|  |
| --- |
|  |

|  |
| --- |
| Projektfeladat |
| ByteBrigade szoftverfejlesztő cég |

****

**Projekt**

A ByteBrigade egy olyan vállalat, ami szoftverfejlesztéssel foglalkozik Magyarországon. A cég dolgozói folyamatosan képzik magukat, hogy a lehető legjobb tudásukkal dolgozzanak. A fejlesztői és biztonság téren folyamatosan a lehető legújabb és legmodernebb eszközöket és programokat alkalmazzák. A cég 3 különböző telephelyen működik Budapesten és Szombathelyen egyaránt.

Budapesten VI. kerületében található a ByteBrigade fejlesztői irodája és igazgatósága, ahol a dolgozók szoftverek fejlesztésével, dizájnolásával és tesztelésével foglalkoznak.

Budapest III. kerületében helyezkedik el az ügyfélszolgálat és technikai támogatási telephely, ahol a szerverek üzemeltetése és karbantartása folyik, továbbá technikai és szakmai segítés és támogatás az ügyfelek számára.

A ByteBrigade távmunkás irodája Szombathelyen helyezkedik el. A szombathelyi irodában van a legtöbb papírmunka. A fejlesztők itt dolgoznak új funkciók tesztelésén és optimalizálásán. A cég és partnerei között megállapodásokat hoznak létre. Az iroda magas sebességű internetkapcsolattal és biztonságos hálózattal rendelkezik. IPv6 címzés található az irodában.

# A hálózat topológiája

A képen diagram, sor, térkép, szöveg látható

Automatikusan generált leírás

# **A képen térkép, diagram, sor, Tervrajz látható Automatikusan generált leírásÜgyfélszolgálat és rendszerfelügyeleti telephely**

1. ábra: Az ügyfélszolgálati és rendszerfelügyeleti telephely topológiája

Ezen a telephelyen a cég ügyfeleinek nyújtanak ügyfélszolgálatot, illetve technikai támogatást, illetve itt található a távmunkás dolgozóknak VPN átjáró is, valamint a itt található a cég belső LAN és külső szervere is. A cég fejlesztői telephelye ezen a telephelyen keresztül csatlakozik az internethez.

## Eszközválasztás

|  |  |
| --- | --- |
| A képen elektronika, Elektrontechnika, gép, Számítógép-alkatrész látható  Automatikusan generált leírás  2. ábra Cisco ISR 4221 forgalomirányító | * Ezen a telephelyen 4 forgalomirányító található, az egyik az átjáró, ami az internettel és a távmunkás irodával (VPN-en keresztül) kapcsolja össze a telephelyet. * A forgalomirányítók a Packet Tracerben 2911-es típusúak, viszont a valós hálózatban mi **4221 ISR** forgalomirányítót választanánk. * Azért ezt a forgalomirányító típust választottuk, mert ez a forgalomirányító jelenleg is támogatott a Cisco által és megkapja a legújabb biztonsági frissítéseket, és a legújabb iOS verzióval rendelkezik. |
| A képen elektronika, villamosenergia-ellátás látható  Automatikusan generált leírás  3. ábra Cisco CBS530 kapcsoló | * A telephelyen található 4 db **Cisco CBS530** kapcsoló is. Ezt a kapcsolótípust azért választottuk, mert költséghatékony, olcsó, stackelhető, moduláris, ezáltal bővíthető és a Cisco legújabb iOS verzióját használja. |

## IP címzés

### Hálózati eszközök

|  |  |  |
| --- | --- | --- |
| **Eszköz** | **Interface** | **IP-cím** |
| **Átjáró forgalomirányító (*GatewayRTR*)** | GigabitEthernet0/0 (*külső*) | 20.120.30.2 /30 |
| GigabitEthernet0/1 (*belső*) | 192.168.1.1 /30 |
| Tunnel0 (*VPN*) | 1.1.1.2 /30 |
| **Hardveres tűzfaleszköz (*GatewayASA*)** | GigabitEthernet1/1 (*outside*) | 192.168.1.2 /30 |
| GigabitEthernet1/2 (*DMZ*) | 192.168.1.21 /30 |
| GigabitEthernet1/3 (*inside*) | 192.168.1.5 /30 |
| Management 1/1 (*mgmt*) | 192.168.1.25 /30 |
| **Központi forgalomirányító (*MainRTR*)** | FastEthernet0/1 (Gateway*ASA felé*) | 192.168.1.6 /30 |
| GigabitEthernet0/2/0 (*UgyfelRTR-backup felé*) | 192.168.1.13 /30 |
| FastEthernet0/0 (*UgyfelRTR felé*) | 192.168.1.9 /30 |
| Serial0/3/0 (*Fejlesztői telephely felé*) | 10.0.0.1 /30 |

|  |  |  |
| --- | --- | --- |
| **Ügyfélszolgálati forgalomirányító (*UgyfelRTR*)** | FastEthernet0/0 (*MainRTR felé*) | 192.168.1.10 /30 |
| GigabitEthernet0/1/0 (*UgyfelRTR-backup felé*) | 192.168.1.17 /30 |
| FastEthernet0/1.1 (*Ügyfélszolgálati LAN felé*) | 192.168.1.129 /25 *HSRP 0 virtuális IP cím:  192.168.1.254* |
| FastEthernet0/1.2  (*VoIP VLAN*) | 192.168.2.1 /24  *HSRP 1 virtuális IP cím:*  *192.168.2.254* |
| Serial1/1/0 (*Fejlesztői telephely felé*) | 20.0.0.1 /30 |
| **HSRP készenléti ügyfélszolgálati forgalomirányító (*UgyfelRTR-backup*)** | GigabitEthernet0/3/0 (*MainRTR felé*) | 192.168.1.14 /30 |
| GigabitEthernet0/1/0 (*UgyfelRTR felé*) | 192.168.1.18 /30 |
| FastEthernet0/0.1 (*Ügyfélszolgálati LAN felé*) | 192.168.1.130 /30 *HSRP virtuális IP cím: 192.168.1.254* |
|  | FastEthernet0/0.2 (*VoIP VLAN*) | 192.168.2.2 /24  *HSRP 1 virtuális IP cím:*  *192.168.2.254* |

### Végberendezések

|  |  |  |
| --- | --- | --- |
| **Eszköz** | **IP-cím** | **Átjáró** |
| **Külső szerver (*DMZ*)** | 192.168.1.22 /30 | 192.168.1.21 |
| **Belső szerver** | 192.168.1.200 /25 | 192.168.1.254 (HSRP 0) |
| **Ügyfélszolgálat munkaállomások** | *DHCP:* 192.168.1.128 /25 | 192.168.1.254 (HSRP 0) |
| **Ügyfélszolgálat VoIP** | *DHCP: 192.168.2.0 /24* | 192.168.2.254 (HSRP 1) |
| **Management laptop** | 192.168.1.26 /30 | 192.168.1.25 |

A telephely IP címzését VLSM (Variable Length Subnet Mask) segítségével alakítottam ki, a 192.168.1.0/24-es hálózatot osztottam fel kisebb részekre.

Biztonsági okokból a pont-pont összeköttetések (pl. forgalomirányító - forgalomirányító) vagy olyan végponti interfészek esetén, ahova csak 1 eszköz csatlakozik, /30-as alhálózati maszkot konfiguráltam, az ügyfélszolgálati irodai LAN-on 192.168.1.128/25-ös hálózatot alakítottam ki, valamint ugyanezen a LAN-on a VoIP telefonoknak külön VLAN-t készítettem, ami a 192.168.2.0/24-es hálózatot kapta, mert a VoIP forgalomnak a kettes VLAN-t választottam. A két VLAN-t alinterfészekkel hoztam létre.

Az IP címek a hálózati eszközöknél és szervereknél statikusan, a végponti eszközöknél dinamikusan DHCP segítségével vannak kiosztva.

## Kábelezés

A hálózatnál mindegy, hogy egyenes vagy keresztkötésű rézkábelt használunk az összeköttetéshez, ugyanis minden eszköz támogatja az AUTO-MDIX funkciót. Az AUTO-MDIX felismeri, hogy milyen kábelt csatlakoztattunk az adott hálózati eszközhöz, és ha szükséges, a kábel ereit keresztezi, így a különböző eszközök között mindig a helyes kábel típust használja, mindegy, hogy milyen típusú kábelt csatlakoztattunk.

Az AUTO-MDIX-et a mdix auto paranccsal lehet aktiválni interfész konfigurációs módban, ha ez alapból nem lenne bekapcsolva az adott hálózati eszközön.

Ezen kívül használtam optikai kábelt is *MainRTR* és *UgyfelRTR-backup* között, valamint *UgyfelRTR* és *UgyfelRTR-backup* közt, ugyanis a Packet Tracerben nem volt a 2811 IOS15 forgalomirányítóhoz megfelelő rézkábeles bővítőmodul, csak így tudtam ezt megoldani.

Emellett a két épület (az Ügyfélszolgálati telephely és a Fejlesztői telephely) között soros kábellel vannak összekötve a forgalomirányítók a nagyobb távolság miatt.

## DHCP

A DHCP protokollal megoldható, hogy a kliens gépek automatikusan kapják az IP címüket, átjárót, DNS-t, stb, ezáltal nem kell ezeket manuálisan beállítani. A telephelyen DHCP szolgáltatást futtató kiszolgáló a topológiában az „*UgyfelRTR*” nevű forgalomirányító (**192.168.1.129, 192.168.2.1**). Az ügyfélszolgálati telephely munkaállomásai erről a kiszolgálóról DHCP-vel kapják az IP címüket a 192.168.1.128/25-ös hálózatból, valamint az IP telefonok is innen kapják IP címüket a 192.168.2.0/24-es hálózatból.

DHCP-ből kizárással megoldottam, hogy a forgalomirányítók (.129, .130), a HSRP virtuális forgalomirányító (.254) és a belső szerver (.200) címét a DHCP kiszolgáló ne ossza ki, valamint az IP telefonok DHCP hatóköre se ossza ki a forgalomirányítók (.1, .2), a HSRP virtuális forgalomirányító (.254) címét, különben DHCP address conflict lenne.

Emellett még a *BelsoSzerver* (192.168.1.200)-n is konfiguráltam DHCP szervert tartalékként az ügyfélszolgálati LANban.

Az alább látható parancsokkal konfiguráltam a kizárásokat (excluded-address), illetve a DHCP hatóköröket (pool) az *UgyfelRTR*-en és az *UgyfelRTR-backup*-on.

IP címkizárások

Ügyfélszolgálati LAN hatókörbeállításai

VoIP VLAN  
hatókörbeállításai

A VoIP eszközök számára a hatókör beállításánál fontos volt beállítani a 150-es DHCP opciót is, amellyel megadjuk, hogy megyik TFTP szerverről érhetik el a konfigurációjukat az IP telefonok, ez a jelen esetben az *UgyfelRTR* és az *UgyfelRTR-backup* HSRP virtuális IP címe.

ip dhcp excluded-address 192.168.1.129

ip dhcp excluded-address 192.168.1.130

ip dhcp excluded-address 192.168.1.200

ip dhcp excluded-address 192.168.1.254

ip dhcp excluded-address 192.168.2.1

ip dhcp excluded-address 192.168.2.2

ip dhcp excluded-address 192.168.2.254

ip dhcp pool UGYFEL

network 192.168.1.128 255.255.255.128

default-router 192.168.1.254

dns-server 192.168.1.200

domain-name bytebrigade.hu

ip dhcp pool VOICE

network 192.168.2.0 255.255.255.0

default-router 192.168.2.254

dns-server 192.168.1.200

domain-name bytebrigade.hu

option 150 ip 192.168.2.254

*DHCP szerver beállítása*

*Egy ügyfélszolgálati kliens IP konfigurációja*

Mivel mindkettő forgalomirányítón a HSRP miatt létrehoztam a hatóköröket, viszont bezavarnának egymásnak ha mindkettőn egyszerre futna a DHCP szolgáltatás, az *UgyfelRTR-backup*-on leállítottam azt a no service dhcp paranccsal. Ha esetleg az *UgyfelRTR* forgalomirányító meghibásodna, ezt engedélyezni kell ideiglenesen a service dhcp paranccsal.

### DHCP snooping

DHCP snooping segítségével javítani tudjuk a DHCP infrastruktúra biztonságát és megakadályozni egy kalóz DHCP szerver létrejöttét.

Annak érdekében, hogy semmilyen illetéktelen személy ne tudja magát kiadni DHCP kiszolgálónak, DHCP snooping-ot akalmaztam az *kapcsolókon*, hogy az egyetlen DHCP-vel megbízott port a **forgalomirányítól felüli** legyen, amin a cég saját DHCP kiszolgálója van. Ezáltal az egyetlen egy DHCP kiszolgáló, ami küldhet *DHCPOFFER* üzeneteket.

ip dhcp snooping

ip dhcp snooping vlan 1,2

interface FastEthernet0/2

ip dhcp snooping limit 1

ip dhcp snooping trust

Ezen kívül azt is beállítottam, hogy a *DHCPOFFER* üzenet 1 másodpercen belüli maximális száma 1 lehet, ezáltal nem lehet leterhelni a hálózatot egy rogue kliensnek ahol folyton DHCP-vel kérnek címeket.

*DHCP Snooping konfiguráció*

### MAC-cím szűrés, Portfast

interface range f0/1-6

switchport mode access

switchport voice vlan 2

switchport port-security maximum 1

switchport mac-address sticky

switchport mode restrict

spanning-tree portfast

A hálózatban MAC-cím szűrést alkalmaztam, hogy egy illetéktelen személy ne tudja bevinni a saját eszközét és azt rácsatlakoztatni a céges hálózatra. A fent látható konfiguráción (UgyfelSW4) beállítottam, hogy ne tudjon a porton lévő kliens trunk kapcsolatot egyeztetni a kapcsolóval (**switchport mode access**), a maximum engedélyezett MAC-címek száma az interfészen 1, a kapcsoló dinamikusan jegyzi meg őket és a restrict portbiztonsági módszer miatt leállás helyett jelez, ha nem egy már alapból megjegyzett MAC-címről érkezne forgalom, majd azokat a csomagokat pedig eldobja.

Emelett be van állítva portfast STP mód is, ugyanis a végponti interfészeken nincs szükség STP-re, így azonnal létrehozzák a kapcsolatot, átugorva az STP tanulási és várakozási időszakait.

## A képen szöveg, képernyőkép, Betűtípus, szám látható Automatikusan generált leírásIP telefónia

A hálózatban konfiguráltam IP telefóniát is, az ügyfélszolgálati irodában.

Az IP telefónia segítségével kiépítettem egy konvergált hálózatot, amely segítségével egy adatkábelen több szolgáltatás is képes áthaladni. Ezen kívül a CME forgalomirányító (*Communications Manager Express*) segítségével kiépítettem egy virtuális telefonközpontot, amely segítségével a cég különböző telephelyeiről elérhetik egymást a dolgozók.

A hálózatban maximum 5 IP telefon lehet, és mindegyik a DHCP-szervertől (*UgyfelRTR*) kapja az IP-címét TFTP-n keresztül. A hálózatban található 1 **ATA** típusú telefon, illetve 4 **Cisco 7960 IP Phone** is.

A VoIP forgalom a 2-es VLAN-on halad az ügyfélszolgálati LAN-on belül, míg a munkaállomásokról származó csomagok az 1-es VLAN-on. Ezáltal a VoIP csomagok gyorsabb prioritást kapnak a másikakkal szemben, ami nélkülözhetetlen a telefonos forgalomak számára.

A telephelyek közti telefonálást **dial-peer** segítségével oldottam meg, az egyik telephelyen a telefonszámok **555**-ös számjegyekkel kezdődnek, a másikon pedig **556**-tal.

dial-peer voice 1 voip

destination pattern 556…

session target ipv4:172.12.1.1

## Forgalomirányítás

### OSPF

A telephelyen forgalomirányításhoz OSPF-et használunk belső hálózaton. Mivel a telephely összes forgalomirányítója a gerinchálózaton helyezkedik el, ezáltal minden egyes forgalomirányító a 0-s területben van a telephelyen. A 0-s területen message-digest hitelesítést használunk annak érdekében, hogy a cég jelszavak és adatok titkosítva legyenek a szállítás közben, ezt interfész konfigurációs módban kell megadni, a ip ospf authentication message-digest és az ip ospf message-digest-key parancsokat használtam. A végponti eszközök felé menő interfészek minden eszközön passzívra vannak állítva a passive-interface OSPF routing konfigurációs parancs segítségével, ezáltal oda nem küldenek ki a forgalomirányítók routing információkat, így csökkentve a hálózat terhelését. Az alább látható példaként az *UgyfelRTR* OSPF konfigurációja:

router ospf 1  
 log-adjacency-changes  
 area 0 authentication message-digest  
 passive-interface FastEthernet0/1  
 network 20.0.0.0 0.0.0.3 area 0  
 network 192.168.1.8 0.0.0.3 area 0  
 network 192.168.1.16 0.0.0.3 area 0  
 network 192.168.1.128 0.0.0.3 area 0  
 network 192.168.2.0 0.0.0.255 area 0

## VPN

A telephelyen egy VPN gateway is található, amely biztosítja a belső hálózat biztonságos és titkosított távoli elérését a távmunkás irodában (*Branch*) lévő dolgozóknak.

A VPN-t GRE over IPSec módszerrel oldottuk meg, mert ezt könnyű konfigurálni és a mi hálózatunkba ennél nagyobb VPN megoldások nem szükségesek.

A GRE (Generic Routing Encapsulation) egy telephelyek közti alagútkezelési protokoll, amely különböző rétegbeli protokollokat, multicast és broadcast forgalmat is képes átvinni az alagúton. De a GRE alapértelmezés szerint nem támogat titkosítást, ezért nem biztonságos, ezért kellett IPSec csomagba foglalni.

A GatewayRTR VPN konfigurációja fentebb látható. Emellett még egy Tunnel 0 interfészt is létre kellett hozni a következőféleképpen:

int tunnel 0

ip add 1.1.1.2 255.255.255.252

tunnel source s0/0/0

tunnel destination 20.110.30.2

tunnel mode gre ip

crypto isakmp policy 101

encr aes

authentication pre-share

group 5

crypto isakmp key cisco address 20.110.30.2

crypto isakmp key cisco address 20.120.30.1

crypto ipsec transform-set R3\_Set esp-aes esp-sha-hmac

crypto map R3\_Map 101 ipsec-isakmp

set peer 20.110.30.2

set peer 20.120.30.1

set transform-set R3\_Set

match address 101

exit

int s0/0/0

crypto map R3\_Map

do wr

## ASA

A cég ügyfélszolgálati telephelyén ASA (hardveres tűzfaleszköz) biztosítja a hálózat védelmét a külső fenyegetésekkel szemben és elkülöníti a külső és belső hálózatot, illetve biztosít egy ún. DMZ szervert. A DMZ szerveren futnak a cég által nyújtott szolgáltatások, amelyekhez az ügyfelek férhetnek hozzá. A cég ügyfélszolgálati telephelye így egy biztonságos és hatékony hálózati infrastruktúrával rendelkezik, amely megfelel az ügyfelek igényeinek és elvárásainak.

A képen szöveg, képernyőkép, diagram, embléma látható

Automatikusan generált leírás

4. ábra: Az ASA interfészei

*ASA interfészei*

|  |  |
| --- | --- |
| A képen szöveg, Betűtípus, képernyőkép, sor látható  Automatikusan generált leírás | Az ASA külső hálózat felé vezető interfésze az ún. **’outside’** interfész. Ennek az interfésznek a biztonsági szintje 0, csak a DMZ szervert érhetik el innen, a belső hálózatot nem. |

|  |  |  |
| --- | --- | --- |
| A képen szöveg, Betűtípus, képernyőkép, sor látható  Automatikusan generált leírás | | Az ASA belső hálózat felé vezető interfésze pedig az **’inside’** interfész. Mivel ez az interfész a belső hálózathoz csatlakozik, ezért megbízhatónak tekintjük és így a biztonsági szintje a lehető legmagasabb, 100. Innen elérhető a DMZ szerver, a távoli iroda és az internet is. |
| A képen szöveg, Betűtípus, képernyőkép, sor látható  Automatikusan generált leírás | Az ASA **’dmz’** interfészén van a cég külső, ügyfelek számára is elérhető DMZ szervere. Ezen a szerveren fut a cég weboldala. Mivel ez az interfész nem annyira megbízható, a biztonsági szintje csak 50  *ASA inside interfész konfigurációja* |

|  |  |
| --- | --- |
| A képen szöveg, Betűtípus, képernyőkép, sor látható  Automatikusan generált leírás | Ezen felül az ASA-hoz csatlakozik még egy kezelési interfész is a Management1/1. Ezen keresztül történik az ASA SSH-s konfigurálása. Az interfész neve **’mgmt’**, biztonsági szintje 100, hiszen ezt az interfészt csak rendszergazdák használják |

## Hozzáférési lista

Alapból a DMZ szerver nem volt elérhető a külső hálózatok számára, illetve nem tudott válaszolni a belső hálózati eszközök kéréseire, mivel a Cisco ASA eszköze alapból nem enged át forgalmat kisebb biztonsági szintű interfészekről nagyobb biztonságú szintű interfészekre. Ennek megoldására hozzáférési listát alkalmaztam.

Ez a hozzáférési lista azt engedi meg, hogy a külső hálózatokból is elérhető legyen a cég webszervere (**192.168.1.22**) ICMP-el, HTTPS-el, és FTP-vel ami a topológiában az ASA DMZ interfészén található. Ezen kívül azt is engedélyezi ez a hozzáférési lista, hogy a DMZ szerver tudjon vissza válaszolni a belső hálózaton lévő ICMP és HTTPS kérésekre, viszont a DMZ szerver ne tudjon kezdeményezni bármilyen forgalmat, csak válaszolni tudjon.

access-list DMZ extended permit tcp any host 192.168.1.22 eq 443

access-list DMZ extended permit tcp any host 192.168.1.22 eq ftp

access-list DMZ extended permit icmp any host 192.168.1.22 echo

access-list DMZ-REPLY extended permit icmp host 192.168.1.22 any echo-reply  
access-list DMZ-REPLY extended permit tcp host 192.168.1.22 any

access-group DMZ in interface outside

access-group DMZ-REPLY in interface dmz

## Hálózati címfordítás

A *GatewayRTR* forgalomirányító GigabitEthernet0/0 és GigabitEthernet0/1 interfészein PAT-ot konfiguráltam. A PAT átfordítja a belső hálózati IP-címeket a forgalomirányító ip nat outside interfészének IP címére, ezáltal el lehet érni az internetet a belső hálózatról is. A PAT egy hozzáférési listában megadott IP-címeket fordítja le, ami a mi hálózatunkban mivel sok fajta alhálózat van, bármilyen címet lefordít. A külső hálózatokban a forgalomirányítók ezt úgy látják, mintha csak a forgalomirányító külső IP-címéről jönnének forgalmak. A PAT a belső hálózatban IP címmel és portszámokkal dolgozik, ezáltal nem fogy ki a NAT address pool soha, mint a dinamikus/statikus NAT esetében.

interface GigabitEthernet0/0

ip nat outside

interface GigabitEthernet0/1

ip nat inside

access-list 1 permit ip any any

ip nat inside source list 1 interface GigabitEthernet0/1 overload

## Rendszerfelügyeleti beállítások

### DNS

A DNS-szerver a hálózatunkban a belső 192.168.1.200-as IP-címmel rendelkező szerver. A DNS-szerverrel megkönnyítjük a tesztelést, a különböző eszközök elérését, hiszen nem kell emlékeznünk az IP-címükre pl. SSH-csatlakozás esetén, illetve elérhetünk vele különböző lokális weboldalakat. A DNS-t hálózati eszközökön az ip name-server 192.168.1.200 parancssal konfiguráltam, a végponti eszközök pedig a szervereknél manuálisan, a PC-k pedig DHCP-vel kapják meg a DNS-szerver címét.

*DNS beállítások a belső szerveren*

*DNS-szerver router konfiguráció és tesztelés*

### SSH

A hálózati eszközök távoli eléréséhez kizárólag SSH-t használunk, mert sokkal megbízhatóbban és biztonságosabban viszi át az adatokat, mint a telnet, ugyanis a telnet nem titkosítja az adatokat, hanem plaintext – egyszerű szöveg formájában továbbítja őket, ezáltal hackerek könnyen el tudják lopni a jelszavakat, illetve a különböző adatokat.

A transport input ssh vonali konfigurációs paranccsal kizárólag SSH-t engedélyeztem a hálózati eszközökön, illetve mindenhol 1024 bit-es RSA kulcsot generáltattam. Az alább látható az SSH konfiguráció az *UgyfelRTR*-en:

hostname UgyfelRTR  
username admin privilege 15 password admin  
enable secret cisco  
ip domain-name bytebrigade.hu  
crypto key generate rsa  
1024  
ip ssh version 2  
line vty 0 15  
login authentication default  
transport input ssh

*UgyfelRTR SSH konfiguráció*

Emellett az ASA-n is konfiguráltam SSH-t, ott viszont konfiguráláskor azt is meg kell adni, hogy melyik interfészről szeretnénk elérni azt és milyen hálózatról. Itt értelemszerűen a *mgmt* interfészt adtam meg, mert azt használjuk az ASA konfigurálására.

ssh 192.168.1.24 255.255.255.252 mgmt

aaa authentication ssh console LOCAL

### SYSLOG

A hálózati eszközök felügyeletére naplózzuk a naplóüzeneteket a belső szerverre, ezáltal ha például valamilyen probléma adódna (pl. egy interfész leáll), a rendszergazda azonnal kap értesítést róla és neki tud állni egyszerre megjavítani a problémát.

A syslog konfigurálásához a következő parancsokat használtam:

logging userinfo  
logging host 192.168.1.200  
logging trap debugging  
logging buffered 8192  
service timestamps log datetime msec

*SYSLOG konfigurációja a routeren*

A fent látható konfigurációval a szerverre (192.168.1.200) naplózzák a hálózati eszközök a felhasználói bejelentkezéseket, mindenféle hibaüzenetet/figyelmeztetést, méghozzá milliszekundum pontossággal, az NTP és a timestamps szolgáltatás segítségével. Ezen kívül még, hogyha elérhetetlen lenne a szerver, az eszközök a saját pufferjükbe is naplóznak, 8192 bájtnyi a pufferméretük. A naplópuffert a show logging paranccsal lehet megtekinteni.

### RADIUS

A hálózati eszközökre történő bejelentkezéseket RADIUS szerver hitelesíti, ezáltal könnyebb átlátni a jogosult felhasználókat, illetve könnyebb helyreállítani a jelszavukat. Egy esetleges RADIUS szerver leállás esetén a hálózati eszközök helyileg hitelesítik a felhasználókat, ha nem tudnak kapcsolatot létesíteni a RADIUS szerverrel.

*RADIUS szerver konfigurációja*

A radius hitelesítést a következőképpen konfiguráltam:

*RADIUS szerver beállítása forgalomirányítón*

aaa new-model

aaa authentication login default group radius local

aaa authorization exec default group radius local if-authenticated

radius server 192.168.1.200

address ipv4 192.168.1.200 auth-port 1645

key cisco

A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, sor, Betűtípus látható

Automatikusan generált leírás

5. ábra: A RADIUS szerver beállításai

6. ábra: A RADIUS szerveren beállított felhasználók és jelszavak

### NTP

Az NTP lényege, hogy a hálózati eszközökön mindig pontos és egymással szinkronizált idő legyen. Rosszul beállított /eltérő idő miatt akár nem is működhetnek bizonyos funkciók, vagy akár nem tudhatjuk, hogy egy adott hiba mikor történt, mert a naplók rossz időpontot írnának ki, ezért érdemes volt az NTP-t beállítani.

A mi hálózatunkban az NTP szerver a 192.168.1.200-as szerver.

Az NTP beálításához az alábbi parancsokat használtam:

ntp authenticate  
ntp authentication-key 1 md5 Cisco  
ntp trusted-key 1  
ntp server 192.168.1.200  
ntp update-calendar

### FTP és TFTP

Az FTP és a TFTP (Trivial File Transfer Protocol) protokollokat fájlok átvitelére használjuk. Ez a mi hálózatunkban azért hasznos, hogy a forgalomirányítók konfigurációját biztonsági mentésként lementsük a szerverre. Az FTP-t és a TFTP-t futtató szerver a 192.168.1.200-as szerver.

A TFTP beállításához nem kellett semmit sem konfigurálni a forgalomirányítókon, csupán a szerveren kellett bekapcsolni a TFTP szolgáltatást. Ellenben az FTP beállításához be kellett állítani egy FTP felhasználónevet és egy jelszót az ip ftp username és az ip ftp password paranccsal, amelyek szintén a szerveren FTP szolgáltatásfülénél is fel kellett venni.

### SNMP

*NTP beállítása*

Az SNMP (Simple Network Management Protocol) egy olyan alkalmazás rétegbeli protokoll, amelyet hálózatmenedzselésre fejlesztettek ki. Az SNMP-t futtató hálózati eszközökkel SNMP PDU-kkal komunikál. 5 fajta üzenettípust tud elküldeni a SNMP az eszközöknek, ezek a

* **SNMPTRAP**: aszinkron üzenet amiben a Manager az ügyféltől valamilyen jelentést kér
* **SNMPGET**: egy vagy több értéket elkér a Mib adatbázisból (management information base)
* **SNMPGETNEXT**: a következő OID-val (object ID) rendelkező értéket elkéri a Mib adatbázisból
* **SNMPGETRESPONSE**: a mendszelt eszköz küldi válaszképp egy SNMPGET vagy SNMPGETNEXT kérésre.
* **SNMPSET**: az SNMP manager elküldi a menedzselt eszköznek, hogy milyen értéket állítson át és mire .

SNMP-t azért konfiguráltam, hogy távolról és könnyedén el lehessen érni a hálózati eszközeinket, és egy grafikus MibBrowser felületen keresztül konfigurálni/felügyelni azokat. Beállításához csupán egy community string kell.

snmp-server community public RO  
snmp-server community private RW

*SNMP szerver konfigurálása Cisco eszközön*

*Router hostname lekérdezése Mib Browserrel*

A ’public’ community string kizárólag olvasásra használható, míg a ’private’ sztring írásra is.

### NetFlow

A NetFlow segítségével tudjuk analizálni az IP hálózati forgalmat amikor ki, vagy éppen be érkezik egy interfészre. A NetFlow használatával egy hálózati rendszergazda olyan adatokat tudhat meg egy adott forgalomról, mint például: forrás vagy cél IP cím, a forgalom típusa, protokoll, stb.

A hálózatban azért használunk NetFlow-t, hogy átlássuk, a hálózat mely pontjain van leterhelve legjobban a hálózat. A NetFlow analizálásához még kell egy analizátor program is, amihez egy valós hálózati környezetben a *SolarWinds NetFlow Analyzer* programját használnánk, viszont a szimulációban a *Cisco Packet Tracer* saját *NetFlow Collectorát* használtuk.

A beállításához globális konfigurációs módban az alábbi parancsokat adtuk ki:

NetFlow Analyzer program port száma  
  
interfész neve, ahol gyűjteni szeretnénk az forgalom adatait

ip flow-export destination 192.168.1.200 9996

ip flow-export version 9

ip flow-export source Serial0/0/1

interface Serial0/0/1   
 ip flow egress

ip flow ingress

## Redundancia

### STP

A második rétegbeli redundanciát a telephelyen STP segítségével oldottam meg. A kapcsolókon prioritások, illetve költségek megváltoztatásával optimalizáltam a forgalmat. Ezzel csökkentettem, az interfészek számát a csomagok útvonalaiban.

Ezen kívül beállítottam az STP-t rapid-pvst módra, hogy az STP gyorsan konvergáljon, ezáltal csökkentve az esetleges kimaradás idejét (max 6 mp.) A képen sor, diagram, képernyőkép, Diagram látható

Automatikusan generált leírás

A két VLAN miatt az Ügyfélszolgálati LAN-ban mindenhol trunk kapcsolatot alakítottam ki, ezáltal csak 1 port került letiltásra az STP által.

7. ábra: Redundáns összeköttetés az Ügyfélszolgálati LAN-ban

Ezen kívül, mint ahogy azt már a MAC cím szűrésnél is említettem, a végponti összeköttetéseknél az STP portfast módra van állítva a gyors konvergálás miatt és az esetleges késleltetések kiküszöböléséért.

Az ügyfélszolgálati LAN-ban VLAN1-en az *UgyfelSW2*, VLAN2-őn az *UgyfelSW1* a gyökérponti híd, ezt a spanning-tree vlan [vlan száma] root primary paranccsal állítottam be.

### HSRP

Harmadik rétegbeli redundancia miatt **HSRP**-t (*Hot Standby Router Protocol*) alkalmaztam az ügyfélszolgálati LAN-nál, illetve a belső szervernél, hogy ha a nekik átjárónak szolgáló forgalomirányító esetlegesen meghibásodna, akkor ne álljon le számukra a belső LAN és az internet elérése. A **standby preempt** parancs segítségével biztosítottam azt, hogy mindig az eredeti forgalomirányító (*UgyfelRTR*) legyen az aktív, ha nem történt meghibásodás.

Egy valós hálózatban érdemesebb lenne GLBP-t használni (Gateway Load Balancing Protocol), ugyanis a HSRP esetében mindig csak az aktív forgalomirányító „működik”, a másik csak vár. GLBP esetében viszont mindkét forgalomirányító tud egyszerre osztozni a csomagok küldésén és elosztásán, ezért a GLBP egy sokkal hatékonyabb protokoll.

A HSRP-t az alábbi parancsok segítségével konfiguráltam a LAN felé vezető interfészen:

interface FastEthernet0/1.1  
standby 0 ip 192.168.1.254  
standby preempt  
standby priority 100  
standby track Serial1/1/0  
standby track FastEthernet0/0  
  
interface FastEthernet0/1.2  
standby 1 ip 192.168.2.254  
standby preempt  
standby priority 100  
standby track Serial1/1/0  
standby track FastEthernet0/0

A standby priority parancs segítségével állítottam be a prioritás értékét a forgalomirányítóknak, ha valamelyik trackelt interfész (Serial1/1/0, vagy FastEthernet0/0) leállna/meghibásodna, akkor ez a prioritási érték lejjebb megy 10-zel. A standby routeren (*UgyfelRTR-backup*) ezt a prioritási értéket 99-re konfiguráltam.

### Lebegő Statikus útvonalak

Ha esetleg az OSPF leállna, harmadik rétegbeli redundancia érdekében a HSRP mellett még lebegő alapértelmezett statikus útvonalakat is használunk a gerinchálózaton.

A lebegő statikus útvonalak csak akkor lesznek használatba véve a forgalomirányítók által, amikor az OSPF leáll, mert az adminisztrációs távolságukat nagyon magasra, **253** és **254**-esre állítottam.

Az alapértelmezett statikus útvonalak például az *UgyfelRTR*-en:

ip route 0.0.0.0 0.0.0.0 FastEthernet0/0 253 🡪 MainRTR felé

ip route 0.0.0.0 0.0.0.0 Serial1/1/0 254 🡪 Fejlesztői telephely felé

# Programozott hálózatkonfiguráció

Mivel az NTP kiszolgáló beállítása minden forgalomirányítón manuálisan egy nagyon monoton munka lenne egy ember számára, illetve a parancs mindenhol ugyanaz, úgy döntöttem, hogy ezt egy Python program segítségével konfigurálom. Az alább látható Python program a netmiko modul ConnectHandler függvényének segítségével rácsatlakozik a megadott eszközökre, és ha még nincs beállítva, beállítja az NTP kiszolgálót, hitelesítést, majd ha be van állítva, lekérdezi az NTP státuszát és az asszociációkat.

A képen szöveg, képernyőkép, szoftver látható

Automatikusan generált leírás

8. ábra: A hálózatkonfiguráció program kódja

# Linux szerver

A Linux szerver a projektünkben HTTP-t, HTTPS-t, DHCP-t, DNS-t, valamint SAMBA Fájlmegosztást kínál.

A Linux szerverhez Ubuntu 22.04-es operációs rendszert választottam, IP címe 192.168.1.200. A teszteléshez egy Windows 10-es klienset használtam.

A legtöbb kiszolgálómodilt **webmin**en keresztül installáltam és konfiguráltam.

## DHCP

A Linux szerver a 192.168.1.128/25-ös tartományban oszt ki címeket, a kliensek ő tőle kapják a domain-nevet, az alapértelmezett átjárót és a DNS szervert is.

A képen szöveg, képernyőkép, szám, Betűtípus látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás9. ábra: DHCP szerver alhálózat beállításai

. ábra: További DHCP beállítások

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

. ábra: Kliens ipconfig kimenete

## HTTP

A szerver HTTP kiszolgálóját Apache webszerverrel konfiguráltam, mert ez egy eléggé megbízható és stabil webkiszolgáló modul.

Konfigurálásához csupán fel kellett telepíteni a Webminből, majd a /var/www/html mappában módosítani az index.html-t.

A képen szöveg, Betűtípus, sor, szám látható

Automatikusan generált leírás

12. ábra: HTTP szerver beállításai

A képen szöveg, képernyőkép, Betűtípus, szoftver látható

Automatikusan generált leírás

. ábra: HTTP weboldal kliensről való elérése

## HTTPS

Mivel az Apache alapból csak sima HTTP szervert indít el, a HTTPS szervert külön kellett konfigurálni.

A HTTPS szerver elindításához szükség volt előszőr arra, hogy mind a 80-as, mind a 443-as portra érkező kapcsolatokat a tűzfal ne blokkolja, ezt a sudo ufw allow „Apache Full” paranccsal értem el.

Utána engedélyezni kellett az Apache számára, hogy tudja kezelni az SSL titkosításokat. Ezt a sudo 2enmod ssl paranccsal engedélyeztem. Ezután újraindítottam az Apache kiszolgálót, majd generáltam SSL certificateket az openssl paranccsal:

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/bytebrigade.key -out /etc/ssl/certs/bytebrigade.crt

14. ábra: Legenerált SSL kulcs

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, Betűtípus, szoftver látható

Automatikusan generált leírásA képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírásA SSL certificate-k legenerálása után be kellett konfigurálni a VirtualHost-ot az Apache konfigurációs fájljainál. Az /etc/apache2/sites-available/192.168.1.200.conf fájlban a VirtualHost alatt megadtam a szerver nevét, dokumentjeinek gyökerét, bekapcsoltam az SSLEngine-t, majd megadtam az SSL certificate és az SSL key helyét.

17. ábra: 0Apache HTTPS oldal VirtualHost konfigurációja

16. ábra: SSL tanúsítvány

Ezt a konfigurációt a a2ensite paranccsal tudtam érvénybe léptetni: sudo a2ensite 192.168.1.200.conf, majd egy Apache újraindítás után már működött is a HTTPS.

Amikor beírjuk a szerver címét https-el előszőr egy figyelmeztetést dob fel, ugyanis a szerver tanúsítványa saját magunk által van aláírva. Itt a tovább a weboldalra opciót kell megnyomni.

## **A képen szöveg, képernyőkép, szoftver, Weblap látható Automatikusan generált leírás**A képen szöveg, képernyőkép, Betűtípus, Márka látható Automatikusan generált leírásDNS

15. ábra: HTTPS tanústvány hiba

16. ábra: HTTPS weboldal kliensoldali tesztelése

Ez a szerver biztosítja a DNS szolgáltatást is az egész hálózatban.

**A képen szöveg, Betűtípus, sor, képernyőkép látható

Automatikusan generált leírás**A szerver DNS kiszolgálóját a BIND DNS szerverrel valósítottam meg, ezen létrehoztam 2 master zónát, egyik domain neveket fordít IP-címekre, míg a másik pedig a címeket fordítja vissza domain nevekre. Ezekben a zónákban szerepelnek a szerver egyéb szolgáltatásainak domain címei is. A DNS-szerver a bytebrigade.hu domaint használja.

17. ábra: DNS master zóna beállításai

## **A képen szöveg, képernyőkép, Betűtípus látható Automatikusan generált leírás**SAMBA Fájlmegosztás

18. ábra: nslookup parancs kimenete a kliensen

Fájlmegosztáshoz a szerveren telepítettem Samba Windows File Sharing kiszolgálómodult, amely lehetővé teszi egy adott mappa megosztását különböző klienseken.

Előszőr is felvettem egy byte-lan csoportot a sudo addgroup paranccsal, majd létrehoztam a gyökérkönyvtárban egy /megoszt mappát, aminek a chgrp paranccsal megváltoztattam a csoportját a *byte-lan*-ra.

A képen szöveg, képernyőkép, képernyő, szám látható

Automatikusan generált leírásA képen szöveg, képernyőkép, sor, Betűtípus látható

Automatikusan generált leírásEzután Webminen keresztül felvettem egy test usert, akinek a csoportját beállítottam a *byte-lan*ra, majd a Samba konfigurációs fülén létrehoztam egy új megosztást megoszt néven.

23. ábra: Felhasználók/csoportok hozzáadása a megosztáshoz

22. ábra: Megosztás beállításai

A képen szöveg, képernyőkép, szoftver, Betűtípus látható

Automatikusan generált leírásA képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírásA kliensen az új hálózati meghajtó csatlakoztatásánál megadtam a \\192.168.1.200\megoszt elérési utat, majd bejelentkeztem a test userrel. Ahhoz, hogy a bejelentkezés sikeres legyen, előszőr a **sudo smbpasswd -a** [felhasználónév] parancsot ki kellett adnom, és a test user jelszavát beállítani, ezután működött a megosztott mappa elérése.

25. ábra: A megoszt mappa tartalma a kliensen

24. ábra: A megoszt mappa tartalma a szerveren

# Tesztelés

**Távmunkás telephely CME router elérése UgyfelPC1-ről:**

**A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás**

A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás

**TFTP szerver tesztelés UgyfelRTR-ről:**

**A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás**

**FTP szerver tesztelés UgyfelRTR-ről:**

**A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás**

**DMZ webszerver elérése és DNS névfeloldás tesztelése:**

**A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás**

**SYSLOG tesztelése:**

**A képen szöveg, képernyőkép, szám, Betűtípus látható

Automatikusan generált leírás**

**NetFlow tesztelése:**

**A képen szöveg, képernyőkép, szoftver, Számítógépes ikon látható

Automatikusan generált leírás**

**SNMP tesztelése:**

**A képen szöveg, szoftver, képernyőkép, sor látható

Automatikusan generált leírás**

**SSH tesztelése UgyfelRTR-en UgyfelPC1-ről:**

**A képen szöveg, Betűtípus, képernyőkép látható

Automatikusan generált leírás**

# **Fejlesztői telephely és igazgatóság**

# Telephely célja, topológia, IP-címzés

Cégünk fő fejlesztői irodái, illetve felsővezetősége Budapesten, egy telephelyen belül található.

A képen sor, diagram, Párhuzamos, tervezés látható

Automatikusan generált leírás  
*Telephely topológiája*

|  |  |  |
| --- | --- | --- |
| **Router\_Dev10** | Serial0/0/0 | 30.30.30.0 /30 |
| Serial0/0/1 | 10.10.10.0 /30 |
| GigabitEthernet0/0.10  (HSRP Aktív interface) | 192.168.20.1 /24 |
| GigabitEthernet0/1.20  (HSRP Passzív interface) | 192.168.30.1 /24 |
| **Router\_Dev20** | Serial0/0/0 | 30.30.30.0 /30 |
| Serial0/1/0 | 20.20.20.0 /30 |
| GigabitEthernet0/0.30  (HSRP Aktív interface) | 192.168.20.128 /24 |
| GigabitEthernet0/1.40  (HSRP Passzív interface) | 192.168.30.128 /24 |
| **Belső Szerver** | FastEthernet0 | 192.168.20.254 /24 |
| **WLC** | GigabitEthernet1 | 192.168.40.1 /24 |

## Kábelezés

A telephelyen csak egyenes kábellel lettek a hálózati eszközök összekötve, mivel a mai modern eszközök támogatják az Auto MDI-X funkciót, ami automatikusan érzékeli, hogy milyen kábeltípus lett használva, és az annak optimális típust fogja alkalmazni. Ezt a konfigurációt interface módban, az ’mdix auto’ parancs megadásával tudjuk engedélyezni.

Ezen telephely és az ügyfélszolgálati telephely felé soros portokon keresztül kapcsolódik a hálózatra.

## PPP

A PPP egy adatkapcsolati rétegbeli protokoll, ami szabványos módszert biztosít többféle adatcsomag szállításához pont-pont linkeken keresztül.

Hálózatunkon a két telephelyet összekötő soros interfészeken konfigurálunk PPP CHAP hitelesítést, ezáltal megnövelve a hálózat biztonságát.

A CHAP egy három fázisú kézfogásos hitelesítő protokoll. A telephelyi forgalomirányító egy „challenge” üzenetet küld a távoli forgalomirányítónak, erre a távoli router ad egy válaszüzenetet, és ha egyezett a hash-elt jelszó a forgalomirányítón lévővel, akkor elfogadja a router a forgalmat, ha nem egyezik akkor pedig elutasítja.

A hitelesítés konfigurálása az alábbi parancsokkal történt az eszközeinken:

hostname MainRTR

username DEV20RTR password titok

interface S0/3/0

ip address 20.0.0.1 255.255.255.252

encapsulation ppp

ppp authentication chap

hostname RTRDEV20

username MainRTR password titok

interface S0/0/0

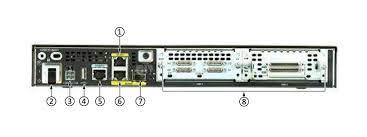
ip address 20.0.0.2 255.255.255.252

encapsulation ppp

ppp authentication chap

# Hálózati eszközök

## Forgalomirányítók

A telephelyre a forgalom két Cisco ISR 4221 Router segítségével halad. Ez az eszköz árát tekintve megfelelő, rendelkezik támogatással, így a jelentős biztonsági frissítéseket megkapja. Ezen kívül a jelenleg legújabb Cisco IOS operációs rendszer fut rajta.

## Kapcsolók

A képen elektronika látható

Automatikusan generált leírás

Második rétegbeli kapcsolók esetén a Cisco WS-C2960S-48LPL-L típuspú eszközöket használunk, szintén olcsó, viszont teljesítményében kiváló eszköz, ami a Cisco IOS operációs rendszer legújabb verziójával rendelkezik.

MultiLayer switch-ek terén a Cisco MDS 9000 széria lett kiválasztva, mivel késleltetése alacsony, teljesítménye kiváló, támogatottsága van, ára megfizethető és visszajelzések alapján egy nagyon megbízható eszköz a hálózat világába.

Cisco MDS 9148V 64G Multilayer Fabric Switch

## Végberendezések, Access Point-ok

Irodáink funkciótól változóan 5-10 személyi számítógéppel rendelkeznek, nyomtatókkal, fénymásolókkal, illetve a hálózat vezeték nélküli elérésének érdekében minden irodába telepítettünk egy Access Point-ot, mindemellett az igazgatói iroda egy belső szerverrel is kibővül.

# Redundancia

Belső hálózatunkon mind második, mind harmadik rétegbeli redundancia került megvalósításra.

## Második rétegbeli redundancia megvalósítása

Mivel minden kapcsolónk össze vannak kötve egymással, ezért az esetleges hálózati leállás bekövetkeztében sem fog elveszni a forgalom, hanem egy másik útvonalat használva fogja elérni a célját.

## Harmadik rétegbeli redundancia megvalósítása

Routereinken használjuk a Cisco által fejlesztett First Hop Redundancy Protocol-t, a **HSRP**-t. Ennek a protokollnak a feladata egy másodlagos átjárót biztosítson a hálózati végberendezések számára. Működése egyszerű, több interface-t kell egy alhálózatból címet kiosztani, amit a HSRP egy virtuális cím alá rendel. A végberendezéseknek ezt a virtuális címet kell megadni átjárónak, a protokoll pedig eldönti, melyik interface-et jelöli aktív, illetve melyeket passzív átjárónak. Ha az aktív interface leáll, esetleg a mögötte lévő link áll le, akkor áthelyezi az egyik passzív átjárót aktív szerepbe, ezáltal a forgalom képes tovább haladni zökkenőmentesen.

A képen szöveg, Betűtípus, fehér, algebra látható

Automatikusan generált leírás A képen szöveg, Betűtípus, fehér, algebra látható

Automatikusan generált leírás

*HSRP beállítások (RTRDEV20)*

A képen szöveg, Betűtípus, fehér látható

Automatikusan generált leírás A képen szöveg, Betűtípus, fehér, algebra látható

Automatikusan generált leírás

*HSRP beállítások (RTRDEV30)*

Ahogy a képeken is látható, mindegyik interface-en megadtunk egy IP-címet, ami a virtuális címként fog szerepelni a router beállításaiban.

A ’preemt’ paranccsal az interface mindig magának fogja igényelni az aktív szerepkört. Ezt érdemes minden interface-n beállítani, ezáltal a szerepkör választásban nem fog semmi hiba történni. A ’track’ paranccsal pedig egy, a routerből kimenő interface állapotát tudjuk nyomon követni, ezáltal, ha az esetleg leállna, a protokoll átadja az aktív szerepkört egy másik HSRP interface-nek.

# Forgalomirányítás

## Dinamikus forgalomirányító protokolljaink

Cégünk belső forgalomirányító protokollként az OSPF (Open Shortest Path First) dinamikus forgalomirányító protokollt választotta. Választásunk azért esett erre, mivel ez a protokoll a költségét legfőképpen sávszélesség alapján számítja ki, ezáltal az csomagok a legrövidebb idő alatt jutnak el a cél felé.

A képen sor, diagram, képernyőkép, Párhuzamos látható

Automatikusan generált leírás

A fenti ábrán a hálózat OSPF topológiája látható. A routerekből kimenő soros portok az úgynevezett ’Backbone’, azaz 0-s gyökérterületbe található. A hálózatra bemenő, GigabitEthernet interface-k a 10-es területben találhatók.

Az OSPF protokoll úgy fedezi fel a hálózatot, hogy OSPF-fel meghirdetett hálózatain ’Hello’ üzeneteket, csomagokat küld, és ha a szomszédos Router is küld ilyen csomagokat, a kapcsolat feláll. Ezekben a ’Hello’ üzenetekben megtalálható a Router által ismert OSPF útvonalak, ezáltal a többi forgalomirányító is fel tudja térképezni a hálózatot.

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás

A fenti ábra a sikeres OSPF kapcsolat felépítését mutatja

## Statikus forgalomirányítás

Mivel nem szeretnénk, hogy belső hálózatunk felesleges terhelés alá kerüljön, a belső hálózatra irányuló interface-eket passzív módba helyezzük, így a ’Hello’ üzeneteket nem továbbítja a végberendezések felé.

Mivel minden protokoll képes hibákba ütközni, így ez alól az OSPF sem kivétel.  
Hálózatunk rendelkezik alapértelmezett lebegő statikus útvonalakkal is, ezzel biztosítva, hogy ha a szomszédság fenttartása nem megoldható OSPF-en keresztül, akkor ezek az útvonalak veszik át a forgalomirányítás szerepét.



A fenti képen az RTRDEV20 forgalomirányító alapértelmezett lebegő statikus útvonalának beállítása látható.

# Kapcsolók konfigurációja

## Feszítőfa protokoll (STP)

A feszítőfa protokoll egy második (Adatkapcsolati) rétegbeli protokoll, ami a hurkok létrejöttét a hálózaton. Mivel hálózatunkon redundáns összeköttetést alkalmazunk, így a protokoll több kapcsolatot is le fog tiltani, hogy ezeket a hurkokat megakadályozza.

A képen sor, diagram, képernyőkép, Diagram látható

Automatikusan generált leírás

A fenti képen látható zöld és narancssárga jelzések mutatják, hol van a port letiltva, ezáltal ott képtelen lesz a forgalom haladni a hálózaton.

A Spanning-Tree Protocol elkezdi a csomagjait küldeni a szomszédos kapcsolóknak, amibe szerepel a Bridge ID, és amelyik switch-nek a legkisebb ez az értéke, az lesz a Route Bridge a hálózaton. Ezután a protokoll elkezd úgynevezett BDPU csomagokat küldeni a többi switch-nek, ezzel kiderítve merre keletkezhet hurok a hálózaton, és ezeket a port-(oka)t passzívvá teszi, azaz erre a forgalom nem tud haladni.

Alkalmaztam a feszítőfa protokoll RAPID-PVST módját, amivel lehetővé teszi a hálózat gyorsabb konvergálását.



## VLAN-ok

Telephelyünkön 2 virtuális helyi hálózat helyezkedik el, az egyik 10-es (felsővezetői), a másik pedig 20-as (fejlesztői) VLAN számmal.   
A VLAN-ok elengedhetetlen részei hálózatunknak, segítenek szegmentálni a hálózatot, illetve szükségesek az alinterfészek létrehozásához is. A telephelyen összesen négy aktív alinterfész van, amik szükségesek a harmadik rétegbeli redundancia kialakításához (lásd HSRP, 5. oldal)

A switch-eket összekötő portok Trunk módra vannak állítva, ezáltal a különböző VLAN-okból érkező forgalom szabadon haladhat a hálózaton.

|  |  |
| --- | --- |
| **VLAN** | **Hálózat** |
| 10 | 192.168.20.0 /24 |
| 20 | 192.168.30.0 /24 |

# Port Aggregation Protocol (PAGP)

A Port Aggregation protokoll egy EtherChannel technológia, ami a Cisco által lett szabadalmaztatva. Feladata, hogy több különálló fizikai portot egy logikai kapcsolat alá vegyen, ezzel megnövelve az adat és forgalomnak a terhelés elosztását. Egy PAgP EtherChannel maximum 8 fizikai linket képes kombinálni egy logikai linkbe. A mi hálózatunk esetében switch-enként két portot fogtunk össze egy logikai kapcsolat alá.

A protokoll két konfigurációs móddal rendelkezik, amiket a port konfigurációja közben adhatunk meg.

**Auto** – az interface képes válaszolni PAgP csomagok egyeztetésére, de ezt a folyamatot önmaga nem indíthatja el.

**Desirable** – az interface aktívan próbál egyeztetni szomszédos PAgP interface-ekkel.

Hálózatunkon az alábbi konfigurációval oldottuk meg a portok logikai linkbe történő összekapcsolását (példa):

Switch 2#conf t

Switch 2(config)# interface range Gig0/22 - 24

Switch 2(config-if-range)#speed 100

Switch 2(config-if-range)#duplex full

Switch 2(config-if-range)#switchport mode trunk

Switch 2(config-if-range)#channel-group 1 mode auto

Switch 2(config-if-range)#end

Switch 1#conf t

Switch 1(config)#interface range Gig0/22 - 24

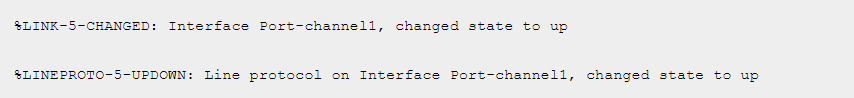
Switch 1(config-if-range)#speed 100

Switch 1(config-if-range)#duplex full

Switch 1(config-if-range)#switchport mode trunk

Switch 1(config-if-range)#channel-group 1 mode desirable

Switch 1(config-if-range)#end



*Siker esetén a következő üzenetet kell megkapjuk*

# SSH (Secure Shell)

Hogy hálózati eszközeinket biztonságosan tudjuk távolról konfigurálni, ahhoz SSH protokollt használunk.

Ennek konfigurálásához eszközünknek szüksége van egy egyedi hostname-re, egy felhasználóra és jelszó párosra, majd meg kell adni a DNS domain címét.

Ezután generálunk egy SSH kulcsot (ebben az esetben 1024 biteset), majd engedélyezzük az SSH-t a virtuális terminálokon.

Ahhoz, hogy megelőzzük a Brute Force támadásokat, megadhatjuk az „ip authentication-retries [maximum lehetőségek száma]” parancsot, így ha átléptük a maximum próbálkozási lehetőséget letiltja a csatlakozást az SSH.

Az alábbi módon állítottuk be routereinken az SSH protokoll-t:

Router (Config)#hostname EgyediHostName  
EgyediHostName(Config)#ip domain-name bytebrigade.local  
EgyediHostName(Config)#ip authentication-retries 2   
EgyediHostName(Config)#crypto-key generate rsa   
EgyediHostName(Config)#line vty 0 15  
EgyediHostName(Config-line)#transport input ssh  
EgyediHostName(Config-line)#exit

Az SSH-nak másik hasznos tulajdonsága, hogy képesek vagyunk vele egy SFTP fájlszervert létrehozni, ahol az adatok biztonságosan kerülnek továbbításra a hálózaton.

Igazgatói iroda

A képen képernyőkép, sor, diagram, tervezés látható

Automatikusan generált leírásAz igazgatói iroda rendelkezik 5 klienssel, egy Access Point-tal a vezeték nélküli elérés érdekében. Ezek mellett kibővül az iroda a belső szerverrel, ami az egész telephely számára címkiosztást, fájlmegosztást, illetve az Active Directory felhasználókat is ez a szerver authentikálja.

Az itt található eszközök címzése dinamikusan történik, amit az irodában található szervertől igényelhetnek a kliensek.

Az iroda a 192.168.20.0 /24 - es címtartományból kapja a címét, átjárója a 192.168.20.254, ami a RTRDEV20 forgalomirányító GigabitEthernet 0/0.10 és az RTRDEV30 forgalomirányító 0/0.30-as alinterface-én helyezkedik el mint virtuális IP-cím. A címtartomány mérete bőven kielégíti a kliensek címeit, emellett az alhálózat skálázható marad, tehát bármikor, leállás nélkül bővíthető további eszközökkel. A DHCP szerver által nem felhasznált címeket letiltottuk a kiosztásból, így növelve a hálózat biztonságát.

Mindemellett a telephely rendelkezik egy Access Point-tal, a vezeték nélküli elérés érdekében, illetve egy hálózati nyomtatóval.

# A képen képernyőkép, diagram, sor, Színesség látható Automatikusan generált leírásÜgyvezetői iroda

Az ügyvezetők irodája 10 klienssel, egy Access Point-tal a vezeték nélküli hálózat érdekében, és egy hálózati nyomtatóval rendelkezik. Az irodában elhelyezkedő eszközök a 192.168.20.0 /24-es címtartományból kapják a címeiket és az egyéb DHCP szolgáltatásokat a belső szerverünktől. Átjárónak a 192.168.20.254-es virtuális interfészt kapták meg a kliensek.

Az Access Point szintén a DHCP szervertől szerzi be az IP-címét, illetve a WLC címét is.

# Fejlesztői irodák

A képen képernyőkép, sor, diagram, kör látható

Automatikusan generált leírásTelephelyünkön két fejlesztők számára berendezett iroda található, amik 10 nagy teljesítményű klienssel, egy-egy Access Point-tal, illetve nyomtatóval rendelkezik.

Az első iroda a 192.168.30.0 /24 - ös tartományból kapja címeit a belső szervertől, emellett hálózati fájlmegosztás lehetőségét is biztosítja.

A második iroda funkcionalitását tekintve megegyezik az elsővel, az egyetlen különbség az, hogy ezen iroda kliensei a 192.168.30.128 /28 – as tartományból kapják címeiket.

# WLC (Wireless LAN Controller)

Telephelyünkön található egy WLAN Controller, ami segít a könnyebb, egyszerű módon konfigurálni, illetve karbantartani hálózatunk Access Point-jait.

Hálózatunkhoz a Cisco által fejlesztett, a Catalyst 9800-80 Wireless Controller névre hallgató eszközre esett a választás.



A választás a nagy terhelhetősége, magas átviteli sebessége, különböző beépített biztonsági megoldásai miatt esett erre a modellre. Mindemellett az egyik legújabb, Cisco IOS XE operációs rendszer fut az eszközön, amivel elérhetők a legmodernebb funkciók is.

Ez az eszköz képes felderíteni a hálózaton található Access Point-okat, független a hálózattól, és a VLAN-tól, amibe tartoznak. Miután a hálózaton lévő AP-kat felfedezte, onnantól kezdve, ha egy klienssel rácsatlakozunk a WLAN Controller-re, onnantól kezdve képesek vagyunk távolról is konfigurálni az AP-kat.

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás(A WLC sikeresen felismerte a hálózatban elhelyezkedő AP-kat, innentől ezeket képesek vagyunk AP csoportokba helyezni.)

## Konfiguráció

A WLC-n létrehoztam két Wireless LAN-t FelsovezWLAN és FejlesztoWLAN néven. A FelsovezWLAN a 10-es VLAN eszközeinek biztosít hálózatelérést, a FejlesztoWLAN a 20-as VLAN eszközeinek.

A képen szöveg, képernyőkép, szoftver, képernyő látható

Automatikusan generált leírás

A WLC DHCP kezelőjében létrehoztam mind a kettő WLAN-nak címkioszást, így a rá csatlakozó eszközök ki fognak tudni jutni a hálózatra.

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás

Ennek az eszköznek egy másik képessége az, hogy különböző frissítéseket (pl.: Szoftverfrissítéseket) képesek biztosítania a távoli elérést szolgáló eszközeink számára.

# Szerverek

## Belső szerver

A telephelyünk belső szervere klienseink számára DHCP funkciókat, azaz IP-címet, átjárót, a fájlszerverek, DNS szerverek címét igényelhetik. Emellett belső hálózati forgalomirányitóink számára RADIUS hitelesítést nyújt belső szerverünk.

A képen szöveg, képernyőkép, képernyő, szám látható

Automatikusan generált leírás

A fenti ábrán a belső szerverünk DHCP bejegyzései találhatóak meg (Packet Tracer)

## Windows Server 2019

Mivel csapatunk a Windows Server 2019-es verziójával rendelkezik tapasztalattal, ezért ez a belső kiszolgáló ezzel az operációs rendszerrel fogja konfigurálni a szolgáltatásokat, amikre a klienseknek szüksége lesz az irodáinkban.

## NIC-Teaming

A szerverünk belső hálózati kártyáit egy logikai kártyává alakítottuk a NIC-Teaming segítségével, ezáltal megnövelve a maximálisan elérhető sávszélességet.

A két belső hálózati kártya logikai összekapcsolásával egy kétszer olyan gyors átviteli sebességre képes digitális kártyát hoztam létre.

A képen szöveg, képernyőkép, képernyő, szoftver látható

Automatikusan generált leírás

## DHCP

A Dynamic Host Configuration Protocol (DHCP) egy kliens/szerver protokoll, ami automatikusan IP-címet, hálózati maszkot, és alapértelmezett átjáróval látja el a klienseket. Ezek az alap információk mellett a DHCP szerver megosztja a kliensekkel a DNS-szerver(ek) címét, fájlszerver(ek) címét.

Számos előnye közül a legfontosabb, hogy a protokoll automatikusan ossza ki a címeket azoknak a klienseknek, akik kérést nyújtanak be a szervernek, ezáltal megkönnyítve a rendszergazda dolgát, akinek nem statikusan kell konfigurálja ezáltal az iroda összes kliensét.

Ezeket a címeket a host-ok egy bizonyos időtartamra bérelhetik, amint ez a bérleti idő (lease time) lejár, abban az esetben egy új DHCP kérést kell küldeni a szervernek, ami ismét információkkal fogja ellátni a klienst. A mi hálózatunkba 12 órára esett a bérleti időnek a hossza, így a leghosszabb műszak esetén is a kliens leállásáig rendelkezni fog a szükséges információkkal.

A DHCP szerver telepítését és konfigurálását az alábbi módon végeztük:

* Telepítettük a szerverre a varázsló segítségével a DHCP szerver szolgáltatást.

A képen szöveg, képernyőkép, szoftver, Weblap látható

Automatikusan generált leírás

* Létrehoztuk a hatókört a Felsővezetőség és a Fejlesztők számára egyaránt

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

Sikeres DHCP kérés után az alábbi címeket kapta meg a kliens a kiszolgálótól:

A képen szöveg, elektronika, képernyőkép, képernyő látható

Automatikusan generált leírás

## DNS (Domain Name Service)

Belső szerverünk névfeloldást is végez, ezért a tartományban lévő számítógépek elsődleges DNS szervere, ha ez meghibásodik akkor pedig a DMZ-ben lévő szerver veszi át a névfeloldó kiszolgáló szerepét.

Szerverünk DNS kiszolgálóján csak Címkeresési zóna lett konfigurálva, mivel Névkeresési zóna létrehozásának különösebb előnye nincs a hálózat részére.

A képen szöveg, képernyőkép, szoftver, képernyő látható

Automatikusan generált leírás

## Active Directory (Címtár)

Ahhoz, hogy a telephelyen elhelyezkedő nagy mennyiségű kliens-et egyidejűleg tudjuk felügyelet alatt tartani, illetve csoportokat és felhasználókat tudjuk létrehozni a Windows szerver Active Directory tartományi szolgáltatásait vesszük igénybe.

A gyökértartomány domain-je a „bytebrigade.local”

A szerver tartományi kiszolgálóvá való előléptetése után létrehoztuk a szervezeti egységünket ByteBrigade néven, amibe két csoportot definiáltunk:

* Felsővezetők
* Fejlesztők

Ahhoz, hogy új felhasználókat egyszerűen lehessen létrehozni a címtárban, mindkét csoport részére létre lett hozva egy minta felhasználó, amit csak át kell nevezni és már alap konfigurációval rendelkezik.

A képen szöveg, képernyőkép, szoftver, képernyő látható

Automatikusan generált leírás

A szerver meghajtóján létrehoztunk egy megosztott mappát „Jelentések” néven, amit mind két csoport tagjai elérnek, viszont ezekhez különböző jogosultságok tartoznak.

A „Jelentések” mappa tartalmaz még két almappát, „Manager jelentések” és „Fejlesztői jelentések” néven.

Az ezen mappákban tárolt fájlokat mindkét csoport tagjai képesek olvasni, viszont egymásét nem képesek módosítani (Átnevezni, eltávolítani stb.).

## Biztonsági mentések

Szerverünkre TFTP protokoll segítségével, biztonsági mentések lettek készítve hálózatunk forgalomirányítóinak, kapcsolóinak konfigurációjáról, így azok meghibásodása esetén is helyre tudjuk állítani az eszközök beállításait a lehető leghamarabb.

## Csoportházirendek

A Windows szerverek egyik hatalmas előnye a csoportházirend, amivel megoldható a tartományban lévő felhasználók, számítógépek, csoportok jogosultságainak egyidejű szabályozása.

A ’Számítógépek’ elnevezésű csoportházirend objektumban kezeljük a tartomány klienseit.

A fejlesztők csoport tagjainak első bejelentkezéskor automatikusan feltelepül a Visual Studio C# fejlesztői környezete, illetve a Visual Studio Code program.

## Külső szerverek

Természetesen ahhoz, hogy fájljainkat teljes mértékbe biztonságba tudhatjuk hálózatunk rendelkezik másodlagos fájlszerverrel is, ami az Ügyfélszolgálati telephelyen található, ahol a biztonsági mentéseinket tároljuk. Ez a szerver még NTP szolgáltatást nyújt a forgalomirányítóink számára, így minden eszközünkön szinkronizálva van az idő.

A képen szöveg, Betűtípus, nyugta, képernyőkép látható

Automatikusan generált leírás

NTP (Network Time Protocol) beállítása forgalomirányítón, adatait a külső szerverről szerzi be

# Tesztelés

A telephely kliensei elérik a többi telephely eszközeit(Távmunkás telephely, Ügyfélszolgálati telephely):

A képen szöveg, képernyőkép, Betűtípus, tervezés látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

DNS szerver tesztelése:

A képen szöveg, képernyőkép, szoftver, képernyő látható

Automatikusan generált leírás

Távoli elérés tesztelése:

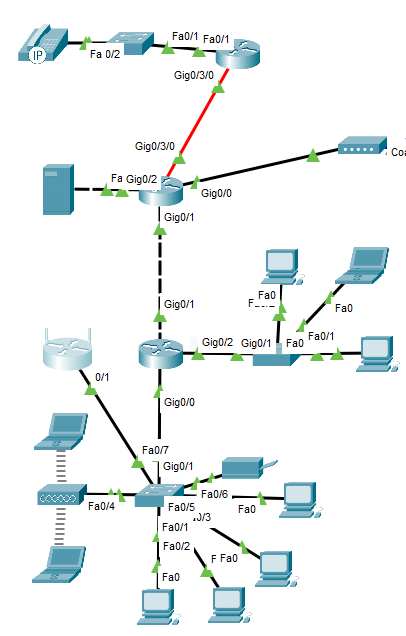
A képen szöveg, képernyőkép látható

Automatikusan generált leírás

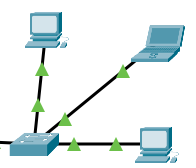
# **Távmunkás iroda**

A távmunkás iroda a felhőben kapcsolódik a többi irodával. A Byte Brigade távmunkás irodája Szombathelyen helyezkedik el. A szombathelyi irodában van a legtöbb papírmunka. A fejlesztők itt dolgoznak új funkciók tesztelésén és optimalizálásán. A cég és partnerei között megállapodásokat hoznak létre. Az iroda magas sebességű internetkapcsolattal és biztonságos hálózattal rendelkezik.

A távmunkás iroda a felhőben kapcsolódik a többi irodával. Beállítások terén DHCP, IPv4 és IPv6 címezés, Port Forwarding és WIFI kerül beállításra. Access Point-ok, BGP, DHCPv6 szerver. A forgalomirányítás EIGRP-vel van megoldva.

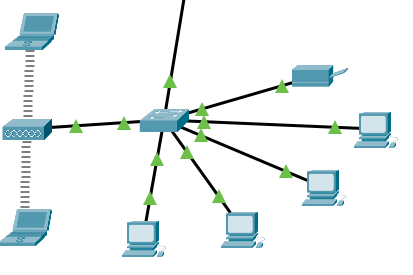


# Igazgatói iroda



Az igazgatói irodában folyik minden egyes tesztelési és fejlesztési folyamat és projekt. Ebben az irodában felügyelik a telephelyi irodák munkáit, projektjeit és a feladatokat is innen adják ki a dolgozóknak. Az igazgató iroda fontos szerepet tölt be, mivel itt döntjük el, hogy kivel mikor és milyen megállapodású szerződést kötünk.

# Telephelyi iroda



Ebben az irodában folynak kisebb tesztelések és fejlesztések akár a hálózatban, akár magát az irodában, de a fő fejlesztő rész az az igazgatósági iroda feladata. mivel az iroda külön helyezkedik el a többi telephelytől, sokkal szabadabb a légkör. Az irodában köttetnek meg a szerződések nagy százaléka. Itt dolgozunk az új funkciók fejlesztésé, létrehozásán és tökéletesítésén. Ha a tervek szerint haladunk akkor idővel mind a kettő másik telephely is megkapja a fejlesztéseket, melyen sikerült optimalizálni és minden hibát kijavítani, helyrehozni, hogy a lehető legtökéleteseb legyen.

# Kábelezés

A hálózatnál mindegy, hogy egyenes vagy keresztkötésű rézkábelt használunk az összeköttetéshez, ugyanis minden eszköz támogatja az **AUTO-MDIX** funkciót. Az AUTO-MDIX felismeri, hogy milyen kábelt csatlakoztattunk az adott hálózati eszközhöz, és ha szükséges, a kábel ereit keresztezi, így a különböző eszközök között mindig a helyes kábel típust használja, mindegy, hogy milyen típusú kábelt csatlakoztattunk.Az AUTO-MDIX-et a mdix auto paranccsal lehet aktiválni interfész konfigurációs módban, ha ez alapból nem lenne bekapcsolva az adott hálózati eszközön.

# Eszközök

* Ebben az irodában 2 forgalomirányító található, az egyik az átjáró, ami az internettel és az ügyfélszolgálattal (VPN-en keresztül) kapcsolja össze az irodát.A képen elektronika, Elektrontechnika, gép, Számítógép-alkatrész látható

  Automatikusan generált leírás
* A forgalomirányítók a Packet Tracerben 2911-es típusúak, viszont a valós hálózatban mi a **Cisco 422 Series Integrated Services Router** forgalomirányítót választanánk.
* Azért ezt a forgalomirányító típust választottuk, mert ez a forgalomirányító jelenleg is támogatott a Cisco által és megkapja a legújabb biztonsági frissítéseket, és a legújabb iOS verzióval rendelkezik.

A képen elektronika, villamosenergia-ellátás látható

Automatikusan generált leírás

* Az irodában található 2 db **Cisco CBS530** kapcsoló is. Ezt a kapcsolótípust azért választottuk, mert költséghatékony, olcsó, stackelhető, moduláris, ezáltal bővíthető és a Cisco legújabb iOS verzióját használja. Ezenkívül 10 hálózati portja, támogatja a PoE-t, akár 20 Gb/s kapacitásra képes és IPv6 támogatást biztosít.
* WIFI Routernek a Linksys Velop MX12600 Routert választottuk, mivel ez a WIFI router az egyik legmodernebb.A képen hangszóró, tervezés látható

  Automatikusan generált leírás
* Támogatja a WIFI 6 szabványt és a WPA3 autentikációt.
* Egyszerű beállítani a Linksys applikációval.
* A Távmunkás irodában nem helyeztem el wifi routert, de ha lenne akkor mindenféleképpen ezt a típust választottam volna.
* Access Pointnak a Cisco AIR-AP28021-E-K9-et választottuk, mivel rendelkezik belső antennával és támogatja a PoE-t az egyszerűsített integráció érdekében.A képen computer, számítógép, alma látható

  Automatikusan generált leírás
* 802.11ac Wawe 2, kettős 5GHz-és és rádió támogatás.
* A képen elektronika, Elektronikus eszköz látható

  Automatikusan generált leírásAz Access Pointot azért helyeztük el a Távmunkás irodába, hogy ne keljen wifi routert használni. Az AP a 2 munkáslaptopnak oszt címeket.
* Munkaállomásnak a DELL PC Optiplex 5000 MT-választottuk, mivel Intel Core i5-12500-as CPU-val , 8GB RAM-al és 256GB-os SSD-vel van felszerelve. (OS: Windows 10)
* Ebből a kialakítású pc-ből 7db helyezkedik el az irodában.
* A DELL Latitude 7280-as Laptopot választottam az irodába.A képen elektronika, computer, Elektronikus eszköz, Netbook látható

  Automatikusan generált leírás
* Processzora: Intel® Core i5-6200U 2.30 GHz, memória 8GB DDR4 és a háttértás 256GB SSD.
* A telephelyen 3 db laptop található.
* Kiszolgálónak a Hewlwtt Packard Enterprise HPE ProLiant ML110 G10 4.5U Tower Servert választottuk, mivel Intel Xeon Silver 4208-as CPU-val, 16GB RAM-al és Seagate 2TB Barracuda SATA3 HDD-vel van felszerelve (OS: Windows)A képen elektronika, Elektronikus eszköz, Számítógép-alkatrész, Számítógépes hardver látható

  Automatikusan generált leírás
* Nyomtatónak a Canon Pixma TS705A Nyomtatót választottam az irodába.A képen elektronika, nyomtató, fedett pályás, fénymásoló látható

  Automatikusan generált leírás
* Egy okos eszkeszkör és vagy alkalmazás segítségével akár egy gombnyomásal is lehet vele nyomtatni.
* A színes és fekete patronokat könnyen lehet cserélni és beszerezni egyaránt.

# IP címzés

|  |  |  |
| --- | --- | --- |
| **Eszköz** | **Interface** | **IP cím/ Mask** |
| Távmunkás Router 1 | GigabitEthernet0/0 | 10.110.30.2/24 |
| GigabitEthernet0/1 | 172.16.0.1/16 |
| GigabitEthernet0/2 | 9.9.9.1/28 |
| GigabitEthernet0/3/0 | 172.11.1.1/24 |
| Tunnel10 | 1.1.1.1/30 |
| Távmunkás Router 2 | GigabitEthernet0/0 | 192.168.200.1/24 |
| GigabitEthernet0/1 | 172.16.0.2/16 |
| GigabitEthernet0/2 | 192.168.210.1/24 |
| Távmunkás Router 3 | GigabitEthernet0/1 | 172.12.1.1/24 |
| GigabitEthernet0/3/0 | 172.11.1.2/24 |

# Végberendezések

|  |  |
| --- | --- |
| Eszköz | IP cím |
| TavSzerver | 9.9.9.9/28 |
| HMLaptopok | DHCP |
| TMPC-k | DHCP |
| TIMPC-k és TIMLaptop | DHCP |
| Nyomtató | 192.168.200.10/24 |

# FTP

Jelentése: Az FTP a File Transfer Protocol rövidítése, azaz a kifejezést magyarra fordítva „Fájl átviteli protokoll”, ami egy állományátvitelre szolgáló szabvány.

A projektbe azért raktam bele a FTP-t, mert a használata rendkívül egyszerű. A szerveren lévő felhasználónévvel és jelszóval védett mappához könnyen hozzátudunk férni, ahol fájlokat tudunk feltölteni, letölteni, módosítani vagy akár törölni is.

A projektben az FTP alkalmazására a TavSzervert alkalmaztam. A szerveren a szolgáltatások fülön kiválasztottam az FTP fület, ahol megadtam a felhasználónevet a Tavmunkast és létrehozatam egy jelszót, ami nem a legbiztonságosabb, de a jelenlegi helzetben tökéletes. A lehetséges eszközökből mindent kiválasztottam, így tudunk a mappába írni, olvasni, törölni, átnevezni és listázni is.

A képen szöveg, képernyőkép, képernyő, szoftver látható

Automatikusan generált leírás

## Tesztelése

A FTP tesztelése a TMPC1-et választottam. Először csináltam egy fájlt Projekt néven a TMPC1 Text Editorában majd a Command Prompt ablakban a dir paranccsal ellenőriztem, hogy létrejött-e.

A képen szöveg, szoftver, Számítógépes ikon, Weblap látható

Automatikusan generált leírás

A képen szöveg, elektronika, képernyőkép, szoftver látható

Automatikusan generált leírás

# HTTPS

Azért döntöttem a HTTPS mellett a projektben, mivel a HTTPS a HTTP protokoll biztonságos verziója. A HTTPS titkosított kapcsolatot biztosít a Távmunkás iroda gépei között, mivel védi a felhasználói adatokat az illetéktelen hozzáférésektől.

A projetben a Tavszervert választottam, ahol a szolgáltatások fülön először kikapcsoltam a http titkosítást mivel arra nem volt szükségem. Utána létrehoztam a Projekt.html fájlt. Ezek után már csak az tesztelés maradt hátra.

A képen szöveg, képernyőkép, képernyő, szám látható

Automatikusan generált leírás

## Tesztelése

A HTTPS tesztelésére a TIMPC1-et választottam, ahol a Web Browser ablakban beírtam a szerver ip címét a 9.9.9.9-et. A mi fontos, hogy az URL-nél nem http van, hanem https.

A képen szöveg, elektronika, képernyőkép, képernyő látható

Automatikusan generált leírás

# DHCP

A dinamikus állomáskonfiguráló protokoll (Dynamic Host Configuration Protocol) azaz a DHCP egy számítógépes hálózati kommunikációs protokoll. Ezzel a protokollnak köszönhetően a kliens gépek és laptopok autómatikusan kapják az ip címüket és a maszkukat. A DHCP-nek köszönhetően NEM kell manuálisan beállítani az ip címeket.

A projektben azért alkalmaztam dynamic host configuration protocolt mert ennek köszönhetően nem kell minden egyes pc-nek, laptopnak, szervernek, nyomtatónak vagy bármilyen olyan eszköznek statikusan IP címet konfigurálni, mert a DHCP megoldja, hogy autómatikusan kapjanak IP címet és maszkot is, de még akár DNS-t is.

Az irodában a DHCP-t használó szerver a TavSzerver. Kettő külöbálló DHCP van az irodában. Az egyik a Tav1 a másik pedig a Tav2. A Tav1 a TMPC-nek és a HMLaptopoknak azaz a TavMunkás gépeknek és a hordozható munkás laptopoknak oszt ip-t és maszkot (192.168.200.1/24). A Tav2 pedig a TIMPC-nek és TIMLaptopnak azaz Táv igazgatósági Munkás gépeknek és laptopnak oszt (192.168.210.1/24).

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

## DHCP Tav1

A képen szöveg, képernyőkép, szám, Betűtípus látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, sor, Betűtípus látható

Automatikusan generált leírás

## DHCP Tav2

A képen szöveg, képernyőkép, szám, Betűtípus látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás

A hálózat, program, hálózat és a szerver könnyebb futtatása érdekében a felesleges és nem használt szolgáltatásokat kikapcsoltam. Ide tartozik a HTTP, a DHCPv6, az AAA, az NTP, az EMAIL és az IoT.

# DNS

A Domain Name System (DNS), azaz a tartománynévrendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az [internetre](https://hu.wikipedia.org/wiki/Internet) vagy egy [magánhálózatra](https://hu.wikipedia.org/wiki/Mag%C3%A1nh%C3%A1l%C3%B3zat) kötött bármilyen erőforrás számára. A részt vevő entitások számára kiosztott [tartománynevekhez](https://hu.wikipedia.org/wiki/Tartom%C3%A1nyn%C3%A9v) különböző információkat társít. Legfontosabb funkciójaként az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető numerikus azonosítókká „fordítja le”, „oldja fel”, melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton.

Az internet működéséhez két fő [névteret](https://hu.wikipedia.org/wiki/N%C3%A9vt%C3%A9r) tartanak fönt: a tartománynév-hierarchiát és az IP-címteret. A Domain Name System a tartománynév-hierarchiát üzemelteti és fordítási szolgáltatást nyújt a tartománynevek és az IP-címterek között.

Ha a távmunkás szerver leállna vagy tönkre menne akkor az ügyfélszolgálat és az igazgatósági szervert másodlagos és harmadlagos dnst biztosítana a távmunkás iroda számára.

A projektben a Tavszervert választottam a DNS alkalmazására. A szerver szolgáltatási közül kiválasztottam a DNS-t, amiben létrehoztam a tav nevű dns kiszolgálót aminek a címe megegyezik a szerver ip címével azaz a 9.9.9.9-el.

A képen szöveg, képernyőkép, szám, Betűtípus látható

Automatikusan generált leírás

## Tesztelése

A dns ellenőrzésére a TavmunkasPC1-et választottam. A Pc desktop fülén kiválasztottam a Web Browsert és a keresőbe beírtam a dns szerver nevét, vagyis azt hogy tav. A képen szöveg, képernyőkép, képernyő, Betűtípus látható

Automatikusan generált leírás

# NAT

A hálózati cím fordítás (NAT) nyilvános vagy globálisan továbbítható Internet protokoll (IP) címekké változtatja a belső vagy magán címeket. A NAT a portokat is lefordítja. Az irodában azért lesz előnyös a NAT, mert a NAT megvalósításához elegendő egyetlen 1 IP címet megadnunk. Ezenkívül azért is használtam NAT-ot, mert kevesebb számítógép erőforrást használ, mint a SOCKS vagy a proxy szerverek. A hátrány viszont az, hogy csak minimális naplózási szolgáltatásokat biztosít számunkra.

A projektbe azért alkalmaztam NAT-ot, mert elmenti a nyilvános IP címeket, átlátszó a kliens számára, így lehetővé teszi kliensek széles körének támogatását és elrejtí a belső hálózat IP címeit.

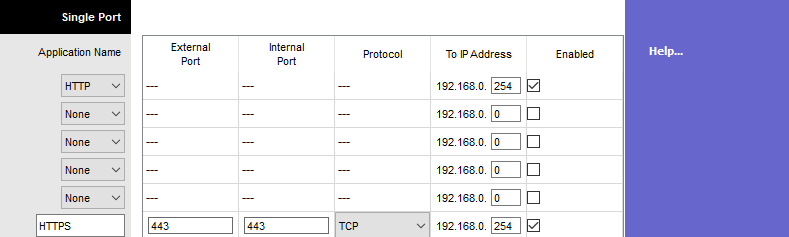
Beállítása:

A képen szöveg, képernyőkép látható

Automatikusan generált leírás

# Port Forwarding

Azért alkalmaztam a projektben a porttovábbítást, mert megkönnyíti a távoli számítógépek, például [az internetes](https://en.wikipedia.org/wiki/Internet) gazdagépek csatlakozását egy adott számítógéphez vagy szolgáltatáshoz a [helyi hálózaton](https://en.wikipedia.org/wiki/Local_area_network) (LAN-on) belül.



# IPv6 címzés

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Eszköz** | **Interface** | | **IP cím/ Mask** | |
| Távmunkás Router 1 | GigabitEthernet0/1 | | 2002::CAFE/64 | |
| GigabitEthernet0/2 | | 2001::CAFE/64 | |
| Távmunkás Router 2 | GigabitEthernet0/0 | | 2002::8100:0:0:0/64 | |
| GigabitEthernet0/1 | | 2002::DEAD/64 | |
| GigabitEthernet0/2 | | 2003::1/64 | |
| TavSzerver | FastEthernet0/0 | | 2001::FF15/64 | |
| PC-k és laptopok | | Autómatikus (2003::…) | |

A projektben az IPv4 mellet azért tartottam fontosnak az IPv6 alkalmazását, mivel számos előnnyel jár a használata. Az IPv6 címtartomány hatalmas, ami lehetővé teszi a hatalmas mennyiségű eszköz egyidejű kezelését és az egyedi címek biztosítását minden eszköz számára anélkül, hogy ki kellene találni trükkös címtartományokat vagy NAT-ot alkalmazni. Az IPv6 hatékonyabb és biztonságosabb protokoll, amely lehetővé teszi a gyorsabb adatátvitelt és a fejlettebb biztonsági funkciók használatát, például a beépített IPsec támogatást. Mivel az IPv6 a jövőbeli internet protokollja, az IPv4-es címek kimerülése miatt egyre fontosabbá válik az IPv6 címezés használata a hálózatokban. A projekt IPv6-kompatibilissá tétele elősegíti a hosszú távú skálázhatóságot és kompatibilitást.

A projektben az IPv6 címzés szinte csak a távmunkás irodában található. A jövőre való tekintettel az IPv6 alkalmazása és fejlesztgetése tesztelés jelleggel működik. Mivel a jövőben valószínűleg az ipv6 sokkal fejlettebb lesz és több fejlesztést kap, ezért is alkalmaztam ipv6-ot.

# Forgalomirányítás

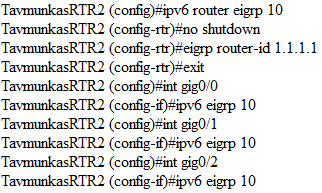
## 

## EIGRP

Az Enhanced Interior Gateway Routing Protocol azaz a EIGRP egy [hálózati protokoll](https://www.techtarget.com/searchnetworking/definition/protocol) , amely lehetővé teszi [az útválasztók](https://www.techtarget.com/searchnetworking/definition/router) számára, hogy hatékonyabban cseréljenek információkat, mint a korábbi hálózati protokollok, mint például az Interior Gateway Routing Protocol azaz a IGRP vagy a Border Gateway Protocol azaz a [BGP](https://www.techtarget.com/searchnetworking/definition/BGP-Border-Gateway-Protocol).

Először is elindítittam az EIGRP-t ezzel a paranccsal: ipv6 router eigrp. A látható szám az autonóm rendszerszám, amelynek mindkét útválasztón meg kellett egyeznie. Minden EIGRP útválasztónak szüksége van egy útválasztó azonosítóra, amely az útválasztó legmagasabbIPv4-címe. Ha nincs IPv4-címe, akkor magának kell megadnia az útválasztó azonosítóit a paranccsal router-id.

konfigurálása a TavmunkasRTR2-ön:



A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, Betűtípus, sor látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás



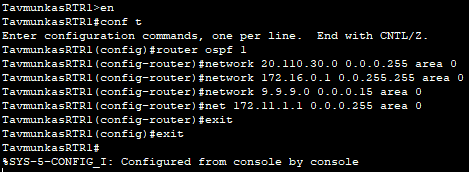
Lehetne beállítani passzív interface-t, de és szeretném hogyha mindenki megkapni minden egyes forgalomirányító protokolt. (Ez csak egy példa:)



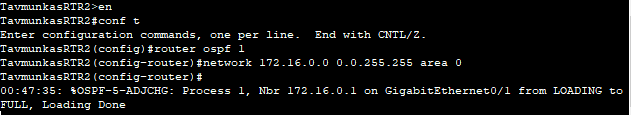
## OSPF

Az OSPF az Open Shortest Path First rövidítése. Magyarul legrövidebb út először. Az OSPF egy kapcsolatállapot alapú forgalomirányító protokoll.

A projektben azért alkalmaztam OSPF-t, mivel gyors konvergenciát biztosít, könnyen skálázható és nincs periódikus frissítés. A hálózaton belül a Tavmunkas RTR1-en konfiguráltam ospf-et.



Ezután beállítottam az ospf-et a TavmunjasRTR2-őn is és ellenőriztem, hogy létrejött-e a szomszédság. A kapcsolódás sikeresen összejött.



# IP telefónia

A hálózatban konfiguráltam IP telefóniát is, az ügyfélszolgálati irodában. Ez csak tesztelés gyanánt van benne az irodában. Ha minden a tervek szerint halad akkor a megkapja az iroda a fejlesztéseket és teljes körben alkalmazni fogjuk. Az IP-telefon olyan eszköz, amely a hang továbbítását IP-hálózaton keresztül biztosítja. Az IP-alapú hangszolgáltatások összefoglaló neve VoIP azaz Voice over IP. Az IP-telefonok és kliensek egy kiszolgáló segítségével közös hálózatba kapcsolhatók. Az összekapcsolt eszközök rövid hívószámokon keresztül is elérik egymást a nehezen megjegyezhető IP-szám helyett. Megfelelő átjáró (gateway) használatával az IP-telefon képes kapcsolatot teremteni más telekommunikációs hálózatokkal. Ezt a lehetőséget a mobilszolgáltatók már évek óta elérhetővé tették.

A képen telefon, Elektronikus eszköz, Vezetékes telefon, elektronika látható

Automatikusan generált leírás

# 

# Access Point

Az irodába azért telepítettünk access pointot mivel több mint 5 gép helyezkedik el és az access point jelentősen megkönnyíti a folgunkat

Az Access Point magyarul Hozzáférési Pont egy olyan eszköz, ami vezeték nélküli kommunikációs végberendezéseket kapcsol össze vezetékes hálózattal.

Access Pointra akkor van szükség, ha az útválasztó nem tud WLAN-hálózatot létrehozni, és így funkcionális bővítésként szolgál.

Ezenkívül egy hozzáférési pont növelheti a WLAN-jel hatótávolságát. Ez különösen akkor fontos, ha egy végberendezést már nagyon nagy távolságra használnak az útválasztótól, és a jelerősség túl gyenge.

Az Access Point hatótávolsága a modelltől függ, és akár 100 méter is lehet. Általában az egysávos hozzáférési pontok nagyobb hatótávolsággal rendelkeznek, mint a kétsávos hozzáférési pontok.

# Mentések

A Tavszerverre a TFTP protokoll segítségével, biztonsági mentéseket készítettem a távmunkás telephelyi és igazgatósági irodák forgalomirányítóinak, kapcsolóinak konfigurációjáról, így azokat hiba esetén is helyre tudjuk állítani.

# Tesztelések

TMPC1-től pingeltem a 192.168.210.1-et azaz a TIMPC2 IP címét. A pingelés sikeres volt, tehát látják egymást és tudnak kommuníkiálni egymással.

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

**A projekt feladatelosztása:**

A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás

Tartalom

[A hálózat topológiája 2](#_Toc165838219)

[**Ügyfélszolgálat és rendszerfelügyeleti telephely** 3](#_Toc165838220)

[Eszközválasztás 3](#_Toc165838221)

[IP címzés 4](#_Toc165838222)

[Hálózati eszközök 4](#_Toc165838223)

[Végberendezések 5](#_Toc165838224)

[Kábelezés 6](#_Toc165838225)

[DHCP 6](#_Toc165838226)

[DHCP snooping 8](#_Toc165838227)

[MAC-cím szűrés, Portfast 8](#_Toc165838228)

[IP telefónia 9](#_Toc165838229)

[Forgalomirányítás 9](#_Toc165838230)

[OSPF 9](#_Toc165838231)

[VPN 10](#_Toc165838232)

[ASA 11](#_Toc165838233)

[Hozzáférési lista 13](#_Toc165838234)

[Hálózati címfordítás 13](#_Toc165838235)

[Rendszerfelügyeleti beállítások 14](#_Toc165838236)

[DNS 14](#_Toc165838237)

[SSH 14](#_Toc165838238)

[SYSLOG 14](#_Toc165838239)

[RADIUS 15](#_Toc165838240)

[NTP 16](#_Toc165838241)

[FTP és TFTP 16](#_Toc165838242)

[SNMP 16](#_Toc165838243)

[NetFlow 17](#_Toc165838244)

[Redundancia 17](#_Toc165838245)

[STP 17](#_Toc165838246)

[HSRP 18](#_Toc165838247)

[Lebegő Statikus útvonalak 19](#_Toc165838248)

[Programozott hálózatkonfiguráció 20](#_Toc165838249)

[Linux szerver 21](#_Toc165838250)

[DHCP 21](#_Toc165838251)

[HTTP 22](#_Toc165838252)

[HTTPS 23](#_Toc165838253)

[DNS 25](#_Toc165838254)

[SAMBA Fájlmegosztás 26](#_Toc165838255)

[Tesztelés 28](#_Toc165838256)

[**Fejlesztői telephely és igazgatóság** 31](#_Toc165838257)

[Telephely célja, topológia, IP-címzés 31](#_Toc165838258)

[Kábelezés 32](#_Toc165838259)

[PPP 32](#_Toc165838260)

[Hálózati eszközök 33](#_Toc165838261)

[Forgalomirányítók 33](#_Toc165838262)

[Kapcsolók 33](#_Toc165838263)

[Végberendezések, Access Point-ok 33](#_Toc165838264)

[Redundancia 34](#_Toc165838265)

[Második rétegbeli redundancia megvalósítása 34](#_Toc165838266)

[Harmadik rétegbeli redundancia megvalósítása 34](#_Toc165838267)

[Forgalomirányítás 35](#_Toc165838268)

[Dinamikus forgalomirányító protokolljaink 35](#_Toc165838269)

[Statikus forgalomirányítás 36](#_Toc165838270)

[Kapcsolók konfigurációja 36](#_Toc165838271)

[Feszítőfa protokoll (STP) 36](#_Toc165838272)

[VLAN-ok 38](#_Toc165838273)

[Port Aggregation Protocol (PAGP) 39](#_Toc165838274)

[SSH (Secure Shell) 40](#_Toc165838275)

[Ügyvezetői iroda 41](#_Toc165838276)

[Fejlesztői irodák 42](#_Toc165838277)

[WLC (Wireless LAN Controller) 42](#_Toc165838278)

[Konfiguráció 43](#_Toc165838279)

[Szerverek 45](#_Toc165838280)

[Belső szerver 45](#_Toc165838281)

[Windows Server 2019 46](#_Toc165838282)

[NIC-Teaming 46](#_Toc165838283)

[DHCP 47](#_Toc165838284)

[DNS (Domain Name Service) 49](#_Toc165838285)

[Active Directory (Címtár) 50](#_Toc165838286)

[Biztonsági mentések 51](#_Toc165838287)

[Csoportházirendek 51](#_Toc165838288)

[Külső szerverek 51](#_Toc165838289)

[Tesztelés 52](#_Toc165838290)

[**Távmunkás iroda** 55](#_Toc165838291)

[Igazgatói iroda 56](#_Toc165838292)

[Telephelyi iroda 56](#_Toc165838293)

[Kábelezés 56](#_Toc165838294)

[Eszközök 57](#_Toc165838295)

[IP címzés 59](#_Toc165838296)

[Végberendezések 60](#_Toc165838297)

[FTP 61](#_Toc165838298)

[Tesztelése 62](#_Toc165838299)

[HTTPS 63](#_Toc165838300)

[Tesztelése 63](#_Toc165838301)

[DHCP 64](#_Toc165838302)

[DHCP Tav1 65](#_Toc165838303)

[DHCP Tav2 66](#_Toc165838304)

[DNS 67](#_Toc165838305)

[Tesztelése 67](#_Toc165838306)

[NAT 68](#_Toc165838307)

[Port Forwarding 69](#_Toc165838308)

[IPv6 címzés 69](#_Toc165838309)

[Forgalomirányítás 70](#_Toc165838310)

[EIGRP 70](#_Toc165838311)

[OSPF 71](#_Toc165838312)

[IP telefónia 72](#_Toc165838313)

[Access Point 73](#_Toc165838314)

[Mentések 74](#_Toc165838315)

[Tesztelések 74](#_Toc165838316)