszó
Mikor használjuk?	élesben tilos	mindig ezt, a 2-es verziót

Miért veszélyes a Telnet?

- A Telnet mindent **simán szöveggént** küld: a jelszót, a parancsokat és a válaszokat is.
- Aki a hálózaton **lehallgatja a forgalmat** (pl. a **Wireshark** programmal), az mindent elolvas. A Wiresharkban: szűrő telnet → jobb gomb egy sorra → **Follow** → **TCP Stream**: a teljes beszélgetés szöveggént látszik.
- Forgalmat rögzíteni **csak a saját laborhálózatunkon** szabad. Más forgalmának lehallgatása jogellenes.

Belépés Packet Tracerben

PC → Desktop → **Command Prompt**:

```
telnet 192.168.10.2
ssh -l admin 192.168.10.2
```

Kilépés: exit. (Valódi gépen: PuTTY → Telnet vagy SSH → a cím.)

Az SSH beállítása – 6 lépés

Az 1. lépés, az eszköznév (hostname S1), az alapkonfigurációból már megvan.

```

S1(config)# ip domain-name tk.local
S1(config)# username admin secret Adm1nPa55
S1(config)# crypto key generate rsa general-keys modulus 1024
S1(config)# ip ssh version 2
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit

```

Lépés	Miért kell?
eszköznév	a kulcs neve a gépnévből és a tartománynévből készül (pl. S1.tk.local). A gyári Switch névvel nem enged kulcsot generálni.
tartománynév	ugyanezért: nélküle nincs kulcsgenerálás
helyi felhasználó	az SSH felhasználónevet és jelszót kér; ezt magán az eszközön tároljuk, hash-elve
RSA-kulcspár	ezzel titkosít az eszköz. A 2-es verzióhoz legalább 768 bit kell, ezért 1024. Ha nem írod a parancs végére, rákérdez.
ip ssh version 2	az 1-es verzió elavult és sebezhető
transport input ssh	a VTY-vonalakon csak SSH , a Telnet le van tiltva
login local	a belépéskor a helyi felhasználót kéri, nem a régi vonali jelszót

Ellenőrzés

Parancs	Mit mutat?
show ip ssh	be van-e kapcsolva az SSH, és melyik verzió
show ssh	az éppen aktív SSH-kapcsolatok
telnet <cím> a PC-ről	transport input ssh után a Telnet már nem enged be

Az SSH-t sem lehet „feltörni” a titkosításán keresztül, de egy gyenge jelszót igen. Élesben erős, egyedi jelszó kell.

Fogalmak röviden

VTY-vonal · Telnet (TCP 23, titkosítatlan) · SSH (TCP 22, titkosított, 2-es verzió) · csomagelfogás, Wireshark · TCP-folyam követése · RSA-kulcspár · tartománynév · helyi felhasználó · login local · transport input ssh

L4 – Távoli elérés: Telnet és SSH

Név: _____ Osztály: _____

Cél

Távolról belépsz a kapcsolókra Telnettel, megnézed, mit lát, aki lehallgatja a forgalmat, majd beállítod a biztonságos SSH-t.

Kiindulás: a saját `Osztaly_Nev_alaphalozat.pkt` fájlod (az L3 végállapota).

Fontos: forgalmat rögzíteni csak a saját laborhálózatunkon szabad. Más forgalmának lehallgatása jogellenes.

1. rész – Telnet és a lehallgatás

Telnet

- ☐ 1. PC-A → Command Prompt → telnet 192.168.10.2 → a jelszó: cisco
- ☐ 2. enable → class → show ip interface brief → exit
- ☐ 3. Lépj be ugyanígy S2-re is (192.168.20.2). Sikerült? _____ Miért tudtál belépni egy másik hálózatban lévő eszközre?

A Telnet-forgalom elfogása (Wireshark)

A Packet Tracer nem tud Wiresharkkal rögzíteni, ezért egy valódi hálózaton rögzített mintafájlt elemzel. A Wireshark a laborgépre telepített, ingyenes program.

- ☐ 4. Indítsd el a **Wiresharkot** → **File** → **Open** → a tanártól kapott telnet-minta.pcap fájlt.
- ☐ 5. Fent a szűrősávba (*Apply a display filter*) írd be: telnet → Enter.
- ☐ 6. Kattints jobb gombbal bármelyik sorra → **Follow** → **TCP Stream**. A felugró ablakban az egész Telnet-beszélgetés olvasható szöveggént: **pirossal** amit a kliens küldött, **kékkel** amit a szerver válaszolt.
- ☐ 7. Mit láatsz a TCP Stream ablakban? Megtalálod a jelszót? Írd le: _____

2. rész – SSH

S1-en, globális konfigurációs módban:

- ☐ 8. Tartománynév: ip domain-name tk.local A kulcs neve a gépnévből és a tartománynévből készül (pl. S1.tk.local). Tartománynév nélkül a kapcsoló nem engedi létrehozni a kulcsot.
- ☐ 9. Helyi felhasználó: username admin secret Adm1nP455 Az SSH felhasználónevet és jelszót is kér. Ezt a fiókot a kapcsolón tároljuk („helyi”), titkosítva.
- ☐ 10. RSA-kulcs: crypto key generate rsa general-keys modulus 1024 Ezzel a kulcspárral titkosítja a kapcsoló a kapcsolatot. A 1024 a kulcs hossza bitben: minél hosszabb, annál erősebb. Az SSH 2-es verziójához legalább 768 kell. A kulcs elkészülése után az SSH magától bekapcsol.

- ☐ 11. SSH 2-es verzió: `ip ssh version 2` Az 1-es verzió régi és sebezhető, ezért csak a 2-est engedjük.
- ☐ 12. A VTY-vonalakon:

```
line vty 0 15
  transport input ssh
  login local
  exit
```

transport input ssh: a távoli belépés csak SSH-val mehet, a Telnet le van tiltva. login local: a belépéskor a 9. lépés helyi felhasználóját és jelszavát kéri (nem a régi password cisco-t).

- ☐ 13. Csináld meg ugyanezt S2-n is.

Ellenőrzés

- ☐ 14. S1: `show ip ssh` → mit ír ki a verzióról? _____
- ☐ 15. PC-A → `ssh -l admin 192.168.10.2` → jelszó: Adm1nPa55 → sikerült? _____
- ☐ 16. PC-A → `telnet 192.168.10.2` → mi történik most? _____
- ☐ 17. S1 (konzolon): `show ssh` → mit látsz? _____
- ☐ 18. Gondold végig: ha Wiresharkkal egy SSH-belépést rögzítenél (szűrő: `ssh`) → Follow → TCP Stream, olvasható lenne a jelszó? _____ Miért?
- ☐ 19. Mentés mindkét kapcsolón (`copy running-config startup-config`) és a PT-fájlé is.

Kérdések

1. Töltsd ki a táblázatot:

	Telnet	SSH
Port		
Titkosított?		
Mit kér belépéskor?		
Mikor használjuk?		

2. Miért kell a `login local` parancs a VTY-vonalakon?

3. Miért nem lehet RSA-kulcsot generálni, ha a kapcsoló neve még Switch?