****

**VIZSGAREMEK**

Készítették:

Gál Máté János - Szabó Gergely – Borbély Gergely

Konzulens:

Csontos Dénes

Miskolc

2025.

Miskolci SZC Kandó Kálmán Informatikai Technikum

Miskolci Szakképzési Centrum

Informatikai rendszer- és alkalmazás-üzemeltető technikus

Dokumentáció

Gál Máté János – Szabó Gergely - Borbély Gergely

2024-2025

Tartalomjegyzék

Tartalomjegyzék

[A vizsgaremek bemutatója - 4 -](#_Toc193873119)

[1. Adatok - 5 -](#_Toc193873120)

[1.1 IP Táblázat: - 5 -](#_Toc193873121)

[1.2 VLAN Táblázat: - 6 -](#_Toc193873122)

[1.3 IPv6 Tábla: - 7 -](#_Toc193873123)

[2. Megvalósítás - 8 -](#_Toc193873124)

[2.1 Harmadik rétegbeli redundancia (HSRP): - 8 -](#_Toc193873125)

[2.2 VLAN: - 9 -](#_Toc193873126)

[2.3 Második rétegbeli redundancia (Etherchannel): - 10 -](#_Toc193873127)

[2.4 Jelszavak, biztonság, nap üzenete: - 11 -](#_Toc193873128)

[2.5 FTP (File Transfer Protocol) mentés Szerverre: - 12 -](#_Toc193873129)

[2.6 Kron automatizált mentés: - 13 -](#_Toc193873130)

[2.7 DHCPv4 Szerver: - 14 -](#_Toc193873131)

[2.8 Windows IIS HTTPS: - 15 -](#_Toc193873132)

[2.9 Windows Win-AcMe: - 16 -](#_Toc193873133)

[2.10 Windows HTML Struktúra: - 17 -](#_Toc193873134)

[2.11 Windows IIS Tűzfalszabály: - 18 -](#_Toc193873135)

[2.12 Windows IIS DNS: - 19 -](#_Toc193873136)

[2.13 Linux Szerver DNS: - 20 -](#_Toc193873137)

[2.14 Linux Szerver Samba: - 21 -](#_Toc193873138)

[2.15 NAT Címfordítás: - 22 -](#_Toc193873139)

[2.16 ACL (Access Control List): - 23 -](#_Toc193873140)

[2.17 Portbiztonság: - 24 -](#_Toc193873141)

[2.18 Forgalomirányítás: - 25 -](#_Toc193873142)

[2.19 IP Route: - 26 -](#_Toc193873143)

[2.20 WAN (Wide Area Network): - 27 -](#_Toc193873144)

[2.21 GRE Tunnel (Generic Routing Encapsulation): - 28 -](#_Toc193873145)

[2.22 SSH beállítás: - 29 -](#_Toc193873146)

[2.23 WiFi: - 30 -](#_Toc193873147)

[2.24 DHCP Routerek: - 31 -](#_Toc193873148)

[3. Összegzés - 32 -](#_Toc193873149)

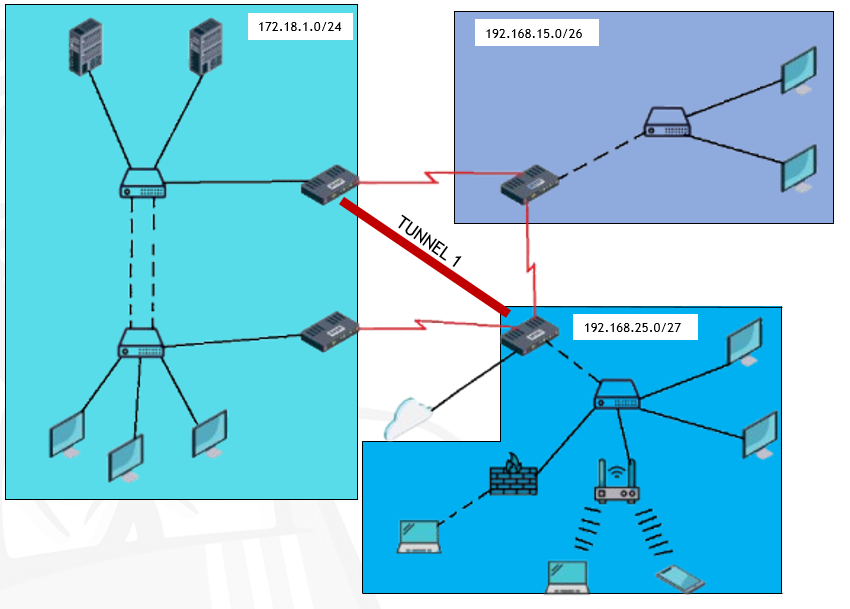
# A vizsgaremek bemutatója

Vizsgaremekünk elkészítése alapjául a miskolci KFC hálózatot próbáltuk megvalósítani mivel egyik nagy kedvencünk ez az étterem lánc. Hiányosak az információink a pontos hálózatról ezért a saját elképzelésünk alapján próbáltuk megvalósítani. A projekt feladatot emiatt egy kitalált hálózattal valósítottuk meg. A tervet úgy hoztuk létre, hogy a követelményeknek megfelelően a három telephelyes hálózatot meglehessen valósítani.

A projektünk átfogó tömör lényegretörő képét a bemutatónk illusztrálja a legjobban

Link a PPT-re:

A dokumentációnk végén link formájában megtalálhatóak a tesztelési dokumentációk és videók, illetve a bemutatónk.



Fizikai Topológia (Visme)

# Adatok

## 1.1 IP Táblázat:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP Cím Tábla | | | | |
| Név | Port | IP | Maszk | Gateway |
| KFC Miskolc Pláza | Serial0/2/0 | 10.10.10.5 | 255.255.255.252 (/30) |  |
| Gig0/0/0.35 | 172.18.1.2 | 255.255.255.192 (/26) |
| Gig0/0/0.45 | 172.18.1.66 | 255.255.255.224 (/27) |
| Gig0/0/0.55 | 172.18.1.98 | 255.255.255.224 (/27) |
| Tunnel1 | 10.0.0.1 | 255.255.255.252 (/30) |
| KFC Pesti út Auchan | Serial0/2/0 | 10.10.10.1 | 255.255.255.252 (/30) |
| Gig0/0/0.35 | 172.18.1.3 | 255.255.255.192 (/26) |
| Gig0/0/0.45 | 172.18.1.67 | 255.255.255.224 (/27) |
| Gig0/0/0.55 | 172.18.1.99 | 255.255.255.224 (/27) |
| KFC Szentpéteri kapu | Serial0/1/0 | 10.10.10.6 | 255.255.255.252 (/30) |
| Serial0/1/1 | 10.10.10.9 | 255.255.255.252 (/30) |
| Gig0/0/0 | 192.168.25.1 | 255.255.255.192 (/26) |
| KFC József Attila út Auchan | Serial0/2/1 | 10.10.10.10 | 255.255.255.252 (/30) |
| Serial0/2/0 | 10.10.10.2 | 255.255.255.252 (/30) |
| Gig0/0/0 | 192.168.25.1 | 255.255.255.224 (/27) |
| Tunnel1 | 10.0.0.2 | 255.255.255.252 (/30) |
| SW1 | VLAN35 | 172.18.1.4 | 255.255.255.192 (/26) |
| VLAM45 | 172.18.1.69 | 255.255.255.224 (/27) |
| SW2 | VLAN55 | 172.18.1.101 | 255.255.255.224 (/27) |
| SW3 | VLAN1 | 192.168.25.2 | 255.255.255.224 (/27) |
| Windows Server | Fa0 | 172.18.1.62 | 255.255.255.240 (/28) | 172.18.1.1 |
| 221.93.222.132 | NAT Címfordítás | |
| Linux Server | Fa0 | 172.18.1.94 | 255.255.255.224 (/27) | 172.18.1.65 |
| 221.93.222.133 | NAT Címfordítás | |
| G. Máté PC | Fa0 | **DHCP** | | 172.18.1.1 |
| B. Gergely PC | Fa0 | 172.18.1.65 |
| Sz. Gergely PC | Fa0 | 172.18.1.97 |
| Egon PC | Fa0 | 192.168.25.1 |
| Egon Telefon | Fa0 | 192.168.35.1 |
| Dönci PC | Fa0 | 192.168.25.1 |
| Dönci Laptop | Fa0 | 192.168.35.1 |
| Áron PC | Fa0 | 192.168.15.1 |
| Zsombor PC | Fa0 | 192.168.15.1 |

## VLAN Táblázat:

Ez a táblázat egy **VLAN (Virtual Local Area Network) konfigurációt** mutat, amely egy szervezett hálózati felosztást reprezentál.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VLAN Tábla | | | | |
| Eszköz | VLAN Azonosító | VLAN Neve | Portok | Hálózat |
| KFC Miskolc Pláza | 35 | VLAN35 | Gig0/0/0.35 | 172.18.1.0/24 |
| 45 | VLAN45 | Gig0/0/0.45 | 172.18.1.64/27 |
| 55 | VLAN55 | Gig0/0/0.55 | 172.18.1.96/27 |
| KFC Pesti út Auchan | 35 | VLAN35 | Gig0/0/0.35 | 172.18.1.0/24 |
| 45 | VLAN45 | Gig0/0/0.45 | 172.18.1.64/27 |
| 55 | VLAN55 | Gig0/0/0.55 | 172.18.1.96/27 |
| G. Máté PC | 35 | VLAN35 | Fa0 | 172.18.1.0/24 |
| B. Gergely PC | 45 | VLAN45 | 172.18.1.64/27 |
| Sz. Gergely PC | 55 | VLAN55 | 172.18.1.96/27 |
| Zsombor PC |  | | 192.168.15.0/26 |
| Áron PC | 192.168.15.0/26 |
| Dönci PC | 192.168.25.0/26 |
| Eugén PC | 192.168.25.0/26 |
| Dönci Laptop | 192.168.25.0/26 |
| Egon Telefon | 192.168.25.0/26 |
| Windows Szerver | 35 | VLAN35 | 172.18.1.0/24 |
| Linux Szerver | 45 | VLAN45 | 172.18.1.64/27 |
| SW1 | 35 | VLAN35 | Fa0/24 |  |
| 45 | VLAN45 | Fa0/23 |
| 55 | VLAN55 | Fa0/22 |
| SW2 | 35 | VLAN35 | Fa0/24 |
| 45 | VLAN45 | Fa0/23 |
| 55 | VLAN55 | Fa0/22 |

## IPv6 Tábla:

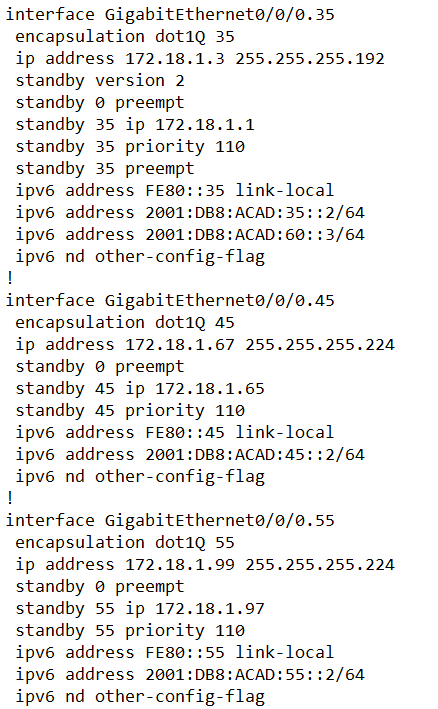
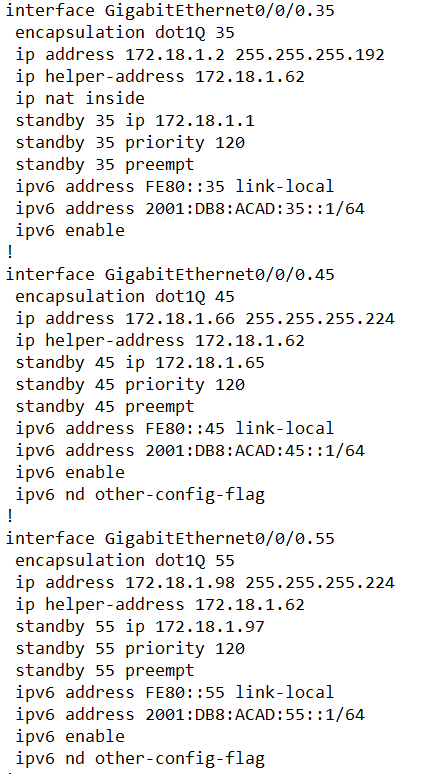
Ez a táblázat az IPv6 címzési struktúrát mutatja, ahol a KFC telephelyek, PC-k és egyéb eszközök kapcsolódnak különböző interfészeken keresztül.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IPv6 Táblázat | | | | |
| Név | Port azonosító | IP | Maszk | Gateway |
| KFC Miskolc Pláza | Gig0/0/0.35 | 2001:db8:acad:35::1 | /64 | fe80::35 |
| Gig0/0/0.45 | 2001:db8:acad:45::1 | /64 | fe80::45 |
| Gig0/0/0.55 | 2001:db8:acad:55::1 | /64 | fe80::55 |
| KFC Pesti úti Auchan | Gig0/0/0.35 | 2001:db8:acad:35::2 | /64 | fe80::35 |
| Gig0/0/0.45 | 2001:db8:acad:45::2 | /64 | fe80::45 |
| Gig0/0/0.55 | 2001:db8:acad:45::2 | /64 | fe80::55 |
| KFC Szent Péteri kapu | Gig0/0/0 | 2001:db8:acad::1 | /64 | fe80::35 |
| KFC József Attila Auchan | Gig0/0/0 | 2001:db8:acad::1 | /64 | fe80::35 |
| G.Máté PC | Fa0 | SLAAC | | |
| B.Gergely PC | Fa0 |
| Sz.Gergely PC | Fa0 |
| Áron PC | Fa0 |
| Zsombor PC | Fa0 |
| Dönci PC | Fa0 |
| Egon PC | Fa0 |
| Dönci Laptop | Fa0 |
| Egon Telefon | Fa0 |

# Megvalósítás

## 2.1 Harmadik rétegbeli redundancia (HSRP):

A HSRP egy harmadik rétegbeli redundanciát azért használjuk, hogy egy hálózatban **automatikusan biztosítsa a redundáns útvonalat**, ha az elsődleges útvonalat biztosító router meghibásodik vagy elérhetetlenné válik. Több Router egy virtuális Routerré kombinál. A HSRP csoporton belül az egyik router lesz az aktív router, amely a forgalmat továbbítja és egy másik router lesz a **tartalék (standby) router,** amely átveszi a forgalomirányítást, ha az aktív router meghibásodik. Az alábbi ábrákon látható, hogy a VLAN-oknak megfelelő HSRP beállításokat alkalmaztuk pl.: standby 35, ami a VLAN35 HSRP beállításai.

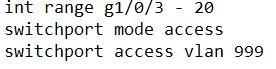


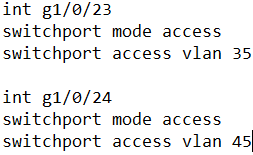
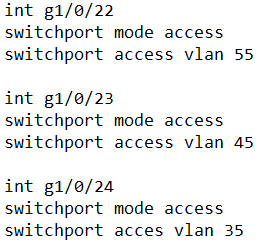
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HSRP Tábla | | | | | | |
| Eszköz | Port | Csoport | Prioritás | Státusz | Készenlét IP | Virtuális IP |
| KFC Miskolc Pláza | Gig0/0/0.35 | 35 | 120 | Aktív | 172.18.1.3 | 172.18.1.1 |
| Gig0/0/0.45 | 45 | 120 | Aktív | 172.18.1.67 | 172.18.1.65 |
| Gig0/0/0.55 | 55 | 120 | Aktív | 172.18.1.99 | 172.18.1.97 |
| KFC Pesti út Auchan | Gig0/0/0.35 | 35 | 110 | Készenlét | Helyi | 172.18.1.1 |
| Gig0/0/0.45 | 45 | 110 | Készenlét | 172.18.1.65 |
| Gig0/0/0.55 | 55 | 110 | Készenlét | 172.18.1.97 |

## 2.2 VLAN:

A **VLAN (Virtual Local Area Network)** egy **logikailag elkülönített** hálózati szegmens, amely lehetővé teszi, hogy egy fizikai hálózatot több különálló virtuális hálózatra osszunk fel. És mivel egy hálózaton belül több végberendezésünk van és elég nagy az egész hálózatunk, ezért alakítottuk ki. Az alábbi ábrán látható, hogy három VLAN-t használtunk amiből kettő adat VLAN a 35-ös és a 45-ös. A harmadik VLAN-unk a VLAN999 amit arra használtunk, hogy a nem használt protokat bele raktuk és letiltottuk a biztonsági szempontok miatt. A VLAN 999 a másik két Switchunkön is létrelett hozva és a nem használt portok bele lettek pakolva.





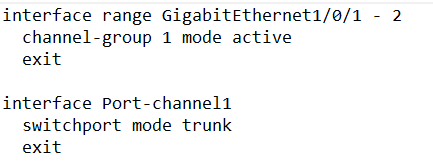
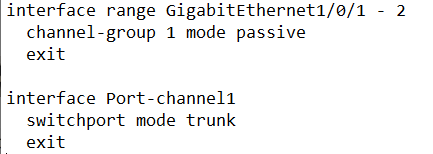


## Második rétegbeli redundancia (Etherchannel):

Az **EtherChannel** egy link aggregation technológia, amely lehetővé teszi több fizikai link összefűzését egy **logikai csatornává**. Ezáltal növeli a sávszélességet, redundanciát, megbízhatóságot és a terheléselosztást a hálózatban. Az EtherChannel ugy működik, hogy több kábellel kötünk össze kettő Switchet, két típusa van amiből mi az LACP protokolt választottuk. Az LACP egy gyártófüggetlen protokoll. Az alábbi konfigurációs részben látható, hogy active és passive módot használtunk ami az LACP protocol konfigorációja.



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Etherchannel tábla | | | | | |
|  | | Csoport | Mód | Protokoll | Port |
| Eszközök | SW1 | 1 | Active | LACP | Fa0/1, Fa0/2 |
| SW2 | 1 | Passive | LACP | Fa0/1, Fa0/2 |



## Jelszavak, biztonság, nap üzenete:

A hálózati eszközök eléréséhez az alábbi jelszavakat állítottuk be. A jövőben ezeket a jelszavakat biztonságosabb jelszavakra (minimum 12 karakter, kisbetű, nagybetű, szám, szimbólum) cserélnénk, de a gyorsabb haladás érdekébe most az egyszerűbb jelszavak mellett döntöttünk.

* SSH:
  + Domain: kfc.hu
  + user: admin jelszó: cisco/class
* Jelszavak:
  + sima: cisco

Nap üzenete:

WARNING: Unauthorized Access Prohibited! This system is for authorized users only. All activities are monitored and logged. Unauthorized access, use, or modification of this device is strictly prohibited and may be punishable by law.

s

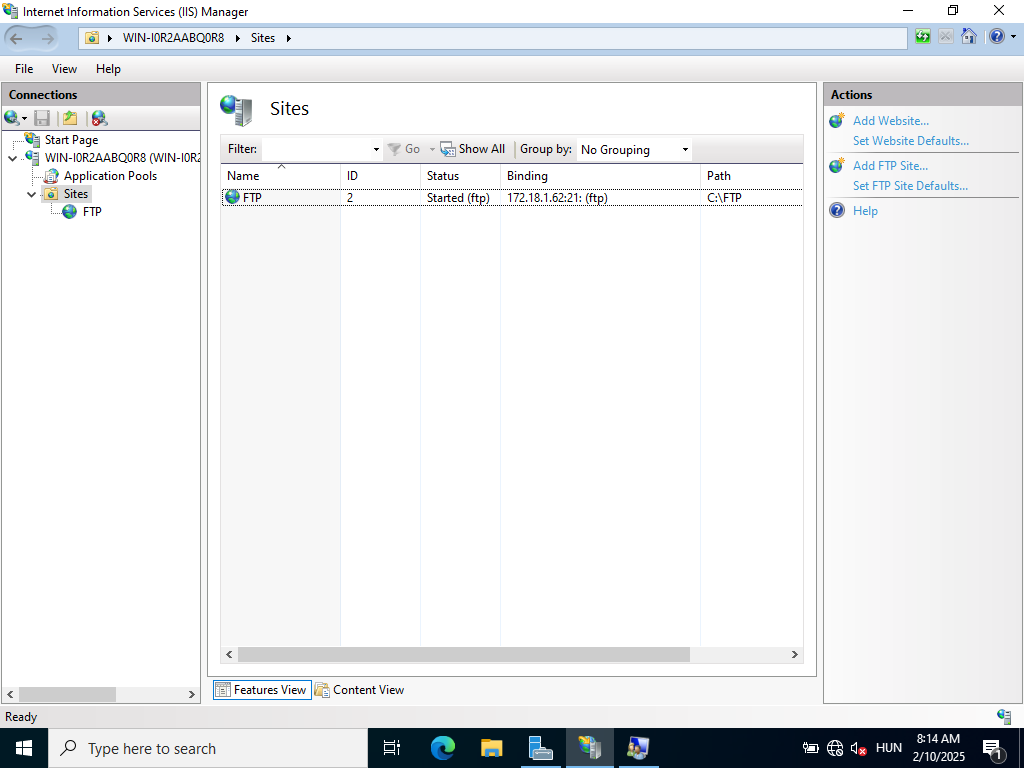
* + secret: class
* Console:
  + cisco
* Telnet:
  + cisco
* WiFi:
  + PipiHusika



* Linux Szerver:
  + - user: kfcadmin
    - jelszó: Passw.rd
* Windows:
  + Admin, Benjámin, Eugén, Hektor
  + FTP és felhasználók jelszavai: Passw.rd

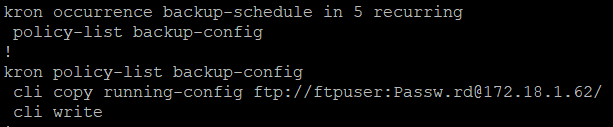
## FTP (File Transfer Protocol) mentés Szerverre:

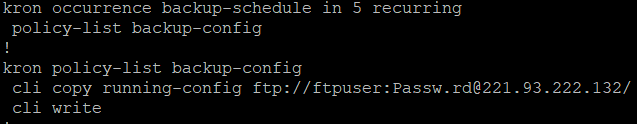
Az **FTP (File Transfer Protocol)** egy elterjedt módszer fájlok átvitelére hálózaton keresztül. Az FTP mentés szerverre lehetővé teszi, hogy egy hálózati eszköz (pl. router vagy switch) konfigurációs fájljait egy távoli szerveren tároljuk, biztosítva ezzel az adatmentést és az egyszerű visszaállítást hiba esetén. Az egyik képen látható a Windows-alapú **IIS (Internet Information Services) Manager** használatával létrehozott FTP szerver lehetővé teszi a fájlok fogadását, a másik képen pedig az összes hálózati eszközön megadott FTP User és Jelszó látható.



## Kron automatizált mentés:

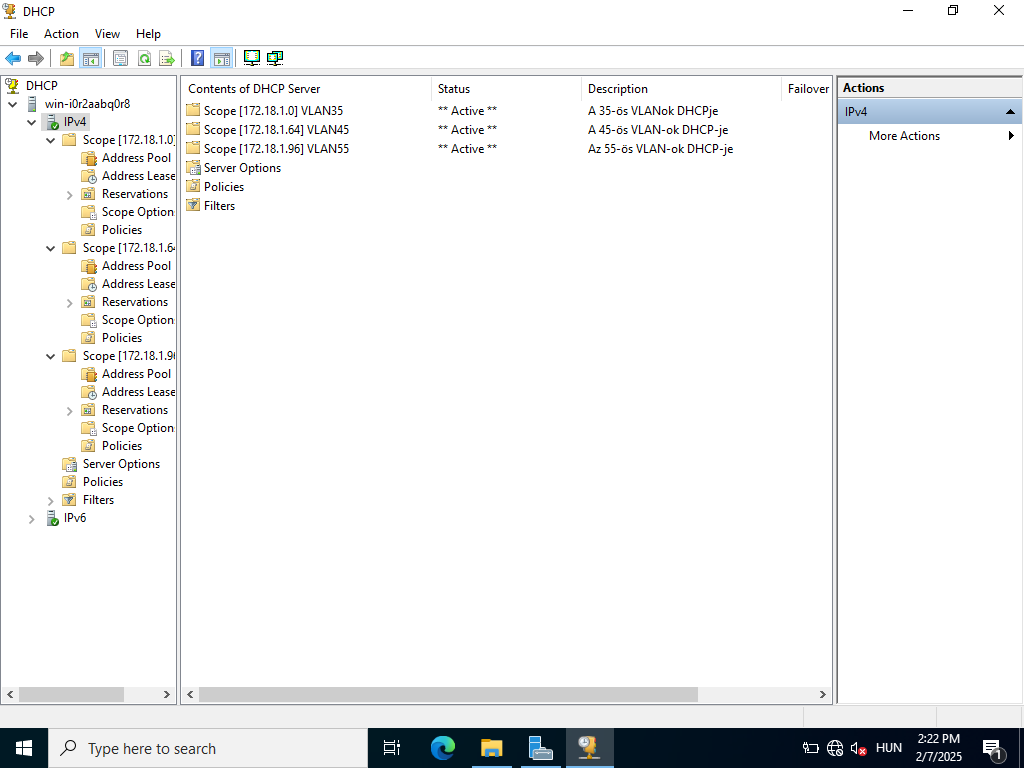
Az automatizált mentés fontos szerepet játszik a hálózati eszközök megbízhatóságának fenntartásában. A lenti konfigurációban a **KRON** parancs segítségével egy **időzített mentési folyamatot** hozunk létre a NAT-olt (címfordított) és a privát IP-re, amely automatikusan elmenti a hálózati eszköz konfigurációját az **FTP szerverre**.





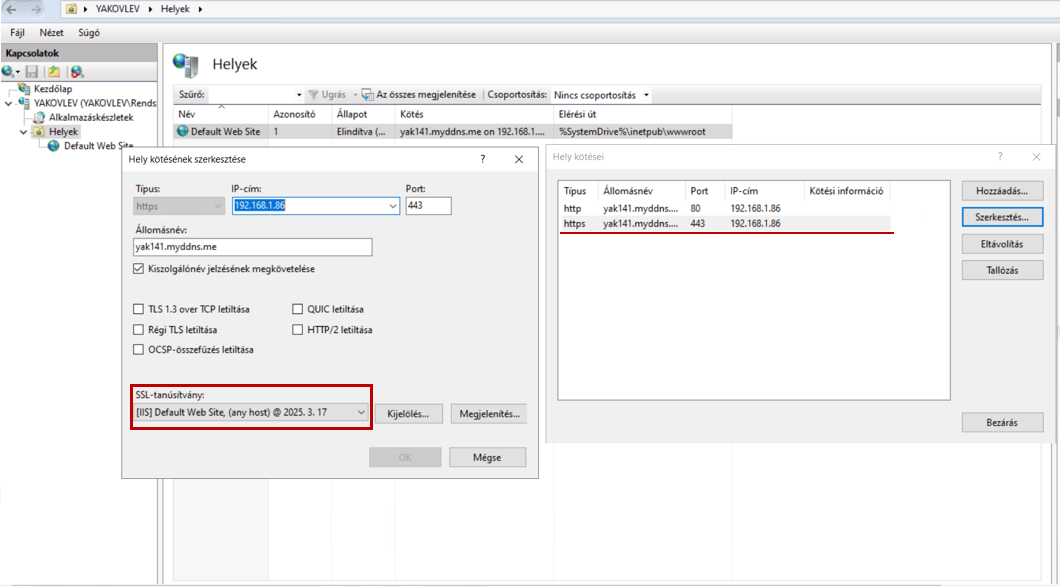
## 2.7 DHCPv4 Szerver:

A **DHCPv4 szerver (Dynamic Host Configuration Protocol v4)** egy automatikus IP-cím kiosztásra használt hálózati szolgáltatás. Ez az eszközök konfigurálását egyszerűsíti azáltal, hogy automatikusan kiosztja az **IP-címeket, alhálózati maszkokat, átjárókat és DNS szervereket** a hálózati kliensek számára. A képen a Windows Server **DHCP konzolja** látható, amely több **DHCP tartományt (scope)** kezel. Ezek a tartományok különböző VLAN-okhoz vannak rendelve.



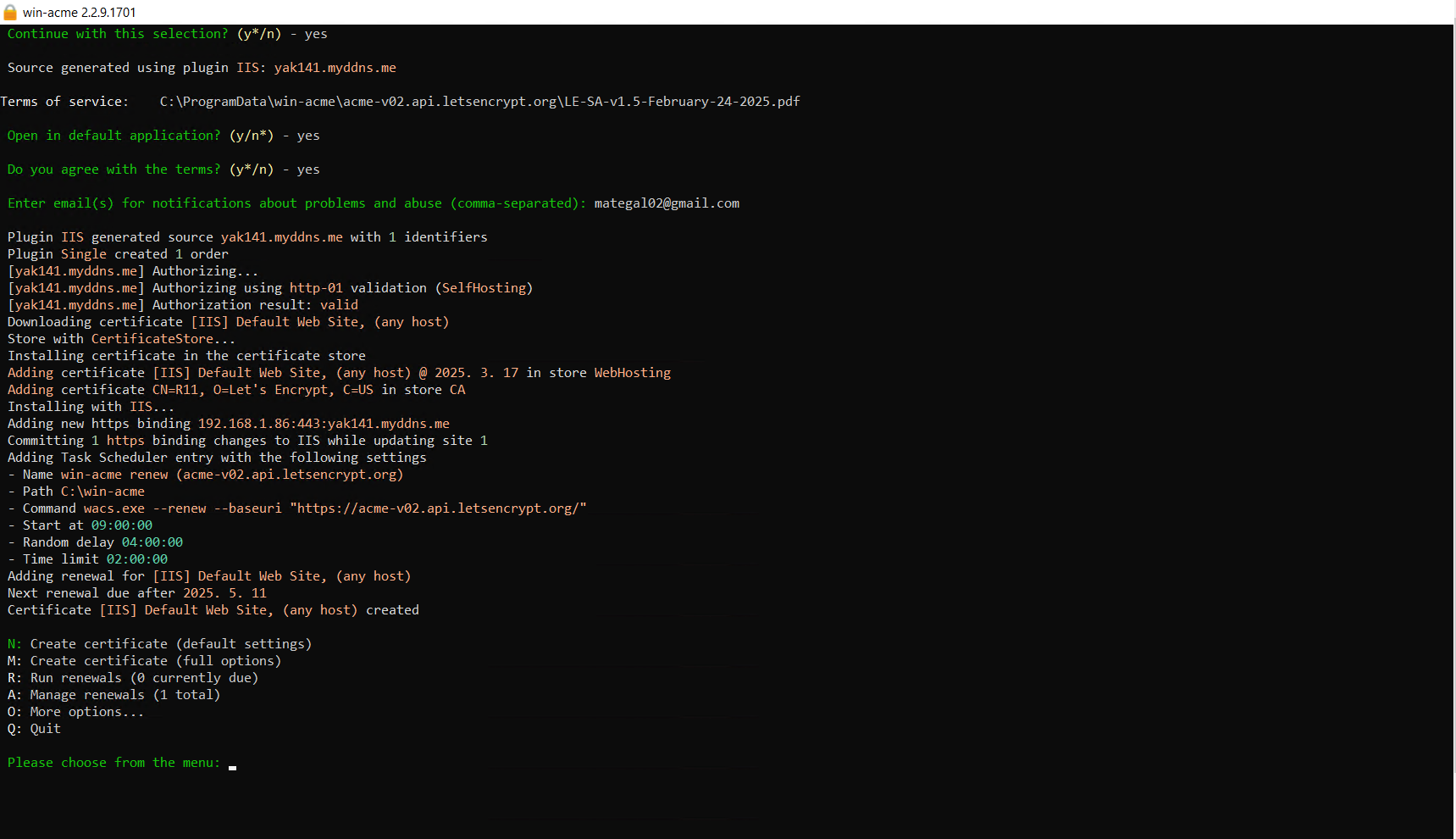
## Windows IIS HTTPS:

Az Internet Information Services (IIS) egy Microsoft által fejlesztett webszerver, amely támogatja mind a **HTTP** (80-as port), mind a **HTTPS** (443-as port) protokollokat. A képen látható konfiguráció azt mutatja be, hogyan lehet egy **HTTPS-alapú biztonságos kapcsolatot beállítani** egy weboldalhoz az IIS-ben.



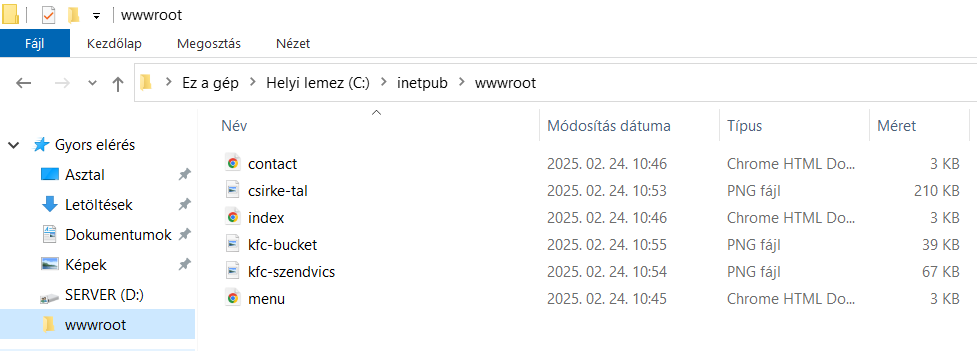
## Windows Win-AcMe:

A **Win-AcMe** egy ingyenes és nyílt forráskódú eszköz, amely lehetővé teszi a **Let's Encrypt SSL-tanúsítványok** automatikus létrehozását és megújítását Windows rendszeren, különösen az **IIS (Internet Information Services) webszerverhez.** A képen egy SSL generálás folyamata látszódik.



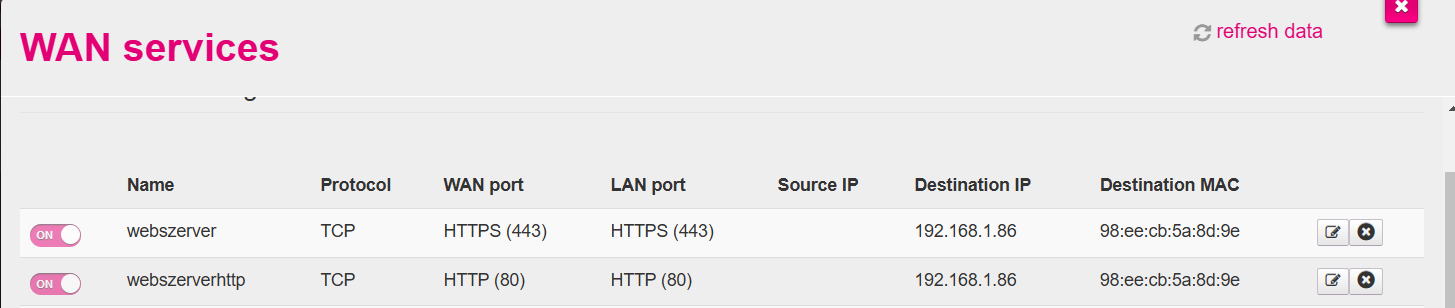
## Windows HTML Struktúra:

Ez a kép az IIS webszerver **wwwroot** mappájának tartalmát mutatja. A **wwwroot** az alapértelmezett gyökérkönyvtár az IIS (Internet Information Services) alatt, ahol a kiszolgált **HTML és egyéb webes fájlok** találhatóak.



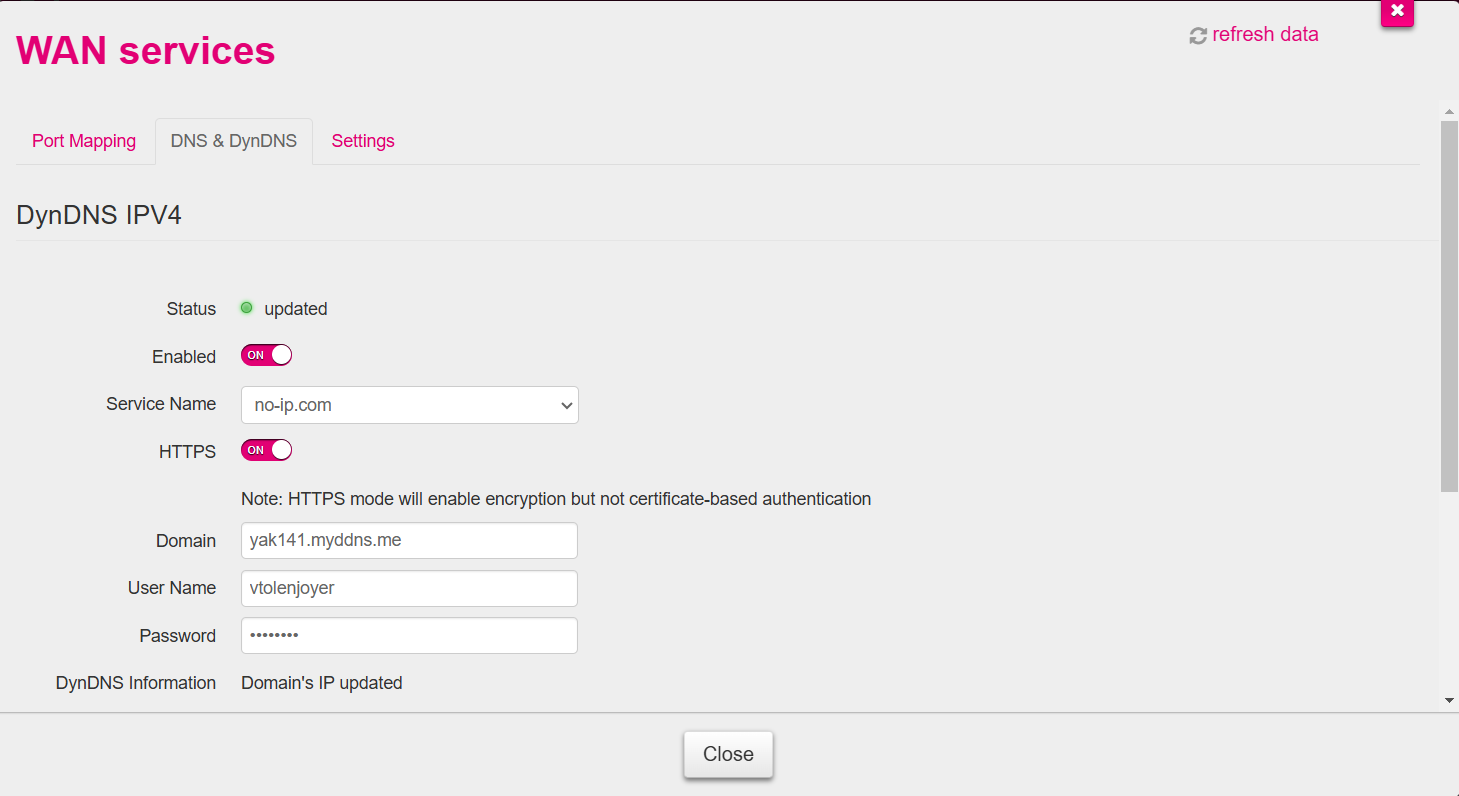
## Windows IIS Tűzfalszabály:

Ez a kép egy **tűzfalbeállítást és porttovábbítást** mutat egy Windows alapú **IIS webszerverhez**. Ez a beállítás lehetővé teszi, hogy a **Windows IIS webszerver** mind a helyi hálózaton (LAN), mind az interneten (WAN) keresztül elérhető legyen a **80-as és 443-as portokon.** Ha nyilvánosan elérhető szervert üzemeltetsz, fontos az **SSL használata és a megfelelő biztonsági beállítások alkalmazása.**



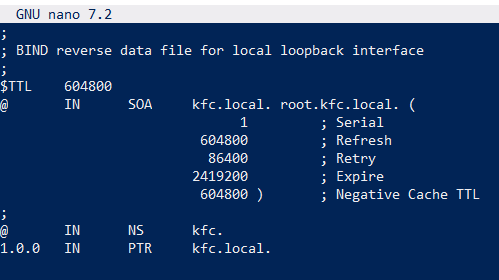
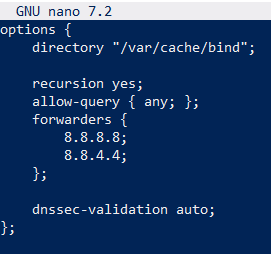
## Windows IIS DNS:

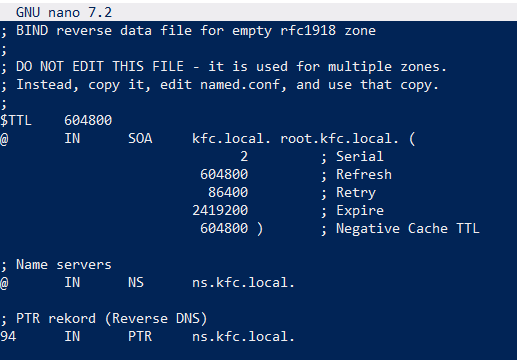
Ez egy **Dynamic DNS (DynDNS) konfigurációs oldal** egy router vagy tűzfal beállításaiban. A DynDNS lehetővé teszi, hogy egy **változó IP-címmel rendelkező hálózat** egy **állandó domain néven** legyen elérhető az interneten keresztül.

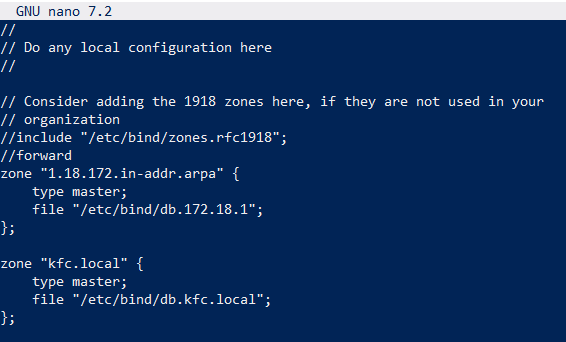


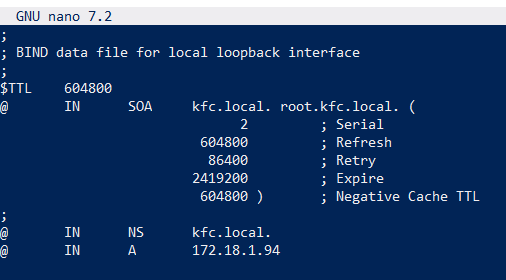
## 2.13 Linux Szerver DNS:

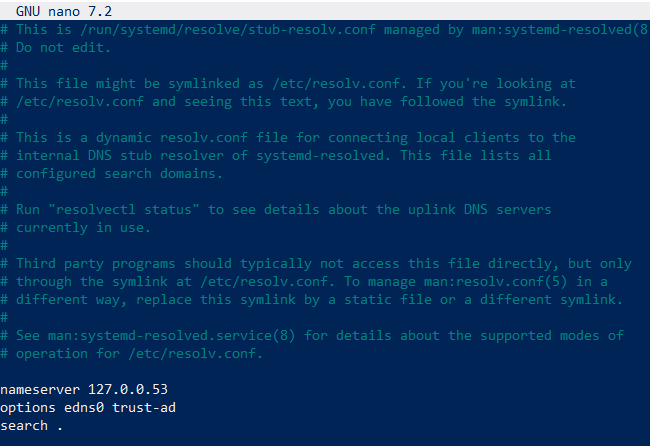
A **BIND9 (Berkeley Internet Name Domain)** a leggyakrabban használt DNS-szerver szoftver Linux és UNIX rendszereken. Fő célja a névfeloldás, vagyis a **domainnevek (pl. google.com) IP-címekké alakítása** és fordítva. A BIND9 egy **rugalmas és erőteljes DNS-szerver,** amely lehetővé teszi a hálózat számára a **gyors és hatékony névfeloldást**, mind **előre**, mind **visszafelé**. Ideális **helyi hálózatok, vállalati infrastruktúrák** és **internetszolgáltatók számára** is. Az alábbi ábrákon azokat a konfigurációs fájlokat látjuk amelyeket a DNS sikeres beállításához kellett alkalmazni.



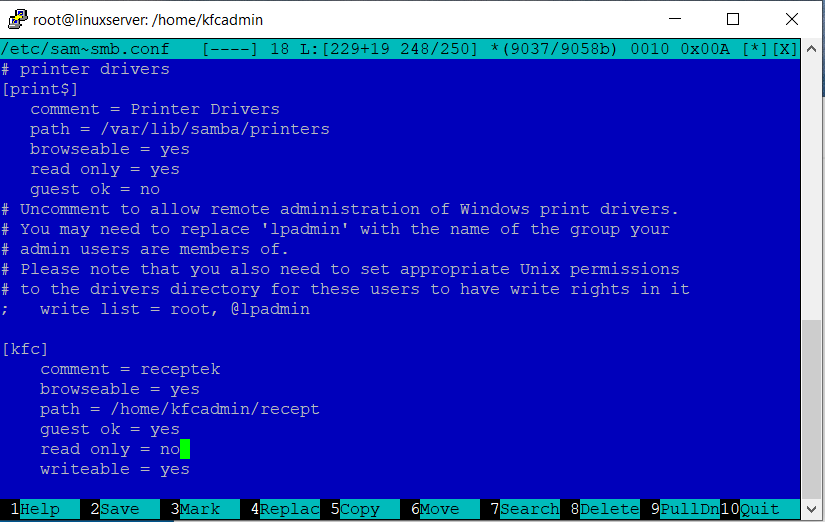
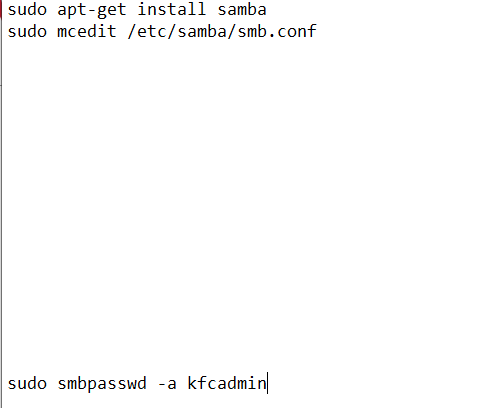






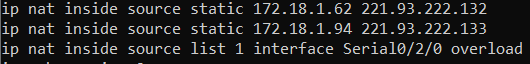


## 2.14 Linux Szerver Samba:

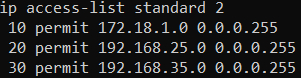
A képen egy **Linux Samba szerver konfigurációja** látható, amely lehetővé teszi a fájlmegosztást a hálózaton belül. Ez különösen hasznos, ha Windows és Linux rendszerek között szeretnénk egyszerű adatcserét biztosítani. A megosztás KFC néven jelenik meg, ami a /home/kfc/recept mappára mutat, ennek a tartalmát lehet írni és olvasni és bárki hozzáférhet. Ennek az eléréshez létrehoztunk egy kfcadmin nevű samba felhasználót.

## 2.15 NAT Címfordítás:

A képen a NAT (Network Address Translation) címfordítás konfigurációja látható. A NAT egy hálózati technológia, amely lehetővé teszi a privát IP-címek nyilvános IP-címekre történő fordítását, így az eszközök elérhetik az internetet. A konfiguráció első két sora statikus NAT beállítását mutatja, ez azt jelenti, hogy a **172.18.1.62** privát IP-cím a **221.93.222.132** nyilvános IP-re lesz leképezve, míg a **172.18.1.94** a **221.93.222.133**-ra. Ez statikus NAT, amelyet általában szervereknél használnak, hogy azok elérhetőek maradjanak kívülről is. A harmadik sor a **dinamikus PAT (Port Address Translation)** konfigurációját mutatja, ez azt jelenti, hogy az **1-es hozzáférési listában** szereplő privát IP-k egyetlen nyilvános IP-címen osztoznak a **Serial0/2/0** interfész segítségével. Az **"overload"** paraméter teszi lehetővé, hogy több eszköz is egy IP-címet használjon, de eltérő portokkal.

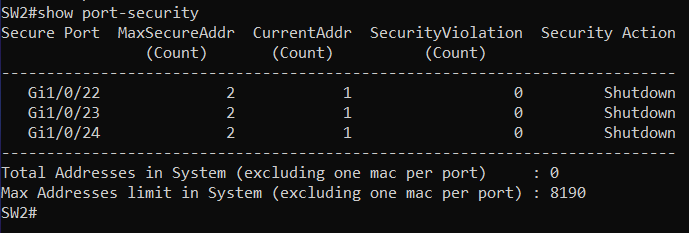
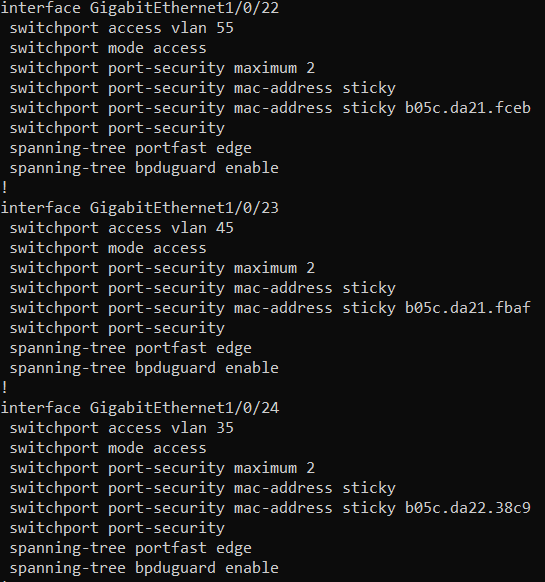
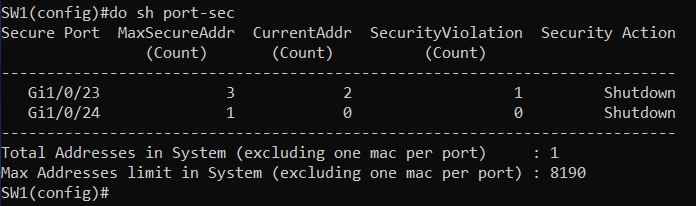
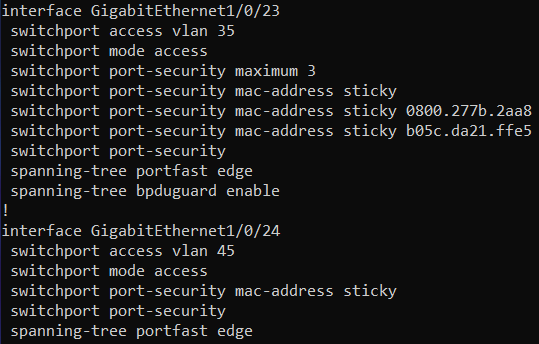


## 2.16 ACL (Access Control List):

A képen egy **ACL (Access Control List)** konfiguráció látható. Az ACL-eket arra használják, hogy forgalomszűrést alkalmazzanak egy adott hálózaton, meghatározva, mely IP-címek vagy hálózatok férhetnek hozzá bizonyos erőforrásokhoz. A standard ACL-ek az IP-forgalmat kizárólag forrás IP-cím alapján szabályozzák, tehát a fenti beállítások lehetővé teszik a listában szereplő hálózatokból érkező csomagok áthaladását, míg minden más implicit módon el lesz utasítva. A József\_Attila\_KFC\_Auchan telephelyen bevan állítva, hogy csak ezekből a hálózatokból lehessen elérni biztonságos távoli eléréssel (SSH) elérni a hálózati eszközöket.

## 2.17 Portbiztonság:

A switch portbiztonsági beállításai korlátozzák, hogy egy interfészen hány eszköz csatlakozhat. A példákban látható, hogy a portokhoz **sticky MAC-címeket** rendeltünk, és **maximális címkorlátokat** állítottuk be. Ha egy porton több eszköz próbál csatlakozni (2-nél több), mint amennyi engedélyezett, a rendszer **shutdown (lekapcsolt)** állapotba helyezi a portot biztonsági okokból.



## 2.18 Forgalomirányítás:

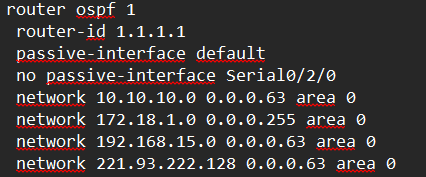
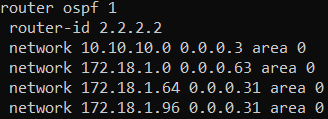
Az **OSPF (Open Shortest Path First)** egy dinamikus irányító protokoll, amelyet IP-hálózatokban használnak az útvonalak automatikus megtanulására és optimalizálására. Az OSPF-et nagyobb, több alhálózatból álló hálózatokban alkalmazzák, hogy a forgalom mindig a legjobb elérhető útvonalon haladjon. Segít a hálózat stabilitásának fenntartásában, gyorsan reagál a hálózatban bekövetkező változásokra, és minimalizálja a kézi konfiguráció szükségességét. Az OSPF-et 1-es process ID-val hoztuk létre, a területet pedig a 0-ás azonosítóval láttuk el mindenhol. Egyterületű OSPF-et használtunk, ezen belül még beállítottuk a Router ID-kat ami egyértelműen azonosítja a Routert az OSPF területen belül.

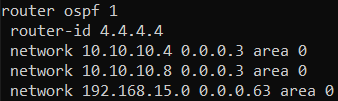
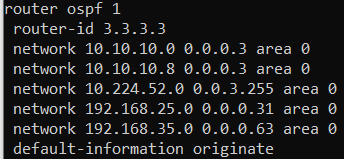
**A Routerek az OSPF segítségével**: -**felismerik egymást** és információt cserélnek az útvonalakról

-k**iszámítják a legrövidebb útvonalat** minden célhálózat felé

-**automatikusan frissítik a táblázataikat**, ha egy útvonal változik vagy elérhetetlenné válik.

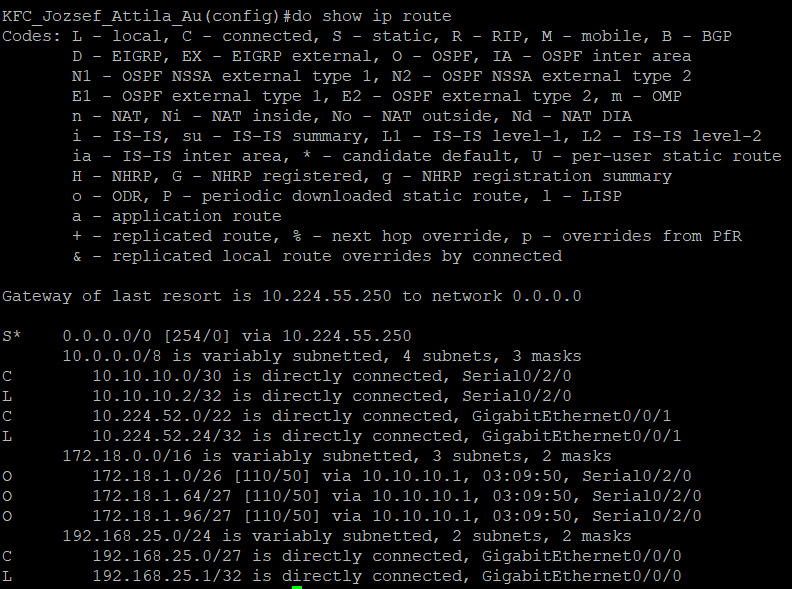
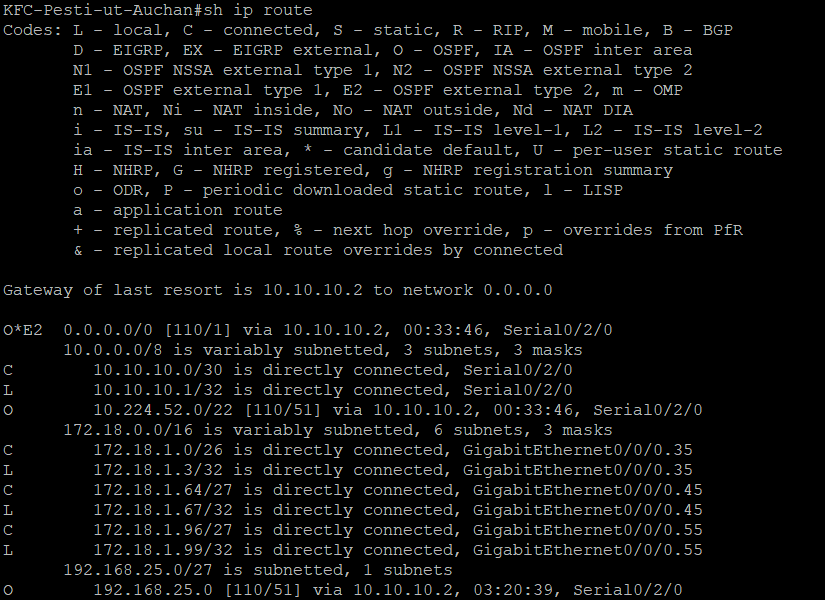
 -**különböző területek között is képesek működni**, ezzel hatékonyabbá téve a nagy hálózatokat.

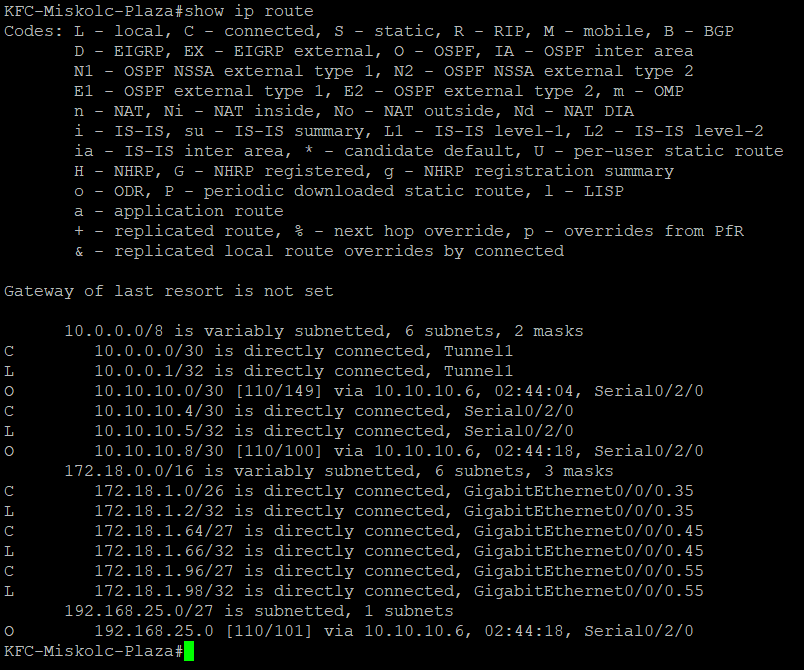
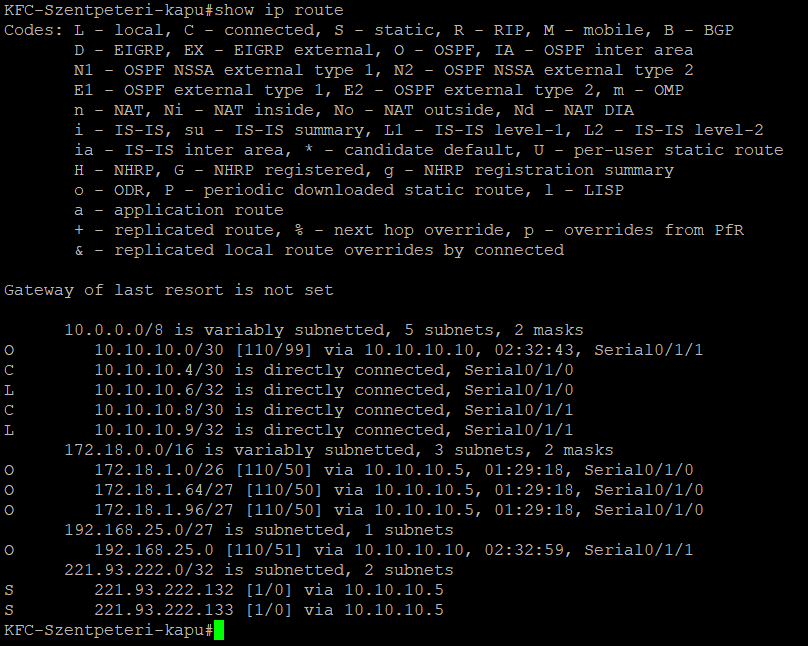






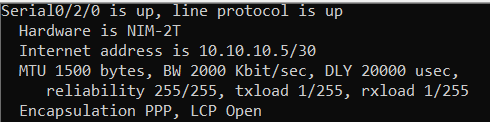
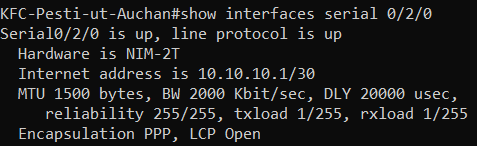
## 2.19 IP Route:

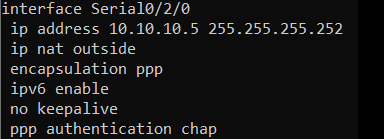
Az IP routing (útválasztás) a hálózatok közötti adatcsomagok irányításának folyamata. Az útválasztók (routerek) az IP-címek alapján döntik el, hogy merre küldjék tovább az adatokat, hogy azok elérjék a céljukat. Az IP routingot arra használjuk, hogy különböző hálózatok közötti adatforgalmat irányítsunk. Ez elengedhetetlen az internet és a nagyobb vállalati hálózatok működéséhez, mivel segít az adatok megfelelő célba juttatásában, akár helyi (LAN), akár távoli (WAN) hálózatok között. A képeken látható routerek különböző helyszíneken találhatók (pl. KFC-József Attila út, KFC-Pesti út-Auchan, KFC-Miskolc-Pláza, stb.), és a hálózatok összekapcsolásáért, valamint az adatok megfelelő célba juttatásáért felelősek.

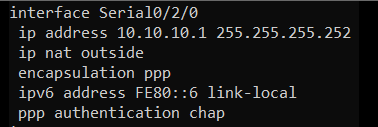


## 2.20 WAN (Wide Area Network):

A képeken egy WAN (Wide Area Network) hálózatot látunk. A routerek különböző telephelyeket kötnek össze soros interfészeken keresztül, és biztosítják az adatok továbbítását a vállalat különböző egységei között. Soros kapcsolaton és PPP hitelesítést alkalmaztunk azon belül CHAP hitelesítést használunk amely biztonságosabbá teszi a kapcsolódást. A PPP helyes működéséhez a szomszédos Routereken felhasználót és jelszót kell létrehozni olyan formába, hogy a szomszéd Router nevét kell megadni és egy egyező jelszót. A NAT lehetővé teszi a belső IP-címek külső címekre való fordítását, ami segíti az internetelérést és a biztonságot.

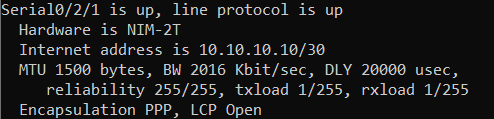
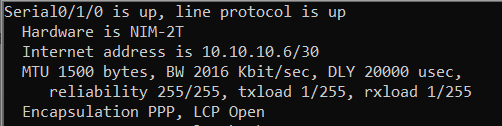


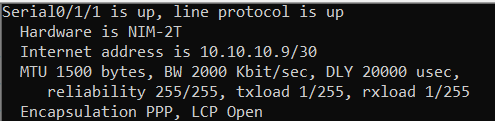
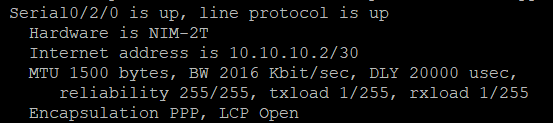


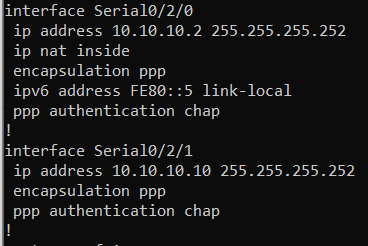
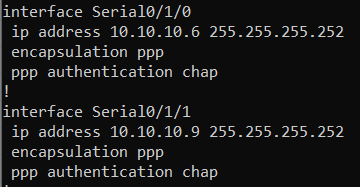








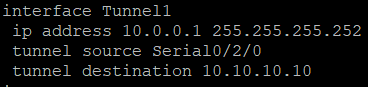
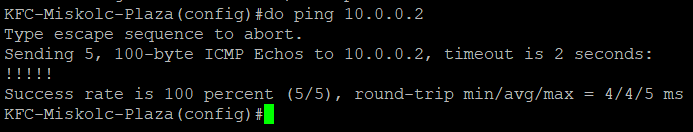
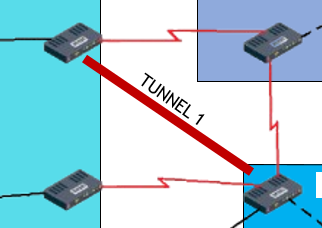
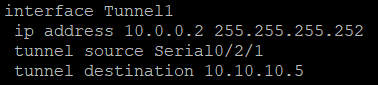
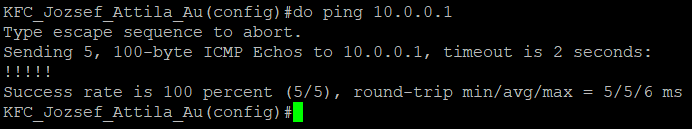






## 2.21 GRE Tunnel **(Generic Routing Encapsulation)**:

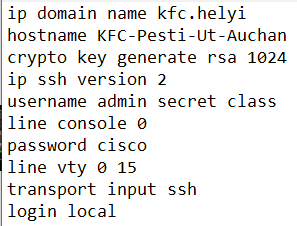
A képeken a **GRE (Generic Routing Encapsulation) alagút** beállításai és működése látható két telephely között, amelyek a **KFC Miskolc Plaza** és a **KFC József Attila Auchan** helyszíneken találhatók. A routerek feladata a hálózatok összekapcsolása és az adatforgalom irányítása. A rendszer célja, hogy egy privát, **titkosítatlan** alagút segítségével összekösse a két különböző telephelyet, lehetővé téve a hálózati forgalom átvitelét egy meglévő infrastruktúrán keresztül. Ez egy **hatékony módszer** a távoli telephelyek közötti összeköttetés megteremtésére anélkül, hogy közvetlen fizikai kapcsolatot kellene kiépíteni.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tunnel | | | | |
| Eszköz | IP | Maszk | Tunnel Forrás | Tunnel Cél |
| KFC Miskolc Plaza | 10.0.0.1 | 255.255.255.252 (/30) | Serial0/2/0 | 10.10.10.10 |
| KFC József Attila Auchan | 10.0.0.2 | 255.255.255.252 (/30) | Serial0/2/1 | 10.10.10.5 |

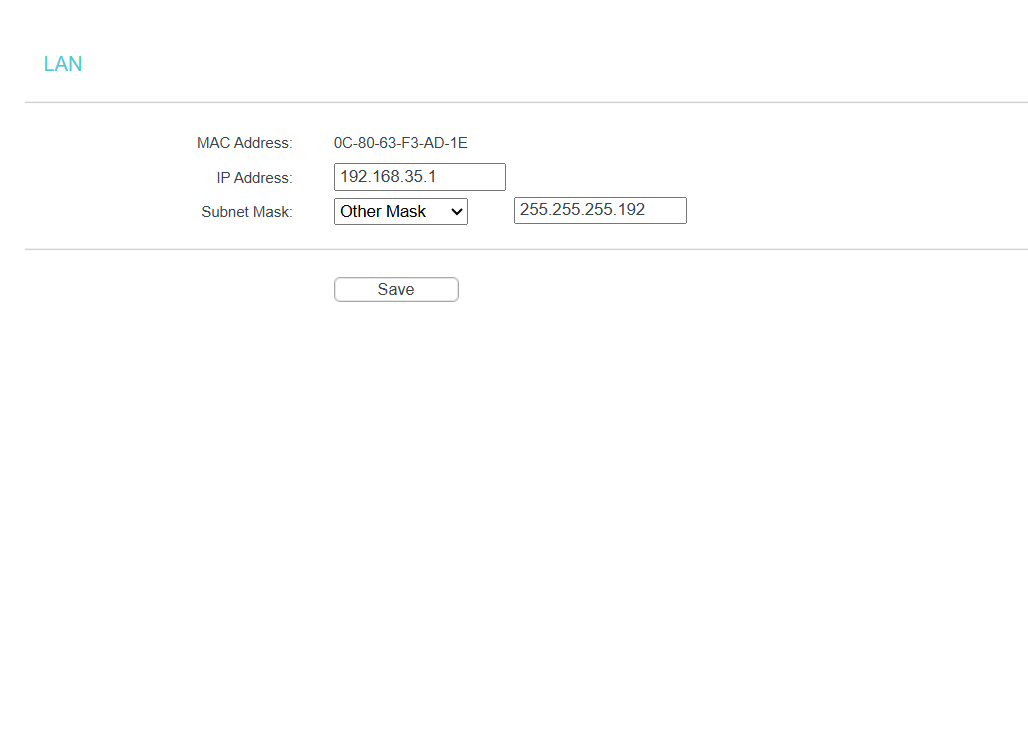
## 2.22 SSH beállítás:

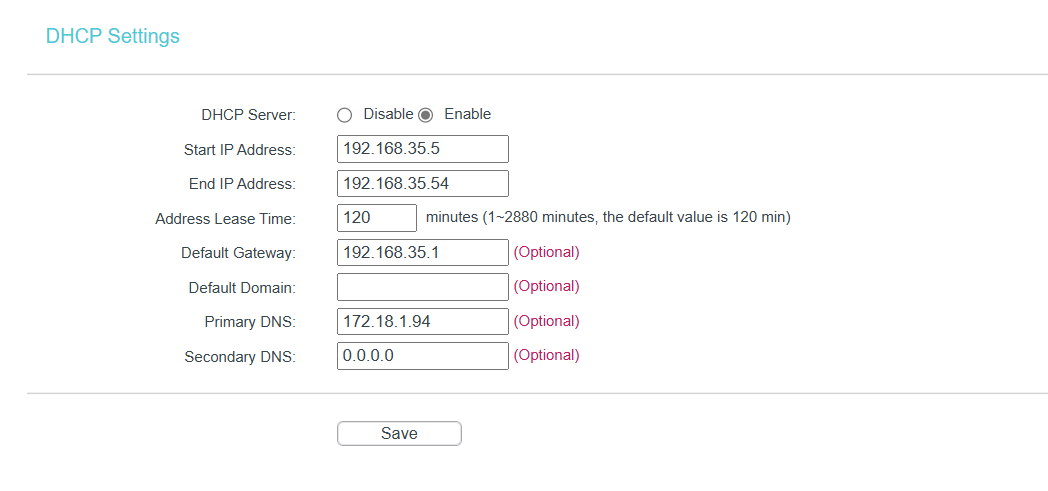
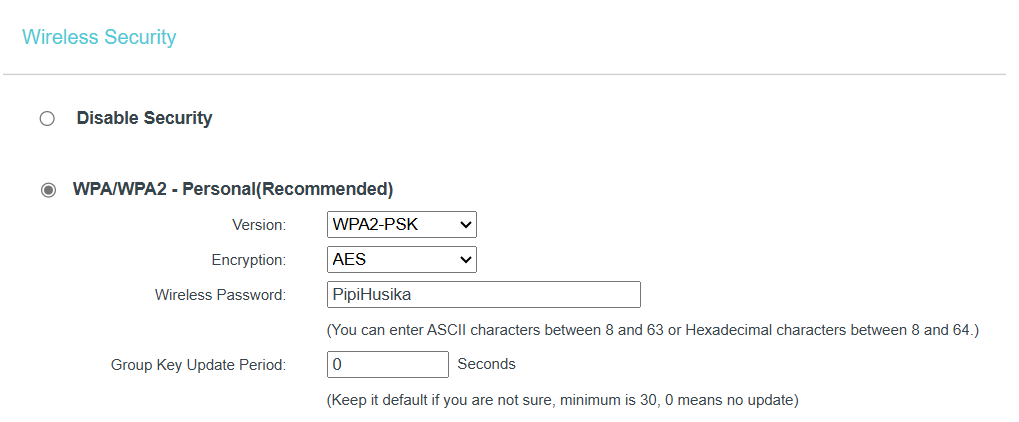
A feltöltött képen **SSH (Secure Shell) beállítások** láthatók. Ez a beállítás lehetővé teszi a **titkosított távoli elérést** a routerekhez SSH-n keresztül, biztonságosabb alternatívát nyújtva a nem titkosított Telnet kapcsolatok helyett. Ezt minden hálózati eszközön létrehoztuk az egyszerűség kedvéért. Minden router egyedi hostnévvel lett ellátva, amely segíti az azonosítást és az adminisztrációt. Az eszköz esetében a **domain név "kfc.hu"**, amely szükséges az SSH titkosítás alapjául szolgáló RSA kulcsgeneráláshoz. A biztonságos kapcsolat érdekében **1024 bites RSA kulcs** került generálásra minden routeren. Az RSA kulcs a titkosított SSH kommunikációhoz szükséges. Bár az SSH működéséhez minimum 768 bites kulcs is elegendő lenne, a **1024 bites titkosítás** már megfelelő biztonságot nyújt. A routerek konfigurációjában **SSH verzió 2 (SSHv2)** került engedélyezésre ami erős hitelesítést és biztonságot létesít. Minden routerhez egyedi **adminisztrátori fiók** lett létrehozva, amelyet a **"admin"** felhasználónév és egy titkosított jelszó véd. A routerek védelme érdekében a konzolos és távoli bejelentkezésekhez szükséges beállítások is definiálásra kerültek. **A** transport input ssh **letiltja a nem biztonságos Telnet kapcsolatokat**, így kizárólag SSH-n keresztül lehet csatlakozni.



## 2.23 WiFi:

A képeken látható WiFi router beállításai a hálózat konfigurációját és biztonságát szabályozzák. A router IP-címe **192.168.35.1**, amely a belső hálózat központi eszköze, azaz a forgalom ezen keresztül zajlik. A DHCP szerver **192.168.35.5 - 192.168.35.54** közötti IP-címeket oszt ki a csatlakozó eszközök számára. A DNS beállítások lehetővé teszik, hogy a hálózat megfelelő névfeloldást végezzen. A WiFi SSID neve **"KFC\_Wireless"**, és **WPA2-PSK** titkosítást használ **AES** algoritmussal, ami biztonságos kapcsolatot biztosít a kliensek számára. A WiFi jelszó **"PipiHusika"**, amelyet a csatlakozó eszközöknek meg kell adni.





## 2.24 DHCP Routerek:

A képen látható DHCP konfiguráció célja, hogy két különböző hálózati szegmens számára automatikusan IP-címeket osszon ki a megfelelő routereken keresztül. A DHCP (Dynamic Host Configuration Protocol) lehetővé teszi, hogy a hálózati eszközök automatikusan kapjanak IP-címet anélkül, hogy manuálisan kellene beállítani őket. A konfigurációban két különböző router szolgáltatja az IP-címeket a különböző helyszínekhez, az adott hálózati beállításokkal. Ez csökkenti az adminisztrációs terheket és biztosítja a hatékony hálózati működést.

**1. DHCP pool – József Attila Auchan KFC**

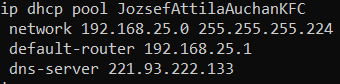
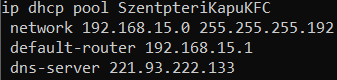
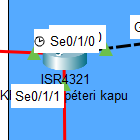
* A hálózat címe: **192.168.25.0/27** (255.255.255.224)
* Az alapértelmezett átjáró (default-router): **192.168.25.1**
* A DNS szerver címe: **221.93.222.133**

Ez a beállítás biztosítja, hogy az adott hálózathoz csatlakozó eszközök dinamikusan kapjanak IP-címet, és az internet vagy más hálózati szolgáltatások eléréséhez az **192.168.25.1** IP-címen keresztül kapcsolódjanak.

**2. DHCP pool – Szentpéteri Kapu KFC**

* A hálózat címe: **192.168.15.0/26** (255.255.255.192)
* Az alapértelmezett átjáró: **192.168.15.1**
* A DNS szerver: **221.93.222.133**

Ez a második DHCP pool ugyanazt a DNS szervert használja, de egy másik hálózati szegmensre vonatkozik.



# Összegzés

A dokumentumban bemutatott konfigurációk célja a hálózati eszközök megfelelő működésének biztosítása, beleértve a routerek, switchek és vezeték nélküli hálózatok beállításait. A csapatmunka megfelelően működött és a feladatot egy-két nehézség ellenére (pl.: ACL, NAT, DNS, ASA stb.) sikeresen teljesítettük. Ha valami bajba akadtunk akkor először a csapaton belül kértünk segítséget és próbáltuk megoldani a problémát, de ezen kívül a különböző csapatokba lévő tagoktól, felkészítő Tanárunktól, fórumokból és ChatGPT-től kértünk segítséget.

