**Informatikai rendszer- és alkalmazás-üzemeltető technikus projektfeladat**

Projekt Feladat • 2025. február 10.

**Hálózat tervezési dokumentáció**

|  |  |
| --- | --- |
| **Gacsal Ákos** | **2/14\_IR** |
| **Lénárt Zsolt** |
| **Kádár Zsolt** |

**A feladatunk egy összetett hálózat ki építése volt az alábbi szempontok alapján:**

• a hálózati infrastruktúrának legalább 3 telephelyet vagy irodát kell lefednie

• legalább egy telephelyen több VLAN kialakítását foglalja magában

• tartalmaz második és harmadik rétegbeli redundáns megoldásokat

• IPv4 és IPv6 címzési rendszert egyaránt használ

• Vezeték nélküli hálózatot is tartalmaz

• statikus és dinamikus forgalomirányítást egyaránt megvalósít

• statikus és dinamikus címfordítást alkalmaz

• WAN-összeköttetéseket is tartalmaz

• virtuális magánhálózati kapcsolatot (VPN) is megvalósít

• programozott hálózatkonfigurációt is használ

• forgalomirányítón megvalósított biztonsági funkciókat tartalmaz (pl. ACL-ek)

• hardveres tűzfaleszközt is alkalmaz

• Minimum 1-1 Linux és Windows kiszolgálót tartalmaz, melyek legalább az alábbi szolgáltatásokat nyújtják:

­ Címtár (pl. Active Directory)

­ DHCP

­ DNS

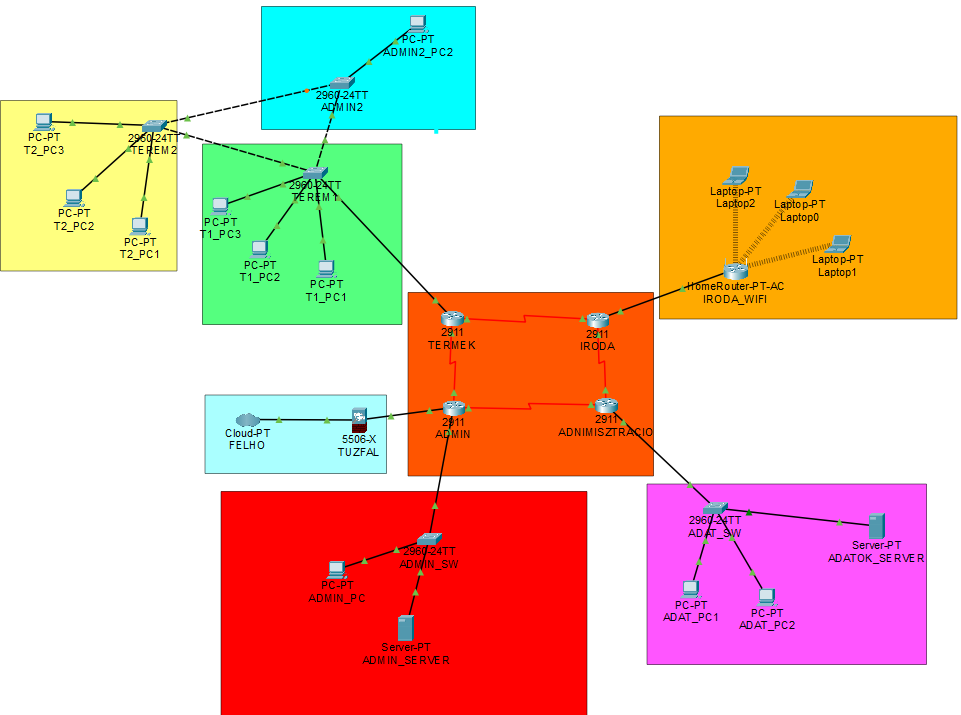
­ HTTP/HTTPS

­ Fájl és nyomtató megosztás

­ Automatizált mentés

­ Kliens számítógépekre automatizált szoftvertelepítés

**A mi csapatunk egy iskolai hálózatott tervezet amit az alábbi képpen oldottunk meg:**

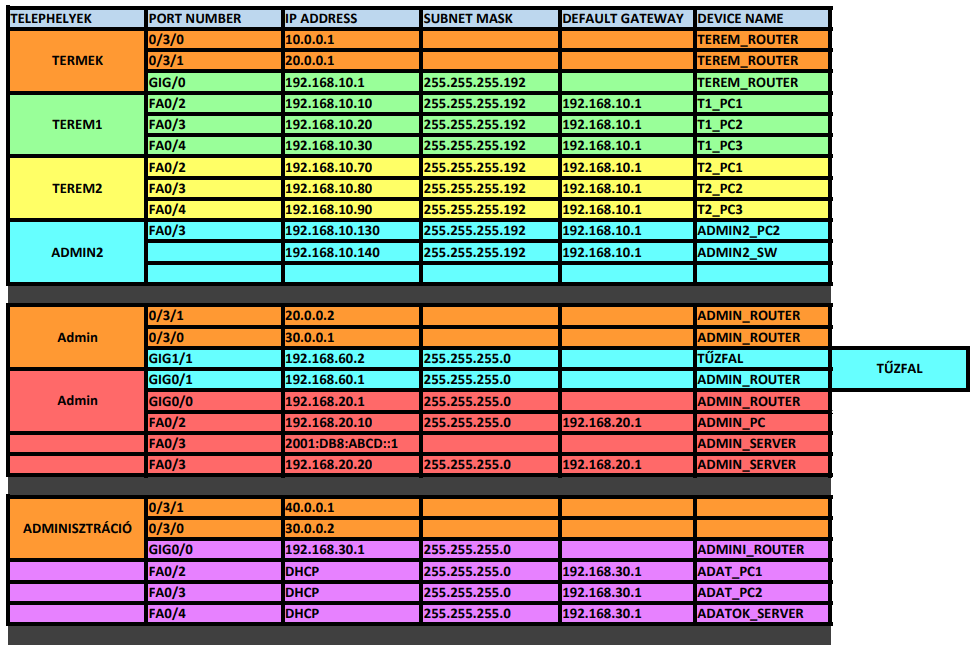


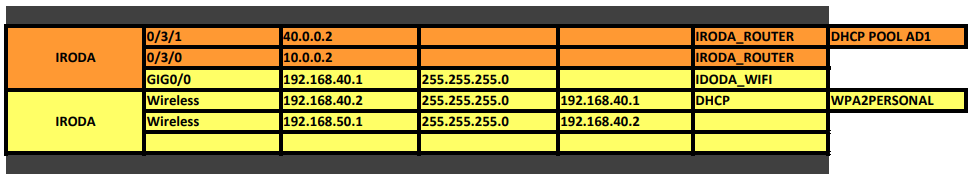
**5 fő szegmensre osztottuk a hálózatott, amik az alábbiak:**

* **Telephelyek**
* **Admin**
* **Adminisztráció**
* **Iroda**
* **Termek**

IP-cím kiosztás

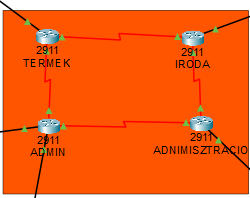
Az alábbi IP-címeket használtunk a feladat megoldásához.





Telephelyek

A hálózati infrastruktúra tervezésekor és implementálásakor több kritikus szempontot kellett figyelembe venni, hogy biztosítsuk a hatékony, biztonságos és skálázható működést. Az alábbiakban részletezzük a választott konfigurációt, annak előnyeit, valamint a biztonsági és funkcionalitási szempontokat.



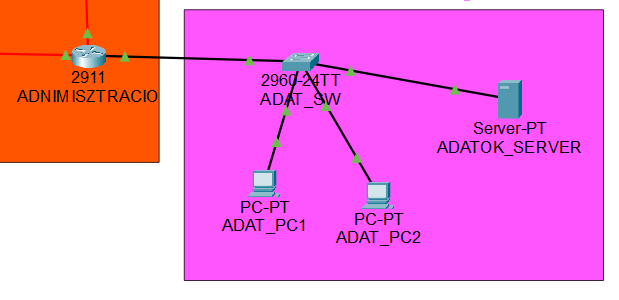
WAN-kommunikáció és OSPF használata

Az iskola négy routerből álló hálózatában az OSPF nevű útválasztási rendszert használjuk, mert ez biztosítja a gyors és megbízható adatáramlást az egyes telephelyek között.

Az OSPF előnyei:

Gyors reagálás ha egy kapcsolat megszakad vagy megváltozik, a rendszer gyorsan új útvonalat keres az adatok számára, így elkerülhetők a hosszabb leállások.

Kevesebb hálózati terhelés az OSPF csak a szükséges információkat küldi el a hálózatban, így csökkenti a felesleges adatforgalmat és növeli a rendszer hatékonyságát.



A hálózat tervezésekor a statikus és dinamikus útválasztás kombinációját alkalmaztuk, hogy biztosítsuk a megbízható, gyors és biztonságos adatáramlást az egyes telephelyek között. Az alábbiakban részletesen kifejtjük, miért volt szükség mindkét megoldásra, és milyen előnyökkel jár az Önök vállalatának.

Speciális hálózati szegmensek védelme – Bizonyos szerverek vagy érzékeny adatok védelme érdekében az útvonalakat manuálisan állítottuk be, hogy ne legyenek elérhetők minden eszköz számára.

✅ Biztonsági megfontolások – Egyes érzékeny adatforgalmat nem engedtünk át a dinamikus útválasztási rendszerbe, hogy elkerüljük az illetéktelen hozzáféréseket.

✅ Alternatív útvonalak vészhelyzet esetére – Ha az OSPF alapú útválasztás valamilyen hiba miatt nem működne, a statikus útvonalak biztosítják, hogy az alapvető kapcsolatok továbbra is működjenek.

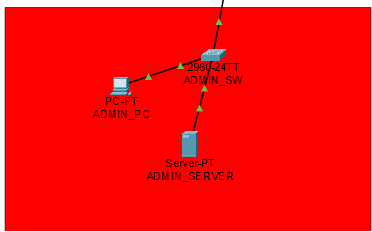
Ezeknek az előnyöknek köszönhetően a különböző telephelyek közötti kommunikáció zavartalan, gyors és hatékony, ami elengedhetetlen a stabil működéshez.

A WAN titkosítás során a CHAP használata növeli a kapcsolat biztonságát, mert a jelszót nem küldi ki nyílt szövegként, folyamatos hitelesítést biztosít, és megakadályozza az adatlopásra irányuló támadásokat. Ezáltal a hálózat megbízhatóbb és ellenállóbb lesz a biztonsági fenyegetésekkel szemben.

A routerek között alítottunk clock ratet az adat kommunikáció megvalósításához.

Admin

Az Admin Szoba egy lokális hálózat része, amely a vállalat belső adminisztratív eszközeinek kommunikációját biztosítja. A hálózat célja, hogy az adminisztrációs dolgozók számára gyors, megbízható és biztonságos kapcsolatot nyújtson a szükséges informatikai erőforrásokhoz.



ADMIN\_PC (PC-PT) – A rendszergazda által használt számítógép, amely csatlakozik a hálózathoz és hozzáfér a szerverhez.

A rendszergazdai számítógépre Linux operációs rendszert telepítettünk.

A Linux és a Windows operációs rendszerek közötti választás nagyban függ attól, hogy milyen célra szeretnénk használni az adott rendszert.

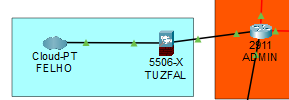
A mi esetünkben a megbízhatóság és a egyszerűség volt a fő szempont hiszen a Linux szervereket akár évekig lehet futtatni anélkül, hogy újra kellene indítani őket , jobban kezeli a memóriahasználatot és a többfeladatos működést, így kevésbé hajlamos a rendszerösszeomlásra.

ADMIN\_SERVER (Server-PT) – Egy dedikált szerver, amely tartalmazza a vállalat belső adatbázisait, fájlmegosztását.

A szerver kapott egy IPv6-os címet is hiszen közel korlátlan címzési lehetőséget biztosít, így az admin szerver minden interfésze és eszköze saját egyedi IP-címet kaphat, könnyebben konfigurálható a hitelesített és titkosított adminisztrációs hozzáférés.

A szerveren titkosított módon tárolhatók a konfigurációs fájlok, így védve vannak illetéktelen hozzáférés és adatlopás ellen.

Ennek köszönhetően végeztünk biztonsági mentést is a konfigurációkról ami azt edeményezi ha egy router vagy switch meghibásodik, az eszközön tárolt konfiguráció elveszhet. A szerveren történő mentés biztosítja, hogy az adatok mindig elérhetők maradjanak.



ADMIN\_Router : Ha egy router nincs megfelelően védve, könnyen illetéktelen hozzáférés áldozata lehet, ami komoly biztonsági kockázatot jelenthet. Ezt megakadályozva beállítottunk egy jelszót ami a router konfigurációját védi igy megakadályozva az imént említetteket.

Dinamikus címfordítás(NAT)

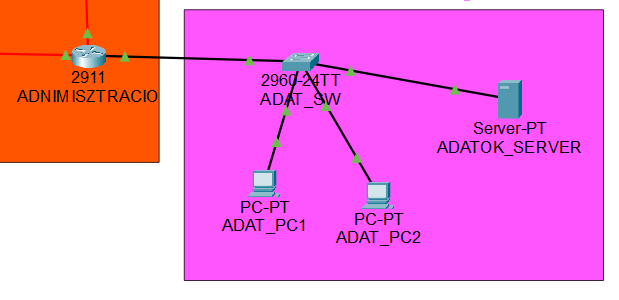
A belső, privát hálózaton található eszközök egy privát IP-címtartományból kommunikálnak.

🔹 Amikor egy eszköz kifelé kommunikál az internetre vagy egy másik hálózatra, a router vagy tűzfal a privát IP-t egy nyilvános IP-re cseréli egy előre meghatározott címkészletből.

A mi esetünkben a FELHŐ a szolgáltatótól kapott internetet jelképezi . A nagyobb biztonság érdekében elhelyeztünk egy hardveres TŰZFAL(at). Az iskolai hálózatról érkező kérést a dinamikus nat egy IP-címre fordítja át igy megoldható hogy a hálózaton lévő összes eszköz ugyanazon IP-címmel kommunikáljon a szolgáltató felé.

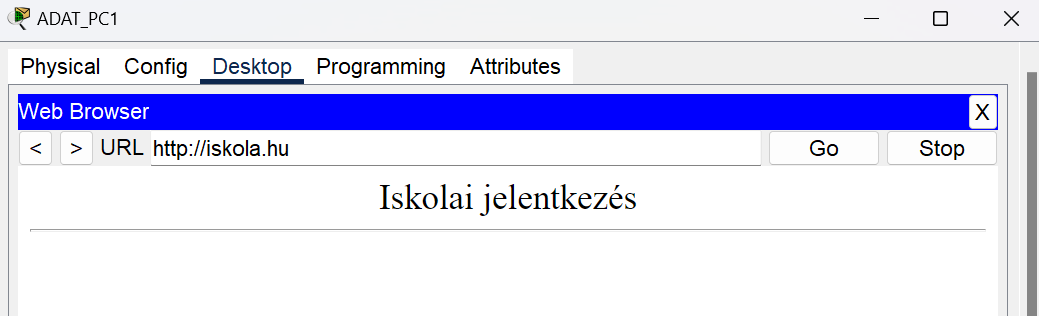
Adminisztráció

A hatékony működés érdekében egy modern, stabil és biztonságos hálózati rendszert hoztunk létre. Az alábbi megoldásokkal biztosítjuk a gyors és megbízható adatáramlást az adminisztrációs részlegen belül.



Az ADATOK\_SERVER-re telepített **webszerver** lehetővé teszi, hogy az alkalmazottak könnyen és biztonságosan elérhessék a szükséges információkat, belső dokumentációkat és egyéb erőforrásokat egy böngészőn keresztül. Ez csökkenti a papíralapú adminisztrációt, és gyorsítja a munkafolyamatokat.

Létrehoztunk egy iskolai webszervert, amely lehetőséget biztosít a diákok és tanárok számára, hogy könnyen és gyorsan csatlakozzanak az iskola saját digitális felületeihez.

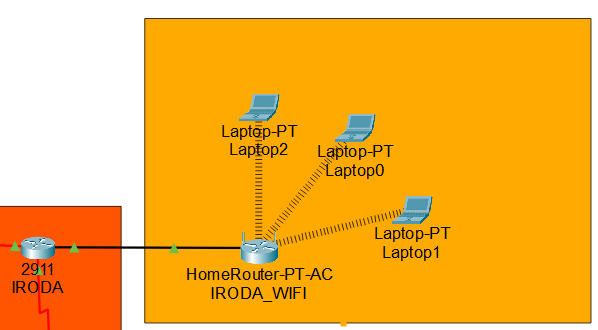


ADMINISZTRÁCIÓ\_ROUTER : A routeren beállított statikus NAT (Network Address Translation) biztosítja, hogy a belső szervere elérhető legyene az internet felől is, de csak az előre meghatározott, biztonságos módon. Ez azt jelenti, hogy például egy külső ügyfél vagy partner egy adott IP-címen keresztül érheti el a weboldalát, miközben a hálózat többi része védett marad a jogosulatlan hozzáférésektől.

A routeren konfigurált DHCP (Dynamic Host Configuration Protocol) automatikusan kiosztja az IP-címeket a számítógépek és egyéb eszközök számára. A DHCP biztosítja, hogy ne legyenek IP-cím ütközések, ami javítja a hálózat stabilitását és megbízhatóságát.

Iroda

A hatékony munkavégzés és a stabil hálózati kapcsolat érdekében létrehoztunk egy modern, vezeték nélküli hálózatot az iroda számára. Az IRODA\_WIFI névre keresztelt Wi-Fi hálózat biztosítja a gyors és megbízható internetkapcsolatot az irodai laptopok és egyéb eszközök számára.



Az irodai dolgozók bárhol kényelmesen csatlakozhatnak a hálózatra, nincs szükség felesleges kábelezésre.

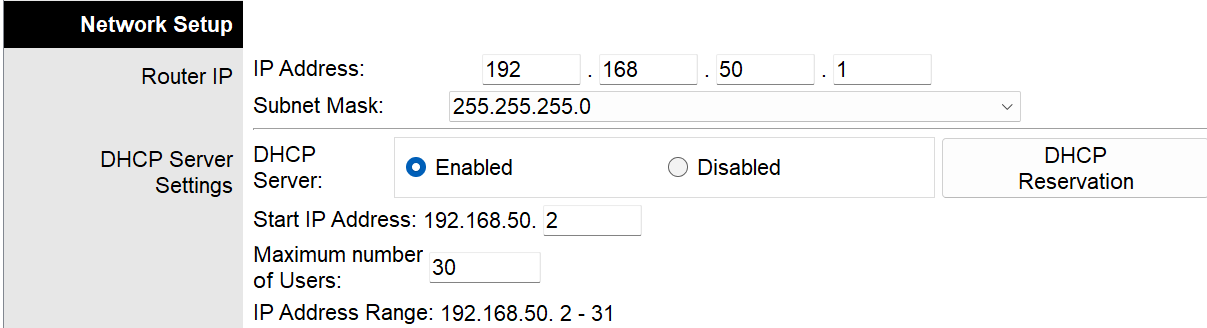
A beállított HomeRouter-PT-AC típusú eszköz erős és folyamatos jelet biztosít, így a munkavégzés zavartalan és hatékony.

A hálózatot WPA2-Personal védelemmel láttuk el, amely:

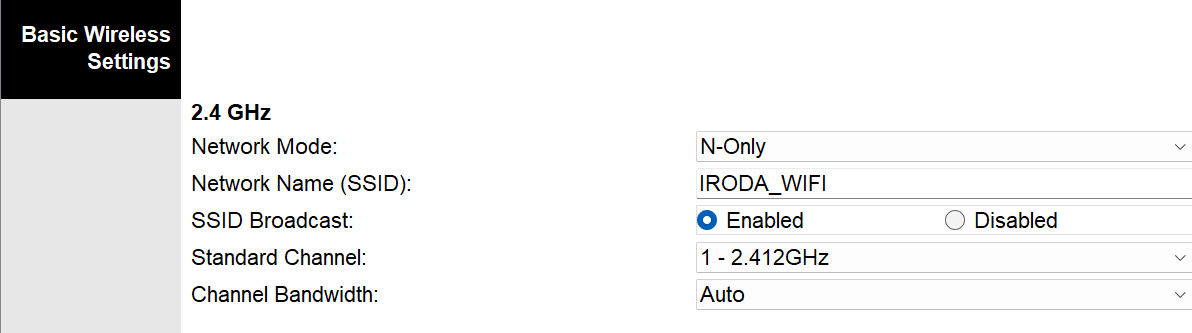
Erős titkosítást biztosít a felhasználói adatok számára

Megakadályozza a jogosulatlan hozzáférést, így csak a megfelelő hitelesítéssel rendelkező eszközök csatlakozhatnak

Biztonságosabbá teszi az online munkavégzést, megvédve az adatokat a külső fenyegetésektől



Ez a DHCP-konfiguráció biztosítja a hatékony, biztonságos és automatizált IP-címkezelést a hálózat számára. Az optimális beállítások garantálják a gyors csatlakozást, a megbízható működést és a problémamentes hálózatkezelést.

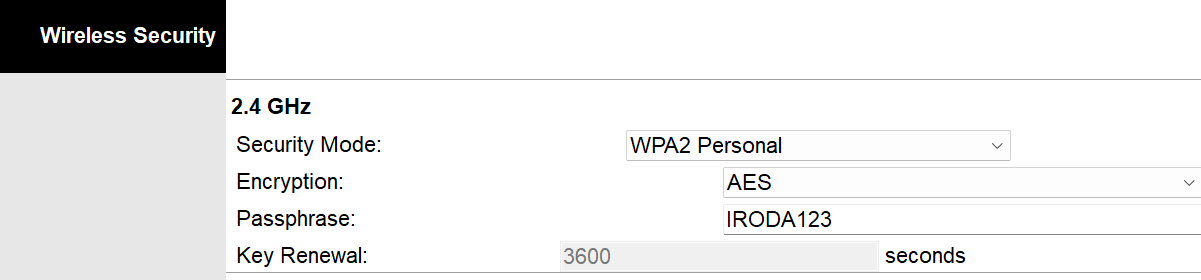


Hálózat neve (SSID): IRODA\_WIFI

A hálózat kizárólag az 802.11n szabványt használja, amely jobb sebességet és stabilitást biztosít a régebbi b/g szabványokhoz képest.

Ez biztosítja, hogy csak modernebb eszközök csatlakozhatnak, amelyek támogatják ezt a technológiát, így optimalizálva a teljesítményt.

A csatorna sávszélessége automatikusan alkalmazkodik a környezethez, így csökkenti a zavaró jeleket és stabilabb kapcsolatot biztosít.



A hálózatunk védelme érdekében WPA2-Personal biztonsági módot alkalmaztunk, amely a AES titkosítást használja. Ez a megoldás garantálja, hogy az irodai Wi-Fi hálózat biztonságos és védett maradjon a jogosulatlan hozzáférésekkel szemben.

A WPA2-Personal jelenleg az egyik legbiztonságosabb Wi-Fi titkosítási mód, amely megakadályozza, hogy illetéktelenek hozzáférjenek a hálózathoz.

Az AES titkosítás nagyobb biztonságot nyújt, mint a korábbi TKIP titkosítás, és a modern eszközök is támogatják.

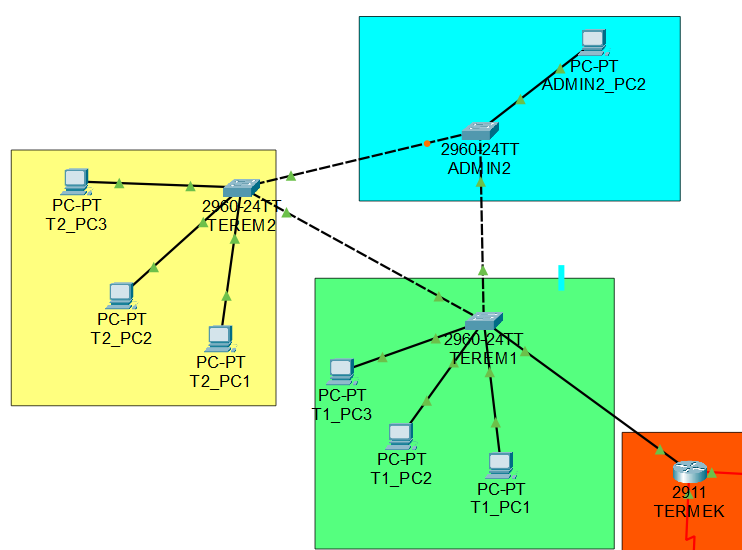
A jelszóvédelem biztosítja, hogy csak az engedélyezett felhasználók csatlakozhassanak a Wi-Fi hálózathoz.



Termek

A hálózatunk optimális működése érdekében VLAN (Virtual Local Area Network) és VTP (VLAN Trunking Protocol) technológiákat alkalmaztunk. Ezek a megoldások biztosítják, hogy az egyes tantermek és az ADMIN\_2 hálózat logikailag elkülönüljön, miközben hatékony adatforgalmat és jobb hálózatkezelést tesznek lehetővé.

A mi esetünkben ez azt eredményezi hogy az egyes termek nem tudnak kommunikálni egymással.



A különböző termekhez különböző VLAN-okat hoztunk létre . Az ADMIN\_2-höz tartozó eszközöket is külön VLAN-okba soroltuk, így a forgalom nem keveredik.

Például a tanulók számítógépei nem férnek hozzá az ADMIN\_2 eszközökhöz, így védve vannak az érzékeny adatok.

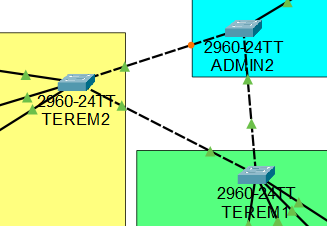


A fenti hálózati topológia több különálló switchből és egy központi routerből áll, amely különböző termeket és az ADMIN\_2 részt köti össze. A hatékony VLAN-kezelés érdekében VTP-t (VLAN Trunking Protocol) állítottunk be.

A VTP automatizálja és leegyszerűsíti a VLAN-kezelést, megkönnyíti az új eszközök hozzáadását, és csökkenti az adminisztrációs terheket. Ezzel a megoldással egy biztonságos, rugalmas és könnyen skálázható hálózatot hoztunk létre, amely hosszú távon is hatékonyan működik.

Az ADMIN2-re telnetet állítottunk be annak érdekében hogy a rendszergaza távolról is elérje ,konfigurálni tudja az eszközt.

Egy rendszergazda egyszerre több hálózati eszközhöz is hozzáférhet, így hatékonyabban kezelheti a hálózatot.



A hálózati diagramon jól látható, hogy több switch és kapcsolódási útvonal is van, ami egy redundáns hálózati topológiára utal. A redundancia célja, hogy növelje a hálózat megbízhatóságát és elérhetőségét, minimalizálva a kieséseket.