Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

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

***száma:*** 5-0612-12-02

**VIZSGAREMEK**  
**Szász Tamás István korház bemutatása**

Fazekas Gábor János, Kun Leon

2/14B

Budapest, 2024.

Tartalom

[Cégleírás 5](#_Toc165281962)

[A hálózat dokumentációja 6](#_Toc165281963)

[Kék terület 6](#_Toc165281964)

[VLAN (Virutal Local Area Network) 8](#_Toc165281965)

[PAgP (Port Aggregation Protocol) 10](#_Toc165281966)

[Feszitőfa protokoll (Spanning Tree Protocol) 11](#_Toc165281967)

[Port-Security (Portbiztonság) 12](#_Toc165281968)

[DHCP (Dynamic Host Configuration Protocol) 13](#_Toc165281969)

[DHCP-Snooping 14](#_Toc165281970)

[SSH (Secure Shell) 15](#_Toc165281971)

[Rózsaszín terület 16](#_Toc165281972)

[DHCP 16](#_Toc165281973)

[Biztonság 16](#_Toc165281974)

[Zöld terület 18](#_Toc165281975)

[Port-Security (Portbiztonság) 19](#_Toc165281976)

[DHCP 20](#_Toc165281977)

[VTP 21](#_Toc165281978)

[Lila terület 21](#_Toc165281979)

[GRE Tunnel 21](#_Toc165281980)

[IPv6 22](#_Toc165281981)

[Sárga terület 22](#_Toc165281982)

[PPP(Pont-Pon-Protokoll) 23](#_Toc165281983)

[ZPF 23](#_Toc165281984)

[AWS felhőszolgáltatás 24](#_Toc165281985)

[Piros terület 24](#_Toc165281986)

[ASA 25](#_Toc165281987)

[Szürke terület 25](#_Toc165281988)

[Mikrotik Router 25](#_Toc165281989)

[Windows PDC, AD, DNS, DHCP szerver (GUI) 27](#_Toc165281990)

[PDC(Primary Domain Controller): 27](#_Toc165281991)

[AD(Active Directory): 27](#_Toc165281992)

[DNS(Domain Name System): 28](#_Toc165281993)

[Automatikus Biztonsági Mentés 31](#_Toc165281994)

[Csoportházirendek (Group Policy-k) 31](#_Toc165281995)

[Alapértelmezett háttérkép 31](#_Toc165281996)

[Vezérlőpulthoz és egyéb PC beállítások módosításának tiltása 33](#_Toc165281997)

[Parancssor és egyéb windows alkalmazások hozzáférésének tiltása 34](#_Toc165281998)

[Cserélhető adathordozók csatlakoztatásának letiltása 35](#_Toc165281999)

[Minimális jelszóhossz beállítása és jelszó lejárati idejének megváltoztatása 36](#_Toc165282000)

[Windows BDC (Core) 37](#_Toc165282001)

[BDC(Backup Domain Controller): 37](#_Toc165282002)

[DHCP-Failover 38](#_Toc165282003)

[Linux Web, File és Print szerver (CLI) 38](#_Toc165282004)

[WEB: 39](#_Toc165282005)

[Print: 40](#_Toc165282006)

[File 41](#_Toc165282007)

[HSRP (Hot Standby Router Protocol) 41](#_Toc165282008)

[NAT 42](#_Toc165282009)

[Acl (Access Control List) 43](#_Toc165282010)

[Telehelyek között alkalmazott forgalomirányító protokoll 44](#_Toc165282011)

[OSPF 44](#_Toc165282012)

[Hálózatprogramozás 48](#_Toc165282013)

[PNET 48](#_Toc165282014)

[Netmiko 48](#_Toc165282015)

[Ábrajegyzék 49](#_Toc165282016)

# Cégleírás

**InnoTech Networks kft.**

Az InnoTech Networks kft. egy magyarországi székhelyű cég, amely hálózati megoldásokra specializálódott. Több mint 100 elégedett ügyféllel rendelkeznek Magyarországon és külföldön, akiknek a legújabb technológiákat és innovatív megoldásokat alkalmazzák a hálózati tervezés, kivitelezés és üzemeltetés területén.

**Szakértői tudás, egyedi igényekre szabva:**

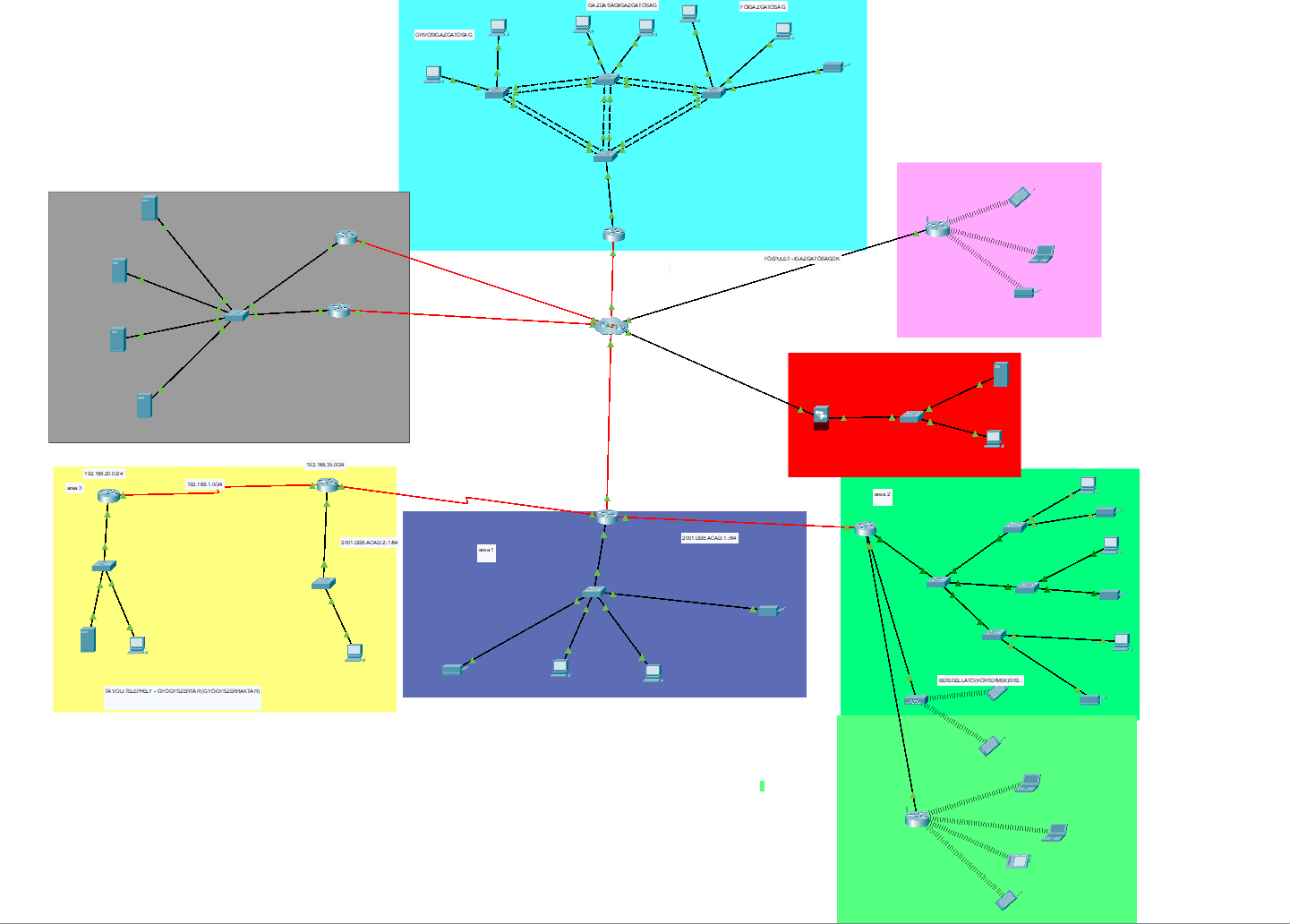
Az InnoTech Networks kft. rugalmas és hatékony megközelítéssel illeszkedik az ügyfelek egyedi igényeihez. A legújabb technológiákat alkalmazzák a hálózati infrastruktúra optimalizálására, növelve a vállalati folyamatok sebességét, stabilitását és eredményességét. Biztonságos és megbízható hálózati környezetet teremtenek a zavartalan működéshez.

**Széleskörű tapasztalat, átfogó szolgáltatások:**

Kimagasló szakértelemmel rendelkeznek a különböző iparágak hálózati igényeinek kiszolgálásában, legyen szó az egészségügyről, oktatásról, kereskedelemről vagy szolgáltatásról. Komplex hálózati projektek megvalósításában is jártasak, és folyamatos karbantartással és üzemeltetéssel biztosítják a hálózat zökkenőmentes működését.

**Az InnoTech Networks kft. kulcsfontosságú partnere lehet a vállalkozásoknak a digitális fejlődésben.**

# A hálózat dokumentációja

A kiépítendő hálózatot a Packet Tracer nevű szimulációs programban terveztük meg. A tervezetet az 1. ábrán látható:

ábra 1 - A hálózat topológiája

## Kék terület

A kék színnel jelölt terület a kórház igazgatóságának telephelye.

Ezen a telephelyen 30 fő részére kellett biztosítanunk egy zökkenőmentes hálózatot.

A kék területen az alábbi eszközöket alkalmaztuk:

* 2db 2911-es Forgalomirányító
* 4db 2960 Switch
* Szerver
* Számítógépek
* Nyomtatók

Az alábbi protokollokat alkalmaztuk a telephelyen:

* Második rétegbéli redundáns megoldások:
  + STP
    - Hurkok és szórási viharok kialakulásának meggátolásának érdekében
  + Link Aggregáció
    - Port összefogás

Forgalomirányítók:

* SSH
  + Titkosított távoli hozzáférést biztosít.

Kapcsolók (Switchek)

* Vlan Trunk Protocol
  + Kapcsolók közötti **VLAN** információ csere
* Port-security
  + Az interfészek 1 címet tanulhatnak meg maximum, ismeretlen cím esetén, eldobják a nem ismert címet, és logolják, a „sértést”
* DHCP Snooping
  + Csak ismert interfészeknek oszt címet a DHCP
* jelszó titkosítás
  + SECRET jelszavak
  + service password-encryption
* SSH
  + Titkosított távoli hozzáférést biztosít az adminnak.

### VLAN (Virutal Local Area Network)

Egy LAN-hoz a hozzáférést biztosítani normál esetben egy hozzáférési rétegbéli kapcsoló feladata. Egy második rétegbeli (Layer 2) kapcsolón virtuális helyi hálózatok (**VLAN, Virtual Local Area Network**) hozhatók létre a szórási tartományok méretének csökkentésére, harmadik rétegbéli (Layer 3) eszközhöz hasonló funkcióval. A hálózatot rendszerint eleve VLAN-ok használatával tervezik meg, ami megkönnyíti, hogy a hálózat kiszolgálja egy szervezet céljait. Az igazgatóság telephelyén vlanokat alkalmaztunk a könnyebb kezelés érdekében.

Virtuális Helyi Hálózatokat nagyon egyszerűen hozhatunk létre.

A globális konfigurációs módba lépve, a vlan <vlan\_azonosító> parancs kiadásával már létre is hoztuk az alkalmazni kívánt vlan-t, a könnyebb azonosítás érdekében pedig, a   
name <vlan\_neve> parancs adható ki. Miután mindennel megvagyunk, ezt a folyamatot minden használni kívánt switchen ki kell adnunk, hacsak nem alkalmazunk **VTP**-t a hálózatban. Ezután az adott **interface**hez hozzá kell rendelni, a megfelelő vlan-t, amit úgy tehetünk meg, hogy a portot hozzáférhető állapotba tesszük a switchport mode <access/trunk> parancs kiadásával, majd a switchport access vlan <vlan\_azonosító> paranccsal hozzá is rendeltük a kívánt vlan-t.

A **natív VLAN** egy 802.1Q trönk porthoz van hozzárendelve. A trönk portok azok a kapcsolók közötti linkek, amelyek egynél több VLAN forgalmának a továbbítását is lehetővé teszik. Egy 802.1Q trönk port a különböző VLAN-okból érkező forgalmat, valamint a nem VLAN-ból származó forgalmat egyaránt továbbítja.

A Kék színnel jelölt telephelyen öt különböző **VLANT** hoztunk létre. Hármat, hogy az igazgatóság tagjai zavartalanul végezhessék munkájukat, egy alapértelmezett (default) VLAN-t, illetve egy **NATÍV VLAN-**t, hogy a nem VLAN-ból érkező információk is továbbításra kerüljenek.

ábra 2 - show vlan brief parancs kimenetele

VTP (VLAN Trunk Protocol)

A **VLAN Trunking Protocol** (VTP) segítségével a Cisco eszközök automatikusan cserélik a VLAN konfigurációs információkat a hálózaton keresztül. Ez megkönnyíti a VLAN-ok kezelését a hálózaton, mivel a változásokat elegendő egy, az ún. **szerver** switchen elvégezni, majd ezek a változások automatikusan szétterjednek az összes VTP-t támogató eszközre.

A VTP-nek két módja van. A szerver, és a kliens. Ezt a vtp mode <server/client> parancs kiadásával állíthatjuk be.

**Szerver:** Lehetővé teszi, hogy létrehozzon, eltávolítson és módosítson VLAN-okat az egész hálózaton. Beállíthat más konfigurációs opciókat is, mint például a VTP verzió, és be- vagy kikapcsolhatja a VTP pruninget az egész VTP domain számára. A VTP szerverek hirdetik a VLAN konfigurációjukat a többi, ugyanabban a VTP domainben lévő switch felé, és szinkronizálják a VLAN konfigurációjukat a trunk linkeken érkező üzenetek alapján.

**Kliens:** Lehetővé teszi, hogy létrehozzon, megváltoztasson és töröljön VLAN-okat a helyi eszközön. A VTP kliens módban egy switch tárolja a legutóbb ismert VTP információkat.

ábra 3 - show vtp status parancs kimenetele

### PAgP (Port Aggregation Protocol)

A PAgP a Cisco saját fejlesztésű protokollja, mely az EtherChannel kapcsolatok automatikus létrehozását segíti. Használata esetén a kapcsolók PAgP-csomagokkal egyeztetnek a portok között az EtherChannel kialakításához. Ha a PAgP megfelelő Ethernet portokat talál, összefogja azokat egy EtherChannel-be, amely ezután egyedi portként vesz részt a feszítőfában.

Cégünk cisco routereket alkalmaz, ezért a PAgP-t választottuk. A PAgP csak cisco routereken működik, cserébe viszont sokkal egyszerűbb beüzemelni, illetve menedzselni.

A portösszefogás beüzemelése nagyon egyszerű. Első lépésként létrehozzuk a szükséges Port-Channeleket. Ezt az interface port-channel <csatorna\_azonosító> parancs kiadásával tehetjük meg. Ezután az adott switchen, belépünk az interface range <int,int> paranccsal az összevonni kívánt interfacekbe és a channel-group <azonosító> mode <active/passive/desirable/on> parancsot kiadva, beállítjuk, hogy milyen módon fusson a Link Aggregation. Az utolsó paraméter attól függ, hogy LACP-t, vagy PAgP-t használunk. Cégünk esetében, a desirable paramétert kellett megadni.

Fontos, hogy ezen parancsok kiadása alatt, le kell kapcsolni azon interfaceket, amelyeket éppen konfigurálunk.

ábra 4 - show etherchannel parancs kimenetele, S1\_SWITCHEN

### Feszitőfa protokoll (Spanning Tree Protocol)

A redundanciát a hálózatok terén azért alkalmazzuk, hogy növeljük a megbízhatóságot, és alternatív útvonalak álljanak rendelkezésre. Az alternatív útvonalak viszont problémához vezethetnek, ha egy-egy csomag körbe jár a redundáns útvonalakon.

Ha redundánsan kötünk össze kapcsolókat, azok automatikus tanulási és továbbítási működése miatt, természetes módon alakulnak ki a hurkok. Ehhez hozzájárul az is, hogy a második rétegben működő kereteknek nincs lejárati ideje, azaz Time To Live számlálójuk.

A redundáns kapcsolatok még veszélyesebbek szórásos üzenetek esetén. Ha a szórásos üzenetek továbbítása során a teljes sávszélességet elfoglalják a keretek, akkor szórási viharról beszélünk, angolul broadcast storm. Az ilyen viharok kialakulásához néhány másodperc is elég.

A feszítőfa protokoll biztosítja, hogy elkerüljük a hurkokat. A protokoll két járható port közül az egyiket mindig zárva tartja, tartaléknak. Az így lezárt porton csak akkor enged forgalmat, ha az elsődleges útvonal meghibásodik.

A lezárt portokat az STP saját céljaira használja, úgynevezett BPDU-keretek küldésére. A BPDU, a Bridge Protocol Data Unit, rövidítése, magyarul hídprotokoll adategységnek fordítható. Egy BPDU üzenet portokról, címekről, prioritásokról és költségekről tartalmaz információkat, amelyek biztosítják a hurkok felismerését.

A PortFast a Cisco PVST+ környezetben használt funkciója. A PortFast beállítás a kapcsolóportot lezárt állapotból azonnal továbbító állapotba váltja, amellyel megkerüli a szokásos figyelő és a tanuló állapotokat. A PortFast arra szolgál, hogy a hozzáférési portok eszközei azonnal elérjék a hálózatot, ne kelljen megvárniuk konvergálását minden egyes VLAN-on. Hozzáférési porton az egyetlen munkaállomást vagy szervert csatlakoztató portot értjük.

Szabályos PortFast beállítások esetén sosem érkezhetnek BPDU-k, mert ez azt jelentené, hogy a portra másik híd vagy kapcsoló csatlakozik, ami feszítőfa hurokhoz vezethetne.

A Rapid Per-VLAN Spanning Tree Plus (PVST+)

biztosítja a kapcsolat gyors helyreállítását egy eszköz, egy eszközport vagy egy LAN meghibásodása után. Emellett gyors konvergenciát biztosít a szélső portok, az új gyökérportok és a pont-pont kapcsolatokon keresztül csatlakoztatott portok számára.

A Rapid PVST+ minden egyes virtuális helyi hálózathoz (VLAN) külön feszítőfa példányt futtat. Ez lehetővé teszi a port számára, hogy egyes VLAN-okat továbbítson, miközben más VLAN-okat blokkol. A PVST+ biztosítja a VLAN-ok terheléselosztását több porton, ami a hálózati erőforrások optimális kihasználását eredményezi.

A gyors PVST+ segítségével a konvergencia gyorsan történik. Alapértelmezés szerint a feszítőfa protokollban minden kijelölt port 2 másodpercenként küld egy BPDU-t (Bridge Protocol Data Unit). A topológiában egy kijelölt porton, ha három egymást követő alkalommal kimaradnak a hello üzenetek, vagy ha lejár a maximális életkor, a port azonnal törli az összes protokollinformációt a táblából. Egy port úgy tekinti, hogy elveszíti a kapcsolatot a közvetlen szomszédos kijelölt porttal, ha három BPDU-t kihagy, vagy ha a maximális kor lejár. A protokollinformációk ilyen gyors öregedése lehetővé teszi a hibák gyors észlelését.

### Port-Security (Port biztonság)

A port biztonság megvédi a hálózatot az ismeretlen **MAC**-címek elárasztásától azáltal, hogy korlátozza a portonként megtanult **MAC**-címek számát.

A kapcsolókhoz maximum 1 cím tartozhat, melyeket sticky, azaz ragadós módszerrel rendeltük hozzá. Sértés esetén pedig a „restrict” állapot lép életbe,

A port biztonságra a későbbiekben bővebben kitérünk.

### DHCP (Dynamic Host Configuration Protocol)

A **DHCP**, vagyis a Dynamic Host Configuration Protocol, egy olyan hálózati protokoll, amely automatikusan biztosítja a hálózati végpontok (kliensek) számára a szükséges IP címeket és egyéb hálózati beállításokat anélkül, hogy manuális beavatkozásra lenne szükség.

A DHCP alkalmazásához szükségünk van egy DHCP-Poolra, amelyet az   
ip dhcp pool <pool\_név> parancs kiadásával hozhatunk létre, a globális konfigurációs szinten. Ha megvan a pool, meg kell adnunk, hogy mely hálózat számára osszon IP címeket a szerver/router, illetve a hálózat alapértelmezett átjáróját. Ehhez a   
network <cím\_tartomány> <alhálózati\_maszk> illetve a   
default-router <alapértelmezett\_átjáró> parancsot szükséges kiadni.

Vannak olyan esetek, amikor nem szeretnénk, hogy bizonyos IP címek kiosztásra kerüljenek, mint például a forgalomirányító IP címe, vagy esetleg egy területen alkalmazott szerveré. Ehhez ki kell adnunk globális konfigurációs szinten, az   
ip dhcp excluded-address <kezdeti\_IP-cím> <vég\_IP-cím>  
A fontosabb parancsok ezzel meg is vannak.

Ha szükséges, a a dns-server <DNS\_szerver\_cím> parancsot kiadva, beállíthatjuk, hogy milyen **DNS** címet adjon a DHCP a klienseknek. A KÉK területen, az igazgatóság tagjait rendeltük hozzá az FTP-hez, hogy a fontosabb iratok, adatokat, együttesen tudják kezelni, egy közös tárhelyen.

Ha mindennel készen vagyunk, a privilegizált EXEC szinten a   
show ip dhcp pool kiadásával megtekinthetjük, az aktuális beállításokat.

ábra 5 - A kék területen routerén alkalmazott DHCP beállításai

### DHCP-Snooping

A DHCP-Snooping egy DHCP biztonsági funkció, amely a nem megbízható DHCP-üzenetek szűrésével, valamint a DHCP-Snooping kötési táblázat létrehozásával és karbantartásával nyújt biztonságot. A nem megbízható üzenet olyan üzenet, amely a hálózaton vagy tűzfalon kívülről érkezik, és a hálózaton belül forgalmi támadásokat okozhat.

A DHCP-Snooping kötési tábla tartalmazza a MAC-címet, az IP-címet, a bérleti időt, a kötés típusát, a VLAN-számot és a kapcsoló helyi, nem megbízható interfészeinek megfelelő interfészinformációkat; a megbízható interfésszel összekapcsolt állomáshelyekre vonatkozó információkat nem tartalmazza. A nem megbízható interfész olyan interfész, amely úgy van konfigurálva, hogy a hálózaton vagy tűzfalon kívülről érkező üzeneteket fogadjon. A megbízható interfész olyan interfész, amely úgy van konfigurálva, hogy csak a hálózaton belülről érkező üzeneteket fogadjon.

A DHCP-Snooping tűzfalként működik a nem megbízható állomás és a DHCP-kiszolgálók között. Emellett lehetőséget ad a végfelhasználóhoz csatlakozó nem megbízható és a DHCP-kiszolgálóhoz vagy egy másik kapcsolóhoz csatlakozó megbízható interfészek megkülönböztetésére.

### SSH (Secure Shell)

Az SSH olyan hálózati protokoll, mely segítségével titkosított hálózati kapcsolattal jelentkezhetünk be egy távoli gépre. Az SSH gyakorlatilag lehetővé teszi a biztonságos kommunikációt két távoli számítógép között még egy nem biztonságos hálózaton keresztül is. Ugyanakkor nem csak távoli elérésre alkalmas, hanem fájlok másolására, titkosított csatornák létrehozására (stunnel) és parancsok kiadására is a távoli gépen.

## Rózsaszín terület

A rózsaszínnel jelölt terület, az otthoni dolgozó telephelye. Ő a rendszer fenntartásáért, monitorozásáért. Probléma esetén, SSH segítségével be tud lépni a hálózati eszközökbe, helyreállítani a problémát.

A rózsaszín területen az alábbi eszközök, protokollok megtalálhatóak:

* WRT300N Vezeték nélküli forgalomirányító
  + DHCP
  + Jelszótitkosítás
* Laptop
* Nyomtató
* Okostelefon

### DHCP

A forgalomirányító DHCP-vel oszt IP címet az otthoni dolgozónak.

ábra 6 - Otthoni dolgozó DHCP konfiguráció

### Biztonság

Az otthoni dolgozó telephelyén(otthonában) vezeték nélküli hálózat, egy WiFi üzemel.

A hálózat **OTTHON\_WIFI** névvel lett ellátva. A megfelelő biztonság érdekében WPA2-PSK biztonsági protokoll üzemel, ugyanis elődei a WEP és a WPA könnyedén sebezhető.

A **WPA2-PSK** a Wi-Fi Protected Access 2 - Pre-Shared Key rövidítése. Ez egy olyan biztonsági protokoll, amelyet vezeték nélküli hálózatok, különösen otthoni és kis irodai hálózatok védelmére használnak.

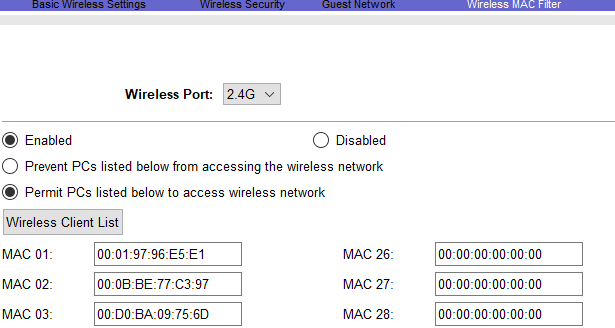
A **WPA2-PSK** biztonságos kommunikációt biztosít a vezeték nélküli hálózathoz csatlakoztatott eszközök között. Megfelelő biztonsági intézkedések nélkül illetéktelenek hozzáférhetnek a hálózathoz, és potenciálisan ellophatják az érzékeny információkat. A WPA2-PSK az adatok titkosításával és a hozzáféréshez szükséges egyedi jelszóval segít megelőzni ezt.

Emellett fontos a WPA2-PSK titkosítási formátumának megadása. A területen alkalmazott titkosítási forma az **AES (Advanced Encryption Standard)**, amely a **TKIP** újabb formátumát használja, és erősebb titkosítással rendelkezik.

#### MAC-Címszűrés

A legtöbb szélessávú router és egyéb vezeték nélküli hozzáférési pont tartalmaz egy opcionális funkciót, az úgynevezett MAC-címszűrést vagy hardveres címszűrést. Ez javítja a biztonságot azáltal, hogy korlátozza a hálózathoz csatlakozó eszközöket.

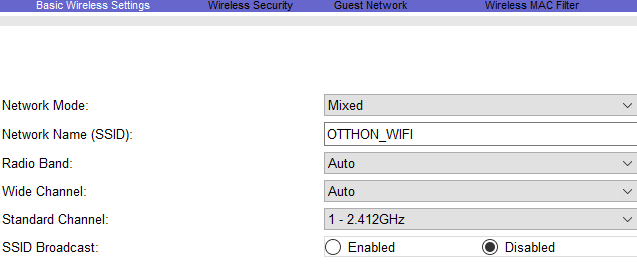
Az otthoni dolgozó telephelyén fontos, hogy csakis a saját eszközei férjenek hozzá a hálózathoz, emiatt szükséges volt a szűrés alkalmazása.



ábra 7 - Mac-Címszűrés

#### SSID Broadcast

Az SSID Broadcast, a vezeték nélküli hálózatok/hozzáférési pontok folyamatos csomagküldése, mely a hálózatok elérhetőségét jelzi. Ezen funkckió kikapcsolása esetén csakis az SSID, azaz a hálózat nevének tudatában lehet csatlakozni a hálózatra.



ábra 8 - SSID Broadcast

## Zöld terület

A zöld területen, a kórház főépületének topológiája látható. A területen 10 sebész, 4 urológus, és 4 bőrgyógyász dolgozik, illetve 50 vendég számára, vezeték nélküli hálózatot biztosít a váróteremben. Emellett van egy betegellátó, ami további 70 főnek képes vezeték nélküli kapcsolatot biztosítani

A területen az alábbi eszközöket alkalmaztuk:

* 2911-as forgalomirányító
* WRT300N Vezeték nélküli forgalomirányító
* 4db 2960-as Switch
* Access Point
* Számítógépek
* Nyomatók

A telephelyen alkalmazott protokollok:

Forgalomirányítók:

* DHCP:
  + Az Access Point és a Vezeték nélküli forgalomirányító DHCP segítségével oszt IP-Címet a betegek számára.

Kapcsolók (Switchek):

* VTP:
  + Vlanok közötti információ csere
* Port-Security:
  + Az interfészek az orvosoknak megfelelő számú címet tanulhatnak meg maximum, ismeretlen cím esetén, eldobják a nem ismert címet, és logolják, a „sértést”

### Port-Security (Portbiztonság)

A portbiztonság megvédi a hálózatot az ismeretlen **MAC**-címek elárasztásától azáltal, hogy korlátozza a portonként megtanult **MAC**-címek számát.

Az adott interfészen 3 beállítást végezhetünk el. Megadhatjunk, hogy miként ismerje fel a hozzá csatlakozó eszköz/eszközök **MAC**-címét, emellett megadhatjuk, a maximum **MAC-**címek számát, illetve, hogy sértés esetén, hogy reagáljon a kapcsoló.

A **MAC**-cím beállítását kétféleképpen tehetjük meg. Megathatjuk statikusan, vagy bekapcsolhatjuk a „sticky” nevű funckiót, amivel felismeri és eltárolja, az akkor hozzá csatlakozó eszköz **MAC**-címét. Cégünk az utóbbi beállítást alkalmazta a hálózaton.

Sértés esetén, három funkció közül válaszhatunk.

* protect
  + A switch eldobja a keretet.
* restrict
  + Amellett, hogy eldobja a keretet, naplózza az eszköz **MAC-**címét, illetve, a behatolási kísérletek számát.
* shutdown
  + Tulajdonságai alapján megegyezik az előzővel, viszont, sértés esetén a portot disabled állapotba helyezi, amit csak manuálisan tud visszakapcsolni a rendszergazda.

A telephelyen a restrict állapotot alkalmaztuk, ugyanis tulajdonságait tekintve ez a legbiztonságosabb, illetve, nem szükséges manuális beavatkozás, hiszen a folyamat megy tovább, nem kapcsol le a sértett port.

### DHCP

A zöld területen két forgalomirányító oszt **DHCP-vel** IP címet.  
A FOEPULET\_R forgalomirányító az orvosok számára, illetve a várakozó betegek számára oszt IP-címet egy Acces Point segítségével.

ábra 9 - Zöld terület DHCP

Az fentebbi képen, a forgalomirányítón alkalmazott DHCP konfigurációi láthatók

Emellett, a vezeték nélküli forgalomirányító is rendelkezik aktív DHCP konfigurációval, mely a kórtermekben lévő, de maximum 70 beteg számára tud kapcsolatot biztosítani.



ábra 10 - BETEG\_W DHCP

### VTP

A zöld területen alkalmaztunk VTP, ugyanis így könnyedén, egységesen tudjuk konfigruálni a kapcsolókat

A telephelyen négy VLAN-t hoztunk létre, a 10-es VLAN-T a **UROLÓGUSOK** számára, a 20-as VLAN-t a **BŐRGYÓGYÁSZOK** számára, és a 30-as VLAN-t a **SEBÉSZEK** számára.  
Emellett megtalálható a 99-es VLAN, ami a korábban már említett **NATÍV** szerepet tölti be.

ábra 11 - Zöld terület VLAN

## Lila terület

A lila színnel jelzett területen, a kórház laborja látható. Ide érkeznek a kivizsgálásra kerülő humán minták.

Területen alkalmazott eszközök:

* 2911-es forgalomirányító
* 2960-as Switch
* Számítógépek
* Nyomtatók

A telephelyen alkalmazott protokollok:

Forgalomirányító:

* OSPF (IPv6 & IPv4)
* GRE

### GRE Tunnel

A GRE Alagút egy olyan virtuális pont-pont kapcsolat, amely fizikailag nem létezik, de a forgalomirányítás számára egy létező útvonalat biztosít a (szoftveres, virtuális) interfészek összekapcsolásával. A LABOR területén fontos volt, a GRE alagút alkalmazása, hiszen a **LABOR**, ipv6-os címekkel dolgozik. Alapvető esetben, az ipv6-os címmel rendelkező forgalomirányító, nem tud kommunikálni IPv4-es címekkel dolgozó forgalomirányítóval. Emellett fontos azon szempontból is, hogy az ISP, azaz a szolgáltató forgalomirányítója nem támogat IPv6-os címeket.

### IPv6

IPv6-os címeket (Internet Protocol version 6) az ipv4-es címek korlátozottsága miatt hozták létre. Cégünk a külön kérésre Ipv6-os címeket alkalmazott a lila és sárga területen. Az ipv6-os címek 128 bites hexadecimális IP címek, így nagyobb címtartománnyal rendelkezik, mint az IPv4 32 bites címei. Ez segíti a skálázhatóságot és a biztonságot a hálózaton belül. Az ipv6 automatikus címzést is kínál, ami megkönnyíti az eszközök csatlakoztatását és konfigurálását. Az ipv6 több típusú címet támogat: Unicast azaz a hagyományos címek, Multicast azaz a csoportos címeket és Anycast amelyek az irányított címek.

## Sárga terület

A területen a kórház gyógyszertára és annak raktára látható. Innen kerülnek továbbításra a zöld terület által berendelt gyógyszerek.

Területen alkalmazott eszközök:

* 2db 2911-es forgalomirányító
* 2db 2960-as Switch
* Számítógépek
* Felhőszolgáltatás Adatbázis

A telephelyen alkalmazott protokollok:

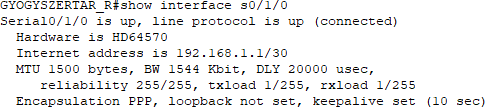
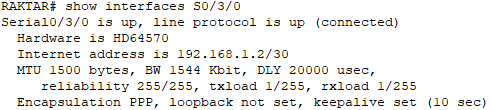
Forgalomirányító:

* PPP
* ZPF tűzfal
* OSPF (IPv6 & IPv4)

### PPP(Pont-Pont-Protokoll)

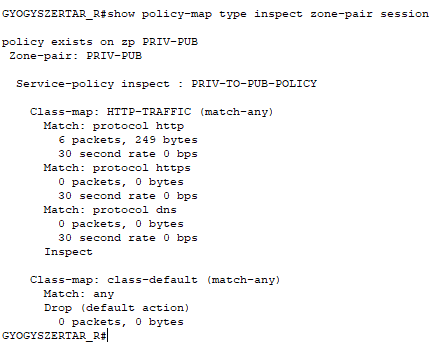
A **Pont-Pont protokoll** (PPP) egy magas szintű adatkapcsolati protokoll, amely kétpontos vonalakhoz használható. A PPP lehetővé teszi a hibajelzést, többféle protokoll támogatását, dinamikus IP-cím hozzárendelést és hitelesítést.

A PPP kétféle hitelesítési módszert használ. Ez a két hitelesítési módszer a **PAP** és a **CHAP**.

****  
 A PAP hitelesítés létrejötte után nincs szükség az újbóli azonosításra. Ezáltal a hálózat sebezhetővé válik a támadásokkal szemben. Az egyszeri hitelesítést végző PAP protokollal ellentétben a CHAP ismétlődő kihívásokat intézve ellenőrzi, hogy a távoli állomás valóban érvényes jelszót ismer-e. Cégünk, ezen okból kifolyólag a CHAP hitelesítést alkalmazta a **RAKTÁR** és a **GYÓGYSZERTÁR** között.

ábra 12 - RAKTAR\_R és GYOGYSZERTAR\_R PPP állapota

### ZPF

A Cisco Zone-Based Policy Firewall (ZPF) egy hálózati biztonsági megoldás, amely a hálózatot különböző biztonsági zónákra osztja. A ZPF szabályokat határoz meg a zónák közötti forgalomra, így védve a hálózatot a jogosulatlan hozzáféréstől, támadásoktól és behatolásoktól. A ZPF előnyei közé tartozik a rugalmasság és az erős biztonság. Azonban hátrányai is lehetnek, mint a nem hatékony skálázhatóság nagy hálózatok esetén. Cégünk arra használta a ZPF-et hogy csak a HTTP és HTTPS csomagokat tudjanak kiküldeni a hálózatból.

ábra 13 - ZPF Policy Map

### AWS felhőszolgáltatás

A korház cégünket külön megkérte, hogy implementáljunk egy adatbázist a gyógyszertár raktárnak. Cégünk erre használta az AWS-t, ami az amazon felhőszolgáltatása. A felhőben fut egy debian linux web szerver és azon belül egy MYSQL szerver. A szerverre telepítettünk egy Joomla felületet a könnyebb átláthatóság érdekében. A szervert a dynu.com dns szolgáltatás használatával kapta meg a szaszkh.ddnsfree.com domain címet. A MYSQL szerver információt tartalmaz a gyógyszerek nevéről, fajtájáról és darabszámáról így a dolgozók számára könnyebben látható, hogy mely gyógyszer hiánycikk. A képen látható az adatbázis „Gyogyszerek” táblája

## 

ábra 14 - AWS adatbázis

## Piros terület

A piros terület, egy ún. irattár.

Ezen a területen tárolják a kórház/páciensek bizalmas, megőrzendő adatait. Az adatok egy adatbázis szerveren kerülnek eltárolásra. Fontos, hogy ezek a bizalmas információk ne kerüljenek ki a nyilvánosság részére. Erre a célra, egy ASA-t helyeztünk az ISP, és a forgalomirányító közé.

### ASA

A Cisco ASA, az **Adaptive Security Appliance** rövidítése. Ezek az eszközök egységes fenyegetéskezelési megoldásként működnek, egyetlen készülékben több hálózati biztonsági funkciót egyesítve.

Egyszerűbben fogalmazva, a Cisco ASA egy többfunkciós biztonságiőrként működik a hálózat számára. Végrehajtja a biztonsági irányelveket, és felügyeli a bejövő és kimenő forgalmat, megvédi a hálózatot az illetéktelen hozzáféréstől és a rosszindulatú szoftverektől.

Az ASA működéséhez elengedhetetlen a feltételkészlet (class-map), és annak megadása, hogy mit tegyen az ASA a feltétellel (policy-map).

A feltételkészletnek cégünk az alapértelmezett csomagvizsgálatot adta meg, mely vizsgál egyaránt ftp-t, tftp-t, icmp-t, http-t, és még sok mást.

Ezen információk megadása után, a létrehozott készletet, hozzárendeljük egy ún. policy-map-hez, melyben pontosítjuk, hogy a megadott készletből pontosan mely csomagokat vizsgálja.

# Szürke terület

A szürke terület egy szerverszoba, ahol 4db szerver található, amik külön feladatokat látnak el a hálózatunkon. Ezen felül használtunk HSRP-t is a területen.

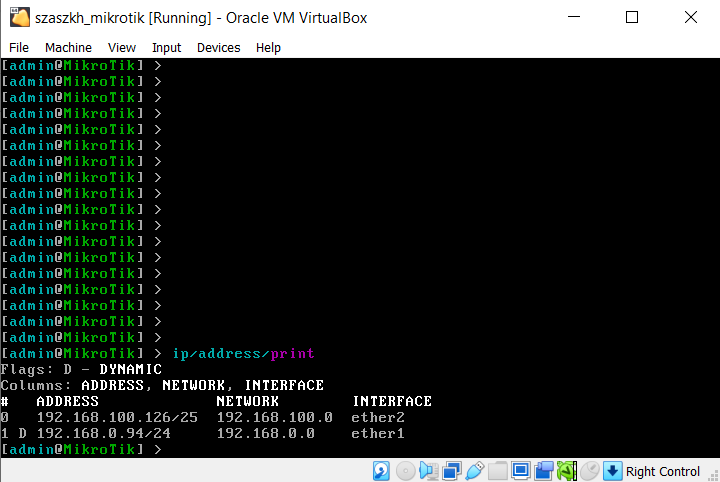
Szerverek:

* Windows PDC, AD, DNS szerver (GUI)
* Windows BDC (Core)
* Linux Web és Print szerver (CLI)

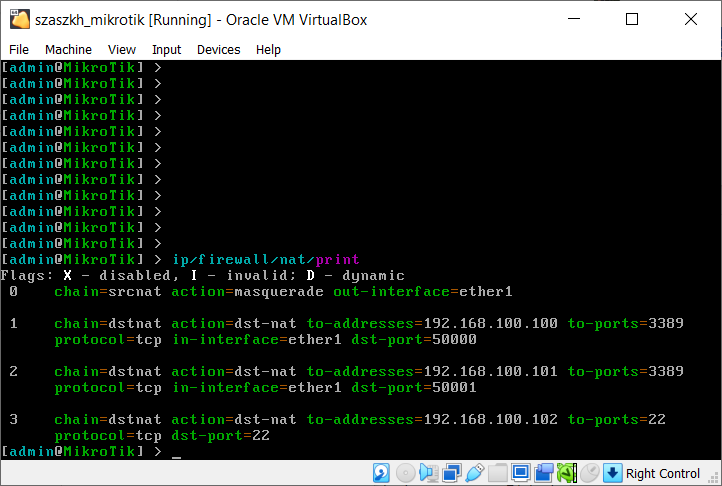
### Mikrotik Router

A szerver környezet szimulációs megvalósításához, egy ún. Mikrotik RouterOS-t alkalmaztunk, mely egy virtuális router szoftverként fut, és lehetővé teszi a hálózati funkciók tesztelését anélkül, hogy fizikai hardvert kellene használnunk, a tesztelés során.

A forgalomirányító, a valós környezet szerint oszt IP címet a hálózatnak

Emellett szükséges volt tűzfalbeállításokat elvégezni a routeren, annak érdekében, hogy a szervereket, a Putty nevezetű szoftver segítségével virtuális környezeten kívül is kezelni tudjuk, ami lényegesen megkönnyíti a konfigurálást.

ábra 15 - Mikrotik Router IP konfiguráció



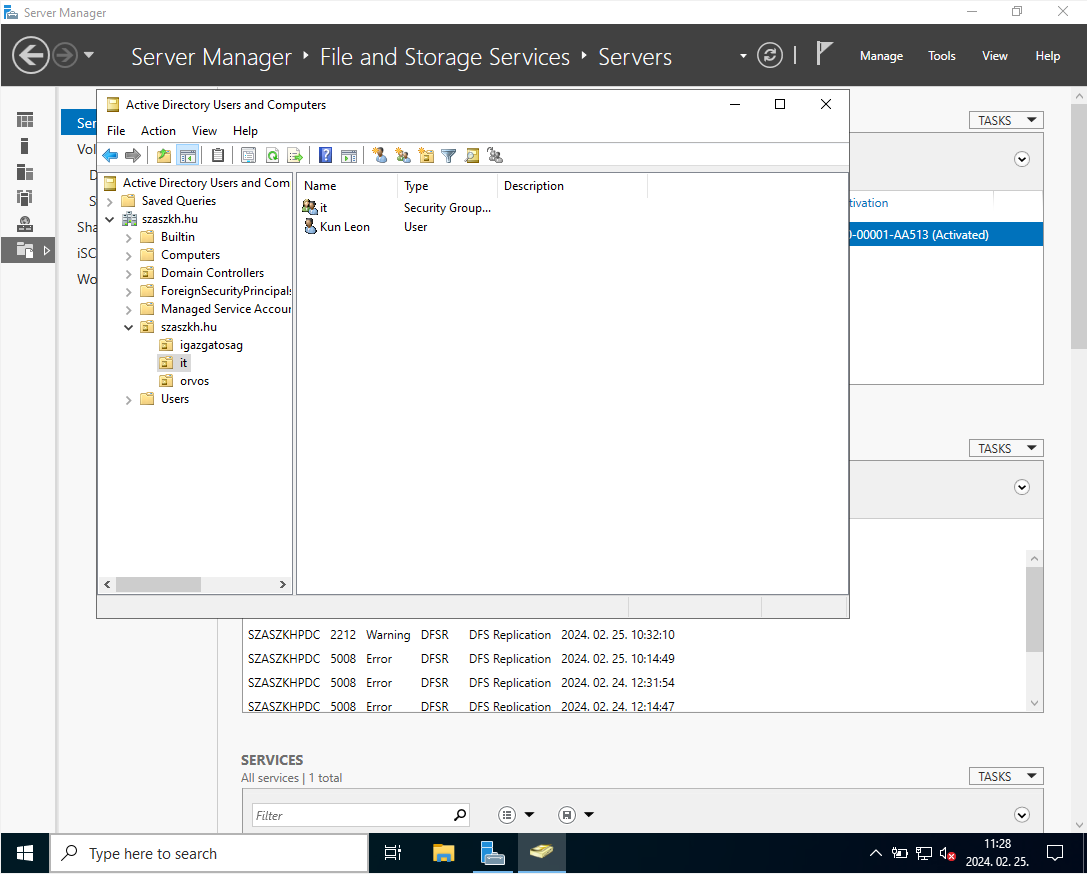
ábra 16 - Mikrotik Router tűzfalbeállítások

A fenti képen látható, hogy a .100- és a .101 végződésű hálózat, elérhető távoli asztali kapcsolattal, illetve a .102-es linux alapú szerver, konfigurálható SSH segítségével, a 22-es porton.

## Windows PDC, AD, DNS, DHCP szerver (GUI)

Ezen a szerveren Windows 2022 server GUI operációs rendszer van telepítve. 4 főbb szolgáltatást használtunk a PDC, AD és DNS és DHCP.

PDC(Primary Domain Controller):elsődleges tartományvezérlő, a Windows NT környezetben egy olyan szerver, ami a Windows tartományon belül autentikációs és autorizációs szolgáltatásokat nyújt. Minden tartományban egy PDC lehet csak a többi az BDC(Backup Domain Controller) lehet.

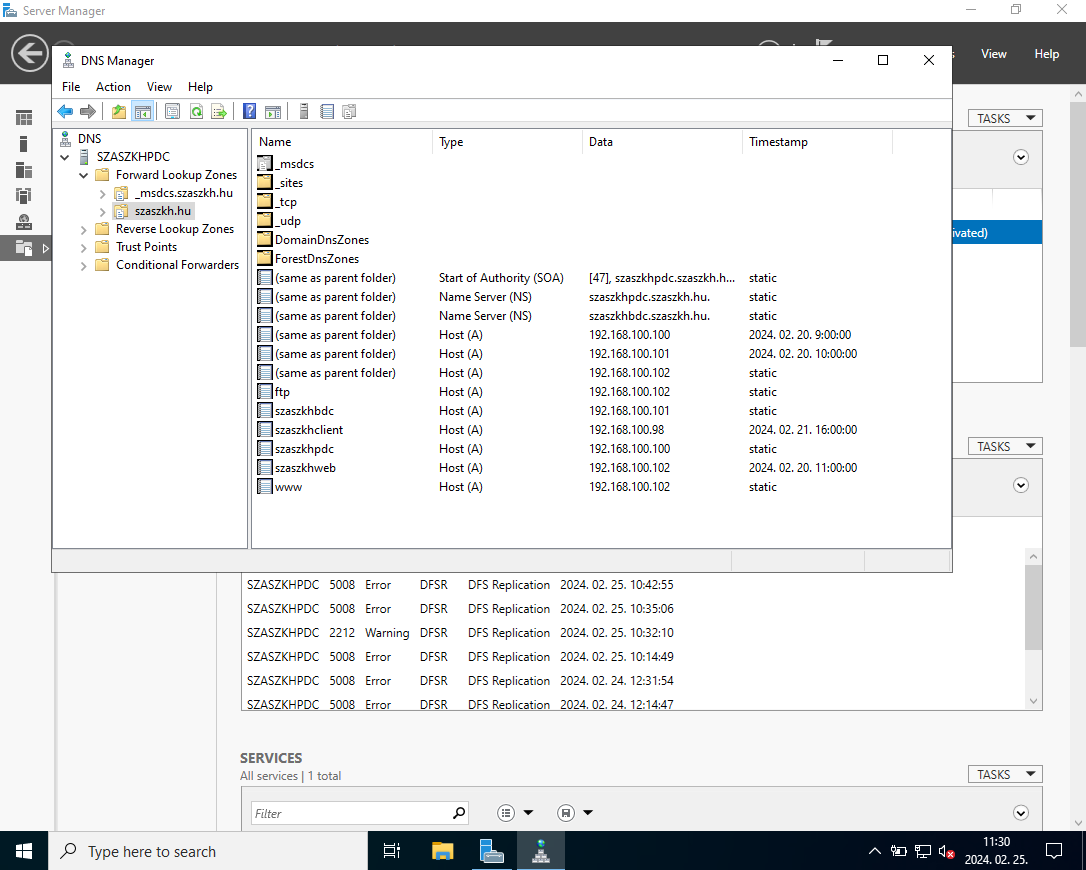
AD(Active Directory): Microsoft által fejlesztett könyvtárszolgáltatás, amely lehetővé teszi a hálózati erőforrások (például felhasználói fiókok, számítógépek, nyomtatók stb.) kezelését és szervezését. Ez elősegíti a felhasználók moderálástát a hálózaton. Az AD-ban különböző objektumokat lehet létrehozni amik lehetnek felhasználók, számítógépek, nyomtatók. Ezen objektumok csoportosításához szervezeti egységeket (Organizational Units) használunk. Cégünk **3** db szervezeti egységet hozott létre a felhasználók számára. ****

ábra 17 - Win Server AD szervezeti egységek

Található egy szervezeti egység az orvosoknak, a rendszergazdágnak, melyhez cégünk is hozzáfér, illetve az igazgatósági tagoknak

DNS(Domain Name System): A legfontosabb funkciója, hogy az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető numerikus azonosítókká „fordítja le”. Ez lehetővé teszi, hogy könnyedén elérjük a különböző weboldalakat és szolgáltatásokat az interneten**.** A DNS-el kapcsolatban fontos megemlíteni a Forward, illetve a Reverse Lookup Zone-t**.**

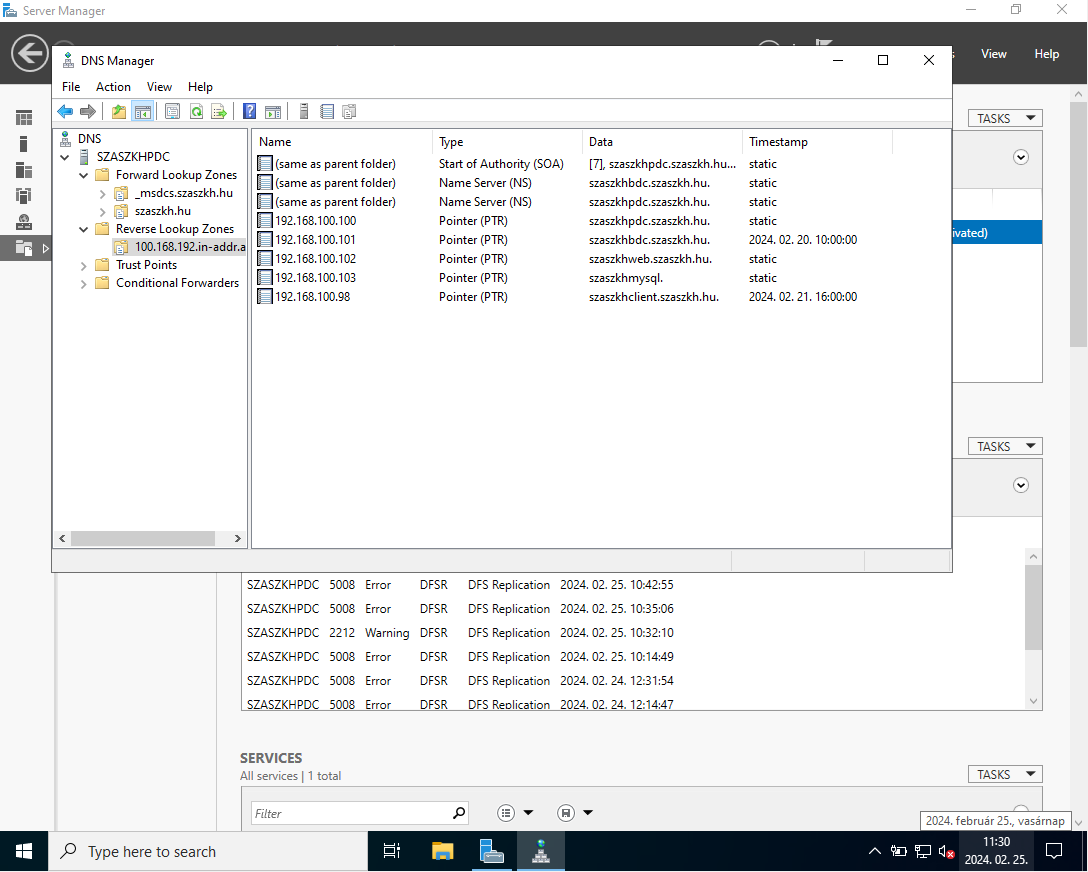
A **Forward Lookup Zone** egy olyan zóna, mely a domain neveket fordítja IP-címekre.



ábra 18 - Win Server PDC Forward Lookup Zones

A fenti példán látható, hogy a „**szaszkhweb”** domain nevet, a „**192.168.100.102**”-es címre fordítja.

A **Reverse Lookup Zone**, szintén, egy DNS Zóna, mely az IP-címeket fordítja hosztnevekre

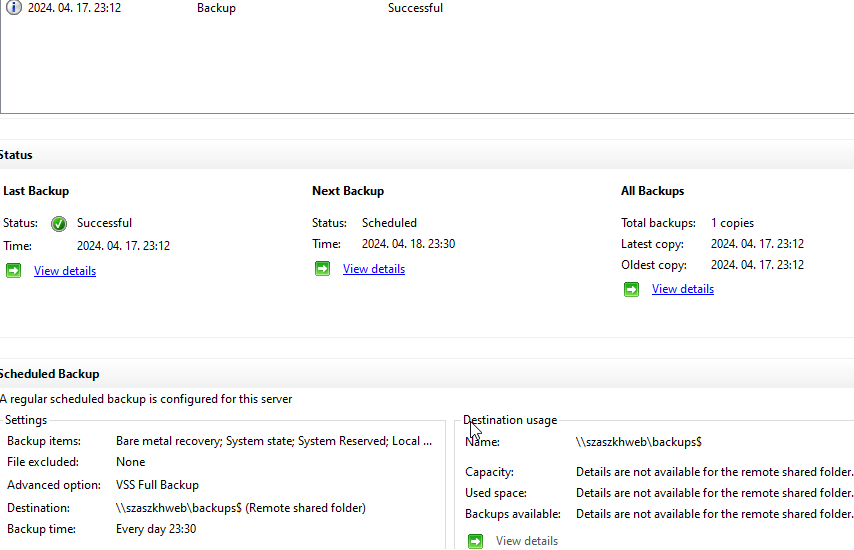


ábra 19 - Win Server PDC Reverse Lookup Zones

Itt látható, hogy a „**192.168.100.102**”-es címet, a DNS lefordítja „**szaszkhweb.szaszkh.hu”** hosztnévre.

### Automatikus Biztonsági Mentés

Az automatikus biztonsági mentés egy olyan folyamat, amely automatikusan ment másolatokat a PDC szerver adatairól, jelen esetben a Linux alapú fájlszerverre. A PDC szerver minden nap végén készít egy mentést, a teljes Szerverről. Ez azért fontos, ugyanis, ha bármilyen behatás (áramkimaradás, hardverhibák) következtében elvesznek a szerver adatai, könnyedén visszaállíthatjuk azokat.



ábra 20 - Automatizált Mentés

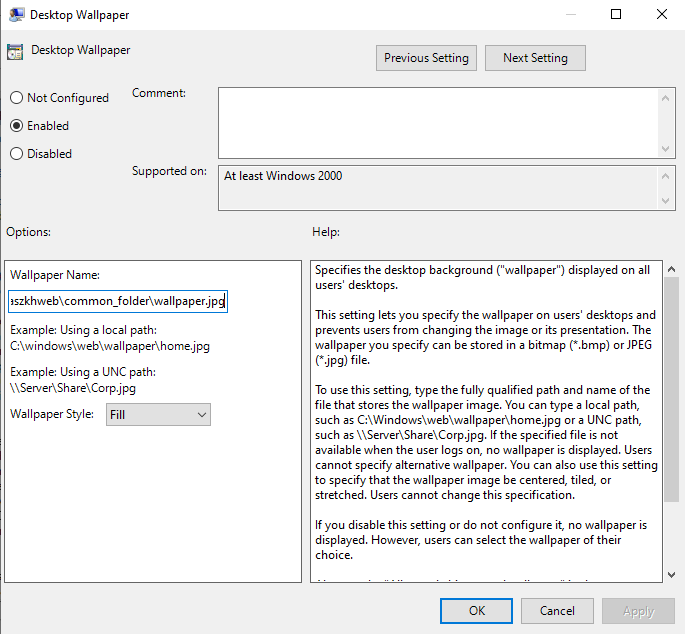
Mint látható, a biztonsági mentést a webszerver rejtett **backup$** mappájába mentette, melyről a rendszergazda könnyedén visszaállíthatja a rendszert.

### Csoportházirendek (Group Policy-k)

Annak érdekében, hogy a céget belülről sem érhesse támadás, csoportházirendeket kell létrehozni. Ezek a csoportházirendek tiltanak/engedélyeznek bizonyos funkciókat a felhasználói kliensgépeken.

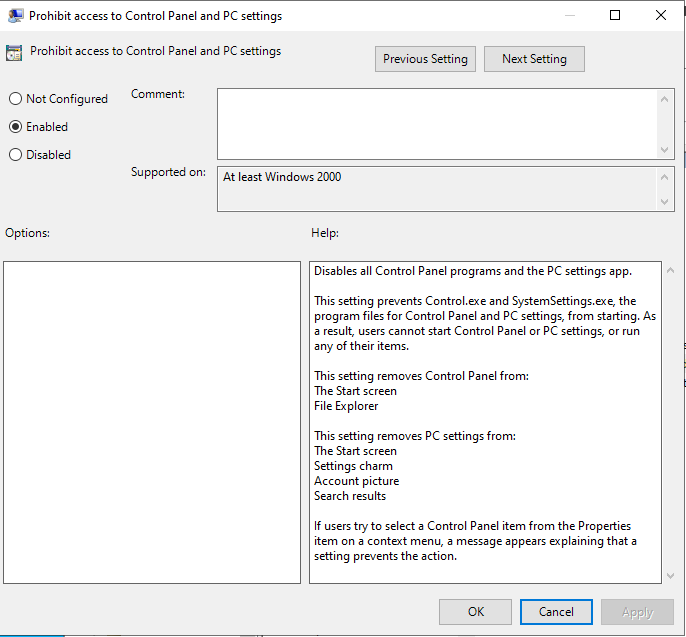
### Alapértelmezett háttérkép

A megrendelő kérésére, minden kliensgépnek egységes megjelenést állítottunk be.

Erre a feladatra a lentebb látható Csoportházirend alkalmazására volt szükség, mely a fileszerveren tárolt háttérképet automatikusan beállítja.

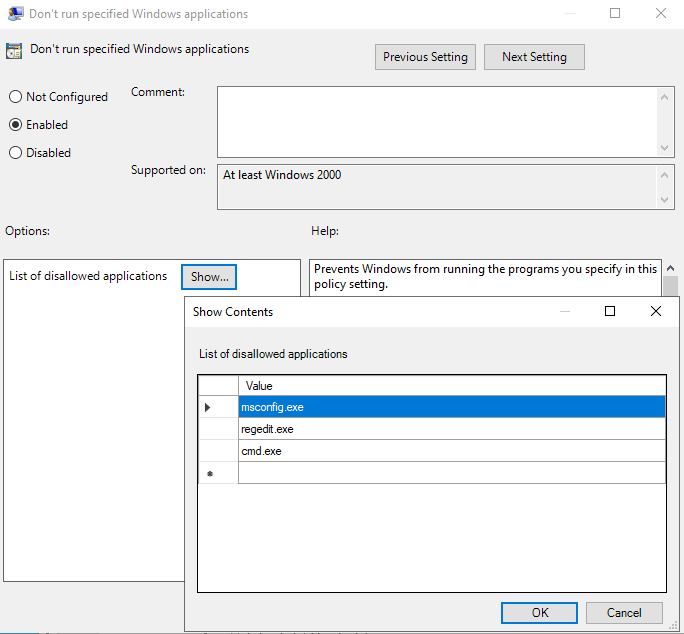
ábra 21 - Alapértelmezett háttérkép

### Vezérlőpulthoz és egyéb PC beállítások módosításának tiltása

Fontos, hogy a felhasználó ne férjen hozzá a kliensgép módosításaihoz, ugyanis bizonyos beállítások módosítása kárt okozhat a rendszerben.

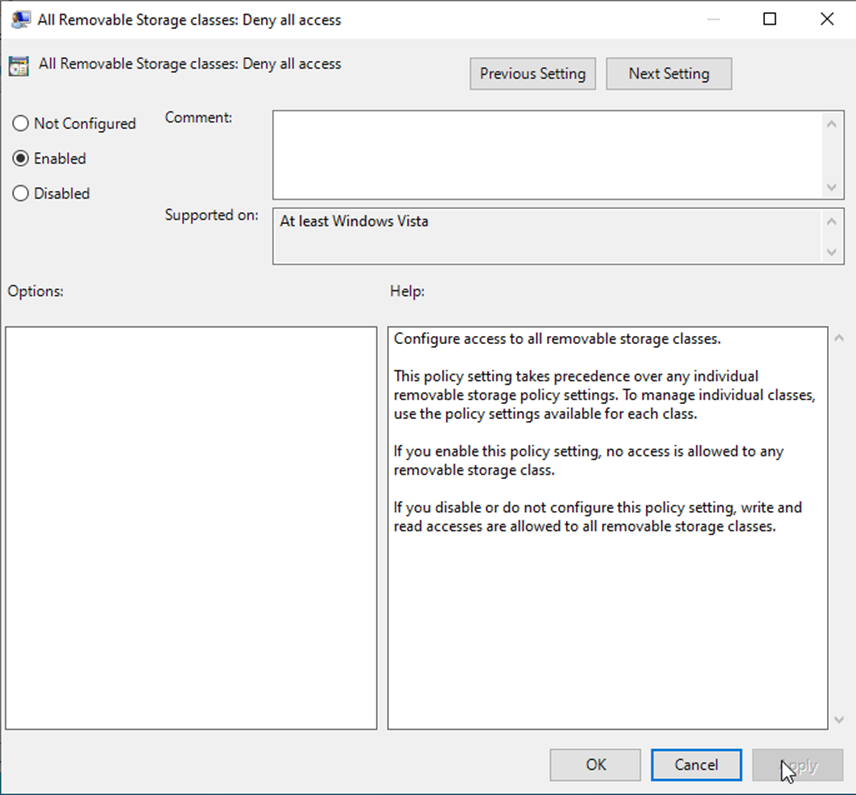
ábra 22 - Vezérlőpult letiltása

### Parancssor és egyéb windows alkalmazások hozzáférésének tiltása

A felhasználó, parancssoron/egyéb alkalmazásokon keresztül, hatalmas károkat tud okozni a hálózatban/rendszerben, ezért fontos, hogy a dolgozók ne férjenek hozzá ezekhez az alkalmazásokhoz.

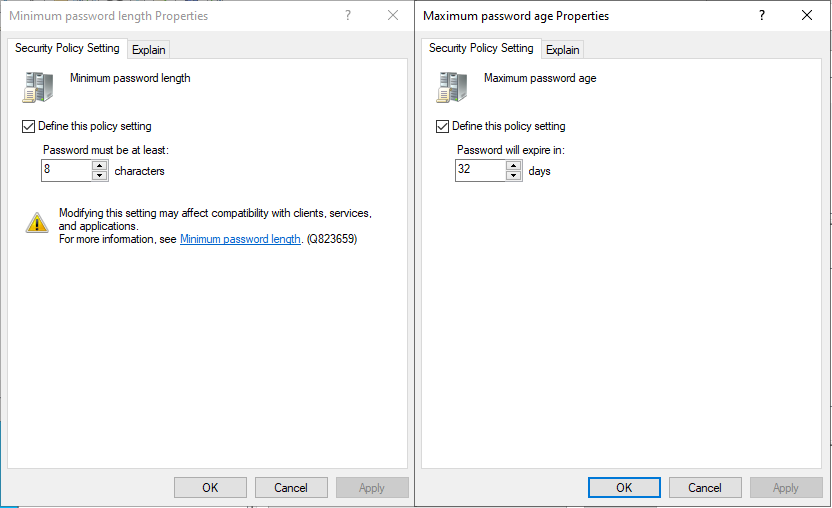
ábra 23 - Alkalmazások elérésének tiltása

### Cserélhető adathordozók csatlakoztatásának letiltása

Biztonságtechnikai okokból az adathordozók csatlakoztatása letiltásra került, így elkerülhető az adatszivárogtatás, illetve a vírusok feltelepítése.

ábra 24 - Cserélhető adathordozók tiltása

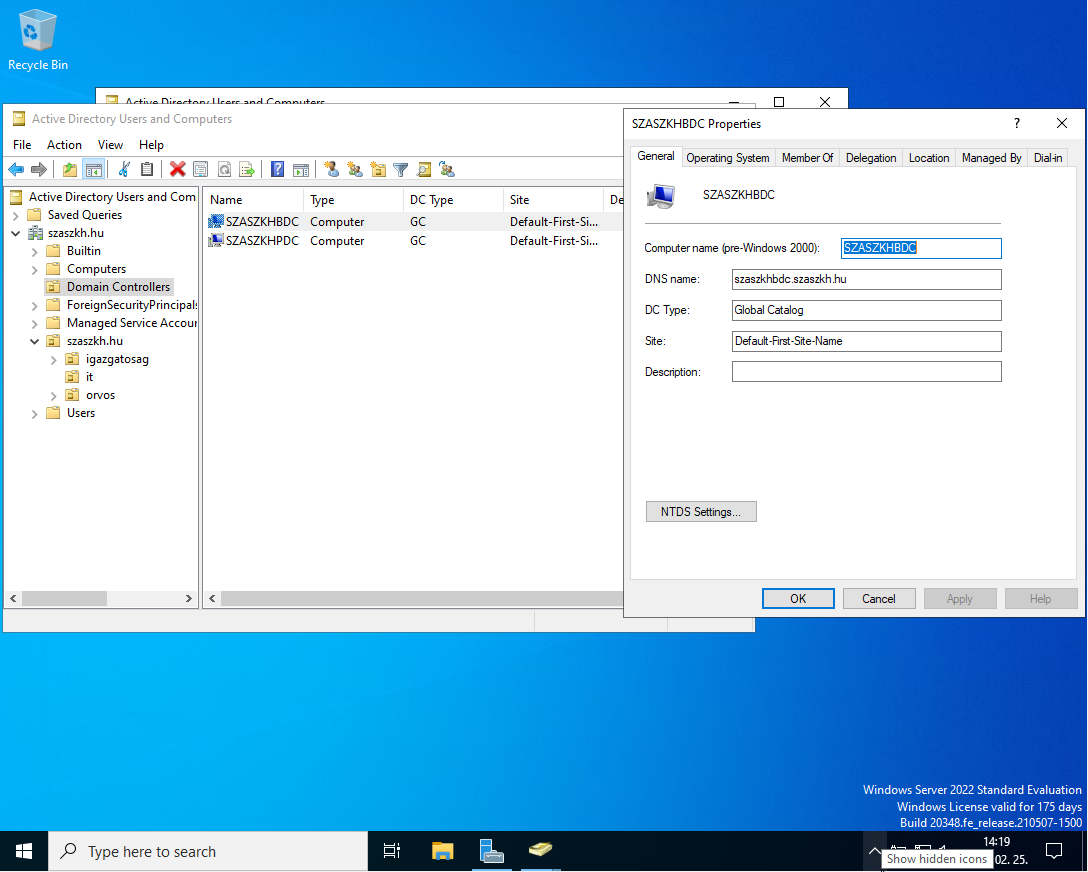
### Minimális jelszóhossz beállítása és jelszó lejárati idejének megváltoztatása

Biztonsági okokból, a megrendelő kérésére 32 naponta szükséges jelszóváltoztatás. Fontos, hogy ennek a jelszónak legalább 8 karakter hosszúságúnak kell lennie. 

ábra 25 - Minimális jelszóhossz, maximális időtartam

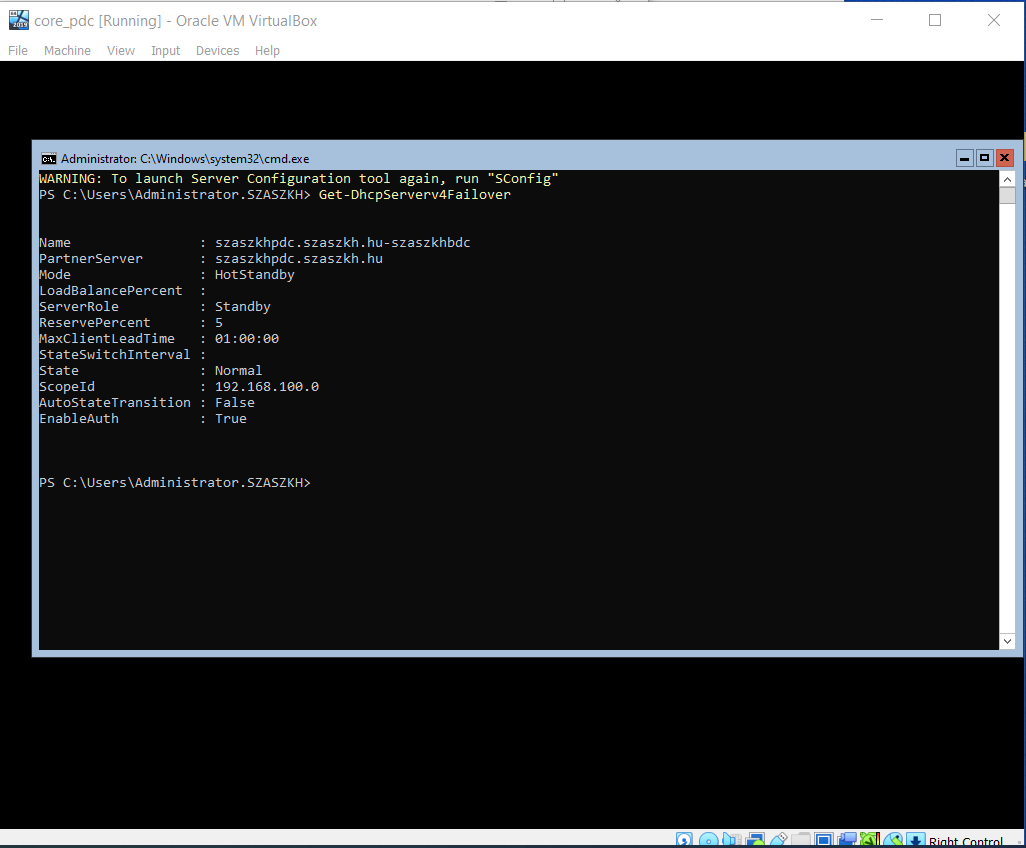
### Windows BDC (Core)

Ezen a szerveren Windows 2022 server Core operációs rendszer van telepítve. Két fontos szerepet lát el szolgáltatást lát el, a BDC-t és a DHCP Failover-t.

BDC(Backup Domain Controller): A BDC képes a felhasználók autentikálására, de a tartomány változásait (új felhasználók, jelszóváltozások, csoporttagság-változások) csak a PDC-n keresztül lehet rögzíteni, ahonnan azután ezek a változások tovább terjednek a tartomány összes BDC-jére. Ha a PDC éppen elérhetetlen a BDC átveszi a szerepét. ****

ábra 26 - Win Server BDC

### DHCP-Failover

A DHCP-Failover alkalmazása fontos, abban az esetben, ha a **PDC** leáll. A Failover továbbít minden információt, a DHCP-ről, a Backup Domain Controllernek. Abban az esetben, ha leáll a PDC, a végberendezések továbbra is megkapják az IP-Címüket, a BDC-től. 

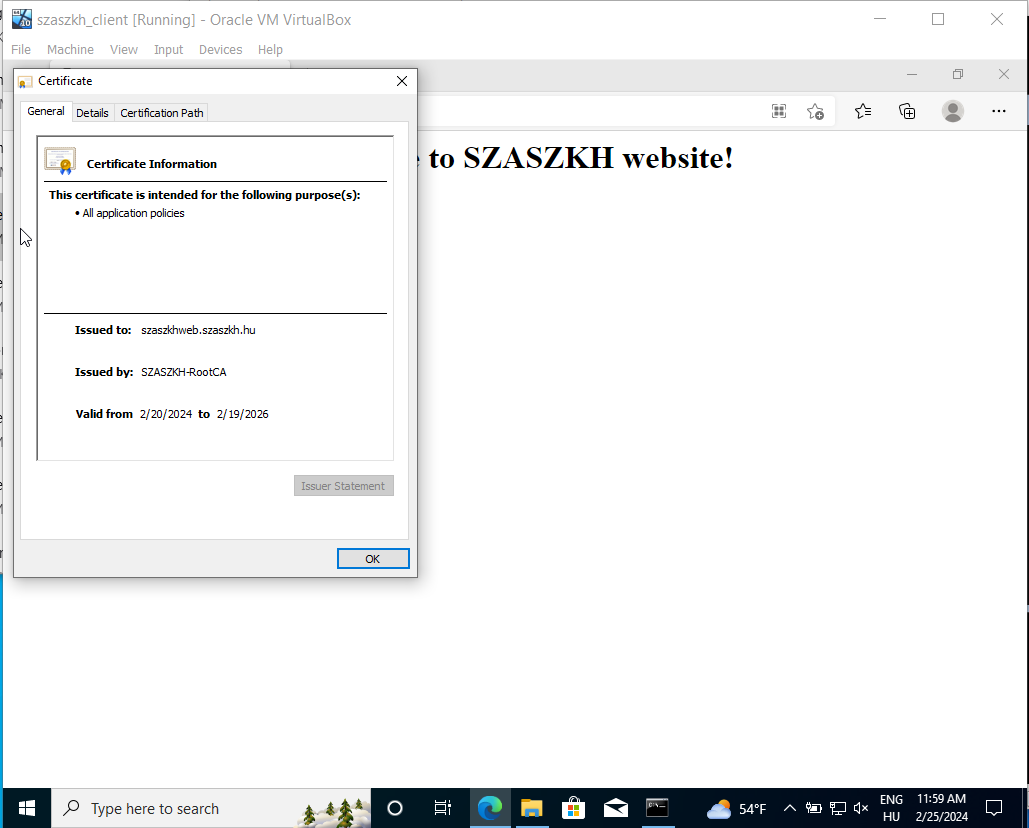
ábra 27- BDC DHCP Failover konfiguráció

A „**Get-DhcpServerv4Failover**” parancsot kiadva, láthatjuk, a Failover beállításait.

### Linux Web, File és Print szerver (CLI)

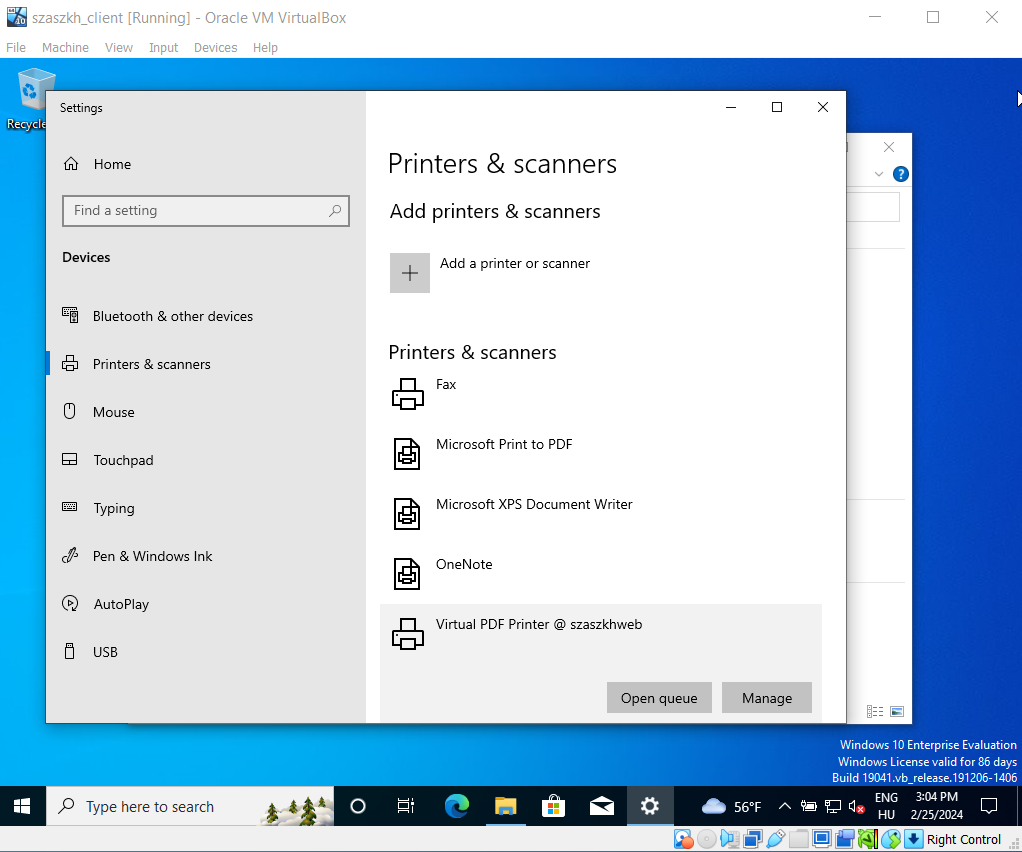
Ezen a szerveren Linux Debian 12es verziójú operációs rendszert használtunk. Web, nyomtató, illetve fájlmegosztás szolgáltatásokat használtunk.

WEB: Weboldalakat elérhetővé teszi a felhasználók számára a HTTP protokollon keresztül. A webszerver felelős a weboldalak és egyéb webes tartalmak kiszolgálásáért.



ábra 28 - Weboldal tanúsítvány

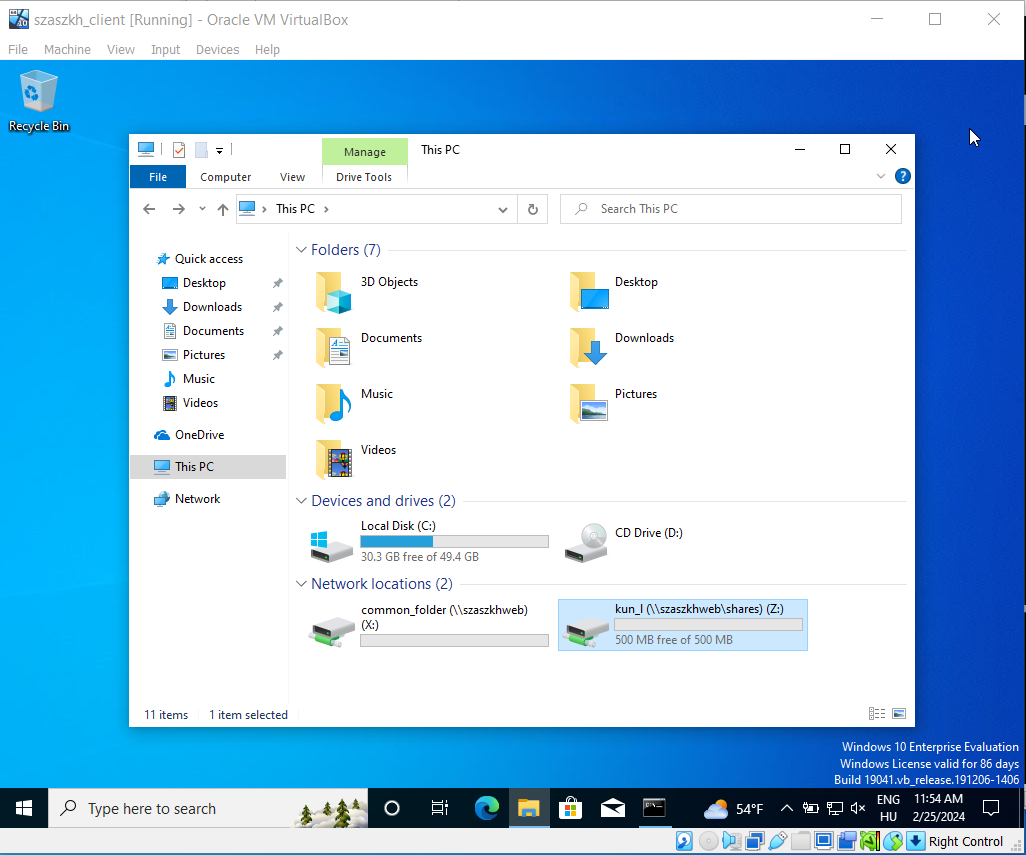
A fenti képen látható, hogy a kliensek elérik, a Szerver által biztosított tanúsítvánnyal ellátott weboldalt

Print:A print szerverek lehetővé teszik, hogy több felhasználó is ugyanazt a nyomtatót használja, anélkül, hogy közvetlen kapcsolatot kellene létrehozniuk minden egyes számítógép és nyomtató között 

ábra 29 - Printszerver Nyomtató

A printszervernek köszönhetően, a dolgozók a saját számítógépükről tudnak nyomtatást kezdeményezni távolról, nem gátolva mások nyomtatását. A nyomtató a beküldött nyomtatások alapján nyomtatási sorrendet alakít ki.

File: A Linux fileszerverek kiválóan alkalmasak a fájlok tárolására és megosztására a hálózaton.



ábra 30 - Fileszerver Mappamegosztás és saját mappák

A fileszervernek köszönhetően, a dolgozóknak van egy saját mappájuk, melyre feltölthetik a fájljaikat. Ennek a mappának egy 500 MB-os kvótát állítottunk be.

### Biztonsági mentés

Annak érdekében, hogy a fileok biztonságban legyenek, egy script megírására volt szükség a linux szerveren. A script megírásához az **Rsync** nevű programot használtuk.

Az **Rsync** egy sokoldalú fájlmásoló eszköz. Sajátossága, hogy csökkenti a másolandó adatok mennyiségét azáltal, hogy csak a forrás és a cél közötti különbségeket másolja, azaz növekményes mentést készíthetünk a segítségével.

 A Script:

ábra 31 - Backup script

A Scriptnek köszönhetően a *common\_folder* és a *shares* mappa tartalmáról készített biztonsági mentés a **/mnt/sdc1/backups** mappában tárolódik, az aktuális dátummal ellátva.

### HSRP (Hot Standby Router Protocol)

A Cisco saját fejlesztésű FHRP-je, az alapátjáró IPv4-eszköz hibatűrő működtetésére. A HSRP magas szintű hálózati elérhetőséget biztosít, az IPv4 alapértelmezett átjárót használó állomások számára ad első ugrás forgalomirányító redundanciát. A HSRP a forgalomirányítók egy csoportjából választ ki aktív és készenléti (standby, tartalék) eszközt. Az aktív eszköz végzi a csomagok továbbítását, a készenléti vagy tartalék eszköz pedig, megfelelő feltételek teljesülése esetén, átveszi a kiesett aktív eszköz szerepét. A HSRP tartalék forgalomirányítójának feladata figyelni a HSRP-csoport működését és gyorsan átvenni a csomagtovábbítás feladatát az aktív eszköz hibájakor.

Beállítása igen egyszerű. Először ki kell választanunk, hogy melyik az aktív, és melyik a tartalék forgalomirányító. A mi esetünkben az aktív forgalomirányító a SZERVER\_R, a tartalék pedig a SZERVER\_BACKUP. Beállításához az aktív routeren be kell lépnünk a szükséges interface(ek)be, majd a standby <azonosító> ip <virtualis\_forg\_ip> parancsot kiadva, meg kell adnunk a virtuális IP címet (A SZÜRKE területen, ez a 192.168.100.126), majd beállítjuk a forgalomirányító prioritását, ezzel jelezve, hogy melyik legyen az aktív. Ezt a standby 1 priority <prioritás> paranccsal tehetjük. Minél kisebb a prioritás, annál nagyobb elsőbbséget élvez a forgalomirányító, tehát az lesz az aktív. Emellett az aktív routeren, ki kell adnunk a standby 1 preempt parancsot, mely megmondja, hogy a router, kerekedjen felül, a többi aktív routeren.

### NAT

A NAT elsődleges célja a nyilvános IPv4-címekkel való takarékoskodás. A hálózatokon belül megengedi a privát IPv4-címek használatát, és publikus címre való fordítást csak akkor biztosít, ha arra szükség van, Emellett hozzáad egy bizonyos fokú titkosságot és biztonságot a hálózathoz, mert elrejti a belső IPv4-címeket a külső hálózatok elől.

A NAT-képes forgalomirányítók egy vagy több érvényes nyilvános IPv4-címmel is konfigurálhatók. Ezeket a nyilvános címeket NAT-címkészlet néven ismerjük. Amikor egy belső eszköz forgalmat küld ki a hálózatból, a NAT-képes forgalomirányító lefordítja a készülék belső IPv4-címét egy a NAT-címkészletből származó nyilvános címre. A külső eszközök szemszögéből úgy tűnik, mintha mind a be-, mind a kilépő forgalom egy a címkészletből származó nyilvános IPv4-címmel rendelkezne.

**Típusai:**

* Statikus címfordítás (statikus NAT) - Egy-az-egyhez típusú hozzárendelés a helyi és a globális címek között.
* Dinamikus címfordítás (dinamikus NAT) - Több-a-többhöz típusú hozzárendelés a helyi és a globális címek között.
* Port címfordítás (Port Address Translation, PAT) - Több-az-egyhez típusú megfeleltetés a helyi és a globális címek között. Ezt a módszert túlterhelésként (NAT overloading) is ismerjük.

Cégünk a Szervertelepen **Statikus NAT**-ot alkalmazott

A **statikus NAT** különösen hasznos olyan webszerverek és egyéb eszközök számára, amelyeknek egy állandó, interneten keresztül is elérhető cím kell. Ilyen például egy vállalati webszerver. Szintén hasznos olyan eszközök esetében, amelyeknek az arra jogosult, de telephelyen kívül tartózkodó személyzet számára hozzáférhetőnek kell lenniük, de az internetes nagyközönség számára nem.

Cégünk a belső hálózatban a 192.168.100.0-ás hálózati címet osztotta ki a szervereknek, azonban fontos, hogy a belső cím ne kerüljön a nyilvánosság részére. Ezért fontos volt a NAT alkalmazása.

A kórház esetében fontos, hogy az otthoni rendszergazda távolról is elérje a Szervertelepen található szervereket 

ábra 32 - Admin FTP kapcsolat szerver publikus címével

### ACL (Access Control List)

Az ACL célja a hálózati forgalmak szabályozása. Lehetővé teszi a hálózati adminisztrátorok számára, hogy meghatározzák, hogy mely forrás IP-címek férhetnek hozzá a cél IP-címekhez és portokhoz, és melyek nem. Az ACL-eket tűzfalakon, útválasztókon és más hálózati eszközökön lehet konfigurálni. Az ACL-eknél használhatunk azonosítókat és neveket is ezeket hívjuk nevesített ACL-nek

Két fő tipusú ACL létezik: Szabványos és a kiterjesztett acl

**Szabványos:**

* Csak a forrás IP-címek alapján szűr
* 1-99 és 1300-1999 közötti azonosítókat használ
* Egyszerű konfiguráció
* Ideálisak egyszerű hálózatokhoz, ahol a forrás IP-cím alapján történő szűrés elegendő.

**Kiterjesztett:**

* Forrás IP-cím, Cél IP-cím, protokoll, port és forgalom típusa alapján szűri a csomagokat
* 100-199 és 2000-2699 közötti azonosítókat használ
* Bonyolultabb konfiguráció
* Rugalmas.
* Összetettebb hálózatokhoz ideálisak, ahol a forrás IP-címen kívül más kritériumok alapján is szűrni kell

Cégünk fontosnak tartja, hogy a szerverek mindig elérhtőek legyenek a dolgozók számára ezért próbáljuk minél teher mentesebbé tenni a hálózatot. Erre a célra használtunk egy kiterjesztett nevesített ACL-t, amit NOICMP-nek neveztünk el. Ez az ACL letiltja a bejövő ICMP csomagokat, de engedélyezi az átjárást a szerverek működéséhez szükséges csomagokat.

ábra 33 - Ping letiltása ACL segítségével

## Telehelyek között alkalmazott forgalomirányító protokoll

### OSPF

Az OSPF egy kapcsolatállapot alapú forgalomirányító protokoll. Lényeges előnye más forgalomirányító protokollokkal szemben, hogy nagyobb hálózatok esetében gyorsabb konvergenciát és méretezhetőséget biztosít.

**Jellemzői**

* **Osztály nélküli** - Tervezéséből eredően osztály nélküli, azaz támogatja a VLSM-et és CIDR-t.
* **Hatékony** - A forgalomirányítás változásai váltják ki a forgalomirányítás frissítéseket (nincsenek periodikus frissítések). A legjobb útvonal kiválasztásához az SPF-algoritmust használja.
* **Gyors konvergencia** - A hálózat változásai gyorsan elterjednek.
* **Skálázhatóság** - Egyaránt jól működik kis - és nagy hálózatok esetében is. Hierarchikus rendszerek kialakításának érdekében a forgalomirányítók csoportokba szervezhetők.
* **Biztonságos** - Támogatja a Message Digest 5 (MD5) alapú azonosítást. Ha az engedélyezve van, akkor az OSPF forgalomirányítók a társaiktól csak olyan kódolt irányítási frissítéseket fogadnak el, ahol megegyezik az osztott kulcs.

Az OSPF három adatbázist hoz létre és tart karban (lásd 1. ábra):

* **Szomszédsági adatbázis** – ez alkotja a szomszédsági táblát (neighbor table).
* **Kapcsolatállapot adatbázis** - ez alkotja topológia táblát (topology table).
* **Továbbítási adatbázis** – ez pedig az irányítótábla (routing table).

Ezek tartalmazzák azon szomszéd forgalomirányítók listáját, melyekkel forgalomirányítási adatokat kell cserélnie.

Az OSPFv2 öt különböző típusú csomagot használ a szomszédos útválasztókkal való kommunikációhoz, valamint a kapcsolatállapot-hirdetések (LSA-k) kéréséhez és küldéséhez.

* Hello csomagok
  + Az OSPF forgalomirányítók közti szomszédsági kapcsolatok létrehozására és karbantartására szolgál.
* Adatbázis leíró csomagok
  + A topológia kezdeti cseréjekor az LSA fejlécek cseréjére szolgál, hogy a szomszédok rendelkezzenek az útválasztó LSA-inak listájával.
* Kapcsolatállapot kérés csomagok (LSR csomagok)
  + A fogadó forgalomirányítók egy LSR küldésével többletinformációt kérhetnek a kapott DBD bármelyik eleméről.
* Kapcsolatállapot frissítés csomagok (LSU csomagok)
  + Az LSR-ek megválaszolására és új adatok hirdetésére szolgál.
* Kapcsolatállapot visszaigazoló csomagok
  + Ha egy forgalomirányító LSU-t kap, akkor annak nyugtázására egy LSAck-ot küld. Az LSAck adatmezője üres.

**Az algoritmus**

A CPU a szomszédsági és topológiai táblákat Dijkstra SPF-algoritmusával dolgozza fel. Az SPF-algoritmus meghatározza az egyes célok elérésének teljes költségét.

Az SPF-algoritmus felépít egy SPF-fát, amely a forgalomirányítótól - mint a fa gyökerétől - kiindulva minden más csomópontohz kiszámítja a hozzá vezető legrövidebb útvonalat. Ezek után az SPF-fa szolgál a legjobb útvonalak meghatározására. Az OSPF a legjobb utakat behelyezi a forgalomirányító adatbázisba, amelyet az irányítótábla felépítéséhez használ.

A forgalomirányítási információk karbantartására, a konvergencia elérése érdekében az OSPF forgalomirányítók az alábbi általános kapcsolatállapot alapú forgalomirányítási folyamatot hajtják végre:

**1. Szomszédsági kapcsolatok létrehozása**

Az adatok megosztása előtt az OSPF forgalomirányítóknak fel kell deríteniük egymást a hálózaton. Ennek érdekében egy OSPF forgalomirányító valamennyi OSPF által használt interfészén Hello csomagokat küld ki annak kiderítésére, hogy vannak-e szomszédok ezeken a kapcsolatokon. Ha talál egy szomszédot, akkor azzal az OSPF forgalomirányító megpróbál ezzel a szomszéddal egy szomszédsági kapcsolatot kialakítani.

**2. Kapcsolatállapot hirdetések (Link-State Advertisements, LSA) cseréje**

A szomszédségi kapcsolatok létrehozását követően a forgalomirányítók kapcsolatállapot hirdetéseket (LSA) váltanak. Az LSA valamennyi közvetlenül kapcsolódó kapcsolat állapotát és költségét tartalmazza. A forgalomirányítók az LSA-kkal elárasztják a kapcsolódó szomszédjaikat. Ha egy kapcsolódó szomszéd LSA-üzenetet kap, akkor azonnal továbbítja azt a saját kapcsolódó szomszédjai felé, mígnem a terület összes forgalomirányítója az összes LSA-t meg nem kapja.

**3. Topológia tábla építése**

Az LSA-k begyűjtését követően, az OSPF forgalomirányítók az LSA-kból topológia táblát építenek. Ez az adatbázis lényegében a hálózat topológiájának minden részletét tartalmazza.

**4. Az SPF-algoritmus végrehajtása**

Ezt követően a forgalomirányítók végrehajtják az SPF-algoritmust. Az ábra fogaskerekei az SPF-algoritmus végrehajtását szimbolizálják. Az SPF-algoritmus eredményeként jön létre az SPF-fa.

Az OSPF úgynevezett területeket (area) használ a hierarchikus forgalomirányítás megvalósításához, amely ezáltal még hatékonyabbá és skálázhatóbbá válik

Az OSPF az alábbi két módon valósítható meg:

* **Egyterületű OSPF (Single-Area OSPF)**

Aforgalomirányítók egyetlen területhez, a gerinc területhez tartoznak.

* **Többterületű OSPF (Multiarea OSPF)**

Valamennyi területnek a gerinc területhez (area 0) kell kapcsolódnia. A területeket összekötő forgalomirányítókat határ forgalomirányítónak (Area Border Routers, ABR) nevezzük.

A többterületű OSPF-el, a hierarchikus forgalomirányítás támogatására az OSPF egy nagyméretű autonóm területet (autonomous system - AS) több kisebb területre tud felosztani. Hierarchikus forgalomirányítás esetén továbbra is megtörténik a területek közti forgalomirányítás (interarea routing), viszont a számításigényes forgalomirányítási feladatok, mint például az adatbázisok újraszámítása, az egyes területeken belül maradnak.

Az 1-es típusú OSPF csomag a Hello csomag. A Hello csomagokat az alábbi esetekben használják:

* Az OSPF szomszédok felderítése és a szomszédsági kapcsolatok kialakítása.
* Azon paraméterek hirdetése, melyekben a két forgalomirányítónak meg kell egyeznie, hogy szomszédsági kapcsolatba kerülhessenek.
* A kijelölt forgalomirányító (Designated Router, DR) és a tartalék kijelölt forgalomirányító (Backup Designated Router, BDR) kiválasztása a többes hozzáférésű hálózatok esetében, mint pl. az Ethernet és a Frame Relay. Pont-pont kapcsolatok esetén nincs szükség DR-re és BDR-re.

**Hello csomag felépítése:**

* **Típus (Type)** – A csomag típusát határozza meg. Az egyes (1) a Hello csomag típust jelöli. A 2-es érték a DBD csomagot jelenti, a 3-as az LSR csomagot, a 4-es az LSU csomagot és az 5-ös pedig az LSAck csomagot.
* **Forgalomirányító azonosító (Router ID)** – 32 bites mező, pontozott decimális formában (egy IPv4 cím), mely egyértelműen azonosítja a forrás (kezdeményező) forgalomirányítót.
* **Területazonosító (Area ID)** - Azt a területet jelöli, ahonnan a csomag származik.
* **Hálózati maszk (Network Mask)** – A küldő interfészhez tartozó alhálózati maszk.
* **Hello időintervallum (Hello Interval)** – A Hello csomagok küldésének gyakoriságát adja meg másodpercben. A Hello időintervallum alapértelmezett értéke többes hozzáférésű hálózatok esetében 10 másodperc. Ezen időzítő értékének a szomszédos forgalomirányítókon meg kel egyeznie. Ellenkező esetben a szomszédsági kapcsolat nem jön létre.
* **Forgalomirányító prioritás (Router Priority)** – A DR/BDR választás során használatos. Az OSPF forgalomirányítók alapértelmezett prioritása 1, amelynek 0 és 255 közötti értékre manuálisan megváltoztatható. Minél magasabb az érték, annál valószínűbb, hogy egy forgalomirányító DR lesz az adott kapcsolaton.
* **„Halott” intervallum (Dead Interval)** – Másodpercekben mérve az az időtartam, amennyit egy forgalomirányító a szomszédjának az üzenetére vár, mielőtt azt elérhetetlennek nyilvánítaná. Alapértelmezés szerint egy forgalomirányító "halott" időtartama a Hello időintervallumnak a négyszerese. Ezen időtartamnak is azonosnak kell lennie a szomszédos forgalomirányítókon. Ellenkező esetben a szomszédsági kapcsolat nem jöhet létre.
* **Kijelölt forgalomirányító (Designated Router, DR)** – A DR forgalomirányító azonosítója.
* **Tartalék kijelölt forgalomirányító (Backup Designated Router, BDR)** – A BDR forgalomirányító azonosítója.
* **A szomszédok listája (List of Neighbors)** – Valamennyi szomszédsági kapcsolatban lévő forgalomirányító azonosítóját felsoroló lista.

**Hitelesítés**

Az MD5 (Message-Digest algorithm 5) egy kriptográfiai hash funkció, amelyet az adatok hitelességének ellenőrzésére használnak. Egy router esetében az MD5 gyakran használatos a hálózati forgalom, például a BGP (Border Gateway Protocol) üzenetek hitelesítésére.

Cégünk az MD5-öt minden router között alkalmazta. Beállítani rendkívül egyszerű. Minden forgalomirányító OSPF protokollján beállítjuk az ip ospf message-digest-key KEY\_ID md5 KEY. Nálunk a kulcs a „szaszkh” volt. Végül a hitelesítés engedélyezéséhez be kell írnunk az ip ospf authentication message-digest parancsot.

## Hálózatprogramozás

### PNET

A Packet Tracer krolátai miatt, szükség volt egy úgynevezett PNETLAB nevű szoftver igénybevétele.

A **PNETLAB** segítségével úgynevezett "laborokat" hozhatunk létre, melyben valós hálózati eszközök, mint például a cisco, vagy a huawei rendszereit tudjuk bekonfigurálni és tesztelni.

### Netmiko

A netmiko egy python modul, mely, SSH-kapcsolaton keresztül kommunikációt biztosít a hálózati eszközzel. Segítségével, egy teljesen automatizált hálózatot biztosíthatunk a megrendelőnek.

A script részletesen, a videóban bemutatásra kerül.

## Ábrajegyzék

[ábra 1 - A hálózat topológiája 6](#_Toc165541451)

[ábra 2 - show vlan brief parancs kimenetele 8](#_Toc165541452)

[ábra 3 - show vtp status parancs kimenetele 9](#_Toc165541453)

[ábra 4 - show etherchannel parancs kimenetele, S1\_SWITCHEN 10](#_Toc165541454)

[ábra 5 - A kék területen routerén alkalmazott DHCP beállításai 13](#_Toc165541455)

[ábra 6 - Otthoni dolgozó DHCP konfiguráció 15](#_Toc165541456)

[ábra 7 - Mac-Címszűrés 16](#_Toc165541457)

[ábra 8 - SSID Broadcast 17](#_Toc165541458)

[ábra 9 - Zöld terület DHCP 19](#_Toc165541459)

[ábra 10 - BETEG\_W DHCP 19](#_Toc165541460)

[ábra 11 - Zöld terület VLAN 20](#_Toc165541461)

[ábra 12 - RAKTAR\_R és GYOGYSZERTAR\_R PPP állapota 22](#_Toc165541462)

[ábra 13 - ZPF Policy Map 22](#_Toc165541463)

[ábra 14 - AWS adatbázis 23](#_Toc165541464)

[ábra 15 - Mikrotik Router IP konfiguráció 25](#_Toc165541465)

[ábra 16 - Mikrotik Router tűzfalbeállítások 25](#_Toc165541466)

[ábra 17 - Win Server AD szervezeti egységek 26](#_Toc165541467)

[ábra 18 - Win Server PDC Forward Lookup Zones 27](#_Toc165541468)

[ábra 19 - Win Server PDC Reverse Lookup Zones 28](#_Toc165541469)

[ábra 20 - Automatizált Mentés 29](#_Toc165541470)

[ábra 21 - Alapértelmezett háttérkép 30](#_Toc165541471)

[ábra 22 - Vezérlőpult letiltása 31](#_Toc165541472)

[ábra 23 - Alkalmazások elérésének tiltása 32](#_Toc165541473)

[ábra 24 - Cserélhető adathordozók tiltása 33](#_Toc165541474)

[ábra 25 - Minimális jelszóhossz, maximális időtartam 34](#_Toc165541475)

[ábra 26 - Win Server BDC 35](#_Toc165541476)

[ábra 27- BDC DHCP Failover konfiguráció 36](#_Toc165541477)

[ábra 28 - Weboldal tanúsítvány 37](#_Toc165541478)

[ábra 29 - Printszerver Nyomtató 38](#_Toc165541479)

[ábra 30 - Fileszerver Mappamegosztás és saját mappák 39](#_Toc165541480)

[ábra 31 - Backup script 39](#_Toc165541481)

[ábra 32 - Admin FTP kapcsolat szerver publikus címével 41](#_Toc165541482)

[ábra 33 - Ping letiltása ACL segítségével 42](#_Toc165541483)

## Forrás

VLAN, VTP, DHCP ,OSPF, Port-Security, STP, IPv6: <https://netacad.com>

GRE Tunnel: <https://iktblog.hu/2020/12/16/gre-alagut-keszitese/>

ACL,NAT, HSRP, : <https://szit.hu>

Szerverek AWS: iskolai segédlet