Baranya Megyei SZC Simonyi Károly Technikum és Szakképző Iskola

ZÁRÓDOLGOZAT

Készítette: Név: Juhos Benjámin

Név: Laboda Dániel

Név: Hernádi Emma

Pécs

2022

*Baranya Megyei SZC Simonyi Károly Technikum és Szakképző Iskola*

*Szakképzés megnevezése: Informatikai rendszer- és alkalmazás-üzemeltető technikus*

*A szakma azonosító száma: 5-0612-12-02*

***Záródolgozat***

***Cím: LDAP Ingatlan***

*Készítette: Név:* Juhos Benjámin

*Név:* Laboda Dániel

*Név:* Hernádi Emma

*Pécs*

*2022*

**Projektmunka Bevezetés**

* 1. **Célok és indoklás**

Ezt a projektet elkészítő csapat:

* Juhos Benjámin
* Laboda Dániel
* Hernádi Emma

A célja, hogy ki alakítsunk egy jól működő, gyors és biztonságos hálózatot egy ingatlannal foglalkozó cég számára. Maga a cég lakás eladással foglalkozik ingatlan iroda révén, ezt figyelembe véve alakítjuk megfelelően, dolgozzuk ki a nekik rendszert. Illetve figyelembe vettük a projekt munkához megadott paramétereket is.

Több szempontot figyelembe véve döntöttünk egy ingatlan cég mellet. Megnéztük mik az előirt protokollokat és szolgáltatásokat ezt a tanáraink tanácsaival és a saját tapasztalatainkkal összevetve döntöttünk úgy, hogy egy ,,ingatlan cég” keretein belül tudjuk a legjobban kifejteni a hálózatunkat.

Ez után elkezdtük kialakítani, hogy osszuk fel a céget, hány telephely legyen, szolgáltatások, eszközök száma és hogy mennyi elméleti ember dolgozik a különböző területeken. Ezeknek letisztázása nélkül neki se tudunk állni a munkának. Maga a kialakítást úgy tervezük, hogy lesz egy központi hely és több kisebb munkaállomás, szám szerint három, amik különböző városokban helyezkednek el. A fő feladatunk megoldani kis telephelyeken belüli, illetve egymással és a központi hellyel (központon belül is) való jó kommunikáció, adatcserélést és azoknak el mentését, megvédését.

kép: [ingatlancég - Portfolio.hu](https://www.portfolio.hu/cimke/ingatlanc%C3%A9g)

* 1. **Ütemterv**

Az ütemterv:

* A megépítendő hálózat követelményeit felmérjük az az pontosan hány emberhez szükséges eszközzel, lefedettséggel kell számolnunk. erre párnapot szánunk.
* A tényleges infrastruktúra megtervezéséhez szükséges legalább egy-két hónap.
* Miután tisztában vagyunk a hálózat, eszközök paramétereivel és az infrastruktúrával egy szimulációs programban a Packet tracerben el kezdjük tesztelni a működését nagyjából 2-3 hét szükséges ehhez (Valószínűsíthetőleg, ha ténylegesen a valóságban is ki építenénk ehhez több hónapra lenne szükség telephelyenként).

Míg a konfigurációkat és a protokollokat a Packet tracerben készítjük el a különböző szolgáltatásokat virtuálboxban üzemelt kettő szerveren fog működni. Az egyik egy Windows szerver lesz a másik egy Linux szerver. Ezeknek elkészítését, kialakításának részleteit ez a dokumentáció fogja ismertetni a későbbiekben.

* A két szerver hiba nélküli működéséhez párnap rosszabb esetben párhét szükséges.
* Az egész projekt munka össze hangolása és tesztelése szintén párnap.
* Végezetül amíg ezt az egészet pontról pontra dokumentáljuk, át beszéljük és a feljövő problémákat korrigáljuk és teszteljük a munkánk működését az nagyjából még 1 hónap.
  1. **Feladat leosztás**

A feladatok elosztását a szerint döntöttük el, hogy a csapatunk tagja mi be jeleskedtek az elmúlt időbe és hogy miben dolgoznak szívesen.

* Juhos Benjámin része a Linux szerver elkészítése az összes megadott paraméterrel
* Laboda Dániel a window szerver kialakítása.
* Hernádi Emma írja a dokumentációt és készíti a packet tracerben a hálózat kialakítása

Ez az alapvető leosztás de valamelyest kollektíven készítjük a vizsgamunkát, emellett rendszeres megbeszélést tartunk és amennyiben bárkinek szüksége van segítségre vagy meg akad részt veszünk az ő munka részében is és segítünk ahogy csak tudunk. Munka közben rendszeresen tárgyalunk a konzulens tanárunkal.

Mivel nem csak az iskolán belül halladunk a projekttel hanem otthon is ezért ezekben az esetekben különböző platformokat használunk ahhoz, hogy tudjunk egymással kommunikálni, illetve fájlokat cserélni.

**Cég felmérés**

**2.1 cégfelmérés**

Ahhoz, hogy a cégnek megfelelően működjön a hálózata ezeket az eszközöket éreztük szükségesnek a megfelelő beállításokkal:

**Központ (Center):**

- Asztali számítógép

- Laptopok

- Szerver

- Nyomtatok

- Router

- Switch

- AccessPointok

**Kisebb telephelyek:**

- Admin gép

- Laptopok

- Nyomtatok

- Tabletek

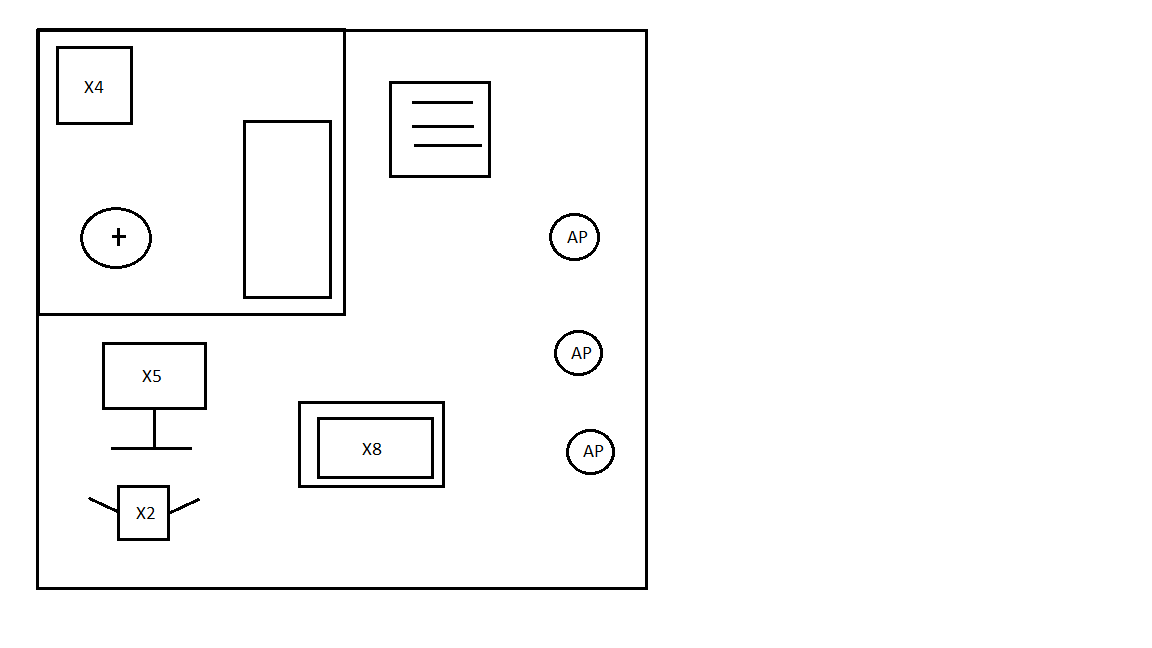
Miután ezt meg állapítottuk számitásba kell venni, hogy hányan dolgoznak a cégnél ez által azt is, hogy hány eszközre van szükség. Ez azért fontos mert minél több eszköz van, ami kapcsolódni tud a hálózathoz annál jobban bővíteni kell a hálózatot és az új eszközök ezt engedélyezni kell, hogy hozzá férhessenek a szerverek és felhőszolgáltatásokhoz.

**2.2 Vizuális megjelenítés**

Alkotunk pár alap nem túl részletes rajzot, hogy legyen alap kép, hogy könnyebb legyen vizualizálni. A szimulációban nem teljesen ugyan így jelenek meg az eszközök és nem egészen azonos mennyiségben a packet traceres feladat részünk egy reprezentatív hálózatott jelenít meg.

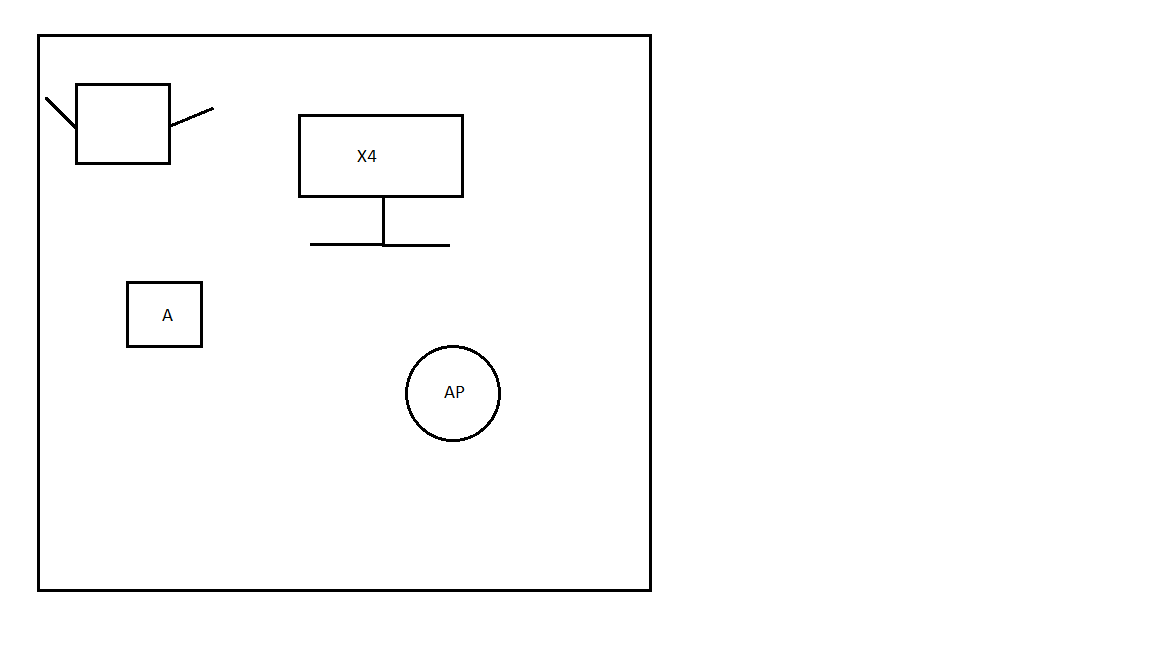
**Center:**

* Az összes közül a center az az a központi telephelynek van szüksége a legtöbb eszközre és úgy terveztük, hogy itt lesz kellően elegendő hely arra, hogy itt helyezhessük el a két szervert.



**Site 1-3:**

* + A sitokból ahogy már előzőleg is említettük 3 darab van. Lényeges kisebbre terveztük őket mivel a centeren keresztül kapják a szolgáltatásokat így fizikálisan csak azokra az eszközökre van szükség, amiket az ott dolgozok a munkára használnak.



**Dolgozok légyszáma:**

A dolgozok légyszámának mennyiségének megállapítása részben az eszközök mennyiségének megállapítására, illetve a költség számitás hoz is szükséges.

**központi telephely:**

- Rendszerüzemeltető 1 fő

- Vezetés, könyvelés, HR (2) 5 fő

- üzletkötő 8 fő

**1.site:**

- 1 Fő vezető

- 3 üzletkötő

**2.site:**

- 1 fő vezető

- 3 üzletkötő

**3.site:**

- 1 fő vezető

- 3 üzletkötő

**Eszközök:**

Alapvetően úgy terveztük, hogy több eszköz lesz a feladatunkba, de a jobb működés és az egyszerűbb elkészítés miatt a packet tracer feladatban csak típusonként van bemutatva az eszközök.

**Központ (Center)**

- 5 db laptop

- 2 nyomtató

- 2 db router (firewall)

- 3 db switch

- 2 db szerver

- 2 db accesspoint

- 8 db tablet

**Kisebb telephelyek**

- 4 db laptop, tablet

- 1 db switch

- 1 db router

- 1 db accesspoint, 1 db nyomtató

**2.3 Költségszámolás**

A költség számítással meghatározzuk a cégnek, hogy mennyibe fognak kerülni az eszközök, illetve azt is, hogy a mi ,,bérünk” mennyi lenne, ha a valóságban ténylegesen kiépítenénk egy cégnek a hálózatát és a hozzá való szolgáltatásokat.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Költségelszámolás** | | | | | |
| **Eszközök** | **Darabszám** | **Márka,név** | **Ár** | **Bolt, weboldal** | **Végső ár** |
| Nyomtató | 5 db | Canon MAXIFY MB2155 multifunkciós nyomtató (0959C029) | 59 900 Ft | [camerakft.hu](https://webshop.camerakft.hu/Canon_MAXIFY_MB2155_multifunkcios_nyomtato_0959C029) | 299 500 Ft |
| Tablet | 14 db | Apple iPad 9 2021 10.2 64GB | 132 490 Ft | [planetgsm.hu](https://planetgsm.hu/Apple-iPad-9-2021-10-2-64GB-WiFi-asztroszurke) | 1 854 860 Ft |
| Asztali gép | 4 db | DELL Optiplex 3060 Mini Tower | 184 900 Ft | [mysoft.hu](https://www.mysoft.hu/details.aspx?pn=3881I3UA1_S250SSD_S) | 739 600 Ft |
| Egér | 7 db | Hama MC-300 (182606) | 2 090 Ft | [emag.hu](https://www.emag.hu/hama-mc-300-eger-fekete-182606/pd/DJKZP1BBM/?utm_source=price_comparer&utm_medium=cpc_emag&utm_campaign=arukereso_new_2018&utm_content=arukereso_hu&cmpid=72648) | 14 630 Ft |
| Monitor | 7 db | Samsung S22F350FHR Monitor | 43 790 Ft | [emag.hu](https://www.emag.hu/samsung-led-monitor-22-ips-full-hd-1920x1080-hdmi-fekete-ls22f350fhrxen/pd/DWV19TMBM/?utm_source=price_comparer&utm_medium=cpc_emag&utm_campaign=arukereso_new_2018&utm_content=arukereso_hu&cmpid=72648) | 306 530 Ft |
| Billentyüzet | 7 db | Hama Casano К681 (53813) | 3 499 Ft | [mediamarkt.hu](https://www.mediamarkt.hu/hu/product/_hama-casano-vezet%C3%A9kes-magyar-billenty%C5%B1zet-53813-1104669.html?rbtc=aru%7cpf%7c1104669%7c%7cp%7c%7c) | 24 493 Ft |
| Laptop | 11 db | Lenovo V15 82NB001BHV Notebook | 169 990 Ft | [laptop.hu](https://www.laptop.hu/lenovo-v15-g1-82nb001bhv-grey-nos) | 1 869 890 Ft |
| CiscoRouter | 3 db | C891F-K9 | 494 962 Ft | [senetic.hu](https://www.senetic.hu/product/C891F-K9) | 1 484 886 Ft |
| Switch | 4 db | D-Link DGS-1210-52MP Gigabit Web Smart PoE Switch | 307 710 Ft | [bevachip.hu](https://bevachip.hu/d-link-dgs-1210-52mp-gigabit-web-smart-poe-switch-p516828/) | 1 230 840 Ft |
| Server | 2 db | HP ProLiant MicroServer G10 Plus | 400 900 Ft | [mysoft.hu](https://www.mysoft.hu/details.aspx?pn=P16006-421&utm_source=arukereso.hu&utm_campaign=arukereso.hu_szerver&utm_medium=cpc&utm_term=P16006-421) | 801 800 Ft |
| Accespoints | 6 db | IP-COM AC1200 Wave 2 Gigabit Access Point (iUAP-AC-LITE) | 25 790 Ft | [pcx.hu](https://www.pcx.hu/ip-com-ac1200-wave-2-gigabit-access-point-iuap-ac-lite--00174949) | 154 740 Ft |
| Router | 2 db | ISR4331-SEC/K9 | 1 461 950 Ft | [senetic.hu](https://www.senetic.hu/product/ISR4331-SEC/K9?gclid=CjwKCAjwu_mSBhAYEiwA5BBmfwb3Mc0cQMosubvUo_Pmsd3t4Bi0UuFWulkEIe8LVWMRvp95HdhO1hoCcisQAvD_BwE) | 2 923 900 Ft |
| SSD | 7 db | 240GB Kingston SSD SATA3 2,5" A400 meghajtó (SA400S37/240G) | 11 890 Ft | [aqua.hu](https://aqua.hu/alkatrszek/240gb-kingston-ssd-sata3-25-a400-meghajto-sa400s37240g-t521204) | 83 230 Ft |
| HDD | 7 db | 2TB Seagate BarraCuda 3.5" winchester (ST2000DM008) | 18 900 Ft | [aqua.hu](https://aqua.hu/alkatreszek/2tb-seagate-barracuda-35-winchester-st2000dm008-t641812) | 132 300 Ft |
| Végösszeg |  |  |  |  | 11 921 199 Ft |

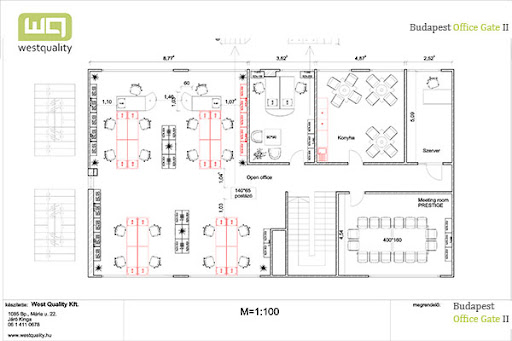
Ahhoz, hogy az óradíjunkat meg tudjuk határozni szükségünk lenne az irodaházak tervrajzára, hogy lássuk milyen vastagok a falak, illetve a csövek és különböző más kábel elhelyezkedése miatt, hogy hol és mennyit tudunk fúrni, ha arra van szükség. Más szóval azért kell, hogy pontosan megtudjuk mondani, hogy hogyan tudjuk megoldani a kábelezést és az eszközök elhelyezését.

**2.4 Tervrajz**

Mivel ugye ezek nem léteznek ezt úgy oldottuk meg hogy választottunk két tervrajzot az internetről és azokhoz viszonyítjuk az óra bérünket. Bár kábelezés és a csövek elhelyezkedését így sem tudjuk meg teljesen pontosan, de pontosabban kitudjuk számolni az óra bérünket.

A közös meg egyezés és a tervrajz alapján úgy döntöttünk, hogy nagyjából 2000 Ft óránként.

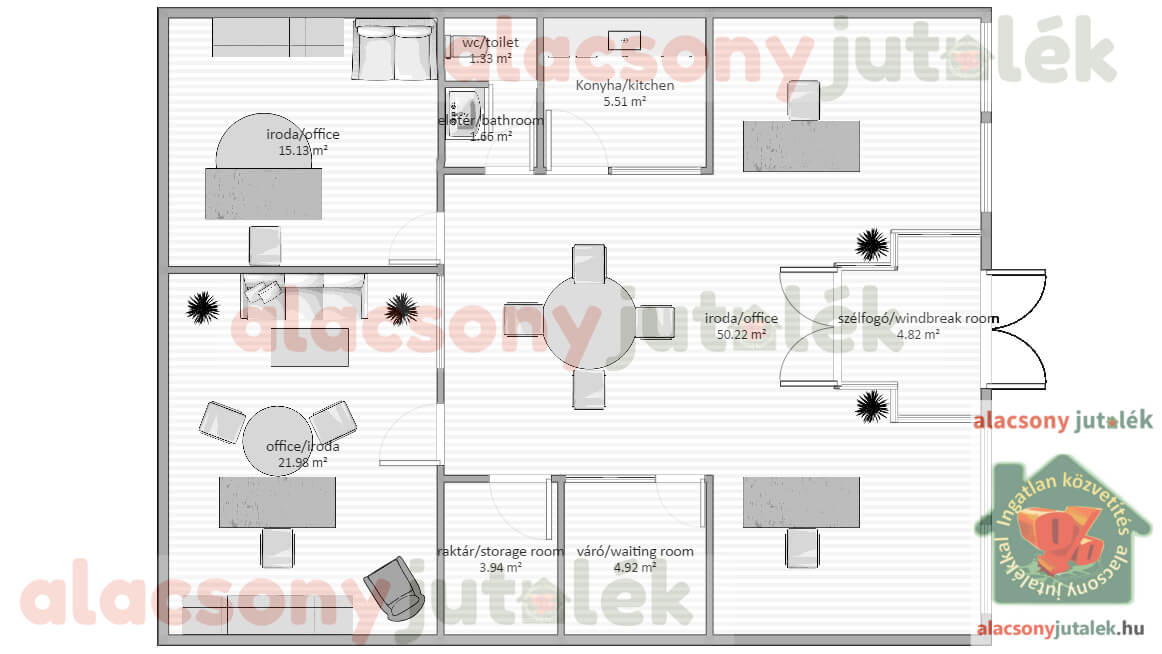
**Központi telephely:**



kép: <http://www.westquality.hu/szolgaltatasok/szolgaltatasok/dijmentes-3ds-latvanytervezes>

**Site-ok 1-3:**

kép:<https://alacsonyjutalek.hu/>



**Hálózat kialakítása elkészítése**

**3.1 Biztonsági Zónák**

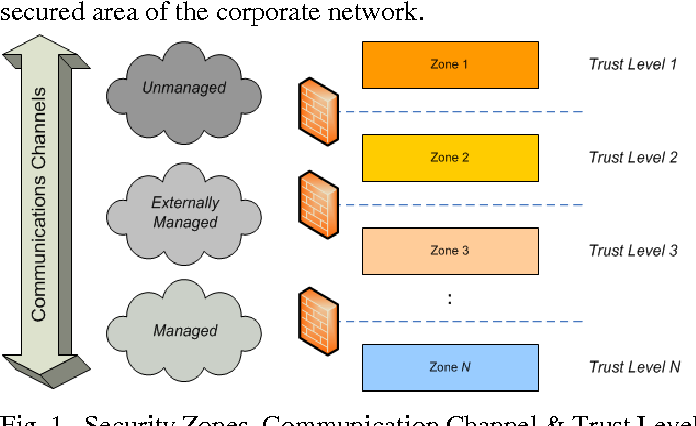
Ezek lesznek a biztonsági zónaink (security zones). Arra szolgálnak, hogy megszabjuk az jogosultságokat (ki mihez férhet hozzá) ezt nyilván a szerint alítjuk, amit megkövetel a vevő.

* Public:
  + 192.168.63.0 /24 (a hálózata)
  + külső wifi, internethez való csatlakozás
* Worker:
  + Windows szerver
  + Linux szerver
  + Hálózati eszközök
  + Nyomtatok
  + 192.168.113.0 /25

A public az, amihez bárki hozzáférhet csak az internethez biztosit hozzáférést az ügyfelek számára, akik éppen valami ügyet intéz a cégnél. A worker hálózat pedig hozzá férést biztosit a cég szolgáltatásaihoz az ott dolgozok számára és a siteokat kapcsolja össze a belső hálózattal ez által a site-ok is hozzá férnek a központi hely fájljaihoz, adataihoz és az adminak biztosit hozzáférést minden hálózati eszközhöz így azokat felügyelni tudja.

**Példa**:

Ezt hasonlóan kell elképzelni, mint ezen a képen is látható, hogy idéző jelesen több biztonság szinte (zónára) bontjuk a dolgozok és az ügyfelek hozzá férését, csak nem túl nagy cég révén, illetve az egyszerűség érdekében mi ezt kevesebb ,,level-lel” (biztonsági zónával) oldottuk meg.

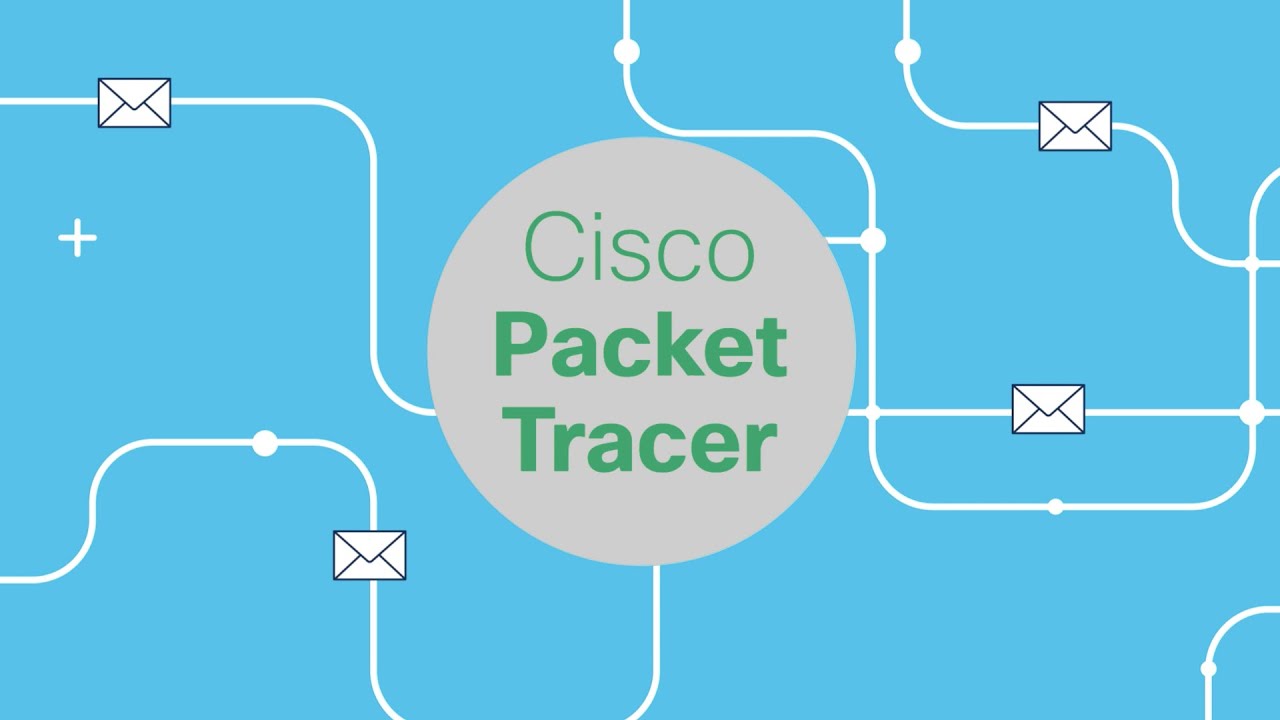


Kép:<https://www.semanticscholar.org/paper/Cyber-Security-Zone-Modeling-in-Practice-Gontarczyk-Mcmillan/87c06b0af4ecb9af3864b0d2a37a7818e83c3df2>

**3.2 Packet tracer :**

Mint ahogy a legelső bekezdésben volt említve a projekt feladathoz adót szempontokat is egyesitettük a cég igényeivel és a mi tudásunkkal, amit az elmúlt két év során szereztünk. Ezeket felhasználva alkottuk meg a vizsga munkánk packet tracer feladat részét. Ez a különböző részekhez volt lebontva mint például a hálózat szimulációnál.

kép:[\*](https://computingforgeeks.com/how-to-install-and-configure-openldap-server-on-debian/?fbclid=IwAR3vNZQtU5O4BoX8Fcoow_0H1jtFyX8fsPnGR42GpuY8i-PM1qoQ9oS8570)



**Elvárt konfigurációk Packet tracerben:**

Itt soroltuk fel, hogy milyen protokollokat kell megjelenítenünk a feladat során. Mindegyiket sora veszük egyesével és elmagyarázzuk, hogy a különböző protokollok mire szolgálnak, a velük való tapasztalatainkat és problémáinkat. Emelet miként és hogyan találtuk meg az adott problémákra a megoldást. A példák magyarázata végén leírjuk a feladattal kapcsolatos tapasztalatainkat és összegezük a teljes faladatrészt.

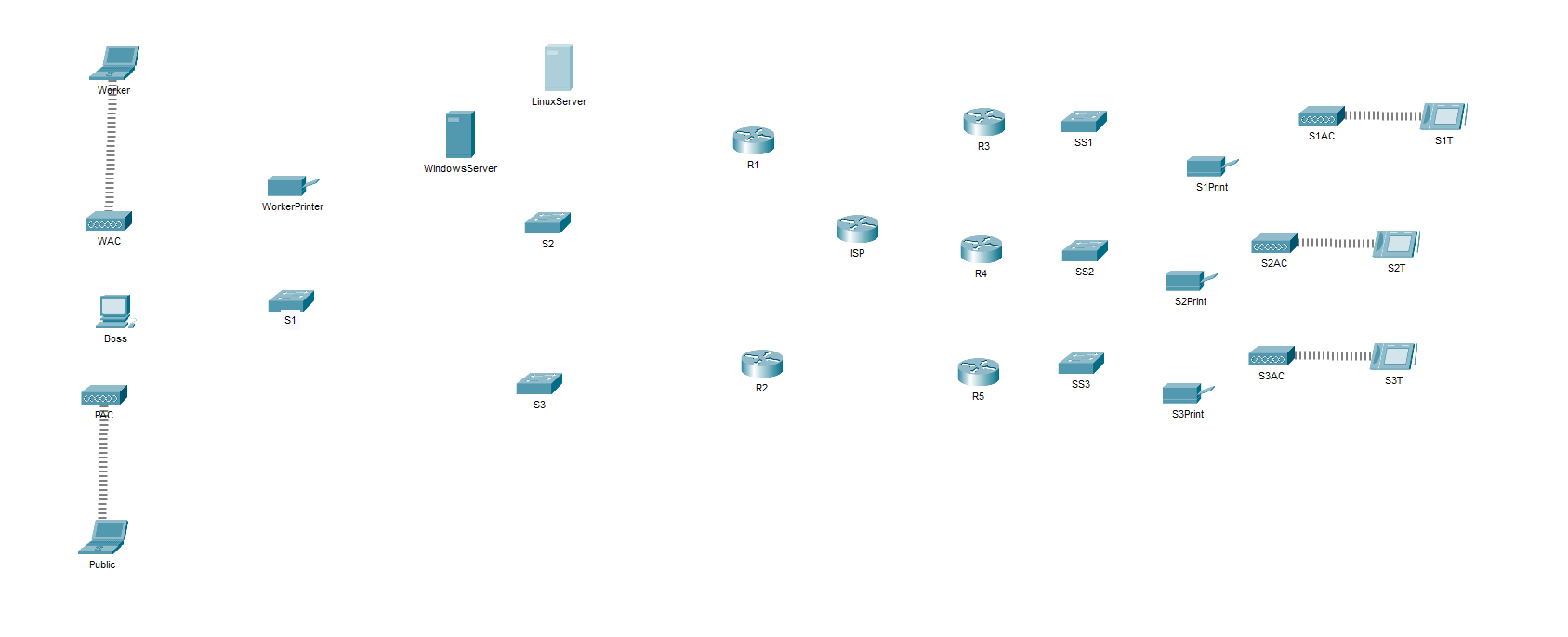
* Etherchanel
* PPP CHAP
* NAT 64
* VPN IPSEC
* Szerver statikus NAT
* ACL
* Port forward
* STP protokoll
* OSPF
* HSRP
* DHCP

**Konfigurációk és protokolok:**

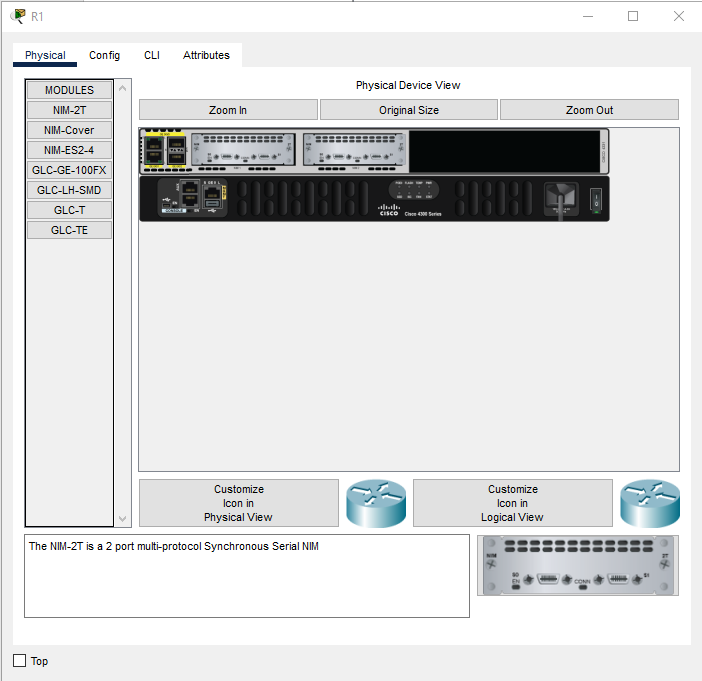
**Alapbeállítások:**

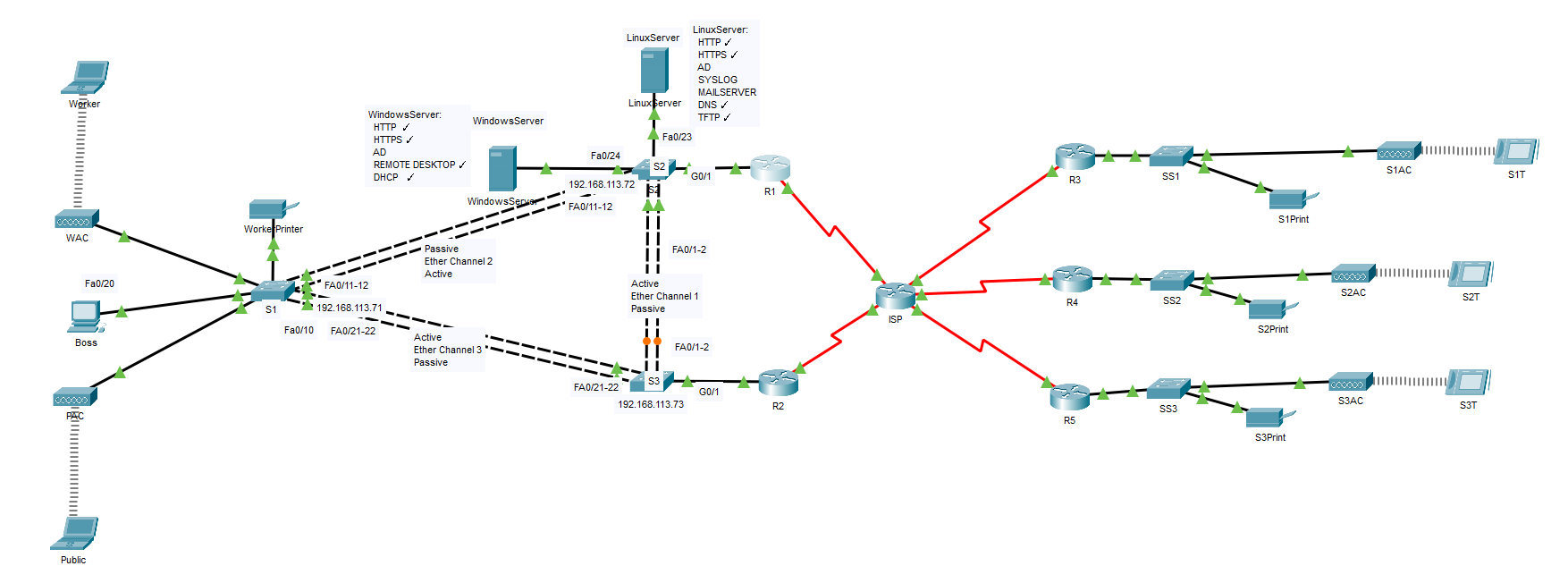
A feladat megkezdéséhez előszőr ki kell választanunk és el kell helyeznünk az eszközöket. Ez után elnevezzük őket.

**Példa:**

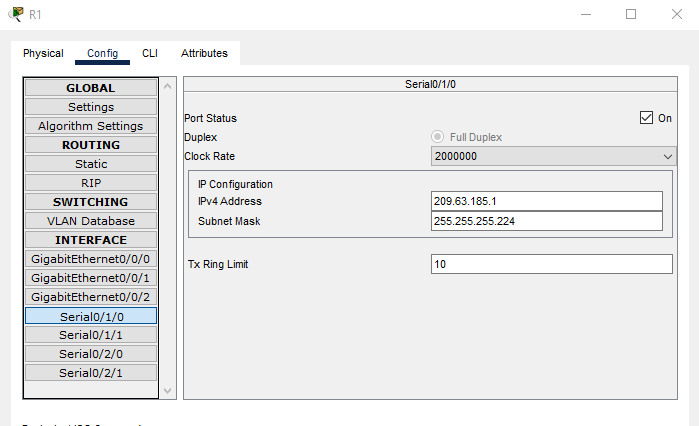


Utána összekötjük őket a szükséges kábellel, amit az általunk alakított topológia alapján teszünk meg. Ha az eszközöknél nem tudjuk olyan formátumú interfacebe kötni amire nekünk szükségünk van akkor bemegyünk az eszközt fizikailag megjelenítő fülre lekapcsoljuk azt és elhelyezünk a helyzetnek megfelelő bővítő kártyát (a képen az egyik router látható).





Miután összekötöttük őket a topológiánk alapján be konfiguráljuk őket az az ip címeket, maszkokat, gatewayt (alapértelmezettátjárót) és DNS adunk nekik. Ezt egy táblázatban vezettük le.



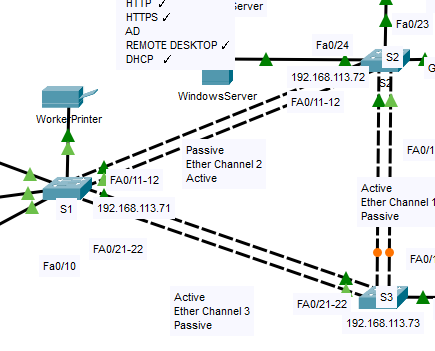
Ezt nem az összesnél tesszük meg mert bizonyos eszközök más módon kapnak ilyen alapbeállításokat ezt egy másik pontnál a ,,DHCP-nél” fejtük ki.

Alapbeállításnak tekintjük azt is, hogy elsők között állítottunk minden switchen és routeren enable jelszót. Most, hogy mindent beállítottunk tudjuk elkezdeni hálózatunk tényleges kiépítését.

**Etherchanel:**[**\***](https://net.fandom.com/hu/wiki/Etherchannel?fbclid=IwAR0PZnyhG3NTBXRan6rtcKqNFissT-meNRtZWlENCfaSnSALKGnpkMWmhwQ)

Ez egy port trunk1 technológia, amit a switchek használnak, meg engedi több Ethernet port2 összefogását egyetlen logikai kapcsolattá ezzel nőhet a sebeség és a hiba tűrés. Erre nekünk azért volt szükség a feladathoz mert alkalmaznunk kellet az STP protokollt, amiről egy későbbi pontban fogunk beszélni.

Alapvetően ennek a beállítása nem okozott különösebb gondot a kisebb bizonytalanságunk miatt utána néztünk egy régebbi feladatunkban, néhány hibánk kijavítása után már tökéletesen működőt. A legfőbb ,,problémánk” az volt, hogy többször át variáltuk a feladatott az újabb és újabb ötleteink miatt ezért többször is újra kellet írnunk.



A három switch, ami képen látható alkotják az etherchanelt. Ennek a létrehozásához kétféle mód volt mi a cisconál is használatos LACP-ét használtuk, ami annyit tesz, hogy a portókat aktív és passzív párokká tettük.

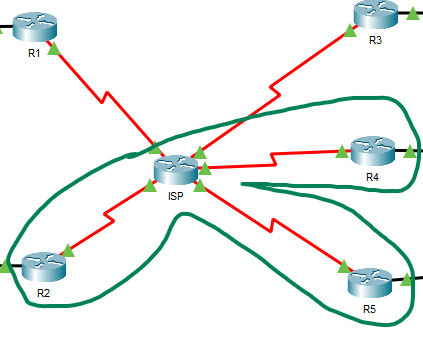
1.trunk: Egyszere több virtuális lan hálózatot engedünk a portón vagy portokon

2. Ethernet port: Hálózati csatlakozó.

**PPP CHAP:**

A PPP az a Point to Point Protocol ez kell ahhoz, hogy alkalmazni tudjuk a CHAPot ez PPP nélkül nem lehetséges.

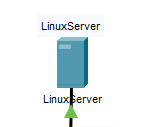
A CHAP Challenge-handshake authentication protocol ez egy biztonságos eljárás, hogy kapcsolódjunk a rendszere. Úgy működik, hogy miután felált a kapcsolat az egyik résztvevő kiküld egy kihívó üzenetet annak, aki kapcsolódni szeretne és a kapcsolódó eszköz válaszol egy megszerzet értékel, amit egy egyirányú HASH funkcióval kap (a PAP egy ehhez hasonló protokoll csak a CHAP sokkal biztonságosabb). Röviden a csatlakozó eszköznek ismerni kell a nevét és az enable jelszavát annak az eszköznek, amelyhez csatlakozni akar és az egész titkosítva van.

Ezzel a protokollal inkább olyas fajta problémáink voltak, hogy nem tudunk arról, hogy bizonyos más protokolok nem tudnak együtt működni vele ezért sokszor át kellet alakitanunk a hálózatunk egy részét, hogy benne maradhasson a feladatunkba.

Végül az lett a megoldás, hogy nem minden vonalon fog működni, hanem az R2-től az ISP keresztül az R4 és az R5 felé működik.

**Szerver statikus NAT:**[**\***](https://hu.gadget-info.com/difference-between-nat)

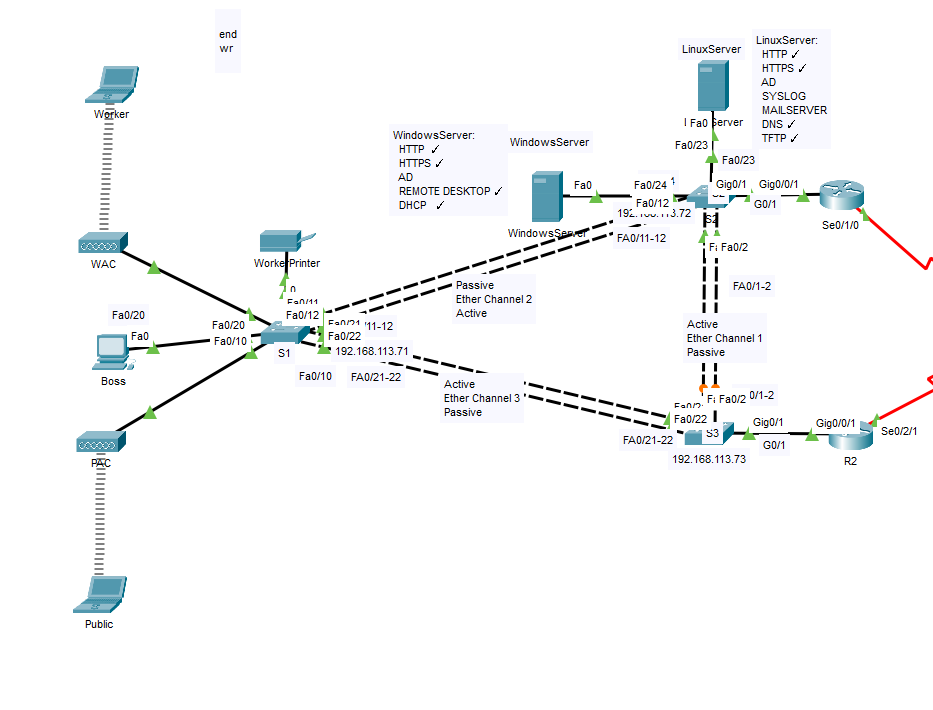
Azért van ki emelve így, hogy szerver statikus NAT mert a feladatban a szerveren kellet statikus NAT-ot használni. Önmagában ez azt jelenti, hogy mi egy olyan fix IP cím fordítást adunk meg a routernek, ami által elrejtjük a jelen esetben a mi szerverünk igazi IP címét, de még is elérhető a hálózaton kívülről egy általunk megadott publikus címen. Mint már mondtuk a követelmény az volt, hogy a szerverhez kell statikus NAT-ot használni úgy, hogy ezért nem jelenik meg a feladatunk más részein.



**Dinamikus NAT, PAT:**[**\***](https://hu.gadget-info.com/difference-between-nat)

Magáról a NAT-ról már beszéltünk a ,,Statikus NAT” pontnál úgy, hogy azt itt már nem fejtük ki. A dinamikus NAT lehetővé teszi, hogy a nem regisztrált magán címet a nyilvános ip címekből regisztrált nyilvános ip címre fordítsák.

De mi is az a PAT egy olyan dinamikus NAT típus, amelyen keresztül a cím fordítás konfigurálható a port szintjén és a fen maradó ip cím használat is optimalizált. A PAT több forrás helyi címét és portját egyetlen globális ip címre és portra leképezi a cél hálózaton továbbítható ip címekből. Itt az interface IP címét a port számmal együtt használják és több gazda gépnek ugyan az a címe mert a port szám egyedül álló.

A Worker alhálózatunkat engedjük ki a dinamikus nat segítségével az R2 routeren keresztül az internetre.

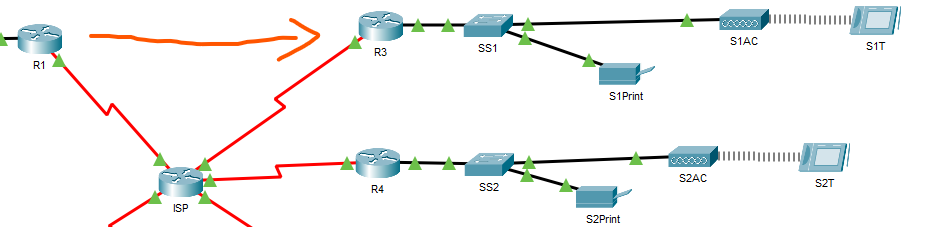
**VPN IPSEC:**[**\***](https://hu.wizcase.com/blog/teljeskoru-vpn-utmutato-kezdok-szamara/?fbclid=IwAR1IZXNKle_rHJ00HNxQFUVQbWdlYpPLMi8UdpWxryX8JsrO2PVrpcd4ukY)

A VPN egy virtuális magán hálózat, amivel esetünkbe biztonságos kapcsolatot létesit a központ és az egyik site között azzal, hogy adat védelmet és névtelenséget biztosit. Ezt azért helyeztük el a munkánkban mert részben kitétel volt és mert így betudunk mutatni egy olyan protokollt, ami szinte teljes körű védelmet biztosit az ip címek lekövetése ellen, illetve a jelszavak ellopása ellen mert mindent le titkosít ezért kiválóan védi a fájlokat is.

Jelen helyzetben mi itt side to side VPN-et alkalmaztunk, ami azt jelenti, hogy két létező hálózatott köt össze.

Itt több problémát is tapasztaltunk például a már említett CHAP működés képtelené teszi a VPN-et ezért ezt a kettőt nem vezethettük el ugyan azon vonalon. Ez jelentős időbe került mire rájöttünk úgy, hogy rengetegszer alkottuk újra akár az egész feladatott emiatt, hogy rájöjjünk erre. Egy idő után, hogy ne kelljen újra kezdenünk készítettünk külön mentéseket és azokban kísérleteztünk.

Illetve némely esettben nem működtek azok a parancssorok, amiket ismertünk a VPN elkészítéséhez, de miután magát a programot az az a Packet tracert újra indítottuk már működtek.

****

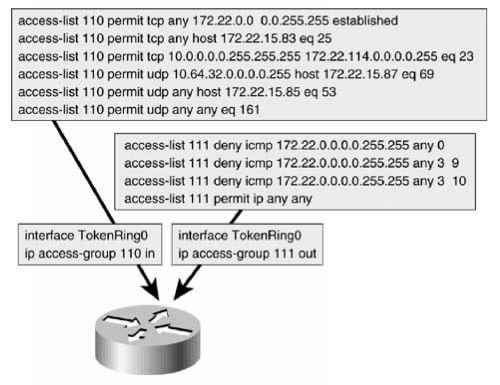
Az R1 és az R3 között alkottunk Side to site VPN kapcsolatot.

**ACL:**[**\***](https://www.ccexpert.us/routing-tcp-ip/calling-the-access-list.html)

Az az Access control list hozzá férés jogosultság ellenőrző, ami lényegében egy hozzá férési lista, ami tartalmazza, hogy kik haladhatnak át a routeren és melyik irányba (kifelé vagy befelé)

A feladatunkba több helyen is alkalmaztuk az access listeket például a dinamikus natnál mert részben ez alapján tud szűrni. Ezen kívül szükség van ahhoz, hogy létra hozzuk a VPN kapcsolatot mert enélkül nem tudnánk kommunikálni a IPsec tunnelbeés használtunk ACL-t, hogy le tiltsuk a Public hálózatot a Siteok-ról.

kép[\*](https://www.ccexpert.us/routing-tcp-ip/calling-the-access-list.html)



Nem volt kifejezeten probléma bár mikor elkészült akadtak problémák több dolog sem működött, de végül kiderült, hogy az nem köthető ehhez de eleinte azt hittük.

**DHCP:** [**\***](https://hu.education-wiki.com/7863438-what-is-dhcp)

A DHCP a Dynamic Host Configuration Protocol-t jelenti. Ez egy hálózati menedzsment protokoll, amely az alkalmazás rétegben található. A DHCP segítségével az Internet Protokoll IP-címet dinamikusan hozzá lehet rendelni bármilyen eszközhöz vagy csomóponthoz, hogy ezek az IP-vel kommunikálhassanak. A DHCP alapvető célja egy egyedi IP-cím hozzárendelése a hostokhoz. Egyéb hálózati címeket is biztosít, például -

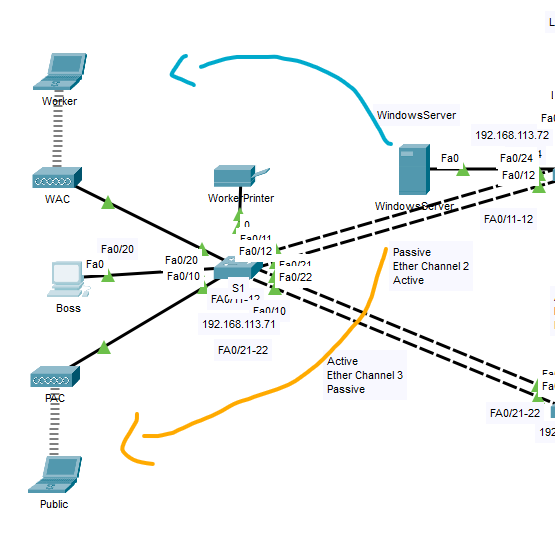
Alhálózati maszk

Router címe

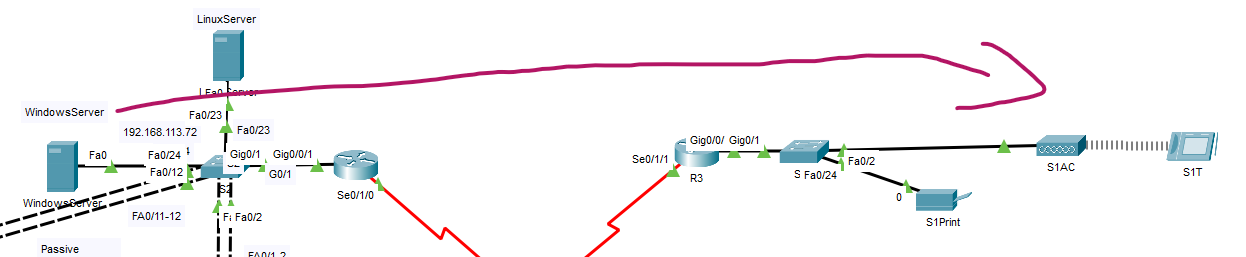
DNS-cím

Eladó osztály azonosítója

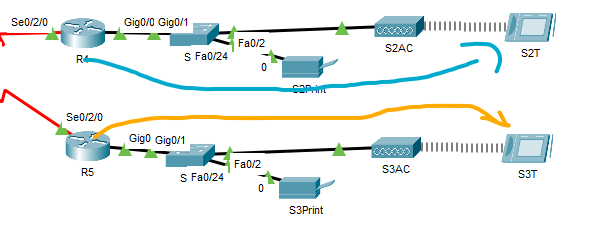
A mi feladatunkba nagy részében megjelenik a DHCP. Alap esetben a router osztaná a DHCP ez is a leggyakoribb, de mivel nekünk kellet telepíteni szervereket egyszerűbb volt a szervereknek az az a Windows szervernek kiadni ezt a munkát így használva a felhőszolgáltatásokban megszerzet tudásunkat és csökkenteni a terhelést a routeren.



A centerben két virtuális alhálózaton megy két DHCP folyamat. Az egyik a Worker felé a másik a Public felé. Itt a két kivétel a Worker Printer és a Boss mert ők statikusan kapnak IP címet.



A Site 1 kap még DHCP-t a VPN kapcsolaton keresztül.

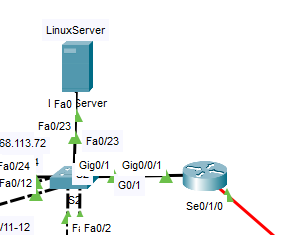


A többi Site a saját routereik osztják a DHCP-t mert itt nem építettünk ki VPN kapcsolatot. Kivéve a Printerek mert ők minden alhálózatban statikusan kapnak IP címet.

**Port forwarding:**[**\***](https://en.wikipedia.org/wiki/Port_forwarding)

Tulajdon képen ez nem különbözik sokban a statikus NAT-tól mivel Port forwarding arra való, hogy egy konkrét porton keresztül engedjük ki a szervert, amivel egy konkrét szolgáltatáshoz juttatjuk el. Úgy, hogy a statikus NAT parancsot, amit a szervere irtunk ki bővítettük a TCP1 protokolal és a 80-portal hogy elérjék a webszervert

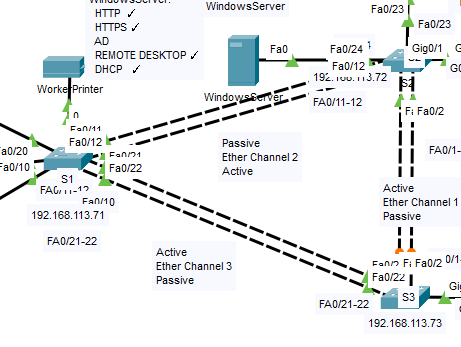
1. A TCP protokol egy folyamatos kapcsolatot igénylő protokol ami le ellenőrzi hogy az akinek küldi az információt még figyeli az információ folyamot ha nem akkor megszakítja a kapcsolatot (Lassabb mint az UDP).



Ezen a szerveren és routeren engedtük át a port forwardingot statikus NAT-al.

**STP protokol:**[**\***](https://szit.hu/doku.php?id=oktatas%3Ahalozat%3Acisco%3Aredundans_kapcsolok&fbclid=IwAR2lc-iTfFbANQgSBZbfe5okX-UA6PI3D8XTAgOaHsPn_T7WEXCAg6UkGqA)

Az STP protokol a feszitőfa algoritmust használja. AZ algoritmus kiválaszt egy kapcsolót, amelyet referenciaként használja ezt a kapcsolót gyökérponti hídnak nevezzük. A lényege az, hogy redundást kapcsolatot építsen ki a LAN eszközöknél és a hurok kialakulását hivatott meg akadájozni.



A három switch jelzi és amit az imént írtuk a hurkok kialakulása ellen használjuk ezt a protokolt a hálózatunkban.

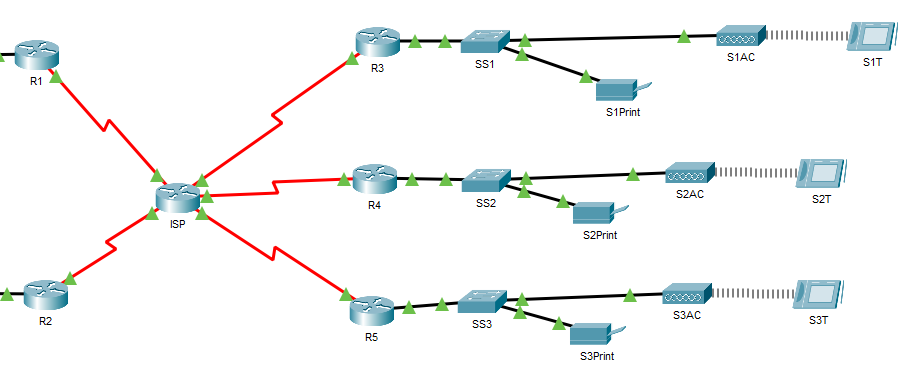
Bár nem csináltuk ezt túl gyakran többször beszéltünk róla az elméleti órákon és nem túl bonyolult parancssorokból áll úgy, hogy probléma nélkül megoldottuk.

**OSPF:**[**\***](https://hu.education-wiki.com/3990219-what-is-ospf)

Az OSPF az Open Shortiest Path-ot jelenti. Először egy útválasztási protokoll, amelyet az Internet Protocol (IP) hálózatban használnak. Az OSPF kapcsolat állapot-irányító algoritmusokat használ, és egyetlen autonóm rendszeren belül működik. Ez egy linkállapotú, nyílt, szabványos útválasztási protokoll.

Az OSPF az egyik legszélesebb körben használt protokoll a nagyvállalati hálózatokban. Úgy tervezték, hogy támogassa a változó hosszúságú alhálózati maszkolás (vagy VLSM) és az osztály nélküli tartományok közötti útválasztás (CIDR) címet, modelleket. Az OSPF egyik erőssége, hogy gyorsan felismeri a topológiában bekövetkező változásokat, például a kapcsolat hibákat, és ha a változásokat megtalálják, egy új hurok nélküli útválasztási struktúra csupán másodpercek alatt konvergálható.

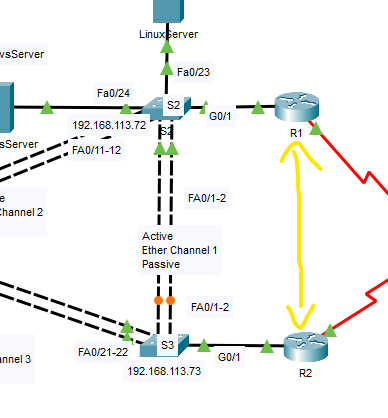
Mi ezt a feladatunkban mondhatni az egész hálózatot átfogóan használtuk főleg az internet (ISP) szimulálásánál.



OSPF-fel már sokat foglalkoztunk a 2 év során úgy hogy nem okozott különösebb problémát a használata. Csak akkor változtatunk rajta vagy vettük ki teljesen esetleg, ha éppen egy másik protokol hibáira próbáltunk rájönni.

**HSRP:**[**\***](http://www.inf.u-szeged.hu/projectdirs/bohusoktat/regi/szhaloanyagok/esszek2006/levelezok/HSRP.pdf?fbclid=IwAR11dxdQ8wY83VL3zqmKP5S-91EKsZT16Xi2ohfnVVNmcYoj4Bq8L6NwUmE)

Ez a Hot Standby Routing Procotol. A HSRP a Cisco Systems Inc. által kidolgozott megoldás, amely segítségével hibatűrő IP hálózattokat lehet építeni. A protokoll megvéd az alapértelmezett átjáró (útválasztó) meghibásodásától azon hostoknál is, melyek nem képesek dinamikusan megtanulni az átjáró címét. A protokollt többszörös hozzáférésű (multi-access), multicast vagy broadcast képes LAN-okra fejlesztették ki. A HSRP-t nem a többi dinamikus átjáró felfedező protokoll helyett készítették, hanem a nagyszámú erre képtelen hostnak (pl: PC Windows operációs rendszerrel). A HSRP használatánál útválasztók egy csoportja létrehoz egy virtuális útválasztót (átjárót) a LANon lévő hostoknak, ezt a csoportot HSRP vagy Standby csoportnak nevezzük. A csoportból kiválasztódik egy aktív és egy készenléti útválasztó. Az aktív lesz a felelős a csomagok továbbításáért. Amikor az aktív útválasztó meghibásodik, akkor a készenléti átveszi a helyét. Amikor a készenléti hibásodik meg vagy lesz aktív, akkor egy másik útválasztó lesz a készenléti. Bármennyi útválasztó is van a csoportban, csak az aktív továbbítja a csomagokat.



Ez lényegében a hálózatunkba a hiba tűrést javította mivel ha kiesik az egyik router a másik router ami rendelkezik a virtuális standby ip-vel át veszi a helyét.

A protokol használata közben volt egy parancs a priority amit általunk ismeretlen

okokból a router rendszeresen törölt a konfigurációjából, de szerencsére enélkül is működik mert erre nem találtunk megoldás.

**IP címek táblázata**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Eszközök | Interfacek | IP címek | Maszk | Gateway |
| R1 | Gig0/0/1.10 | 192.168.63.2 | 255.255.255.0 (24) |  |
| Gig0/0/1.20 | 192.168.113.77 | 255.255.255.128 (25) |  |
| Se0/1/0 | 209.63.185.1 | 255.255.255.224 (27) |  |
| R2 | Gig0/0/1.10 | 192.168.63.3 | 255.255.255.0 (24) |  |
|  | Gig0/0/1.20 | 192.168.113.78 | 255.255.255.128 (25) |  |
|  | Se0/2/1 | 209.63.185.129 | 255.255.255.224 (27) |  |
| ISP | Se0/1/0 | 209.63.185.30 | 255.255.255.224 (27) |  |
|  | Se0/1/1 | 209.63.185.62 | 255.255.255.224 (27) |  |
|  | Se0/2/0 | 209.63.185.126 | 255.255.255.224 (27) |  |
|  | Se0/2/1 | 209.63.185.158 | 255.255.255.224 (27) |  |
|  | Se0/3/0 | 209.63.185.94 | 255.255.255.224 (27) |  |
| R3 | Gig0/0/1 | 192.168.116.1 | 255.255.255.0 (24) |  |
|  | Se0/1/1 | 209.63.185.33 | 255.255.255.224 (27) |  |
| R4 | Gig0/0/1 | 192.168.114.1 | 255.255.255.0 (24) |  |
|  | Se0/2/0 | 209.63.185.65 | 255.255.255.224 (27) |  |
| R5 | Gig0/0/1 | 192.168.115.1 | 255.255.255.0 (24) |  |
|  | Se0/2/0 | 209.63.185.97 | 255.255.255.224 (27) |  |
| Worker |  | DHCP |  | 192.168.113.79 |
| Public |  | DHCP |  | 192.168.63.1 |
| Boss |  | 192.168.113.74 | 255.255.255.128 (25) | 192.168.113.79 |
| WorkerPrinter |  | 192.168.113.75 | 255.255.255.128 (25) |  |
| S1 | Vlan20 | 192.168.113.71 | 255.255.255.128 (25) | 192.168.113.79 |
| S2 | Vlan20 | 192.168.113.72 | 255.255.255.128 (25) | 192.168.113.79 |
| S3 | Vlan20 | 192.168.113.73 | 255.255.255.128 (25) | 192.168.113.79 |
| Win Szerver |  | 192.168.113.80 | 255.255.255.128 (25) | 192.168.113.79 |
| Linux Szerver |  | 192.168.113.90 | 255.255.255.128 (25) | 192.168.113.79 |
| S1Print |  | 192.168.116.2 | 255.255.255.0(24) | 192.168.116.1 |
| S2Print |  | 192.168.114.2 | 255.255.255.0(24) | 192.168.114.1 |
| S3Print |  | 192.168.114.2 | 255.255.255.0(24) | 192.168.115.1 |
| S1AC, S2AC, S3AC |  |  |  |  |
| Tűzfal |  | 192.168.113.76 | 255.255.255.128(25) |  |

Ezt a táblázatott azért csináltuk, hogy láthatóak legyenek milyen címeket, maszkokat és hasonlókat használtunk. Valamint a feladat készítése közben is a segítségünkre volt mert jobban át láttuk a topológiánkat.

**3.3 Szerverek és felhőszolgáltatások:**

Egy cégnek nem csak fizikális eszközöket kell biztosítani, hanem különböző felhőszolgáltatásokat, szervereket is. Azt, hogy éppen milyeneket az a cégtől és a vevőtől függ.

Általunk biztosítva lesz egy Windows és egy Linux alapú szerver is. A Windowsból a 2019-et, Linuxból debiánt és abból is a legújabbat a debian 11.2 -et. Tapasztalataink, ismereteink alapján választottuk ezt a kettőt.

**Windows szerver szolgáltatások**[**\***](https://hu.wikipedia.org/wiki/Windows_Server)

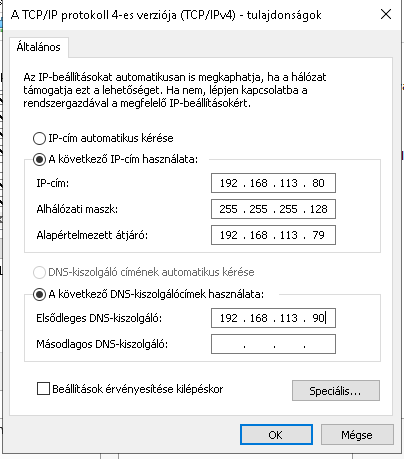
* http és HTTPS (az SSL certificate)
* Activ directory
* DHCP
* Távoli asztal elérés

**Windows Szolgáltatások**

**Alapbeállítások:**

Amiket minden windows szerveren alapvetően be kell állítani, hogy bármit is tudjunk csinálni

* + A szerver neve
  + IP címe
  + Alapértelmezettátjáró
  + DNS (internethez)

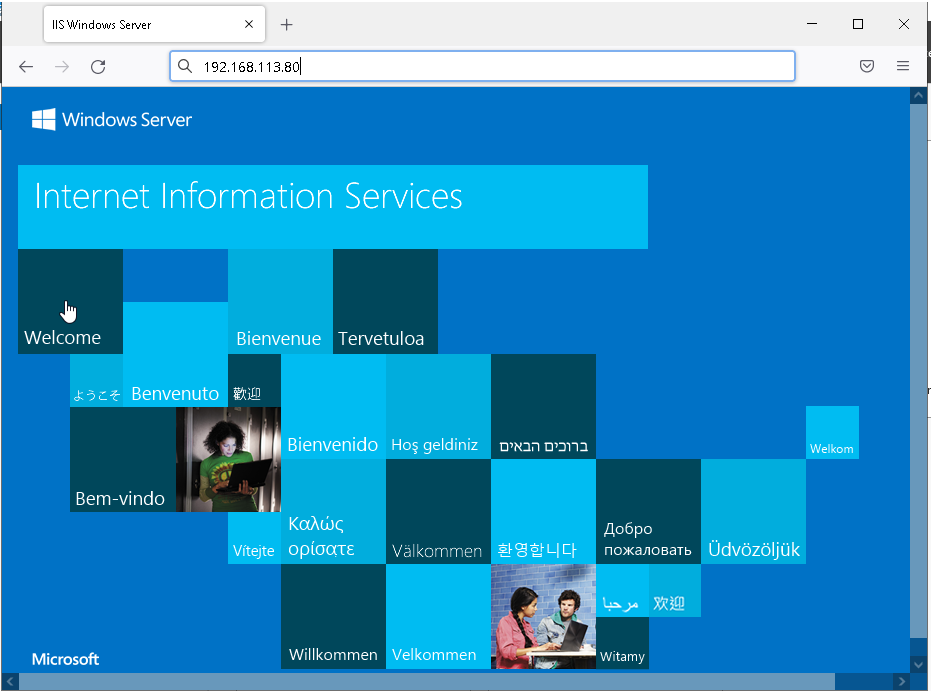


Ezek nélkül nem tudnánk semmilyen frissítést vagy telepitést csinálni a szerveren. Hiba nélkül és szinte már reflexből ment nekünk.

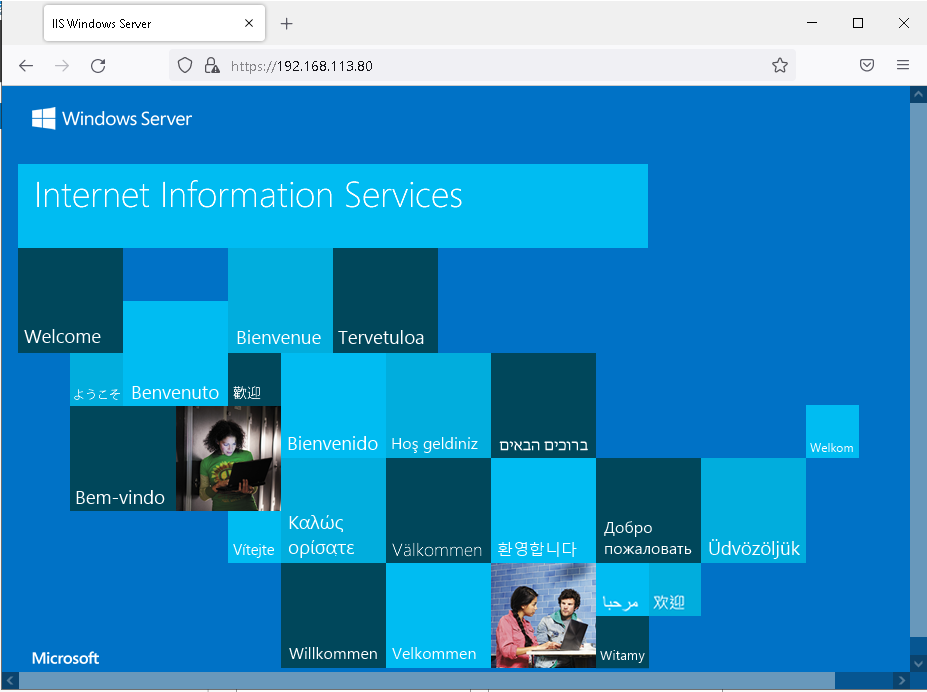
**HTTP és HTTPS:**[**\***](https://heritage-offshore.com/net-admin/mi-az-iis-windows-web-server-hogyan-kell-hasznalni/?fbclid=IwAR0OsBFM4_EpZlegmA6Pf5r793ztjdWiJ4F-XJ_ef-dGmOY_SZ-S3A3wSKM)

Ahhoz, hogy ezeket telepíteni tudjunk IIS szolgáltatást kell telepítenünk. Mint webszerver Az IIS-nek megvan a maga Process Engine amely kezeli az összes kérést az ügyféltől a szerverig. Lényegében az ügyfél kérést küld a kiszolgálónak, majd az IIS feldolgozza a kérést, és választ küld az ügyféllel. Az IIS feldolgozási architektúrája két különálló rétegre osztható. A http 80-as porton közlekedik egy weblapot biztosit nekünk a HTTPS ugyan ez csak 443-as porton közlekedik és SSL-t használ. Semmilyen probléma nem merült fel a telepités során.

HTTP



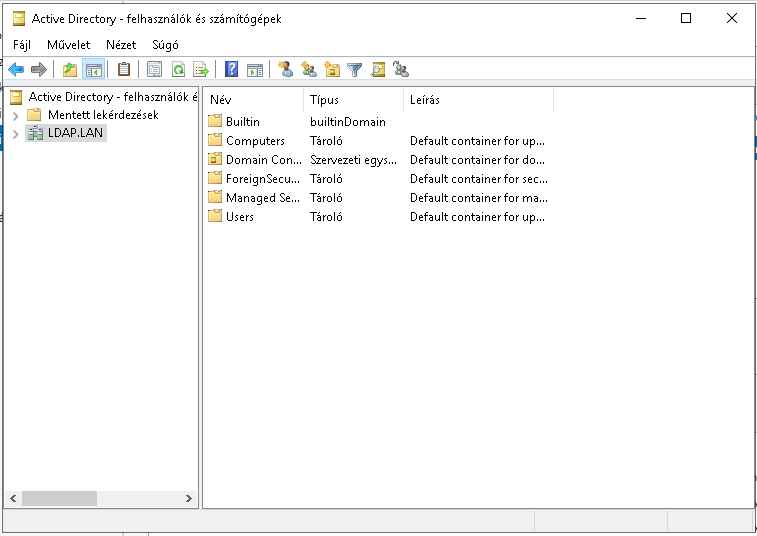
HTTPS

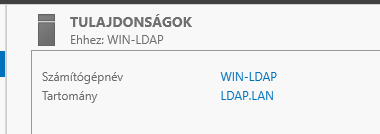


**Activ directory:**[**\***](https://hu.wikipedia.org/wiki/Active_Directory?fbclid=IwAR2eeKnKDRN5_WMY9F9elbPgFMuNPO7skVzsECL59P1ik4Eb89gQI-z7R1g)

Az Active Directory címtár az adatbázisból és az azt futtató Active Directory szolgáltatásból áll. Fő célja a Windowst futtató számítógépek részére autentikációs és autorizációs szolgáltatások nyújtása, lehetővé téve a hálózat minden publikált erőforrásának (fájlok, megosztások, perifériák, kapcsolatok, adatbázisok, felhasználók, csoportok stb.) központosított adminisztrálását – vagy éppen a rendszergazdai jogosultságok delegálásával a decentralizált felügyeletét. Számos különböző erőforráshoz (megosztott mappák, nyomtatók, levelezés stb.) egyetlen felhasználónév/jelszó páros megadásával biztosít hozzáférést (Single Sign On, SSO).

A mi általunk készített domain neve LDAP.LAN. Egyaránt a Linux és a Windows szerveren is megtalálható.



****

**DHCP:**

A DHCP működését már elmagyaráztuk a packet tracer feladatnál. Itt másfelületen állítjuk be, de funkciói ugyan az és ugyan azokat a hálózattokat állítottuk be.

Hálózataink:

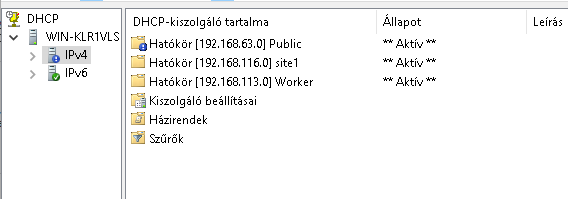
* 192.168.113.0/25
* 192.168.63.0/24
* 192.168.116.0/24

DNS:

* 192.168.113.90/25

Alapértelmezettátjáró:

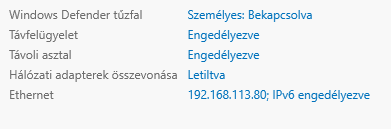
* 192.168.113.79
* 192.168.63.1
* 192.168.116.1

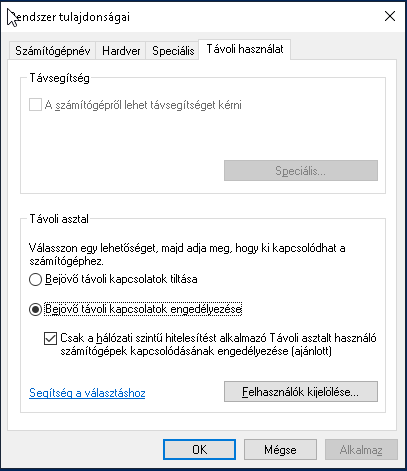


Az utolsó DHCP-vel, amit a VPN-en keresztül vezetünk nem sikerült elsőre.

**Távoli asztal elérés:**[**\***](https://support.microsoft.com/hu-hu/windows/a-t%C3%A1voli-asztal-haszn%C3%A1lata-5fe128d5-8fb1-7a23-3b8a-41e636865e8c?fbclid=IwAR2v6dtNb2Zqe_iga1y68TLdBsri0KM0NBRPPcCFTsPy1L1M27WzZGbilOY)

A Távoli asztal lehetővé teszi, hogy Windows, Android vagy iOS rendszerű eszközén távolról csatlakozzon egy Windows 10 rendszerű számítógéphez vagy esetünkben a szervert is lehet kezelni távolról.





Problémát nem tapasztaltunk nagyjából két parancsból ált amit alkalmaztunk a power shellben

**Linux szerver szolgáltatások**

* HTTP és HTTPS
* AD
* SYSLOG
* DNS
* TFTP
* Nyomtató szerver

**Linux szolgáltatások**

**Alapbeállítások:**

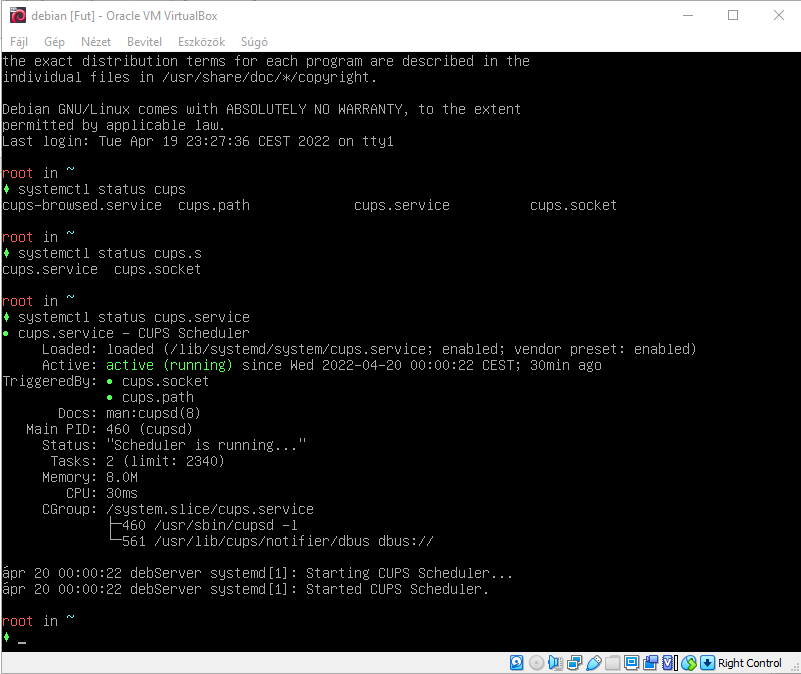
Amiket minden linux szerveren alapvetően be kell állítani, hogy bármit is tudjunk csinálni

* + IP címe
  + Alapértelmezettátjáró
  + DNS (internethez)

Ez a unix alapu szerver volt a másik követelmény mi a debian 11.2-őt választottuk. Mert ezzel van a legtöbb tapasztalatunk, az internet és a tanáraink is ezt ajánlották.

**Nyomtató szerver, avagy CUPS**

Mivel úgy terveztük, hogy vannak nyomtatók ezért egy printer server szolgáltatást is raktunk fel és azért választottuk a cups-ot mert ezt

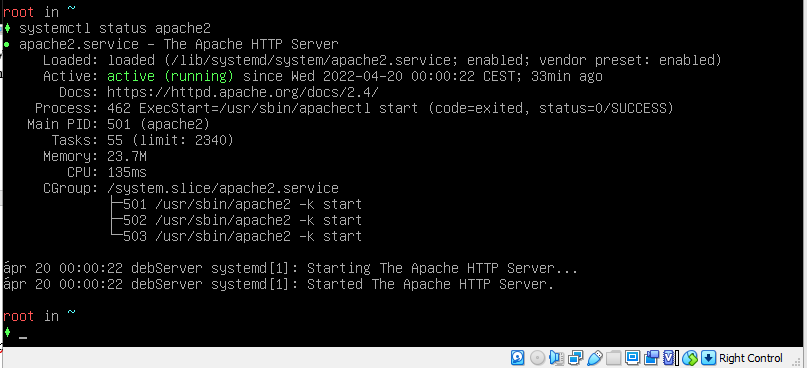


Tanultuk meg az óráink során és viszonylag könnyen is kezelhető. Annyi probléma volt nehezen vette fel a hálózatban lévő printert (nyomtatot).

**HTTP és HTTPS:**

Ennek a működését már elmagyaráztuk a windows szervernél.

Ezt a linuxon belül ezt az apache 2 telepitésével értük el. Igazából az apache2 ugyan azt a feladatott látja el, mint a windows-nál az IIS.



Ez a része teljesen probléma mentesen indult

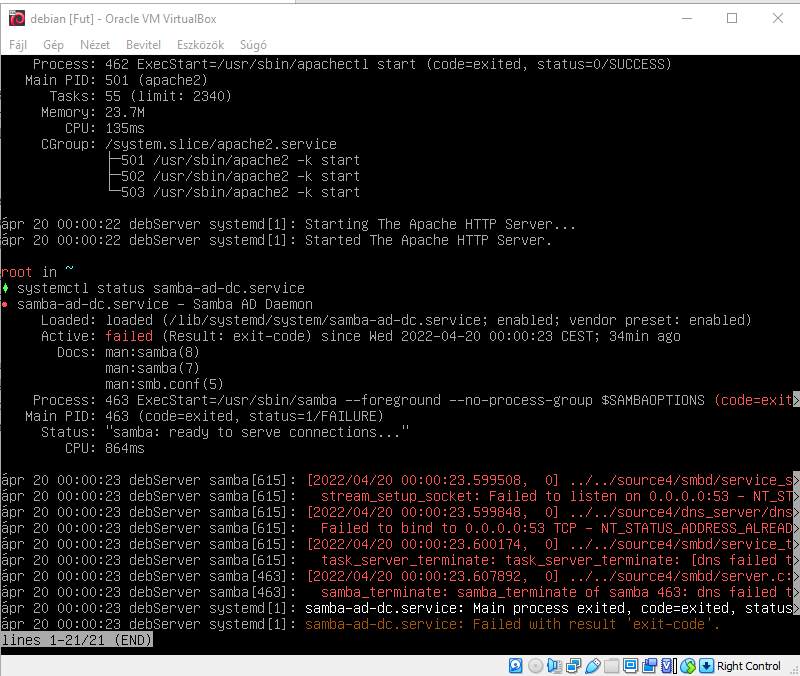
**Activ Directory:**

Ennek az elméletet szintén már leírtuk a windows szervernél. A debiánban ugyan azt a funkciót látja majd el, mint a másik szerveren lehetőleg együtt működve vele. Más fajta szerver lévén más, hogy kell telepíteni, de csak ennyi a különbség.

SAMBA 4 és AD:

Samba egy a Windows „Fájl és nyomtatómegosztás”, illetve a „Microsoft Networks Kliens” szolgáltatásokat, valamint sok hasznos segédprogramot tartalmazó programcsomag. Illetve ez üzemelteti az active directoryt.

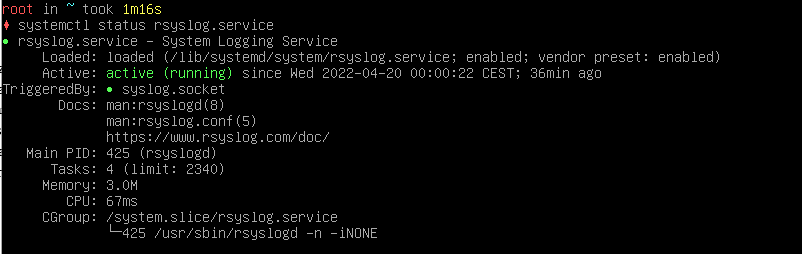
A szoftvercsomag hozzáférhető forráskódként, illetve a fontosabb Unix/Linux verziókhoz hozzáférhető lefordított (bináris) állományként.



Többször is elő fordult, hogy vagy nem volt hajlandó elindulni, vagy nem működőt együtt a windows activ directory-jával. Ezért sokszor újra kellet telepíteni amig megtaláltuk a megfelelő beállításokat. Nem találtuk meg a megfelelő beállításokat mert ugyan egyszer sikerült el indítani, de többször nem.

**SYSLOG:**[**\***](https://hu.theastrologypage.com/system-log)

A rendszernapló (syslog) az operációs rendszer (OS) események rekordját tartalmazza, amely jelzi a rendszer folyamatainak és az illesztőprogramok betöltésének módját. A syslog megjeleníti a számítógép operációs rendszerével kapcsolatos információs, hiba- és figyelmeztető eseményeket. A naplóban szereplő adatok áttekintésével a rendszergazda vagy a felhasználó hibaelhárításával azonosíthatja a probléma okát, vagy azt, hogy a rendszer folyamatainak betöltése sikeres-e.

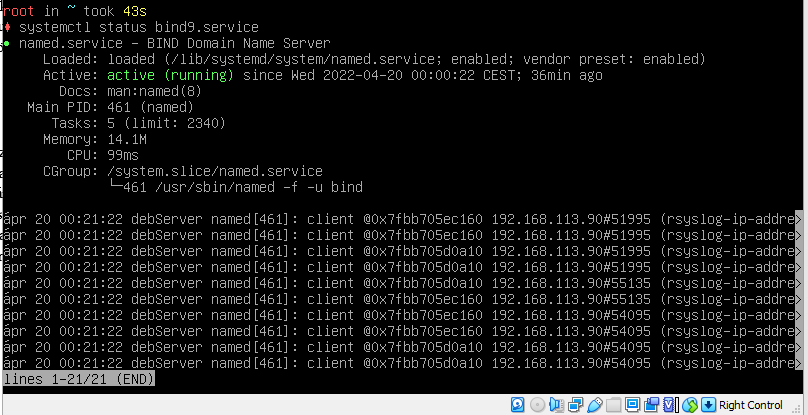


Eredetileg a syslogot az LDAP adta volna a feladatunkban, de mivel az nem működött és kiszedtük ezért más, hogy oldottuk meg.

**DNS:**[**\***](https://www.domdom.hu/domain-regisztracio/mi-az-a-dns-rendszer?fbclid=IwAR3YM605kYJS_pORziLixQ4Wv8N2b--sQI-QW4T6sFDO_w55HRFDUUHvwEQ)

A DNS rendszere egy olyan hatalmas adatbázis, amiben nevek és számok vannak egymáshoz rendelve. Például a google.com domain névhez a 172.217.20.14 IP cím tartozik. Ennek köszönhetően, ha a böngészőnkbe beírjuk, hogy google.com, akkor a 172.217.20.14 IP címen lévő gép adatait érjük el.

Az internet hálózatához hasonlóan, a DNS rendszere is egy osztott hálózat. Nem egyetlen DNS adatbázis van, hanem sok DNS szerver szerte a világon, amelyek mind képesek egymással kommunikálni.



Esettünkben nagy szerepe a hálózatunkban a DNS-nek mivel szükség van az activ directory domain controlerhez. Illetve általa tudunk a webszerverekhez csatlakozni névvel.

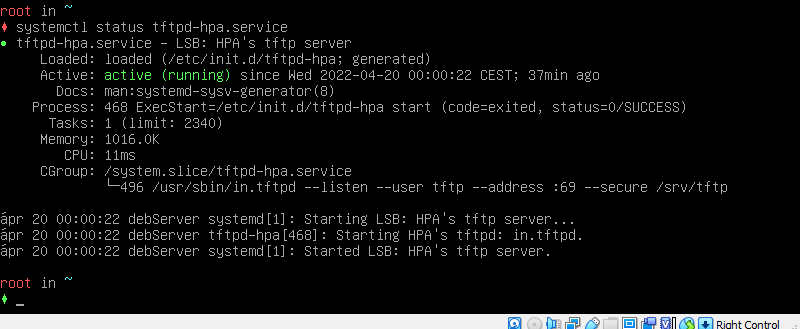
Egyszer-kétszer rosszul állítottuk be de hamar kiküszöböltük.

**TFTP:**[**\***](https://hu.eyewated.com/trivialis-fajlatviteli-protokoll/)

A TFTP jelentése a Trivial File Transfer Protocol. Ez egy technológia a fájlok hálózati eszközök közötti átvitelére, és az FTP (File Transfer Protocol) egyszerűsített változata.

A TFTP-t az 1970-es években fejlesztették ki olyan számítógépek számára, amelyekben nincs elegendő memória vagy lemezterület a teljes FTP támogatáshoz. Manapság a TFTP a fogyasztói szélessávú forgalomirányítókon és a kereskedelmi forgalomban kapható routereken is megtalálható.

A házi hálózati rendszergazdák néha TFTP-t használnak az útválasztó firmware frissítéséhez, míg a hivatásos adminisztrátorok a TFTP-t is használhatják a szoftverek vállalati hálózatokon történő terjesztésére.



Nálunk a TFTP szükséges volt a hálózathoz, de nem is igazán a fájlok megosztása miatt, hanem a cisco eszközök miatt. Mert ezek az eszközök csak ezen a protokolon keresztül tudják lementeni konfigurációjukat egy szervere.

Ennek telepitésével és működésével semmi problémánk nem volt

**TAPASZTALATAINK**

**4.1 Packet Tracer**

A feladat elkészítése során több esetben amikor problémák adottak több mentést készítettünk a feladatról, hogy ne kelljen újra kezdenünk ha esetleg valami nagyobb dolgot el rontanánk a kísérletek során.

A tavalyi évhez képest rengeteg új protokolt tanultunk, amiket itt alkalmaznunk kellet. Emiatt volt néhány dolog, amit nem egészen értetünk elsőre, de aztán pár gyakorló feladat után vagy tanitó videó után megértetünk és így már tudtunk vele dolgozni

**4.2 Windows szerver**

Elsőre vizuálisan lett telepítve szerencsére a windows 2019-nek nagyon segítőkész felülete van úgy, hogy probléma mentesen tudunk telepíteni mindent viszont, hogy legyen scripthez alapanyag ezért power shellben is fel lett telepítve kivéve az activ directory.

**4.3 Linux szerver**

Talán ezzel a résszel volt a legtöbb problémánk rengeteg hiba merült fel, amikre sokáig nem tudtunk rájönni, van amelyikre egyáltalán nem sikerült megoldást találnunk úgy, hogy ki kellet szedni a projektből. A folyamatos tesztelések alatt sokszor kellet újra tenni, gyakorlatilag az utolsó pillanatban is egyszer újra kellett tenni. Az a szerencse, hogy gyorsabban települ, mint a Windows.

**PROBLÉMÁK AZOK MEGOLDÁSAI:**

Mint minden feladatban természetesen itt is akadtak hibák, problémák, amik megoldásra szorultak, amit úgy gondolunk a csapatunk jól kezelt és együttesen megoldottuk azokat

Az egyik igen komoly probléma az volt, hogy egy félreértés során rosszul, hiányosan dolgoztuk ki a feladatunkat, ami nagyjából másfél hónappal a leadási határidő előtt derült ki. Ez által akkor majdnem teljesen ellőről kellet kezdenünk a záróvizsgánk nagyrészét. De a félreértéseket tisztáztuk és sikeresen időben elkészültünk a megfelelő minőségű munkával.

A másik, ami jócskán megnehezítette a dolgunkat az az volt, hogy egy olyan protokolal akartunk és kezdtünk is dolgozni a szervereken, amit nem csak hogy mi nem ismertünk igazán, hanem még a segítséget nyújtó tanáraink se. Ez volt az LDAP

A követelmény az volt, hogy legyenek automatizálva a mentések és a telepitéseket. Ezeket nem tudtuk meg tenni mert még nem tanultuk és nem maradt időnk rá. Illetve nem teljesen igaz mert a script, amit tettünk bele az hasonlóan működik. Mert ugyan a scriptet nekünk kell elindítanunk viszont, ha ezt megtettük onnantól mindent magától telepit.

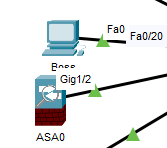
**LDAP**: [\*](http://padre.web.elte.hu/ldap.html?fbclid=IwAR2fLUE6Uqf9nJWNMd26jClPOvmg80WqPLYzA37wD8Zo7-4riDHZJSKcd3M)

Ez nem több egy protokollnál, nem egy konkrét szoftverről van tehát szó. Ez a protokoll directory szolgáltatások elérését szabályozza.

Majd nem a feladatunk végén jöttünk rá hogy hiába próbálkozunk vele sajnos ez most nem fér bele az időnkbe úgy hogy lemondtunk róla és inkább csak sima activ directoryt használunk helyette.

Ezen kívül minden feladat közben felmerülő nehézséget a protokolok felsorolásánál már leírtunk.

Végezetül annyi, hogy a legvégén elhelyeztünk egy tűzfalat a packet tracerbe ezért nem látható egyik képen sem.



**ÖSSZEGZÉS:**

Összeségében izgalmasnak találtuk, akadtak problémák, de végül sikerült mindent megoldani (ezeket a következő pontban fejtük ki). Meglehetősen stresszes volt némely helyzetben amikor úgy éreztük, hogy megrekedtünk és nem tudtuk hogyan tovább ilyenkor a konzulens tanárunk biztatott minket, aminek köszönhetően tudtunk tovább haladni. Izgultunk, hogy jól sikerüljön és hogy be tudjuk időbe fejezni. Azért be kell látnunk voltak részek, amit kifejezeten élveztünk, mint például a feladat kitalálása és annak megtervezése, a csapatmunka a társainkkal és a tanárainkkal, hogy új dolgokat vagy más módszereket találtunk aztán próbáltunk ki a vizsga munkaelkészítéséhez. Még akkor is, ha sajnos nem mindegyik sikerült és így nem hagyhattuk benne a végeredménybe.

Az utolsó közös konzultálásnál azt is leültünk megbeszélni, hogy őszintén ki hogyan vet részt a munkába. Nyilván még a legjobb csapatokban is vannak összezördülések ezek nálunk sem voltak máshogy mindenkinek volt párszor rossznapja vagy épp nem ment úgy neki a munka. Más másemberek vagyunk különböző munka morállal volt amelyikünk otthon tudott inkább haladni volt, aki az iskolában. A közös megegyezésünk alapján azt kell mondjuk, hogy mindannyian igyekeztünk 100% nyújtani a munkába és mi úgy gondoljuk, hogy ez sikerült is.

Amig a projekt munkát készítettük rengeteg tapasztalatot szereztünk és még több újdolgot tanultunk.

**TESZTEK**

Mivel a feladatunkról készül egy 2-3 perces teszt videó a dokumentációba nem helyeztünk el se képet se videókat a tesztelésről.

**FORRÁSOK:**

Ide elhelyeztük az összes olyan weboldalt, amit felhasználtunk információ szerzésre vagy például az összes eszköznek a weboldala, amit az, eszköz táblázatnál felhasználtunk.

Ahol használtunk bármilyen webes segítséget ott csillaggal hozzá kapcsoltuk a weboldalt a feladat címéhez vagy azokhoz a képekhez, amiket szintén ilyen oldaltól használtunk fel. Amely szövegek, illetve képek mellet nincs ilyen az a saját tulajdonunkba lévő információ, képek.

* [Calling the Access List - Routing TCP IP - Cisco Certified Expert (ccexpert.us)](https://www.ccexpert.us/routing-tcp-ip/calling-the-access-list.html)
* [ingatlancég - Portfolio.hu](https://www.portfolio.hu/cimke/ingatlanc%C3%A9g)
* [oktatas:halozat:cisco:redundans\_kapcsolok [szit]](https://szit.hu/doku.php?id=oktatas%3Ahalozat%3Acisco%3Aredundans_kapcsolok&fbclid=IwAR2lc-iTfFbANQgSBZbfe5okX-UA6PI3D8XTAgOaHsPn_T7WEXCAg6UkGqA)
* [Mi az a VPN és hogyan működik? Útmutató kezdőknek (2022) (wizcase.com)](https://hu.wizcase.com/blog/teljeskoru-vpn-utmutato-kezdok-szamara/?fbclid=IwAR1IZXNKle_rHJ00HNxQFUVQbWdlYpPLMi8UdpWxryX8JsrO2PVrpcd4ukY)
* [Etherchannel | Informatikai hálózatról magyarul | Fandom](https://net.fandom.com/hu/wiki/Etherchannel?fbclid=IwAR0PZnyhG3NTBXRan6rtcKqNFissT-meNRtZWlENCfaSnSALKGnpkMWmhwQ)
* [HSRP, Hot Standby Routing Protocol (u-szeged.hu)](http://www.inf.u-szeged.hu/projectdirs/bohusoktat/regi/szhaloanyagok/esszek2006/levelezok/HSRP.pdf?fbclid=IwAR11dxdQ8wY83VL3zqmKP5S-91EKsZT16Xi2ohfnVVNmcYoj4Bq8L6NwUmE)
* [A hozzáférési jogosultság ellenőrzése – Wikipédia (wikipedia.org)](https://hu.wikipedia.org/wiki/A_hozz%C3%A1f%C3%A9r%C3%A9si_jogosults%C3%A1g_ellen%C5%91rz%C3%A9se?fbclid=IwAR1jsnICs-OioH5vNjq9fEnoqOjL-3kyHNoKYrXfzuJJLrdgDzansJ6ErYU)
* [Osztályok (google.com)](https://classroom.google.com/u/0/h)
* [Windows Server – Wikipédia (wikipedia.org)](https://hu.wikipedia.org/wiki/Windows_Server)
* [Facebook – Lépj be, vagy regisztrálj!](https://www.facebook.com/?stype=lo&jlou=Afd38XpkaR_DoAB_4FI6JS9qf5Yb3GeMiew2p02J8ea88zl0AG0wexatkBQxXrQQCcAoUH78HVK9v1bY3ksCxOMdHgVL6J9tEF7cQgaGWNcqJQ&smuh=789&lh=Ac_VqzxP1fHJxL8a1Nc)
* [Discord | A beszélgetés és lazítás helye](https://discord.com/)
* [Saját meghajtó – Google Drive](https://drive.google.com/drive/u/0/my-drive)
* [Sign in to GitHub · GitHub](https://github.com/login?client_id=78a2ba87f071c28e65bb&return_to=%2Flogin%2Foauth%2Fauthorize%3Fclient_id%3D78a2ba87f071c28e65bb%26redirect_uri%3Dhttps%253A%252F%252Fcircleci.com%252Fauth%252Fgithub%253Freturn-to%253D%25252F%26scope%3Drepo%252Cuser%253Aemail%26state%3D5z2apw8fIO9HeeDwPzG-9hEfIbYa1DbldfoWr9R2XZZBYcmF8xg3iRoksu8qZNYKpxHfVwm96tEoRwbO)
* [Mi az IIS / Windows Web Server? Hogyan kell használni, Legjobb eszközök és források (heritage-offshore.com)](https://heritage-offshore.com/net-admin/mi-az-iis-windows-web-server-hogyan-kell-hasznalni/?fbclid=IwAR0OsBFM4_EpZlegmA6Pf5r793ztjdWiJ4F-XJ_ef-dGmOY_SZ-S3A3wSKM)
* [Active Directory – Wikipédia (wikipedia.org)](https://hu.wikipedia.org/wiki/Active_Directory?fbclid=IwAR2eeKnKDRN5_WMY9F9elbPgFMuNPO7skVzsECL59P1ik4Eb89gQI-z7R1g)
* [A Távoli asztal használata (microsoft.com)](https://support.microsoft.com/hu-hu/windows/a-t%C3%A1voli-asztal-haszn%C3%A1lata-5fe128d5-8fb1-7a23-3b8a-41e636865e8c?fbclid=IwAR2v6dtNb2Zqe_iga1y68TLdBsri0KM0NBRPPcCFTsPy1L1M27WzZGbilOY)
* [LDAP-ról pár szóban (elte.hu)](http://padre.web.elte.hu/ldap.html?fbclid=IwAR3nrqMr1X38T1ZNHARgqMFgGR-zCdeF3o-wmZywE-Hu1ILAkNKtlwjXOyQ)
* [HSRP, Hot Standby Routing Protocol (u-szeged.hu)](http://www.inf.u-szeged.hu/projectdirs/bohusoktat/regi/szhaloanyagok/esszek2006/levelezok/HSRP.pdf?fbclid=IwAR11dxdQ8wY83VL3zqmKP5S-91EKsZT16Xi2ohfnVVNmcYoj4Bq8L6NwUmE)
* [Cisco Packet Tracer - YouTube](https://www.youtube.com/watch?v=i9quK-Mcikk)
* [HSRP, Hot Standby Routing Protocol (u-szeged.hu)](http://www.inf.u-szeged.hu/projectdirs/bohusoktat/regi/szhaloanyagok/esszek2006/levelezok/HSRP.pdf?fbclid=IwAR1S97UuxPMW79-wQ034dPKARVgKlevGMBkCbjbMR2-GaaPyXsUjyIt6ag8)
* [Etherchannel | Informatikai hálózatról magyarul | Fandom](https://net.fandom.com/hu/wiki/Etherchannel?fbclid=IwAR3xx_wpPPFeElmrbfbsoJOPexEYoDTU3wtiJJCAO7QcsFv2O0ht_5u4FBw)
* [Install OpenLDAP Server on Debian 11 / Debian 10 | ComputingForGeeks](https://computingforgeeks.com/how-to-install-and-configure-openldap-server-on-debian/?fbclid=IwAR3vNZQtU5O4BoX8Fcoow_0H1jtFyX8fsPnGR42GpuY8i-PM1qoQ9oS8570)
* [A NAT és a PAT közötti különbség (gadget-info.com)](https://hu.gadget-info.com/difference-between-nat)
* [Mi az OSPF? | Hogyan működik? | Az OSPF végrehajtása és alkalmazása (education-wiki.com)](https://hu.education-wiki.com/3990219-what-is-ospf)
* [Mi a DHCP? | Hogyan működik | Megértés és előnyei (education-wiki.com)](https://hu.education-wiki.com/7863438-what-is-dhcp)
* [Port forwarding - Wikipedia](https://en.wikipedia.org/wiki/Port_forwarding)
* [Díjmentes tervezés - Westquality](http://www.westquality.hu/szolgaltatasok/szolgaltatasok/dijmentes-3ds-latvanytervezes)
* [Központban az ingatlan. (alacsonyjutalek.hu)](https://alacsonyjutalek.hu/)
* [[PDF] Cyber Security Zone Modeling in Practice | Semantic Scholar](https://www.semanticscholar.org/paper/Cyber-Security-Zone-Modeling-in-Practice-Gontarczyk-Mcmillan/87c06b0af4ecb9af3864b0d2a37a7818e83c3df2)
* [Mi a rendszernapló (syslog)? - meghatározás a techopedia alapján - A hírekben - 2022 (theastrologypage.com)](https://hu.theastrologypage.com/system-log)
* [Mi az a DNS rendszer? Mi a DNS jelentése? (domdom.hu)](https://www.domdom.hu/domain-regisztracio/mi-az-a-dns-rendszer?fbclid=IwAR3YM605kYJS_pORziLixQ4Wv8N2b--sQI-QW4T6sFDO_w55HRFDUUHvwEQ)
* [Mi a TFTP? (Trivial File Transfer Protocol) (eyewated.com)](https://hu.eyewated.com/trivialis-fajlatviteli-protokoll/)

**Nyilatkozat**

Alulírott Juhos Benjámin, Laboda Dániel, Hernádi Emma Julianna a Pécsi Szakképzési Centrum Simonyi Károly Szakgimnáziuma és Szakközépiskolájának tanulói kijelentjük, hogy a büntetőjogi felelősségünk tudatában nyilatkozunk és aláírásunkkal igazoljuk, hogy a benyújtott záródolgozatunk saját munkánk.

Az abban hivatkozott nyomtatott és elektronikus szakirodalom felhasználása a szerzői jogok szabályinak megfelelően készült.

Tudomásul vesszük, hogy a záródolgozat esetén plágiumnak számít:

- szószerinti vagy attól kismértékben eltérő idézet közlése idézőjel és hivatkozás megjelölése nélkül,

- tartalmi idézet hivatkozás megjelölés nélkül,

- más publikált gondolatainak (cikk, dolgozat) sajátunkként való feltüntetése.

Alulírott kijelentjük, hogy a plágium fogalmát megismertük és tudomásul vettük, hogy plágium esetén a záródolgozatunk visszautasításra kerül.

Pécs, 2022. április 19

Aláírás: Juhos Benjámin

Aláírás: Laboda Dániel

Aláírás: Hernádi Emma Julianna

**KÖSZÖNJÜK A FIGYELMET!**