**Baranya Vármegyei SZC Mohácsi Radnóti Miklós Technikum és Szakképző Iskola**

**Vizsgaremek**

Készítették:

Horváth Máté

Vajta Gerda Franciska

**Mohács**

**2025**

**Baranya Vármegyei SZC Mohácsi Radnóti Miklós Technikum és Szakképző Iskola**

Szakma megnevezése:

Informatikai rendszer- és alkalmazás-üzemeltető technikus

A szakma azonosító száma: 506121202

**Vizsgaremek**

SKYNET

Készítették:

Horváth Máté

Vajta Gerda Franciska

**Mohács**

**2025**

Tartalomjegyzék

Tartalom

[Feladat rövid ismertetése 3](#_Toc191547233)

[Bevezetés 3](#_Toc191547234)

[Cél 3](#_Toc191547235)

[Jövőbeli tervek 3](#_Toc191547236)

[Használt technológiák 4](#_Toc191547237)

[Hálózati tervező eszközök 4](#_Toc191547238)

[Hálózati komponensek 4](#_Toc191547239)

[Hálózati szimuláció típusa 6](#_Toc191547240)

[Egyéb technológiák 6](#_Toc191547241)

[Hálózat 8](#_Toc191547242)

[A hálózat rövid magyarázata 8](#_Toc191547243)

[Az alhálózatok jellemzése: 10](#_Toc191547244)

[A tesztelés: 12](#_Toc191547245)

[Tesztelési folyamat és módszertan 12](#_Toc191547246)

[Tesztelési típusok 12](#_Toc191547247)

[A prototípus részletes leírása: 13](#_Toc191547248)

[Telephelyek: 13](#_Toc191547249)

[Vlan/ok: 13](#_Toc191547250)

[2. és 3. rétegbeli redundancia: 14](#_Toc191547251)

[IPv4 és IPv6-os címzés: 15](#_Toc191547252)

[Vezeték nélküli hálózat: 15](#_Toc191547253)

[Statikus és dinamikus forgalomirányítás: 16](#_Toc191547254)

[Statikus és dinamikus címfordítás: 17](#_Toc191547255)

[WAN összeköttetés: 18](#_Toc191547256)

[VPN: 19](#_Toc191547257)

[Programozott hálózatkonfiguráció: 20](#_Toc191547258)

[ACL: 21](#_Toc191547259)

[Tűzfal: 22](#_Toc191547260)

[Linux és Windows szerver: 22](#_Toc191547261)

[Csapatmunka 23](#_Toc191547262)

[Jiras haladásunk az egész projekt alatt: 25](#_Toc191547263)

[Jövőbeli tervek: 26](#_Toc191547264)

# Feladat rövid ismertetése

Bevezetés  
A projekt során egy olyan kezdetleges prototípus elkészítését tűztük ki célul, amely Magyarország segélyhívó rendszerének működését modellezi. Az ötlet alapját a sürgősségi szolgáltatások közötti adatkommunikációs és hálózati igények vizsgálata adta. A prototípus egy informatikai hálózatot fog bemutatni, amely képes szimulálni a segélyhívások továbbítását és az érintett szervezetek közötti kommunikáció alapvető folyamatait. A fejlesztés során az informatikai hálózatok tervezésének és kiépítésének elméleti és gyakorlati oldalát vesszük alapul, hogy a prototípus a lehető legjobban tükrözze a valós rendszer működésének alapjait. A dokumentáció részletesen bemutatja majd a rendszer technológiai elemeit és a fejlesztési folyamat lépéseit.

## Cél

A projekt célja egy olyan alapvető informatikai hálózat megtervezése és megvalósítása, amely bemutatja, hogyan lehet a segélyhívó rendszer különböző résztvevői között gyors és megbízható kommunikációt biztosítani. A prototípus tervezése során kiemelten figyelünk a hálózat biztonságára, rendelkezésre állására és skálázhatóságára. A célunk, hogy egy egyszerűen kezelhető, mégis hatékony rendszer alapjait hozzuk létre, amely a valóságban alkalmazható rendszerek működéséhez adhat inspirációt. Hosszú távon olyan technológiai megoldásokat kívánunk bemutatni, amelyek segítik a vészhelyzeti szolgáltatások összehangolt működését, javítják a reakcióidőt és növelik az állampolgárok biztonságát. A rendszer fejlesztése során különös figyelmet fordítunk arra, hogy a hálózat jól illeszkedjen a modern informatikai követelményekhez, és megfelelő alapot nyújtson a későbbi továbbfejlesztésekhez.

## Jövőbeli tervek

A prototípus elkészítése után a projekt jövőbeli célja a rendszer továbbfejlesztése egy teljesen működőképes segélyhívó hálózattá, amely valós környezetben is alkalmazható. Elsődleges tervünk a rendszer funkcionalitásának bővítése, például a különböző szolgáltatások (mentők, rendőrség, tűzoltóság) közötti automatikus feladatkiosztás bevezetése, valamint egy felhasználóbarát kezelőfelület megvalósítása. Ezen kívül további fejlesztési cél a hálózat teljesítményének optimalizálása, hogy nagy terhelés mellett is stabil és gyors maradjon.

A rendszer biztonsági funkcióinak erősítése is kulcsfontosságú, különösen az adatvédelem és a jogosulatlan hozzáférés elleni védekezés szempontjából. Hosszabb távon a hálózat országos lefedettségének biztosítása, valamint a legmodernebb technológiák, például a mesterséges intelligencia és az IoT eszközök integrálása is szerepel a tervek között. A végső cél egy olyan rugalmas és fejlett segélyhívó rendszer létrehozása, amely jelentősen hozzájárul a vészhelyzeti szolgáltatások hatékonyságához, és amely a mindennapi működés során is magas szintű megbízhatóságot garantál.

# Használt technológiák

## Hálózati tervező eszközök

A projekt során a hálózati rendszer tervezéséhez és szimulációjához a Cisco Packet Tracer eszközt használtuk. Ez a szoftver lehetővé teszi a hálózati topológiák vizuális megtervezését, a konfigurációk tesztelését, valamint a hálózat működésének szimulációját.

## Hálózati komponensek

1. **Hálózati eszközök**
   * Routerek
   * Switchek
   * PC-ék (Számítógépek), Laptopok
   * Szerverek és végponti eszközök
   * Nyomtatók
   * Tablet/ek
2. **Protokollok és konfigurációk**
   * IPV4 és IPV6 IP-címzési stratégiák
   * VLAN-ok és szegmentáció
   * Redundancia protokollok
   * Dinamikus routing protokollok (RIP)
   * Statikus forgalomirányítás
   * VPN
   * Statikus és dinamikus címfordítás
   * DHCP
   * STB

## Hálózati szimuláció típusa

A rendszer szimulációja a Cisco Packet Tracer segítségével készült. Ez az eszköz nemcsak a fizikai topológia vizualizációját tette lehetővé, hanem a logikai működés teljeskörű szimulációját is biztosította. Így a hálózati konfigurációkat és kapcsolódási pontokat hatékonyan tesztelhettük, mielőtt éles környezetben alkalmaztuk volna.

# Egyéb technológiák

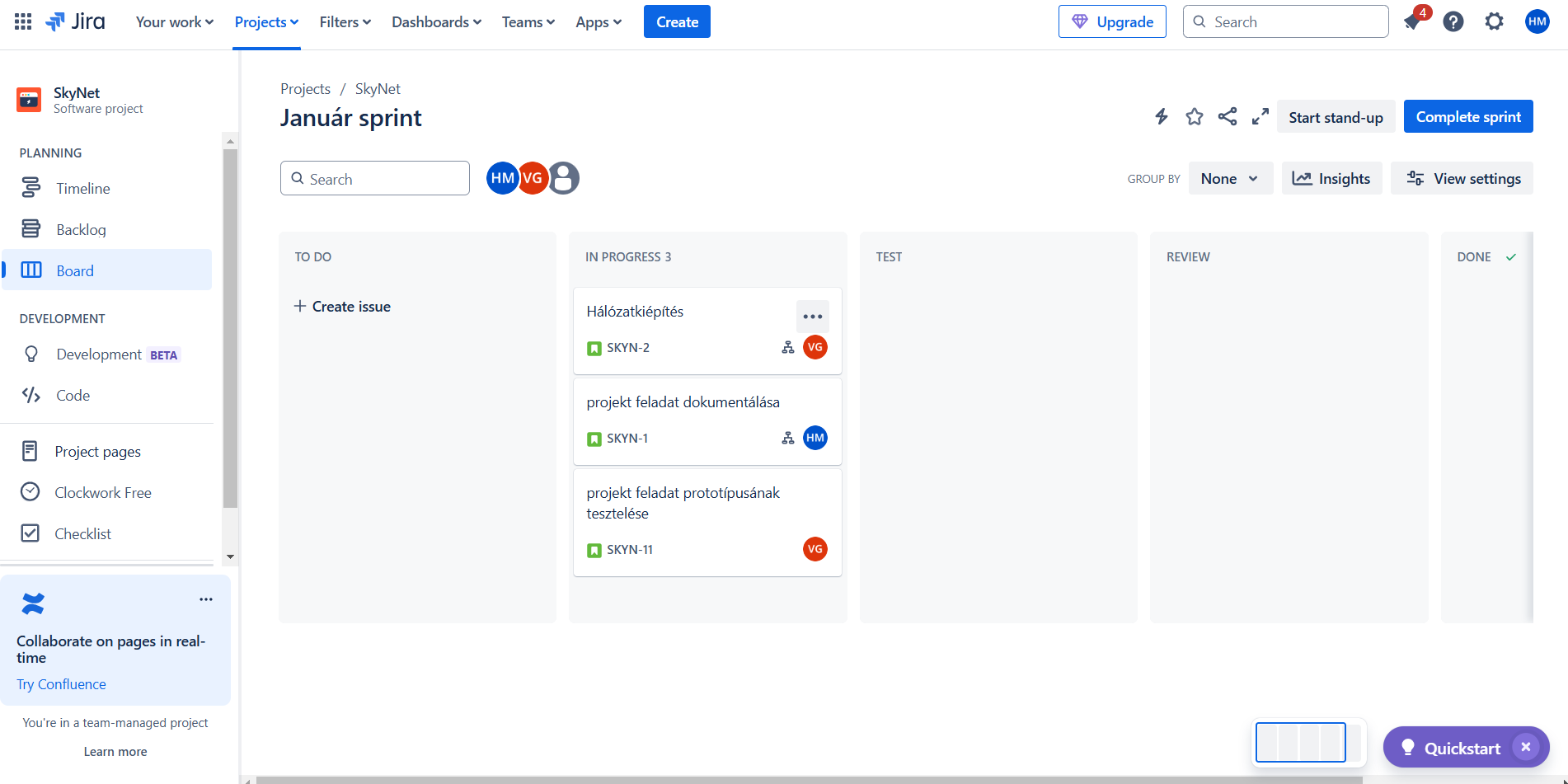
1. **Jira**

A Jira egy projektmenedzsment eszköz, amely segíti a csapatokat abban, hogy nyomon kövessék projektjeiket, kezeljék a feladatokat, és hatékonyan szervezzék a fejlesztési folyamatokat. Az eszköz támogatja a feladatok rendszerezését, a prioritások felállítását, valamint megkönnyíti a csapattagok közötti kommunikációt.

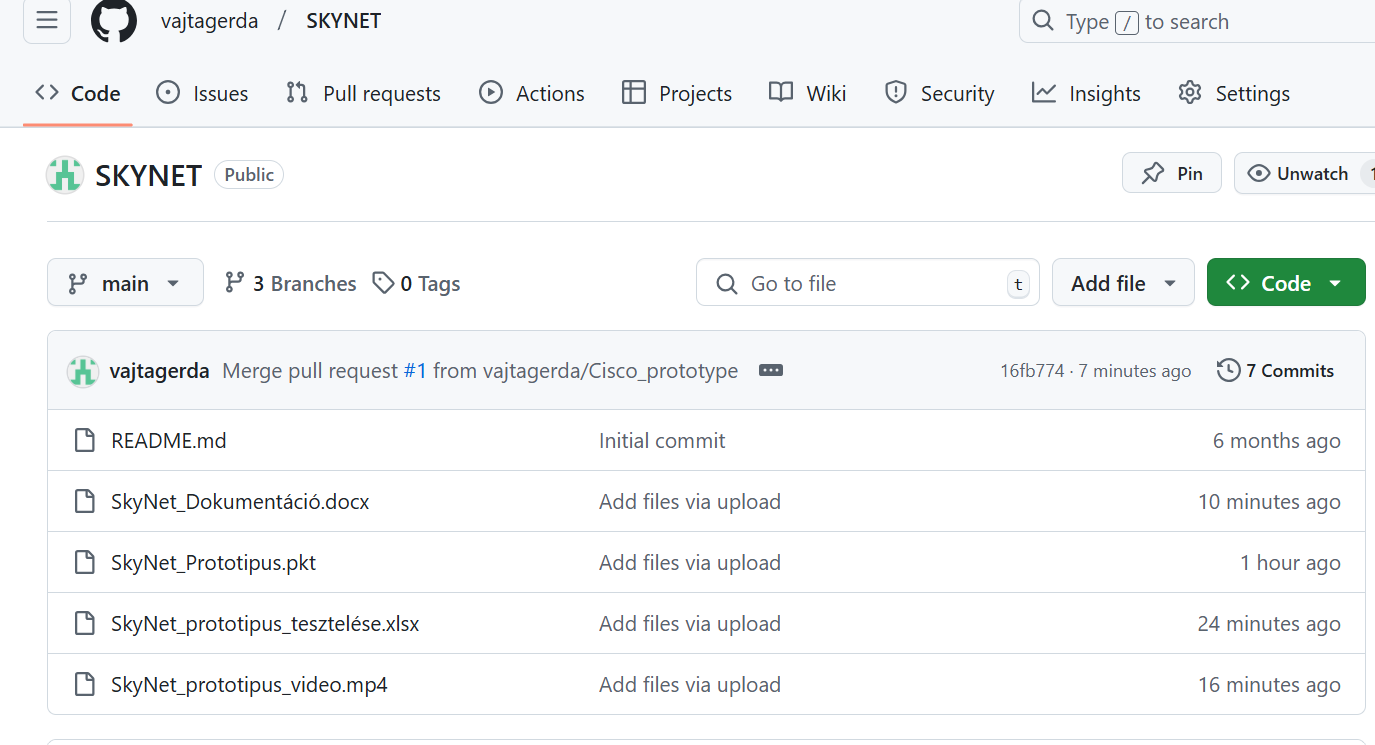
1. **Git**

A Git egy elosztott verziókezelő rendszer, amely lehetővé teszi a fejlesztők számára a kódbázis változásainak nyomon követését, a módosítások kezelését és a csapaton belüli hatékony együttműködést. Az elosztott működés előnye, hogy párhuzamosan lehet dolgozni, miközben egyszerűen létrehozhatók és visszaállíthatók visszatérési pontok (commit-ek).

A képen az egyik havi sprintünk a jirából látható:



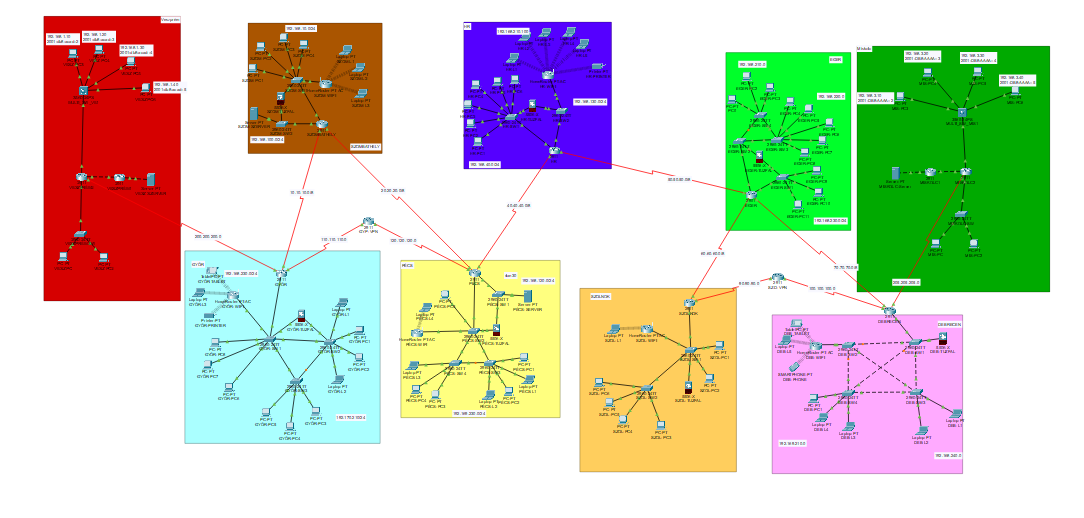
A képen a githubunk látható:



# Hálózat

## A hálózat rövid magyarázata

A segélyhívó rendszer hatékony működéséhez elengedhetetlen egy stabil és jól megtervezett hálózati infrastruktúra. A hálózat biztosítja a segélyhívások gyors továbbítását, az információk valós idejű feldolgozását, valamint az adatbiztonságot. A rendszer redundáns és hierarchikus felépítése minimalizálja a szolgáltatás kiesésének kockázatát, így folyamatos elérhetőséget garantál a kritikus helyzetekben. A hálózati topológia tartalmazza a központi vezérlőegységeket, a helyi kommunikációs csomópontokat, valamint a végponti eszközöket, például operátori munkaállomásokat és kommunikációs szervereket. Az egyes szegmensek közötti kapcsolatokat nagysebességű routerek és switchek biztosítják, lehetővé téve a zökkenőmentes adatáramlást a rendszer minden pontján. A rendszer a legmodernebb protokollok és biztonsági megoldások integrációjával készült, hogy az adatok ne csak gyorsan, hanem teljesen biztonságosan kerüljenek továbbításra. A megfelelően konfigurált hálózati eszközök támogatják a rendszer skálázhatóságát, lehetővé téve a jövőbeni bővítéseket. Mindez hozzájárul a segélyhívások gyors feldolgozásához, a helyszíni egységek koordinálásához, és biztosítja, hogy a rendszer minden körülmények között készen álljon a feladatára.



A képen a rendszerünk hálózati topológiája látható, amely a hálózat különböző eszközeinek és azok kapcsolatainak vizuális ábrázolása. A diagram elemei között megtalálhatók a routerek, switchek, szerverek, valamint a végponti eszközök. A hálózat szegmensei különálló csoportokra vannak bontva, amelyek egy-egy funkcionális területet vagy szervezeti egységet képviselnek. A kapcsolatokat a diagramon a hálózati interfészek közötti összeköttetések jelölik, amelyek az adatforgalom irányát és útvonalait is szemléltetik. Az eszközök IP-címzéssel vannak konfigurálva, a különböző alhálózatok elkülönítése érdekében. A hálózat hierarchikus felépítése biztosítja az adatforgalom hatékony irányítását, miközben a redundancia és a biztonság érdekében több tartalék kapcsolat is kialakításra került. A diagramon továbbá megfigyelhetők a dinamikus routing protokollok, VLAN szegmentációk és az egyes eszközök kapcsolati típusai, amelyek hozzájárulnak a hálózat zökkenőmentes és megbízható működéséhez.

# Az alhálózatok jellemzése:

A kép alapján a hálózatok különböző részekre bonthatók:

1. HR fő hálózat (Kék):

A képen látható HR központ a segélyhívó hálózat központi eleme, amely több alhálózattal és végponti eszközzel kapcsolódik. Ez a központ biztosítja az összesített adatkezelést, a kommunikáció irányítását, valamint az erőforrások elosztását a különböző hálózati szegmensek között. A HR központi router az összeköttetések és az adatforgalom kezelésének kulcspontja, garantálva a hálózat zavartalan működését.

1. Szombathely alhálózat (Barna):

A képen látható Szombathely telephely a segélyhívó hálózat egyik fontos regionális egysége, amely helyi végponti eszközökkel és szerverrel rendelkezik. A telephely hálózati forgalma egy dedikált routeren keresztül csatlakozik a központi HR hálózathoz, biztosítva az adatok hatékony továbbítását és a zavartalan kommunikációt. Szombathely kulcsszerepet játszik a helyi kapcsolatok kezelésében és a segélyhívások gyors feldolgozásában.

1. Eger alhálózat (Világoszöld):

A képen látható EGER telephely a világoszöld alhálózat része, amely szorosan integrálódik a segélyhívó rendszerbe. A telephelyen található végponti eszközök, például munkaállomások, stb, helyi switcheken keresztül csatlakoznak, miközben egy dedikált router biztosítja az összeköttetést a központi HR hálózattal. EGER telephelyének infrastruktúrája a gyors és megbízható adatforgalomra van optimalizálva, lehetővé téve a hatékony helyi és országos szintű kommunikációt.

1. Győr alhálózat (Cián):

A képen látható GYŐR telephely, amely a ciánkék alhálózatot képviseli, fontos regionális szerepet tölt be a segélyhívó rendszerben. A telephely különböző végponti eszközöket – például számítógépeket, nyomtatót, tabletet, stb – foglal magában, amelyek helyi switcheken keresztül kapcsolódnak egymáshoz. A hálózat központi eleme egy router, amely felelős a telephely forgalmának összekapcsolásáért a központi HR hálózattal, valamint más telephelyekkel. GYŐR telephelye hatékony adatáramlást és gyors információmegosztást biztosít, támogatva a zavartalan helyi és országos működést.

1. Pécs alhálózat (Citromsárga):

A kép alapján látható PÉCS telephely, amely a citromsárga alhálózatot képviseli, a segélyhívó rendszer egyik kulcsfontosságú regionális egysége. A telephelyen található eszközök – például számítógépek, szerverek stb – egy helyi hálózaton belül switcheken keresztül kapcsolódnak egymáshoz. Egy központi router biztosítja a kapcsolatot a központi HR hálózattal és más telephelyekkel, lehetővé téve a hatékony kommunikációt és adatáramlást. PÉCS telephelye fontos szerepet játszik a régió segélyhívásainak kezelésében és a hálózat folyamatos működésének biztosításában.

1. Szolnok alhálózat (Narancssárga):

A kép alapján látható SZOLNOK telephely, amely a narancssárgás árnyalatú alhálózatot képviseli, egy fontos regionális csomópont a segélyhívó rendszerben. A telephely hálózati eszközei – például számítógépek, laptop és egyéb végponti berendezések mint pl: A tűzfal, ami minden alhálózatban megtalálható, köztük ebben is. – switcheken keresztül kapcsolódnak egymáshoz, biztosítva a belső kommunikációt és adatáramlást. Egy központi router felel a telephely külső kapcsolataiért, összekötve azt a központi HR hálózattal és más telephelyekkel. SZOLNOK alhálózata megbízható működést biztosít a helyi segélyhívások kezelésében és a rendszer hatékony működésében.

1. Debrecen alhálózat (Rózsaszín):

Az előbbi kép alapján látható rózsaszín DEBRECEN alhálózat egy jelentős telephely a segélyhívó rendszerben, amely több végponti eszközt és hálózati berendezést foglal magában. A helyi számítógépek és egyéb eszközök switcheken keresztül kapcsolódnak egymáshoz, míg egy központi router biztosítja az adatok továbbítását a többi telephely és a HR központ felé. A redundáns kapcsolatok és a struktúrált hálózati felépítés garantálja a zavartalan működést, így a Debreceni egység hatékonyan tudja kezelni a beérkező segélyhívásokat és az adatkommunikációt más hálózati szegmensekkel.

1. Veszprém alhálózat (Piros):

A fenti kép alapján látható piros Veszprém alhálózat egy kisebb, de fontos telephely a segélyhívó rendszerben. A hálózat központi eleme egy router, amely biztosítja a kapcsolatot a többi telephely felé. A helyi infrastruktúra tartalmaz egy szervert és munkaállomásokat(pc-ket), amelyek a helyi forgalom kezeléséért és a segélyhívások továbbításáért felelősek. A kapcsolódási pontok és a hálózati eszközök megfelelő elrendezése garantálja a stabil működést és a hatékony adatkommunikációt.

1. Miskolc alhálózat (Sötétzöld):

A most beküldött képen látható sötétzöld Miskolc alhálózat egy kisebb, de stratégiai szerepet betöltő telephely a segélyhívó hálózatban. A hálózat központi elemei között található egy router, amely biztosítja a kapcsolatot a központi HR rendszerhez és más telephelyekhez. Mivel ez az alhálózat a piros tükörképe ezért a helyi infrastruktúrában egy szerver és munkaállomásként használt pc-ék találhatók, amelyek az adatok kezelését és a kommunikáció fenntartását szolgálják. A hálózat kialakítása biztosítja a hatékony adatáramlást és a folyamatos szolgáltatást a segélyhívások megfelelő továbbítása érdekében.

# A tesztelés:

## Tesztelési folyamat és módszertan

A hálózati infrastruktúra kiépítését követően **Cisco Packet Tracer** környezetben végeztünk részletes teszteléseket annak érdekében, hogy biztosítsuk a megfelelő működést. A tesztelési folyamatot **manuális teszteléssel** hajtottuk végre, és az eredményeket egy **Excel táblázatban** rögzítettük, amely 100 egyedi tesztesetet tartalmazott vagy még annál is többet.

A tesztelési folyamat során egy iteratív, agilis megközelítést alkalmaztunk, amely hasonlít a Scrum módszertanra. Rendszeresen ellenőriztük a konfigurációkat, visszajelzések alapján módosításokat végeztünk, és sprintekben haladtunk a hálózati beállítások optimalizálásával.

## Tesztelési típusok

**1. Manuális tesztelés**

A manuális tesztelés során különböző hálózati elemek működését ellenőriztük a Cisco Packet Tracerben. Az alábbi szempontok szerint végeztük a vizsgálatokat:

* **Hálózati elérhetőség tesztelése (Ping tesztek)**
  + Ellenőriztük, hogy az egyes alhálózatokban lévő eszközök elérik-e egymást.
  + Megnéztük, hogy az útválasztók megfelelően továbbítják-e a csomagokat.
* **DHCP működésének ellenőrzése**
  + A dinamikus IP-kiosztás megfelelő működését vizsgáltuk.
  + Megnéztük, hogy az ügyfélgépek kapnak-e IP-címet az adott alhálózaton belül.
* **NAT és internetkapcsolat tesztelése**
  + A belső hálózat eszközeinek internetelérése ellenőrizve lett.
  + Megvizsgáltuk, hogy a NAT megfelelően fordítja-e a privát IP-ket publikus IP-kké.
* **VPN kapcsolatok ellenőrzése**
  + A távoli telephelyek közötti biztonságos adatkapcsolatok tesztelése.
  + A titkosítás és az adatátvitel megfelelő működésének vizsgálata.
* IPV 4 és IPV6 címek ellenőrzése:
*  **IPv4 tesztelés:** Ping teszt és traceroute végrehajtása a távoli helyek között IPv4 címekkel, hogy ellenőrizze a kapcsolat stabilitását és elérhetőségét.
*  **IPv6 tesztelés:** Ping teszt és traceroute végrehajtása a távoli helyek között IPv6 címekkel, hogy biztosítsa a kapcsolat működését és az útvonalak helyes működését.

**2. Hibajavítás és optimalizálás**

A tesztek során talált **hibákat és konfigurációs problémákat** nem nagyon észleltünk ezért nem is alkalmaztunk sem hibajavítást és optimalizálást.

# A prototípus részletes leírása:

## Telephelyek:

A hálózati infrastruktúránk kiterjedt rendszert alkot, amely összesen kilenc alhálózatot foglal magában, biztosítva a különböző telephelyek és irodák közötti megbízható és biztonságos kommunikációt.

A rendszer központi eleme a HR központ, amely a hálózat gerincét képezi, és összeköti a különböző alhálózatokat, biztosítva az adatforgalom hatékony kezelését és a megfelelő erőforrás-elosztást.

## Vlan/ok:

A hálózati infrastruktúra kialakítása során különös figyelmet fordítottunk a **VLAN-ok (Virtual Local Area Networks) alkalmazására**, amely lehetővé teszi a hálózati szegmensek hatékonyabb elkülönítését és optimalizálását. A VLAN technológia biztosítja, hogy az egyes telephelyeken belül a forgalom szeparált módon haladjon, növelve ezzel a biztonságot és a teljesítményt.

Az alhálózatok közül **négy telephelyen (Veszprém – piros, Miskolc – sötétzöld, Szombathely – barna és a központi HR hálózat – kék) nem alkalmaztunk VLAN szegmentációt**, mivel ezek kisebb infrastruktúrával rendelkeznek, és az eszközök elhelyezése nem indokolta a további szétválasztást.

A többi alhálózatban azonban **VLAN-ok kerültek kialakításra**, biztosítva a forgalom szeparációját és a hálózati teljesítmény optimalizálását:

* **Eger (világoszöld)** hálózatában **három különböző VLAN** működik, amelyek a feladat követelményei szerint különböző funkciókat látnak el. Ez a VLAN struktúra lehetővé teszi az eltérő osztályok vagy részlegek elkülönítését, miközben a hálózati forgalmat hatékonyan menedzseli.
* **Győr (ciánkék)**, **Pécs (sárga)**, **Szolnok (narancssárga)** és **Debrecen (rózsaszín)** esetében szintén VLAN-ok biztosítják a belső hálózatok logikai szegmentálását, ami elősegíti a **jobb erőforrás-kezelést, a biztonságosabb adatforgalmat és a zavartalan működést**.

A VLAN konfigurációk **megfelelnek a hálózati szabványoknak**, és a megfelelő hálózati eszközökön (switch-ek és routerek) kerültek beállításra..

Ez a megvalósítás biztosítja, hogy az egyes telephelyek és irodák közötti adatforgalom **strukturált, biztonságos és optimalizált módon működjön**, miközben teljes mértékben megfelel a hálózati architektúrával szemben támasztott követelményeknek.

## 2. és 3. rétegbeli redundancia:

A **második rétegbeli redundanciát** a hálózatban a **Spanning Tree Protocol (STP)** segítségével valósítottuk meg, amely megakadályozza a hálózati hurkok kialakulását és biztosítja a stabil adatáramlást. Az STP dinamikusan választja ki az optimális útvonalakat, és automatikusan letiltja a redundáns kapcsolatokat, majd szükség esetén újraaktiválja azokat. Ez különösen fontos a nagyobb hálózatok esetében, ahol több kapcsoló is szerepet kap az adatátvitelben, hiszen a redundáns útvonalak lehetőséget adnak a gyors helyreállításra egy esetleges meghibásodás esetén.

A **harmadik rétegbeli redundanciát** a **RIP (Routing Information Protocol)** segítségével biztosítottuk, amely négy routert kapcsol össze. A RIP protokoll dinamikusan frissíti az útvonalakat, így biztosítva, hogy az adatok mindig a legrövidebb és legoptimálisabb útvonalon haladjanak. Az automatikus útvonalválasztás lehetővé teszi a hálózat számára, hogy egy meghibásodás esetén alternatív útvonalat találjon, ezáltal minimalizálva a hálózatkieséseket és biztosítva a folyamatos kommunikációt az alhálózatok között.

## IPv4 és IPv6-os címzés:

A hálózatban mindenhol alkalmaztunk IPv4-es címzést, amely biztosítja a különböző eszközök és alhálózatok közötti megbízható kommunikációt. Az IPv4-es címzés minden hálózati szegmensben jelen van, és lehetővé teszi az eszközök egyértelmű azonosítását és elérését a rendszerben.

Az IPv4 mellett bizonyos hálózatokban IPv6-os címzés is megtalálható, különösen a piros és a sötétzöld alhálózatokban. Az IPv6 bevezetése ezekben a hálózatokban nemcsak a jövőbeni bővíthetőséget támogatja, hanem lehetőséget biztosít a modernebb hálózati megoldások alkalmazására is. Az IPv6 használata ezen alhálózatokban hozzájárul az IP-címek kimerülésének kezeléséhez, valamint fejlettebb biztonsági és hatékonysági mechanizmusokat nyújt, például a jobb multicast és automatikus címkonfiguráció révén.

A hálózat struktúrája több különálló alhálózatra épül, amelyek routereken keresztül kapcsolódnak egymáshoz. Ezek az alhálózatok eltérő földrajzi helyszíneken lehetnek, de megfelelő útválasztási szabályokkal és konfigurációval biztosított az adatok zavartalan áramlása közöttük. A hálózati eszközök, például a switchek és routerek, kulcsszerepet játszanak a forgalom irányításában, valamint az eszközök közötti kapcsolat fenntartásában.

A szerverek és munkaállomások megfelelő IP-konfigurációval rendelkeznek, hogy mind az IPv4, mind pedig az IPv6 környezetben működni tudjanak ott, ahol ezt a rendszer megköveteli. A piros és sötétzöld hálózatokban az eszközök már kettős címzési módszerrel (dual-stack) működnek, amely lehetővé teszi mind az IPv4, mind az IPv6 használatát. A címzés logikusan van felépítve, hogy a hálózat áttekinthető és hatékony maradjon. A hálózat felépítése és címzési rendszere biztosítja a bővíthetőséget, valamint a különböző kommunikációs protokollok együttes használatát.

## Vezeték nélküli hálózat:

A hálózatban vezetékes és vezeték nélküli eszközök egyaránt megtalálhatók, és egy komplex, több alhálózatból álló rendszert alkotnak. Az infrastruktúra különböző földrajzi helyszíneken elhelyezkedő hálózatokat köt össze, amelyeket routereken keresztül kapcsoltak egymáshoz. Minden alhálózat önálló eszközparkkal rendelkezik, amelyben szerverek, munkaállomások, switchek és egyéb hálózati eszközök biztosítják a hatékony működést. Az IP-címzés elsősorban IPv4-re épül, de bizonyos helyeken IPv6-os címzés is használatban van, ami elősegíti a modern hálózati követelményeknek való megfelelést és a hosszú távú bővíthetőséget.

A hálózat működését dinamikus útválasztás és megfelelő konfigurációk biztosítják, amelyek lehetővé teszik az optimális adatforgalmat és a redundancia fenntartását. A különböző alhálózatok közötti kapcsolatot több útvonal is biztosítja, ezáltal növelve a hálózat megbízhatóságát. Az eszközök címzése és elrendezése logikusan van felépítve, így a hálózati adminisztráció egyszerűbbé válik. A szerverek különböző szolgáltatásokat nyújtanak, például fájlmegosztást, távoli elérést és hálózatbiztonsági megoldásokat, amelyek biztosítják a rendszer stabil működését.

A hálózat kialakítása lehetővé teszi a skálázhatóságot és a könnyű bővíthetőséget, így a jövőbeli fejlesztésekhez is megfelelő alapot biztosít. Az adatforgalmat megfelelően konfigurált tűzfalak és biztonsági protokollok védik, ezáltal növelve a hálózat biztonságát. A rendszer felépítésében nagy szerepet játszanak a központi routerek és switchek, amelyek biztosítják az eszközök közötti gyors és stabil kommunikációt. A hálózati infrastruktúra kialakítása figyelembe veszi a redundanciát és a hibamentes működést, így egy esetleges hiba esetén is fennmarad a kapcsolat az egyes alhálózatok között.

A hálózat fő célja egy hatékony és stabil adatátviteli rendszer biztosítása, amely különböző földrajzi területeken elhelyezkedő munkaállomások és szerverek számára lehetővé teszi az információk gyors és megbízható elérését. Az eszközök konfigurációja és az alkalmazott hálózati technológiák garantálják a folyamatos működést, valamint a biztonságos és gyors adattovábbítást.

## Statikus és dinamikus forgalomirányítás:

A hálózatban statikus és dinamikus forgalomirányítás egyaránt megvalósításra került, biztosítva ezzel a hatékony adatáramlást és a hálózat optimális működését. A statikus útvonalak konfigurálása lehetővé teszi az egyes alhálózatok közötti stabil kapcsolat fenntartását, míg a dinamikus forgalomirányítás (RIP) automatikusan kezeli az útvonalakat, így alkalmazkodik a hálózat változásaihoz.

A piros és a sötétzöld hálózatok kivételével mindenhol alkalmazásra került statikus forgalomirányítás, amely biztosítja a meghatározott útvonalakon történő adatátvitelt. Ezzel szemben a dinamikus forgalomirányítás (RIP) minden hálózatban aktív, beleértve a piros és a sötétzöld hálózatokat is. Ennek köszönhetően az útválasztók képesek automatikusan frissíteni az útvonalakat, reagálva a hálózati topológia változásaira, így növelve a rugalmasságot és csökkentve az adminisztrációs terheket.

A kombinált megoldás előnye, hogy a statikus útvonalak biztosítják a kritikus hálózati kapcsolatok stabilitását, míg a dinamikus forgalomirányítás gondoskodik az alternatív útvonalak fenntartásáról és az esetleges hálózati hibák gyors kezeléséről. Ennek köszönhetően a hálózat hatékonyan és megbízhatóan működik, alkalmazkodva az aktuális forgalmi viszonyokhoz.

## Statikus és dinamikus címfordítás:

A hálózatban mind statikus, mind dinamikus címfordítást (NAT – Network Address Translation) alkalmaznak, a különböző hálózatok igényeihez igazodva. A címfordítás lehetővé teszi, hogy a belső hálózatok eszközei megfelelően kommunikáljanak a külső hálózatokkal, például az internettel, miközben biztosítja az IP-címek hatékony kihasználását és növeli a biztonságot. Az egyes alhálózatok eltérő módon használják a NAT különböző típusait, attól függően, hogy milyen kapcsolatokat és működési feltételeket igényelnek.

A sötétzöld hálózat az egyetlen olyan rész a teljes rendszerben, ahol kizárólag statikus címfordítás található. Ez azt jelenti, hogy minden belső eszköz manuálisan beállított egyedi külső IP-címmel rendelkezik, amelyen keresztül kommunikál a külső hálózatokkal. A statikus NAT előnye, hogy kiszámítható és stabil kapcsolatot biztosít, különösen olyan esetekben, amikor egy adott eszköznek mindig ugyanazon a címen kell elérhetőnek lennie, például szerverek vagy egyes speciális hálózati eszközök esetében.

Ezzel szemben a piros hálózat az egyetlen olyan rész, ahol kizárólag dinamikus címfordítást alkalmaznak. Ez azt jelenti, hogy a hálózatba kapcsolódó eszközök nem rendelkeznek előre meghatározott külső IP-címmel, hanem a NAT automatikusan kiosztja számukra az elérhető külső címeket, amikor erre szükség van. A dinamikus címfordítás különösen hasznos, ha sok belső eszköznek kell időszakosan csatlakoznia külső hálózatokhoz, de nincs szükség állandó egyedi külső IP-címre. Ez az eljárás hatékonyan csökkenti a szükséges nyilvános IP-címek számát, és rugalmasan kezeli a hálózat változó forgalmát.

Fontos megjegyezni, hogy a hálózat egyes részein kizárólag az egyik vagy a másik típusú címfordítás található meg. Ahol statikus NAT van jelen, ott nem alkalmaznak dinamikus címfordítást, és fordítva: ahol dinamikus NAT működik, ott nincs statikus NAT. Ez az egyértelmű elhatárolás segít az erőforrások optimális kihasználásában és a hálózat egyértelmű konfigurálásában.

Az eltérő címfordítási stratégiák alkalmazása biztosítja a hálózat hatékony működését, a megfelelő elérhetőséget és a biztonsági szempontok figyelembevételét. A statikus címfordítás megbízható és stabil kapcsolatokat nyújt, míg a dinamikus címfordítás rugalmasságot és hatékony címkiosztást tesz lehetővé. Ezen megoldások kombinációja segít abban, hogy a hálózat képes legyen alkalmazkodni a változó igényekhez, miközben fenntartja a zavartalan adatkapcsolatokat.

## WAN összeköttetés:

A hálózatban WAN-összeköttetések is megtalálhatók, amelyek kulcsszerepet játszanak az egyes alhálózatok közötti adatkommunikáció biztosításában. Ezek az összeköttetések lehetővé teszik, hogy a különböző földrajzi helyeken elhelyezkedő hálózati szegmensek egymással kommunikáljanak, és zökkenőmentesen továbbítsák az adatokat. A WAN-kapcsolatok nélkül a hálózat egyes részei elszigetelten működnének, és nem lenne lehetőség az erőforrások közös használatára vagy a hálózati szolgáltatások egységes működtetésére.

A WAN-kapcsolatok szorosan kapcsolódnak a hálózatban használt dinamikus forgalomirányítási protokollhoz, amely esetünkben a RIP (Routing Information Protocol). A RIP protokollt minden hálózatban alkalmazzák, beleértve a piros és a sötétzöld hálózatot is, amelyeken egyébként statikus forgalomirányítás nem található. A WAN-összeköttetések segítségével a RIP képes dinamikusan frissíteni az útvonalakat és biztosítani, hogy az adatok mindig a leghatékonyabb úton jussanak el a célállomásra.

A hálózat szerkezetéből jól látszik, hogy a különböző alhálózatok közötti összeköttetések nagyrészt WAN-kapcsolatokon keresztül valósulnak meg, amelyek biztosítják a folyamatos és megbízható adatáramlást. Ezek a kapcsolatok létfontosságúak a hálózat egészének működésében, különösen a RIP által vezérelt dinamikus útvonalválasztás miatt, amelynek segítségével az útvonalak automatikusan frissülnek és alkalmazkodnak a hálózati forgalom változásaihoz.

Összességében a WAN-kapcsolatok nemcsak a hálózat struktúrájának alapvető elemei, hanem szoros összefüggésben állnak a dinamikus forgalomirányítással is, amely nélkülözhetetlen a hálózat hatékony és rugalmas működéséhez.

## VPN:

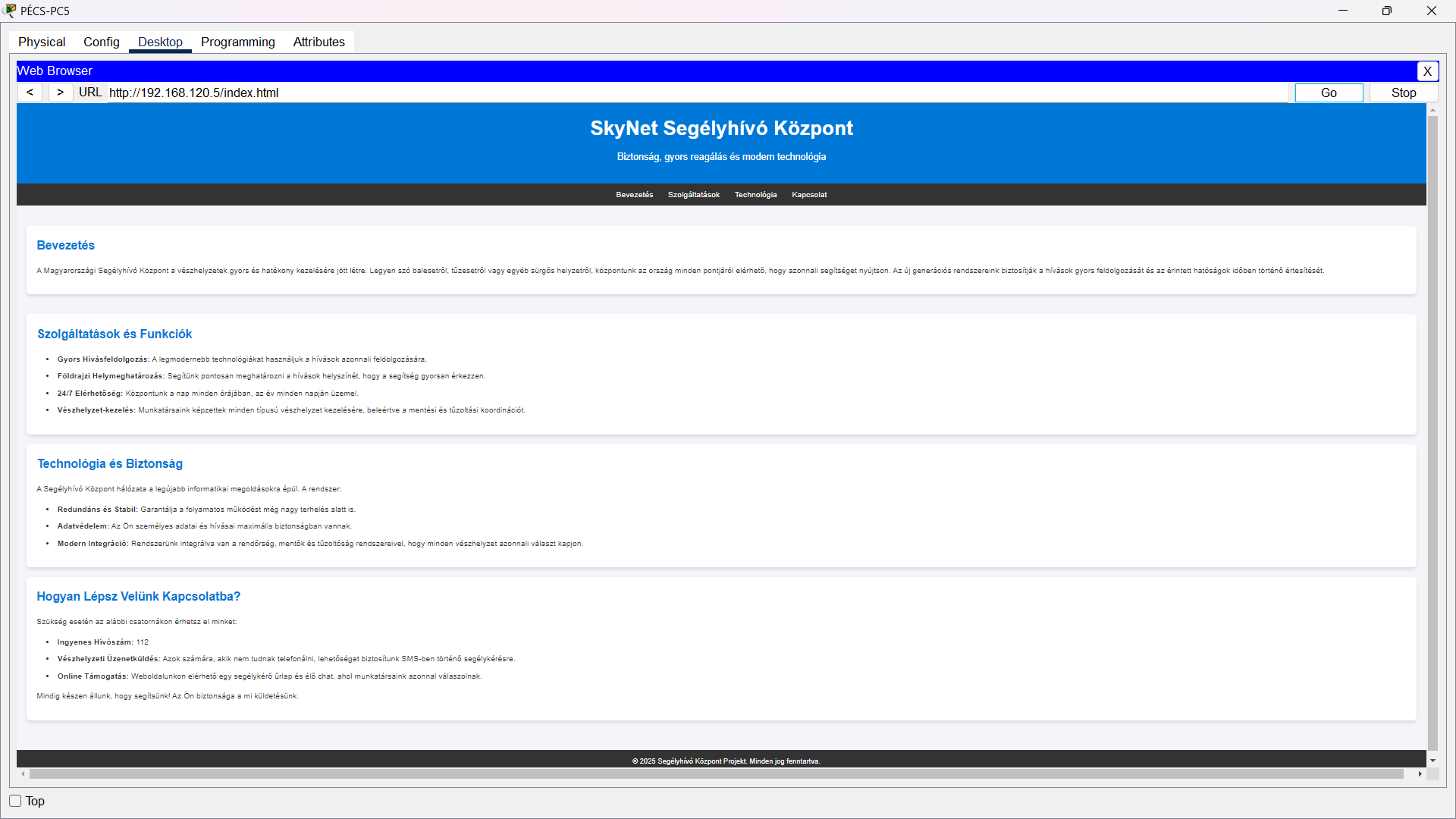
A hálózatunkban **virtuális magánhálózati kapcsolatot (VPN)** is kialakítottunk, amely két különálló kapcsolatot foglal magában. Az első VPN-t a **ciánkék (Győr) és a sárga (Pécs)** hálózat között hoztuk létre, míg a második VPN kapcsolat a **narancssárga (Szolnok) és a rózsaszín (Debrecen)** hálózat között biztosít titkosított és biztonságos adatforgalmat.

A VPN megoldások egyik legfontosabb szerepe, hogy a **távoli telephelyek közötti biztonságos kommunikációt** biztosítsák. Mivel ezek a telephelyek földrajzilag távol helyezkednek el egymástól, a hagyományos hálózati kapcsolatok helyett egy titkosított, biztonságos csatornát kellett létrehozni. A VPN kapcsolataink segítségével az adatok úgy áramolhatnak a különböző alhálózatok között, mintha azok egyetlen belső hálózat részei lennének, ezáltal garantálva a **folyamatos és zavartalan működést**.

A VPN-ek alkalmazása lehetővé teszi, hogy a nyilvános hálózatokon keresztül is biztonságosan lehessen adatokat továbbítani. Ehhez **titkosítási protokollokat** használunk, amelyek védik az érzékeny információkat az illetéktelen hozzáféréstől. Ezen kívül a VPN kapcsolatok segítségével csökkenthetők a **biztonsági kockázatok**, például a lehallgatás vagy az adatok manipulálása.

A Győr–Pécs és a Szolnok–Debrecen közötti VPN kapcsolatok nemcsak az **adatbiztonságot**, hanem a **hálózat stabilitását és hatékonyságát** is növelik. Ezek a megoldások garantálják, hogy a vállalat belső rendszerei, erőforrásai és szolgáltatásai minden telephely számára egyformán elérhetők legyenek, miközben minimalizálják a külső támadások és hálózati sérülékenységek kockázatát.

## Programozott hálózatkonfiguráció:



A programozott hálózatkonfiguráció egy olyan modern megközelítés, amely lehetővé teszi a hálózati infrastruktúra automatizált és dinamikus kezelését. A hagyományos, manuálisan beállított hálózatokkal szemben itt a konfigurációk és az erőforrások központilag, szoftveresen vezérelhetők, ami nagyobb rugalmasságot és gyorsabb reakcióidőt biztosít a különböző hálózati igényekre.

A fenti kép egy konkrét példát mutat be arra, hogyan alkalmaztuk ezt a megközelítést. A hálózatban egy **SkyNet Segélyhívó Központ** rendszer működik, amely modern technológiákat használ a gyors reagálás és biztonság érdekében. A weboldal az egyik címen érhető el mint pl ez, de nem csak ez az egy cím amin elérhető az oldal: **http://192.168.120.5/index.html** címen érhető el, és ez az interfész biztosít hozzáférést a szolgáltatásokhoz, például a gyors hívásfeldolgozáshoz, a földrajzi helymeghatározáshoz és a vészhelyzeti beavatkozásokhoz.

A programozott hálózatkonfiguráció lehetővé teszi az ilyen típusú rendszerek hatékony működését, hiszen a központi szervereken keresztül automatikusan kezelhetők az útválasztási szabályok, a redundancia, valamint a biztonsági protokollok. A rendszer például folyamatosan monitorozhatja a hálózat állapotát, és szükség esetén automatikusan újrakonfigurálhatja az eszközöket, hogy az adatforgalom mindig optimális legyen.

A képen látható weboldal is bizonyítja, hogy a szervereinken egy ilyen interfészt használtunk a hálózat menedzselésére és a segélyhívó rendszer biztosítására. A webes felület nemcsak az ügyfélkapcsolatot segíti, hanem a háttérrendszer konfigurációjának ellenőrzésére és finomhangolására is lehetőséget nyújt.

Összességében a programozott hálózatkonfiguráció kulcsfontosságú szerepet játszik a modern rendszerekben, különösen akkor, ha olyan kritikus infrastruktúrákról van szó, mint a segélyhívó központok, ahol a gyors reagálás és a megbízhatóság elsődleges szempont.

## ACL:

A hálózatunk **biztonsági funkciókkal ellátott forgalomirányítást** alkalmaz két kiemelt alhálózatban: a **sárga (Pécs) és a világoszöld (Eger)** hálózatban. Ezeken a helyszíneken **hozzáférési vezérlési listákat (ACL-eket)** használtunk, hogy növeljük a hálózat biztonságát és ellenőrizzük a forgalom áramlását.

Az **ACL-ek (Access Control Lists)** lehetővé teszik a hálózati csomagok **engedélyezését vagy blokkolását** meghatározott kritériumok alapján, például **IP-cím, protokoll vagy portszám** szerint. Ezzel a módszerrel biztosítható, hogy a nem kívánt vagy potenciálisan veszélyes forgalom ne érje el a védett alhálózatokat. A szabályokat úgy alakítottuk ki, hogy a **hálózat normál működését ne akadályozzák, de hatékonyan kiszűrjék a jogosulatlan hozzáféréseket**.

A **Pécs (sárga) alhálózatban** az ACL-eket elsődlegesen a **külső támadások elleni védekezésre és a belső erőforrások szegmentálására** használjuk. Az adott telephelyen például korlátozzuk bizonyos belső IP-címek hozzáférését az internet felé, ezzel csökkentve az illetéktelen adatforgalom kockázatát.

Az **Eger (világoszöld) alhálózatban** három különálló VLAN működik, így az ACL-eket **a VLAN-ok közötti forgalom szabályozására** is alkalmazzuk. Ezzel megakadályozzuk, hogy a különböző osztályokhoz vagy részlegekhez tartozó eszközök illetéktelenül hozzáférjenek egymás adataihoz. Emellett itt is biztosított a **külső forgalom szűrése**, amely meggátolja, hogy ismeretlen vagy gyanús IP-címek elérjék a hálózat kritikus erőforrásait.

Az ACL-ek használata jelentős mértékben növeli a hálózat **biztonságát és stabilitását**, mivel megakadályozza a nem kívánt kommunikációt, csökkenti a támadási felületet és lehetővé teszi a pontos **hálózati forgalomszabályozást**. Ezzel biztosítható, hogy a hálózat megfelelően védett maradjon anélkül, hogy a normál munkafolyamatokat akadályoznánk.

## Tűzfal:

A hálózat biztonságának növelése érdekében a legtöbb alhálózatban hardveres tűzfaleszközt alkalmaztunk. Ezek az eszközök kulcsszerepet játszanak az illetéktelen hozzáférések megelőzésében, a hálózati forgalom szűrésében, valamint a hálózati támadások elleni védelemben. A tűzfalak lehetővé teszik az egyes alhálózatok közötti forgalom szabályozását, valamint védelmet nyújtanak a külső és belső fenyegetésekkel szemben.

A jelenlegi hálózati topológia alapján a hardveres tűzfaleszközök minden alhálózatban megtalálhatóak, kivéve a piros és a sötétzöld alhálózatokat. Ezeken a helyeken más típusú biztonsági mechanizmusokat alkalmaztunk, vagy az infrastruktúra kialakítása nem igényelte a tűzfal beépítését. Azonban a többi alhálózat esetében a tűzfalak szerepe elengedhetetlen a stabil és biztonságos működéshez.

A tűzfalak lehetőséget biztosítanak a forgalomszűrésre, az IP-cím alapú hozzáféréskorlátozásra és az adathalász vagy egyéb rosszindulatú tevékenységek blokkolására. Az alkalmazott hardveres megoldások képesek a hálózati csomagok részletes elemzésére és azok protokollszintű vizsgálatára, így az esetleges biztonsági fenyegetéseket azonnal kiszűrik.

Összességében a hardveres tűzfaleszközök alkalmazása jelentős előrelépést jelent a hálózat biztonságának garantálásában. A különböző alhálózatok megfelelő védelmének biztosítása révén minimálisra csökkenthető az illetéktelen behatolások és a hálózati fenyegetések kockázata, miközben a hálózati forgalom zavartalanul működhet.

## Linux és Windows szerver:

A hálózati infrastruktúra tervezése során fontos szempont volt, hogy a rendszer tartalmazzon legalább egy Linux és egy Windows alapú kiszolgálót, amelyek különböző szolgáltatásokat biztosítanak a hálózat számára. Az előzetes tervek szerint a következő szolgáltatásokat kellett volna implementálnunk:

* **Címtárszolgáltatás (Active Directory vagy LDAP)**: A hálózatban működő eszközök és felhasználók központi hitelesítésére és jogosultságkezelésére.
* **DHCP (Dynamic Host Configuration Protocol)**: Az IP-címek automatikus kiosztására a hálózati eszközök számára.
* **DNS (Domain Name System)**: A hálózati nevek és IP-címek összerendelésére.
* **HTTP/HTTPS**: Webszolgáltatások biztosítására.
* **Fájl- és nyomtatómegosztás**: Központi adattárolás és nyomtatási szolgáltatások elérhetővé tételére.
* **Automatizált mentés**: A rendszeres adatmentés biztosítására a szerverek és kliensgépek védelme érdekében.
* **Kliens számítógépekre automatizált szoftvertelepítés**: Az új eszközök gyors és hatékony beállítására.

**Cisco Packet Tracer korlátai és a megvalósítás kihívásai**

Bár a fenti szolgáltatások kritikus szerepet játszanak egy vállalati hálózat működésében, a **Cisco Packet Tracer** szimulációs környezet nem támogatja ezek teljes körű megvalósítását. A szoftver elsősorban hálózati eszközök (routerek, switchek, végpontok) működésének szimulációjára szolgál, és nem rendelkezik a fenti szolgáltatások megfelelő modellezéséhez szükséges szerveroldali támogatással.

Ennek következtében a projekt során nem tudtuk ténylegesen beállítani a Linux és Windows szervereket a kívánt szolgáltatásokkal, de a hálózati topológia tervezésekor figyelembe vettük a szerverek szükségességét, és úgy alakítottuk ki a hálózatot, hogy ezek a kiszolgálók egy valós környezetben integrálhatók legyenek.

# Csapatmunka

**Vajta Gerda vállalt szerepei és felelősségi területei a következők voltak a projekt során:**

1. **Project manager (Projektmenedzser)** 
   * Feladata a projekt egészének irányítása és felügyelete.
   * Koordinálta a csapatmunkát és ütemezte a fejlesztési folyamatokat.
   * Hatékony kommunikáció biztosítása a csapattagok között és a projekt érintettjeivel.
   * Kezelte mind projekt menedzser a jirát és a git felűletét.
2. **A prototípus**

* Megtervezte a prototípust.
* Majd később segített a fontos lépésekben a prototípus előre haladása érdekében pl:
* Eszközök be ip-zése, valamint eszközök elnevezése
* VPN konfigurálás
* Statikus és dinamikus címfordítás
* Tűzfalak konfigurálása
* Szervereken lévő weboldal konfigurálása
* IPv6 Beálítása

1. **A tesztelés**
   * Levezetve megcsinálta a 100 tesztelésből álló Exel dokumentumot.
2. **A Ppt**
   * Megcsinálta a szükséges ppt-t a részletes projekt prezentálásához
3. **A Videó**

* Segített felvenni a szükséges 2-5 perc terjedelmű videót.

**Horváth Máté vállalt szerepei és felelősségi területei a következők voltak a projekt során:**

1. **A prototípus**

* Segített minden szükséges lépésben a projektmenedzsernek

pl:

* DHCP konfigurálás
* Vlan megcsinálása
* VPN konfigurálás
* WAN megoldás kiépítése
* Statikus és dinamikus forgalomirányítás konfigurálása
* IPv6 Beálítása

1. **Dokumentáció**

* Megcsinálta a több mint 20 oldalas dokumentációt. A benne szereplő dolgokkal pl:
* A hálózat részletes leírt működése
* A csapatmunka leírása
* A célok megfogalmazása
* A jövőbeli tervek leírása

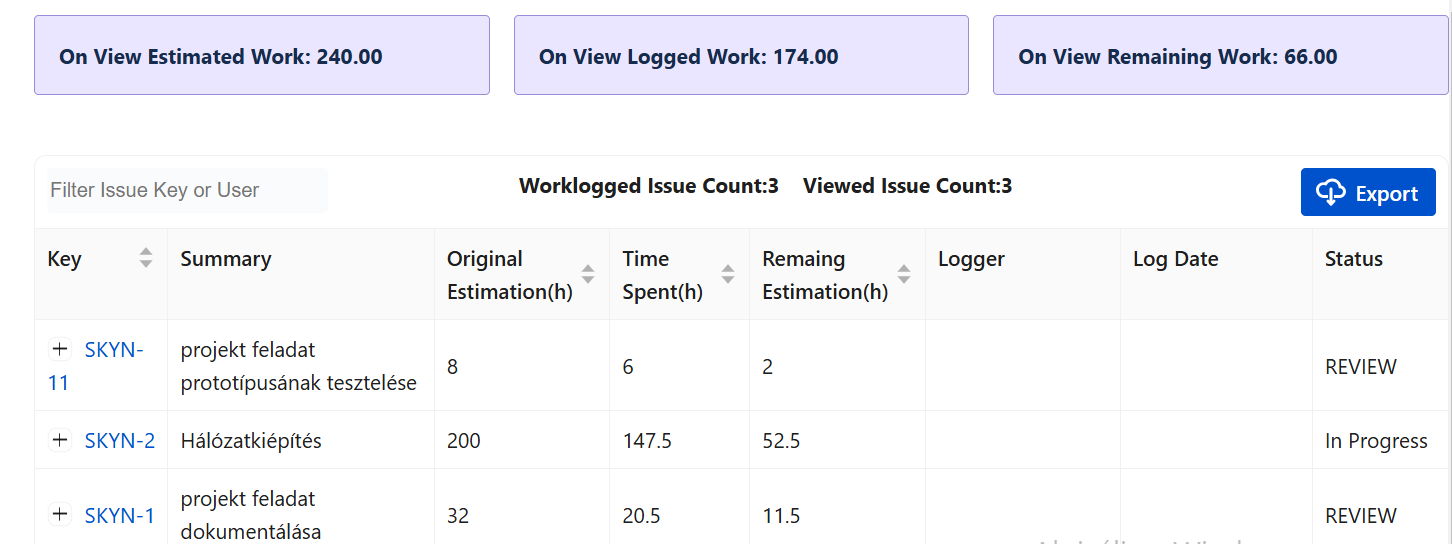
1. **A Ppt**

* Segített a projektmenedzsernek a ppt megcsinálásában

1. **A videó**

* Segített a projektmenedzsernek felvenni a prototípusról készült videót

## Jiras haladásunk az egész projekt alatt:



# Jövőbeli tervek:

A jövőbeli tervek a vállalati hálózati infrastruktúra továbbfejlesztésére irányulnak, hogy biztosítsák a zökkenőmentes és biztonságos működést a folyamatosan bővülő és fejlődő környezetben. Az alábbi fejlesztéseket tervezzük:

1. **További telephelyek integrálása**: A hálózati infrastruktúra folyamatos bővítésével új telephelyek és irodák csatlakoztatása szükséges, hogy a vállalat növekvő igényeit és a távoli munkavégzés szükségleteit kiszolgáljuk. Az új telephelyek biztonságos összekapcsolása VLAN alapú szegmentálással lesz biztosítva, hogy különböző osztályok és csoportok forgalmát elkülönítsük.
2. **Redundáns megoldások fejlesztése**: A hálózati redundancia tovább bővül a második és harmadik rétegbeli megoldásokkal. A hibaelhárítás és a zökkenőmentes működés érdekében olyan protokollokat implementálunk, mint a Spanning Tree Protocol (STP) és dinamikus forgalomirányítási protokollok (OSPF, EIGRP), amelyek biztosítják a folyamatos rendelkezésre állást.
3. **IPv4 és IPv6 egyidejű támogatása**: A jövőben teljes körű dual-stack címzési konfigurációval működünk, hogy biztosítsuk mindkét protokoll, IPv4 és IPv6 zökkenőmentes működését, és megfeleljünk a növekvő adatforgalmi igényeknek, valamint a jövőbeli bővítéseknek.
4. **Vezeték nélküli hálózati fejlesztések**: A vezeték nélküli hálózat tovább fejlődik, hogy biztosítsa a mobil eszközök csatlakoztatását minden telephelyen. A jövőbeli bővítések során erősítjük a WLAN biztonságát titkosítással és eszközhitelesítéssel.
5. **Forgalomirányítási rendszerek továbbfejlesztése**: A forgalomirányítási rendszert folyamatosan optimalizáljuk, hogy még rugalmasabban alkalmazkodjon a hálózati környezet változásaihoz. A dinamikus forgalomirányítást és a statikus útvonalakat egyaránt finomítjuk a jobb teljesítmény és a gyorsabb hibaelhárítás érdekében.
6. **Címfordítási (NAT) technológiák fejlesztése**: A címfordítási mechanizmusokat fejlesztjük, hogy a privát IP-címek védelme és a hálózati forgalom kezelése még hatékonyabb legyen, figyelembe véve a bővülő eszközkörnyezetet és felhasználói igényeket.
7. **WAN összeköttetések továbbfejlesztése**: A távoli telephelyek közötti WAN összeköttetések fejlesztése révén biztosítjuk a zökkenőmentes kommunikációt és az adatcserét a vállalat különböző helyszínei között, figyelembe véve a folyamatosan változó üzleti környezetet.
8. **VPN infrastruktúra bővítése**: A virtuális magánhálózati (VPN) kapcsolatok szélesebb körű bevezetése lehetővé teszi a távoli dolgozók számára, hogy biztonságosan csatlakozhassanak a vállalati hálózathoz, ezáltal növelve a munkahelyi rugalmasságot és a biztonságot.
9. **Biztonsági megoldások további erősítése**: A hálózati biztonság további erősítése érdekében a jövőbeli fejlesztések során fokozottan alkalmazzuk a tűzfalakat és a hozzáférés-ellenőrzési listákat (ACL), hogy megvédjük a vállalati infrastruktúrát a különböző kibertámadásokkal szemben.

A jövőbeli terveink biztosítják, hogy a hálózati infrastruktúra a legújabb technológiai trendeknek és biztonsági előírásoknak megfelelően működjön, támogatva a vállalat növekedését és a folyamatosan változó munkakörnyezetet.