

Tavaszi

2017

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software Engineering

Számítógép-hálózatok 3. gyakorlat

Hálózatépítés alapok

Vezetéknélküli hálózatok (WLAN)

Bordé Sándor

Tartalomjegyzék

Bevezetés 3

Elméleti háttér 3

Host.....	3
Switch.....	3
Router	4
AP (Access Point)	4
Gateway (Átjáró).....	4
IP címek.....	4
IPv4.....	5
Különleges IP címek.....	5
PING.....	5
Traceroute.....	5
ICMP	6
Beágyazódás (encapsulation)	6

Packet Tracer 7

A Packet Tracer felülete	7
A zöld színnel keretezett rész – a munkaterület	7
A kék színnel keretezett rész – hálózati eszközök.....	7
A piros színnel keretezett rész – „toolbox”	7
A sárga színnel keretezett rész – üzenetek.....	8
Eszközök vizsgálata	8
Szimuláció.....	8
Gombok és jelentésük	9
Event list	9
Csomag részletei	10
Hasznos tudnivaló	10

A vezeték nélküli technológia..... 11

Áttekintés	11
Infravörös	11
Rádiófrekvencia.....	12
Előnyök és korlátok.....	12
A vezeték nélküli hálózatok típusai és kötöttségei.....	12
WPAN.....	13
WLAN	13
WWAN	13

Vezeték nélküli helyi hálózatok (WLAN)..... 13

Szabványok.....	13
WLAN összetevői.....	13
Hozzáférési pont (AP)	13
Vezeték nélküli kliensek (STA)	14
Vezeték nélküli híd.....	14
Antennák.....	14
SSID	14
WLAN kiépítési módok.....	14
Ad-hoc.....	14
Infrastruktúra mód	14
Csatornák.....	15
A hálózat felépítése.....	15
Hostok konfigurálása	16
Hozzáférési pont konfigurálása.....	16
Laptopok konfigurálása.....	17
Modul beépítése	17
Konfiguráció	18

Beugró kérdések

Bevezetés

A mai gyakorlat témája a *Packet Tracer* nevű program használata és egy modellezett hálózati infrastruktúra elemzése lesz, illetve elkezdjük az OSI modell részletesebb megismerését a WiFi áttekintésével.

A *CISCO Packet Tracer* egy hasznos hálózati szimulációs program, mely segítségével megfigyelhetjük a hálózatok működését, kipróbálhatunk különböző eseteket. Segítségével szimulálhatjuk, vizualizálhatjuk a hálózatokat.

A program csak *CISCO Networking Academy* oktatói és hallgatói számára érhető el. Ezen kívül elérhetővé tettük a Számítógép hálózatok kurzus hallgatói számára is, letölthető a Coospaceről.

Fontos! A program nem terjeszthető, valamint nem szabad nyilvánosan elérhetővé tenni semmilyen formában (tehát nem szabad feltölteni pl. Dropboxra, Google Driverre, saját tárhelyre, emailben elküldeni...)!

Elméleti háttér

A *Packet Tracer* használatának megértéséhez szükség van néhány alapfogalom ismeretére. A ebben a jegyzetben mindegyik eszközről csak a legszükségesebbeket írtuk le, ami kell a megértéshez. Ha valakit részletesebben érdekel, a megadott linkeken utánajárhat.

Host

A *host* egy hálózathoz kapcsolódó eszköz. A *host*okat egy hálózati rétegbeli címmel (IP) azonosítjuk.

Minden *host* egy fizikai csomópont (*node*) a hálózaton, de ez fordítva nem igaz. Pl. egy *switch*, *hub* vagy *modem*, bár fizikailag egy hálózati csomópont, nincs hozzá rendelve IP cím.

Bővebben a hostokról: [http://en.wikipedia.org/wiki/Host_\(network\)](http://en.wikipedia.org/wiki/Host_(network))


A *host* jele a packet tracerben (pl. egy PC): 

Switch

A *switch* egy olyan hálózati eszköz, ami a hálózat egyes elemeit köti össze egymással, tehát a helyi hálózatok kialakításáért felel. Az OSI modell 2. (adatkapcsolati) rétegébe tartozik, de egyes eszközök (úgy nevezett *többrétegű switchek*) végezhetnek adatfeldolgozást magasabb szinteken is. (Ilyen eszközökkel nem foglalkozunk a félév során.)

A *switch*ek manapság fontos részét képezik a LAN-oknak (*Local Area Network*). Feladatuk, hogy a portjaikra kapcsolódó számítógépek zavartalanul kommunikálhassanak egymással (ld. múlt óra). Tehát, ha egy *switch*hez négy *host* kapcsolódik, akkor A-B és C-D gép kommunikációja ne zavarja egymást.

Switch a wikipédián: http://en.wikipedia.org/wiki/Network_switch

A *switch* jele a packet tracerben: 

Router

A *router* egy olyan hálózati eszköz, amely számítógépes hálózatok – LANok – között továbbítja a csomagokat. A beérkező csomag fejlécéből kiolvassa a végső célpontot, majd az irányítási szabályokat figyelembe véve továbbítja azt. Az interneten a *router*ek látják el a forgalomirányító szerepét: az adatok egyik *router*től a másikig haladnak egészen addig, amíg el nem jutnak a célig.

A *router*eket arra is használhatjuk, hogy különböző címtartománnyal ellátott alhálózatokat kössünk össze egymással.

További információk: [http://en.wikipedia.org/wiki/Router_\(computing\)](http://en.wikipedia.org/wiki/Router_(computing))

A router jele a packet tracerben:



AP (Access Point)

Az *AP* (*Access Point*, hozzáférési pont) egy speciálisan konfigurált hálózati csomópont, mely egy vezeték nélküli hálózat központi rádiójel-vevőjeként működik. Támogatja a Wi-Fi vezeték nélküli szabványokat is.

Az AP segítségével összekapcsolhatunk vezetékes és vezeték nélküli hálózatokat egymással.

További információk: http://compnetworking.about.com/cs/wireless/g/bldef_ap.htm

Jele a packet tracerben:



Gateway (Átjáró)

Az átjáró nem egy külön eszköz, hanem a routernek az a hálózati interfésze, amelyre a hálózat eszközei a távoli hálózatba címzett csomagokat küldik. Fogadja a hozzá érkező csomagokat, a csomag címzett a címtartománya alapján megállapítja, hogy mely hálózatban található, majd továbbítja ezt a csomagot a megfelelő irányba az útvonal választó táblázat alapján.

Az *átjáró cím* (*gateway address*) az ennek az interfésznek az IP címe.

IP címek

A hálózaton a számítógépeket egy egyedi cím, az IP cím azonosítja. Minden gépnek van egy címe, de egy gépnek több címe is lehet (minden szolgáltatásának egy-egy), illetve egyes címekhez több gép is tartozhat (céges hálózat), valamint egy gépnek lehet mindig másik címe (dinamikus IP). Az IP címeknek két verziója van: IPv4 és IPv6. Az IPv4 4 bájtban (32 biten), az IPv6 címek pedig 128 biten tárolódnak. Az IP címekről a félév során többször fogunk még szót ejteni.

Bővebben: [Wikipedia](https://en.wikipedia.org/wiki/IP_address)

IPv4

Az IPv4 címek 32 bitesek. Négy, egymástól ponttal elválasztott 8 bites, decimális számmal ábrázoljuk. (Tehát minden szám 0-255 lehet.) Az IP címeknek két fő része van: az első rész a hálózatot, a második rész a hostot azonosítja. Régebben az IP címeket osztályokba sorolták, ma már nem igazán használják, de még néhány helyen hivatkoznak rá.

A négy fő osztály:

1. **A: 1.0.0.0 - 127.255.255.255:** 128 hálózat, egyenként 16 millió host
2. **B: 128.0.0.0 - 191.255.255.255:** 16384 hálózat, egyenként 65536 host
3. **C: 192.0.0.0 - 223.255.255.255:** 2 millió hálózat, egyenként 256 millió host
4. **D: 224.0.0.0 - 239.255.255.255:** multicast (többsküldés)

Az E osztályt (**240.0.0.0 - 255.255.255.255**) későbbi használatra tartják fenn.

Különleges IP címek

- A **0.0.0.0** címet a hostok elindulásakor használják.
- Egy adott hálózat legnagyobb címe a *broadcast* cím (adatszórás).
- A 127-tel kezdődő címek a saját gépünket jelentik, a visszacsatolós teszteléshez használjuk (pl. **127.0.0.1** a localhost).
- Helyi privát címek pl. **10.0.0.0 - 10.255.255.255**

PING

A *ping* egy hálózati segédprogram, melynek segítségével ellenőrizhetjük, hogy egy host elérhető-e a hálózaton és mérhetjük az üzenetek visszatérési idejét a tesztelt hostról.

Ezt a küldő a gyakorlatban úgy valósítja meg, hogy küld a célgépnek egy [ICMP „echo request”](#) csomagot, majd várja az *„echo response”* csomagot és méri a közben eltelt időt. A program futása után kapunk egy statisztikát a legrövidebb-, leghosszabb- és az átlagos visszatérési időről, valamint az elveszett csomagok számáról.

A *ping* parancs egy nem rendeltetésszerű használata a *DoS* támadások egy egyszerű változata, melynek során a támadó elárasztja és túlterheli *„echo request”* csomagokkal az áldozat gépét.

A *ping* program indítása (parancssorból/terminálból):

```
ping <IP cím/host név>
```

Traceroute

A *traceroute* szintén egy hálózatelemző eszköz. Arra szolgál, hogy feltérképezze egy csomag útját a kiindulási és a cél gép között (tehát milyen hálózati csomópontokon halad keresztül), valamint méri az egyes csomópontoknál az átviteli késleltetést.

Ez is ugyanúgy az [ICMP](#) protokoll „*echo request*” csomagját használja. Ha ennek a csomagnak sikerül elérni a célgépet, akkor elindul visszafelé egy „*echo response*” csomag. Ez a csomag tartalmazza azon routerek adatait és időbélyegzőit, amelyeken a csomag áthaladt.

A program indítása (Windows alatt):

tracert <IP cím/host név>

Linux alatt traceroute névvel érhető el.

ICMP

Az *ICMP (Internet Control Message Protocol)* protokollt főként hálózatba kötött számítógépek operációs rendszerei használják pl. hibaüzenetek küldésére, illetve valamilyen lekérő üzenetek küldésére. Leggyakrabban IP csomagok hibáinak jelzésére, diagnosztikai vagy forgalomirányítási célra használják.

ICMP üzenetek teljes listáját [itt olvashatod](#).

ICMP bővebben: [Wikipedia](#)

Beágyazódás (encapsulation)

Az OSI rétegnél szó volt arról, hogy az egyes rétegek mindig közvetlenül csak az alattuk (illetve felettük) lévő réteggel kommunikálnak. Küldéskor az adat elindul valamelyik felsőbb szintről, és mindig eggyel alacsonyabb szintre kerül. Mind-egyik szint, amikor megkapja a felette levőtől a csomagot, akkor beágyazza azt a saját csomagformátumába és kiegészíti egy szükséges információkat tartalmazó fejléccel (esetleg még egy lábléccel is), és ezt továbbítja az alsóbb rétegek felé.

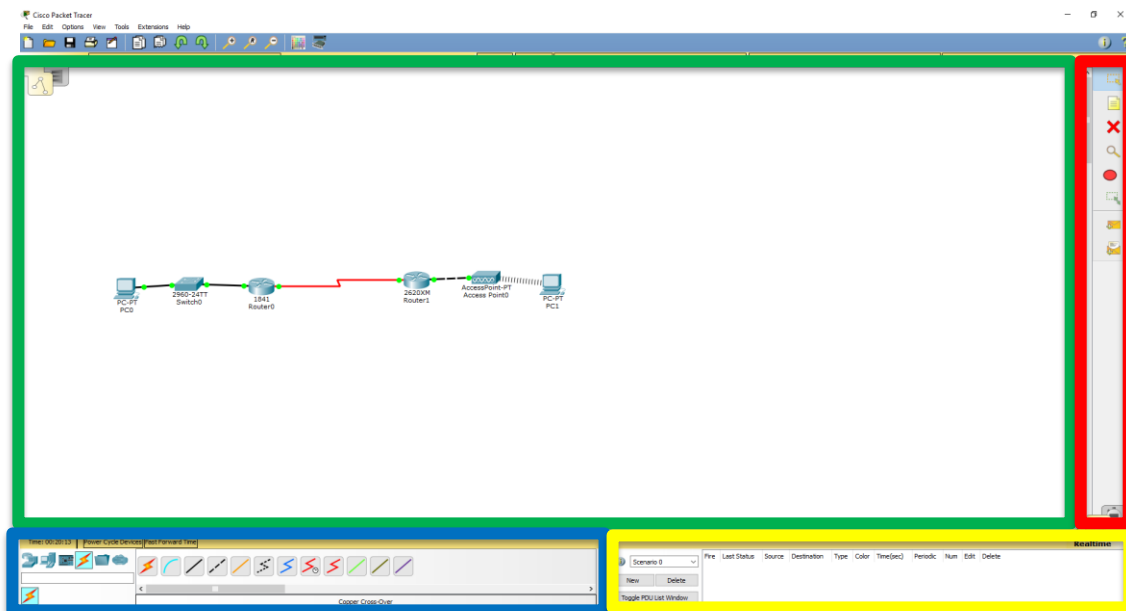
Csomag fogadásakor értelemszerűen alulról felfelé irányul az átadás, és az adott szintek kicsomagolják a saját részüket és úgy adják tovább felfele.

Részletesebben ábrával: [Datagram Encapsulation](#)

Packet Tracer

A következő néhány oldalon a Packet Tracer nevű programmal ismerkedünk meg.

A Packet Tracer felülete



1. ábra - A Packet Tracer felülete

A zöld színnel keretezett rész – a munkaterület

Itt lehet létrehozni egy új hálózat modelljét, illetve betöltéskor ide kerülnek a már létrehozott eszközök. Ha esetleg akkora a hálózat modellünk, hogy nem fér ki egy képernyőre, akkor megjelennek függőleges-vízszintes gördítősávok, amikkel lehet navigálni a munkaterületen.

A kék színnel keretezett rész – hálózati eszközök

Új hálózat létrehozásakor innen húzhatjuk be az egyes eszközöket. Az eszközök típusonként vannak csoportosítva (végesszközök, routerek, switchek, vezetékek stb.)

A piros színnel keretezett rész – „toolbox”

A munkaterület módosítására használható eszközök, fentről lefele sorban:

- kijelölés (akár többet is)
- megjegyzés elhelyezése a munkaasztalon
- törlés (az aktuálisan kijelöltet, ha ilyen nincs, akkor amelyikre kattintunk)
- vizsgálat (az eszköz adatait olvashatjuk le vele)
- alakzat rajzolása
- átméretezés (rajzolt objektumokat méretezhetjük át, erre most nincs szükség)
- egy egyszerű üzenet (ping) küldése
- egy összetett üzenet küldése (paraméterezhető)

A sárga színnel keretezett rész – üzenetek

Amikor teszteljük a hálózatot, akkor a küldött üzenetek állapotát követhetjük itt nyomon.


Eszközök vizsgálata

Az eszközök tulajdonságait több módon is megnézhetjük.

A legegyszerűbb és leggyorsabb megoldás, ha a kívánt eszköz fölé visszük az egér mutatóját és ott tartjuk pár másodpercig. Ekkor a felugró ablakban leolvashatjuk az eszköz legfontosabb adatait.

Egyes eszközöknél (pl. router) több adatot is megtudhatunk. Ekkor a „[toolbox](#)” nagyító ikonjára kattintsunk, és ezzel a nagyítóval a kívánt eszközre. Ekkor egy helyi menüből választhatjuk ki, hogy mire vagyunk kíváncsiak.

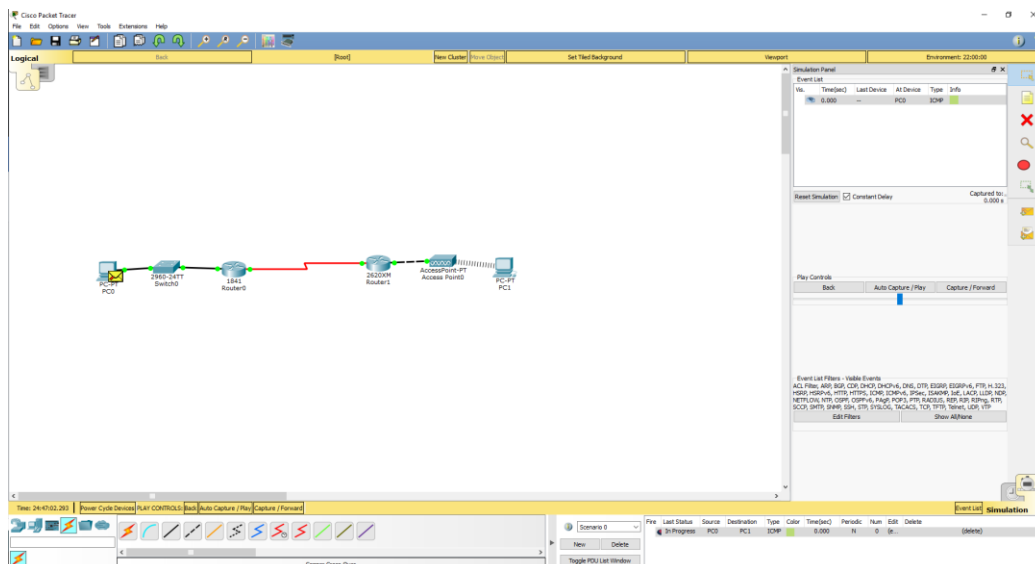
A legrészletesebb listát akkor kapjuk, ha a kijelölő eszközzel kétszer az adott eszközre kattintunk. Itt nem csak adatokat olvashatunk le, hanem azoknak értékét is adhatunk, modulokat tehetünk be/vehetünk ki, konfigurálhatjuk az eszközt stb.

Az átviteli közegekről nem nyerhetünk így információt (mivel a jellegükön kívül más tulajdonságuk nincs is). Hogy melyik jel milyen közeget jelöl, azt a bal alsó sarokban a  jelre kattintva deríthetjük ki. Itt, ha az egyes vezeték típusok fölé visszük az egér mutatóját, akkor alatta megjelenik a típus neve.

Szimuláció

Hogy meggyőződjünk arról, hogy a hálózatunk két csomópontja között létezik-e összeköttetés, küldjünk egy ICMP csomagot az egyik hostról a másikra. Ha visszaér, akkor helyes a hálózatunk felépítése. (Ez éles helyzetben is hasonlóan működik.)

ICMP csomagot legegyszerűbben a „toolboxon” található kis boríték ikonnal küldhetünk. Kattintsunk rá (ekkor az egér mutatója átalakul szintén borítékká), majd ezután a forrás és a cél hostra. Ekkor elindul az üzenet, és a jobb alsó sarokban lévő listán láthatjuk az eredményt. Ha hiba történt a csomag küldése közben, vagy szeretnénk részletesebben látni a csomag útját (esetleg a teljes hálózati forgalmat), akkor lehetőségünk van áttérni valós időből (Realtime mode) szimulációs módba. Ebbe a módba a jobb alsó sarokban látható stopperórát ábrázoló földre kattintva léphetünk át.



2. ábra Szimulációs mód

Szimulációs módban lehetőségünk van arra, hogy megállítsuk az időt, és esemenként lépünk az időben, növelhetjük-csökkenthetjük a sebességet, illetve lejátszhatjuk visszafelé a szimulációt.

Gombok és jelentésük

- Reset simulation – az adott csomag továbbításának szimulációja újra
- Back – a szimulációban egy eseménnyel visszalépünk
- Capture/Foreward – a következő eseményre lépünk
- Auto Capture/Play – automatikus esemény léptetés
- A gombok alatti csúszka – animáció sebességének beállítása
- Edit filters – beállítható, hogy mely csomagok jelenjenek meg a szimulációban

Event list

Itt, mint ahogy a neve is mutatja, látható az események sorozata. Láthatjuk, hogy melyik időpillanatban, honnan, hova érkezett csomag és ez milyen típusú. Az utolsó oszlop azt jelöli, hogy a munkaterületen milyen színű a boríték.

Csomag részletei

PDU Information at Device: Router0

OSI Model Outbound PDU Details

At Device: Router0
Source: Router0
Destination: PC0

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer 3: IP Header Src. IP: 192.168.0.1, Dest. IP: 192.168.0.2 ICMP Message Type: 3 ICMP Message Type: 8
Layer2	Layer 2: Ethernet II Header 0030.A379.7801 >> 0030.A3A8.56EA
Layer1	Layer 1: Port(s): FastEthernet0/0

1. The device sends back an ICMP Host Unreachable message.
2. The device looks up the destination IP address in the routing table.
3. The routing table finds a routing entry to the destination IP address.
4. The destination network is directly connected. The device sets destination as the next-hop.

Challenge Me << Previous Layer Next Layer >>

3. ábra Csomag részletes adatai

Ha duplán kattintunk az eseménylista utolsó oszlopára (a színes négyzetre), akkor egy felugró ablakban láthatjuk, hogy néz ki a csomag szerkezete (a második, „Outbound PDU Details” fülre kattintva), valamint azt, hogy az egyes rétegekben milyen beágyazások és műveletek történtek.

Az *In Layer* a bejövő, *Out Layer* pedig a kimenő csomag kezelését mutatja. Az oszlopban a megfelelő rétegre kattintva alul megjelenik pontokba szedve, milyen műveletek mentek végbe küldés előtt (maga a küldés a legalsó réteg dolga).

Hasznos tudnivaló

Ezt az anyagrészt könnyebb elsajátítani, ha látjátok a dolgokat működés közben is. Ezért ajánlott megnézni az ehhez tartozó videós tutorialokat is, ami ezen a címen érhető el:

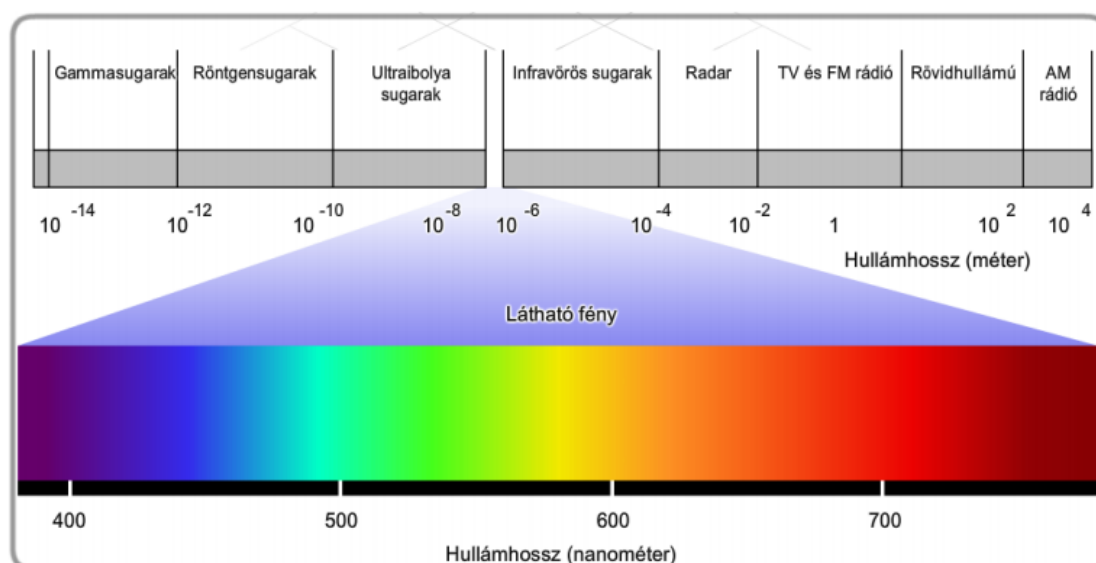
<http://engweb.info/cisco/Packet%20Tracer%20Tutorials.html>

A vezeték nélküli technológia

A jegyzet második részében a vezeték nélküli összeköttetésről lesz szó. Először egy rövid elméleti áttekintő a vezeték nélküli technológiákról, majd megnézzük ennek megvalósítását Packet Tracerben.

Áttekintés

A vezeték nélküli eszközök elektromágneses hullámokat használnak az egymással történő kommunikációhoz. Ugyanez a közeg szállítja a rádiójeleket is az éteren keresztül. A lenti ábrán látható az elektromágneses frekvenciaspektrum, amelyen megfigyelhetjük, hogy melyik hullámhosszú elektromágneses hullámot mire használjuk.



4. ábra - az elektromágneses spektrum

Bizonyos típusú elektromágneses hullámok nem alkalmasak az adatátvitelre, míg mások állami szabályozás alatt vannak és használatukat csak adott szervezeteknek egy bizonyos célra engedélyezik (pl. mobilszolgáltatók). A tartomány más részeit közhasználatra tartják fenn (ilyen például a következőkben tárgyalt rádiófrekvenciás és infravörös tartományok is). Érdekes megjegyezni, hogy az emberi szemmel érzékelhető spektrum a teljes tartománynak csupán egy elenyésző részét képezi. A következő részekben átvesszünk két vezetékmentes technológiát.

Infravörös

Az angol terminológia szerint **IR**nek, azaz **InfraRed**nek nevezik. Ez egy igen gyakran használt technológia, amely főként a mobil eszközökben, PDA-kban, távirányítókban, vezeték nélküli egerekben és billentyűzetekben terjedt el. Viszonylag alacsony energiaszintű, kis hatótávolságú, így a jelei nem képesek áthaladni a falakon vagy egyéb akadályokon.

Az eszközök az egymás közötti információcseréhez egy **IrDA (Infrared Direct Access, Infravörös Közvetlen Hozzáférés)** nevű különleges kommunikációs portot használnak. A technológia csak pont-pont típusú kapcsolatot tesz lehetővé, tehát az eszközök csak közvetlenül egymáshoz kapcsolódhatnak.

Rádiófrekvencia

A rádiófrekvenciás hullámok nagyobb energiájúak, mint az előbb említett infravörös technológia, így ezek már képesek a falakon is áthatolni, ezáltal sokkal több alkalmazási lehetősége van, főként a telekommunikáció területén.

A rádiófrekvenciás tartomány bizonyos részeit szabad felhasználásra tartják fenn, mint például vezeték nélküli helyi hálózatoknak és egyéb számítógépes perifériáknak. Ilyen frekvenciák a 900MHz, 2,4GHz és a 5GHz sávok. Ezen frekvenciák az **ISM (Industry, Science and Medicine)** azaz **Ipari, Tudományos és Orvosi** sávokként ismertek és csekély megszorítások mellett használhatók. A *Bluetooth* egy ilyen kommunikációs technika, amely a 2,4GHz-es sávon működik. Korlátozott sebességű és rövid hatótávolságú, de megvan az az előnye, hogy egyidejűleg több eszköz kommunikációját teszi lehetővé – ez a tulajdonsága emelte az IR fölé (pl. számítógépes perifériák, mobiltelefonok közötti átvitel).

Egyéb technológiák, amelyek a 2.4GHz és 5GHz tartományt használják a különböző IEEE 802.11-es szabványnak megfelelő vezeték nélküli hálózatok. Ezek abban különböznek a Bluetoothtól, hogy magasabb teljesítményszinten továbbítanak, ez nagyobb hatótávolságot tesz elérhetővé számukra.

Előnyök és korlátok

Bizonyos esetekben előnyösebbek a hagyományos vezetékes hálózatokkal szemben:

- Egyszerűbb csatlakozást tesz lehetővé a mobilis felhasználók számára.
- Egyszerűen bővíthető több felhasználó fogadása és a lefedettségi terület bővítése esetén.
- Hatókörön belül bárhol, bármikor kapcsolódhatunk.
- Egyetlen eszköz telepítése számos felhasználó kapcsolódását teszi lehetővé.
- Egyszerűen beüzemelhetők veszélyes és ellenséges környezetben is.
- Ott is használható, ahol a hagyományos vezetékes kapcsolat nem (vagy csak nagyon drágán) alakítható ki.

Ezen jó tulajdonságokon felül viszont hátrányai is vannak a rendszernek. Ezek pedig a következők:

- A vezeték nélküli technológia érzékeny a többi elektromágneses erőteret keltő eszközöktől származó interferenciára.
- A vezeték nélküli LAN technológiát (*Wireless LAN*) az átvitelre kerülő adatok hozzáférésére és nem azok védelmére tervezték. Ebből kifolyólag védtelen bejáratot biztosíthat a hálózatba.
- Bár a vezeték nélküli technológia folyamatosan fejlődik, jelenleg nem biztosítja a vezetékes hálózatok által nyújtott sebességet és megbízhatóságot.

A vezeték nélküli hálózatok típusai és kötöttségei

A vezeték nélküli hálózatokat fizikai kiterjedésük alapján három csoportba szokták sorolni. A hálózat hatókörét viszonylag nehéz pontosan meghatározni, mivel az átvitel hatótávolságát számos körülmény (mind környezeti, mind mesterséges) befolyásolhatja. Pl.: hőmérsékletingadozás, páratartalom változása.

WPAN

Ez a legkisebb kiterjedésű hálózattípus. Ezt általában a számítógéphez tartozó perifériák (nyomtató, egér, billentyűzet) csatlakoztatására használják. Ide tartozik a korábban említett IR és a Bluetooth.

WLAN

A WLAN-t általában a vezetékes helyi hálózatok határainak kiterjesztése érdekében használják. Ez rádiófrekvenciás technológiát használ, és megfelel az IEEE 802.11-es szabványnak. Sok felhasználó számára egy csatlakozási ponton keresztül (**AP**, **A**ccess **P**oint) biztosít kapcsolatot a hálózat többi része felé. A jegyzet további részében ezzel a csoporttal fogunk foglalkozni.

WWAN

Ezen hálózatok óriási méretű területeken biztosítanak lefedettséget, mint például a mobiltelefon hálózatok. Olyan technológiákat használnak, mint például a GSM (**G**lobal **S**ystem for **M**obile **C**ommunication), vagy a CDMA (**C**ode **D**ivision **M**ultiple **A**ccess azaz Kódosztásos Többszörös Hozzáférés).

Vezeték nélküli helyi hálózatok (WLAN)

Szabványok

Ahogy korábban is említettük, a WLAN hálózatokat felépítését az IEEE 802.11-es szabvány határozza meg. Ennek négy fő ajánlása van, amely különböző jellemzőket szolgáltat a vezeték nélküli hálózatok számára. Összefoglaló néven ezeket a technológiákat **Wi-Fi**-nek (**W**ireless **F**idelity) nevezzük. Létezik egy Wi-Fi szövetség nevű szervezet is, amely a különböző gyártók WLAN eszközeinek teszteléséért felelős, és egy emblémát helyez az eszközre, ha az megfelel a szabványoknak. A fentebb említett négy ajánlás:



- **802.11a**: max 54 Mb/s sávszélesség, az 5GHz-es frekvenciát használja
- **802.11b**: max 5,5 Mb/s vagy 11 MB/s, a 2,4GHz-es tartományt használja
- **802.11g**: max 54 Mb/s, és a 2,4GHz-es tartományt használja
- **802.11n**: a legújabb szabvány, max 600Mb/s sávszélességet képes elérni, valamint a 2,4GHz-es frekvenciát használja. Ezen kívül lefelé kompatibilis az „a”, „b” és „g” jelű ajánlásokkal.

WLAN összetevői

Egy vezeték nélküli hálózatnak több összetevőre is szüksége van ahhoz, hogy megfelelően működhessen. Most ezeket fogjuk röviden áttekinteni.

Hozzáférési pont (AP)

Az első, és talán legfontosabb eszköz. Ez biztosítja a vezetékes és a vezeték nélküli hálózatok összekapcsolását, tehát lehetővé teszi a vezeték nélküli kliensek számára, hogy hozzáférjenek a vezetékes hálózatokhoz és viszont. Továbbá átviteli közeg átalakítóként is működik, mivel a vezetékes Ethernet hálózat kereteit fogadja, és mielőtt továbbítaná a WLANra, átalakítja a 802.11-es szabványnak megfelelő keretekké, illetve ezt fordítva is megcsinálja, amennyiben a vezeték nélküli kliensek (STA) felől érkezik a forgalom. Ezek az eszközök egy korlátozott területen

biztosítanak hozzáférést, melyet vezeték nélküli cella, vagy BSS néven (**B**asic **S**ervice **S**et, Alapvető Szolgáltatás Készletként) ismerünk.

Vezeték nélküli kliensek (STA)

Ezek lényegében bármely eszközt jelenthetik, amelyek részt vesznek a hálózatban. A legtöbb eszköz, amely képes vezetékes hálózatra csatlakozni, ellátható vezeték nélküli hálózati kártyával és szoftverrel, amely segítségével képes lesz kapcsolódni a WLAN-okhoz is.

Vezeték nélküli híd

Ezeket két vezetékes hálózat vezeték nélküli összekötésére használják, és nagy távolságú pont-pont kapcsolatot biztosítanak a két hálózat között. Engedélyt nem igénylő frekvenciát használva egymástól 40 km-re, vagy távolabb fekvő hálózatokat tudunk kábelek nélkül összekapcsolni.

Antennák

Ezeket az APk és a vezeték nélküli hidak esetében használják. Hasznuk, hogy megnövelik az eszköz által kibocsátott jel erősségét, ami általában nagyobb hatótávolságot jelent. Ezek fogadni is tudják a kliensek jeleit.

Általában az erősségük alapján osztályozzuk őket. Alapvetően kétfajtát különböztetünk meg; azokat, amelyek minden irányba egyenletes erősséggel sugároznak, illetve azokat, amelyek egy kifejezett irányba sugároznak. Ez utóbbiakat nagy távolságok áthidalására használják, míg az egyenletesen szórót az APk esetében alkalmazzák.

SSID

Nagyon fontos momentum, hogy amennyiben több vezeték nélküli hálózat átfedi egymás területét, akkor az egyes kliensek a megfelelő hálózathoz csatlakozzanak. Erre használják az SSIDt (**S**ervice **S**et **I**Dentifier, Szolgáltatáskészlet azonosító). Az SSID érzékeny a kis- és nagybetűkre, illetve maximum 32 alfanumerikus karakterből állhat. Ez az azonosító megtalálható minden WLAN keret fejlécében.

WLAN kiépítési módok

Ad-hoc

Ez a vezeték nélküli hálózatok legegyszerűbb formája, amikor két vagy több eszközt kapcsolunk össze úgy, hogy azok egyenrangú hálózatot alkossanak. Ezek nem tartalmaznak hozzáférési pontot, minden résztvevője egyenrangú. Ez akkor előnyös, ha például független eszközök egyszeri információcserét akarnak végrehajtani, mivel ilyenkor felesleges lenne egy AP beszerzése és konfigurálása. A hálózat által lefedett terület az **IBSS** (**I**ndependent **B**asic **S**ervice **S**et, független alapvető szolgáltatáskészlet).

Infrastruktúra mód

Az előző módszer működhet kis körben, de amikor például egy épület vezeték nélküli hálózattal való ellátásáról van szó, akkor gondok adódhatnak. Ekkor már be kell szerezni egy AP-t, hogy a nagy mennyiségű forgalmat kezelni tudjuk és megbízhatóvá tegyük a hálózatunkat. Egy ilyen típusú hálózatban az eszközök nem képesek egymással közvetlenül kommunikálni, minden forgalom az APn keresztül történik. A hozzáférési pont törekszik arra, hogy minden eszköznek egyenlő joga

legyen a közeghez való hozzáféréshez. Az AP által lefedett terület az alapvető szolgáltatáskészlet, más néven cella, avagy az angol terminológiával élve **BSS**. Ez a vezeték nélküli hálózatok legkisebb építőeleme. A lefedett terület bővítéséhez több BSS is összeköthető egymással egy elosztórendszer (**Distribution System – DS**) segítségével. Ezzel egy **Extended Service Set (ESS)** jön létre, ahol az egyes AP-k a különböző BSS-ekben vannak.

Azért, hogy a cellák között a jelek elvesztése nélkül biztosítsuk a kapcsolatot, az egyes BSS-ek között megközelítőleg 10%-os átfedésnek kell lennie. Ez lehetővé teszi a kliensek számára, hogy csatlakozzanak azelőtt az egyik AP-ról a másikra, anélkül, hogy a jelet elveszítenék.

Csatornák

Ha egy IBSS, ESS vagy BSS kliensei kommunikálnak egymással, a küldő és a fogadó állomások közötti kommunikációt irányítani kell. Erre egy módszer a csatornák használata.

Ezek a rendelkezésre álló rádiófrekvencia tartomány részekre osztásával jönnek létre. Hasonló ahhoz, mint amikor több televíziós csatornát szolgáltatnak egy átviteli közegen keresztül.

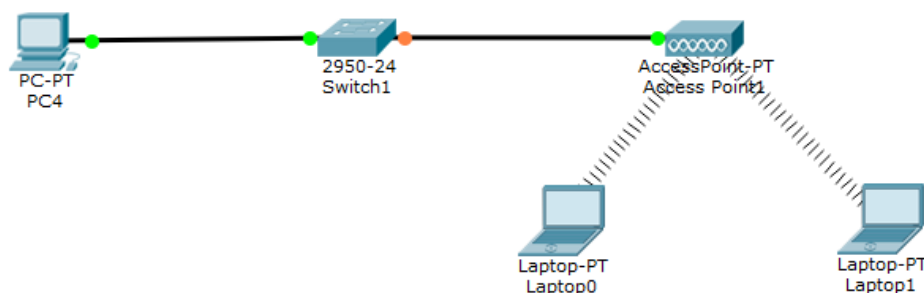
Sajnos az egyes frekvenciák átfedésben lehetnek a mások által használt csatornákkal, így a párbeszédnek egymást nem érintő csatornákon kell zajlaniuk.

Néhány újabb technológia képes arra, hogy több csatornát együtt kezeljen, így egy szélesebb átviteli csatornát hoz létre, amely nagyobb sávszélességet, megnövekedett átviteli sebességet eredményez.

Egy WLANon belül, a cellák közötti határvonal elmosódása miatt lehetetlen a csomagütközéseket pontosan érzékelni, ezért olyan közeghozzáférési módszert használnak a vezeték nélküli hálózatokban, amely biztosítja, hogy ne forduljanak elő ütközések. Ez a technológia az úgynevezett **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**, azaz Vívőjel-érzékeléses többszörös hozzáférés ütközés elkerüléssel). A CSMA/CA lefoglalja a párbeszédre használandó csatornát, és amíg ez a foglalás érvényben van, más eszköz nem használhatja adásra.

A 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.



5. ábra – az elkészítendő hálózat

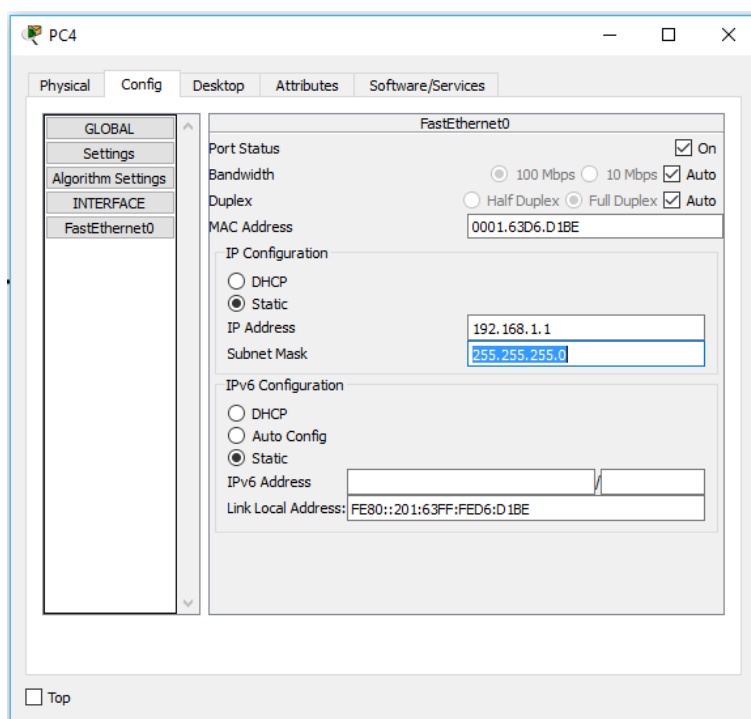
Ahogy a képen is látszik, az *AccessPoint-PT* típusú hozzáférési pontot használjuk. Ezen kívül két laptop csatlakozik a hálózatra. A feladatban mindenhol statikus IP cím kiosztást fogunk használni. Ez rendre 192.168.1.1 a PC4-en, 192.168.1.2 a Laptop0-n, és 192.168.1.3 a Laptop1-en. A hálózati maszk mindenhol az alapértelmezett 255.255.255.0 érték legyen.

Hostok konfigurálása

A hostok összeköttetése 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 máshova, 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.



6. ábra - Host konfiguráció

Hozzáférési pont konfigurálása

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

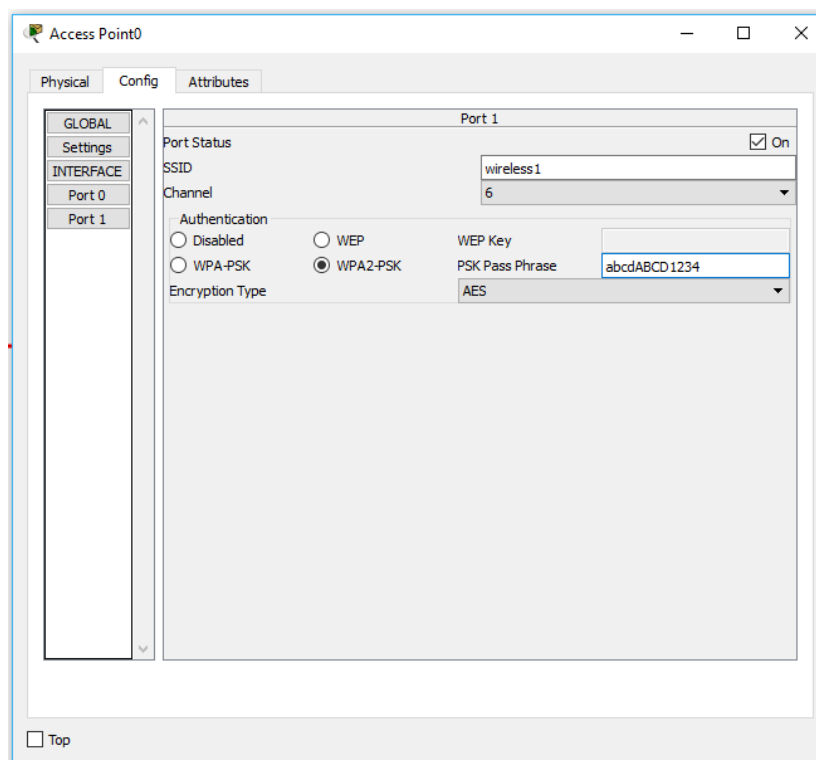
- Az SSID-t, tehát egy azonosítót, amivel a hálózatunknak egy egyedi nevet adunk
- A csatornát, hogy ne interferáljon más hálózatokkal

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 vezetékes 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



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

Laptopok konfigurálása

A laptopok esetén három dolgot kell megtennünk:

- Beépíteni egy vezetékek 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

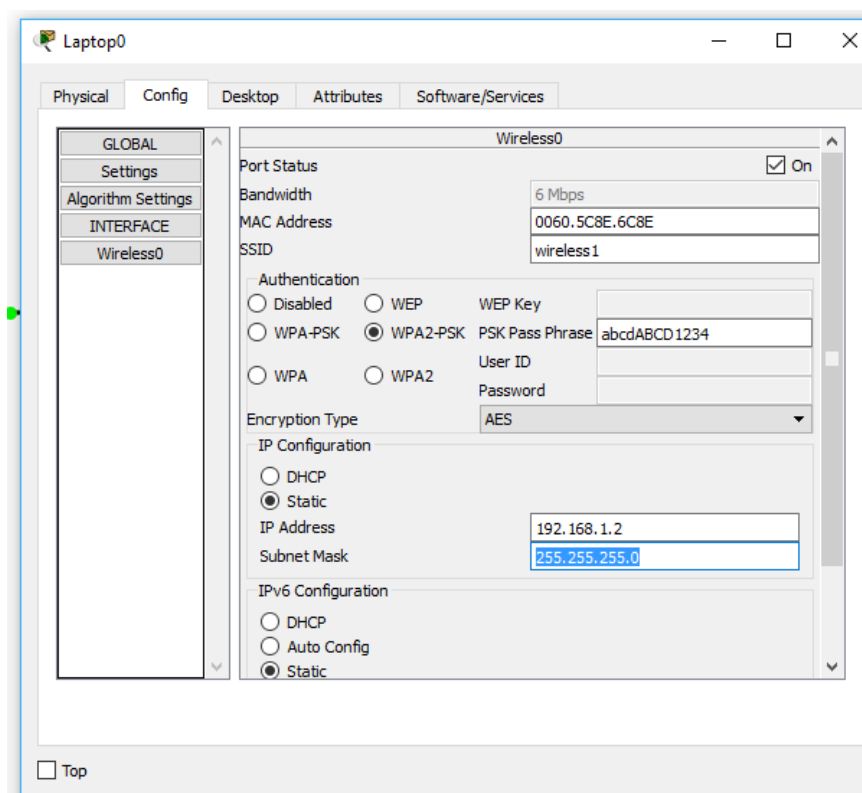
rá a listára a modult), majd válasszuk ki a **PT-LAPTOP-NM-1W** interfészt, és építjük bele a laptopba. Ezután kapcsoljuk vissza az eszközt. Ha ezzel végeztünk, az *“Config”* fülön az eddigi *FastEthernet* port helyett megjelenik egy *“Wireless”* nevű interfész. Itt tudjuk megadni a vezeték nélküli hálózat 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.



8. ábra - az eszköz konfigurációja

Beugró kérdések

1. Mire használhatjuk a *Packet Tracer* programot?
2. A **switch** általában melyik OSI rétegben van?
3. Mit csinál a **router** a hálózatban?
4. Ha az SZTE IP címtartománya **160.114.0.0 – 160.114.255.255**, akkor melyik IP cím osztályba tartozik?
5. Milyen speciális jelentése van a **127**el kezdődő IP címeknek?
6. Mire jó a **ping** parancs?
7. Mire jó a **tracert** parancs?
8. Mi lehet a vezeték nélküli hálózatok **hátránya**?
9. Mit jelent az **AP**?
10. Melyik titkosítás elavult, és nem javasolt a használata?