****Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

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

***száma:*** 5-0612-12-02

**Vizsgaremek**

**Metropolitan Transportation Authority**

Bodnár Martin, Huszár Bence, Mokos Márk  
2/14.A

Budapest, 2023.

Tartalom

[Cégleírás 3](#_Toc131413362)

[A cég megbízása 3](#_Toc131413363)

[A hálózat dokumentációja 4](#_Toc131413364)

[Sárga elipszis terület: Wall Street-i metro megálló 6](#_Toc131413365)

[Wall Street eszközök 7](#_Toc131413366)

[Wall Street VLAN-ok 8](#_Toc131413367)

[VLAN 10 – Kék terület (Jegy nyomtató autómaták) 8](#_Toc131413368)

[VLAN 20 – Narancs terület (Beléptető rendszer) 9](#_Toc131413369)

[VLAN 30 – Magenta terület (Privát WIFI) 10](#_Toc131413370)

[VLAN 40 – Sárga terület (Pékség) 11](#_Toc131413371)

[VLAN 50 – Zöld terület (Admin szoba) 11](#_Toc131413372)

[Wall Street Protokollok 12](#_Toc131413373)

[Spanning-tree 13](#_Toc131413374)

[EIGRP 13](#_Toc131413375)

[IPSec VPN 13](#_Toc131413376)

[Link Aggregation 14](#_Toc131413377)

[VLAN Trunking Protocol 14](#_Toc131413378)

[Port Security 15](#_Toc131413379)

[Zöld elipszis terület: MTA Headquarters 16](#_Toc131413380)

[MTA Headquarters eszközök 16](#_Toc131413381)

[MTA Headquarters VLAN-ok 17](#_Toc131413382)

[Földszinten: 17](#_Toc131413383)

[VLAN 230 – Sárga terület (Recepció) 18](#_Toc131413384)

[VLAN 240 – Narancs terület (Kávézó) 18](#_Toc131413385)

[VLAN 250 – Zöld terület (Admin szoba) 19](#_Toc131413386)

[Első emeleten: 20](#_Toc131413387)

[VLAN 210 – Piros terület (Alkalmazottak) 21](#_Toc131413388)

[VLAN 220 – Lila terület (Privát WIFI) 22](#_Toc131413389)

[Második emeleten: 23](#_Toc131413390)

[VLAN 200 – Kék terület (Helyi szerverek) 23](#_Toc131413391)

[VLAN 210 – Piros terület (Alkalmazottak) 24](#_Toc131413392)

[VLAN 220 – Lila Terület (Privát WIFI) 24](#_Toc131413393)

[VLAN 250 – Zöld Terület (Admin szoba) 25](#_Toc131413394)

[MTA Headquarters Protokollok 25](#_Toc131413395)

[GRE Tunnel 26](#_Toc131413396)

[IPv6 over IPv4 GRE Tunnel 26](#_Toc131413397)

[Rózsaszín elipszis terület: MTA Garázs/Szervíz 27](#_Toc131413398)

[MTA Garázs/Szervíz eszközök 28](#_Toc131413399)

[MTA Garázs/Szervíz VLAN-ok 28](#_Toc131413400)

[VLAN 320 – Kék terület (Dolgozók) 29](#_Toc131413401)

[VLAN 310 – Sötét zöld terület (CEO szoba) 29](#_Toc131413402)

[VLAN 340 – Világos zöld terület (Admin szoba) 29](#_Toc131413403)

[MTA Garázs/Szervíz Protokollok 30](#_Toc131413404)

[HSRP 30](#_Toc131413405)

[Barna elipszis terület: Rocky Mountains szerver terem 31](#_Toc131413406)

[Rocky Mountains eszközök 31](#_Toc131413407)

[Rocky Mountains Protokollok 32](#_Toc131413408)

[Rocky Mountains VLAN-ok 32](#_Toc131413409)

[VLAN 400 – Lila terület (Szerverek) 33](#_Toc131413410)

[FTP, Mail 33](#_Toc131413411)

[SYSLOG\_NTP, AAA 36](#_Toc131413412)

[AD, DNS 37](#_Toc131413413)

[DHCP 37](#_Toc131413414)

[VLAN 410 – Zöld terület (Admin szoba) 38](#_Toc131413415)

[Kék elipszis terület: Távoli dolgozó 39](#_Toc131413416)

[Távoli dolgozó Protokollok 40](#_Toc131413417)

[Távoli dolgozó eszközök 40](#_Toc131413418)

# Cégleírás

A Metropolitan Transportation Authority (MTA) cég felelős a tömegközlekedés biztosításáért a New York City metropolitan területén az USA-ban található New York államnak. Az MTA a legnagyobb tömegközlekedést biztosító cég az USA-ban, mintegy napi 11 millió utast szállítanak egy átlagos hétköznap.

Mivel ennyi utas számít a szolgáltatásra nap mint nap a munkába jutáshoz és egyéb utazási célokból ezért elengedhetetlen a cég dolgozói számára, hogy egy biztonságos és folytonos hálózattal tudjanak dolgozni és igénybe venni a szolgáltatásaikat, hogy biztosítani tudják utasaiknak a fennakadás mentes, menetrendben leírt időre pontos tömegközlekedés lehetőségét.

## A cég megbízása

A metro megállóknak a hálózatát megterverzni és konfiguráni. Mivel a megállók nagyon minimálisan térnek el egymástól, ha egyáltalán eltérnek ezért a szimulációs környezetben elég egy ilyen telephely kiépítése, ami kapcsolódik az internet szolgáltatóhoz a többi megálló topológiája maximum a kiadott üzlethelységben tér el.

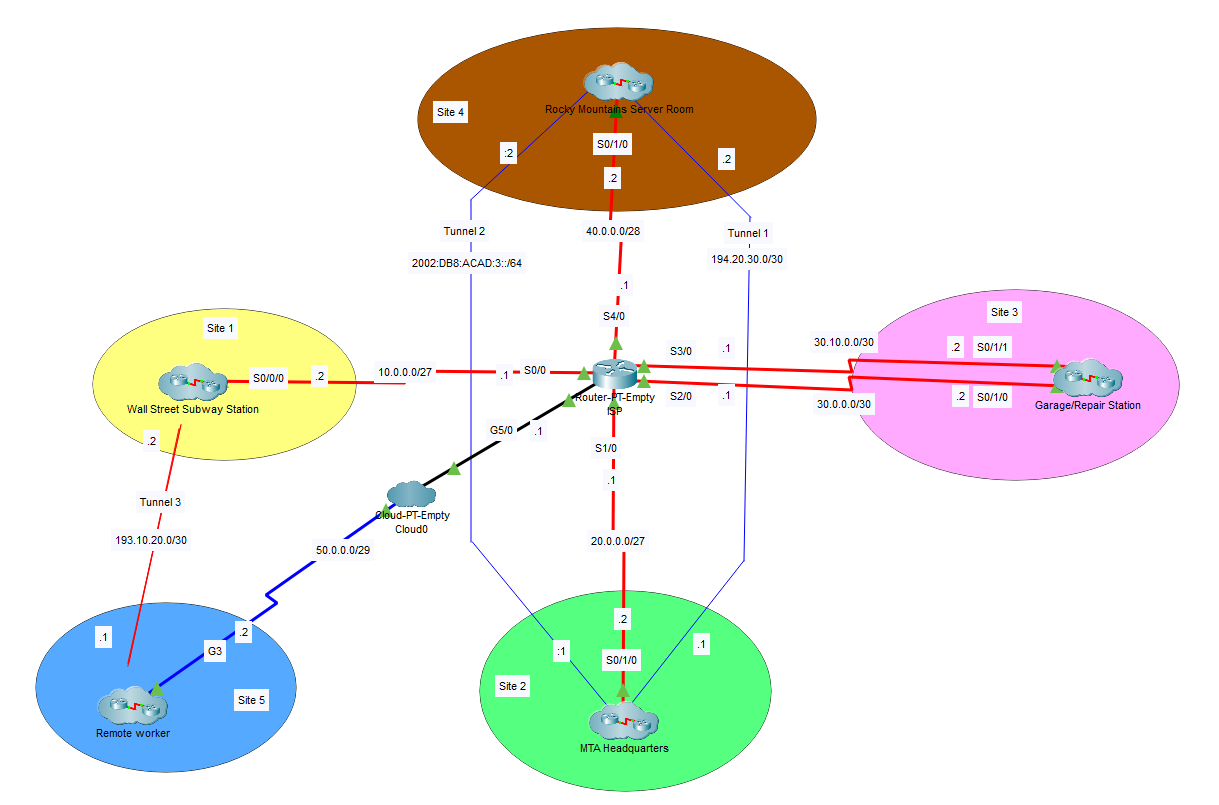
A cég headquarters épületében a hálózat kiépítése az irodák, szerverszoba, admin szoba, kiadott üzlethelység figyelembe vételével. Vezeték nélküli hálózat kiépítése a dolgozók számára. A cég távoli szerverei és a headquarter épülete közötti VPN konfigurálása.

A cég garázsának egyben metro, busz és vonat szerelő állomásnak a hálózatát megtervezni, hogy minden áron elérhető legyen a telephely mert fontos adatokat küldenek az irodában dolgozó munkatársaiknak, ami alapján tudják kalkulálni az esetleges kimaradásokat és minél elöbb tájékoztatni erről az embereket.

A cég távoli szervereinek a telepítése a Sziklás-hegységben és a szolgáltatások biztosítása.

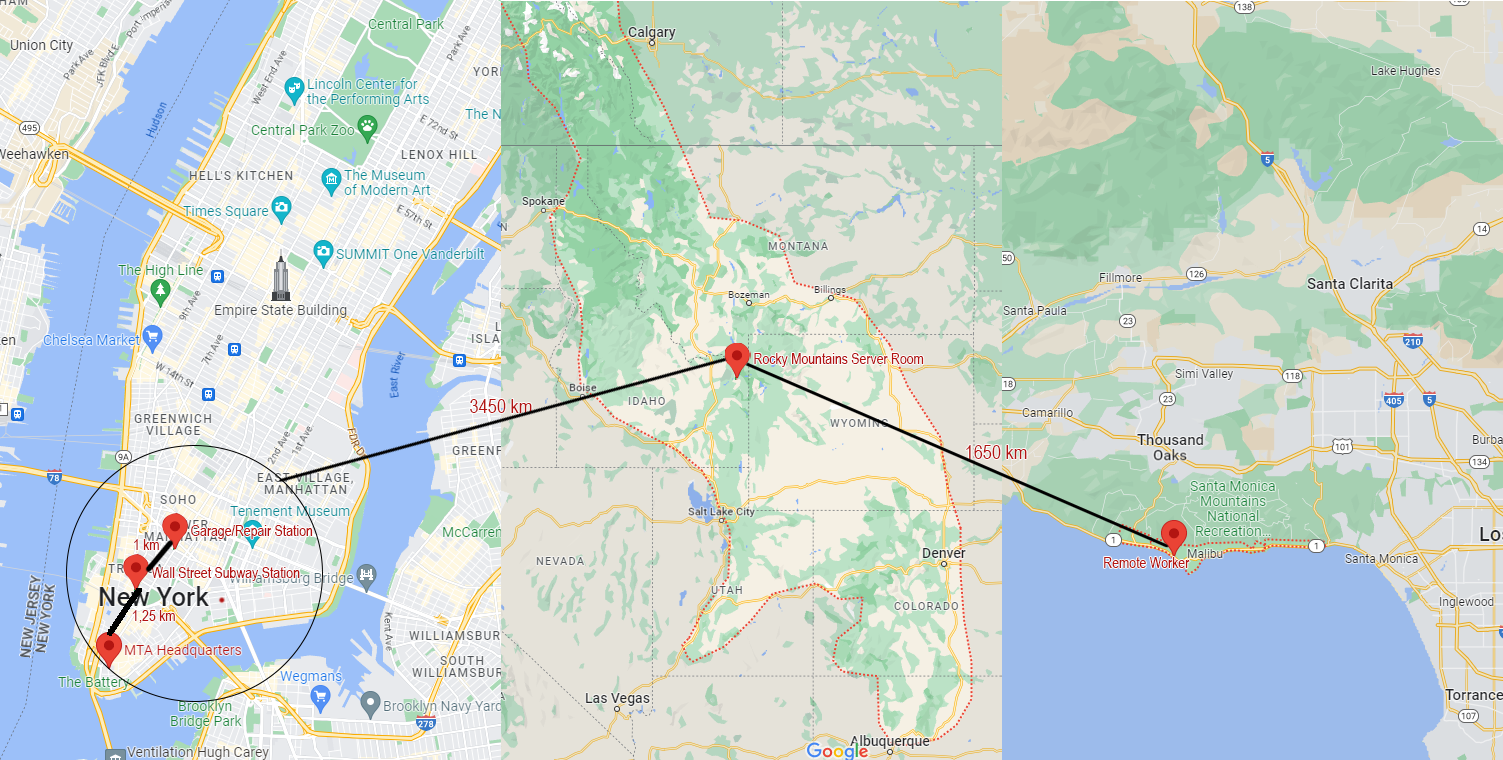
A távoli munkás kapcsolatának biztosítása.

# A hálózat dokumentációja

A prototípus topológiájának felépítéséhez a Cisco Packet Tracer és VirtualBox virtualizációs alkalmazásokat használtuk. A következő képen látható a teljes hálózat topológiája.

1. ábra - A hálózat teljes logikai térképe

A citrom sárga színű terület a Wall Street-i metro megálló, mivel az egyes metro megállók hálózata nagyon hasonló ezért ebből csak 1 telephelyet szimuláltunk le. A zöld színű terület a cég irodaháza. A magenta színű terület egy garázs a metrok számára egyben egy szerviz is. A barna színű terület a cég szerver telepe amely az irodaháztól messze található így védve van a természeti behatásoktól illetve fizikailag se férnek hozzá az esetleges rossz indulatú dolgozók. A kék terület a távmunkás otthoni hálózatát szimulálja. A középen található ISP elnevezésű Router az internetszolgáltatónk, az egyes telephelyek serial kábellel kapcsolódnak az internet felé.



2. ábra – Egyes telephelyek földrajzi elhelyezkedése

# Sárga elipszis terület: Wall Street-i metro megálló

3. ábra – Wall Street-i metro megálló (sárga elipszis terület) logikai térképe

## Wall Street eszközök

A Cisco Packet Tracerben a következő eszközöket használtuk ezen a területen:

* 1 darab Cisco 4331 forgalomirányító
  + - 1 darab HWIC-2T bővítő kártya
* 1 darab Cisco WRT300N vezeték nélküli forgalomirányító
* 3 darab Cisco 2960 kapcsoló
* Nyomtatók
* Számítógépek
* IP telefonok
* 1 darab szerver

4. ábra – Wall Street-i határ forgalomirányító bővítmények

## Wall Street VLAN-ok

A metro megálló hálózatát különböző logikai szegmensekre (VLANokra) osztottuk, így a sárga terület szórási tartományát felosztottuk. Ennek eredménye, hogy a szórásos üzenetek kevesebb sávszélességet foglalnak le mert minden szórásos üzenet csak a saját VLANjába lesz kiküldve.

### VLAN 10 – Kék terület (Jegy nyomtató autómaták)

5. ábra – VLAN 10 – Jegy nyomtató autómaták

A szimulációban 1 ilyen autómatát jelenítettünk meg az átláthatóság kedvéért, valós esetben ebből több van a megállóba.

A Cisco Packet Tracerben ezeket az autómatákat egy számítógéppel és egy nyomtatóval szimuláltuk. A számítógépen az utasok ki tudják választani, hogy milyen jegyet vagy bérletet szeretnének venni, majd a fizetés után a nyomtató kinyomtatja a megfelelő jegyet vagy bérletet. Az eszközök automatikusan kapják IP címüket DHCP-n keresztül, amely a határ forgalomirányítón lett konfigurálva.

### VLAN 20 – Narancs terület (Beléptető rendszer)

6. ábra – VLAN 20 – Beléptető rendszer

A szimulációban 2 ilyen eszközt jelenítettünk meg az átláthatóság kedvéért, valós esetben ebből több van a megállóba.

Mivel a cég nem szeretne kieséseket a bevételében az esetleges bliccelők miatt és a jegyek vagy bérletek eladásából származik a cég bevételének nagyrésze ezért fontos, hogy csak utazásra jogosult utasok tudják használatba venni a metrokat. Ennek érdekében üzemel a beléptető rendszerünk. Miután az utas bedugta a bérletét az autómatába, az összehasonlítja az akkori pontos időt a bérleten szereplő dátummal, amennyiben még érvényes a bérlet az ajtók kinyílnak. Jegy használata esetén elég bedugni a jegyet és miután az autómata kijukaszotta azt, kinyílnak az ajtók. Az eszközök autómatikusan kapják meg IP címeiket DHCP-n keresztül a határ forgalomirányítótól.

### A képen diagram látható Automatikusan generált leírásA képen diagram látható Automatikusan generált leírásVLAN 30 – Magenta terület (Privát WIFI)

8. ábra – Vezeték nélküli forgalomirányító LAN-ja

7. ábra – VLAN 30 – Vezeték nélküli forgalomirányító

A megállóban dolgozók számára (pl. peronőr, pékség dolgozói) a cég szeretett volna egy privát vezeték nélküli hálózatot is biztosítani. A vezeték nélküli forgalomirányító autómatikusan kapja az IP címét DHCP-n keresztül és a saját hálózatának DHCP szerverként is működik.

### A képen diagram látható Automatikusan generált leírásVLAN 40 – Sárga terület (Pékség)

9. ábra – VLAN 40 – Pékség

A pékség a cégtől bérli a metro megallóban fenntartott üzlethelyiséget, ezért számukra is mi építettük ki a hálózatot. A dolgozók számára kellettek számítógépek amin számon vannak tartva a rendelések, egy nyomtató a számlázáshoz, egy IP telefon a rendelések felvételéhez és egy WEB szerver a pékség weboldalához ahol a vásárlók megtekinthetik az aktuális kínálatot, készlet információkat és rendeléseket tudnak leadni webes felületen keresztül is. Az eszközök a szerver kivételével autómatikusan kapják meg IP címeiket DHCP-n keresztül a határ forgalomirányítótól.

### VLAN 50 – Zöld terület (Admin szoba)

10. ábra – VLAN 50 – Admin szoba

Az admin számára fenntartott helyiség ahonnan felügyeli és karban tartja a helyi hálózatot. Az eszközök autómatikusan kapják meg IP címeiket DHCP-n keresztül a határ forgalomirányítótól.

## Wall Street Protokollok

Forgalomirányító:

* DHCP
  + Autómatikus IP címkiosztás a VLAN-oknak
* IPSec
  + A távoli munkás biztonságos kapcsolatának biztosítása.
* EIGRP
  + Dinamikus forgalomirányítás
* NAT/PAT
  + NAT segítségével statikusan fordítunk 1 címet 1 címre.
  + PAT segítségével a számítógépeket kiengedjük az internetre, több címet 1 címre fordítva amik port számok alapján követhetők.

Kapcsolók:

* STP
  + Második rétegbeli redundancia
  + A hurkok és a szórási viharok elkerülésének érdekében.
* Link Aggregation
  + Port összevonás.
  + Nagyobb sávszélesség biztosítása.
* Port Security
  + Az interfészek maximum 1 címet tanulnak meg, az első eszköz címét tanulják meg amit csatlakoztatnak az interfészhez, ismeretlen cím (portsértés) esetén az interfész lekapcsol.
* Vlan Trunking Protokoll (VTP)
  + A szerverként beállított kapcsoló VLAN információkat küldd a kliensként beállított kapcsolók számára a trunk protjain keresztül.

## Spanning-tree

Az STP egy második rétegbeli redundáns megoldás, ami a többszörös kapcsolat miatt keletkezett hibákat kezeli. Az STP biztosítja, hogy bármely két eszköz között csak egy logikai útvonal létezzen, a többit pedig lezárja. Ennek azért van jelentősége, mert alapvetően egy redundáns hálózatban hurkok jönnek létre. Ezek a hurkok több problémát is okoznak: MAC-cím táblát elárasztják, Egyedi keretek kétszeresen érnek céljukba és szórási vihar jön létre, amiben a szórás üzenetek folyamatosan keringenek és többszöröződnek a hálózatban addig, míg az ki nem fekszik túlterhelés miatt. Ezek másodpercek alatt leállíthatják az egész hálózatot, ezért fontos STP-t használni.

Az STP fajtákból a Rapid-PVST-t használjuk, mert ez az egyik leggyorsabban konvergáló. Sok erőforrást igényel, viszont a topológiába használt kapcsolók ezt bőven tudják futtatni. A Root Bridge-t úgy választottunk, hogy a Wall\_St\_SW\_Main switch legyen a Root Bridge. Ahhoz, hogy az STP zavartalanul működjön, több biztonsági funkciót is bevezettünk. Ez a kettő a PortFast és BPDU Guard. A BPDU Guard szerepe, hogy BPDU kereteket ne fogadjon a kapcsoló bizonyos portokról. Ez azért fontos, mert a BPDU keretek fontos szerepet játszanak a Root Bridge kijelölésében és ezekkel vissza lehet élni BPDU támadások esetén. Ha bekapcsoljuk egy interfészen, akkor onnan a kapcsoló nem fog BPDU kereteket elfogadni, ezzel megelőzve bármiféle támadást. A PortFast funkció felgyorsítja a kapcsolóhoz csatlakozó eszközök konvergenciáját azzal, hogy a beállított portokat azonnal forwarding állapotba kapcsolja.

## EIGRP

Forgalomirányító protokollnak az EIGRP protokollt választottuk, mert ez egy „vegyes” protokoll, tartalmaz részeket a távolságvektor és a kapcsolatállapot alapú protokollokból is. A router-hirdetéseket nem periodikusan küldi, hanem csak akkor, amikor topológiai változás történik a hálózatban és ezeket a hirdetéseket nem az összes eszköznek küldi el, hanem csak azoknak, akik közvetlenül érintettek a változásban. Emiatt sokkal kevésbé terheli a hálózatot, mint egy OSPF és gyorsabban konvergál is.

A protokoll azonosító számának a 50-es számot választottuk, az automatikus útvonalösszevonást kikapcsoltuk. MD5-ös hitelesítéssel is felruháztuk a routereket a nagyobb biztonság érdekében. Tervezetünkben key chain-nek EIGRP\_AUTH nevet, a kulcsszámnak 1-et és a kulcsnak az cisco123-at állítottunk be.

Az alapértelmezett kijáratot statikus útvonal segítségével határoztuk meg.

## IPSec VPN

Az Internet Protocol Security (IPsec) VPN (Virtual Private Network) egy protokoll csomag két pontot köt össze az interneten keresztül egy privát csatornán. Ezt a csatornát különböző hálózatbiztonsági és kriptográfia protokollok segítségével biztonságosabbá teszi. Egyrészt elrejti a két kommunikáló felet, ezzel inkognitást tesz lehetővé az Interneten. Másrészt a kommunikációt lebonyolító csatornán átmenő üzenetet titkosítja, ezáltal olvashatatlanná válik egy harmadik fél számára az üzenet. Cégünknél nagyon sok kényes adat van ezért elengedhetetlen volt, hogy a telephelyünk és a távoli munkás között titkosított átjárónk legyen.

Két fő protokoll érhető el: Authentication Header (AH) és Encapsulation Security Protocol (ESP). Attól függően, hogy melyiket választjuk az IPsec keretrendszerben más-más protokollok lesznek elérhetőek. Jelen esetünkben az ESP-t választottuk, mert az AH-val szemben ez képes az üzenet titkosítására is, továbbá rendelkezik visszajátszás elleni védelemmel is.

Megbizonyosodik arról, hogy minden csomag egyedi és semmi se lett módosítva. Miután létre jött a kapcsolat, egy számláló elindul és minden egyes küldött csomagnál az értéke megnő így biztosan tudja milyen számozású csomagot kell kapjon. Titkosításnál AES 256-ot választottuk, Integritásnál pedig SHA hiszen biztonságosabb, mint az MD5, hitelesítésnél „pre-shared” hiszen egyszerű fel konfigurálni.

## Link Aggregation

A Link Aggregation lehetőséget ad arra, hogy a kapcsolók közötti fizikai kábeleket logikailag összekössük. Ez azért szerencsés, mert egyrészt növeli a sávszélességet úgy, hogy nem kell drágább kábelekre költeni és ha esetleg az egyik fizikai kábel kiesne, akkor a hálózat tovább tud működni a másik kábeleken.

Protokollnak az LACP-t választottuk, mert az LACP nem csak a Cisco-s, hanem bármelyik más gyártótól származó switch-et is elfogad. A port-channelek mindkét fele „active” módba lettek állítva.

## VLAN Trunking Protocol

A VTP-t akkor érdemes használni, ha egy hálózatban sok vlan és kapcsoló található. Ez egy Cisco által kifejlesztett protokoll, ami megkönnyíti a VLAN-ok konfigurálását és karbantartását. Így elég egy kapcsolón törölni vagy hozzá adni egy új VLAN-t és az összes kapcsoló megtanulja.

Cégünknél a Wall\_St\_SW\_Main kapcsoló lett kinevezve szervernek, ami azt jelenti, hogy őt kell konfigurálni ahhoz, hogy a többi tanuljon tőle. Jelszóval van ellátva, ami a cisco domain név pedig cisco.com és természetesen 2-es verzióval van felkonfigurálva. A többi kapcsoló kliensnek van beállítva.

A protokoll működési feltétele, hogy a kapcsolók között be legyen állítva a trönkölés. A protokoll segítségével, ha bármikor állítanunk kell valamit, akkor ezt a szerverről meg tudjuk oldani.

## Port Security

A port védelem egy elengedhetetlen védelmi funkció egy cégnél. Segít megakadályozni az illetéktelen behatolást, mégpedig úgy, hogy hozzá rendel az interfészhez egy MAC címet és ha másik eszközt használunk lekapcsolja a portot és megnöveli a számlálóját így a rendszergazda látja, hogy valaki próbálkozott illetéktelenül csatlakozni a rendszerünkhöz. Sajnos könnyen kicselezhető hiszen, ha ismerjük az adott gép MAC címét pár perc alatt MAC cím hamisítást tudunk csinálni így kijátszottuk a rendszert.

Több dolgot betudunk állítani, cégünknél minden porthoz maximum 1db mac címet tanul meg a kapcsoló ezt a switchport port-security maximum 1 paranccsal tudjuk megoldani. A MAC címet automatikusan tanitatjuk meg az eszközzel a switchport port-security mac-address sticky paranccsal majd beállítjuk, hogy automatikusan lekapcsolj a portot, ha esteleg más próbálkozna, szükséges parancs hozzá: switchport port-security violation shutdown.

Minden használaton kívüli portot lekapcsoltunk, es külön vlan-ba raktuk így, ha valaki mégis felkapcsolná a portot nem fog tudni kommunikálni senkivel mert nincs beállítva a forgalomirányítás.

## NAT/PAT

A határ forgalomirányító végez címfordítást 2 okból kifolyólag. Statikus címfordítást a web szervernek, hogy külső címmel elérhető legyen és túlterheléses címfordítást mely alapján internet elérést biztosítunk a különböző vlan-oknak. Az egyes vlan-ok címtartományát fordítjuk egy külső címre melyen kereszül elérhetik az internetet és portszám alapján visszaküvethető a kommunikáció ezért elég 1 címre fordítani egyes vlan-ok címtartományait.

# Zöld elipszis terület: MTA Headquarters

11. ábra – MTA Headquarters (zöld elipszis terület) logikai térképe

## MTA Headquarters eszközök

A Cisco Packet Tracerben a következő eszközöket használtuk ezen a területen:

* 1 darab Cisco 4331 forgalomirányító
  + - 1 darab NIM-2T bővítő kártya

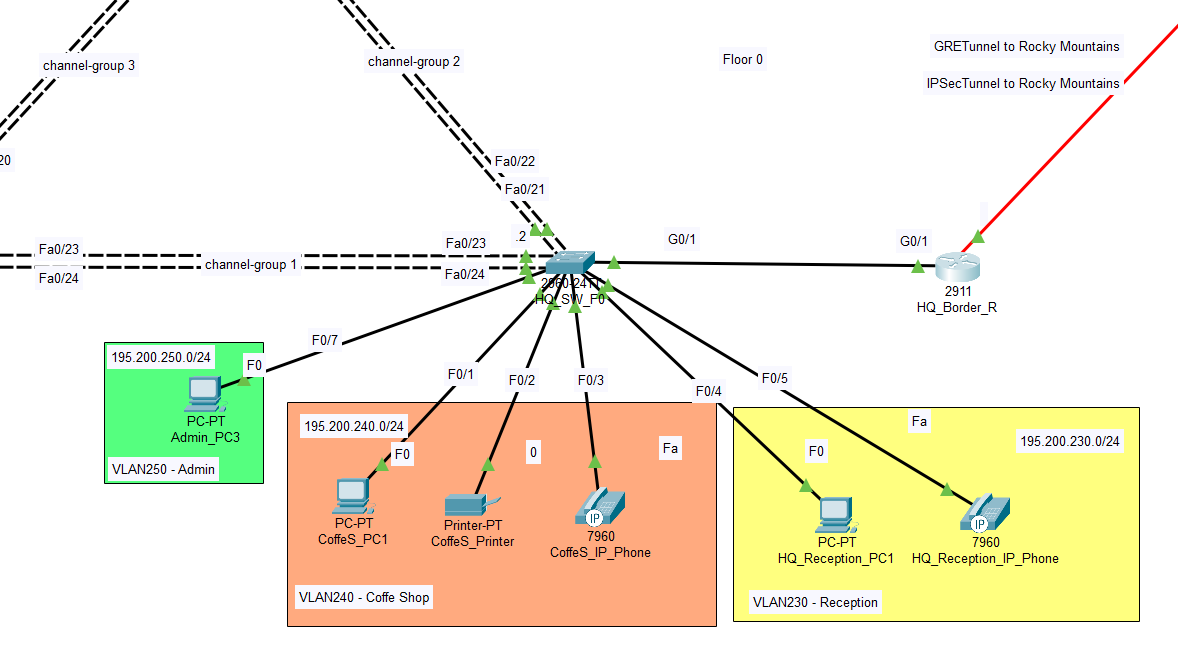
12. ábra – MTA Headquarters határ forgalomirányító bővítmények

* 2 darab Cisco WRT300N vezeték nélküli forgalomirányító
* 3 darab Cisco 2960 kapcsoló
* Nyomtatók
* Számítógépek
* IP telefonok
* 1 darab szerver

## MTA Headquarters VLAN-ok

Az iroda hálózatát VLAN-okkal logikai szegmensekre osztottuk.

### Földszinten:



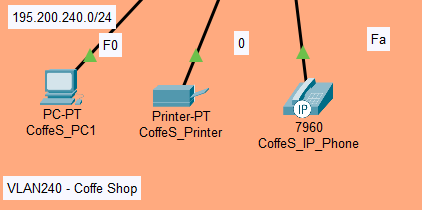
13. ábra – MTA Headquarters épület földszint

### VLAN 230 – Sárga terület (Recepció)

14. ábra – Földszinti recepció

Az ügyfélszolgálat és tájékoztatás elősegítéséért a recepción dolgozó alkamazottaknak biztosítottunk IP telefonokat és számítógépeket a munkaügyek intézéséhez, hívások átirányításához. Az eszközök autómatikusan kapják meg IP címeiket a távoli DHCP szervertől.

### VLAN 240 – Narancs terület (Kávézó)



15. ábra – Földszinti recepció

A kávézó a cégtől bérli az épületben fenntartott üzlethelyiséget, ezért számukra is mi építettük ki a hálózatot. A dolgozók számára kellettek számítógépek, amin számon vannak tartva a rendelések, egy nyomtató a számlázáshoz és egy IP telefon a rendelések felvételéhez. Az eszközök automatikusan kapják meg IP címeiket a távoli DHCP szervertől.

### VLAN 250 – Zöld terület (Admin szoba)

16. ábra – Földszinti admin szoba

Az adminok számára fenntartott helyiség, ahonnan felügyelik és karban tartják a helyi hálózatot. Az eszközök autómatikusan kapják meg IP címeiket a távoli DHCP szervertől.

### Első emeleten: A képen diagram látható Automatikusan generált leírás

17. ábra – MTA Headquarters épület első emelet

16. ábra – MTA Headquarters épület első emelet

### VLAN 210 – Piros terület (Alkalmazottak)

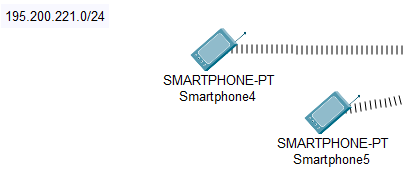
18. ábra – Első emeleti iroda

Az első emelet egy nagy irodának lett kiépítve, ahol a cég 170 alsóbb beosztású alkalmazottja dolgozik. Fontos számukra, hogy minden alkalmazott rendelkezzen 1 számítógéppel és egy IP telefonnal, valamint az emeleten legyen nyomtató is. Az eszközök automatikusan kapják meg IP címeiket a távoli DHCP szervertől.

### VLAN 220 – Lila terület (Privát WIFI)

19. ábra – Első emeleti vezeték nélküli forgalomirányító

20. ábra – Első emeleti vezeték nélküli forgalomirányító LAN-ja

Az épületben dolgozók számára a cég szeretett volna egy privát vezeték nélküli hálózatot is biztosítani. A vezeték nélküli forgalomirányító automatikusan kapja az IP címét a távoli DHCP szervertől és a saját hálózatának DHCP szerverként is működik. Lefedettségi okok miatt emeletenként 1-re szükség van.

### Második emeleten:

21. ábra – MTA Headquarters épület második emelet

### VLAN 200 – Kék terület (Helyi szerverek)

22. ábra – Második emeleti szerver szoba

A cég web szerverét az épületen belül helyeztük el a könnyebb elérhetőség érdekében.

### VLAN 210 – Piros terület (Alkalmazottak)

23. ábra – Második emeleti iroda

A második emeleti irodában a cég 80 magasabb beosztású alkalmazottja dolgozik. Fontos számukra, hogy minden alkalmazott rendelkezzen 1 számítógéppel és egy IP telefonnal, valamint az emeleten legyen nyomtató is. Az eszközök automatikusan kapják meg IP címeiket a távoli DHCP szervertől.

### VLAN 220 – Lila Terület (Privát WIFI)

25. ábra – Második emeleti vezeték nélküli forgalomirányító LAN-ja

24. ábra – Második emeleti vezeték nélküli forgalomirányító

### VLAN 250 – Zöld Terület (Admin szoba)

26. ábra – Második emeleti admin szoba

## MTA Headquarters Protokollok

Forgalomirányító:

* GRE Tunnel
  + IPv4 csomagokat IPv4 csomagokba ágyaz és így kuldi ki az internet felé
  + Ennek eredménye képpen 1 forgalomirányítási területté alakítjuk a távoli szervereinkkel
* IPv6 GRE Tunnel
  + IPv6 csomagokat IPv4 csomagokba ágyaz és így kuldi ki az internet felé
  + Ennek eredménye képpen az ISP-nek nem kell konfigurálva lennie IPv6 csomagok áthaladasára
* IPSec Tunnel
  + A GRE Tunneljeinknek biztonságot ad
* EIGRP
  + Dimaikus forgalomirányítás
* DHCPv6 Stateless
  + Autómatikus IPv6-os címkiosztás
* NAT/PAT
  + NAT segítségével statikusan fordítunk 1 címet 1 címre.
  + PAT segítségével a számítógépeket kiengedjük az internetre, több címet 1 címre fordítva, amik port számok alapján követhetők.

Kapcsolók:

* STP
  + Második rétegbeli redundancia
  + A hurkok és a szórási viharok elkerülésének érdekében.
* Link Aggregation
  + Port összevonás.
  + Nagyobb sávszélesség biztosítása.
* Port Security
  + Az interfészek maximum 1 címet tanulnak meg, az első eszköz címét tanulják meg amit csatlakoztatnak az interfészhez, ismeretlen cím (portsértés) esetén az interfész lekapcsol.
* Vlan Trunking Protokoll (VTP)
  + A szerverként beállított kapcsoló VLAN információkat küldd a kliensként beállított kapcsolók számára a trunk protjain keresztül.

## GRE Tunnel

Generic Routing Encapsulation-t használtunk a headquarters és a távoli szerver farmunk között, ezzel 1 irányítási terület keletkezett belőlük ami lehetővé tette, hogy az interneten kereszül a dolgozók elérjék a szervereket. A forgalomirányító ezt úgy teszi lehetővé, hogy amikor kiküld egy csomagot az internet szolgáltató felé azt becsomagolja még egy GRE csomagba ezzel megváltoztatja a csomag cél IP címét. A csomag fogadásakor a távoli helyen lévő forgalomirányító ezt a csomagot kibontja, kiolvassa belőle a cél IP címet és onnantól tudja tovább küldeni a csomagot a megfelelő helyre. A csomagok megvédése érdekében IPSec Tunnel-t is alkalmaztunk, hogy a csomagokat ne tudja akarki lelopni, kibontani és ezzel veszélynek kitenni a szervereinket.

## IPv6 over IPv4 GRE Tunnel

Az IPv4 címek fogyása, a könnyebb elérhetőség és a modernizáció érdekében létrehoztunk egy IPv6 over IPv4 Generic Routing Encapsulation tunnel-t is. Így a szerverk elérhetők IPv6 címekkel is az interneten kereztül. Ez ugyanúgy működik mint a GRE tunnel annyiban eltérve, hogy egy IPv6-os csomagot ágyaz be egy IPv4 csomagba és ezt küldi ki az internetszolgáltató felé.

## DHCPv6 Stateless

Az SLAAC lehetővé teszi, hogy állomások automatikusan generáljanak egyedi IPv6 címet RA (Route Advertisement) üzenetekkel így viszont nem kapják meg a DNS szerver címét. Ennek a problémának a megoldása, hogy a forgalomirányító ami kiküldi az RA üzeneteket beállítja az O bitet (other bit/flag) 1-es értékre ezzel jelezve az állomásoknak, hogy kommunikálhatnak a stateless DHCPv6 szerverrel és onnan megkaphatják a DNS szerver címét.

# A képen diagram látható Automatikusan generált leírásRózsaszín elipszis terület: MTA Garázs/Szervíz

27. ábra – MTA Garázs/Szervíz (rózsaszín elipszis terület) logikai térképe

# MTA Garázs/Szervíz eszközök

A Cisco Packet Tracerben a következő eszközöket használtuk ezen a területen:

* 3 darab Cisco 2911 forgalomirányító
  + - 2 darab HWIC-2T bővítő kártya (1/határ forgalomirányító)

28. ábra – MTA Garázs/Szervíz aktív/tartalék forgalomirányító bővítmények

* 1 darab Access Point
* 4 darab Cisco 2960 kapcsoló
* Nyomtatók
* Számítógépek
* IP telefonok
* Telefonok és tabletek

## MTA Garázs/Szervíz VLAN-ok

A Garázs/Szervíz hálózatát VLAN-okkal logikai szegmensekre osztottuk.

### VLAN 320 – Kék terület (Dolgozók)

29. ábra – Földszinti dolgozók

A cég azon alkalmazottai dolgoznak, akik a diagnosztikai adatokat feldolgozzák és továbbítják az irodában dolgozó alkalmazottak felé.

### VLAN 310 – Sötét zöld terület (CEO szoba)

30. ábra – Első emeleti CEO szoba

Ezt a szobát a vezérigazatónak alakítottuk ki az itt található felszerelésekkel végzi a napi teendőit.

### VLAN 340 – Világos zöld terület (Admin szoba)

31. ábra – Első emeleti admin szoba

Az adminok számára fenntartott helyiség ahonnan felügyelik és karban tartják a helyi hálózatot. Az eszközök automatikusan kapják meg IP címeiket a routeren található DHCP szervertől.

## MTA Garázs/Szervíz Protokollok

Forgalomirányító:

* EIGRP
  + Dinamikus forgalomirányítás
* HSRP
  + Harmadik rétegbeli redundancia
* DHCP
  + Autómatikus IP címkiosztás
* NAT/PAT
  + NAT segítségével statikusan fordítunk 1 címet 1 címre.
  + PAT segítségével a számítógépeket kiengedjük az internetre, több címet 1 címre fordítva amik port számok alapján követhetők.

Kapcsolók:

* STP
  + Második rétegbeli redundancia
  + A hurkok és a szórási viharok elkerülésének érdekében.
* Link Aggregation
  + Port összevonás.
  + Nagyobb sávszélesség biztosítása.
* Port Security
  + Az interfészek maximum 1 címet tanulnak meg, az első eszköz címét tanulják meg amit csatlakoztatnak az interfészhez, ismeretlen cím (portsértés) esetén az interfész lekapcsol.
* Vlan Trunking Protokoll (VTP)
  + A szerverként beállított kapcsoló VLAN információkat küldd a kliensként beállított kapcsolók számára a trunk protjain keresztül.

## HSRP

A HSRP (Hot Standby Router Protocol) protokoll egy virtuális IP címet kínál fel a LAN hálózatunk számára alapértelmezett átjáróként. Ezt a virtuális IP címet adjuk meg alapértelmezett átjáróként a LAN állomásain. A virtuális IP címen több forgalomirányító is osztozik, egymás között megbeszélve, hogy melyikük fogja az active illetve a standby feladatát ellátni, vagyis melyik forgalomirányító fogja átvenni az alapértelmezett átjáró feladatát. Úgy lettek konfiguráva a forgalomirányítók, hogy az active forgalomirányító kiesése esetén a standby veszi át az active szerepet, de ha újra működésbe lép a kiesett forgalomirányító akkor újra ő veszi át az active szerepet.

# Barna elipszis terület: Rocky Mountains szerver terem

32. ábra – Rocky Mountains szerver terem (barna elipszis terület) logikai térképe –

# Rocky Mountains eszközök

* 1 darab Cisco 4331 forgalomirányító
  + - 1 darab NIM2-T bővítő kártya

33. ábra – Rocky Mountains forgalomirányító bővítmények

* 1 darab Cisco 2960 kapcsoló
* 4 darab szerver
* 1 darab laptop

## Rocky Mountains Protokollok

Forgalomirányító:

* EIGRP
  + Dinamikus forgalomirányítás
* GRE Tunnel
  + IPv4 csomagokat IPv4 csomagokba ágyaz és így kuldi ki az internet felé
  + Ennek eredménye képpen 1 forgalomirányítási területté alakítjuk a távoli szervereinkkel
* IPv6 GRE Tunnel
  + IPv6 csomagokat IPv4 csomagokba ágyaz és így kuldi ki az internet felé
  + Ennek eredménye képpen az ISP-nek nem kell konfigurálva lennie IPv6 csomagok áthaladasára
* IPSec Tunnel
  + A GRE Tunneljeinknek biztonságot ad
* NAT/PAT
  + NAT segítségével statikusan fordítunk 1 címet 1 címre.
  + PAT segítségével a számítógépeket kiengedjük az internetre, több címet 1 címre fordítva, amik port számok alapján követhetők.

Kapcsolók:

* STP
  + Második rétegbeli redundancia
  + A hurkok és a szórási viharok elkerülésének érdekében.
* Link Aggregation
  + Port összevonás.
  + Nagyobb sávszélesség biztosítása.
* Port Security
  + Az interfészek maximum 1 címet tanulnak meg, az első eszköz címét tanulják meg amit csatlakoztatnak az interfészhez, ismeretlen cím (portsértés) esetén az interfész lekapcsol.
* Vlan Trunking Protokoll (VTP)
  + A szerverként beállított kapcsoló VLAN információkat küldd a kliensként beállított kapcsolók számára a trunk protjain keresztül.

## Rocky Mountains VLAN-ok

A szerverterem hálózatát VLAN-okkal logikai szegmensekre osztottuk a biztonság, valamint a könnyebb kezelhetőség érdekében.

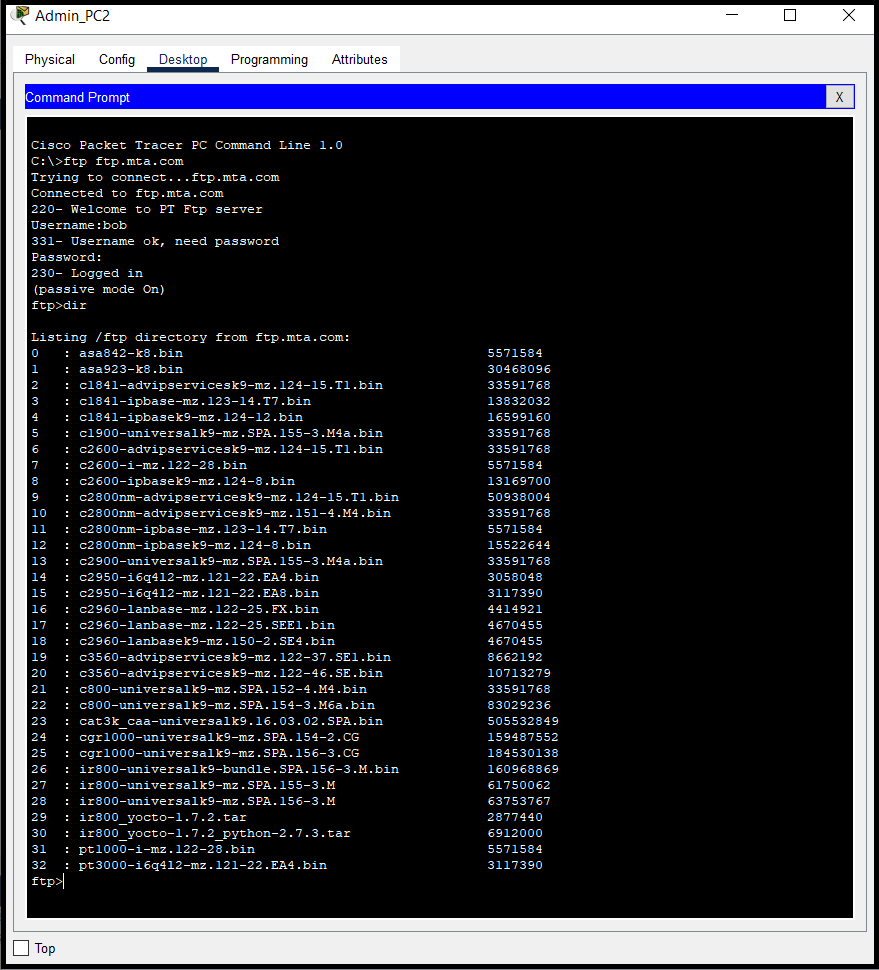
### VLAN 400 – Lila terület (Szerverek)

34. ábra – Szerver terem

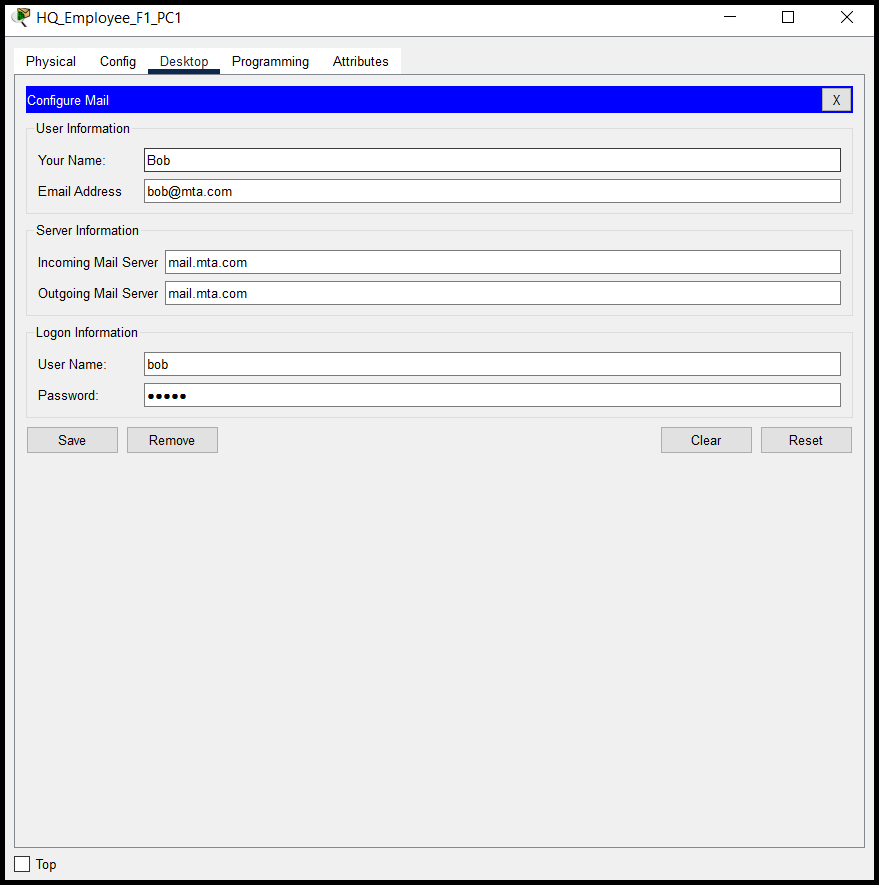
A vállalat szervergépei a Sziklás-hegységben találhatóak, mindegyik más-más feladatot lát el, a hegység hűs levegője megkönnyíti a szerverek hőmérséklet kezelését.

### FTP, Mail

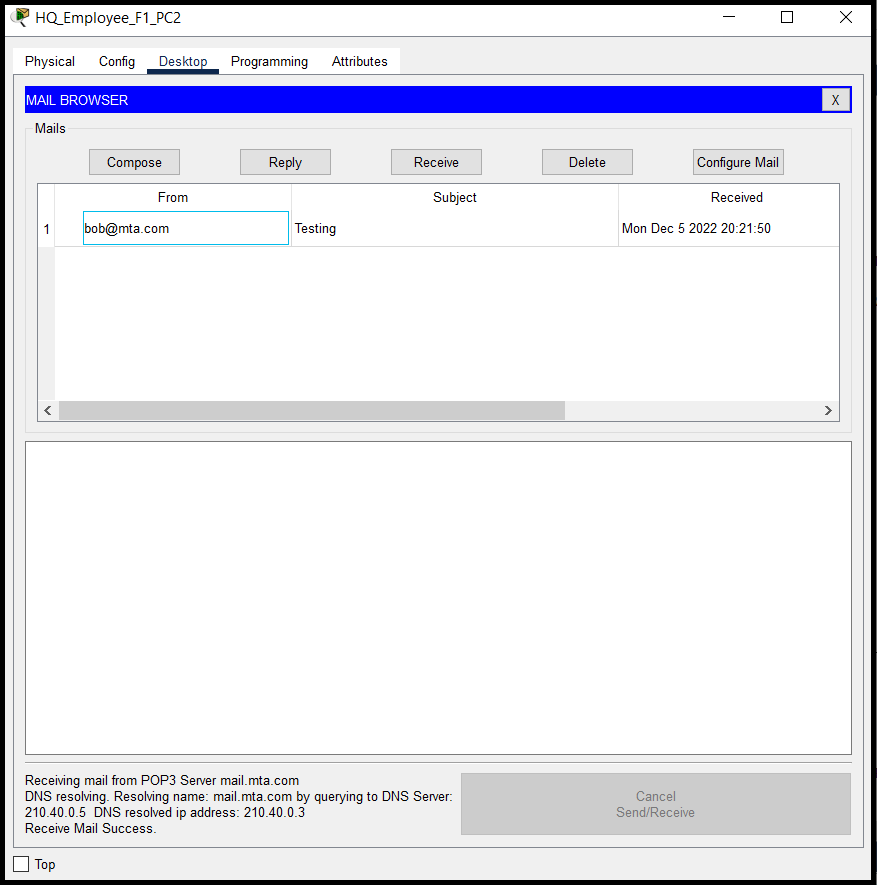
Minden dolgozónak biztosítottunk egy egyedi jelszó, illetve e-mail párost, amivel hozzáférhetnek a levelezőrendszerhez és elérhetik egymást.



35. ábra – FTP szerverhez csatlakozás névfeloldással



36. ábra – Mail kliens konfigurálása névfeloldással



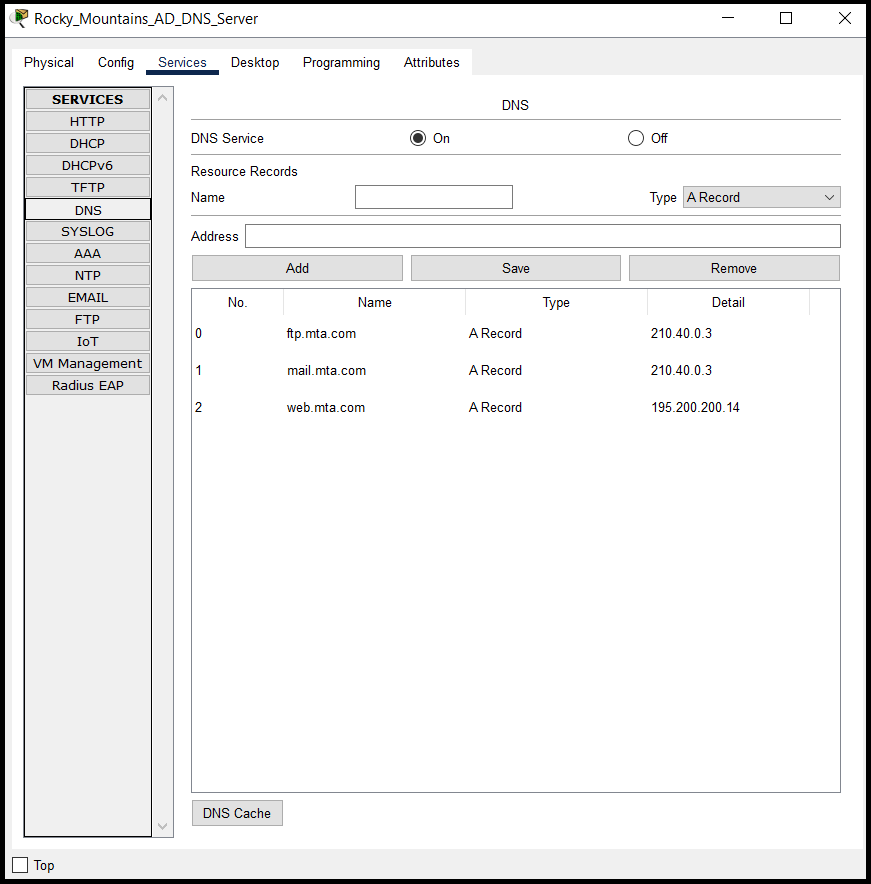
37. ábra – Sikeres email fogadás a kliensek között

### SYSLOG\_NTP, AAA

A rendszer biztonsága érdekében nyomon követjük a felhasználók aktivitásait a rendszeren belül, minden belépést követően a szerver üzenetet kap ami tartalmazza a belépés pontos idejét, valamint tájékoztat a felhasználó tevékenységeiről.

### AD, DNS

A felhasználóknak nehéz lenne számon tartani a különböző szolgáltatások ip címeit ezért elláttuk azokat DNS névvel, így elegendő csak ezeket tudni.



38. ábra – DNS szerver beállításai

### DHCP

A dolgozók eszközei dinamikusan kapnak IPv4 címet a távoli DHCP szervertől.

### A képen diagram látható Automatikusan generált leírásVLAN 410 – Zöld terület (Admin szoba)

39. ábra – Admin szoba

Az adminok számára fenntartott helyiség, ahonnan felügyelik és karban tartják a helyi hálózatot. Az eszközök automatikusan kapják meg IP címeiket a routeren található DHCP szervertől.

# Kék elipszis terület: Távoli dolgozó

40. ábra – Távoli dolgozó (kék elipszis terület) logikai térképe

## Távoli dolgozó Protokollok

Forgalomirányító:

* EIGRP
  + Dinamikus forgalomirányítás
* IPSec Tunnel
  + A GRE Tunneljeinknek biztonságot ad
* NAT/PAT
  + NAT segítségével statikusan fordítunk 1 címet 1 címre.
  + PAT segítségével a számítógépeket kiengedjük az internetre, több címet 1 címre fordítva amik port számok alapján követhetők.

Kapcsolók:

* STP
  + Második rétegbeli redundancia
  + A hurkok és a szórási viharok elkerülésének érdekében.
* Link Aggregation
  + Port összevonás.
  + Nagyobb sávszélesség biztosítása.
* Port Security
  + Az interfészek maximum 1 címet tanulnak meg, az első eszköz címét tanulják meg amit csatlakoztatnak az interfészhez, ismeretlen cím (portsértés) esetén az interfész lekapcsol.

# Távoli dolgozó eszközök

* 1 darab Cisco 4331 forgalomirányító
  + - 1 darab NIM2-T bővítő kártya

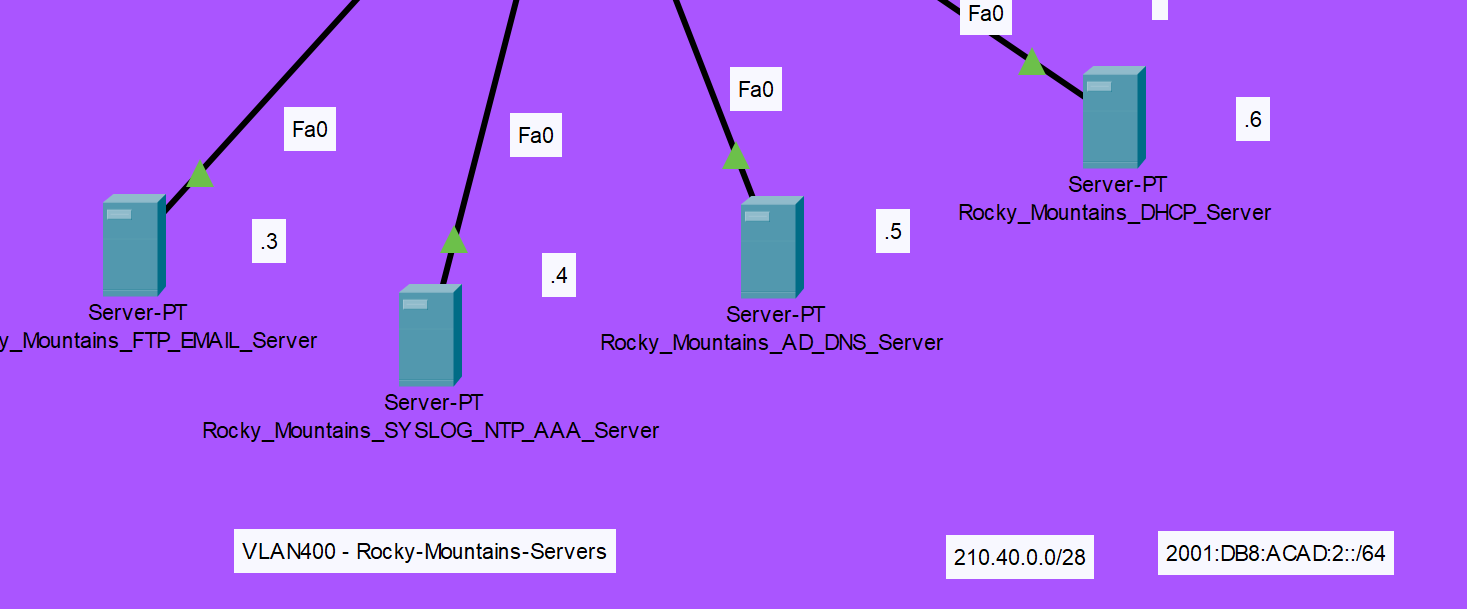
41. ábra – Remote Worker forgalomirányító bővítmények

* 1 darab Cisco 2960 kapcsoló
* 1 darab kábelmodem
* 1 darab számítógép

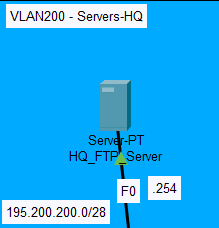
**Szerverek dokumentációja**

A New York-i metróhálózat számára elengedhetetlen egy hatékony szerver infrastruktúra, amely képes fenntartani egy gyors és biztonságos kommunikációt a rendszerben résztvevő összes eszköz között. Ennek érdekében az elsődleges szervereink egy bérelt adatközpontban helyezkednek el, itt folytonos megfigyelés alatt állnak őrök és kamerák által, és felügyelve van minden hálózati forgalom. Itt az esedékes áramszüneteknél is biztosítva van az energiahálózat, szünetmentes áramellátással és tartalék aggregátorokkal. Esetleges áramszünet miatt a saját telepünk is szünetmentes tápegységekkel vannak ellátva, illetve beszereltünk egy saját dízel aggregátort is, ami az épület minden esszenciális létesítményét el tudja látni árammal. A szerverszobába történő belépés csak és kizárólag a hozzá jogosultak azonosítása után történhet meg illetve papírformában is dokumentáljuk a belépő személyek nevét, személyi számát, bent tartózkodás időtartalmát és okát.

**Szolgáltatások**

A Rocky Mountains adatközpontban található négy bérelt szerver. Ezek a szerverek a következő szolgáltatásokat nyújtják: AD, DNS, DHCP, MAIL, NTP, AAA, SYSLOG.

41. ábra – Adatközpont szerver terem

Ezeken felül üzemeltetünk egy céges Windows operációs rendszerű szervert, ami a következő szolgáltatásokat nyújtja: WEB, PRINT, FTP.

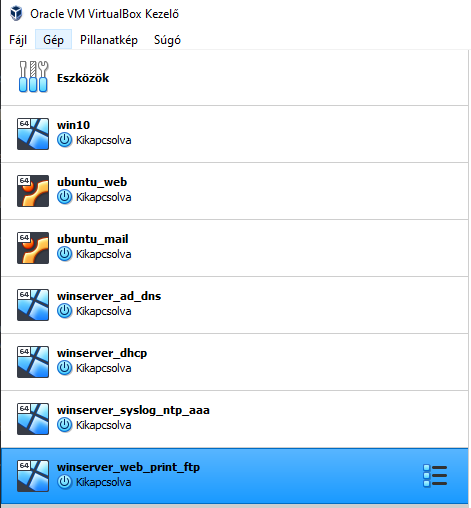
42. ábra – Céges szerver szoba

A képen diagram látható

Automatikusan generált leírásA Wall Street megállói pékség kérésére üzemeltetünk nekik egy Linux operációs rendszerű WEB szervert.

43. ábra – Pékség szerver

**Virtualbox**

A szervereinket az Oracle VM VirtualBox nevű szimulációs szoftverrel virtualizáltuk.

44. ábra - Oracle VM Virtualbox

**Szolgáltatások**

**Active Directory**

Az Active Directory a Microsoft címtárszolgáltatása, mely a Windows Server rendszeren fut és lehetővé teszi az engedélyek kezelését és a hálózati erőforrásokhoz való hozzáférést.

Az Active Directory tartalmazza a felhasználói fiókokat, jelszópolitikákat, csoporttagságokat, számítógépek konfigurációit és az erőforrásokhoz való hozzáférési engedélyeket is. Ezáltal az Active Directory megkönnyíti a felhasználók és erőforrások központi kezelését és nyomon követését a hálózaton belül. Az Active Directory fontos szerepet játszik a nagyvállalati hálózatok, szervezetek, iskolák és kormányzati szervek számítógépes rendszereinek kezelésében és biztonságos működtetésében. Ez a szolgáltatás az egyik külső Windows szerverünkön fut

**Domain Name System**

DNS (Domain Name System) egy hierarchikus rendszer, amely lehetővé teszi, hogy az interneten lévő eszközök könnyen megtalálják egymást. A DNS rendszer a domainneveket (pl. mta.com) fordítja IP-címekre, amelyek azonosítják az interneten található számítógépeket és eszközöket.

A DNS rendszer kulcsfontosságú a modern internet működése szempontjából, mivel lehetővé teszi a felhasználók számára, hogy a könnyen megjegyezhető domainnevek segítségével könnyen hozzáférjenek az interneten található szolgáltatásokhoz és tartalmakhoz, anélkül, hogy emlékezniük kellene a hozzájuk tartozó IP-címekre. A DNS szolgáltatásunk az egyik külső Windows szerveren fut.

**Dynamic Host Configuration Protocol**

DHCP (Dynamic Host Configuration Protocol) egy hálózati kommunikációs protokoll, amely lehetővé teszi, hogy az eszközök automatikusan kapjanak IP-címet és hálózati konfigurációt a hálózaton belül. Az IP-cím egyedileg azonosítja az eszközt a hálózaton, és a hálózati konfiguráció tartalmazza az olyan információkat, mint a háttértár helye, az alapértelmezett átjáró és a DNS-szerver.

A DHCP szerver felelős az IP-címek és hálózati konfigurációk dinamikus kiosztásáért a hálózaton belül. Az eszközök, amelyek DHCP-t használnak, automatikusan kommunikálnak a DHCP szerverrel, amikor csatlakoznak a hálózatra, és a szerver dinamikusan kiosztja az IP-címet és a hálózati konfigurációt. Ez a folyamat megkönnyíti az eszközök csatlakozását a hálózathoz, és lehetővé teszi a hálózati konfiguráció egyszerű kezelését és változtatását. A DHCP szolgáltatásunk külön, az egyik külső Windows szerverünkön fut.

**Mail Server:**

A mail szerver, más néven levelező szerver, egy olyan számítógépes szoftver, amely lehetővé teszi a levelek küldését, fogadását és továbbítását az elektronikus levelezés (e-mail) rendszerében.

A belső hálózatunkban IRedMail-t használunk, amit a felhasználók, előre telepített Mozilla Thunderbird-ön keresztül használhatnak. Az IRedMail a külső Linux szerverünkön fut.

**Internet Information Services**

Ez egy Microsoftos webszerver szolgáltatás, ami a belső Windows szerverünkön fut, és biztosítja a weboldalunk elérhetőségét HTTPS kapcsolaton keresztül.

**Print Server:**

A print szerver olyan számítógép, amelynek fő feladata a nyomtatási feladatok kezelése és irányítása egy vagy több nyomtatóra a hálózatban. A print szerver lehetővé teszi, hogy több felhasználó tudjon nyomtatni a hálózatban lévő nyomtatókra, valamint segítségével a nyomtatók könnyebben konfigurálhatók és karbantarthatók. Ezt a szolgáltatásunkat a belső Windows szerverünkön futtatjuk.

**SSH File Transfer Protocol (sFTP)**

Ez biztosítja két távoli rendszer között a fájlátvitelt. A sima FTP kapcsolatnál biztonságosabb, mert SSH protokollal van kiegészítve. Ez a szolgáltatás a belső Windows szerverünkön fut.

**A hálózatban használt szerverek**

**Rocky Mountains Szerverek**

**Windows Server (1) – AD | DNS**

Hardware és Software beállítások:

* Hálózati kártya 🡪Belső hálózat
* Processzormagok száma: 2
* Memória mérete: 1024 Mb
* Tárhely: 50 Gb (OS)
* Operációs Rendszer: Windows Server GUI 2022

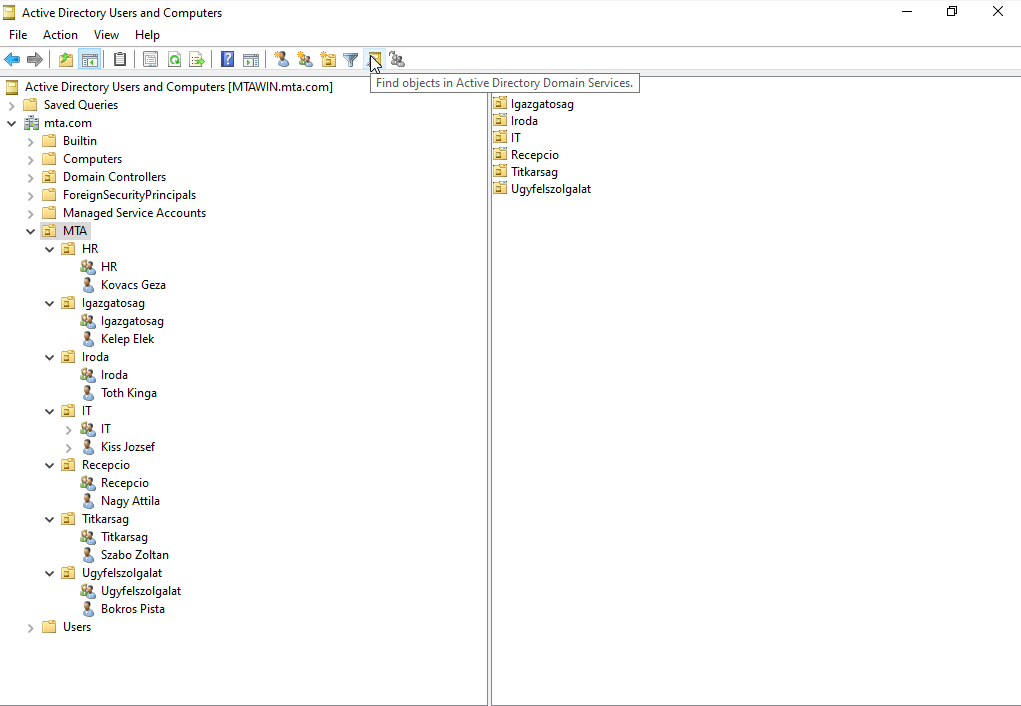
Telepített szolgáltatások:

* Active Directory
* Domain Name System (DNS)

Beállítások:

* Hostname: winserver\_ad
* Szerver admin felhasználónév: admin
* Szerver admin jelszava: Nincs1234
* Statikus IP cím: 210.40.0.5
* Alhálózati maszk: 255.255.255.240
* Alapértelmezett átjáró: 210.40.0.1

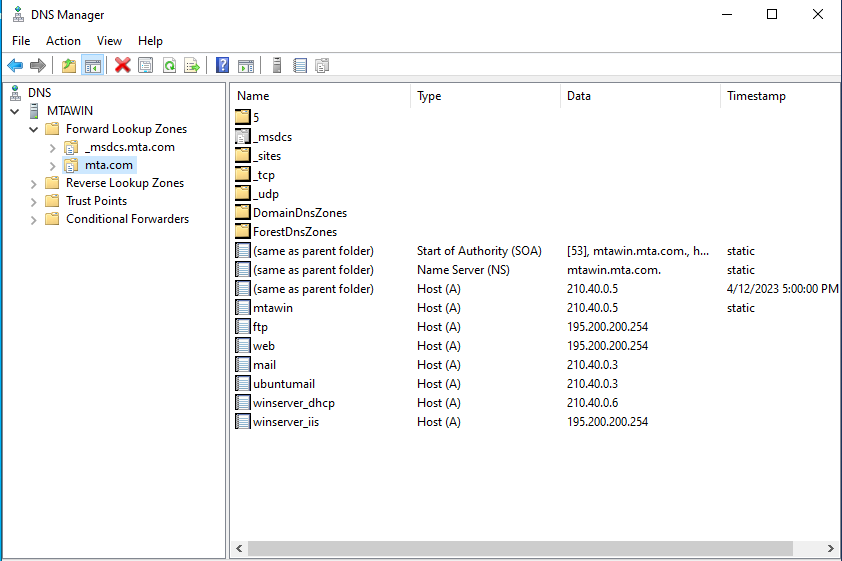
Szervezeti egységek:

* + HR
    - Kovács Geza - kovgez | Nincs1234
  + Igazgatosag
    - Kelep Elek - kelele | Nincs1234
  + Iroda
    - Toth Kinga - totkin | Nincs1234
  + IT
    - Kiss Jozsef - kisjoz | Nincs1234
  + Recepcio
    - Nagy Attila - nagatt | Nincs1234
  + Titkarsag
    - Szabo Zoltan - szazol | Nincs1234
  + Ugyfelszolgalat
    - Bokros Pista - bokpis | Nincs1234
  + ftp\_users
    - joomlaftpuser | Nincs1234

45. ábra - szervezeti egységek és felhasználók

**Forward Lookup Zónák**

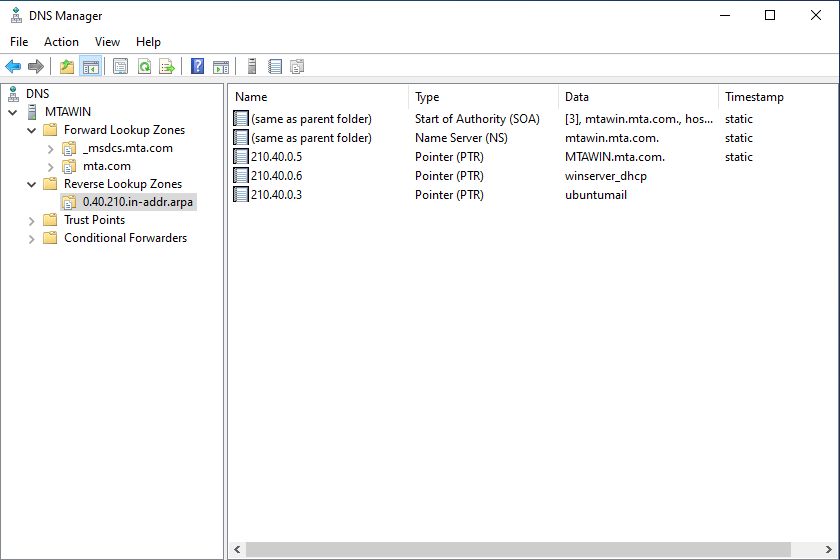
|  |  |  |
| --- | --- | --- |
| Forward Lookup Zones | | |
| Host név | IP cím | DNS |
| ftp | 195.200.200.254 | ftp.mta.com |
| web | 195.200.200.254 | web.mta.com |
| ubuntumail | 210.40.0.3 | ubuntumail.mta.com |



46. ábra – DNS szerver Forward lookup zónák

**Reverse Lookup Zónák**

|  |  |  |
| --- | --- | --- |
| Reverse Lookup Zones | | |
| Host név | IP cím | DNS |
| winserver\_ad | 210.40.0.5 | winserver\_ad.mta.com |
| winserver\_dhcp | 210.40.0.6 | winserver\_dhcp.mta.com |
| winserver\_iis | 195.200.200.254 | winserver\_iis.mta.com |
| ubuntumail | 210.40.0.3 | ubuntumail.mta.com |



47. ábra – DNS szerver Reverse lookup zónák

**Windows Server (2) – DHCP**

Hardware és Software beállítások:

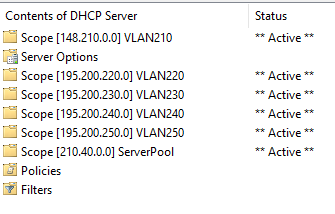
* Hálózati kártya 🡪Belső hálózat
* Processzormagok száma: 2
* Memória mérete: 1024 Mb
* Tárhely: 50 Gb (OS)
* Operációs Rendszer: Windows Server GUI 2022

Telepített szolgáltatások:

* Dynamic Host Configuration Protocol (DHCP)

Beállítások:

* Hostname: winserver\_dhcp
* Szerver admin felhasználónév: admin
* Szerver admin jelszava: Nincs1234
* Statikus IP cím: 210.40.0.6
* Alhálózati maszk: 255.255.255.240
* Alapértelmezett átjáró: 210.40.0.1
  + ServerPool
    - Gateway 210.40.0.1
    - Range 210.40.0.2 – 210.40.0.254
    - DNS 210.40.0.5 ; 8.8.8.8
  + VLAN220
    - Gateway 195.200.220.1
    - Range 195.200.220.2 – 195.200.220.3
    - DNS 210.40.0.5 ; 8.8.8.8
  + VLAN240
    - Gateway 195.200.240.1
    - Range 195.200.240.10 – 195.200.220.254
    - DNS 210.40.0.5 ; 8.8.8.8
  + VLAN230
    - Gateway 195.200.230.1
    - Range 195.200.230.10 – 195.200.230.254
    - DNS 210.40.0.5 ; 8.8.8.8
  + VLAN210
    - Gateway 148.210.0.1
    - Range 148.210.0.10 – 148.210.0.254
    - DNS 210.40.0.5 ; 8.8.8.8
  + VLAN250
    - Gateway 195.200.250.1
    - Range 195.200.250.10 – 195.200.250.254
    - DNS 210.40.0.5 ; 8.8.8.8



48. ábra – DHCP szerver címtartományok

**Ubuntu Server – Mail Server**

Hardware és Software beállítások:

* Hálózati kártya 🡪Belső hálózat
* Processzormagok száma: 2
* Memória mérete: 4096 Mb
* Tárhely: 20 Gb (OS)
* Operációs Rendszer: Ubuntu Server 22.04

Telepített szolgáltatások:

* Mail Server - IRedMail

Beállítások:

* Hostname: ubuntu\_mail
* Szerver admin felhasználónév: root
* Szerver admin jelszava: Nincs1234
* Statikus IP cím: 210.40.0.3
* Alhálózati maszk: 255.255.255.240
* Alapértelmezett átjáró: 210.40.0.1

**MTA Headquarter Server**

**Windows Server – WEB, FILE, PRINT**

Hardware és Software beállítások:

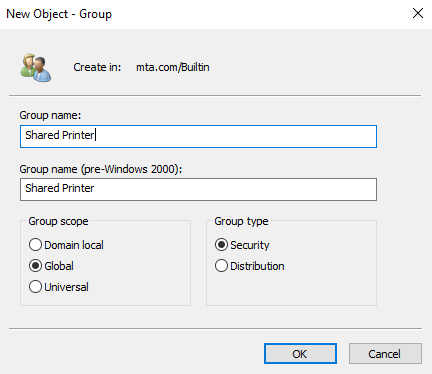
* Hálózati kártya 🡪Belső hálózat
* Processzormagok száma: 2
* Memória mérete: 1024 Mb
* Tárhely: 50 Gb (OS) + 50 gb (backup)
* Operációs Rendszer: Windows Server GUI 2022

Telepített szolgáltatások:

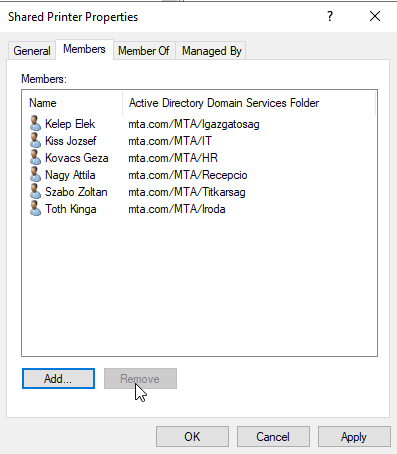
* Group Policy
* Megosztott nyomtató
* Web Server
* File Server

Beállítások:

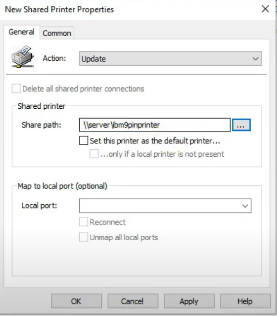
* Hostname: winserver\_web
* Szerver admin felhasználónév: admin
* Szerver admin jelszava: Nincs1234
* Statikus IP cím: 195.200.200.254
* Alhálózati maszk: 255.255.255.0
* Alapértelmezett átjáró: 195.200.200.1



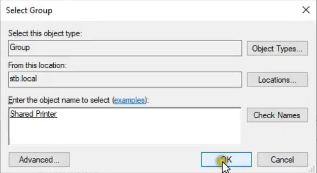
49. ábra – Group Policy készítés



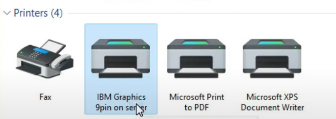
50. ábra – Felhasználók hozzáadása



51. ábra – Nyomtató hozzáadása a GPO-hoz



52. ábra – Security Group hozzáadása a GPO-hoz



53. ábra – A felvett nyomtató