**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.

Iroda részleg:

3 terem biztosítása:

* 1 igazgató illetve igazgatóhelyettes iroda
* 1 titkár és titkárhelyettes iroda
* 1 meeting terem

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

Meeting teremben Vezeték nélküli internet biztosítása, a különféle eszközöknek pl.: Telefon, laptop stb.

Az osztálytermek:

Két részre legyen bontva. Egy Vizsgáztató terem és osztálytermek.

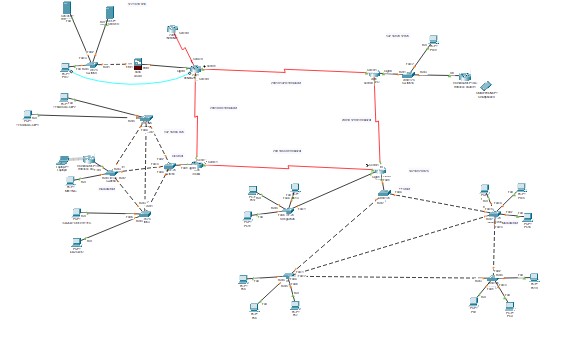
Az osztálytermekben Dinamikusan ossza ki az IP címeket a szervergép.

A vizsgateremben a vezetőség kérésre letiltottuk ACL segítségével a szerverek HTTP és FTP szolgáltatásait.

Az étkezőben legyen lehetőség vezeték nélküli kapcsolatra, illetve a konyhafőnöknek biztosítsunk egy PC-t amely FTP szolgáltatást lát el. Ezzel segítve a konyhai dolgozók munkáját a hozzávalók beszerzésében.

# Megvalósítás

A teljes hálózati terv az elvárások alapján:



# Routerek

Az elvárások alapján úgy döntöttünk, hogy 4db Routerrel építjük ki a hálózatot, így Redundáns hálózat alakul ki.

# Redundáns Hálózat

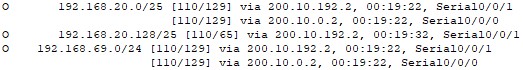
A redundáns hálózat olyan hálózati rendszer, amely több összeköttetést használ egy pont között, hogy biztosítsa a megbízhatóbb és folyamatosabb adatkapcsolatot. A redundáns hálózatok használata jelentősen csökkentheti a hálózati kiesések és a meghibásodások hatását, és javíthatja a hálózat stabilitását 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.

**Belső átjáró protokoll** A routerek közötti kommunikációt OSPF segítségével oldottuk meg. Az OSPF dinamikus irányító protokoll, amely lehetővé teszi a hálózati topológia automatikus észlelését és az útvonalak dinamikus számítását. Ez azt jelenti, hogy az OSPF által biztosított útvonalak mindig a legfrissebb hálózati információkra épülnek, és automatikusan frissülnek, amikor a hálózat változik. Nagyon skálázható, az OSPF hálózatok nagyon nagy méretűek lehetnek, és számos különböző hálózati eszközt támogatnak, beleértve a router-eket, a switch-eket és a tűzfalakat is. Az OSPF redundáns útvonalakat biztosít, ami azt jelenti, hogy ha egy útvonal meghibásodik, akkor az OSPF automatikusan új útvonalakat keres a hálózaton keresztül.

**Miért választottuk az OSPF-et a RIP helyett?**

Mivel Az OSPF lehetővé teszi a teljes topológiai információ megosztását, és jobb útválasztást biztosít a hálózatban. Továbbá több útválasztási metrikát képes figyelembe venni, amely lehetővé teszi a hálózatban lévő adatforgalom optimális útvonalon történő irányítását.

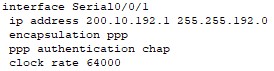
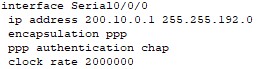


# Titkosítás

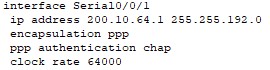
A forgalomirányítók között PPP (Point-to-Point), még hozzá CHAP segítségével.

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.

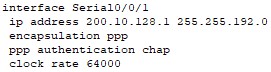
**RENDSZERGAZDA Router**



**IRODA Router**



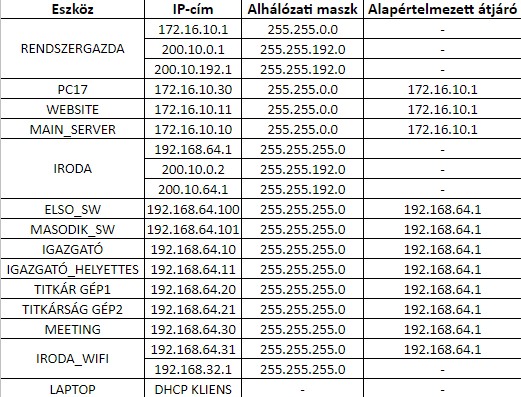
**TERMEK Router**



**ETKEZO Router**

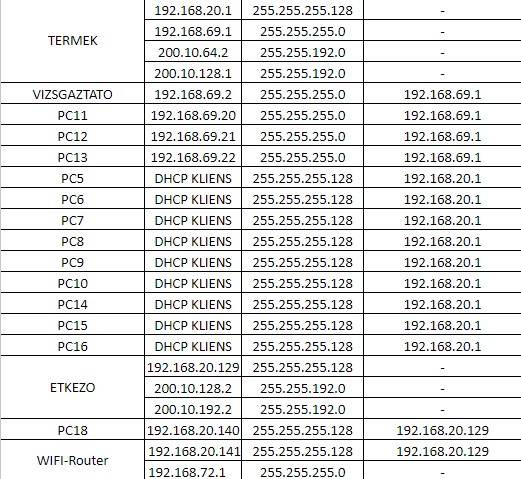


**Kiosztott hálózati Ip címek:**



**Linux szervergép IPv6os változata:**





# IPv4 és IPv6

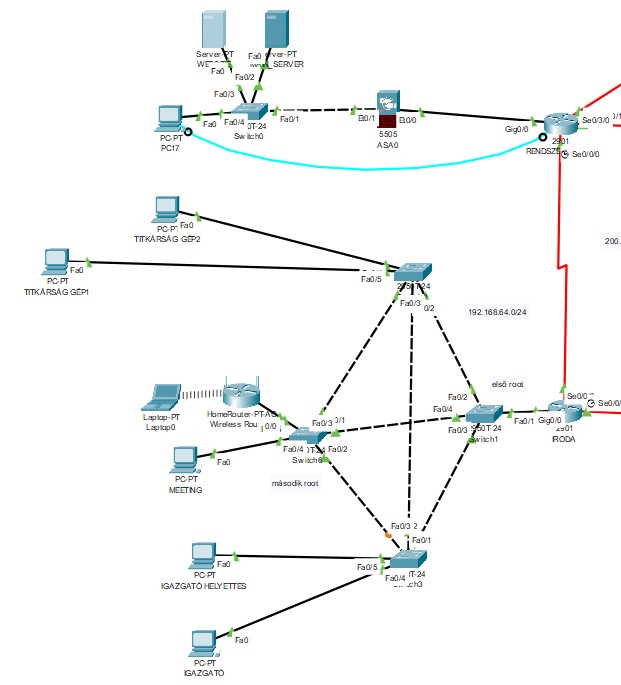
IP cím kiosztásánál legfőképpen IPv4-et használtunk, de a Linux

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.

**Irodai épület:**

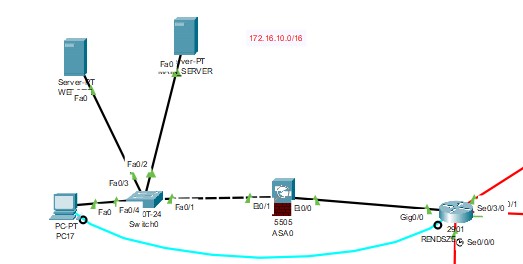
Az iroda ketté bontása érdekében, a két részt 1-1 Routerrel építjük ki. Illetve mindkét szoba rendelkezik saját IP címmel.



A Rendszergazdai Router 172.16.10.0/16 hálózatú IP címmel rendelkezik.



**Admin Szoba:**



Ide építettünk ki a hardveres tűzfalat. A két szerver illetve a rendszergazda PC-je itt található. Az egyik szervergép a Webszerver, a másik pedig Main\_Server a további szolgáltatások biztosítására alkalmazott ilyen például: DHCP, FTP. Mi legfőképpen DHCP-s IP kiosztásra alkalmaztuk. A DHCP (Dynamic Host Configuration

Protocol) egy hálózati menedzsment protokoll, amely az alkalmazás rétegben található. Segítségével az Internet Protokoll IP-címet dinamikusan hozzá lehet rendelni bármilyen eszközhöz vagy csomóponthoz, hogy ezek az IP-vel kommunikálhassanak. A DHCP alapvető célja egy egyedi IP-cím hozzárendelése a hostokhoz. Egyéb hálózati címeket is biztosít(Alhálózati maszk, DNS, Router címe, Osztály azonosító). Kétféleképpen jön létre, azaz kliensként és szerverként jön.

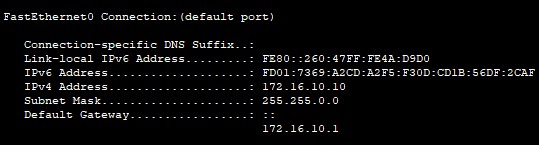
**Előnye:**

* Egyszerűbbé teszi a hálózat bővítését
* IP címeket központilag üzemelteti
* Az IP címek újra felhasználhatók, ezáltal minimalizálva az összes IP cím igényét.
* DHCP-kiszolgálón lévő IP-címtér újrakonfigurálható anélkül, hogy az ügyfelek egyenként kellene újrakonfigurálni.

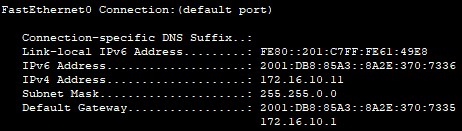
**Hátránya:**

* Konfliktusok IP címek kiosztása közben.

**Main\_Server IP címe:**



**Linux\_Server IP címe:**

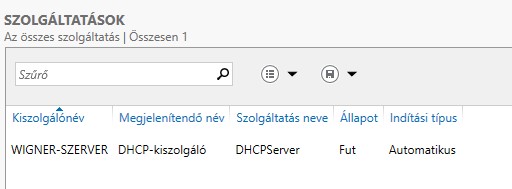


Továbbá az Admin PC-t összekötöttük konzolos kapcsolattal (SSH) a RENDSZERGAZDAI azonosító routerrel. Az SSH (Secure Shell) egy kriptografikus protokoll, amely lehetővé tesz biztonságos kapcsolatot a kliens és a szerver között .Ez a kapcsolat továbbá lehetővé teszi, hogy a hálózati eszközökhöz hozzárendelt személyek kizárólagos hozzáférést kapjanak, így megakadályozva a jogosulatlan hozzáférést és védelmet biztosít a hálózat számára. Létezik egy más fajta protokoll, a TELNET. A Telnet egy hálózati protokoll amely nem használ titkosítást, így az adatok nyilvánosak lehetnek. Ezzel szemben az SSH az adatokat titkosítja, így azok nem olvashatók vagy megfigyelhetők, ha valaki kívülről próbálja lehallgatni a hálózati forgalmat. Illetve az SSH támogatja a felhasználói hitelesítést, és lehetővé teszi a felhasználók számára, hogy biztonságosan és hatékonyan hitelesítsenek, bejelentkezhessenek a szerveren.

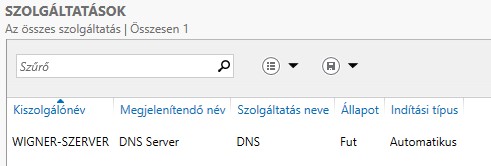
**Main\_Server:**

Ez a Windows szerver DHCP, DNS és FTP szolgáltatásokat biztosít. DHCP-t a Termek épületben került kiosztásra. Kivéve a Vizsgáztató helyiségben. Ott Statikusan kerültek kiosztva az IP címek.

DHCP szolgáltatás

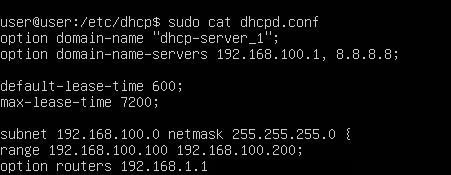


DNS szolgáltatás



**Linux\_Server:**

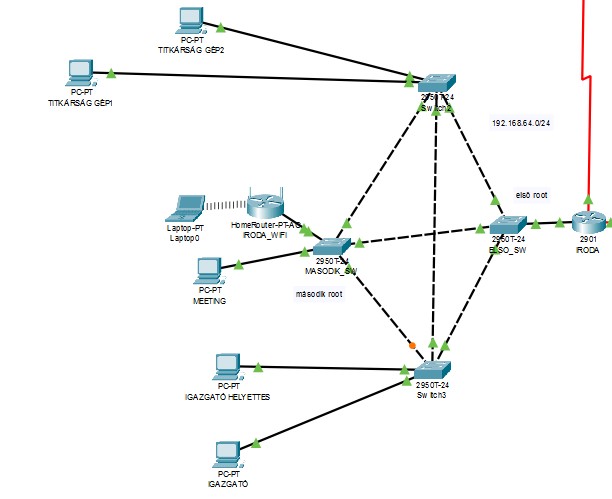
A Linux szintén DHCP-t, illetve webkiszolgáló szolgáltatásokat kezel. DHCP-s kiosztást csak a vendégek számára ad. A vizsgateremben letiltottuk a webkiszolgálót, hogy a vizsgázók ne tudják azt elérni.



**Iroda:**

Az Iroda egy külön hálózattal rendelkezik, C osztályú privát hálózat. (192.168.64.0/24).

Irodában 4db Switch helyezkedik el, STP protokoll miatt.



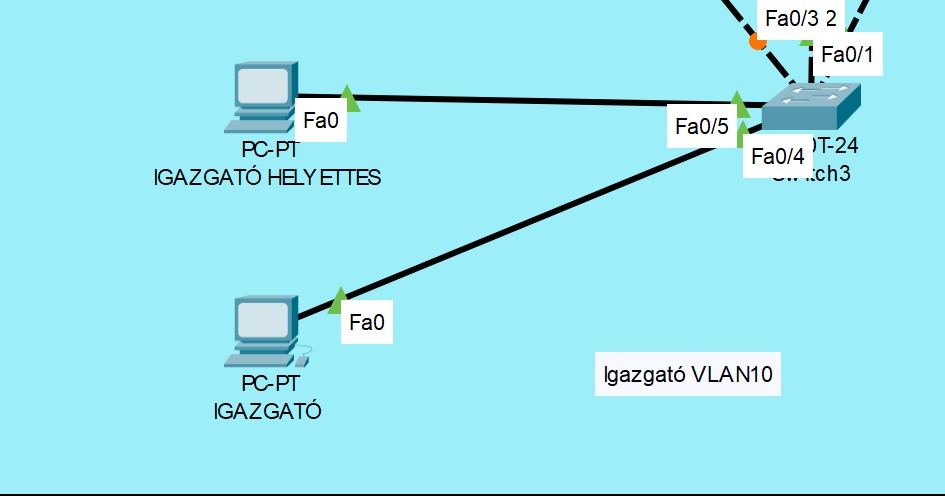
# STP protokoll

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. Az irodát 3 részre bontottuk. 1 igazgatói szoba, 1 titkárság illetve egy meeting terem. Ezeket helyiségeket VLAN segítségével elszeparáltuk.

# VLAN

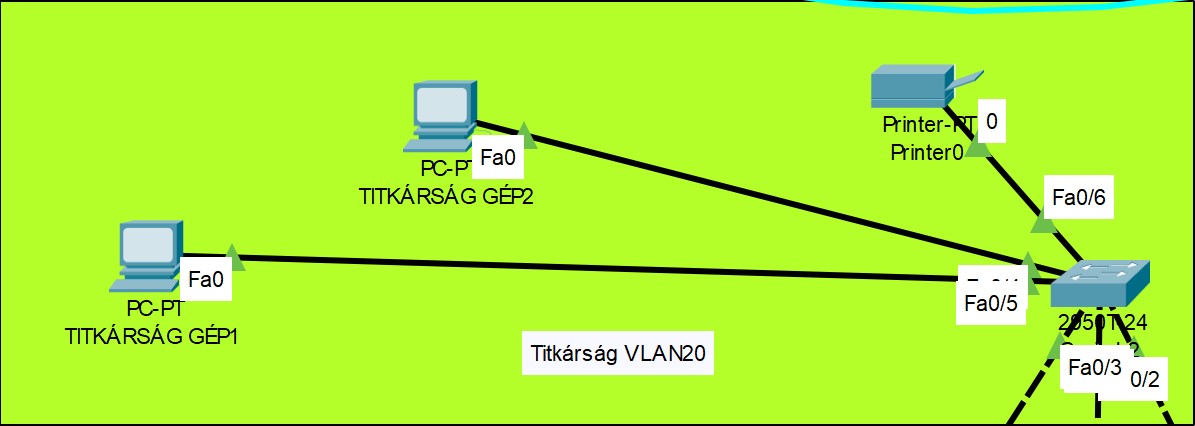
A VLAN (Virtual Local Area Network) egy rendkívül hasznos technológia, amely lehetővé teszi a hálózati erőforrások hatékonyabb használatát és a hálózati biztonság javítását. A VLAN-ok segítségével lehetőség van arra, hogy logikailag elkülönítsük a hálózati eszközöket és szegmenseket, így a hálózati forgalom 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. 2 darab VLAN-t hoztunk létre, egy Igazgató- és Titkárság VLAN-t.

**Az igazgatói VLAN 10-es számú:**



Igazgatói szobában 2db Pc helyezkedik el. Egy az igazgató részére, és egy a helyettesének, hogy könnyebben kommunikáljanak egymással.

**Titkári VLAN 20-as számú:**



A Titkárságban 2db PC és egy nyomtató van elhelyezve, az adminisztrációs munkák érdekében.

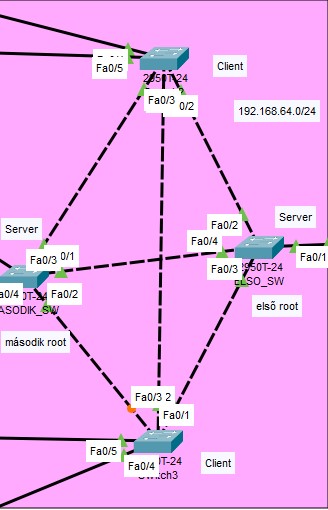
A kapcsolók a VLAN-okhoz VTP segítségével férnek hozzá, így nem kell manuálisan egyesével konfigurálni a Switcheket a VLANok miatt.

# 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

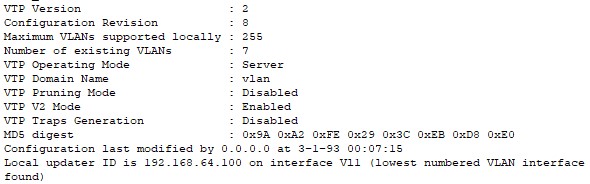
VTP automatikusan továbbítja ezt a változást a többi kapcsolónak is. **A VTP-nek 3 módja van:**

* 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.

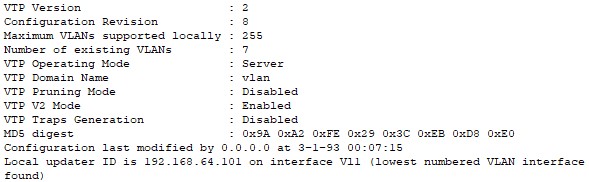


A hálózatban 2 Server és 2 Client található. Annak érdekében hogy ha az egyik kapcsoló meghibásodik(Primary) akkor a Secondary (VTP root) kapcsoló át tudja venni a helyét. 2 Client kapcsoló pedig hirdeti a

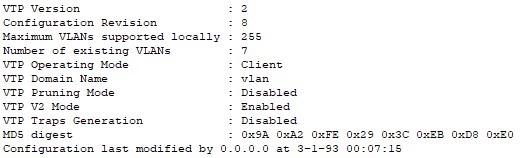
VTP-ket a megadott interfészeknek. **ELSO\_SW:**



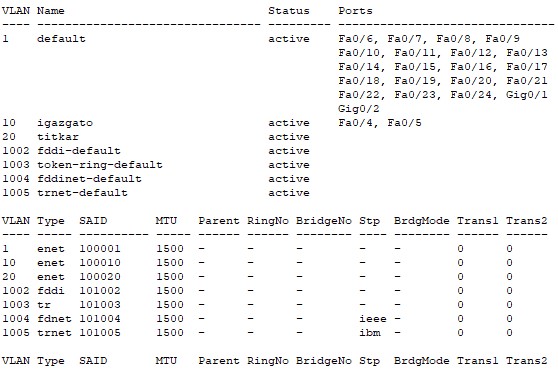
**MASODIK\_SW:**



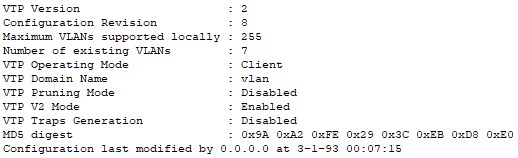
**Switch3:**



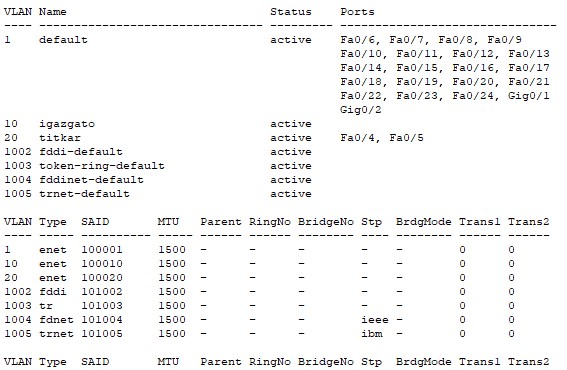
**A Switch3 hirdetett VLAN-ok:**



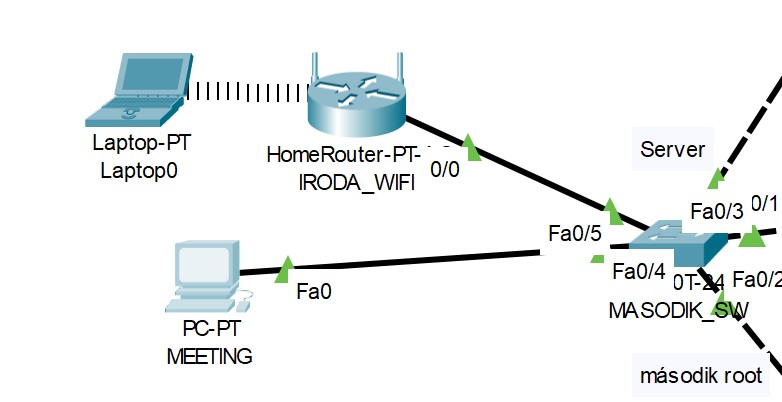
**Switch2:**



**A Switch2 hirdetett VLAN-ok:**



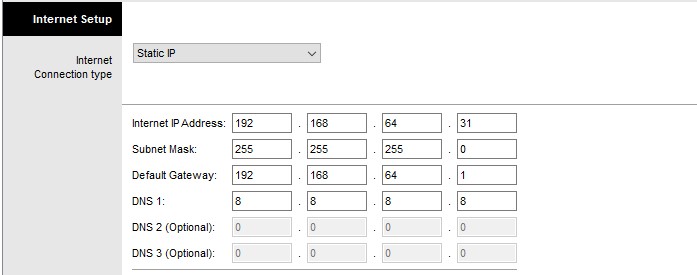
A Meeting teremben elhelyeztünk egy Gépet és egy WIFI Routert, hogy akár saját eszközről is képesek legyenek prezentációt bemutatni.



# 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.

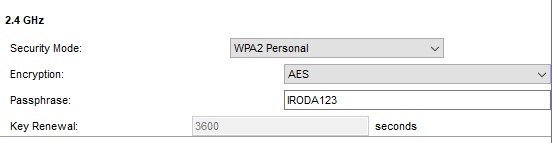
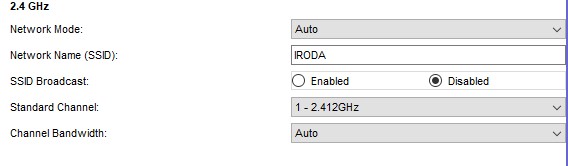
**A Wifi Router konfigurálása:**



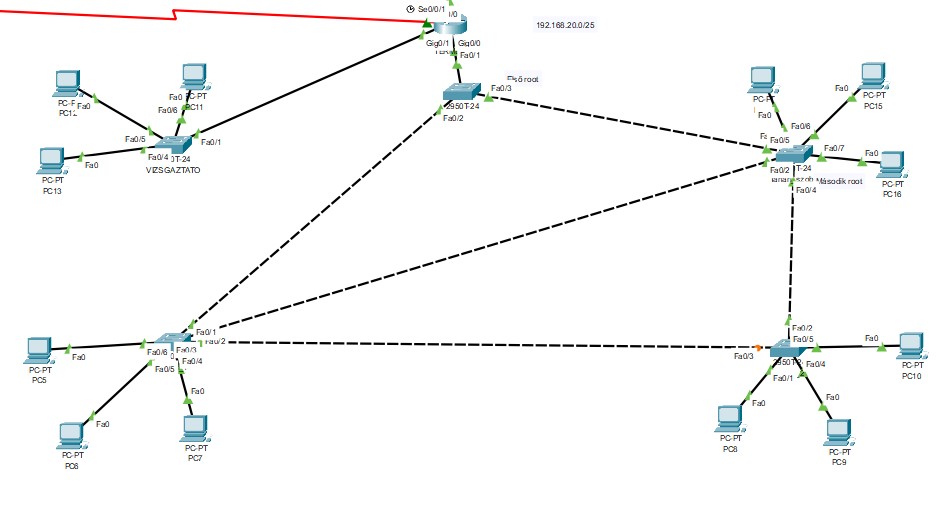
A WIFI Routernek SSID-t nem hirdetünk, és jelszóval levédettük.

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.



**Termek épület:**



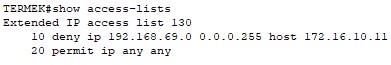
Termek épület 2 nagy részre felosztva. Oktatási termekre illetve

Vizsgáztató teremre van bontva.

Az oktatási termek DHCP-sen kapnak IP címet a MAIN\_SERVER Szervergéptől. Az oktatási termek, és az Étkező ugyanazt hálózati címet kapta csak ketté bontottuk. Egy 192.168.20.0/25 és egy 192.168.20.128/25-re bontottuk. A 4 kapcsoló STP protokollt használ, hogy a Redundáns hálózatban ne alakulhasson ki szórási vihar. Ugyan úgy mint az Irodában, itt is van egy elsődleges, és egy másodlagos kapcsoló.

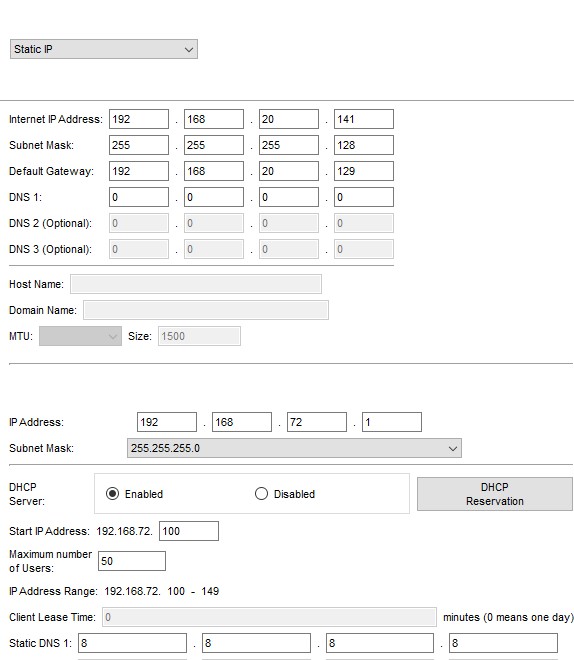
# Access Control List

A vizsgatermet azért kellett elszeparálni az oktatói termektől, mivel Vizsgateremben ACL-t(Access Control List) használunk, hogy letiltsunk Vizsga idő alatt internetelérést WEB\_SERVER felé. De ettől függetlenül a többi hálózatot, illetve szolgáltatást eléri. 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.



**Étkező:**

Az étkező illetve Termeken belül elhelyezkedő Oktatási termek IP címe ketté lett bontva, így nem kellett plusz IP címet kérni az létesítményre. IP címeket ketté osztottuk, 192.168.20.0/25 és 192.168.20.128/25 hálózatokra. Az étkezőben kialakítottunk a diákok számára WIFI Routert, hogy ebédszünet alatt tudjanak internetezni.



Mivel Szünetre kiépített WIFI Routert kértek, ezért nem védettük le jelszóval, ezért a diákok hozzá tudnak férni. Illetve az étkezőben elhelyezkedik még egy PC, ami arra szolgál, hogy a konyhások FTP-n keresztül tudják továbbítani, az iskola felé, hogy milyen élelmiszert kell megrendelni és milyen mennyiségben.

# 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.