****

**VIZSGAREMEK**

Készítették:

Minta Áron – Minta János - Minta István

Konzulens:

Minta Péter

Miskolc

2025.

Miskolci SZC Kandó Kálmán Informatikai Technikum

Miskolci Szakképzési Centrum

Informatikai rendszer- és alkalmazás-üzemeltető technikus

Dokumentáció

tudnivalók a záródolgozathoz

Minta Áron – Minta János - Minta István

2024-2025

Tartalomjegyzék

Tartalom

[1. Fő Telephely 1](#_Toc193705805)

[2. Ip Táblázat 2](#_Toc193705806)

[3. SSH 3](#_Toc193705807)

[4. l2 Security 4](#_Toc193705808)

[4.1 Portbiztonság 4](#_Toc193705809)

[5. Vlanok 8](#_Toc193705810)

[6. Vlanok Közötti Forgalom 10](#_Toc193705811)

[7. ASA-tűzfal 11](#_Toc193705812)

[8. DhcpV4 12](#_Toc193705813)

[9. Ipv6 13](#_Toc193705814)

[10. HSRP 14](#_Toc193705815)

[11. Ether-Channel 15](#_Toc193705816)

[2. WIFI Telephely 16](#_Toc193705817)

[13. SSH elérés access list 17](#_Toc193705818)

[14. WIFI-Router 18](#_Toc193705819)

[15. Laptop , Telefon csatlakoztatása a WIFI hálózathoz 20](#_Toc193705820)

[16. PAT 21](#_Toc193705821)

[3. SERVER Telephely 22](#_Toc193705822)

[17. Windows server 23](#_Toc193705823)

[18. Windows DHCP server 24](#_Toc193705824)

[19. Windows Backup 25](#_Toc193705825)

[20. Active Directory 27](#_Toc193705826)

[21. DNS Szerver 28](#_Toc193705827)

[22. WEBSERVER 29](#_Toc193705828)

[22. http 30](#_Toc193705829)

[23. https 31](#_Toc193705830)

[20. Linux Szerver 32](#_Toc193705831)

[24. SAMBA 33](#_Toc193705832)

[25. FTP Szerver 35](#_Toc193705833)

[4. Forgalom Irányítás 36](#_Toc193705834)

[26. OSPF 37](#_Toc193705835)

[27. WAN (PPP) 38](#_Toc193705836)

[28. GRE-tunnel 39](#_Toc193705837)

[Mellékletek 40](#_Toc193705838)

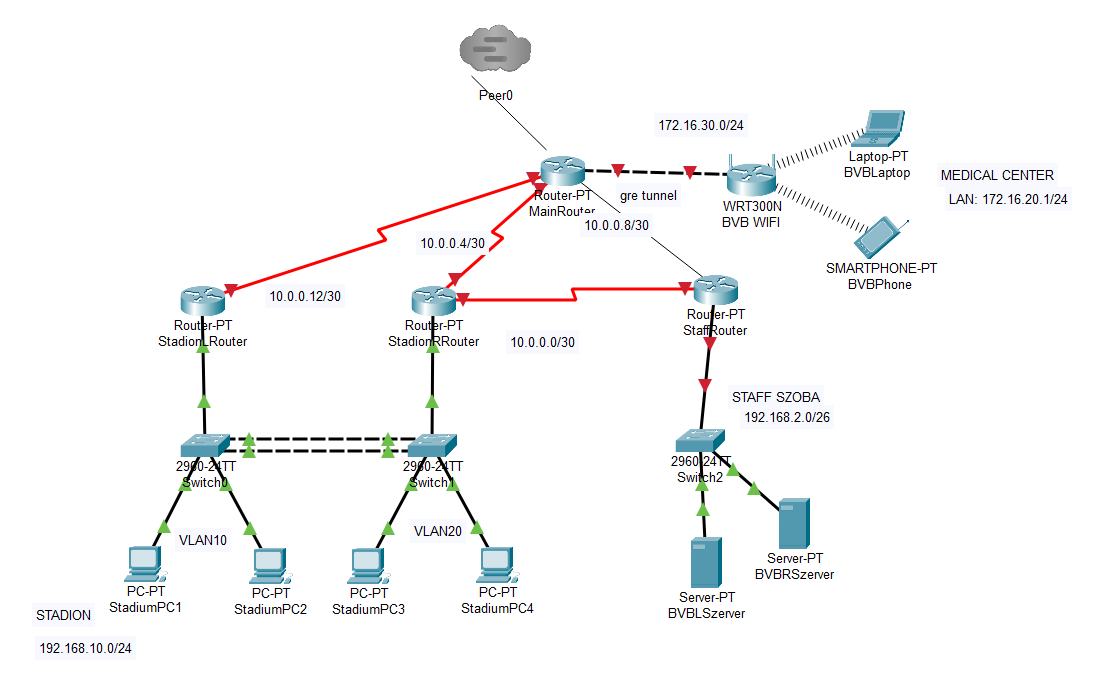
[Index.js: 41](#_Toc193705839)

[index.html: 42](#_Toc193705840)

BVB projektmunka

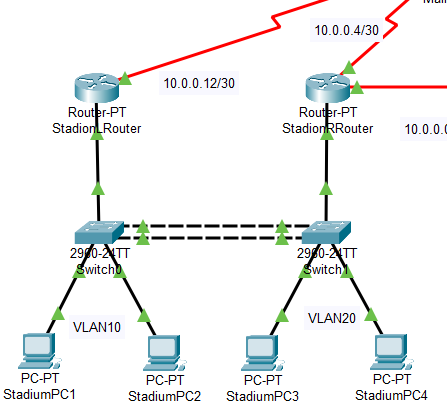
Ebben a prjokektmunkában egy kitalált hálózatot valósítottunk meg a hálózat alapja a borussia dortmund futballcsapat hálózatára épül

azért választottuk ezt a projektet mert nagy rajongói vagyunk a futballnak valamint A Borussia Dortmund internetes hálózata az egyik legfejlettebb és legdinamikusabban fejlődő platform a futballklubok világában. A csapat nemcsak a pályán nyújtott teljesítményével, hanem online jelenlétével is kiemelkedik, hiszen a szurkolók és rajongók számára az internetes térben is folyamatosan új élményeket és lehetőségeket kínál. A projektünk során a különböző hálózati beállításainkat a fizikai eszközök konfigurációiból mentettük ki képek formájában.



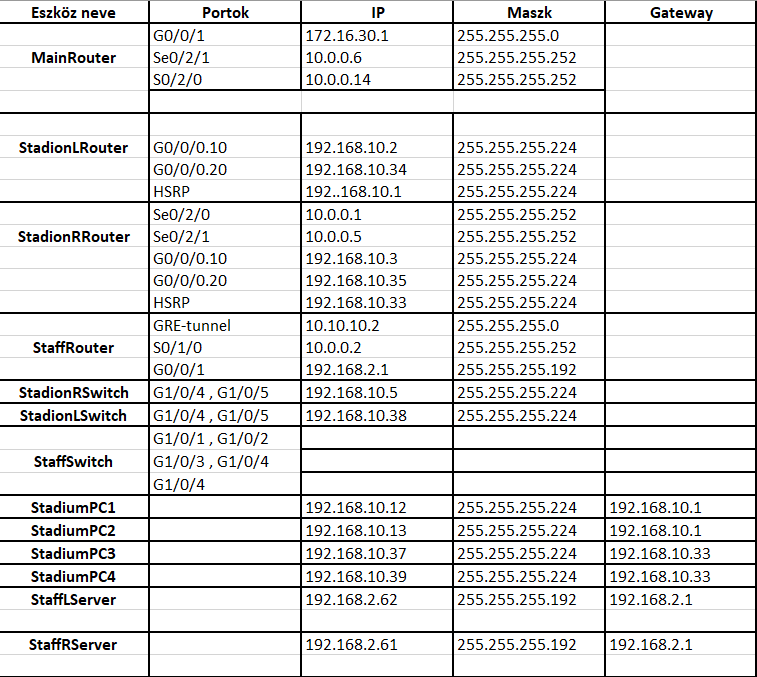
A projektünk 3 különböző telephelyből áll mind a 3 telephely működését szeretnénk bemutatni a dokumentáció során.

# Fő Telephely



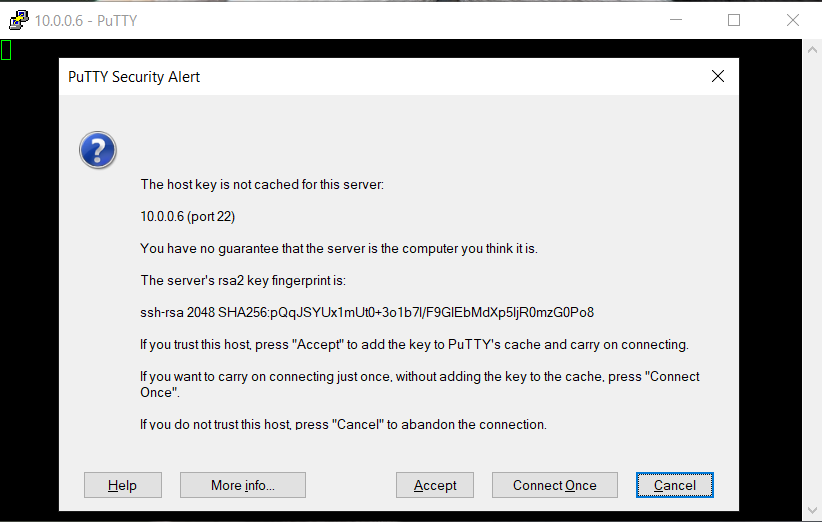
Az első fő telephelyünkben a stadionban lévő hálózati részt mutatjuk be ahol a legtöbb biztonsági és redundanciát biztosító beállításokat végeztük.

## 2. Ip Táblázat



A hálózatban használt ip címeket a VLSM calculator segítségével osztottuk fel és ez alapján állítottuk be.

## SSH



Biztonságos távoli elérést az ssh-val oldottuk meg ezt azért hoztuk létre hogy biztonságosan tudjuk távolról menedzselni a hálózati eszközeinket (roueter , switch).

A képen szöveg, Betűtípus, képernyőkép látható

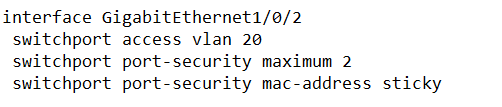
Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Az ssh-hoz szükséges egy domain név amit mi a bvb.hu –ra neveztünk el ami egyébként a weboldalunk domain neve is lett az ubuntu serveren . Odafigyeltünk hogy minden eszközzel csak biztonságosan lehessen belépni amit a transport input ssh parancsal hoztunk létre.

## 4. l2 Security

### 4.1 Portbiztonság

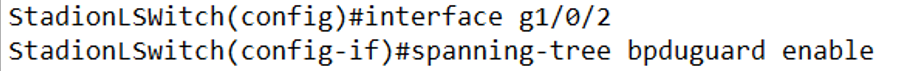
A port-security beállítást azért hoztuk létre hogy a hálózati switchek portjainak védelmet biztosítson amely megakadályozza az illetéktelen eszközök csatlakozását a hálózathoz.



A portbiztonságot úgy állítottuk be azokon a portokon ahol végberendezések vannak hogy maximum 2 végeszköz tudjon csatlakozni. Ha esetleg egy harmadik eszköz rá akar csatlakozni erre a portra a portbiztonság letiltja a portot mivel a legszigorúbb szabályt alkalmaztuk a violation shutdown –t.

#### 4.1.1 Bpduguard

A BPDU Guard egy biztonsági mechanizmus, amely megakadályozza, hogy nem kívánt BPDU csomagok érkezzenek a hálózati portokra, így védve a hálózati topológia integritását, és megakadályozza a huroképződést.



A projektünkben a végberendezések felé engedélyezve van a BPDUGUARD.

#### 4.1.2 Spanning-Tree

A **spanning tree** biztosítja a hurokmentes adatforgalmat egy kapcsolózott hálózaton. A hálózati kapcsolók között előfordulhatnak hurkok, A spanning tree protokoll segít abban, hogy a kapcsolók között csak egy aktív útvonal legyen, így elkerülve a hurkokat.



A **RAPID PVST** egy olyan hálózati protokoll, amelyet a projektünk stabilitására és hatékonyságának növelésére használjuk. Ennek a protokollnak a segítségével gyorsabban detektálhatjuk és kezelhetjük a hálózaton belüli hibaelhárításokat.

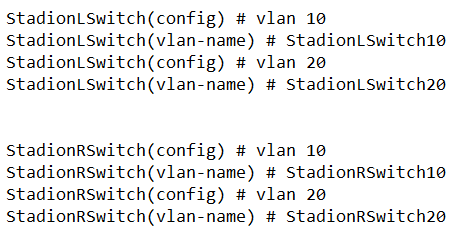
#### 4.1.3 Portfast



A **PortFast** funkció szerepe a hálózatunkban az, hogy gyorsabbá teszi a kapcsolók portjainak aktiválódását, amikor eszközöket csatlakoztatunk a hálózathoz.

## 5. Vlanok

VLAN-okat a hálózati forgalom logikai szeparálására hoztuk létre, hogy csökkentsük a forgalom zűrzavart és javítsuk a biztonságot. Ezt általában switch eszközök konfigurálásával érhetjük el, ahol különböző portokhoz rendeljük a VLAN-okat.



A fő telephelyen két kapcsolót (switch) használtunk mind a két kapcsolon létrehoztuk a 10-es és a 20-as vlant valamint a használt portokat hozzá rendeltük.

## 6. Vlanok Közötti Forgalom

VLAN-ok közötti forgalom irányítása azért fontos, mert lehetővé teszi a különböző hálózati szegmensek közötti biztonságos és szabályozott kommunikációt. Ezt routerek segítségével valósítjuk meg a projektünkben azért hogy meghatározzuk, mely VLAN-ok férhetnek hozzá egymáshoz.

A képen szöveg, Betűtípus, fehér, képernyőkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, Betűtípus, fehér látható

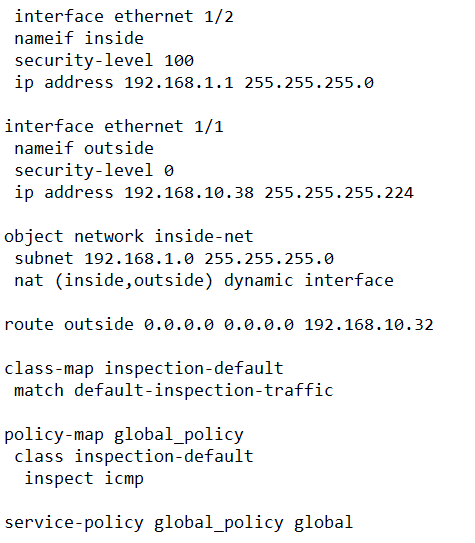
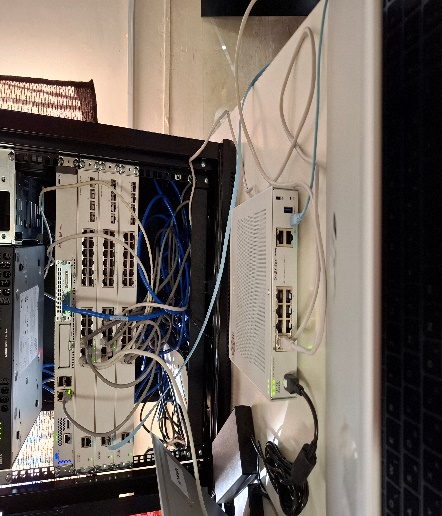
Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A hálózatunkban alinterfészek segítségével oldottuk meg a vlanok közötti forgalmat.

A router switch felé vezető portján hoztuk létre az alinterfészeket melynek az azonositói a vlanok számával egyezik meg . Az encapsulation dot iq parancsal tudják a hálózati eszközök hogy melyik vlanhoz tartozik a forgalom. A felosztott hálózat második kiosztható címét kapták a routerek ip cím ként. Azért a másodikat kapták meg az eszközök mert az első kiosztható cím lesz a hsrp virtualis címe.

## 7. ASA-tűzfal

A tűzfal (firewall) szerepe a hálózaton alapvetően a biztonság biztosítása és a nem kívánt hozzáférések megakadályozása. A tűzfal egy olyan hálózati biztonsági eszköz, amely figyeli és szabályozza a bejövő és kimenő adatforgalmat egy számítógépes rendszer vagy hálózat között.

Az ASA tűzfal a hálózatunkban a StadionRSwitch és a stadionPC4 között let beiktatva . Az Ethernet ½ az inside port ami a végberendezés felé megy erre a pcre egy külön hálózatot hoztunk létre. Az Ethernet 1/1 az outside ami a complex hálózat felé egy ott az adott halózatból állítottunk be egy címet. Az object network inside-net parancsba a 192.168.1.0 –ás hálozat címet adtuk meg. Az elérés céljábol a route outside parancshoz a kulső hálózat network címét írtuk be.

## 8. DhcpV4

A DHCPv4 szerepe egy hálózatban, hogy automatikusan kiossza az IPv4 címeket és más hálózati konfigurációkat a klienseknek. Ez megkönnyíti a hálózatkezelést, mivel nem szükséges manuálisan konfigurálni minden eszközt.

A képen szöveg, Betűtípus, képernyőkép, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A hálózatban 192.168.10.1 - 192.168.10.11 között zártuk ki a címeket ami annyit jelent hogy a kizárt intervallumból a dhcp nem oszthat címet a végberendezéseknek. Azért zártuk ki hogy ezeket statikus IP-címekkel rendelkező eszközök (például routerek, szerverek) számára fenntartsuk. Így elkerülhetjük a címütközést a dinamikusan kiosztott címekkel.

A network az adott hálózat hálózati címe default router meg a hsrp virtuálís cime ez alapján fog a router címet osztani a klienseknek.

## 9. Ipv6

Az IPv6 szerepe a hálózatban, hogy lehetővé tegye az eszközök közötti kommunikációt a növekvő IP-címigények kielégítésére, mivel az IPv4 címek kimerültek. Az IPv6 nagyobb címteret biztosít, javítja a hálózati biztonságot, és hatékonyabb eszközök közötti kommunikációt tesz lehetővé.

A képen szöveg, Betűtípus, fehér, tipográfia látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A beállított link-local cím ás ipv6-os cím után a engedélyezzük az ipv6-ot az ipv6 enable parancsal majd engedélyezzük az ipv6 forgalmat az ipv6 unicast-routing parancsal.

## 10. HSRP

StadionLRouter

StadionRRouter



A HSRP egy redundancia protokoll, amely lehetővé teszi, hogy két vagy több router közösen biztosítson egy virtuális IP-címet, amelyet az eszközök az alapértelmezett átjáróként használnak. Ha az elsődleges router meghibásodik, a második átveszi a forgalmat, így biztosítva a hálózat folytonosságát és magas rendelkezésre állást.

A képen szöveg, Betűtípus, fehér, tipográfia látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.A képen szöveg, Betűtípus, képernyőkép, fehér látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

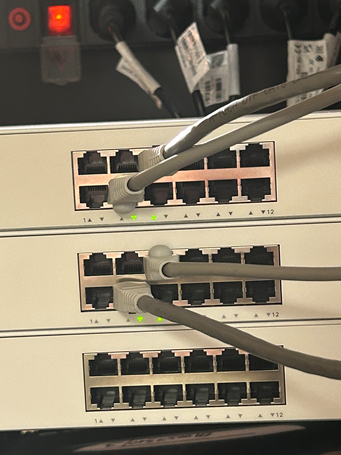
A hsrp virtuális ip címe mind a két eszközön a felosztott hálózat első kiosztható címe lett.

A standby 1 , 2 preempt parancsal allítjuk be a prioritást és , ez alapján dönti el az eszköz melyikük lesz az aktiv és a standby router.

## 11. Ether-Channel

StadionLSwitch

StadionRSwitch



Az EtherChannel szerepe a hálózatban, hogy több fizikai linket egy logikai kapcsolattá kombináljon, ezáltal növelve a hálózati sávszélességet és biztosítva a forgalom redundanciáját.

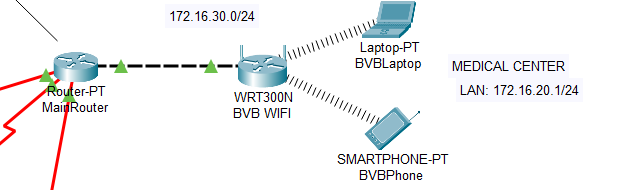
A képen szöveg, Betűtípus, képernyőkép, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.



etherchannel kapcsolat a két switch között van a hálózatunkban a használt portokat az interface range parancsal összefogjuk az adott switch-eken majd a channel group 1 mode active illetve passive parancsal lacp összeköttetést létesítünk. Az LACP előnye, hogy automatikusan kezeli és konfigurálja az EtherChannel-t, így biztosítva a linkek közötti dinamikus terheléselosztást és redundanciát.

# 2. WIFI Telephely



A WIFI telephelyünkben a stadionban lévő WIFI elérést szolgáltató eszközöket arra ssid-vel kapcsolódó végberendezéseket és , WIFI router beállításait mutatjuk be.



## 13. SSH elérés access list

Az ACL a hálózatban szabályozza, mely eszközök férhetnek hozzá a routerekhez vagy switch-ekhez. Az SSH eléréshez alkalmazott ACL-ek lehetővé teszik, hogy csak meghatározott IP-címekről érkező kapcsolatok legyenek engedélyezettek, így növelve a hálózat biztonságát.



Mivel a hálózatunkban minden eszközön biztosítva van biztonságos távoli elérés ( SSH ) , ezért teszt szempontjából a 192.168.10.13 – as ip vel rendelkező végberendezéstől megtiltottuk a távoli elérést az access-list 1 deny host 192.168.10.13 -as paranccsal.

## 14. WIFI-Router

A WiFi router kulcsszerepet játszik a modern hálózatokban, mivel egyszerre több funkciót is ellát.A WiFi router egy modemhez csatlakozik , és biztosítja az internet-hozzáférést a projektünkben az irodai eszközök számára.

A képen szöveg, elektronika, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, képernyő, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus, képernyő látható

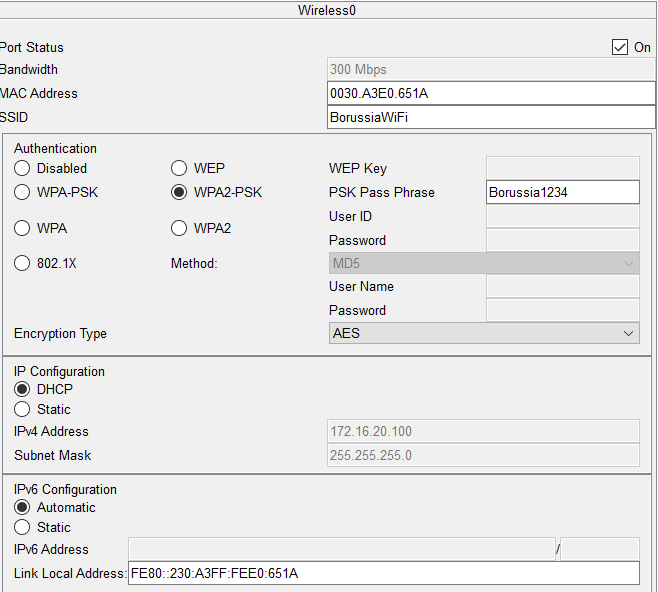
Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A WiFi hálózatot **BVB WIFI** néven állítottuk be, **WPA2-Personal** biztonsági móddal és **AES** titkosítással. A jelszó **Borussia1234 lett . A WAN IP a 172.16.30.3 -at kapta /24 – es maszkkal és, 172.16.30.1 -es átjáróval valamint 8.8.8.8 -as dns server címmel. A dhcp server 172.16.20.100 -tól 150 -ig oszt címet. A router ip címe pedig a 172.16.20.1 lett /24 – es alhálózati maszkkal.**

## 15. Laptop , Telefon csatlakoztatása a WIFI hálózathoz



A laptop és , a telefon csatlakoztatásához tartozó kép a cisco packet tracer-ből lett beillesztve mivel ez jobban szemlélteti a végberendezések csatlakozási útját a hálózathoz mint a fizikai eszközök beállításai. Az SSID BorussiaWiFi a jelszó titkosítási fajtája WPA2-PSK a hálózat jelszava Borussia1234.

## 16. PAT

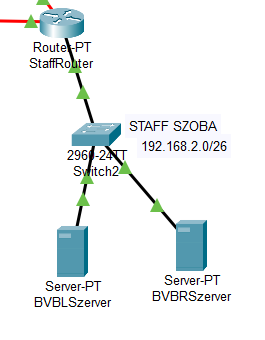
A **PAT**  szerepe a hálózatban az, hogy lehetővé tegye több eszköz számára, hogy egyetlen **nyilvános IP-címen** keresztül kommunikáljon az interneten, miközben a belső hálózaton különböző privát IP-címeket használ.

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Ez a parancs hogy ip nat inside source list 2 interface GigabitEthernet0/0/0 overload dinamikus NAT-ot állít be. A 2-es számú hozzáférési listában szereplő IP-címeket a **GigabitEthernet0/0/0** interfész nyilvános IP-címére fordítja le. Az overload kulcsszó azt jelenti, hogy több belső IP-cím egyetlen külső IP-címet oszt meg, és a kapcsolatokat portok segítségével különbözteti meg .Az ip access-list standard 2 egy standard hozzáférési lista amely meghatározza, hogy mely belső IP-címeket kell NAT-olni. A 10 permit 192.168.0.0 0.0.255.255 parancs engedélyezi a 192.168.0.0/16 tartomány NAT-olását , a 20 permit 172.16.0.0 0.0.255.255 meg engedélyezi a 172.16.0.0/16 tartomány NAT-olását.

# SERVER Telephely



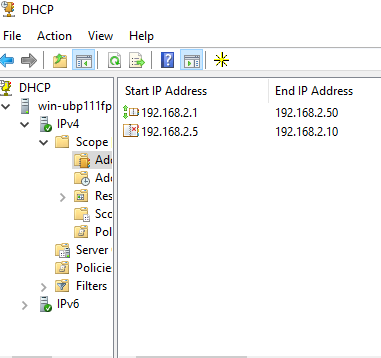
A SERVER telephelyünkön a Windows , Linux ( Ubuntu , Samba ) beállításait muatjuk be a servereken belüli konfigurációkat valamint a DHCP server működését .

## 17. Windows server

A **Windows Server** szerepe a hálózatban az, hogy központi kiszolgálóként biztosítja a különféle hálózati szolgáltatásokat, mint például a fájlmegosztás, a DNS, a DHCP, az e-mail kezelést (Exchange Server) és az Active Directory-val történő felhasználókezelést.

### 18. Windows DHCP server

A **DHCP**  egy hálózati protokoll, amely lehetővé teszi, hogy a hálózati eszközök automatikusan IP-címet kapjanak, anélkül hogy manuálisan kellene beállítani őket. A **Windows DHCP Server** feladata, hogy automatikusan kiossza az IP-címeket a hálózati kliensek számára, mint például számítógépek, nyomtatók, okoseszközök és egyéb eszközök, amelyek a hálózathoz csatlakoznak.

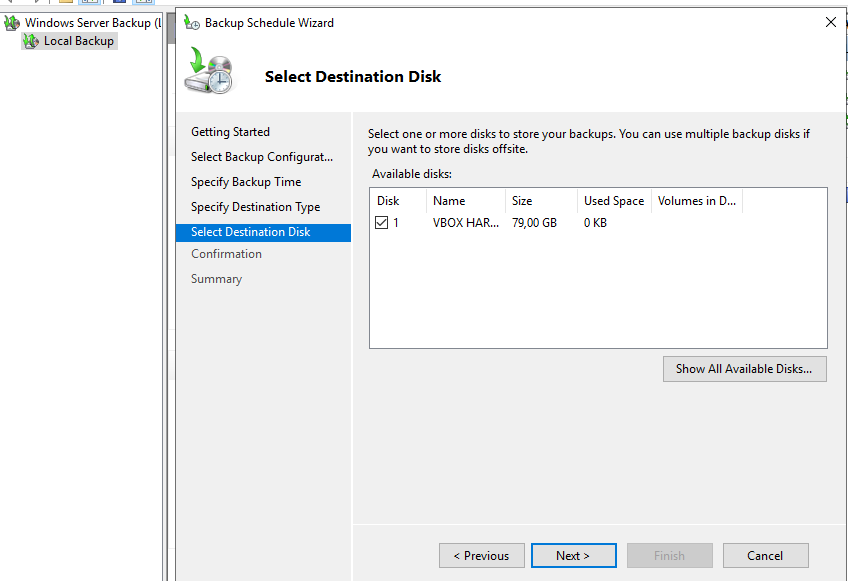


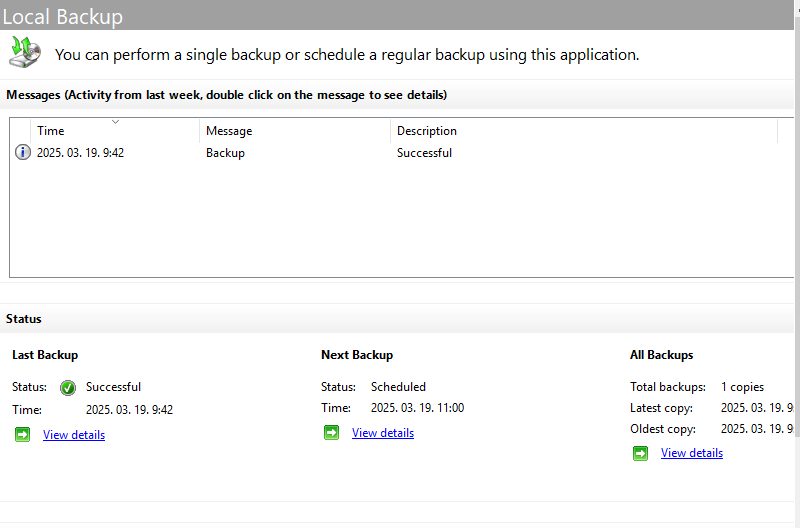
A dhcp server 192.168.2.1 – 192.168.2.50 –ig tud címet osztani de mivel a 192.168.2.5 – 192.168.2.10-ig kizartunk címeket a hálózati hurkok elkerülése miatt , ezért cask 45 hostot képes ip címmel ellátni.

### 19. Windows Backup

Ez egy automatizált mentés amit saját magunk álltal beállított időközönként ment a szerver.

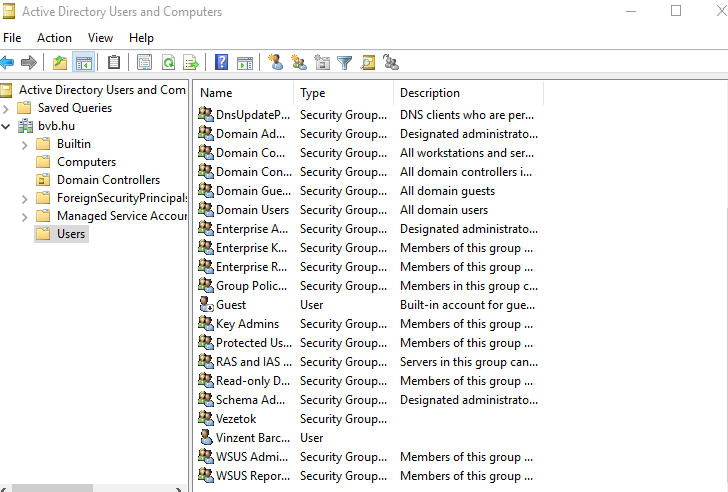
Azért fontos hogy az adott beállítások mindig elérhetőek legyenek a szerveren ne vesszen el semmilyen konfiguráció.Ez egy külön merevlemezen létrehozott mentés ha amit akkor tudunk használni mikor hiba keletkezik a szerverben.





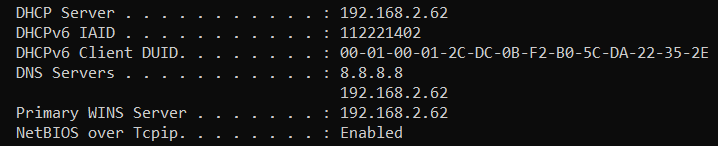
### 20. Active Directory

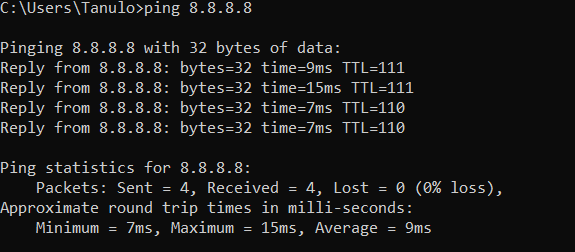
A felhasználók, számítógépek és egyéb erőforrások központi kezelésére szolgál egy hálózaton belül. Hálózati erőforrások kezelését segíti, és fontos szerepet játszik az informatikai infrastruktúra biztonságos működtetésében.



### 21. DNS Szerver

A DNS szerver a hálózaton domain nevek és IP címek közötti leképezést végez. Lehetővé teszi a felhasználóknak, hogy domain nevekkel, például www.bvb.hu kapcsolódjanak a kívánt weboldalakhoz, anélkül hogy IP címeket kelljen használniuk. A DNS biztosítja a hálózaton belüli gyors és hatékony névfeloldást.





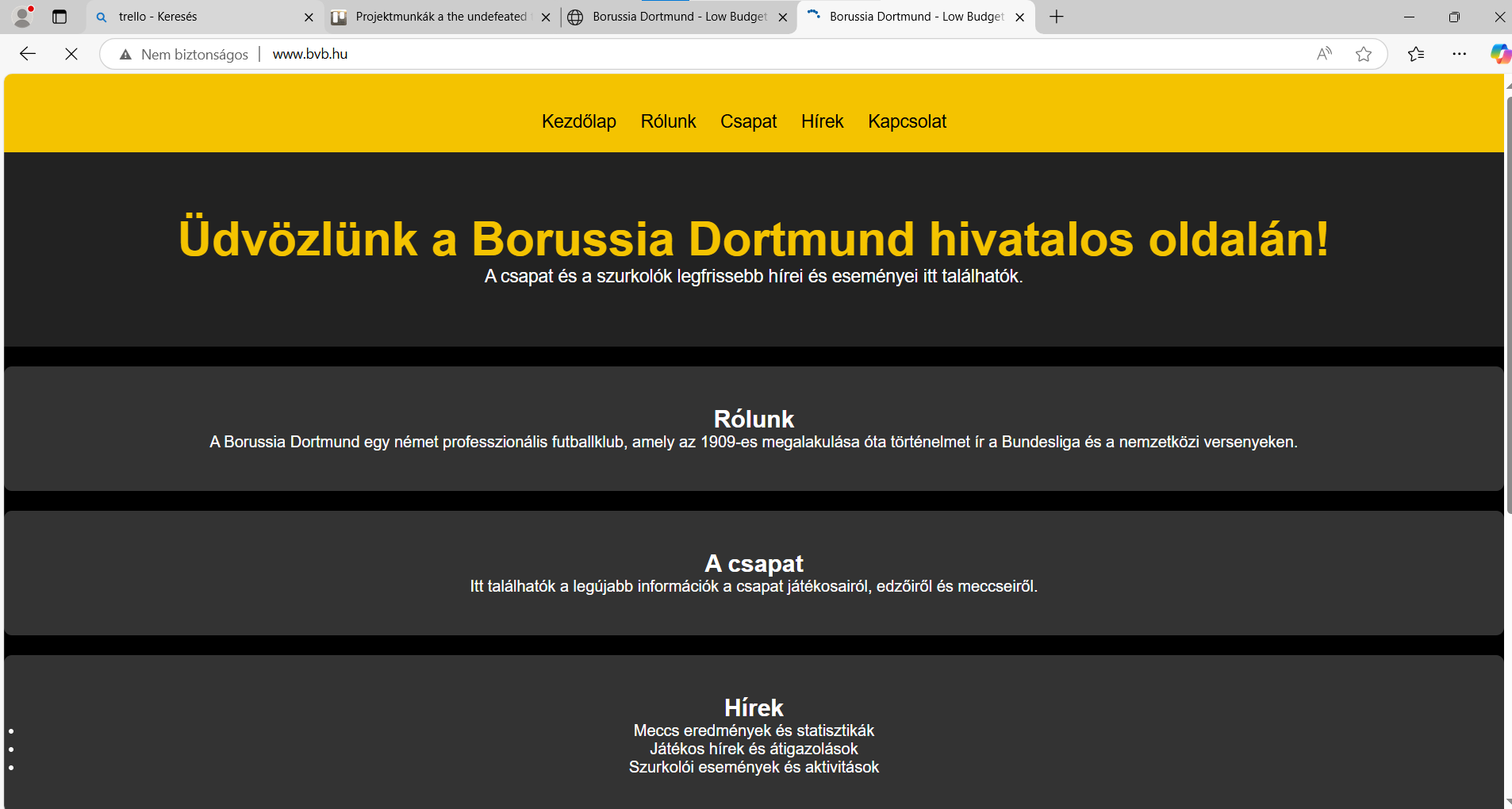
## 22. WEBSERVER

A Borussai Dortmund hivatalos oldalát a 192.168.2.62 illetve a [www.bvb.hu](http://www.bvb.hu) domain en is elértük.

Ezt a szolgáltatás mindegyik telehelyről teszteltük és mindenhol tökéletesen működött.

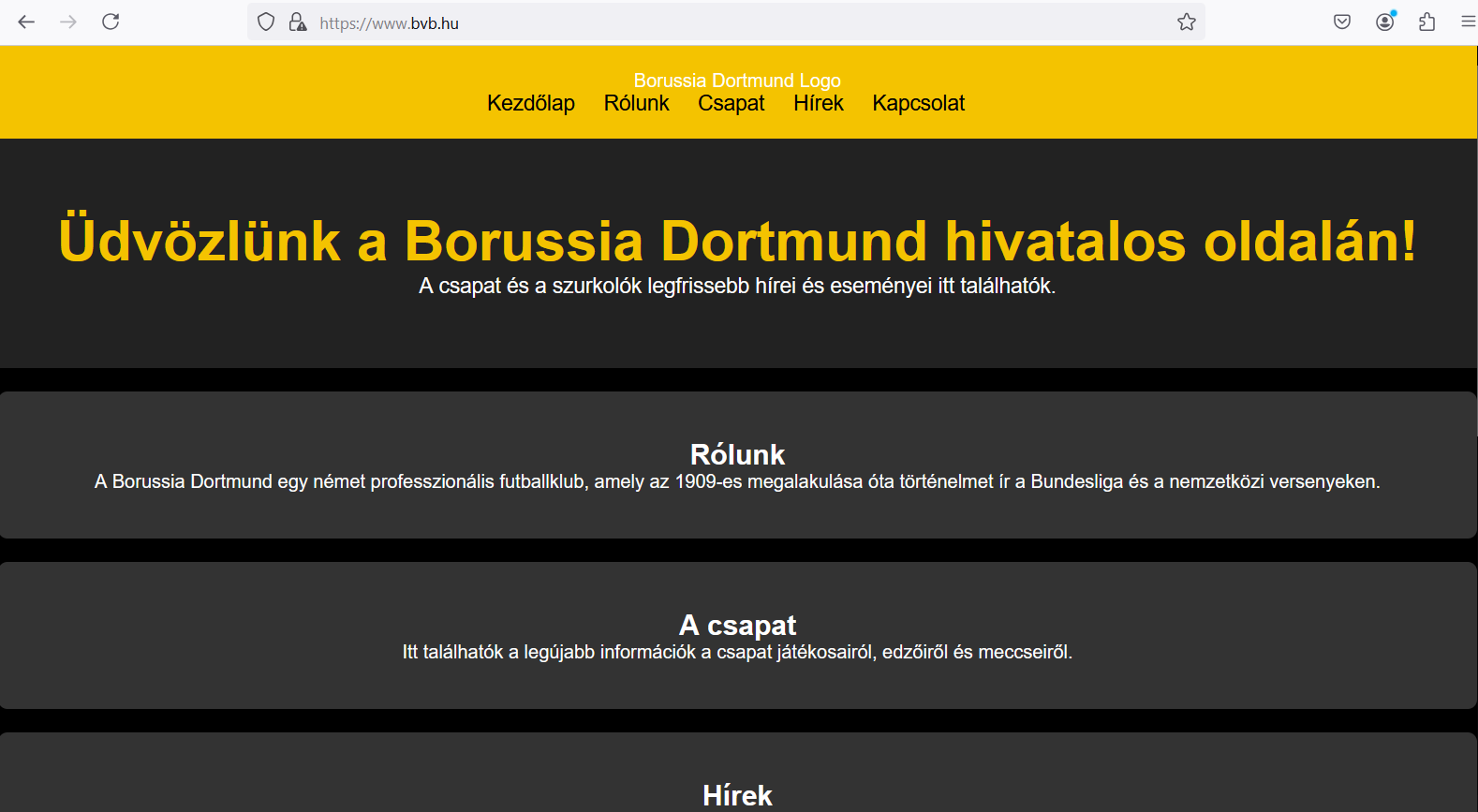
http és https-en is sikeresen elértük a szervert a különbség a kettő közt hogy a https biztonságos.

### 22. http



A HTTP HyperText Transfer Protocol egy alapvető protokoll, amely a weboldalak böngészéséhez szükséges kommunikációt teszi lehetővé az interneten. A HTTP segítségével a böngészők kéréseket küldenek a szervereknek, és azok válaszokat küldenek vissza, amelyek tartalmazzák a weboldalak tartalmát. A HTTP használatával sikeresen elértük a weboldalunkat.

### 23. https



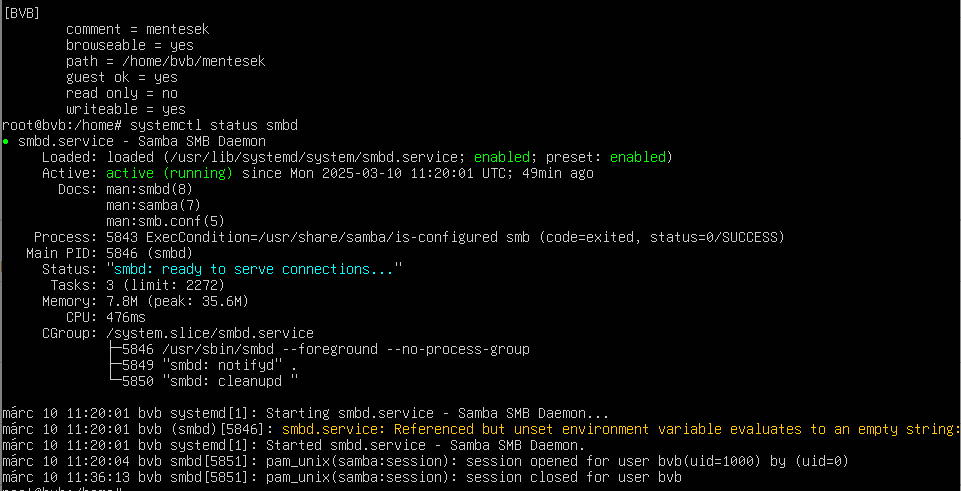
A **HTTPS** (HyperText Transfer Protocol Secure) a **HTTP** biztonságos változata, amely titkosítja az adatforgalmat a böngésző és a webkiszolgáló között.A webservert https en keresztül elértük biztonságosan.

# 20. Linux Szerver

A Linux szerver a hálózaton különböző szolgáltatásokat biztosít, például fájlmegosztást, webhostingot vagy adatbázis-kezelést. Lehetővé teszi a felhasználók számára a fájlok és alkalmazások elérését és kezelését, miközben támogatja a különböző protokollokat, mint például FTP vagy Samba.

### 24. SAMBA

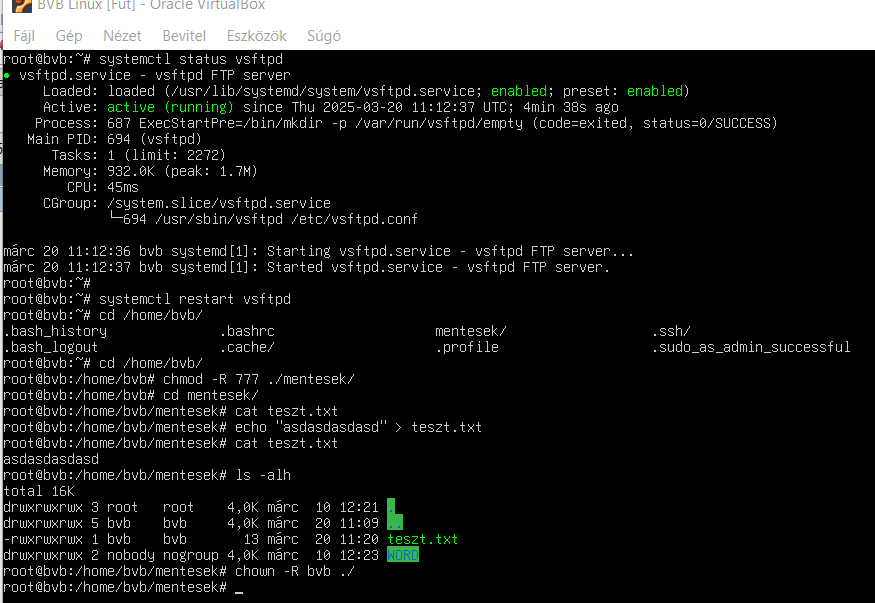
A Samba szerver a hálózaton fájlmegosztást és nyomtatómegosztást biztosít. Lehetővé teszi a fájlok elérését és kezelését különböző operációs rendszerek között, például Windows és Linux között. A Samba protokoll biztosítja a hálózaton belüli adatcsere egyszerűsítését és kompatibilitását.

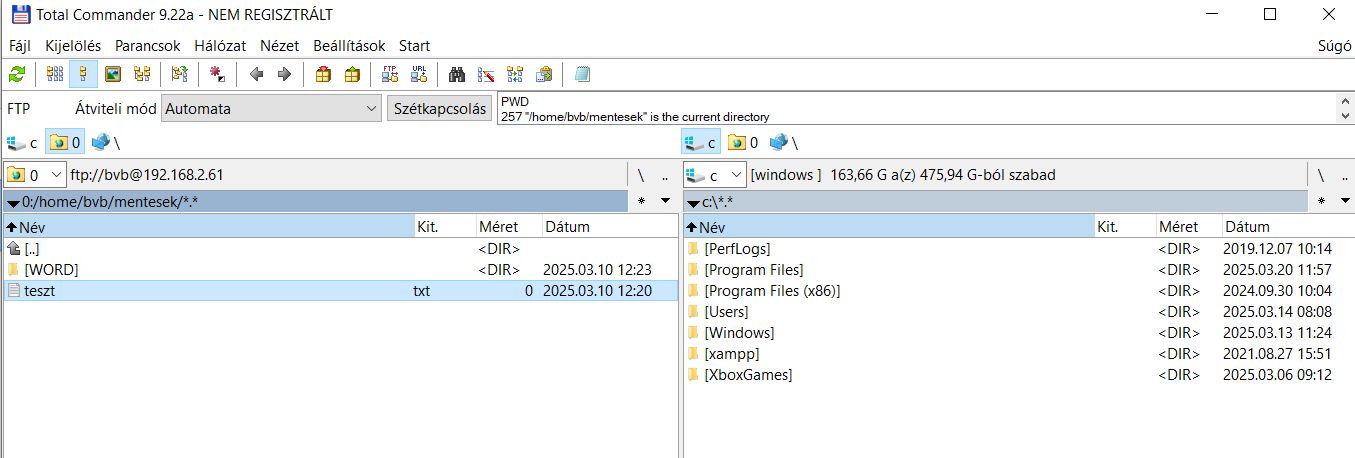




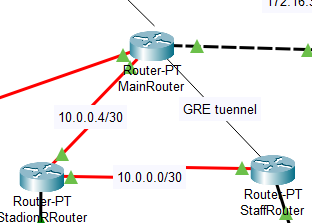
### 25. FTP Szerver

Az FTP szerver a hálózaton fájlok átvitelére szolgáló szolgáltatást biztosít. Lehetővé teszi a fájlok feltöltését, letöltését és kezelését más rendszerek között. Biztonságos és hatékony adatcsere megoldást kínál, különösen nagyobb fájlok esetén.





# Forgalom Irányítás



A forgalom irányítást az OSPF irányító protokollal oldottuk meg . A beállításait a következő oldalban szemléltetjük.

## 26. OSPF

Az **ospf** egy dinamikus routing protokoll, amelyet az IP-alapú hálózatokban használnak. Az OSPF célja, hogy hatékonyan és gyorsan meghatározza az optimális útvonalakat egy hálózaton belül, figyelembe véve a routerek közötti kapcsolatokat és a linkek költségét.

MainRouter

A képen szöveg, Betűtípus, képernyőkép, fehér látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

StadionRRouter

A képen szöveg, Betűtípus, képernyőkép, fehér látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

StadionLRouter

A képen szöveg, Betűtípus, képernyőkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

StaffRouter

A képen szöveg, Betűtípus, fehér, tipográfia látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A projektünkben a router ospf parancs után minden eszközön az 1-es folyamat azonosítót használtuk. A networkok úgy kerültek bállításra hogy minden eszköz a saját illetve a szomszédos hálózat hálózatcímét hírdeti. Az area 0-a parancs segít minimalizálni az útvonalfrissítések számát és gyorsítja a hálózati stabilitást. 

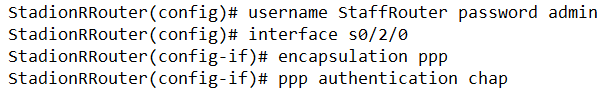
## 27. Statikus Forgalom



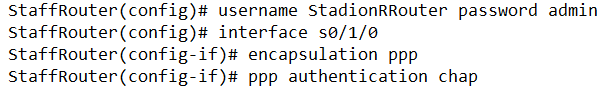
## 27. WAN (PPP)

A PPP egy adatkapcsolati protokoll amelyet a WAN-on belüli pont-pont alapú kapcsolatokhoz használnak. Biztosítja az adatátvitelt két pont között a WAN-on belül, és kezeli a hibajavítást, az autentikációt, valamint a tömörítést.

StadionRRouter



StaffRouter



A hálózatban a PPP kapcsolat a két forgalomirányító routeren működik .

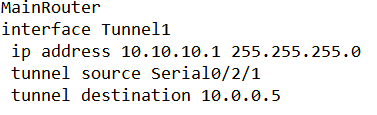
Mind a két routeren a username a szomszédos router hostname-e lett. Ez alapján ismerik fel egymást a routerek . Passwordjuk is azonos admin lett. A szomszéd fele menő portra rálépek majd a encapsulation ppp

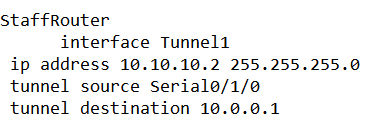
ppp authentication chap parancsal letrehoztuk a pont-pont összeköttetést



## 28. GRE-tunnel

A GRE-tunnel lehetőve teszi adatcsomagok átvitelt olyan hálózati eszközök között, amelyek fizikailag nincsenek közvetlenül összekapcsolva, és lehetőséget ad arra, hogy különböző típusú adatforgalmat egy virtuális csatornában továbbítsunk.





A hálózatunkban a tunnel1 – es csatornát hoztuk létre. Egy 10.10.10.0-ás hálózatot allítottunk be a tunnelnek 255.255.255.0 –ás maszkkal. A tunnel source a két routert összekötő router interfésze a tunnel destination pedig az interfészek ip címjei.



GRE tunnel a MainRouter és a StaffRouter között működik.



# Mellékletek

# Index.js:

const http = require('http');

const fs = require('fs');

const server = http.createServer(function (req, res) {

  switch(true) {

    case req.url === '/' && req.method === 'GET':

      fs.readFile('./index.html', (err, file) => {

        res.setHeader('content-type', 'text/html');

        res.end(file);

      });

      break;

    case req.url === '/script.js' && req.method === 'GET':

      fs.readFile('./public/script.js', (err, file) => {

        res.setHeader('content-type', 'application/javascript');

        res.end(file);

      });

      break;

    case req.url === '/phones' && req.method === 'GET':

      fs.readFile('./phones.json', (err, file) => {

        res.setHeader('content-type', 'application/json');

        res.end(file);

      });

      break;

    case req.url === '/phones' && req.method === 'POST':

      let body = '';

      req.on('data', function (chunk) {

         body += chunk.toString();

      });

      req.on('end', function () {

        const newPhone = JSON.parse(body);

        fs.readFile('./phones.json', (err, data) => {

            const phones = JSON.parse(data);

            phones.push(newPhone);

            fs.writeFile('./phones.json', JSON.stringify(phones), () => {

              res.end(JSON.stringify(newPhone));

            })

        })

      });

      break;

    default:

      res.end('404');

  }

});

server.listen(8080);

# index.html:

<!DOCTYPE html>

<html lang="en">

  <head>

    <meta charset="UTF-8" />

    <meta name="viewport" content="width=, initial-scale=1.0" />

    <title>Document</title>

    <link

      href="https://stackpath.bootstrapcdn.com/bootstrap/4.4.1/css/bootstrap.min.css"

      rel="stylesheet"

      integrity="sha384-Vkoo8x4CGsO3+Hhxv8T/Q5PaXtkKtu6ug5TOeNV6gBiFeWPGFN9MuhOf23Q9Ifjh"

      crossorigin="anonymous"

    />

  </head>

  <body>

    <div class="container">

      <div class="mb-2"></div>

      <button id="fetch-phones" class="btn btn-primary">

        Telefonok lekérdezése

      </button>

      <div id="phone-list-component"></div>

      <form id="create-phone">

        <label>

          Név:

          <input type="text" name="name" class="form-control" />

        </label>

        <label>

          Márka:

          <input type="text" name="brand" class="form-control" />

        </label>

        <button type="submit" class="btn btn-primary btn-sm">

          +

        </button>

      </form>

    </div>

    <script src="script.js"></script>

  </body>

</html>