Hálózati alapok

Az elmélet és az első lépések

Ingyenes online előadás
2016. október 27.

Smart Vision Solutions
taking you one step ahead

Az oktatás menete

- Protokollokra és a problémákra fókuszálunk, amit megoldani hivatottak
- Megoldásokat keresünk
- Az elméleti háttér megkerülhetetlen
- Villám-kérdőívek segítik a tematikán belüli gyorsabb (vagy épp lassabb) előrehaladást

Cél:

- A protokoll koncepciójának megértése (mire jó?)
- Az alkalmazás optimális körülményei (mikor jó?)
- Know-how: bevezetés, alkalmazás
- Hibakeresés, hibajavítás
- Kérdések, alkalmazási lehetőségek, korlátok - folyamatosan

Smart Vision Solutions
taking you one step ahead

A mai menetrend

- A rétegek, rétegződés
- Megfelelő fogalmak

Hozzáférések:

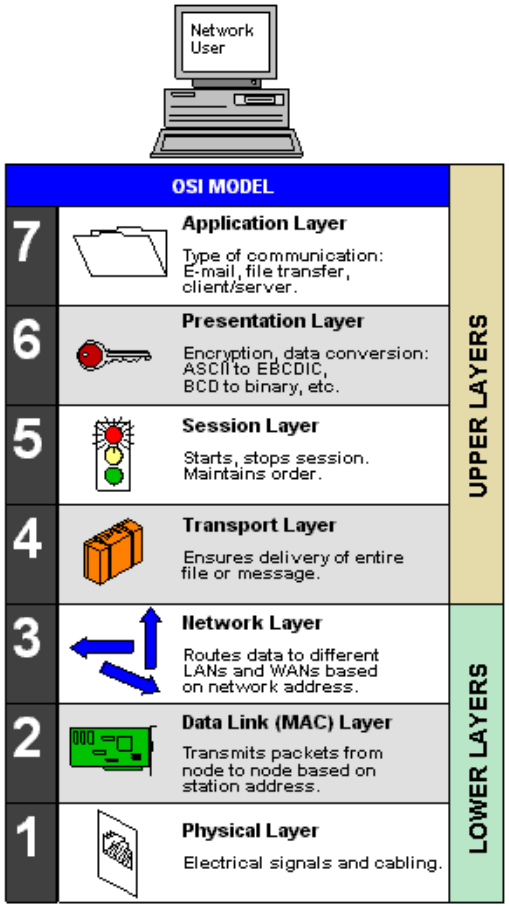
- Helyi
- Távoli
- IP címzés, biztonság, best practice

Rétegek, rétegződések

- Valószínűleg a legtöbbször kitárgyalt téma a világtörténelemben
- OSI = Open Systems Interconnection
- ISO = International Standards Organization

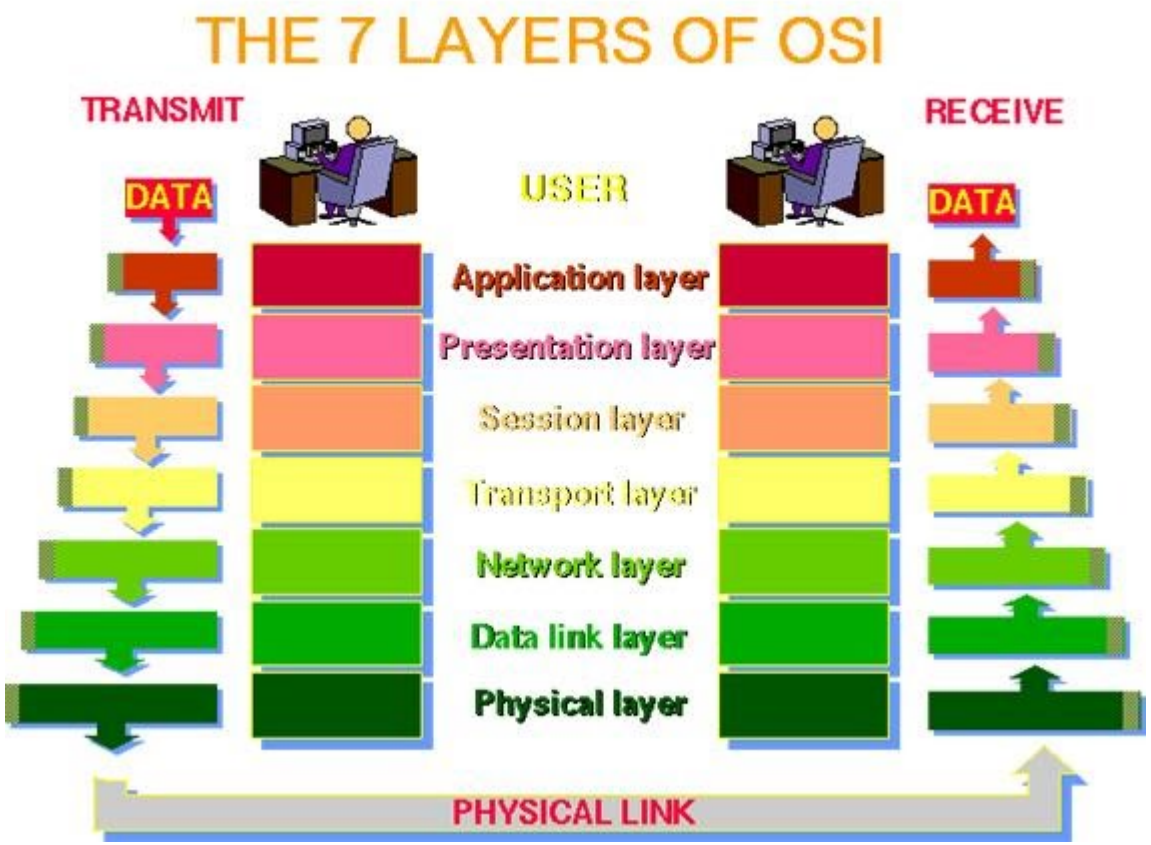
Miért rétegek?

  - Definiált együttműködési pontok
    - Egyszerű szabványosítás
    - Változások, fejlesztések
  - Hibakeresés támogatása
  - Problémák leszűkítése
  - Keep it simple, stupid
  - Hierarchikus viszony
  - Fejléc / payload struktúra



Smart Vision Solutions
taking you one step ahead

A tényleges kommunikáció



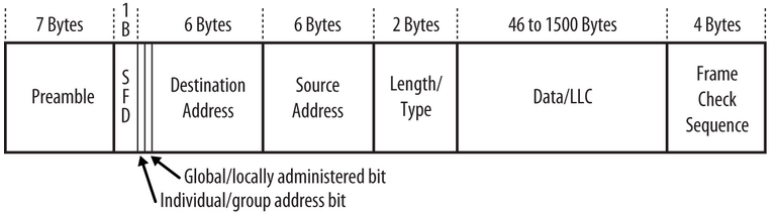
Gyakorlat – rétegek, keretek

Rétegek megfigyelése wiresharkban
[01.pcapng]

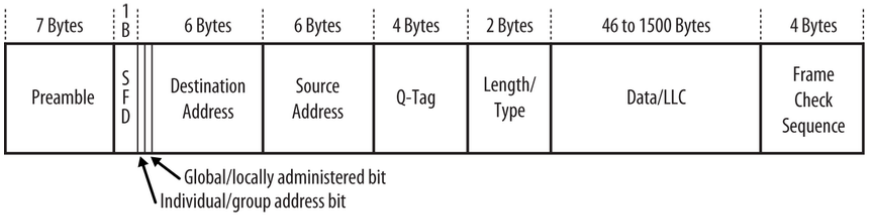
```
17 9.655393000 2605:f700:100:400::c7af:9546 2001:470:1f0b:19e7:4c7a:3430:9776:c306 TLSv1.2 120 Application Data
Frame 17: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
Ethernet II, Src: CiscoInc_7e:6b:a6 (e8:b7:48:7e:6b:a6), Dst: HewlettP_cc:db:e0 (38:63:bb:cc:db:e0)
  Destination: HewlettP_cc:db:e0 (38:63:bb:cc:db:e0)
  Source: CiscoInc_7e:6b:a6 (e8:b7:48:7e:6b:a6)
  Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2605:f700:100:400::c7af:9546 (2605:f700:100:400::c7af:9546), Dst:
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 66
  Next header: TCP (6)
  Hop limit: 54
  Source: 2605:f700:100:400::c7af:9546 (2605:f700:100:400::c7af:9546)
  Destination: 2001:470:1f0b:19e7:4c7a:3430:9776:c306 (2001:470:1f0b:19e7:4c7a:3430:9776:c306)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 993 (993), Dst Port: 8007 (8007), Seq: 1, Ack: 1, Len: 46
  Source Port: 993 (993)
  Destination Port: 8007 (8007)
  [Stream index: 0]
  [TCP Segment Len: 46]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 47    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Header Length: 20 bytes
  .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
  Window size value: 163
  [Calculated window size: 163]
  [window size scaling factor: -1 (unknown)]
  Checksum: 0x2a18 [validation disabled]
  Urgent pointer: 0
  [SEQ/ACK analysis]
Secure Sockets Layer
```

Ethernet: 802.3 (10 mbit/s)
FastEthernet: 802.3u (100 mbit/s)
GigabitEthernet: 802.3z (1000 mbit/s)
Azonos keretezés mindegyik esetben.

Type mező	Jelentés
0x0800	IPv4
0x86dd	IPv6
0x0806	ARP



IEEE 802.3 Basic Frame = Min 64 Bytes, Max 1518 Bytes + preamble



IEEE 802.3 Basic Frame with Q-Tag = Min 64 Bytes, Max 1522 Bytes + preamble

Hol tartunk?

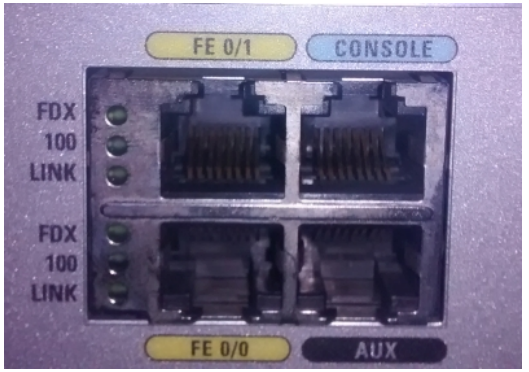
- A rétegek, rétegződés
- Megfelelő fogalmak

Hozzáférések:

- Helyi
- Távoli
- IP címzés, biztonság, best practice

Hozzáférés - konzol

- Leggyakrabban soros porti hozzáférés
- Cisco eszközökön mindig kékkel jelölt
- 3com, HP eszközökön lehet 9 tűs soros port
- Factory default: csak konzol porton át hozzáférhető



- Konfigurálás: praktikus és biztonságos beállítások
  - autentikáció
  - aszinkron naplózás
  - automatikus kiléptetés
- Konzol – távolról: az AUX port

Smart Vision Solutions
taking you one step ahead

Gyakorlat - beállítások

Kapcsolódás konzolon, beállítások

Beépített windows kliens: hyperterminal (xp)

Letölthető windows kliens: putty, kitty, securecrt

“Beépített” linux kliens: minicom

Elegáns megoldás: raspberry pi konzol szerver

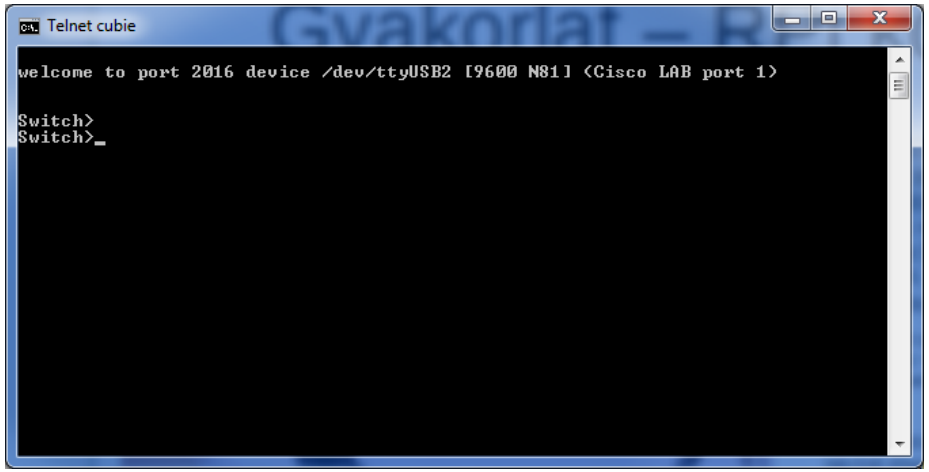
Smart Vision Solutions
taking you one step ahead

Gyakorlat – RPi konzol szerver

- USB-RS232 konverterrel, állandóan elérhetően
- soros port TCP portra “kivetítve” – telnet távolról
- mindez nyilván titkosított kapcsolaton át (vpn)
- Nem RPi hanem CT, de kb. ugyanaz
- scriptelhető (perl, expect)
- több soros porti konverterrel is megy
- laborban, szerverteremben hasznos lehet

```
root@cubie:~# grep -v "^#" /etc/ser2net.conf

BANNER:banner2016:\r\nwelcome to port \p device \d [\s] (Cisco LAB port 1)\r\n\r\n
2016:telnet:600:/dev/ttyUSB2:9600 8DATABITS NONE 1STOPBIT banner2016
```



- ser2net csomag

root@cubie:~# dpkg-query -s ser2net
Package: ser2net
[...]
Conffiles:
/etc/default/ser2net
/etc/init.d/ser2net
/etc/ser2net.conf
Description: Serial port to network proxy
This daemon **allows telnet** and tcp **sessions to be established with a**
Homepage: http://sourceforge.net/projects/ser2net

Smart Vision Solutions
taking you one step ahead

Gyakorlat – aux port, reverse telnet

- Normális esetben a konzolhoz helyben kell lenni – pl a szerverszobában
- A konzol is kipatchelhető az íróasztalhoz kényelmes környezetbe, de kb. ennyi
- Ellenben az AUX port valódi távoli konzolt tesz lehetővé – akár interneten át
- Eredetileg OOB (out of band) hozzáférésre tervezték – pl. modemmel konzolra hívni
- 2016-ban inkább a reverse telnet felhasználása terjedt el. Mi is ez?

```
line aux 0
 modem InOut
 terminal-type xterm
 transport input all
 transport output all
```

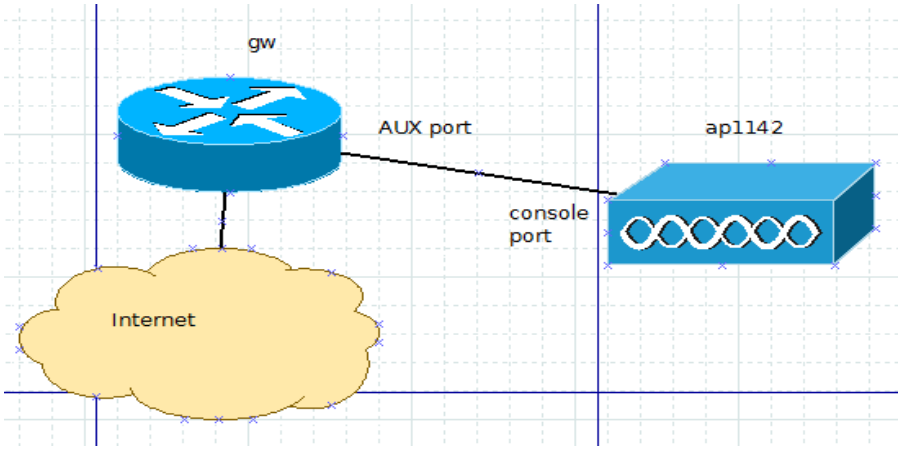
- Az AUX port konfigurálható kifele irányba is
- Kék kábellel másik eszköz konzoljába köthető
- Saját magamra telnetelve a másik eszközbe jutok
- Amíg egyetlen eszköz van, ami elérhető távolról, az AUX porton bejutok az elérhetetlen második eszköz konzoljára
- Nálunk interjúkon beugró kérdés szokott lenni

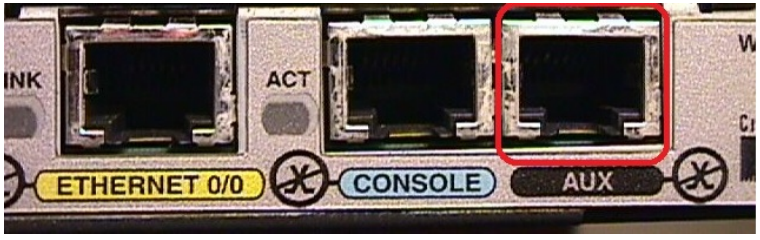
```
c881-bud.lehel#sh line | i AUX
     1 AUX    9600/9600  - inout       -    -    -
c881-bud.lehel#sh ip interface brief | include Loop
Loopback0              172.31.255.126  YES NVRAM
Loopback1              172.31.255.123  YES NVRAM
c881-bud.lehel#telnet 172.31.255.126 2001
Trying 172.31.255.126, 2001 ... Open

User Access Verification

Username: root
Password:
ap1142.bud-lehel>
```

+2000

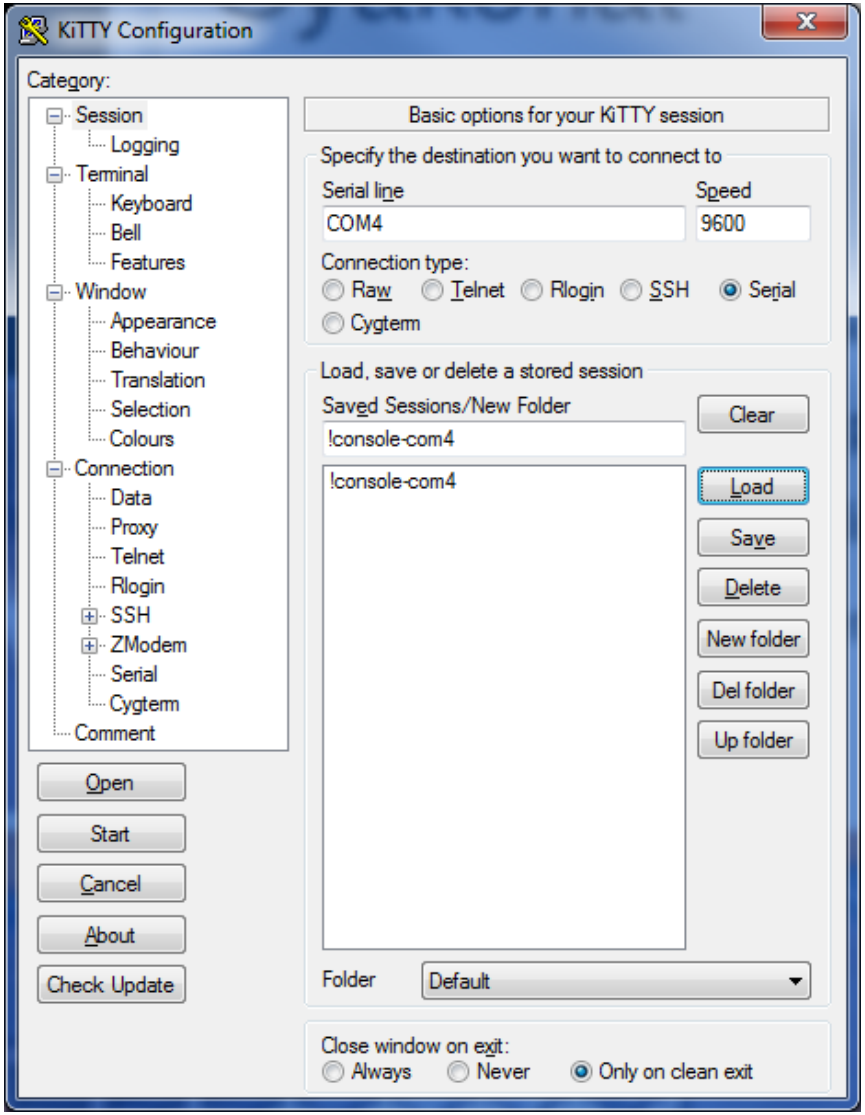




Smart Vision Solutions
taking you one step ahead

Gyakorlat - konzol

Kapcsolódás konzolon, beállítások



A bootolás eszköztől függően 2-10 perc

Feladatok:

- Első bekapcsolás utáni alaphelyzetbe hozás
  - konfigurációs módok
  - jelszó beállítása
  - IP cím (fix IP, dhcp, valamint dhcp hibakeresés)
  - távoli elérés (telnet, ssh, ssh hibakeresés)
  - timeout értékek beállítása konzolon
- Konfiguráció elmentése
  - lokálisan (commit)
  - lokálisan (flash)
  - távolra (tftp)

Smart Vision Solutions
taking you one step ahead

Gyakorlat - konzol

Konfigurációs módok:
- user exec mode
- privilege exec mode
- global config mode
- sub-config mode
- rommon mode
- setup mode

Jelszó beállítás
- enable password / secret
- konzol
- VTY
- jelszótlansági beállítás - LAB

IP cím beállítása
- üres switchen, most bootolt (show ip int brie)
- Most csak Vlan 1 interfészen – alapértelmezett

Távoli elérés
- telnet (jelszó nélkül)
- jelszótitkosítás
  http://www.ifm.net.nz/cookbooks/passwordcracker.html
- enable jelszó – a fentiek tükrében nem az enable password
- ssh + hibakeresés (amit csak lehet, elrontunk, mint egy kezdő)

Timeout értékek
- konzolra és távoli elérésre külön
- legtöbb audit követeli, hogy legyen
- általában 1-2 órát szoktam, de pl. audit követelhet 10 percet (PCI)

Konfiguráció elmentése
- lokálisan, nem felejtő memóriába, mint alapértelmezett
- lokálisan, nem felejtő memóriába, másolatként
- távolra (pl. tftp)
- automatizált mentések, verziókezeléssel a haladó oktatásban

Gyakorlat – best practice beállítások

- telnet / ssh
- Cisco eszközökön alapértelmezetten legfeljebb öt párhuzamos belépés
- Factory default: jelszó nincs, de szükséges –> nem lehet belépni
- Konfigurálás: praktikus és biztonságos beállítások
  - autentikáció
  - aszinkron naplózás
  - automatikus kiléptetés
  - korlátozás biztonságos hozzáférési protokollokra (pl. ssh, telnet helyett)
  - korlátozás IP tartományra (gyenge példa: linux – hosts.allow / hosts.deny)
    - ✗ ennek van rendes elméleti háttere ami nélkül nem célszerű vakon másolni saját eszközbe
    - ✓ ugyanakkor értem és megértem ha valakit ez nem érdekel és csak megoldásokra kíváncsi
    - ✓ ACL – forgalom kijelölése IP címek, tartományok alapján
    - ✓ felhasználás – az ACL által kijelölt forgalomra vonatkozóan csinálunk (vagy nem csinálunk) valamit

Örülök, hogy eljöttél meghallgatni. Kérdések?

Az oktatások tartalma, általános információk:
http://svs.cx

Piaci alapokon működünk, de törekszünk arra, hogy ingyen, vagy legalább igen nagy kedvezménnyel tartsunk további online előadásokat magyar rendszergazdáknak. A kedvezményeket biztosító kódokat a hírlevelekben fogjuk közzétenni.

Megköszönjük, ha véleményezed a munkánkat.

Ha nem tetszik ahogy csináljuk, kérlek mondd el nekünk.
Ha tetszik ahogy csináljuk, kérlek mondd el másoknak!

facebook.com/svsltduk