Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

***Szakképesítés neve:*** Informatikai rendszer- és alkalmazás-üzemeltető technikus

***Szakképesítés száma:*** 5-0612-12-02

IRAÜ Vizsgaremek

Meló-Diák

Informatikai hálózati infrastruktúra kiépítése és konfigurálása

Szervergépek telepítése, konfigurálása, üzemeltetése

Nagy Attila, Szarvas Márton, Kovács Dávid Balázs

2/14A || 2023-2024. tanév

Budapest

Tartalomjegyzék

[Történet 3](#_Toc165841917)

[A hálózat megtervezése 4](#_Toc165841918)

[Az iroda megtervezése 3D-ben 4](#_Toc165841919)

[Topológia 4](#_Toc165841920)

[IP címzés 4](#_Toc165841921)

[Megvalósítás 4](#_Toc165841922)

[ProxMox virtuális környezet 4](#_Toc165841923)

[Meló-Diák iroda 5](#_Toc165841924)

[Kábelmodem 5](#_Toc165841925)

[Forgalomirányítás (EIGRP) 6](#_Toc165841926)

[HSRP 6](#_Toc165841927)

[Dinamikus forgalomirányítás 6](#_Toc165841928)

[Spanning Tree 7](#_Toc165841929)

[TFTP 7](#_Toc165841930)

[DNS 8](#_Toc165841931)

[Szerverpark 8](#_Toc165841932)

[Home Office 8](#_Toc165841933)

[VPN 9](#_Toc165841934)

[Szerverek 10](#_Toc165841935)

[Windows szerver 10](#_Toc165841936)

[Active Directory 10](#_Toc165841937)

[Tartománynévszerver 10](#_Toc165841938)

[Dinamikus forgalomirányítás 11](#_Toc165841939)

[Felhasználók 13](#_Toc165841940)

[Csoportházirendek 14](#_Toc165841941)

[Fájlmegosztás 15](#_Toc165841942)

[Nyomtató-megosztás 17](#_Toc165841943)

[Backup 19](#_Toc165841944)

[RAID tárolás (Windows) 20](#_Toc165841945)

[Linux szerver 21](#_Toc165841946)

[Operációs rendszer 21](#_Toc165841947)

[Web szolgáltatás 22](#_Toc165841948)

[Levelező szolgáltatás 22](#_Toc165841949)

[Tanúsítványok 23](#_Toc165841950)

[VPN 25](#_Toc165841951)

[IOT: 26](#_Toc165841952)

[Ábrajegyzék 27](#_Toc165841953)

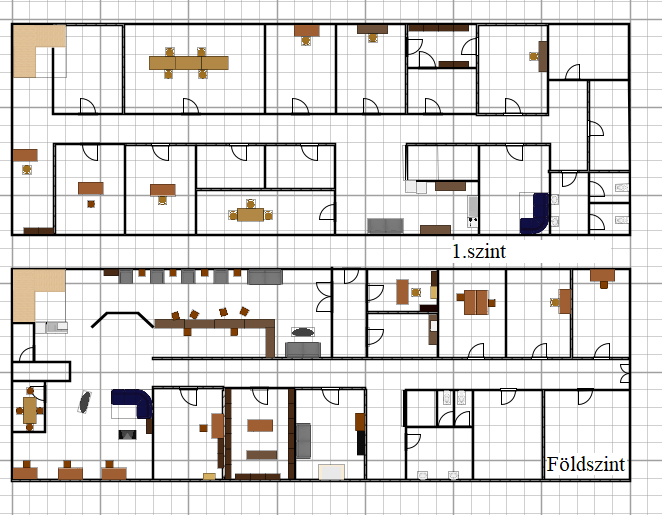
# Történet

A Meló-Diák Magyarország iskolaszövetkezet szeretné fejleszteni informatikai infrastruktúráját, hogy egyszerűbbé és gyorsabbá lehessen tenni a diákmunkára jelentkezők regisztrációját, ugyanakkor a dolgozóknak ne jelentsen több nehézségeket. A szövetkezet vezetősége felkeresett minket, egy informatikai rendszer fejlesztésének céljából, melyben ötlettervét megmutatva munkához is kezdtünk. Felmértük az irodájuk jelenlegi kialakítását, majd hozzákezdtünk a tervezéshez.

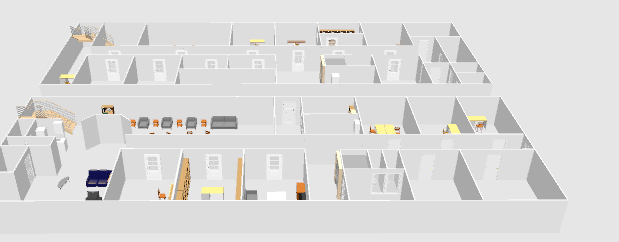
# A hálózat megtervezése

## Az iroda megtervezése 3D-ben

Hogy jobban meg tudjuk tervezni a hálózatot, például hova helyezzük el bizonyos eszközöket, feltérképeztük az irodát egy 3D-s program segítségével, illetve készítettünk egy alaprajzot is, hogy jobban átlássuk az irodát.



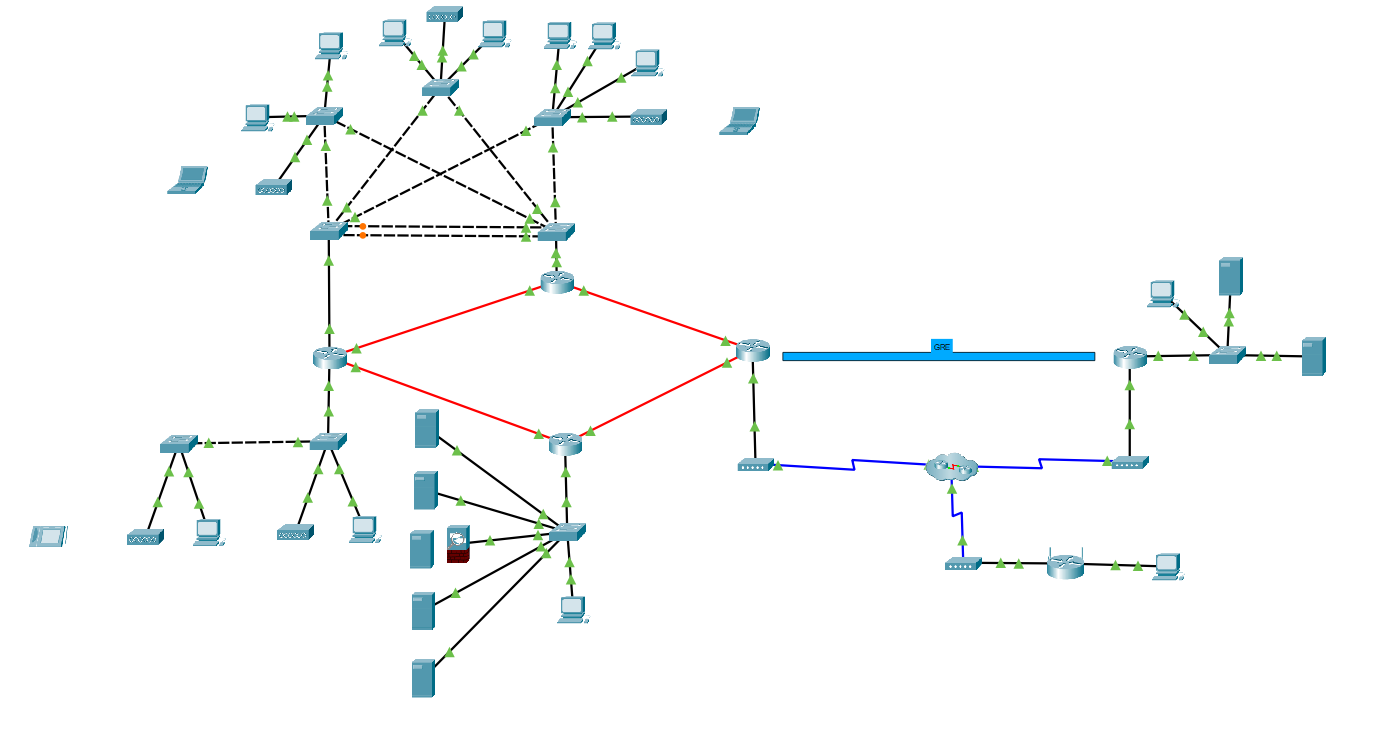
1. ábra Az iroda földszinti és 1. emeleti alaprajza



2. ábra Az iroda 3D-s feltérképezése

## Topológia

Miután a 3D feltérképezés megtörtént, nekiláttunk a tervezésnek. Ebben a Packet Tracer szimulátorban létrehozott topológiában szerepel mind a Meló-Diák irodája, a szerverpark, ami különböző szolgáltatásokat nyújt, egy home office szimulációja, és az internetszolgáltató.



3. ábra A Meló-Diák teljes hálózatának topológiája, beleértve a szerverparkot, Home Office-t és az Internetszolgáltatót

## 

## IP címzés

A topológia felépítését követően, nekifogtunk a kiosztható IPv4-es és IPv6-os címek felosztásának és kiszámolásának. Elkészítettük az iroda VLAN táblázatát és IP cím kiosztását.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Name | Vlan id | Melyik szint? | Network | Default router | DHCP | DHCP server | DNS server |
| OFFICE | 10 | Emelet | 192.168.10.0/25 | 192.168.10.1 | 10-60 | 192.168.10.254 | 192.168.10.254 |
| RECEPTION | 20 | Emelet | 192.168.20.0/26 | 192.168.20.1 | 10-60 | 192.168.10.254 | 192.168.10.254 |
| RECEPTION | 20 | Földszint | 192.168.20.64/26 | 192.168.20.65 | 70-120 | 192.168.10.254 | 192.168.10.254 |
| WIFI | 60 | Emelet | 192.168.60.0/24 | 192.168.60.1 | 100-200 | 192.168.10.254 | 192.168.10.254 |
| GUEST\_WIFI | 64 | Földszint | 192.168.64.0/24 | 192.168.64.1 | 100-200 | 192.168.10.254 | 192.168.10.254 |
| MANAGEMENT | 99 | Emelet | 192.168.99.0/26 | 192.168.99.1 |  |  |  |
| MANAGEMENT | 99 | Földszint | 192.168.99.64/26 | 192.168.99.65 |  |  |  |

# 

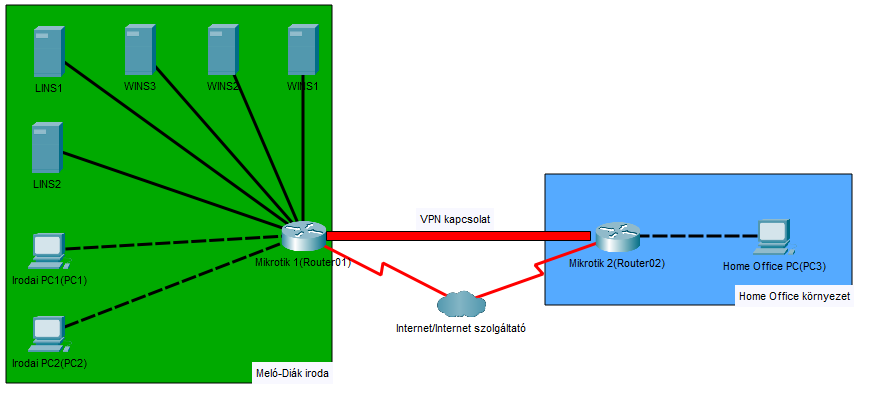
# Megvalósítás

ProxMox virtuális környezet

Mi azonban nem csak egy szimulátort, hanem egy ProxMox nevű virtuális környezet segítségével konfiguráltuk és üzemeljük azon részeit a szimulációban lévő hálózatnak, amiket mi építettünk hozzá, ezekhez az eszközök tartoznak például:

* Forgalomirányítók
* Szervergépek
* Személyi számítógépek

Létrehoztuk a ProxMox virtuális környezetben egy működő és aktívan kommunikáló hálózatot a következőképpen:



4. ábra A ProxMox virtuális hálózata képileg bemutatva

A képen látható a ProxMox-on szimulált és konfigurált eszközök összessége, a jobb átláthatóság érdekében Packet Tracer-ben vizuálisan szimulálva. Az első forgalomirányító, **’Router01’**, egy Mikrotik operációs rendszerű router, ami **összeköti a Meló-Diák irodai eszközeit az Internet többi részével, biztosítva a kommunikációt**. Van egy külső és belső címe. A külső felel az Internettel való kommunikációért. A belső pedig az irodai kapcsolatokhoz szükséges.

A másik, szintén Mikrotik alapú forgalomirányító, **’Router02’**, a **Home Office oldali gépet köti össze az internettel, és irodával egy VPN kapcsolat segítségével**, amit az irodában található szerverek egyike **’LINS1’** szolgáltat, ugyanez a szerver generálja a kulcsokat, amivel be lehet lépni távolról a belső irodai hálózatba. Szintén van egy külső és belső címe. ’LINS1’ felel még a **WEB** szolgáltatásért, ami a cég weboldalát mutatja az internet felé a **VPN** mellett.

**’LINS2’** a **MAIL**, azaz a levelező szolgáltatást, és adatait tárolja. A WEB és a MAIL szolgáltatásoknak készítettünk tanúsítványokat ’LINS1’ által. ’WINS1’-en találhatóak a **DNS**, **DHCP** és **ADDS** szolgáltatások. Ezek felelnek az **irodai gépek címosztásáért, felhasználók jogosultságainak és egyéb adatainak kezeléséért**, illetve a DNS felelős azért, hogy a Linux szervereken tárolt weboldal és levelező oldal **ne IP-címmel, hanem értelmes címnevekkel** legyen elérhető. **’WINS2’** hasonlóan ’WINS1’-hez tartalmazza ugyanazokat a szolgáltatásokat, illetve ’WINS2’ tárolja a biztonsági mentéseit ’WINS1’-nek. Abban az esetben, ha az első szerver nem működik, meghibásodik, a szerverek **szinkronizálva lettek**, így ’WINS2’ azonnal ’WINS1’ helyébe tud lépni, **megszüntetve ezzel a rendszer elérhetőségi állapotának kiesését.**

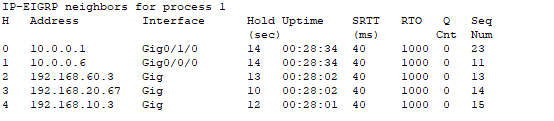
**’WINS3’** tartalmazza az előző két szerver adatait, szolgáltatásait, illetve biztonsági mentéseiket is tárolja. Ez a szerver felel még ezen biztonsági mentések és egyéb adatok feldarabolásáért **RAID** technológia segítségével. A szerver foglalkozik még a nyomtató- és fájlmegosztáson az irodai hálózaton belül, illetve, ha valaki VPN-t használva lépne be, az is hozzáférhet a benti fájlokhoz, tölthet fel és le is onnan.

Meló-Diák iroda:

Kábelmodem:

A hálózatokhoz kábelmodemen keresztül érkezik az internet a szolgáltatótól mind a szerverparkhoz, Irodához és a Home Office-hoz. A kábelmodem egy olyan modem, amely a kábeltelevíziós hálózaton képes kommunikálni. A kábelmodemeket elsősorban széles sávú internetkapcsolat megvalósítására használják.

Forgalomirányítás (EIGRP):

A forgalomirányítást EIGRP protokollal oldottuk meg, ami egy távolság alapú dinamikus útválasztó protokoll. Az előnyei közé tartozik a magas elérhetőség és a nagy szintű automatizálás, ezzel könnyítve a rendszerüzemeltető dolgát.

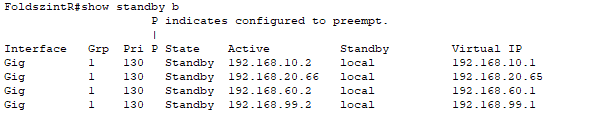
5. ábra Az emeleti forgalomirányító összesítője, milyen címtartományokat ismer az ’1’-es folyamatazonosító alatt

HSRP:

A HSRP több célt is szolgálhat. Az egyik megvalósítása lehet Failover konfiguráció, vagy használhatjuk akár load balancingra is. A jelen esetben mind2 jelen van, ugyanis a HSRP segítségével beállítottjuk, hogy bizonyos VLAN-okat adott router kezelje elsőként. Ezáltal normál üzemben elszeparálva az emeletek forgalmát egymástól.

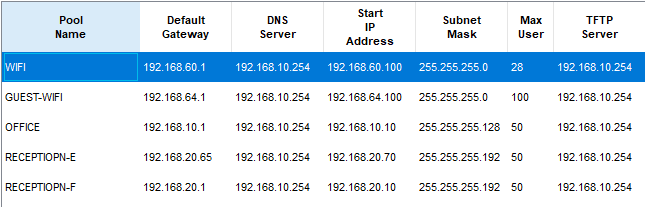


6. ábra HSRP protokoll területe az irodai hálózatban



7. ábra HSRP protokoll információi

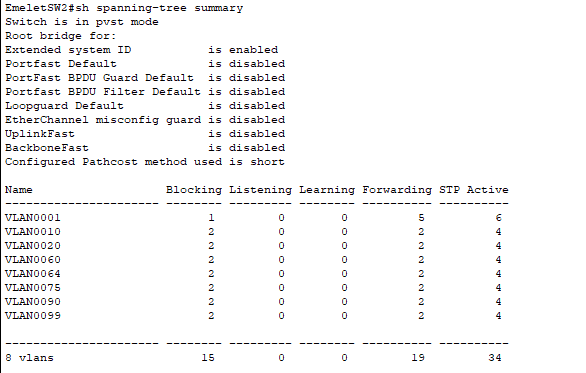
Dinamikus forgalomirányítás:

Ez a protokoll azt oldja meg, hogy a hálózatra csatlakozó hálózati végpontok (például számítógépek) automatikusan megkapják a hálózat használatához szükséges beállításokat. A DHCP szerver-kliens alapú protokoll, nagy vonalakban a kliensek által küldött DHCP-kérésekből, és a szerver által adott DHCP-válaszokból áll. Ebben az esetben a beállított dolgok a IP-cím tartomány ahonnét osztja a címeket a szerver, az alhálózati maszk, kezdeti IP-cím, a maximum kiosztható IP-címek az adott hálózatban, a DNS és TFTP szerverek IP-címei. 

8. ábra A dinamikus címosztó szerver (DHCP) létrehozott ’pool’-jai

Spanning Tree:

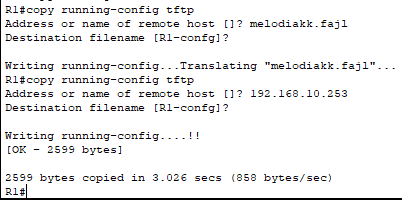
A feszítőfa a második réteg redundanciáját segíti elő mivel a körbe kötött kapcsolók nem alkothatnak hurkot. A hálózatban PVST-t használunk.



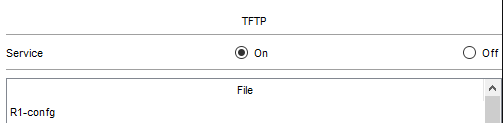
9. ábra Spanning-tree információi

TFTP:

A Trivial File Transfer Protocol (TFTP) egy egyszerű, kis méretű fájlok gyors átvitelére szolgáló protokoll, amely gyakran használatos a hálózati eszközök közötti firmware vagy konfigurációs fájlok frissítéséhez és másolásához. A TFTP egyszerűsége miatt nem tartalmaz beépített hitelesítési mechanizmusokat vagy biztonsági funkciókat, így gyakran csak a hálózatokon belül, megbízható környezetben használják. Azonban gyors és hatékony megoldást kínál a kis méretű fájlok gyors átvitelére a hálózati eszközök között.



10. ábra Az R1-es forgalomirányító futási konfigurációja éppen rá lett mentve a TFTP szerverre



11. ábra A forgalomirányító futási konfigurációja a TFTP szerver ablakában

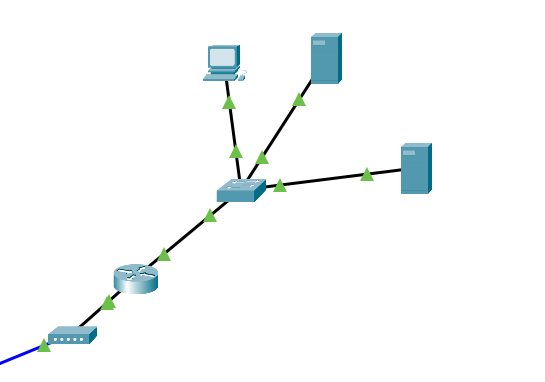
DNS:

A cég a belső hálózatról és az internetszolgáltatótól is kap DNS szolgáltatást. A DNS lehetővé teszi internetes erőforrások csoportjaihoz nevek hozzárendelését olyan módon, hogy az ne függjön az erőforrások fizikai helyétől. A DNS-t lentebb fejtjük ki.

Szerverpark:

A cég nem csak a belső hálózatában lévő szerverektől kap szolgáltatást. Kapcsolatban állnak egy szerverparkkal is, ami web és e-mail szerverszolgáltatásokkal látja el az irodát.

A szimulált parkon belül található a webszerver, a mailszerver és az adminisztrátor számítógépe. A web és e-mail szolgáltatásokat lentebb ismertetjük.



12. ábra A szerverpark topológiája

Home Office:

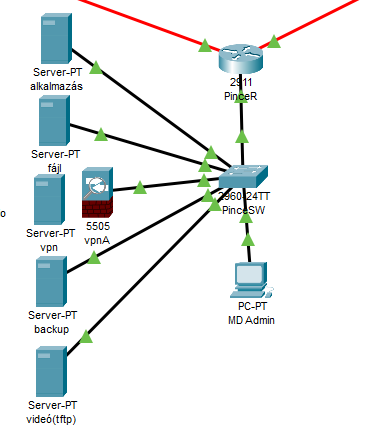
Az iroda méretei miatt nem tud minden dolgozó bent lenni egyszerre, ezért megoldásként otthonról dolgoznak többen is. Sajnos azonban megbízható kapcsolat nem volt semmilyen módon megoldva, és ez olyan belső információk biztonságát veszélyeztetheti, amiket nem szeretne a cég, hogy illetéktelenek útközben elkaphassanak. Tudva erről a lehetséges veszélyről, azt is megkérték tőlünk, hogy vezessünk be egy biztonságosabb és bizalmasabb megoldást.



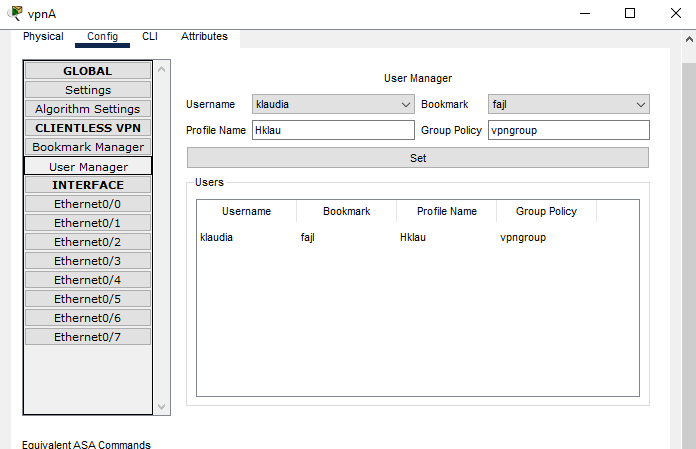
13. ábra A Home Office topológiája

VPN:

A virtuális magán hálózatot (VPN) láttuk a legjobb megoldásnak. Ez a szolgáltatás egy biztonságos utat biztosít két pont között, ebben az esetben egy otthoni számítógép és az irodai hálózat között. Ehhez a megoldáshoz az egyik meglévő Linux szerverüket bővítettük, amire semmi fontosabb feladat nem volt kiosztva. A kódokat és hitelesítési kulcsokat a kapcsolat létrehozáshoz a Linux szerver OpenVPN szolgáltatása fogja generálni.



14. ábra A pincében lévő szerverszobában található a VPN szerver



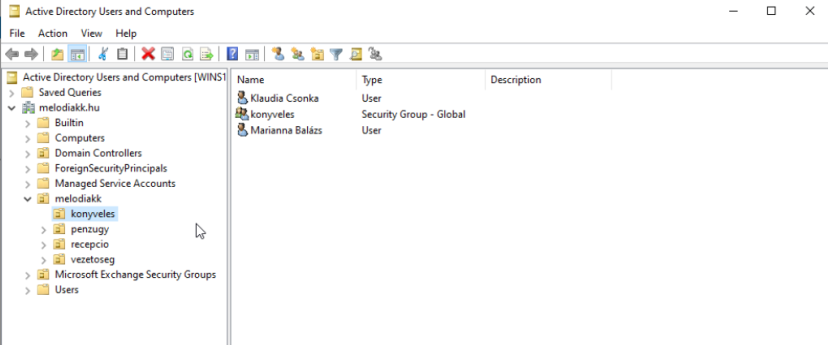
15. ábra A Felhasználó menedzser interfésze

# Szerverek

Windows szerver:

Active Directory:

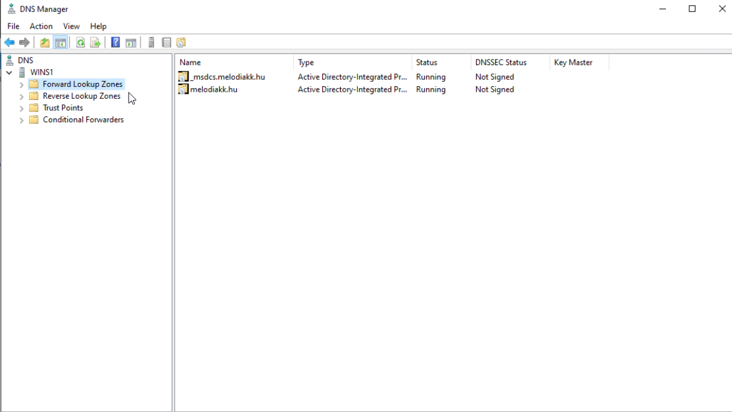
Az Active Directory címtár az adatbázisból és az azt futtató Active Directory szolgáltatásból áll. Fő célja a Windowst futtató számítógépek részére autentikációs és autorizációs szolgáltatások nyújtása, lehetővé téve a hálózat minden publikált erőforrásának (fájlok, megosztások, perifériák, kapcsolatok, adatbázisok, felhasználók, csoportok stb.) központosított adminisztrálását – vagy éppen a rendszergazdai jogosultságok delegálásával a decentralizált felügyeletét.



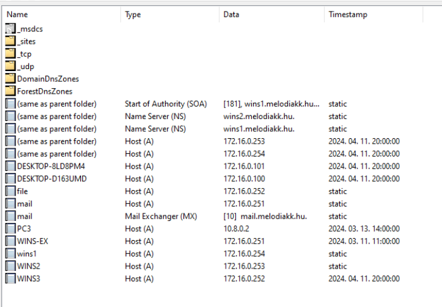
16. ábra Az ADDS ablaka a Windows szerveren

Tartománynévszerver:

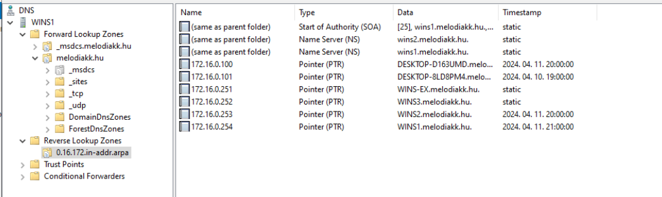
A Tartománynév rendszer (DNS) egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára. A részt vevő entitások számára kiosztott tartománynevekhez (doménekhez) különböző információkat társít. Legfontosabb funkciójaként az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető numerikus azonosítókká „fordítja le”, „oldja fel”, melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton. Erre azért van szükség, hogy az átlagember egyszerűbben megjegyezzen egy címet, és nem egy hosszú számot.



17. ábra A DNS menedzser ablaka

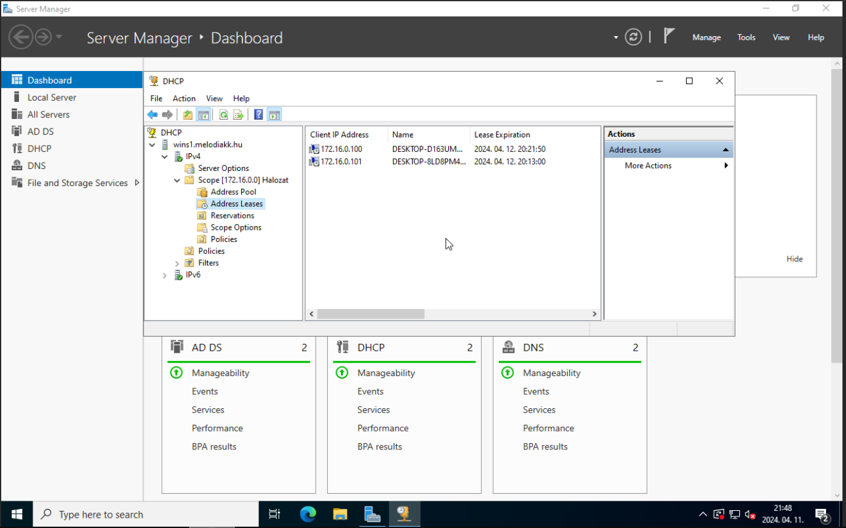


18. ábra A névkiosztások a DNS által

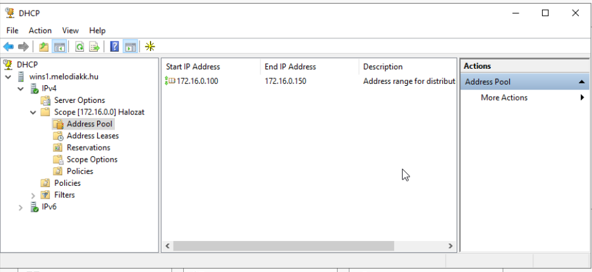


19. ábra Reverse Lookup Zone

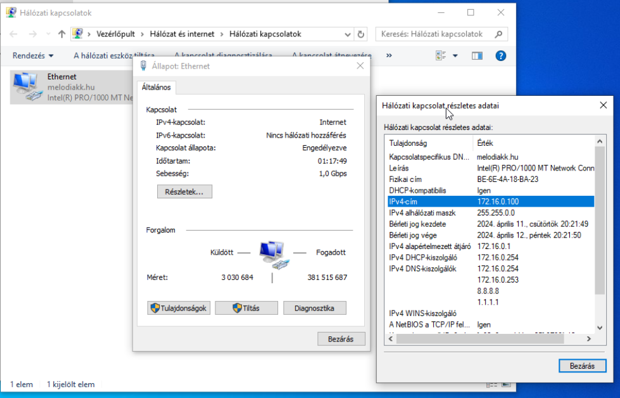
Dinamikus forgalomirányítás:

A feljebb kifejtett dinamikus forgalomirányítást egy Windows szerverkörnyezetben alkalmaztuk, mivel egy könnyen konfigurálható és megérthető protokoll.

20. ábra Kép a kliensgépekről, amik csatlakoznak a szerverhez és címük kiosztva

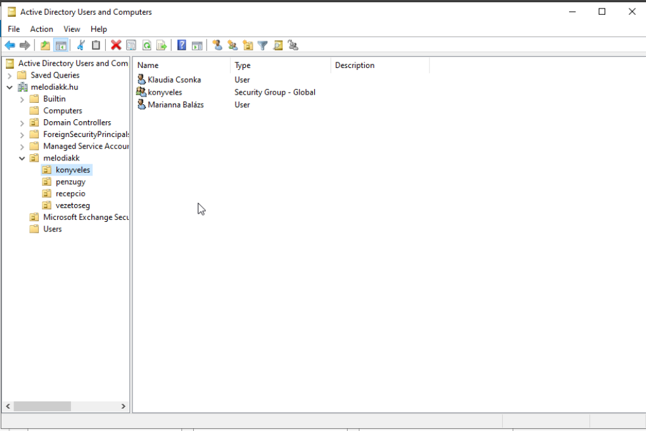


21. ábra A kiosztott címtartomány a szerver által

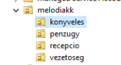


22. ábra Az egyik irodai dolgozó gépe, mint kliensgép és annak IP-cím információi, látszódik hogy megkapta a DHCP által osztott címet

Felhasználók:  
Természetesen el kell különíteni az irodai dolgozók számítógépeit, hogy ne legyen kavarodás. Ez azzal jár, hogy felhasználókat hozunk létre a szerveren, és mindegyik dolgozónak a beosztásának megfelelően csoportosítjuk őket a Csoportházirendek segítségével.



23. ábra A felhasználók létrehozásának felülete az ADDS-ben



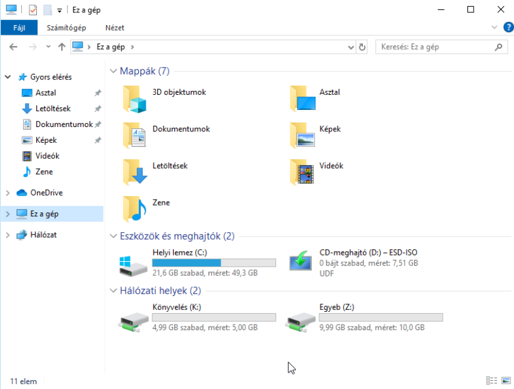
24. ábra A létrehozott csoportok, osztályok



25. ábra Elkészített felhasználók és biztonsági csoport a ’konyveles’ fülből



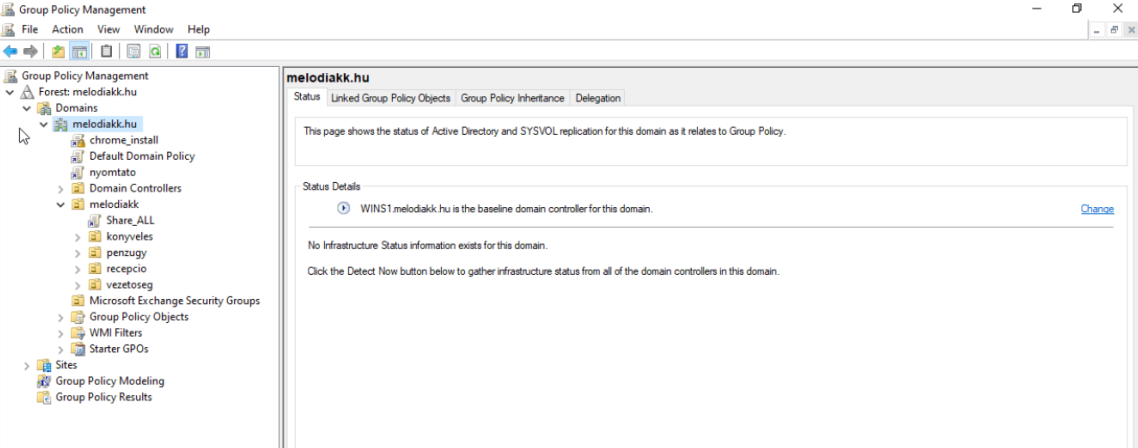
26. ábra Az egyik felhasználó éppen belép a számítógépébe



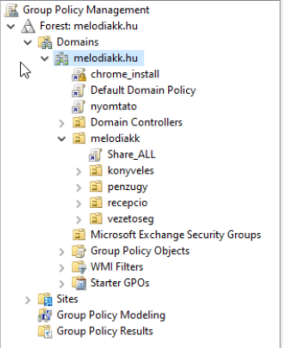
27. ábra Minden felhasználónak van saját és megosztott hálózati tárolóhelye

Csoportházirendek:

Hogy könnyebben meglehessen állapítani, hogy a feljebb létrehozott felhasználók melyik osztályba, beosztásba tartozik, a vezetőség megkért minket, hogy hozzunk létre egy rendszert, amivel ezt meg lehet valósítani. Tehát csoportházirendeket alakítottunk ki. Ezek segítségével nehezebbé tesszük az illetéktelen belépéseket és a keveredéseket az iroda belső hálózatán. A csoportházirendek a Microsoft operációs rendszereinek egy funkciója, amivel megoldható a felhasználók, a számítógépek és a felhasználói munkakörnyezetek viselkedésének és jogosultságainak szabályozása. A csoportházirend Active Directory környezetben lehetővé teszi az operációs rendszerek, alkalmazások és a felhasználók beállításainak központosított konfigurálását és menedzsmentjét. Leegyszerűsítve, a csoportházirenddel többek közt megszabható, hogy a felhasználó mit tehet és mit nem tehet meg a számítógépen. Bár a csoportházirendek alkalmazása nagyvállalati környezetben a legelterjedtebb, találkozhatunk vele iskolákban, kis- és középvállalkozásokban is. A csoportházirendeket gyakran arra használják, hogy potenciális biztonsági réseket zárjanak be vele, pl. tiltják a hozzáférést a Windows feladatkezelőjéhez, korlátozzák bizonyos mappákhoz a hozzáférést, tiltják a futtatható fájlok letöltését és így tovább.



28. ábra A csoportházirendek konfiguráló ablaka



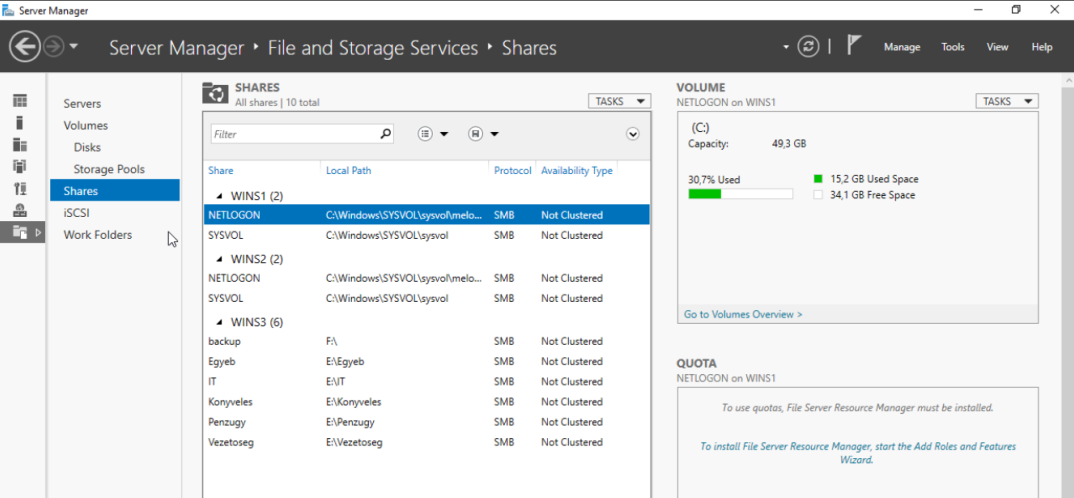
29. ábra

A csoportházirendek meglévő beállításai, ezekhez tartoznak például:

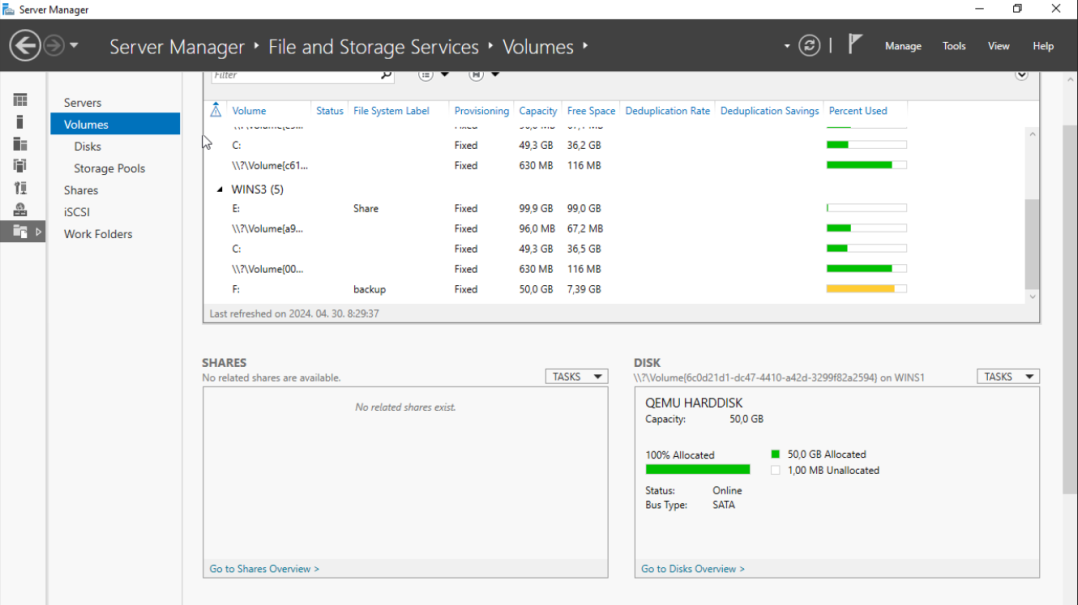
* Felhasználók elkülönítése beosztások alapján (pl.: könyvelők, vezetőség, recepció stb.)
* Nyomtatóhoz való hozzáférés
* E-mail szerver felhasználóinak konfigurálása

Fájlmegosztás:

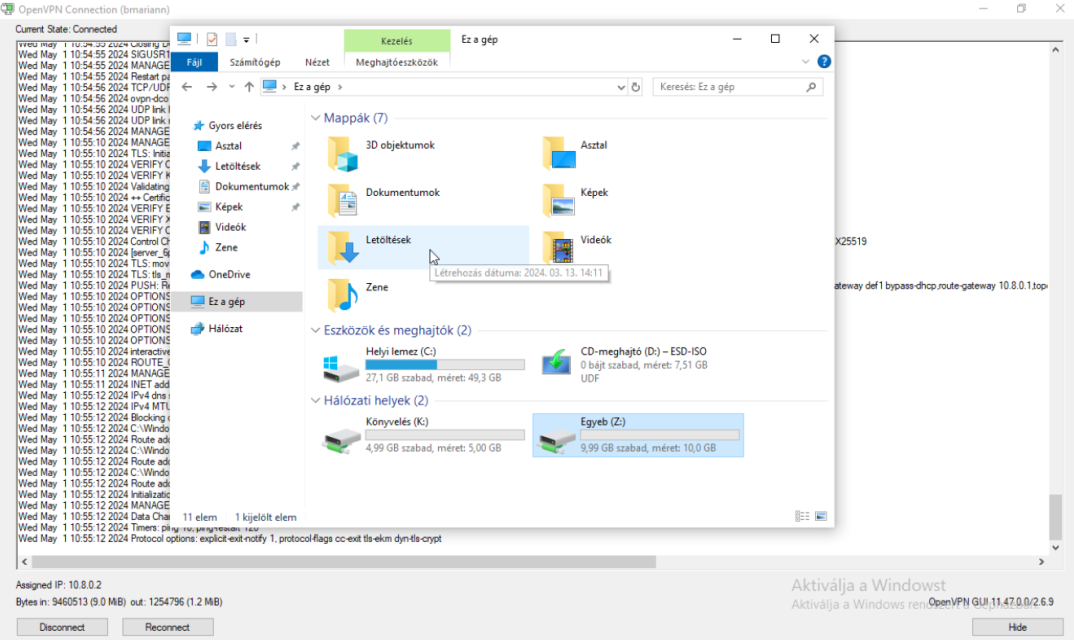
Mivel a dolgozók nem csak az irodában dolgoznak, illetve, hogy egyszerűbbé tegyük a fájlok láthatóságát és mozgatását a dolgozók között, a Windows szerverek segítségével fájlmegosztást hoztunk létre. A fájlmegosztás a digitális fájlok egyik felhasználóról vagy eszközről a másikra történő továbbításának vagy terjesztésének folyamatát jelenti. A fájlok típusai közé tartozhatnak dokumentumok, képek, videók, hangfájlok és egyéb fájlok. A fájlmegosztás célja, hogy lehetővé tegye az együttműködést, az információcserét és a fájlok egyszerű elérését különböző eszközök, helyszínek és személyek között. A fájlmegosztás számos előnyt kínál, amelyek forradalmasították az információk tárolásának és elérésének módját. Elősegíti az együttműködést, mivel lehetővé teszi, hogy több felhasználó is megtekinthesse és dolgozhasson ugyanazon a fájlon, javítva ezzel a termelékenységet és a hatékonyságot.



30. ábra A Fájlmegosztás ablaka, láthatók azok a meghajtók, amiket megoszt a szerver, és magában tárolja el



31. ábra Itt látható még több meghajtó, azoknak elfoglalt tárhelyei, illetve a szerverek biztonsági mentései



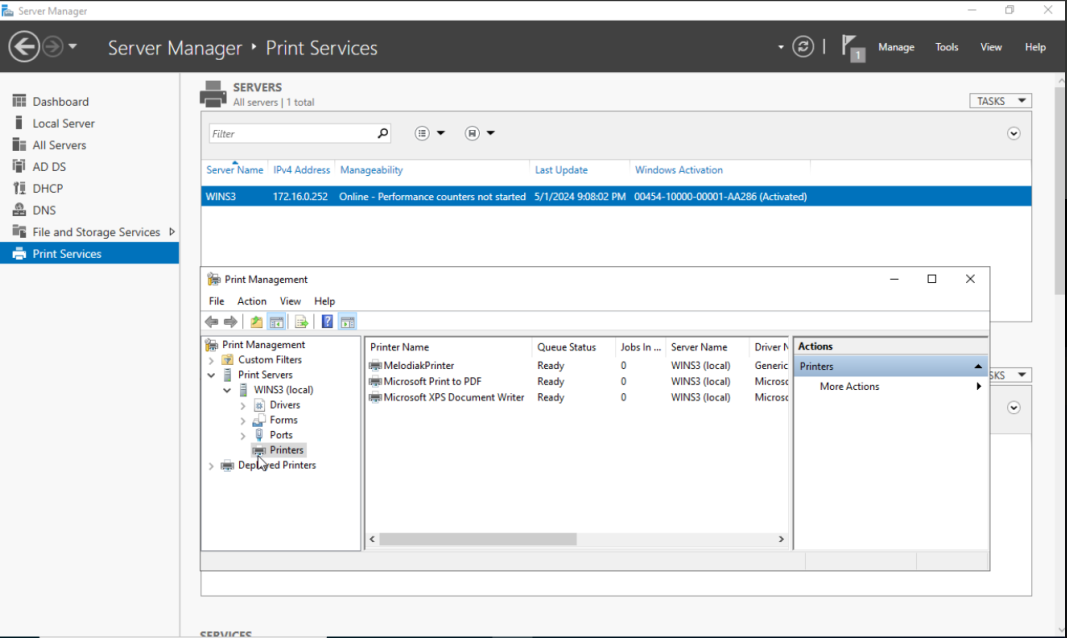
32. ábra A lentebb elmagyarázott VPN szerver segítségével távoli eléréssel, az irodai környezeten kívülről is lehet fájlokat fel- és letölteni

Nyomtató-megosztás:

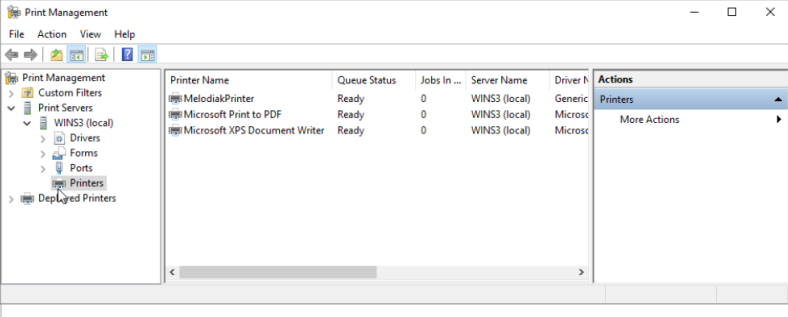
A vezetőség tájékoztatott minket arról, hogy sok papír alapú anyagot nyomtatnak, és egy megoldást kértek arra, hogyan lehetne vezeték nélkül sok ember számára elérhetővé tenni a nyomtatók használatát. Ezért a Windows szerverünkre konfiguráltunk nyomtatómegosztást. A nyomtatómegosztás a hálózati nyomtatókhoz való hozzáférést teszi lehetővé több felhasználó számára ugyanabban a hálózati környezetben. A folyamat az alábbi lépéseket tartalmazza:

1. Nyomtató megosztása: Először is, a nyomtatót meg kell osztani a hálózaton. Ehhez a nyomtatót közvetlenül egy számítógéphez kell csatlakoztatni, amelyen a megosztást aktiválják. A megosztási beállítások általában a számítógép nyomtatókezelési beállításaiban találhatók.
2. Hálózati hozzáférés engedélyezése: A nyomtatót meg kell osztani a hálózati felhasználók számára. Ez lehetővé teszi más számítógépek számára, hogy hozzáférjenek és használják a nyomtatót a hálózaton keresztül.
3. Nyomtató telepítése a hálózati gépekre: A többi számítógépen telepíteni kell a megosztott nyomtatót. Ez általában a nyomtató telepítését jelenti a számítógép nyomtatókezelési beállításaiban, ahol a felhasználók kiválaszthatják a hálózati nyomtatót.
4. Nyomtatás: Amikor egy felhasználó nyomtatni szeretne, az adott számítógépen kiválasztja a megosztott nyomtatót a nyomtatók listájából. A nyomtatási parancsot elküldik a nyomtatóra, amely aztán kinyomtatja a dokumentumot.

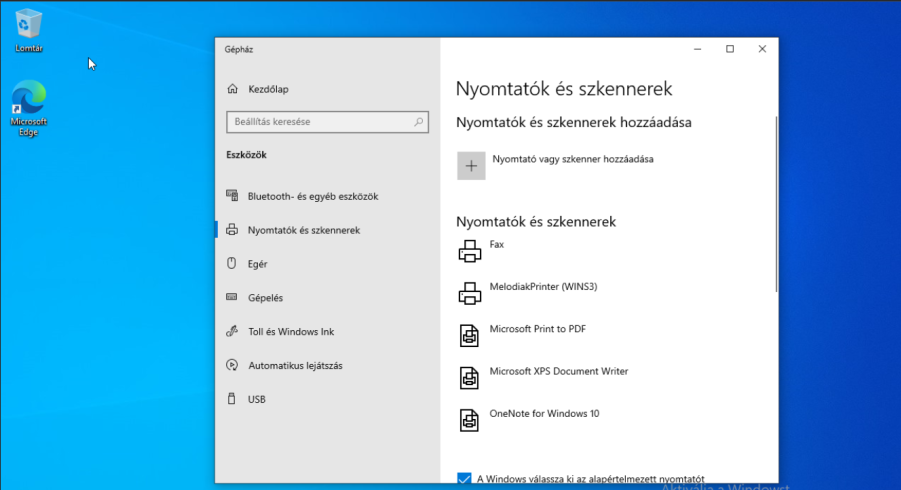
Ezáltal a nyomtatómegosztás lehetővé teszi a hálózati felhasználók számára, hogy közösen használják ugyanazt a nyomtatót a hálózaton keresztül, ami hatékonyabb és költséghatékonyabb megoldást jelenthet a nyomtatási igények kezelésére.



33. ábra A nyomtatószolgáltatás ablaka



34. ábra A szerver által megosztott nyomtatók adatai



35. ábra Kép arról, hogy az irodai gépek látják a nyomtatókat

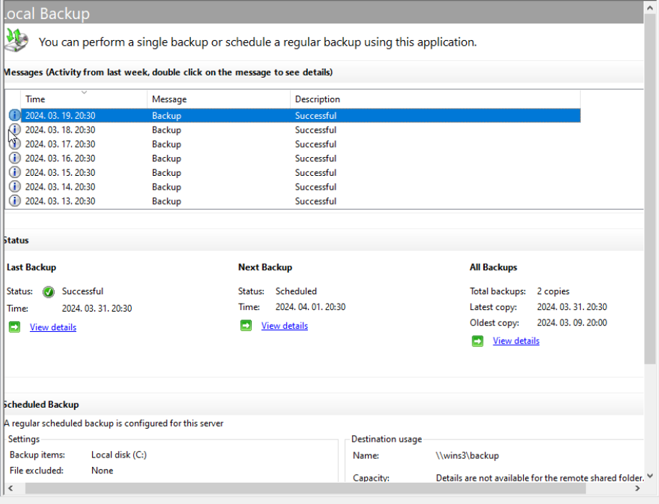
Backup:

Hogy megerősítsük a biztonságát ezeknek a Windows szervereknek, az egyik szervert biztonsági mentések tárolására konfiguráltunk be. Ez azért is jó, hogy ha valamilyen probléma miatt az egyik szerver meghibásodik, vagy bármi komplikáció lépne fel, akkor vissza lehetne állítani erről a szerverről az esetlegesen meghibásodott adatokat, konfigurációkat. Megadott időközönként egy biztonsági mentést készít egy szerver, és továbbítja a kijelölt backup szervernek. Az adatmentés a számítógépen tárolt információkról történő biztonsági másolat készítése, arra az esetre, mikor az eredeti forrás adatokat tartalmazó tároló megsérül. Szoftveres és hardveres megoldások kombinációjaként megy végbe a folyamat. Az adatmentő szoftverek közül a legjobb megoldás a hardverfüggetlen mentőszoftver. Ez azért fontos, mert, ha működésképtelenné válik egy hardver és nem tudunk ugyanolyat vagy hasonlót beszerezni, más hardveren is vissza tudjuk állítani az adatainkat.

A mentés többféle módszer szerint történhet:

* Teljes mentés
* Növekményes mentés
* Differenciális mentés

Mi teljes mentést választottunk a Linux és Windows szervereinken.



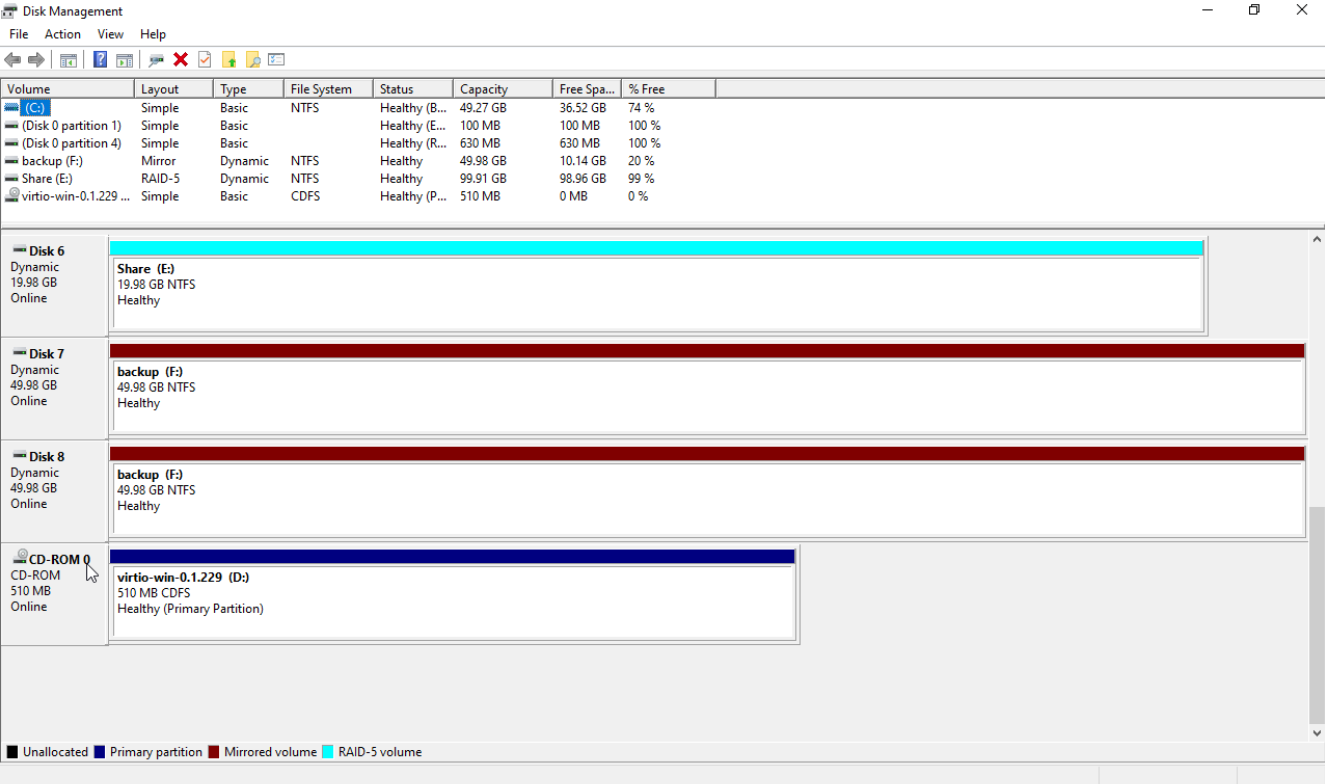
36. ábra A Windows szerver Backup ablaka, látható mikor készült az utolsó mentés, és mikor lesz a következő

RAID tárolás (Windows):

Abban az esetben, hogy ha a backup-ok is meghibásodnak, vagy a fájlok állapot ’korruptálódik’, komoly adatvesztéshez vezethet. A cég vezetősége egy ilyen esetleges probléma ellen megoldást kértek tőlünk ezen a területen is. Mi a RAID tárolási technológiát találtuk a megfelelőnek. A RAID tárolási technológia, mely segítségével az adatok elosztása vagy replikálása több fizikailag független merevlemezen, egy logikai lemez létrehozásával lehetséges. Minden RAID szint alapjában véve vagy az adatbiztonság növelését, vagy az adatátviteli sebesség növelését szolgálja. A RAID-ben eredetileg 5 szintet definiáltak (RAID 1-től RAID 5-ig). Az egyes szintek nem a fejlődési, illetve minőségi sorrendet tükrözik, hanem egyszerűen a különböző megoldásokat. A kezdeti 5 szinthez később hozzávették a RAID 6-ot. RAID 0 jelöli azt a változatot, ahol a lemezeket összefűzzük, azaz redundancia nélkül kapcsoljuk össze.



37. ábra RAID 5 használata a Backup szolgáltatás mellett



38. ábra A Windows szerverek backup-ja tükrözve RAID technológia segítségével, növelve így is az adatok biztonságát

Linux szerver:

Operációs rendszer:

Egy Debian 12.2-es operációs rendszerű szerver gépet alkalmaztunk erre a feladatra, mivel számunkra a környezet ismerős, egyszerű konfigurálni és átlátható. A Debian elnevezés egy gyűjtőfogalom. A többség azonban a népszerű Linux-disztribúciót érti rajta, aminek a helyes megnevezése Debian GNU/Linux, ezzel is jelezve, hogy az adott rendszer a Linux kernelt és nyílt forráskódú, szabad felhasználású (GNU licenc alatt publikált) szoftverek együttesét használja.

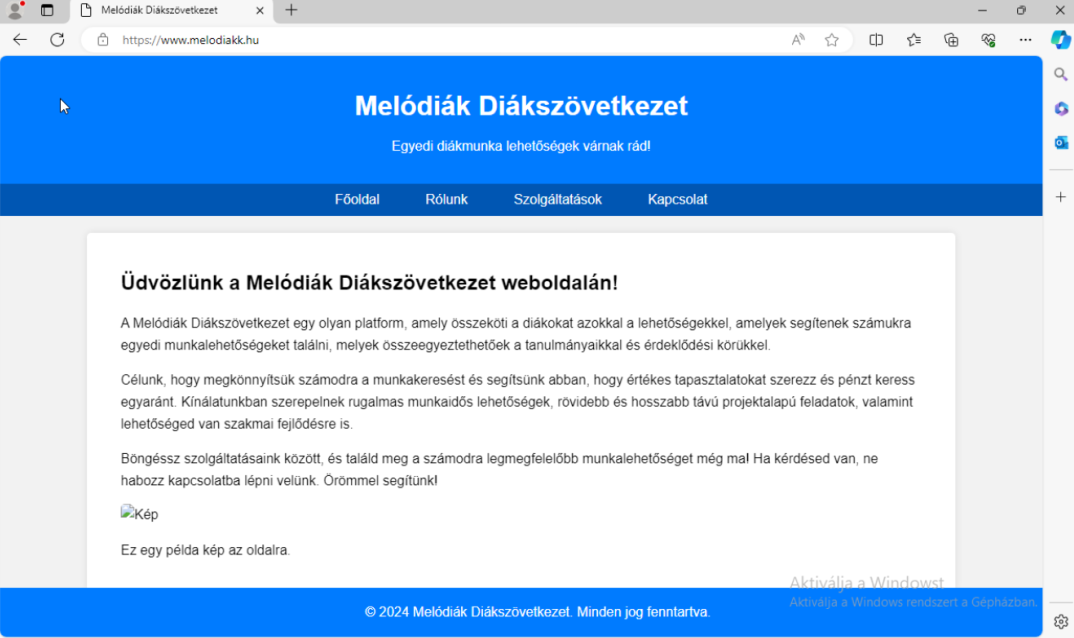
Legfőbb jellemzői:

* teljesen ingyenes és megfelel a Debian szabad szoftver irányelveknek, tehát szabad szoftver
* fejlett csomagkezelő rendszerrel rendelkezik, ami könnyűvé teszi a programok frissítését, telepítését és eltávolítását.

Web szolgáltatás:

A vezetőség tájékoztatott minket arról, hogy szeretnének egy weboldalt, amivel egyszerűbbé lehetne tenni a jelentkezést a bizonyos munkákra, illetve információt és egyéb szolgáltatásokat nyújtson. A weboldalt elkészítették, de megkértek arra, hogy tároljuk el valahol, és tegyük elérhetővé az Interneten is. Erre a megoldásra a webszervert alkalmaztuk. A webszerver egy kiszolgáló, mely elérhetővé teszi a helyileg (esetleg más kiszolgálón) tárolt weblapokat a HTTP protokollon keresztül. A HTTP webszerverekhez webböngészőkkel lehet kapcsolódni. Egy webszerver két típusú lehet:

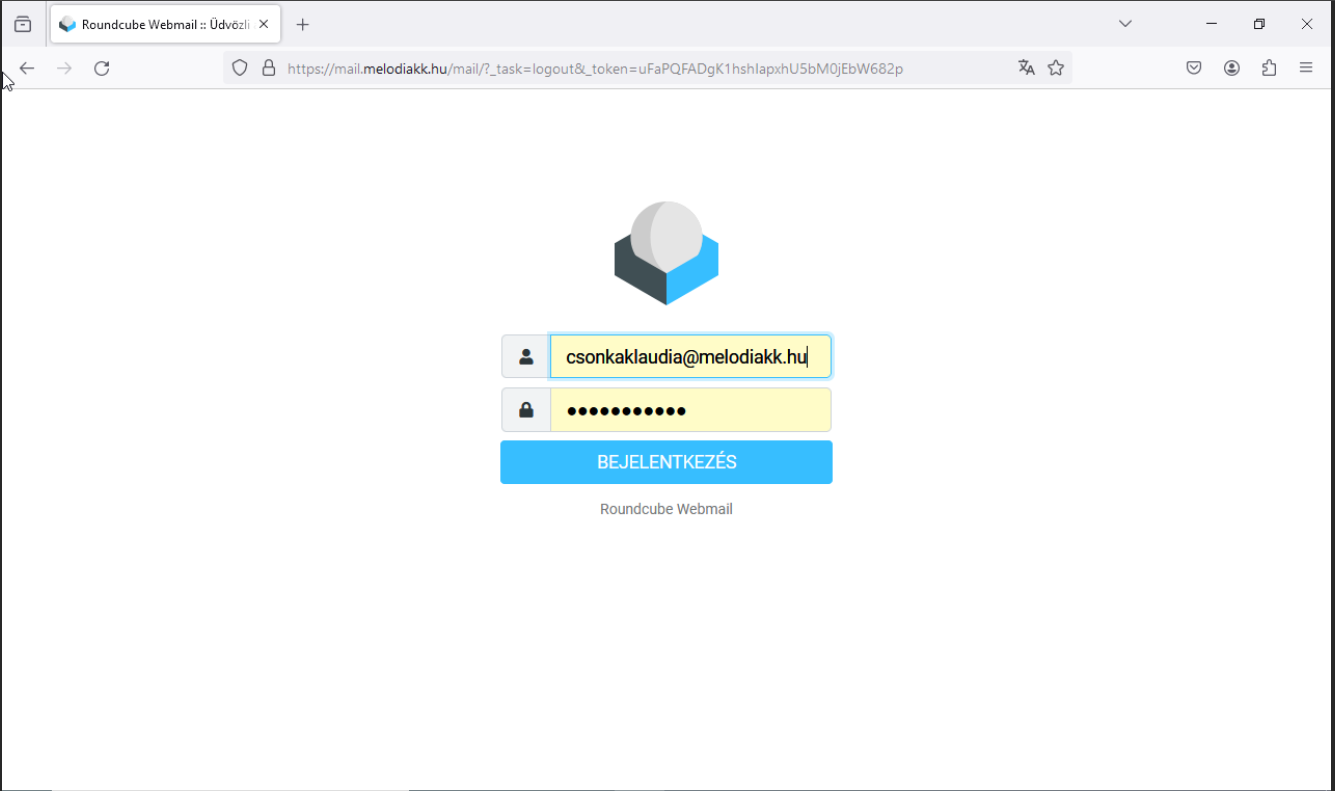
* egy erre a célra kialakított számítógép;
* egy számítógépes program, mely a háttérben futva biztosítja a weblapok elérését.



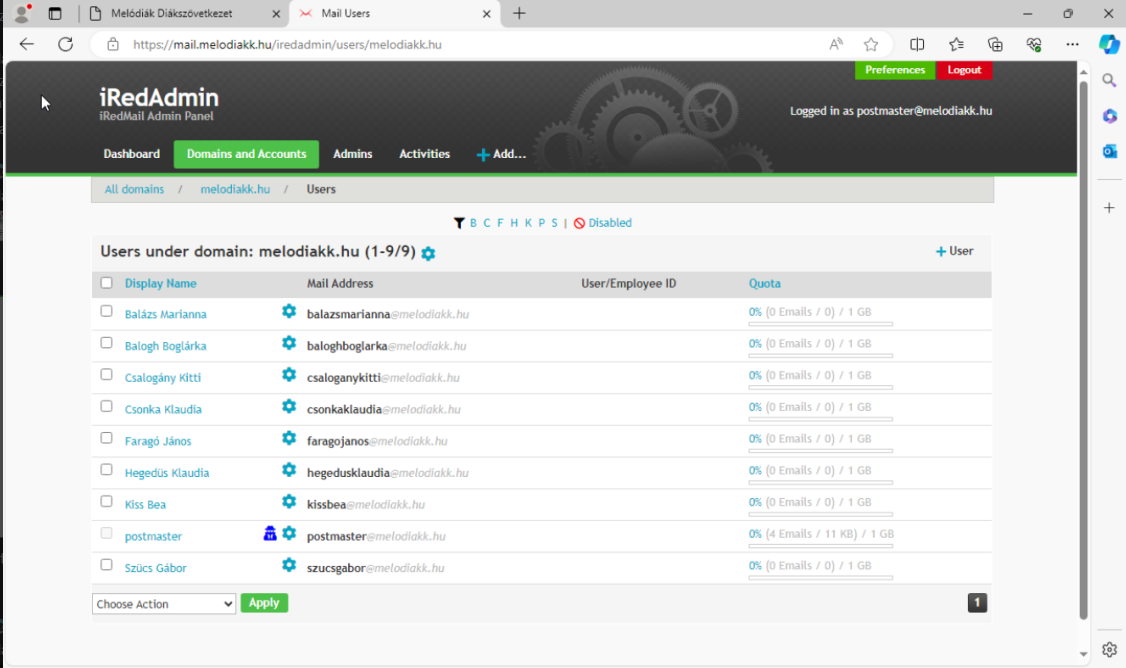
39. ábra A Web szerveren tárolt weboldalunk, elérhető ezen a címen: https://www.melodiakk.hu/

Levelező szolgáltatás:

Hogy a dolgozók egyszerűen és biztonságosabban kommunikálhassanak, egy levelező szolgáltatást is kiépítettünk a Linux szerverünkre. Mi az iRedMail rendszert választottuk. Az iRedMail egy ingyenes, nyílt forráskódú e-mail szerver megoldás, amely teljesen integrált levelezőrendszert biztosít vállalati környezetek számára. A rendszer támogatja az SMTP, IMAP, POP3 protokollokat, valamint tartalmazza a webmail kiszolgálót is. Az iRedMail számos funkciót és biztonsági beállítást kínál, hogy megfeleljen az üzleti igényeknek.



40. ábra A belépési felülete a levelezőszerver oldalára, ezen a címen érhető el: https://mail.melodiakk.hu/mail



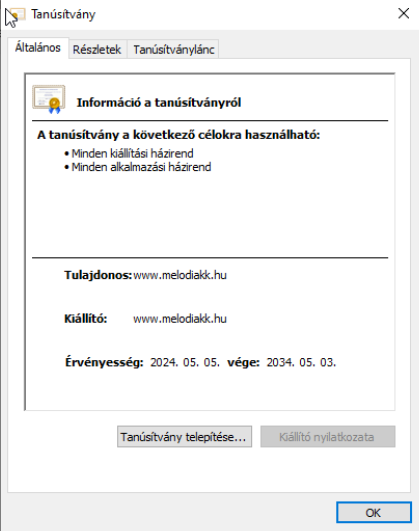
41. ábra A szerver felhasználói és e-mail címük

Tanúsítványok:

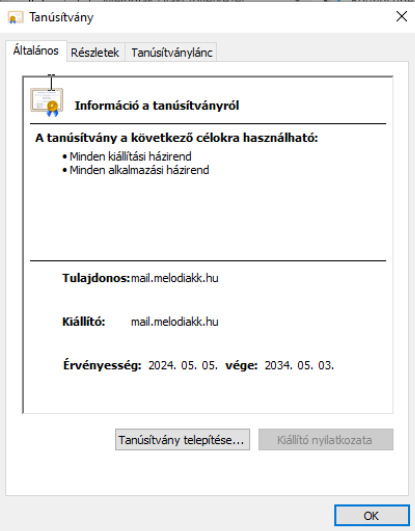
Hogy biztonságossá tegyük létrehozott a weboldalakat, szükségünk lesz tanúsítványokra, amik biztonságos kapcsolatot és megbízhatóságot biztosítanak. Ha egy webszerver nyilvános kulcsát le tudjuk kérdezni, és azzal titkosítunk, akkor az üzenetünket csak a webszerver fogja tudni elolvasni. Az üzenet titkosságával tehát már nincs baj, abban viszont még nem lehetünk biztosak, hogy a titkosított üzenetünk ahhoz jutott, akinek szántuk, hiszen titkosító kulcspárt bárki tud csinálni. Más szóval: a webszerver hitelessége még nincs biztosítva.

A hitelesség biztosításának egyik módja a tanúsítvány. Ez egy igazolás arról, hogy a webszerver nyilvános kulcsa hiteles. Az igazolás kiadója egy tanúsítóhely (*Certificate Authority*), az igazolás hitelességét az ő digitális aláírása biztosítja, valamint az a tény, hogy a tanúsítóhelyet a böngésző írói felvették a böngészőben a hiteles tanúsítóhelyek listájába.

A tanúsítóhelynek tehát hasonló szerepe van a digitális hitelesítésben, mint a közjegyzőnek a papír alapúban. Fontos különbség viszont, hogy a tanúsítóhelyet nem hatóság, hanem a böngésző „nevezi ki”. A tanúsítvány az aláírt tanúsítványkérelem. A kérelem aláírható a szerver (titkos) kulcsával: ez az önmagával aláírt (self-signed) tanúsítvány. Ha ilyen tanúsítványú webszerverre tévedünk, a böngésző figyelmeztet, hogy a tanúsítvány nem megbízható. Csak akkor szabad elfogadni, ha a szerver nyilvános kulcsához megbízható forrásból jutottunk hozzá, nem az internetről. Mi önaláírt tanúsítványokat készítettünk a web és a levelező szolgáltatáshoz egyaránt.



42. ábra A web szolgáltatás önaláírt tanúsítványa, 10 év érvényességet nyújt



43. ábra A levelező szolgáltatás önaláírt tanúsítványa, szintén 10 év érvényességet nyújt

VPN:

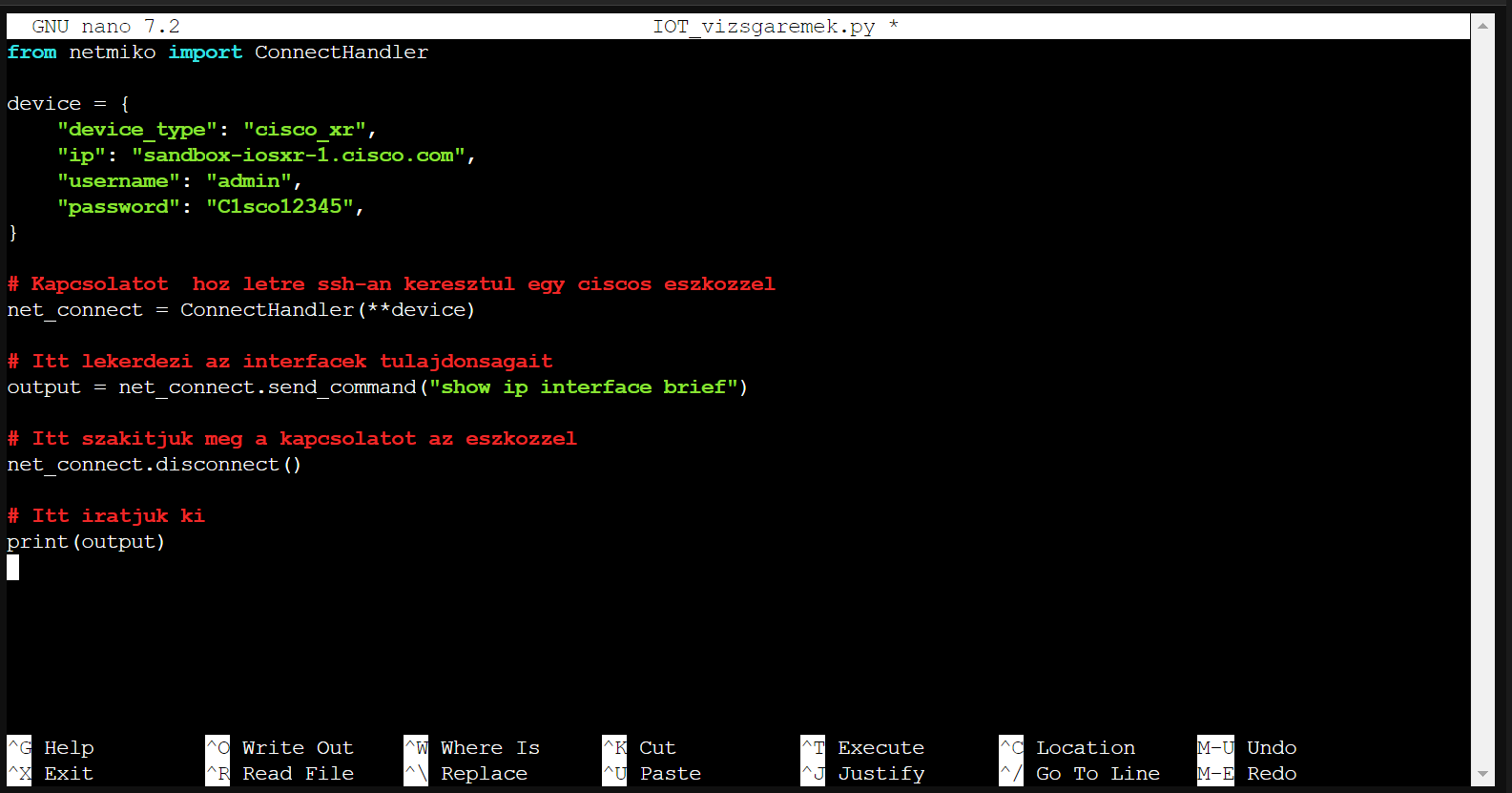
A VPN-t a Linux szerveren oldottuk meg, kulcsot is generáltunk, aminek segítségével be lehet lépni távolról az irodai hálózatba.



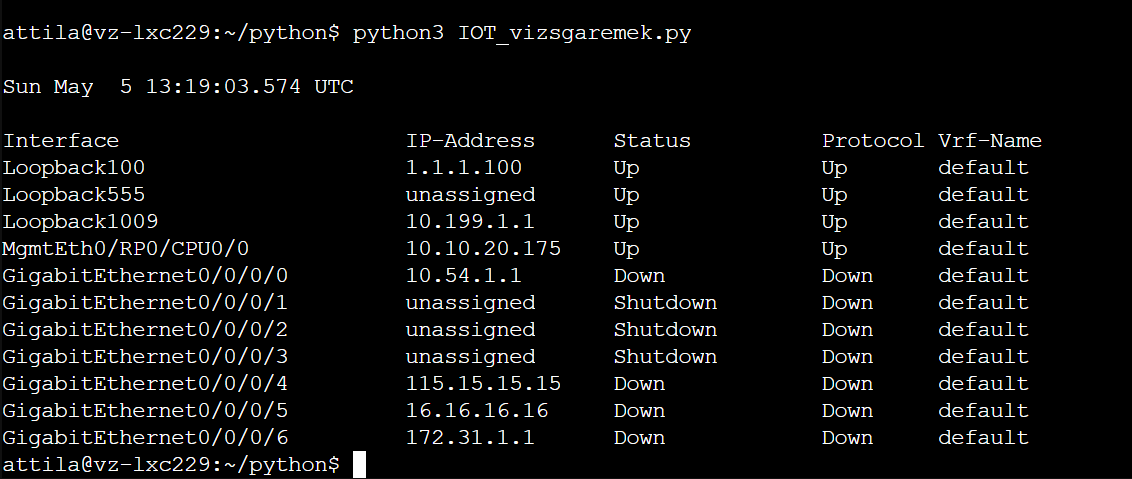
44. ábra A ’bmariann’ felhasználó kapcsolódott home office-ból VPN-en keresztül az irodai hálózatra a szerver által létrehozott kulccsal

# IOT:

Egy harmadik forgalomirányítót ami Cisco operációs rendszerrel konfiguráltunk, még itt tesztelés alatt áll, és a netmiko segítségével egy SSH kapcsolaton keresztül lekérdezhetjük a forgalomirányító összes interfésze, azok állapota és egyéb információk.



45. ábra Ennek a kódnak a segítségével lekérdezzük egy Cisco router interfészének információit, állapotát egy SSH kapcsolaton keresztül



46. ábra

# Ábrajegyzék

[1. ábra 4](#_Toc165844312)

[2. ábra 5](#_Toc165844313)

[3. ábra 5](#_Toc165844314)

[4. ábra 6](#_Toc165844315)

[5. ábra 7](#_Toc165844316)

[6. ábra 8](#_Toc165844317)

[7. ábra 8](#_Toc165844318)

[8. ábra 9](#_Toc165844319)

[9. ábra 9](#_Toc165844320)

[10. ábra 10](#_Toc165844321)

[11. ábra 10](#_Toc165844322)

[12. ábra 11](#_Toc165844323)

[13. ábra 11](#_Toc165844324)

[14. ábra 12](#_Toc165844325)

[15. ábra 12](#_Toc165844326)

[16. ábra 13](#_Toc165844327)

[17. ábra 14](#_Toc165844328)

[18. ábra 14](#_Toc165844329)

[19. ábra 15](#_Toc165844330)

[20. ábra 15](#_Toc165844331)

[21. ábra 16](#_Toc165844332)

[22. ábra 16](#_Toc165844333)

[23. ábra 17](#_Toc165844334)

[24. ábra 17](#_Toc165844335)

[25. ábra 17](#_Toc165844336)

[26. ábra 18](#_Toc165844337)

[27. ábra 18](#_Toc165844338)

[28. ábra 19](#_Toc165844339)

[29. ábra 20](#_Toc165844340)

[30. ábra 21](#_Toc165844341)

[31. ábra 21](#_Toc165844342)

[32. ábra 22](#_Toc165844343)

[33. ábra 23](#_Toc165844344)

[34. ábra 24](#_Toc165844345)

[35. ábra 24](#_Toc165844346)

[36. ábra 25](#_Toc165844347)

[37. ábra 26](#_Toc165844348)

[38. ábra 27](#_Toc165844349)

[39. ábra 28](#_Toc165844350)

[40. ábra 29](#_Toc165844351)

[41. ábra 29](#_Toc165844352)

[42. ábra 31](#_Toc165844353)

[43. ábra 31](#_Toc165844354)

[44. ábra 32](#_Toc165844355)

[45. ábra 33](#_Toc165844356)

[46. ábra 33](#_Toc165844357)