**Informatikai rendszer- és alkalmazás-üzemeltető Technikus**

**-**

**Hálózat tervezési és kivitelezési vizsgaremek dokumentáció**

**-**

**Farkas Gábor, Tóth Ádám, Váradi Kristóf**

# Hálózat tervezés és kivitelezés Vizsgaremek

A hálózatok kiépítésének célja az, hogy egy közepes méretű vállalat 3 fő épületében egy összetett jó védelemmel ellátott hálózatot működtethetünk, ahol mindhárom épület tökéletesen tud működni egymással.

**A vállalat vezetője által meghatározott elvárások következők voltak:** A vállalat 3 fő épülete (Központi iroda, Északi telephely, Déli telephely) között kapcsolat illetve biztonsági védelem létesüljön.

A Központi irodai épület: A Központi irodát Logikailag 3 részre kell bontani VLAN kialakítással, ahol található:

* VLAN 10: Adminisztráció
* VLAN 20: IT
* VLAN 30: Vendéghálózat

Egy laptop/gép biztosítása az Adminnak, gyors problémamegoldás érdekében.

Hardveres Tűzfal extra biztonság érdekében.

Az irodákban VLAN biztosítása, hogy csak az adott Irodán belüli eszközök kommunikálhassanak egymással.

A Központi irodában egy Vezeték nélküli internet biztosítás található, a különféle eszközöknek pl.: Telefon, laptop stb.

# Megvalósítás

A teljes hálózati terv az elvárások alapján:

# Routerek

Az elvárások alapján úgy döntöttünk, hogy 3db Routerrel építjük ki a hálózatot, így Redundáns hálózat alakul ki.

# Redundáns Hálózat

A redundáns hálózat olyan hálózati rendszer, amely több összeköttetést használ egy pont között, hogy biztosítsa a megbízhatóbb és folyamatosabb adatkapcsolatot. A redundáns hálózatok használata jelentősen csökkentheti a hálózati kiesések és a meghibásodások hatását, és javíthatja a hálózat stabilitását és teljesítményét, ami különösen fontos a nagy forgalmú és kritikus üzleti alkalmazások esetén.

A forgalomirányítás az adatok átvitelének irányítására szolgáló folyamat a hálózatban. A routerek között két típusú forgalomirányítás létezik. Statikus és Dinamikus irányítás. A statikus forgalomirányítás esetén a hálózatban az útválasztók statikus beállításokat használnak az adatok továbbítására.ezek az útvonalak nem változnak a hálózati környezet változása esetén. Ez a módszer egyszerű, megbízható és kevesebb erőforrást igényel, de nehezebb kezelni a változó hálózati feltételek esetén. A dinamikus forgalomirányítás esetén a hálózatban az útválasztók automatikusan tanulják meg az optimális útvonalakat az adatok továbbításához. Az útválasztók az útvonalakat dinamikusan meghatározzák a hálózati feltételek és az adatforgalom alapján. Ez a módszer rugalmasabb, mert alkalmazkodni tud a változó hálózati feltételekhez, és lehetővé teszi az optimális útvonalak automatikus kiválasztását, ami hatékonyabbá teszi a hálózatot. Azonban ez a módszer bonyolultabb, és több erőforrást igényel az útválasztási folyamatok végrehajtásához.

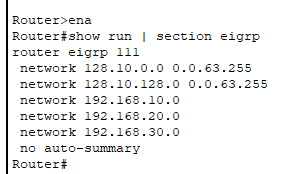
# HSRP Redundancia

A Hot Standby Router Protocol egy Cisco által kifejlesztett redundancia protokoll, amely lehetővé teszi, hogy több router együttműködve egyetlen virtuális átjárót biztosítson egy hálózat számára. Az elsődleges célja a hálózati elérhetőség növelése és a kiesések minimalizálása. Az HSRP működése során egy router aktív szerepet tölt be, míg a többi készenléti állapotban van. Ha az aktív router meghibásodik, a standby router automatikusan átveszi a szerepét, így a hálózati szolgáltatás megszakítás nélkül folytatódik. A protokoll egy virtuális IP-címet és MAC-címet használ, amelyet a kliensek gateway-ként használnak. Az HSRP fontos része a megbízható és folyamatos hálózati működés biztosításának nagyvállalati környezetekben.

**Belső átjáró protokoll** Az EIGRP (Enhanced Interior Gateway Routing Protocol) egy Cisco által fejlesztett, fejlett vektor-alapú routing protokoll, amely ötvözi a távolságvektor és a link-state protokollok előnyeit. Az EIGRP gyors konvergenciát biztosít és hatékonyan kezeli a hálózati útvonalakat a DUAL (Diffusing Update Algorithm) segítségével.

Az EIGRP a közvetlen szomszédokkal kommunikál, és csak a változásokról küld frissítéseket, ezzel csökkentve a hálózati terhelést. Metricáját a sávszélesség, késleltetés, megbízhatóság és terhelés alapján számítja.

Támogatja az IPv4 és IPv6 protokollokat, valamint a VLSM és CIDR rendszereket. Bár kezdetben csak Cisco eszközökön volt elérhető, ma már nyílt szabványként is használható. Az EIGRP megbízható és skálázható választás nagyobb vállalati hálózatokhoz.



**Melyik protokollt használjuk?**

A RIP megfelelő lehet kisebb hálózatok számára, ahol az egyszerű konfiguráció és a kompatibilitás fontosabb, mint a teljesítmény. Az EIGRP viszont nagyobb, összetettebb hálózatokhoz ajánlott, ahol a gyors konvergencia, hatékony útvonalválasztás és skálázhatóság kulcsfontosságú tényezők.

Összegzésképpen elmondható, hogy az EIGRP egy fejlettebb és hatékonyabb protokoll, míg a RIP inkább történelmi jelentőségű, és főként kisebb, egyszerű hálózatokban maradhat életképes megoldás.

# Hálózati Címzési Terv

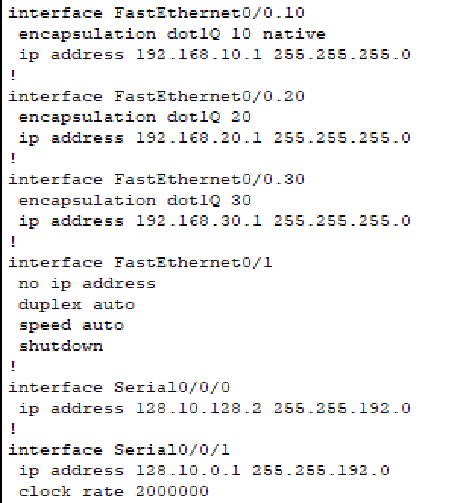
| **Telephely** | **VLAN ID** | **IPv4 hálózat** | **IPv6 hálózat** | **Megjegyzés** |
| --- | --- | --- | --- | --- |
| Központi iroda | 10 | 192.168.10.0/24 | fd00:10: :/64 | Adminisztrációs VLAN |
| Központi iroda | 20 | 192.168.20.0/24 | fd00:20: :/64 | IT VLAN |
| Központi iroda | 30 | 192.168.30.0/24 | fd00:30: :/64 | Vendéghálózat |
| Északi telephely | 40 | 192.168.40.0/24 | fd00:40: :/64 | Gyártási VLAN |
| Déli telephely | 50 | 192.168.50.0/24 | fd00:50: :/64 | Értékesítési VLAN |
| VPN | - | 10.0.0.0/24 | fd00:100: :/64 | VPN hálózat |

# Titkosítás

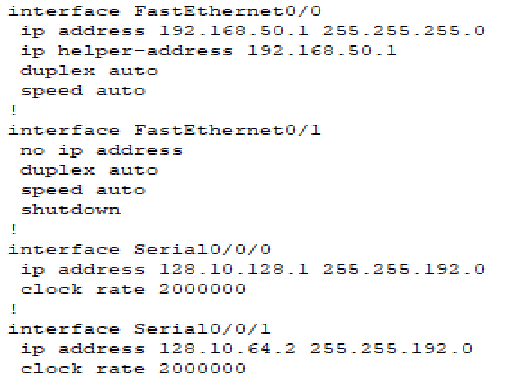
A forgalomirányítók között PPP (Point-to-Point), még hozzá CHAP segítségével.

A CHAP (Challenge-Handshake Authentication Protocol) egy olyan hitelesítési protokoll, amely a kétirányú titkosításon alapul. Ez azt jelenti, hogy mind a kliens, mind a szerver ellenőrzi egymás azonosságát a hálózati kapcsolat felépítésekor. Előnye, hogy a CHAP titkosítás megakadályozza a külső személyek hozzáférését a hálózati kapcsolathoz. Védelmet nyújt a man-in-the-middle támadások ellen. Erősebb védelmet nyújt, mint a szokásos jelszó alapú hitelesítési eljárások. Lehetővé teszi a titkosítási kulcsok rendszeres cseréjét, ami tovább erősíti a biztonságot. A kulcsok rendszeres cseréje megakadályozza az esetleges támadásokat és biztosítja a hálózati kapcsolat folyamatos biztonságát.

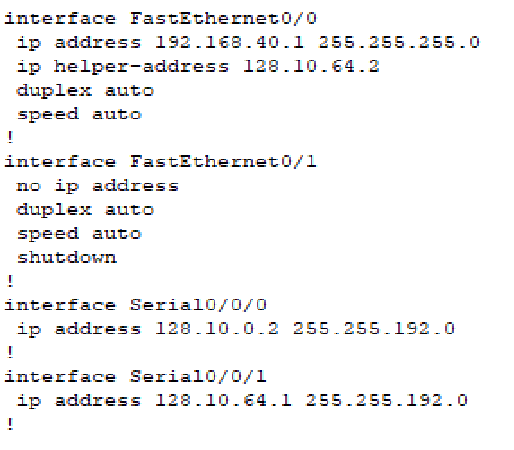
**Központi iroda Router**



**Déli telephely Router**



**Északi telep Router**



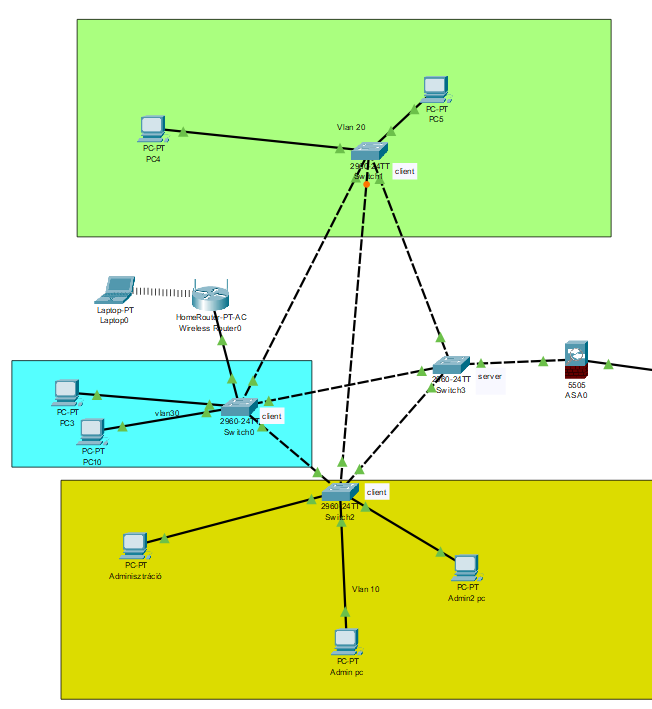
# IPv4 és IPv6

IP cím kiosztásánál legfőképpen IPv4-et használtunk, de a Linux és Windows szervergépnél alkalmaztunk IPv6 címzést is.

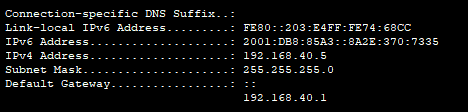
Az IPv4 és az IPv6 az internet protokoll két különböző változata, amelyek a hálózati kommunikáció alapját képezik. Az IPv4 protokoll 32 bites címzést használ, amely 4 bájtból áll. Ez a korlát az internetes fejlődéssel egyre inkább problémává vált, mivel az interneten egyre több eszköz és felhasználó lép fel, ami a rendelkezésre álló IP-címek elfogyását eredményezi. Az Iot és mobilis eszközök terjedésének hatására egyre több címre van szükség, mivel az IPv4 címtartományt az IANA 2011 februárjában osztotta ki az utolsó rendelkezésére álló címtartományt. Ezért vezették be az IPv6-os címzést. Az IPv6 protokoll 128 bites címzést használ, amely 16 bájtból áll. Ez összesen 340 undecillió egyedi IP-címet tesz lehetővé, ami elegendő ahhoz, hogy minden eszköznek és felhasználónak legyen saját IP-címe, és még rengeteg maradjon is.

**Központi iroda épület:**

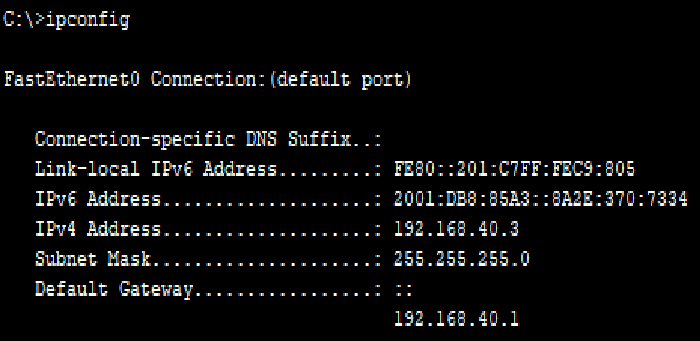
A központi irodát logikailag 3 részre osztjuk Vlan segítségével.



**Windows server IP címe:**



**Linux\_Server IP címe:**



**Windows\_Server:**

A Windows szerveren fut az Active Directory, illetve a fájl-és nyomtató megosztás, és ezen felül automatizált szoftvertelepítés található.

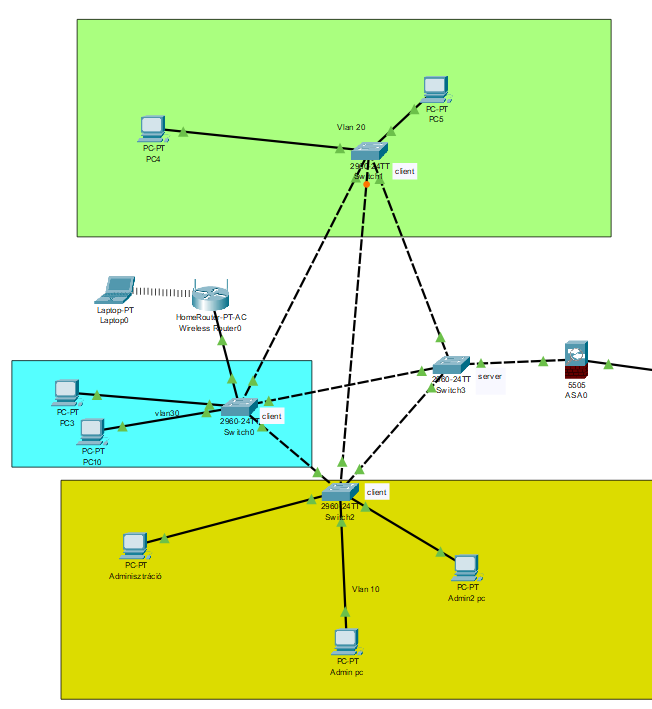
**Linux\_Server:**

A Linux szerveren találhatunk DHCP-t, illetve webkiszolgáló szolgáltatásokat. DHCP-s kiosztást csak a vendégek számára ad. A vizsgateremben letiltottuk a webkiszolgálót, hogy a vizsgázók ne tudják azt elérni.

**Központi iroda:**

A Központi iroda egy külön hálózattal rendelkezik, C osztályú privát hálózat, aminek az IP-címei a következők: 192.168.10.0, 192.168.20.0, 192.168.30.0

A Központi irodában 4db Switch helyezkedik el, az STP protokoll miatt.



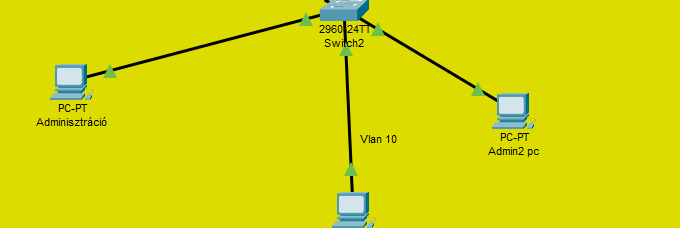
# STP protokoll

Az STP (Spanning Tree Protocol) használata jelentős előnyöket nyújt a hálózatkezelők számára, különösen azokban a hálózatokban, ahol több kapcsoló található. Az STP segít megelőzni a hurokba csatlakozásokat, amelyek létrehoznak redundáns összeköttetéseket a hálózatban, és komoly problémákat okozhatnak, mint például a forgalom túlterhelése vagy a hálózati összeomlás. Az STP működése során a hálózati topológiát ellenőrzi, és automatikusan kikapcsolja a felesleges összeköttetéseket, így biztosítva, hogy csak egy útvonal maradjon aktív minden pont között a hálózaton, ezzel javítva a hálózat stabilitását és megbízhatóságát. Van egy Primary (Elsődleges) illetve egy Secondary (Másodlagos) kapcsolónk, a még nagyobb stabilitás érdekében. A Központi irodát logikailag 3 részre bontottuk. 1 Adminisztráció Vlanra, 1 IT Vlanra illetve 1 Vendég Vlanra.

# VLAN

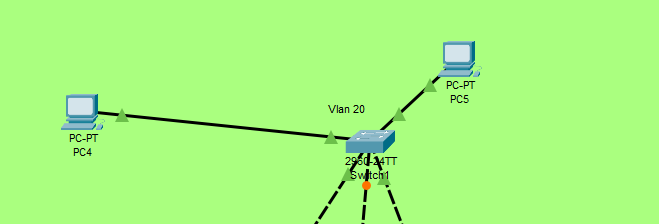
A VLAN (Virtual Local Area Network) egy rendkívül hasznos technológia, amely lehetővé teszi a hálózati erőforrások hatékonyabb használatát és a hálózati biztonság javítását. A VLAN-ok segítségével lehetőség van arra, hogy logikailag elkülönítsük a hálózati eszközöket és szegmenseket, így a hálózati forgalom jobban szervezhető és ellenőrizhető. VLAN-ok csökkentik a hálózati torlódásokat és javítják a hálózat sebességét és átviteli teljesítményét. Lehetővé teszi a hálózat adminisztrátorai számára, hogy korlátozzák a felhasználók hozzáférését bizonyos erőforrásokhoz, mint például a fájlszerverekhez vagy az érzékeny adatokhoz. 3 darab VLAN-t hoztunk létre, egy Adminisztáció, IT Vlant és egy Vendéghálózat Vlan-t.

**Az Adminisztráció VLAN 10-es számú:**



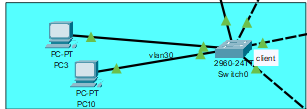
Az Adminisztráció Vlanban 3db Pc helyezkedik el.

**IT VLAN 20-as számú:**



Az IT Vlanban 2db PC helyezkedik el.

**Vendéghálózat Vlan 30-as számú:**



**A Vendéghálózat Vlanban 1 db PC található**

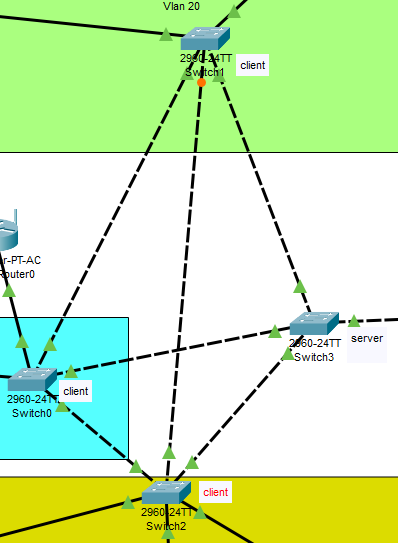
A kapcsolók a VLAN-okhoz VTP segítségével férnek hozzá, így nem kell manuálisan egyesével konfigurálni a Switcheket a VLANok miatt.

# VTP Protokoll

A VTP (Virtual Trunk Protocol) fő előnye az, hogy egyszerűsíti a VLAN-konfigurációt és kezelést, mivel a VTP lehetővé teszi a VLAN-információk automatikus terjesztését a hálózaton. Ennek köszönhetően ha egy új VLAN-t hoznak létre egy kapcsolón, akkor a

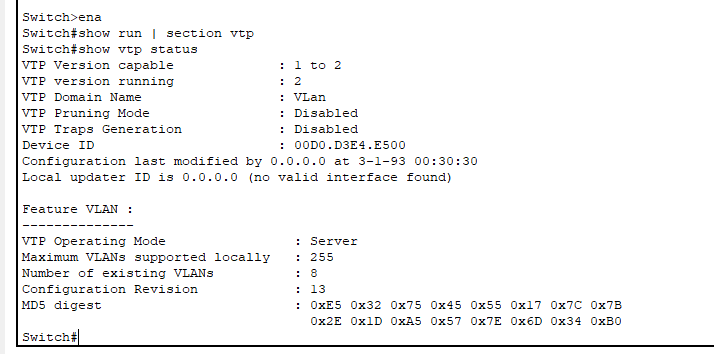
VTP automatikusan továbbítja ezt a változást a többi kapcsolónak is. **A VTP-nek 3 módja van:**

* Server: Kiszolgáló, ami hirdeti a VLAN-okat.
* Client: Szerver által kapott VLAN-okat hirdeti.
* Transparent: Szerver által hirdetett VLAN-okat nem veszi figyelembe, de továbbadja más kapcsolóknak.

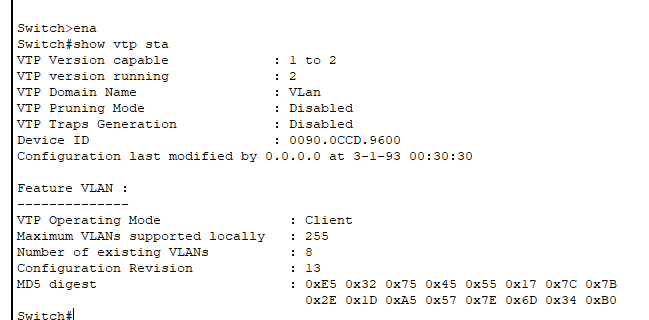


A hálózatban 1 Server és 3 Client található. Annak érdekében hogy ha az egyik kapcsoló meghibásodik(Primary) akkor a Secondary (VTP root) kapcsoló át tudja venni a helyét. 3 Client kapcsoló pedig hirdeti a

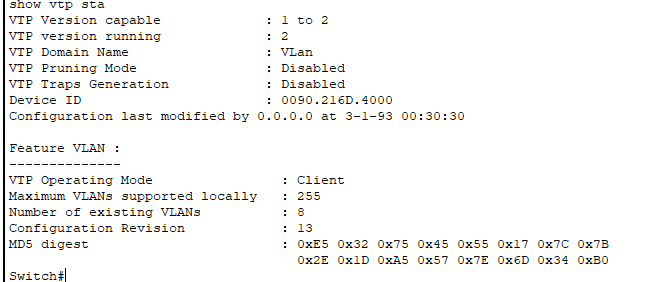
VTP-ket a megadott interfészeknek. **Switch3:**



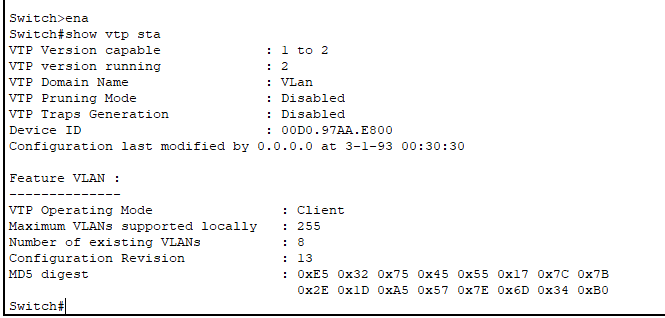
**Switch1:**



**Switch0:**



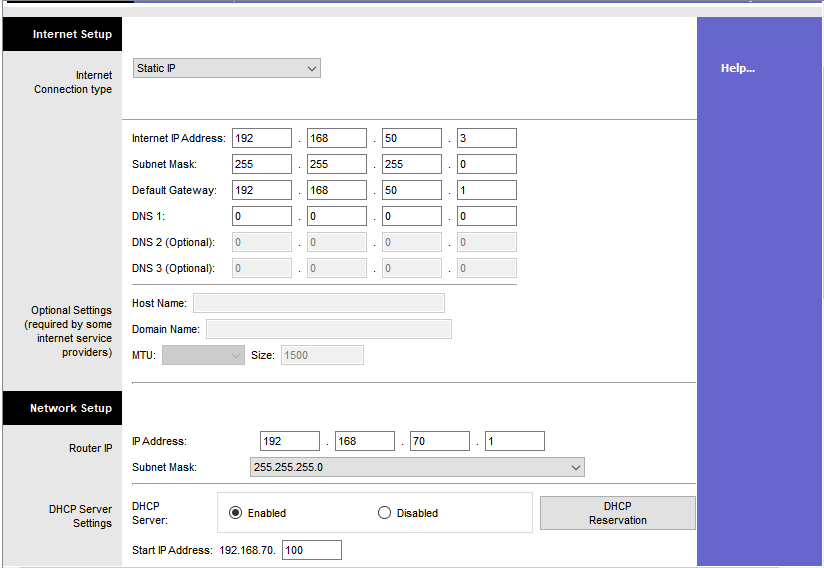
**Switch2:**

****

# Vezeték nélküli forgalomirányító

A WiFi egy vezeték nélküli kommunikációs technológia, amely lehetővé teszi az eszközök közötti adatátvitelt az interneten keresztül. A WiFi-t általában egy routerrel kapcsolják össze, amely egy vezetékes internetkapcsolatot konvertál vezeték nélküli jelekké. A 2,4 GHz és 5 GHz azok a frekvenciasávok, amelyeket a WiFi használ a kommunikációhoz. A 2,4 GHz-es sáv széles körben elterjedt és olcsóbb, de kisebb sávszélességet és kevesebb csatornát kínál, a teljesítmény csökkenhet több eszköz használatakor. A 5 GHz-es sáv kisebb terjedési távolságot kínál, de nagyobb sávszélességet és több csatornát biztosít, amely lehetővé teszi a nagyobb adatátviteli sebességet.

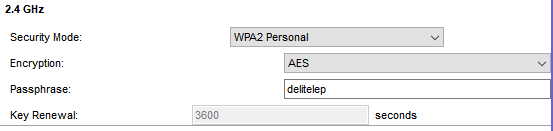
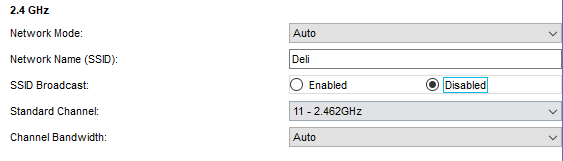
**A Déli telephely Wifi Router konfigurálása:**



A WIFI Routernek SSID-t nem hirdetünk, és jelszóval levédettük.

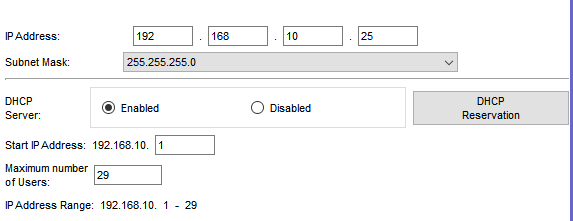
Az SSID egy rövidítés a "Service Set Identifier" kifejezésből, és egy azonosító, amelyet a WiFi-hálózatok használnak azonosítására. Az SSID-t a router beállításai között lehet konfigurálni, és lehetővé teszi a felhasználók számára, hogy azonosítsák és csatlakozzanak a megfelelő hálózathoz. Router Biztonságát WPA2 PSK-vel biztosítottuk.

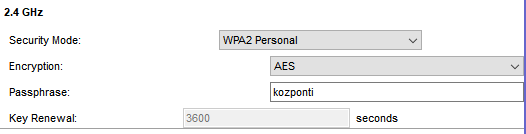
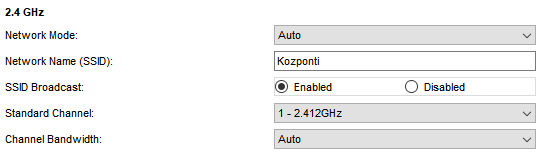
A WPA2 PSK védelem a Wi-Fi Protected Access 2 előírásokon alapuló biztonsági protokoll, amely kódolással védi a WiFi-hálózatot a nem kívánt felhasználók ellen. A PSK rövidítés a "Pre-Shared Key" kifejezésből származik, és azt jelenti, hogy a hálózathoz csatlakozó eszközök egy előre meghatározott jelszót használnak a hálózatba való bejelentkezéshez.

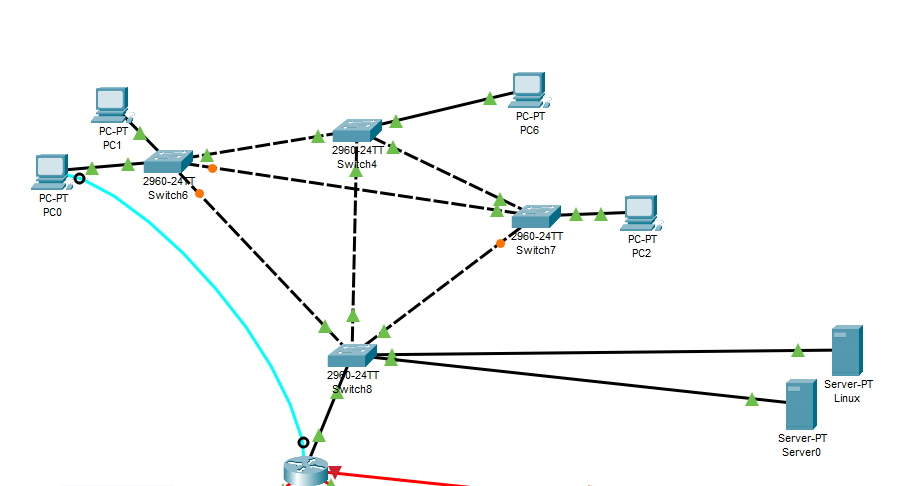


**Központi telephely WiFi router:**

A vendéghálózathoz elhelyeztünk egy WiFi routert, hogy egyszerűbb legyen a hálózatra való csatlakozás.

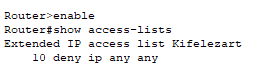






Az Északi telephelyben DHCP-sen kapnak IP címet a LINUX\_SERVER Szervergéptől. Az IP-címeket 192.168.40.11-től osztja ki a gépeknek. A 4 kapcsoló STP protokollt használ, hogy a Redundáns hálózatban ne alakulhasson ki szórási vihar. Ugyan úgy mint a Központi irodában, itt is van egy elsődleges, és egy másodlagos kapcsoló.

# Access Control List

Az Acces Control List-tel beállítottuk, hogy a Központi irodában a Vlanok ne lássanak ki az internetre, csak a belső hálózatot látják. Az ACL egy olyan technológia, amelynek használata számos előnnyel jár a hálózat biztonság terén. Az ACL lehetővé teszi a hálózatkezelők számára, hogy hatékonyan kezeljék az hálózati forgalmat és az erőforrásokhoz való hozzáférést azáltal, hogy meghatározzák, mely felhasználók vagy csoportok milyen típusú hálózati erőforrásokat használhatnak. Az ACL lehetővé teszi a hálózatkezelők számára, hogy pontosan meghatározzák, mely erőforrásokat használhatják a felhasználók, így csökkentve a jogosulatlan hozzáférések kockázatát. Lehetővé teszi továbbá, hogy meghatározzák a forgalom prioritását, valamint szabályozzák a forgalmat azáltal, hogy blokkolják a nem kívánt forgalmat.

# FTP

Az FTP (File Transfer Protocol) egy olyan protokoll, amely lehetővé teszi a fájlok biztonságos és hatékony átvitelét az interneten keresztül. Az FTP rendkívül hasznos lehet azok számára, akiknek rendszeresen szükségük van nagy fájlok. Az egyik legnagyobb előnye az FTP-nek az adatbiztonság. Az FTP használata lehetővé teszi, hogy a fájlok biztonságosan kerüljenek átvitelre, mivel a protokoll titkosítást használ a fájlok védelme érdekében. Ez azt jelenti, hogy az adatok csak a két végpont között lesznek továbbítva, és senki más nem férhet hozzájuk.