

Feszítőfa protokoll (STP)
Vezetéknélküli hálózatok (WLAN)
Bordé Sándor

Tartalomjegyzék

Bevezetés.....	3
Redundáns hálózat	4
Feszítőfa protokoll.....	5
Gyökérponti híd	5
Választási folyamat	6
Gyökérponti port (root).....	7
Kijelölt port (designated)	7
Lezárt port (closed)	7
STP tervezése	7
Feszítőfa egy hierarchikus hálózatban	9
Utasítások.....	10
STP konfigurálása Packet Tracerben	11
Vezeték nélküli hálózat felépítése	13
Hostok konfigurálása	13
Hozzáférési pont konfigurálása	14
Laptopok konfigurálása	15
Modul beépítése.....	15
Konfiguráció	16
Videós segédletek.....	17
STP	17
WiFi	17

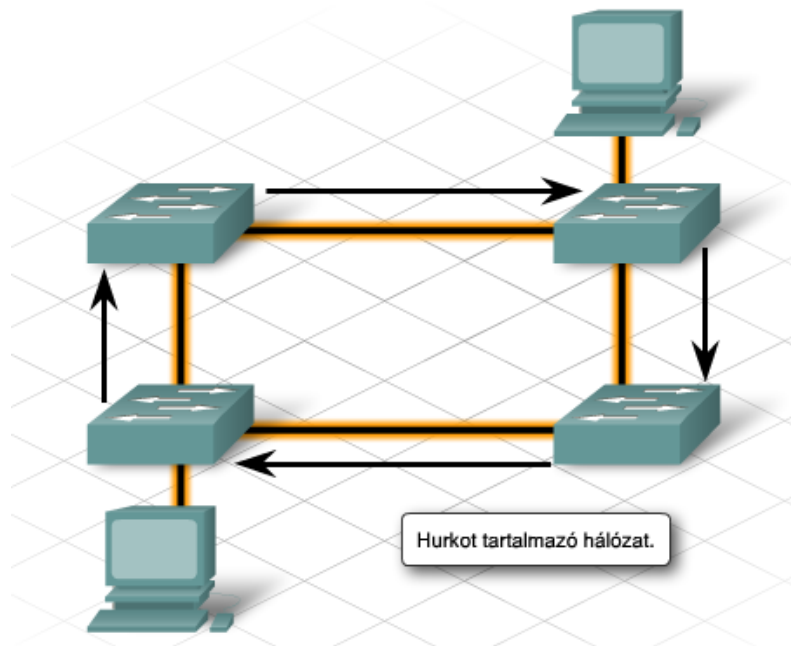
Bevezetés

Az előzőekben megnéztük, hogyan lehet egy jól strukturált helyi hálózatot megtervezni, felépíteni és konfigurálni. Azonban bármikor előfordulhat, hogy egy kapcsolat meghibásodik, ilyenkor minél gyorsabban egy másik kapcsolatnak kell átvenni a helyét. Ez redundáns kapcsolatok kialakításával érhető el legkönnyebben, ekkor viszont újabb problémák merülnek fel. A jegyzet első része az **STP (Spanning-Tree Protocol)** alapjairól fog szólni, amely a fent említett kihívásokat hivatott megoldani.

Redundáns hálózat

Napjainkban egyre nagyobb mértékben támaszkodunk a számítógépes hálózatokra. A vállalatok és a felhasználók elvárják az állandó rendelkezésre állást. Ehhez olyan hálózati topológiát kell terveznünk, amely egy-egy eszköz meghibásodása esetén továbbra is működőképes marad.

A hibátűrés redundanciával érhető el legkönnyebben, azaz a nagy megbízhatóságú hálózatokba a szükségesnél több útvonalat és készüléket helyezünk el. Egy így kialakított topológiában egyetlen elem meghibásodása nem okoz teljes körű leállást. Amint egy eszköz vagy vonal meghibásodik egy másik eszköz vagy útvonal veszi át a helyét.



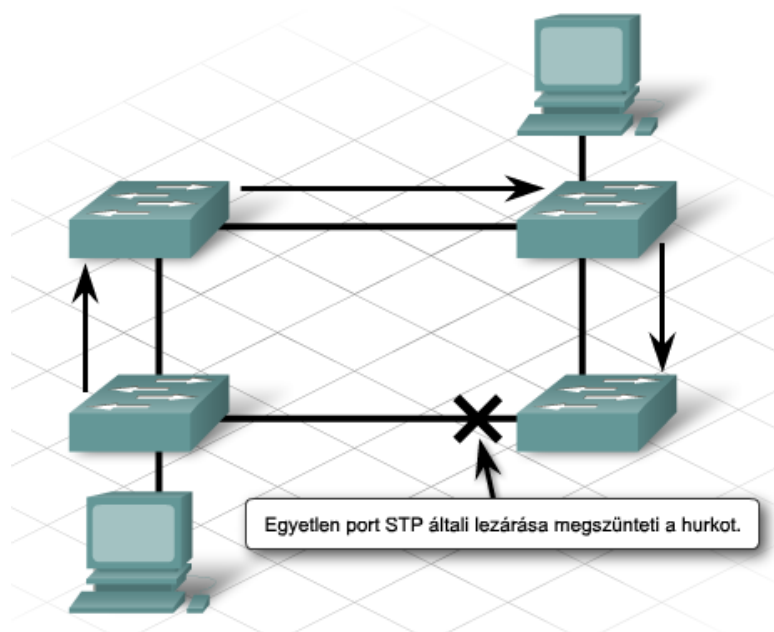
Egy STP nélküli hálózat

A redundáns kapcsolatok viszont felvetnek egy újabb kérdést: irányítási hurok keletkezhetnek a hálózatban, amelyek szórásai viharokhoz és így végső soron a szolgáltatások leállításához vezethetnek. A broadcast kereteket a switchek az összes portjukon kiküldik, (kivéve amelyen beérkezett). A redundáns vonalakon keresztül a switchek újra és újra megkapják egymástól a szórásai üzeneteket. Ezt a jelenséget szórásai viharoknak (*broadcast storm*) nevezzük, és mindaddig folytatódik, amíg egy eszköz ki nem száll a hálózat működéséből. A switchek és a végponti eszközök egyre terheltebbé válnak a szórásos keretek feldolgozása miatt. A túlterheltség miatt az eszközök nem lesznek képesek a felhasználói adatforgalom továbbítására. Ezért a hálózat látószólag leáll vagy drasztikusan lelassul.

Feszítőfa protokoll

Az irányítási hurkok azért jönnek létre, mert a redundáns kapcsolók nem foglalkoznak egymás jelenlétével. Ennek kiküszöbölésére fejlesztették ki a feszítőfa protokollt. Segítségével ki tudjuk használni a redundáns kapcsolatok előnyeit azok hátrányai nélkül. A STP célja egyrészt egy hurokmentes topológia kialakítása, másrészt pedig szakadás esetén a redundáns tartalék kapcsolat mielőbbi felélesztése.

Az STP egy minimális konfigurálást igénylő, lényegében önállóan működő protokoll. Azok a switchek - melyeken engedélyezett az STP - az első bekapcsoláskor ellenőrzik a kapcsolt hálózatok esetleges hurkait. Hurok észlelésekor letiltják az érintett portok valamelyikét, míg a többi porton aktív marad a kerettovábbítás.



Egy hálózat STP-vel

Gyökérponti híd

A problémát az okozta, hogy két hálózati szegmens között kettő vagy több fizikai útvonal is létezik. Az STP feladata, hogy egy időben csak egy útvonal legyen használatban. Az STP a hálózat összes kapcsolóját egy faszerkezetű, kiterjesztett csillag topológiájú hálózattal kapcsolja össze. Ezek a kapcsolók folyamatosan ellenőrzik a hálózatot annak érdekében, hogy ne alakulhassanak ki hurkok és a portok megfelelően működjenek.

A topológia csúcán az ún. gyökérponti híd (*root bridge*) áll. Hogy melyik switch lesz az, egy választási folyamat során dől el. Minden hálózatban csak egy gyökérponti híd létezik, melyet a kapcsolók a hídazonosító (*bridge ID, BID*) alapján választanak ki. Minél kisebb a hídazonosító, annál magasabb a prioritás, tehát a gyökérponti híd a legkisebb hídazonosítóval rendelkező kapcsoló lesz. A hídazonosító alapértelmezett értéke **32,768**. Ha két vagy több kapcsoló hídazonosítója azonos, akkor a legkisebb MAC-című kapcsoló lesz a root bridge.

Választási folyamat

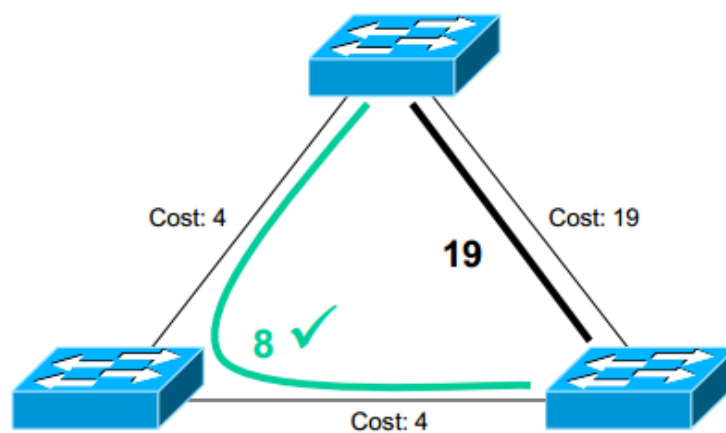
A switchek egymással **BPDU (Bridge Protocol Data Unit)** keretekkel kommunikálnak, melyekkel feltérképezik a hálózatot és megtalálják a root bridge felé vezető összes útvonalat.

Protokoll azonosító	Verzió	Üzenettípus	Jelző bitek	Gyökérponti híd azonosító	Gyökérútvonal költség
Hídazonosító	Portazonosító	Üzenet élettartam	Maximális élettartam	Hello időtartam	Továbbítási késleltetés

a BPDU keret felépítése

A folyamat elején minden eszköz úgy veszi, hogy ő a root bridge és elkezd hirdetni saját magát a hálózaton. Ha érkezik hozzá egy BPDU, akkor megvizsgálja, hogy a kapott vagy az általa hirdetett root id a jobb (azaz kisebb). Ha a kapott jobb, akkor elfogadja azt és többé nem hirdeti a sajátját. Egy idő után mindenki értesülni fog arról, hogy ki lett a gyökérponti híd.

Miután megtörtént a választás, a gyökérponti híd veszi át az irányítást és ő vezényli a továbbiakat. A célja az lesz, hogy őt mindenki a legrövidebb úton érje el.



költségek a hálózatban

Ehhez először kiszámítja minden switchhez minden odavezető útvonal költségét. Egy útvonal költsége az útvonalat alkotó szakaszok költségeinek összege (4. ábra). Egy szakasz költségét szabványban lefektetett értékek határozzák meg, ami összefüggésben áll az átviteli közeg sávszélességével (Ezek a költségek az 1. táblázatban láthatók). Ezek alapján minden switch eldönti, hogy ő melyik útvonalon keresztül jut el a root bridgehez, ez lesz a root port (gyökérponti port).

A gyökérponti port kiválasztása is egy többlépcsős döntési folyamat eredménye lesz:

1. Az a port lesz a gyökérponti port, ami a root felé vezető legrövidebb út felé néz.

- Ha több azonos költségű út is van, akkor ezek közül azt választja, amelyik szomszédjának kisebb a hídazonosítója (**Bridge ID**)
- Ha több olyan útvonal is van, amelyik azonos költségű és azonos a BID, akkor a legkisebb port ID-t választja.

1. táblázat Költségek

Sávszélesség (Mbps)	4	10	16	45	100	155	622	1000	10000
STP költség	250	100	62	39	19	14	6	4	2

A szükséges portok lezárása után kialakul a hálózat feszítőfája. Ez egészen addig állandó marad, amíg valami változás nem történik a hálózatban (meghibásodás vagy eszköz cseréje). Ekkor a gyökérponti híd felel azért, hogy újra optimális útvonalak legyenek aktívak. Az STP fa kialakulása után minden switchnek háromfajta portja lesz: *gyökérponti port*, *kijelölt port* és *lezárt port*.

Gyökérponti port (root)

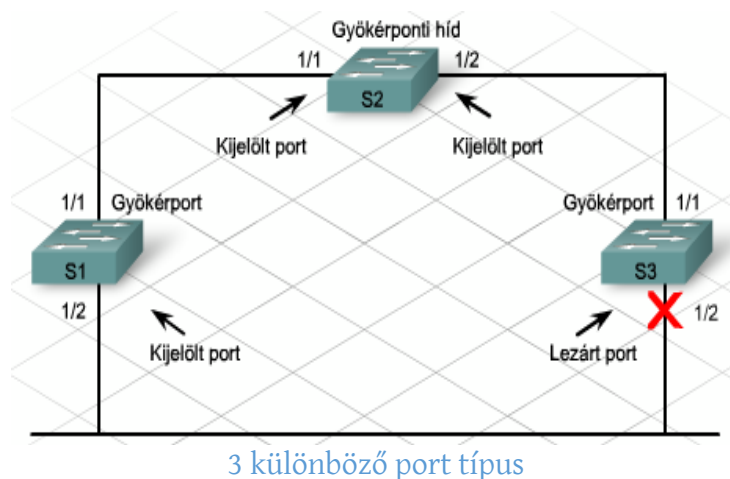
Egy kapcsoló azon portja amelyből a legkisebb költségű útvonal vezet a gyökérponti kapcsolóhoz. A kapcsolók a gyökérponti switchhez vezető útvonal összeköttetései-
nek eredő költségértéke alapján határozzák meg a legkisebb költségű útvonalat.

Kijelölt port (designated)

Egy hálózatszegmens azon portja amelyen át az adott szegmens és gyökérponti híd közötti adatforgalom halad, de nem tartozik a legkisebb költségű útvonalhoz.

Lezárt port (closed)

Olyan port, mely nem továbbít adatforgalmat.



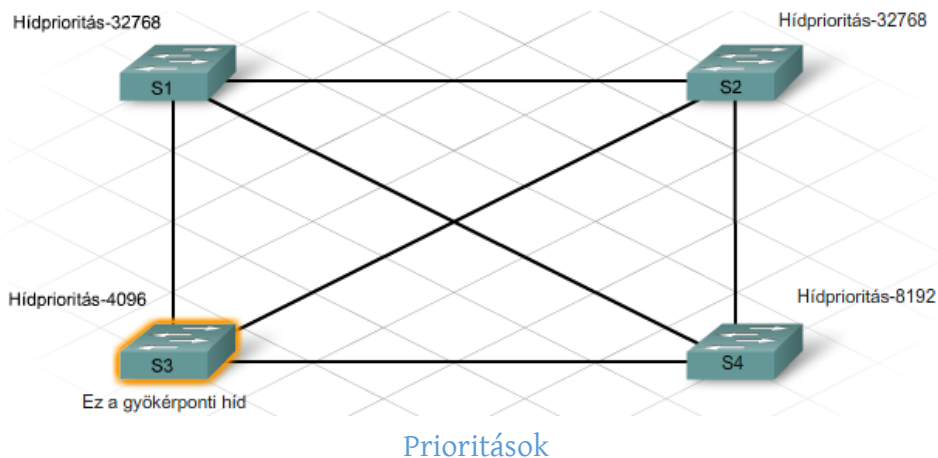
STP tervezése

Egy helyi hálózatban a legkisebb hídazonosítóval rendelkező switch lesz a gyökérponti híd, egyenlőség esetén pedig a legalacsonyabb MAC cím dönt. Azonban egy hálózatban kezdetben minden switchnek megegyezik a bridge IDja, tehát egy automatikus elrendezés lép életbe. Ez azonban nem biztos (sőt, nagyon valószínű), hogy a

legoptimálisabb kialakítást jelenti. Ezért az STP konfigurálása előtt a hálózati rendszergazda elemzi és teszteli a hálózatot, hogy megtalálja a legalkalmasabb switchet a gyökérponti híd szerepére.

Általában egy központi elhelyezkedésű kapcsoló alkalmas leginkább a gyökérponti híd szerepére. A hálózat szélén elhelyezkedő gyökérponti híd ugyanis azt eredményezheti, hogy az adatok hosszabb útvonalon jutnak el a célállomásig, mintha a gyökérponti híd központi elhelyezkedésű lenne.

Mivel a választási folyamat automatikus, ezért csak úgy tudjuk befolyásolni a választás eredményét, hogy a kívánt switchnek alacsony hídprioritást állítunk be.



Feszítőfa egy hierarchikus hálózatban

A gyökérponti híd, a gyökér-, a kijelölt- és a lezárt portok megválasztása után a gyökérponti híd két másodpercenként BPDU csomagokat küld a hálózaton keresztül minden kapcsolónak. Az STP folyamatosan figyeli ezeket a BPDUkat az összeköttetés hibáinak és újabb hurkok keletkezésének elkerülése érdekében.

Ha egy összeköttetés meghibásodik, akkor az STP újból elvégzi a számításokat. Ennek eredményeként:

- Bizonyos lezárt portokat továbbító módba helyez
- Bizonyos továbbító portokat lezárt állapotba helyez
- Új feszítőfát készít a hurokmentes hálózat fenntartása érdekében

Az STP nem azonnal reagál a változásokra. Ha egy összeköttetés meghibásodik, akkor az STP észreveszi a hibát és kiszámolja a legjobb útvonalakat a hálózaton. Ez a számítás akár 30-50 másodpercet is igénybe vehet. Ezen idő alatt nincs adatforgalom az újraszámításban érintett portokon.

Bizonyos felhasználói alkalmazások esetében ez várakozás időtúllépést eredményezhet, ami a termelékenység és ezzel együtt a bevétel csökkenését eredményezheti. Gyakori STP újraszámolások negatív hatást gyakorolnak a hálózat működésére.

Utasítások

A kialakult feszítőfa tulajdonságainak listázása:

```
Switch# show spanning-tree [detail | summary | vlan x ]
```

Üzem mód beállítása (normál / gyors)

```
Switch(config)#spanning-tree mode pvst | rapid-pvst
```

Hídprioritás beállítása (az érték 0-61440 között lehet, 4096-os lépésekkel):

```
Switch(config)#spanning-tree vlan 1 priority 4096
```

Vagy:

```
Switch(config)#spanning-tree vlan 1 root [ primary | secondary ]
```

Hozzáférési portok gyorsstovábbító üzemmódba állítása:

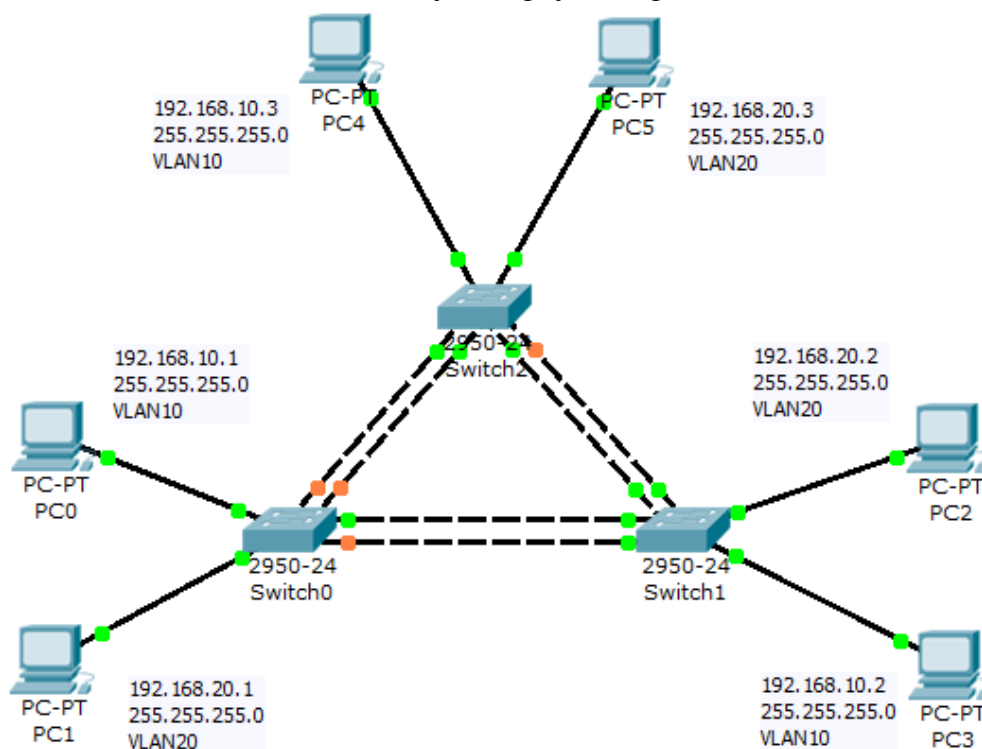
```
Switch(config)#spanning-tree portfast default
```

interfészenként:

```
Switch(config-if)#spanning-tree portfast
```

STP konfigurálása Packet Tracerben

Építsük fel a következő hálózatot, majd vizsgáljuk meg:



Láthatjuk, hogy a port színei különböző színnel villognak. A kapcsoló elindítása után minden port végighalad a következő négy állapot sorozatán: lezárt, figyelő, tanuló és továbbító. Az ötödik, letiltott állapot jelzi, hogy a rendszergazda a portot le-tiltotta.

Megfigyelhető, hogy a *Switch0* és a *Switch2* között a *Switch0* mind a két portja *Lezárt* állapotban van: borostyán sárgán világít, az adatkereteket eldobja. A *Switch1* összes portja továbbító: zölden villogó, továbbítja a kereteket. Valószínű, hogy a *Switch1* lett a gyökér híd (megj: *otthoni kialakítás során nem biztos, hogy ugyanez a végeredmény várható*), ellenőrizzük le. Nyissuk meg a *Switch1* konfigurációs ablakát, majd váltsunk át a CLI földre.

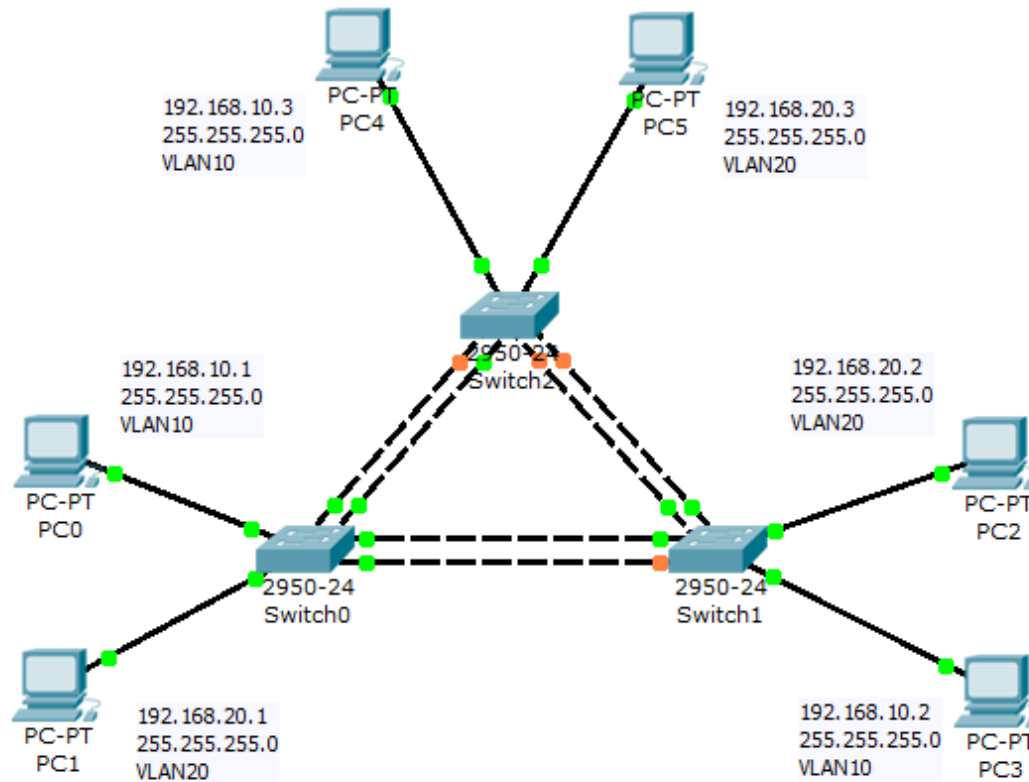
```
Switch>enable  
Switch#show spanning-tree
```

A parancs kiadása után láthatjuk a költségeket, ami mind a 4 interface esetében 19 (a 100Mbps kapcsolat miatt). Megfigyelhetjük mindhárom VLAN-hoz tartozó prioritásokat (VLAN10, VLAN20, illetve VLAN1 a switchek közötti trunk miatt) valamint azt, hogy ez a gyökérponti híd: „*This bridge is the root*”. Mivel ez a gyökérponti híd, az összes csomag keresztülhalad ezen a switchen. Változtassuk meg, hogy a *Switch0* legyen a gyökér híd.

Lépünk a *Switch0* konfigurációs ablakába, majd váltsunk át a CLI földre:

```
Switch>enable
Switch#configure terminal
Switch(config)#spanning-tree vlan 1,10,20 priority 4096
Switch(config)#end
```

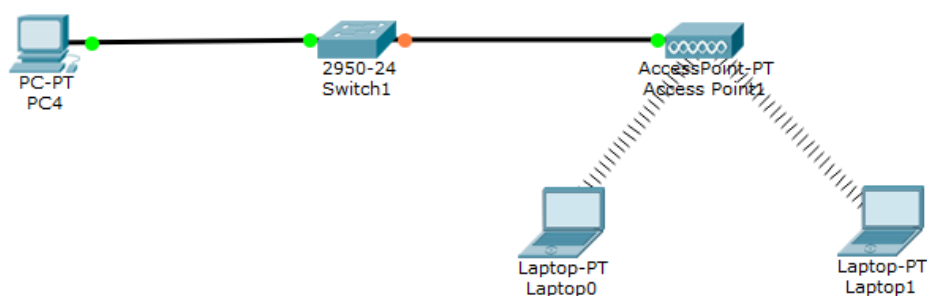
Beállítottuk mind a 3 VLAN-hoz tartozó prioritást a legkisebbre, az STP újból elvégzi a számításokat, majd a központi híd a *Switch0* lesz. Végeredmény:



Vezeték nélküli hálózat felépítése

Az előző fejezetekben megismertük a vezeték nélküli számítógépes hálózatok elméleti alapjait. Most fel fogunk építeni egy egyszerű hálózatot, amelyben mindössze egy hozzáférési pont van. Ehhez kapcsolódik két laptop, illetve egy switch, amihez egy harmadik eszköz (PC) csatlakozik. A hálózati topológia a következő ábrán látszik.

Ahogy a képen is látható, az *AccessPoint-PT* típusú hozzáférési pontot használjuk.



az elkészítendő hálózat

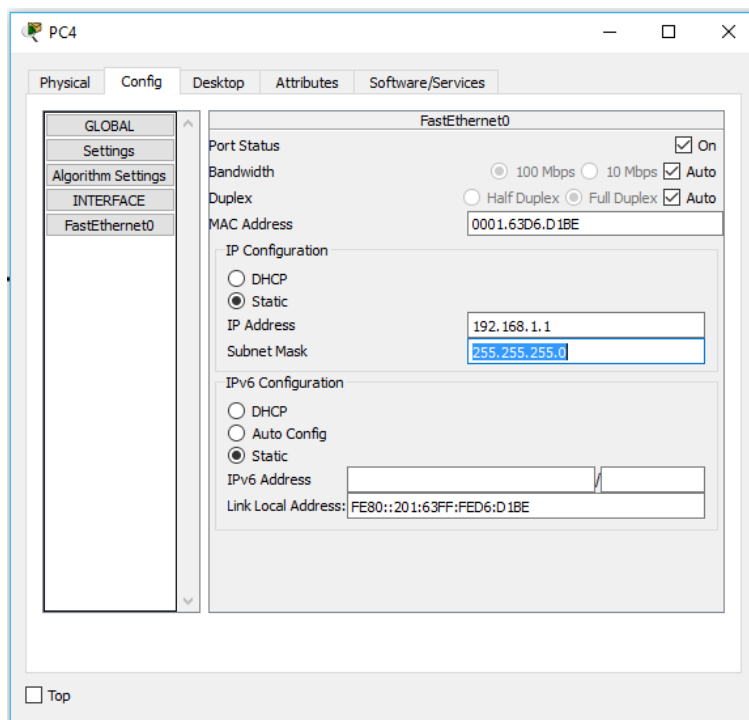
Ezen kívül két laptop csatlakozik a hálózatra. A feladatban mindenhol statikus IP cím kiosztást fogunk használni. Ez rendre 192.168.1.1 a PC4-en, 192.168.1.2 a Laptop0-n, és 192.168.1.3 a Laptop1-en. A hálózati maszk mindenhol az alapértelmezett 255.255.255.0 érték legyen.

Hostok konfigurálása

A hostok összekötése legegyszerűbben úgy oldható meg, ha az összeköttetés típusánál az korábban említett villámjelre kattintunk. Ha ezután sorban, egymás után rákattintunk a két összekötni kívánt gépre, akkor a program kiválasztja számunkra a megfelelő összeköttetést.

A hostokat úgy tudjuk konfigurálni, hogy bal egérgombbal rákattintunk az eszközre, majd a felugró ablakban kiválasztjuk a *Config* fület. Bal oldalt kategorizálva vannak az elérhető beállítások, minket most a *FastEthernet0* fog érdekelni.

Itt jelenleg csak a középen található „IP Configuration” című blokkra van szükségünk. Első lépésben, állítsuk *Staticra* az IP címet (ha eleve így volt, akkor ez a lépés kihagyható). Ezután az *IP Address* mezőbe írjuk be a kívánt IP címet. Ha átkattintunk másra, akkor a PT kitölti a „Subnet mask” mezőt az alapértelmezett értékkel. Mivel a feladat most az alapértelmezett, 255.255.255.0 értéket kéri, ezzel nincs tennivalónk. Az alábbi képen látható a konfiguráció eredménye.



11. ábra - Host konfiguráció

Hozzáférési pont konfigurálása

Az elméleti ismertető alapján tudhatjuk, hogy két dolgot kell beállítanunk az AP-nél:

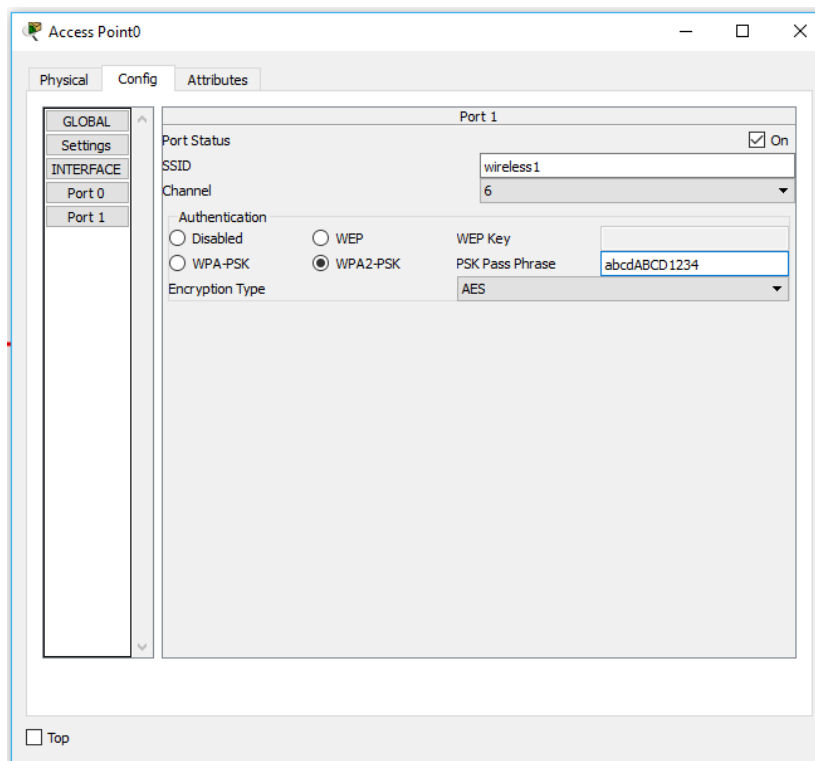
- Az SSID-t, tehát egy azonosítót, amivel a hálózatunknak egy egyedi nevet adunk
- A csatornát, hogy ne interferáljon más hálózatokkal

Ez így viszont még nem a teljes igazság. Korábban elhangzott, hogy nem biztonságosak ezek a hálózatok, hiszen a jel nem egy zárt kábelben halad, hanem a levegőn keresztül. Ezért az idők során különböző titkosítási módok fejlődtek ki. A legrégebbi a WEP (**W**ired **E**quivalent **P**rivacy), amelyet a vezeték nélküli hálózatok biztonságával egyenértékűnek terveztek, viszont elég komoly biztonsági rések voltak benne, így könnyen feltörhető lett. Ezért ma nem ajánlatos a használata.

Egy erre adott gyors válasz volt a WPA, amely már biztonságosabb elődjénél. A legújabb technológia viszont a WPA2, amelyet jelenleg ajánlatos használni. Mi is ezt követjük. Ezen kívül még be lehet állítani a biztonsági protokollokat is, ezek lehetnek az AES, illetve a TKIP. Az előbbi a fejlettebb, és ezt ajánlatos használni.

A lenti ábrán látszik a hozzáférési pontunk konfigurációja, amely összefoglalva:

- A „wireless1” SSID-t kapta
- A 6-os csatornát használja
- WPA2-PSK titkosítást használ, AES biztonsági protokollal, és kötelező hozzá egy jelszót is megadni



1. ábra - 3. ábra: a hozzáférési pont konfigurációja

Laptopok konfigurálása

A laptopok esetén három dolgot kell megtennünk:

- Beépíteni egy vezeték nélküli hálózati csatlakozásra alkalmas modult
- Az AP-nak megfelelően konfigurálni magát az előbb beépített interfészt
- Beállítani a kívánt IP címet (a vezetékes géphez hasonlóan)

Modul beépítése

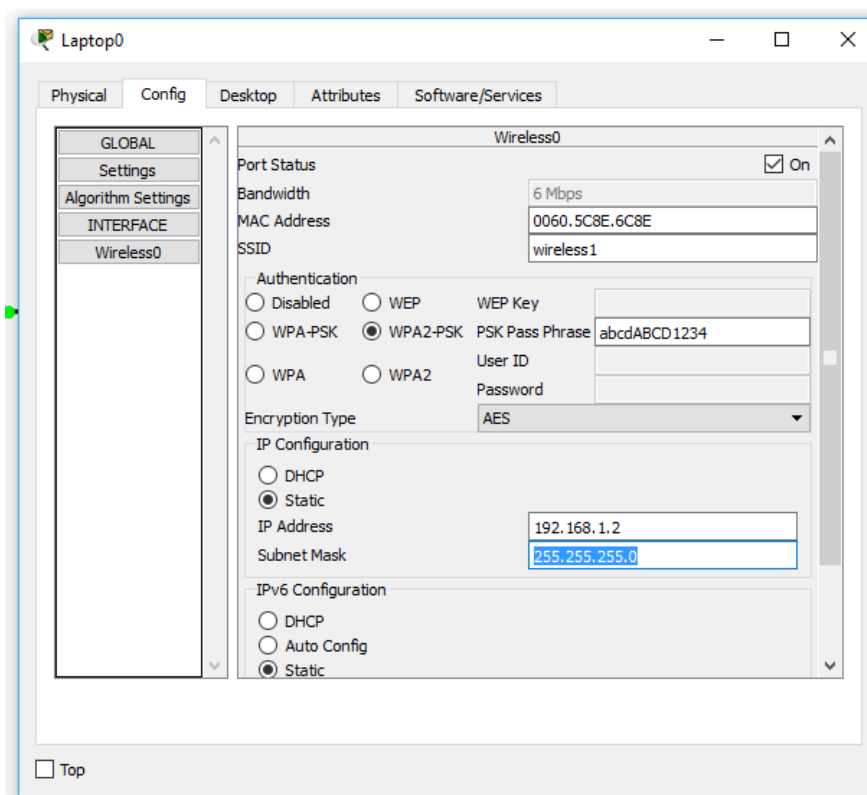
Egy modul beépítése egyszerűen megoldható. Nyissuk meg a laptop konfigurációs ablakát, majd a „Physical” fülön kapcsoljuk ki az eszközt, távolítsuk el a jelenlegi Ethernet modult (kattintsunk bal egérgombbal és a gombot nyomva tartva húzzuk rá a listára a modult), majd válasszuk ki a **PT-LAPTOP-NM-1W** interfészt, és építsük bele a laptopba. Ezután kapcsoljuk vissza az eszközt. Ha ezzel végeztünk, az „Config” fülön az eddigi *FastEthernet* port helyett megjelenik egy *Wireless* nevű interfész. Itt tudjuk megadni a vezeték nélküli hálózat adatait.

Konfiguráció

Ez a lépés is igen egyszerű, hiszen az előbb beállított hozzáférési pont beállításait kell alkalmazni minden egyes hozzá csatlakozó kliensre is. Tehát:

- Az SSID-t állítsuk be „**wireless1**”re
- A titkosítás legyen WPA2-PSK, AES titkosítási protokollal, illetve „abcdABCD1234” jelszóval.
- Alul, az *IP Configuration* részben kattintsunk a „*Static*” opcióra, és az *IP Address* mezőben adjuk meg a laptop IP címét, alatta pedig hagyjuk alapértelmezetten a maszkot 255.255.255.0 értéken.

Az alábbi ábrán látható az előbb leírt folyamat eredménye. Amennyiben ezekkel készen vagyunk, az ötödik ábrán látható módon kell a hálózatnak kinéznie.



12. ábra - az eszköz konfigurációja

Videós segédletek

STP

https://youtu.be/jgs1zeGT_fY

<https://youtu.be/Rj3OyJYQu7c>

WiFi

<https://youtu.be/ppbDkPmPHjA>

<https://youtu.be/WXG7kUYmFmA>

<https://youtu.be/a0qLqqLJcOk>