

Tavaszi

2017

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS  
**UNIVERSITY OF SZEGED**  
*Department of Software Engineering*

# Virtuális Helyi Hálózatok

Somogyi Viktor

## Tartalomjegyzék

<b>Bevezetés.....</b>	<b>3</b>
<b>A hálózatok méret szerinti csoportosításai .....</b>	<b>3</b>
LAN (Local Area Network) .....	3
MAN (Middle Area Network).....	3
WAN (Wide Area Network) .....	3
<b>VLAN (Virtual LAN) .....</b>	<b>3</b>
Miért lehet szükség virtuális helyi hálózatokra? .....	3
A VLAN-ok felépítése .....	4
<b>VLAN-ok építése Packet Tracerben.....</b>	<b>5</b>
Konfigurálás GUI-n keresztül.....	6
Konfigurálás CLI-n keresztül .....	8
Összefoglalás.....	9
<b>Beugró kérdések.....</b>	<b>9</b>

## Bevezetés

Az előző órán áttekintettük a hálózatok alacsony szintű felépítését. Most eggyel továbblépünk, és megtanuljuk, hogyan lehet az egyes hálózatok struktúráját még jobban megtervezni és felépíteni virtuális hálózatok segítségével.

## A hálózatok méret szerinti csoportosításai

A hálózatokat egy háromrétegű hierarchiába rendezi az Ethernet. Ez volt a hozzáférési réteg, az elosztási réteg, és a központi réteg. Mindegyikhez különböző eszközöket rendeltünk (például az elosztási réteghez a routereket), és mindegyik szintnek megvolt a maga feladata.

Ezekén kívül viszont még a hálózatokat gyakran csoportosítják kiterjedés szerint is. Három ilyen szintet különböztetünk meg hagyományosan: LAN, MAN és WAN.

### LAN (Local Area Network)

Magyarul helyi hálózatnak fordítják. Ahogyan a nevéből is adódik, főként kisebb kiterjedésű rendszerek jelölésére használják. A kifejezés önálló helyi hálózatra utal, vagy egy csoport, közös adminisztratív irányítás alatt álló, egymással összekötött helyi hálózatra. A hálózatok kezdeti időszakában gyakran fizikailag egy helyen elhelyezkedő, kisméretű hálózatként határozták meg. Ma viszont már hozzáértjük akár az otthoni, akár a több száz gépet, több épületet és helyet magában foglaló vállalati hálózatokat is.

A LAN-ok jellemzően Ethernet vagy Wireless kapcsolatokat használnak, és nagy sebesség jellemzi őket.

Az Intranet gyakran egy szervezethez tartozó privát LAN-t jelöl, amit úgy terveztek, hogy csak a szervezet tagjai férhessenek hozzá.

### MAN (Middle Area Network)

A LAN-nál nagyobb, de kevésbé használt. Méretben valahol a LAN és a WAN között van, és egy nagyobb területet fed le, mint például egy város. Gyakran a kormányzatok és nagyobb szervezetek számára van jelentősége.

A gyakorlaton nem fogunk a továbbiakban foglalkozni MAN-okkal.

### WAN (Wide Area Network)

Ha egy vállalat több, egymástól távoli telephellyel rendelkezik, akkor szükség lehet egy távközlési szolgáltató (TSP – Telecommunication Service Provider) bevonására a különböző LAN-ok összekapcsolásához. Az egymástól távol eső LAN-okat összekapcsoló hálózatokat nagytávolságú hálózatoknak (WAN) nevezzük.

## VLAN (Virtual LAN)

### Miért lehet szükség virtuális helyi hálózatokra?

A helyi hálózatok főként fizikailag egymás közelében levő gépek halmazát jelentik. A hubokat és switcheket alkalmazó Ethernet révén viszont sok esetben lehetővé vált, hogy a LAN-okat ne fizikai, hanem logikai úton alakítsák ki. Ha egy vállalat  $k$  darab LAN-t akart, akkor vásárolt  $k$  darab switchet. Ha kellő gondot fordítottak arra, hogy melyik csatlakozót melyik switchbe dugják, akkor a LAN-

ok tagjait viszonylag elhelyezkedéstől függetlenül, a szervezeti felépítésnek megfelelően lehetett változtatni. Persze, ha két ember ugyan annál a részlegnél, de messzebb, más épületben dolgozik, akkor valószínűleg más LAN-okhoz fognak tartozni. Viszont ez nem egy tökéletes megoldás, mert körülményes tervezést kíván a hálózatépítőktől.

A rendszergazdák több okból kifolyólag is szeretik, ha a LAN-okon lévő felhasználói csoportok nem a fizikai elhelyezkedést tükrözik, hanem az intézmény szervezeti rendjét. Az első ilyen a biztonság. Sok esetben vannak olyan felhasználó csoportok egy vállalatnál (például egy kutatási, fejlesztési részleg), amelyek információit nem szeretnénk azon a körön kívül látni. Ilyenkor célszerű őket egy LAN-ba tenni, mert egy magasabb fokú biztonság őrizhető meg így. A vállalati vezetés pedig nem szívesen hallja, hogy egy ilyen elrendezést csak akkor lehet megvalósítani, ha a részleg összes dolgozóját egymás közelébe, például szomszédos irodákba kell tenni, mivel ez igen nagy átrendezésekkel járhat. Ehhez kapcsolódó problémák a szervezeti változások, ugyanis egy nagyobb cég életében ezek szinte mindennaposak. Ha a LAN-okat fizikai helyük szerint rendeznénk, akkor hatalmas többletmunkával és költséggel járna átszervezni a hálózatot.

A másik gondot a terhelés jelenti. Egyes LAN-okat sokkal intenzívebben használnak, mint másokat, és olykor kívánatos lehet elkülöníteni az ilyeneket. Ha például a kutatási részlegen mindenféle remek kísérletet folytatnak, amik felett néha elvesztik az uralmukat, és telítődik a LAN-juk, akkor a könyvelésen lehet, hogy nem fognak lelkesedni azért, hogy némi hálózati kapacitással segítsék ki a kollégákat.

A harmadik ok az adatszórás kérdése. A legtöbb LAN támogatja az adatszórást, és sok felsőbb rétegbeli protokoll alaposan ki is használja ezt. Ez megint nagy forgalmat generál, így egy rosszul megtervezett hálózaton igen sok felesleges adat fog áramolni, ami leterheli az egész rendszert. Ezen felül, ha egy eszköz meghibásodik, akkor folyamatos adatszórásos üzenetekkel (broadcaststorm) áraszthatja el, és így béníthatja meg a hálózatot.

Láthatjuk tehát, hogy ha különválasztjuk a logikai és fizikai topológiákat, akkor a hálózatunk egyrészt sokkal áttekinthetőbbé, másrészt sokkal költséghatékonyabbá válik. Ezen indokok hívták létre a virtuális helyi hálózatokat.

### A VLAN-okfelépítése

A VLAN-ok, azaz virtuális helyi hálózatok egy szórási tartományba<sup>1</sup> sorolnak olyan állomásokat, amelyek fizikailag különbözőekben vannak.

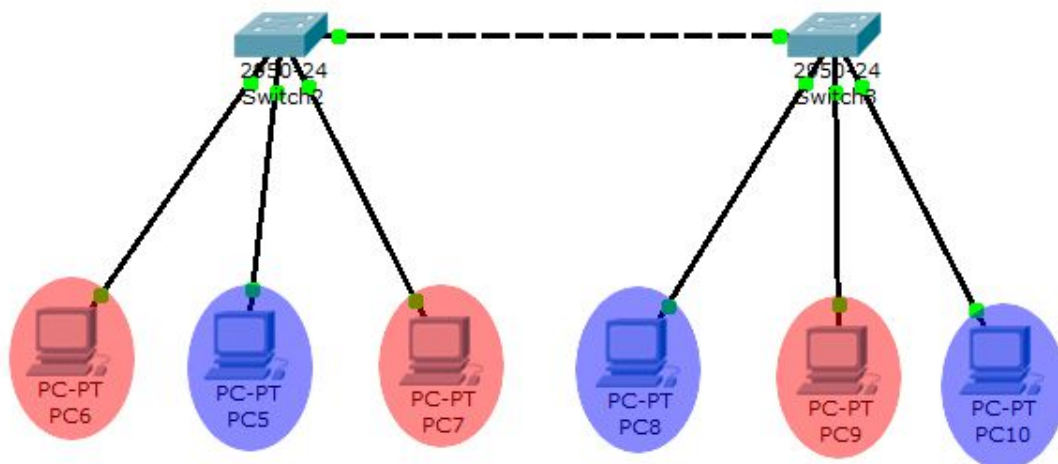
Ezzel a módszerrel tehát biztosítani tudjuk, hogy a fizikailag viszonylag távol levő állomások is egy LAN-hoz tartozhassanak. Az 1. ábrán egy példa is látható erre, ahol a különböző VLAN-okat más színekkel jelöltük. Két VLAN ismerhető fel, a piros és a kék.

Ahhoz, hogy a VLAN-ok helyesen működjenek, az egyes switch-ekben egy-egy táblázatot kell felállítani, hogy megmondják, hogy az egyes VLAN-okat melyik port(ok) segítségével lehet elérni (ez magában foglalja azt is, hogy egy porton keresztül akár több VLAN-t is elérhetünk). Ha egy üzenet érkezik, mondjuk az

---

<sup>1</sup> Szórási tartományon a hálózat egy olyan logikai felosztását értjük, amiben minden csomópont képes egymást elérni az adatkapcsolati rétegen keresztül üzenetszórás segítségével. Például az ugyan azon switchre kapcsolódó gépek ugyan azon szórási tartományba tartoznak.

egyik piros gépről, akkor a switch a piros gépek közül keresi ki a címzettet. Ebből következik az is, hogy a két VLAN között nincs átjárás, és ez megfelel a korábban elvárt követelményeknek is.

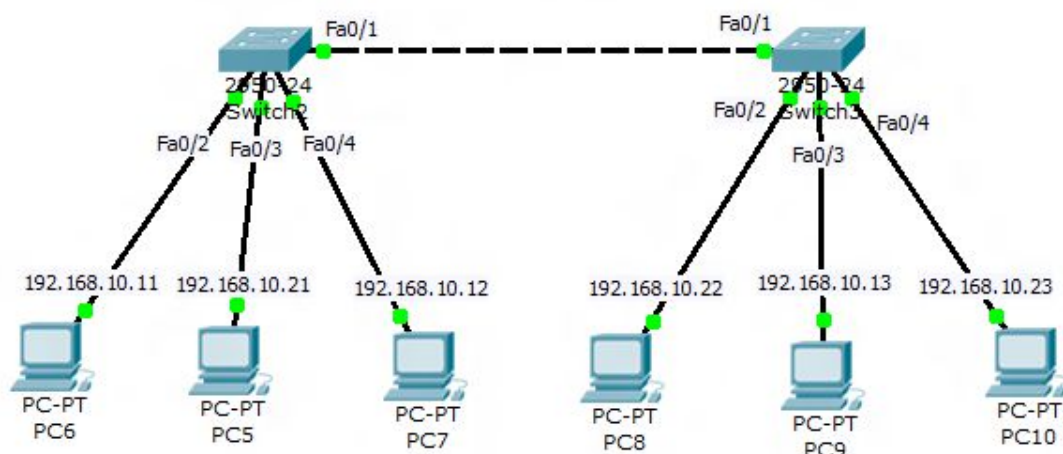


1. ábra, „piros” VLAN és „kék” VLAN

Eddig nem beszéltünk arról, hogy az egyes csomagokról hogyan mondjuk meg, melyik VLAN-hoz tartoznak. Eredetileg az Ethernet kereteknek nem volt semmilyen tartalékezője a VLAN azonosító számára. Így meg kellett változtatniuk az Ethernet csomagok fejrészét, és az új szabványt IEEE 802.1Q néven adták ki. Így a switchek az Ethernet keretből informálódnak arról, hogy az áthaladó csomag melyik VLAN-hoz tartozik, és így az előbbiek alapján merre kell tovább küldeni.

## VLAN-ok építése Packet Tracerben

A következőkben az első ábrán látott hálózatot fogjuk megépíteni, és konfigurálni a VLAN-okat. A hálózatunkat első lépésben konfiguráljuk a 2. ábrán látható módon. Meg kell jegyezni, hogy a gyakorlaton switcheket használunk, de ugyan az érvényes a hubokra is.



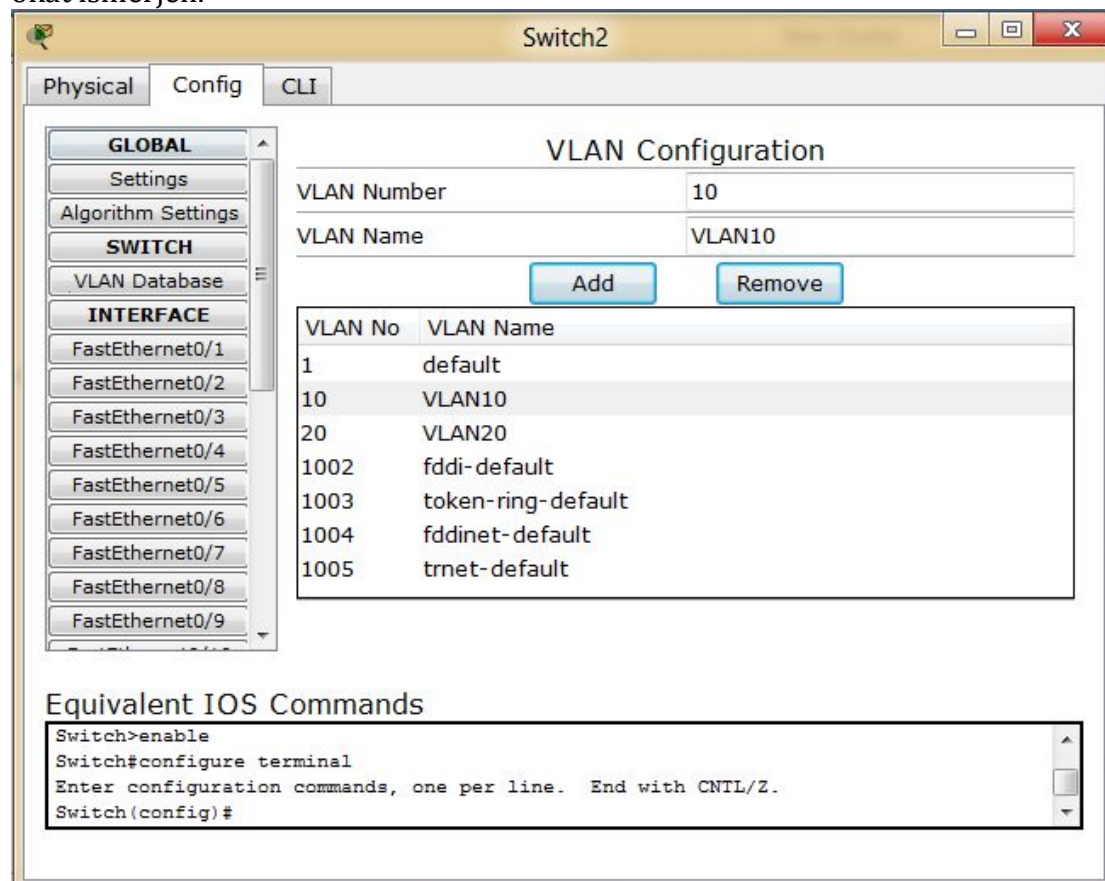
2. ábra, a beállítandó hálózat

Az egyes gépek IP címét az ábrának megfelelő módon állítsuk be (az alhálózati maszk mindenhol 255.255.255.0 legyen, az alapértelmezett átjárót pedig hagyjuk

üresen). Figyeljünk arra, hogy a megfelelő csatlakozók a megfelelő portokra kerüljenek (a FastEthernet jelölés helyett a rövidebb Fa jelölést használjuk). Ezek után a switchek fogják vezérelni, hogy melyik porton melyik VLAN-hoz tartozó eszköz van. A konfigurálást kezdjük a Switch2-vel, azaz rákattintva nyissuk meg az konfigurációs ablakot. A VLAN-t kétféleképp is konfigurálhatjuk: a Config fülön, vagy a CLI parancsain keresztül. Mindkét módszert megnézzük.

### Konfigurálás GUI-n keresztül

Az előbbihez kattintsunk a Config fülre, majd bal oldalon keressük meg a „VLAN Database” menüt. Ezzel tudjuk megmondani a switchnek, hogy milyen VLAN-okat ismerjen.



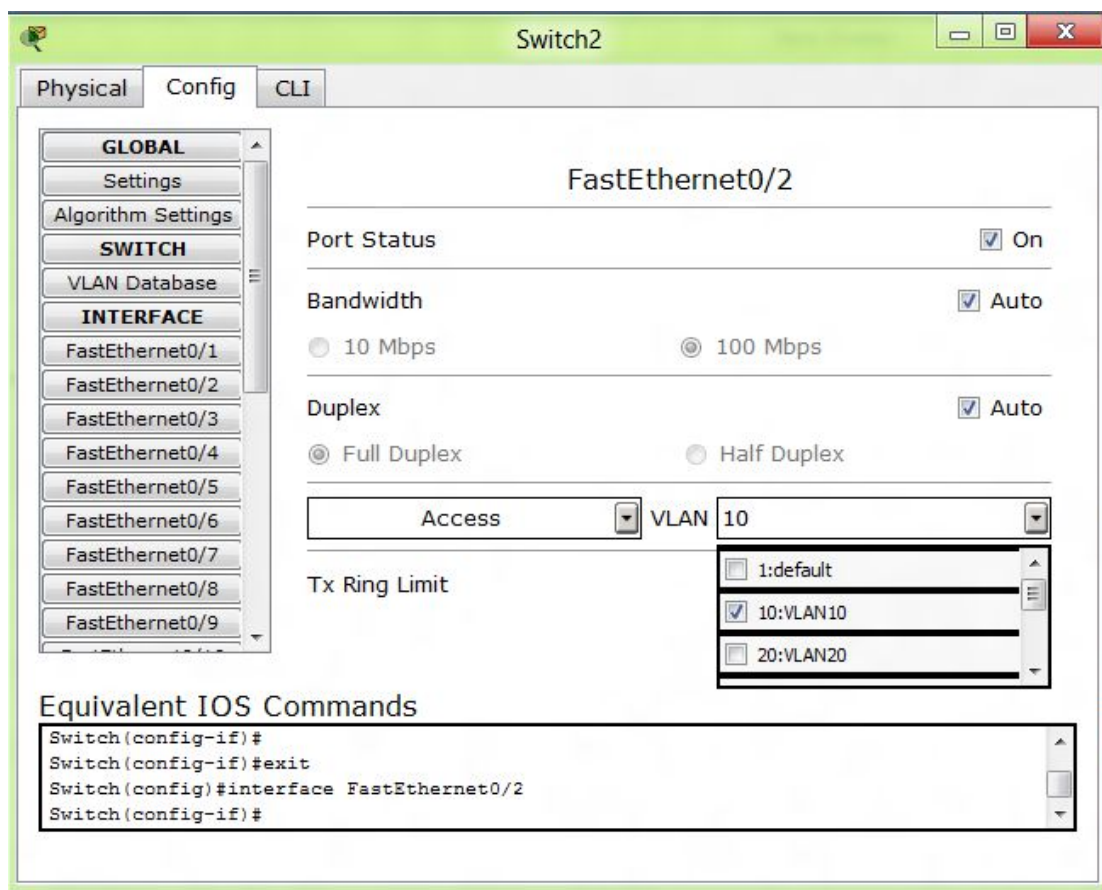
3. ábra, Switch2 konfigurációja

Itt két virtuális hálózatot fogunk hozzáadni. Az első azonosítója (VLAN Number) legyen 10, és a neve (VLAN Name) pedig „VLAN10”. Ugyan így a második azonosítója 20, és a neve VLAN20.

A következő lépés az, hogy megadjuk, hogy az egyes portokhoz melyik hálózat tartozik. Nem titkolt szándékunk, hogy a 192.168.10.1x tartományba tartozó gépek lesznek a VLAN10, a 192.168.10.2x gépei pedig a VLAN20 részei.

A 4. ábrán láthatjuk, hogy hogyan kell bekonfigurálni egy FastEthernet portot a switchen. Szintén a bal oldali listából kell kiválasztani a konfigurálandó interfészt, majd ezután a lenti módon kell beállítani. Ehhez hasonlóan állítsuk be az Fa0/2, Fa0/4 interfészeket a switch2-n, és az Fa0/3-at a switch3-on. A többi csatlakozó, azaz (Fa0/1 switch2-n és Fa0/2, valamint Fa0/4 a switch3-on) a VLAN20-at kapja.





4. ábra, a FastEthernet0/2 VLAN konfigurálása

A következő ábrán egy összefoglalást láthatunk a konfigurációról. Itt megfigyelhető, hogy mindkét VLAN egy alhálózatban van. Szükséges feltétel, hogy egy adott VLAN (pl. VLAN10) minden gépe egy alhálózatban legyen, mert különben nem tudnának egymással kommunikálni. Viszont minden egyes VLAN alkothat külön-külön alhálózatot, ilyenkor viszont amiatt nem tudnak kommunikálni egymással, mert külön alhálózatban vannak.

Állomás neve	Állomás IP címe	Melyik Ethernet portra csatlakozik	Melyik switchre csatlakozik	VLAN neve
PC6	192.168.10.11	Fa0/2	Switch2	VLAN10
PC7	192.168.10.12	Fa0/4	Switch2	
PC9	192.168.10.13	Fa0/3	Switch3	
PC5	192.168.10.21	Fa0/3	Switch2	VLAN20
PC8	192.168.10.22	Fa0/2	Switch3	
PC10	192.168.10.23	Fa0/4	Switch3	

Amennyiben a fentiekkel készen vagyunk, a VLAN-unk már majdnem teljesen működőképes. Már csak annyit kell megtenni, hogy mindkét switchnél a FastEthernet0/1 konfigurációját megnyitjuk a bal oldali listából, és az „Access”-t átállítjuk „Trunk”-ra. A Trunk (magyar zsargonban „trönk”) egy olyan összeköttetés két switch között, amely egyszerre több VLAN forgalmát is át tudja engedni. Tehát a két switchet úgy kell bekonfigurálnunk, hogy egymás felé több

VLAN forgalmát is át tudják engedni. A másik mód, az „Access” a trónk ellentéte, mivel itt csak egy VLAN-t adhatunk meg, így ez csak azokat a csomagokat fogja áteresztetni, amelyek arra a virtuális hálóra mennek.

### Konfigurálás CLI-n keresztül

Itt is hasonló lépéseket kell végrehajtanunk, mint az előzőekben. Először is, nyissuk meg az egyik switch konfigurációs ablakát, majd váltsunk a CLI földre. A VLAN Database-t fogjuk először feltölteni. Mindenek előtt, viszont privileged módba kell lépnünk, ezt az enable paranccsal tehetjük meg:

```
Switch>enable
```

Ezután belépünk a konfigurációs módba:

```
Switch#configure terminal
```

Itt a következő parancsokkal tudjuk hozzáadni a VLAN10-et:

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name VLAN10
```

Majd az exit paranccsal kilépünk a VLAN konfigurációból:

```
Switch(config-vlan)#exit
```

Ezek után ismételjük meg a folyamatot VLAN20-ra, illetve a másik switchen is VLAN10-re és VLAN20-ra!

Amint készen lettünk a fenti parancsok beírásával, konfigurálni kell a FastEthernetportokat is. Hasonlóan lépünk be az egyik router CLI felületére, privileged módba, és azon belül is konfigurációs módba:

```
Switch>enable
```

```
Switch#configure terminal
```

Ezek után lépünk be az első (munkaállomáshoz kapcsolódó) interfész konfigurációs módjába:

```
Switch(config)#interfaceFastEthernet 0/2
```

Majd a következő utasításokkal be tudjuk állítani, hogy ezen a porton a 10-es VLAN-ra, azaz a VLAN10-re érkező csomagokat továbbítsa.

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport access vlan 10
```

Itt az első utasítás az „Access” és „Trunk” módok közötti választás, ahol Access-t választunk, mivel nem trónkként akarjuk kezelni az adott portot. Ismételjük meg ezeket a lépéseket minden szükséges portra.



Miután ezekkel megvagyunk, az `exit` paranccsal innen is kiléphetünk, és legvégül elvégezhetjük mindkét switchre a trónkók konfigurálását. Ezt a következő utasítássorozat adja meg:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

### Összefoglalás

Még egyszer összefoglalva tehát az alábbi lépéseket kell végrehajtani mind CLI-s, mind pedig a GUI-s konfiguráláskor:

1. A hálózatot rakjuk össze, fizikailag, azaz rakjuk be az eszközöket, és az azokat összekötő vezetékeket.
2. Töltsük ki a VLAN Database-t azokkal a VLAN-okkal, amelyek áthaladhatnak a switchen.
3. Az egyes állomások felé menő FastEthernet portokat is állítsuk be megfelelően, azaz mindegyikre jelöljük be, hogy melyik VLAN hálózat csomagjai haladhatnak keresztül.
4. A két switchet összekötő portokat állítsuk be trónkóknak.

### Beugró kérdések

1. Mi a LAN definíciója?
2. Milyen előnyei lehetnek a VLAN-oknak?
3. Mit definiál az IEEE 802.1Q szabvány?
4. Milyen tulajdonságnak kell feltétlenül teljesülnie ahhoz, hogy két számítógépet egy VLAN-ba tudjunk helyezni?
5. Mire szolgál a VLAN Database?
6. Mit jelent a Trunk?
7. Mire szolgál a switchport access vlan 10 utasítás?
8. Mire szolgál a switchport mode trunk utasítás?
9. Melyik lépést NEM kell végrehajtani VLAN konfigurálásakor?
10. Melyik parancs szolgál egy Ethernet port Access módban a 10-es azonosítójú VLAN-ra állítására?