Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

Informatikai rendszer- és alkalmazás-üzemeltető technikus

5-0612-12-02

**VIZSGAREMEK**

**Magyarországi Hotel komplexum**

Görhöny Márk, Vanyek Máté, Vigh Zoltán

2/14.B

Budapest, 2023

Tartalomjegyzék

[1.Bevezetés 3](#_Toc165764992)

[2. Hálozat felépítése 3](#_Toc165764993)

[2.1 Center 5](#_Toc165764994)

[2.1.1 *Üzemeltetők* konfigurációja 7](#_Toc165764995)

[2.1.2 *New York Hotel* konfigurációja 10](#_Toc165764996)

[2.1.3 *Backup* konfigurációja 13](#_Toc165764997)

[2.1.4 *Laguna Motel* konfigurációja 17](#_Toc165764998)

[2.1.5 *Kávézó* konfigurációja 19](#_Toc165764999)

[2.2 Üzemeltetők 20](#_Toc165765000)

[2.3 Motel 21](#_Toc165765001)

[2.4 Kávézó 24](#_Toc165765002)

[2.4.1 *EBED\_S* konfigurációja: 27](#_Toc165765003)

[2.4.2 *BAR\_S* konfigurációja: 28](#_Toc165765004)

[2.4.3 *IRODA\_S* konfigurációja: 29](#_Toc165765005)

[2.5 New York Hotel 30](#_Toc165765006)

[2.6 Otthoni dolgozó 33](#_Toc165765007)

[2.7 ISP 34](#_Toc165765008)

[2.7.1 ISP Konfigurációja: 35](#_Toc165765009)

[36](#_Toc165765010)

[3. Hálózat programozás 37](#_Toc165765011)

[4. Szerverek és felhőszolgáltatás 39](#_Toc165765012)

[4.1 Felvett felhasználók és belépési adatok területenként 43](#_Toc165765013)

# 1.Bevezetés

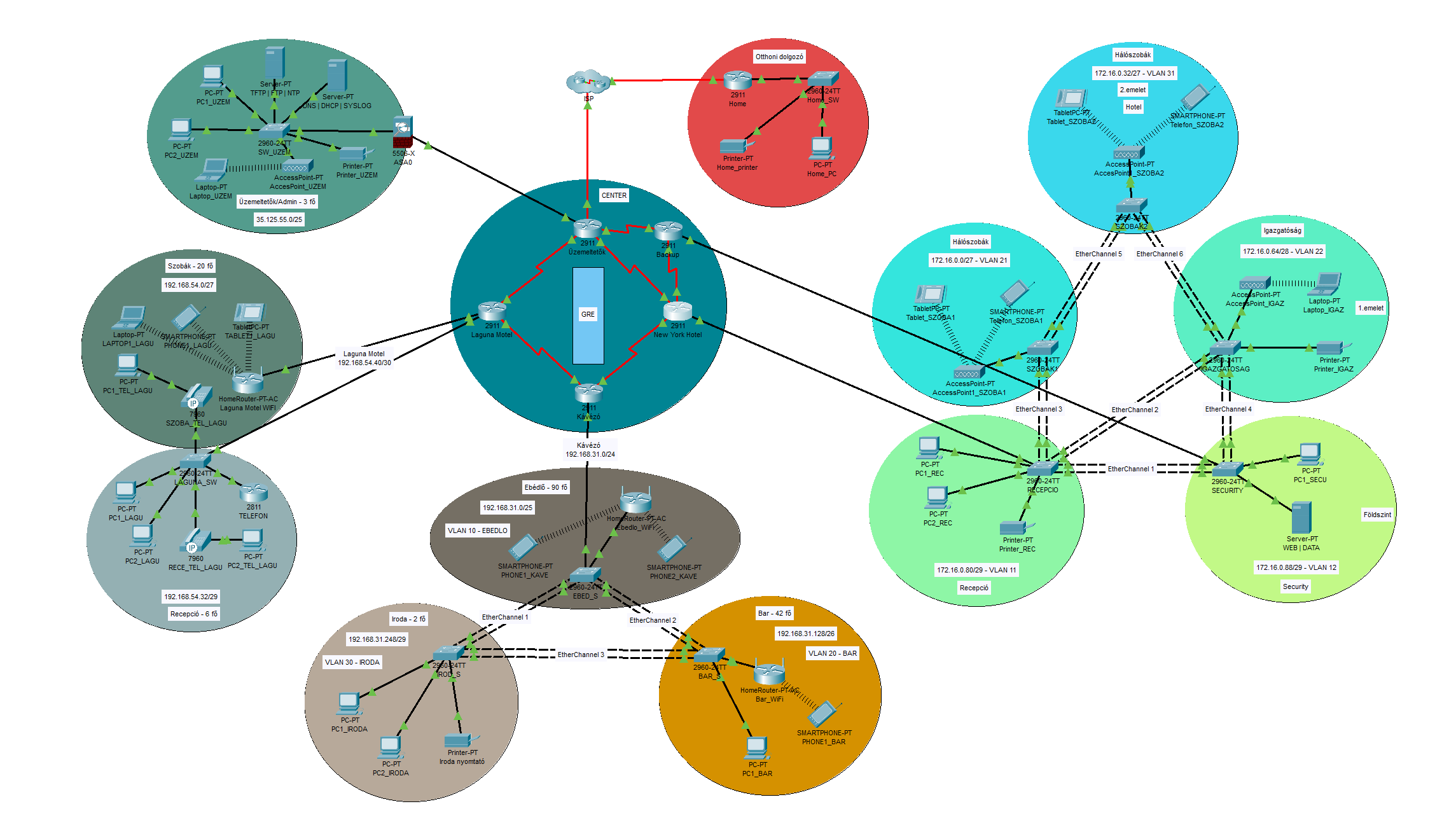
Ebben a dokumentációban látható a Linkwave Solutions cég által üzemeltett Hotel, Motel és az ezekhez tartozó kávézó topológiájának leírása és tesztelése. A cég dolgozói Görhöny Márk, Vanyek Máté és Vigh Zoltán, akik a hálózat zavartalan működéséért felelnek.

Körbejárjuk a topológia egyes részeit, felépítésüket, működésüket.

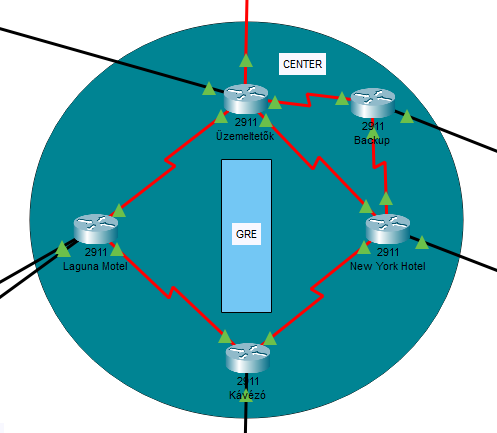
Külön részben kiemelve láthatjuk a hálózatban használt eszközöket;

* A szerveket, amelyek különféle funkciókat látnak el
* A programokat, amelyek a konfigurálásnál és karbantartásnál is segítenek.
* És szó esik a gyakorlatban alkalmazott IOT eszközről is.

# 2. Hálozat felépítése



## 2.1 Center



A **center** terület felel meg a **Hotel Komplexum** hálózat forgalomirányításáért. Az *„Üzemeltetők”* routeren, amelyen keresztül a forgalom kimegy a hálózatra alkalmaztunk **címfordítást**. A hálózati címfordítás *(NAT)* egy olyan technika, amely lehetővé teszi a privát IP-címek *(pl. 192.168.1.10)* leképezését nyilvános IP-címekre *(pl. 216.254.123.45)*. Ez azért hasznos, mert a **nyilvános IP-címek korlátozott** számban állnak rendelkezésre, míg a **privát IP-címekből korlátlan** számú létezhet. A NAT lehetővé teszi, hogy **több privát IP-című eszköz** is csatlakozzon az internethez **egyetlen nyilvános IP-cím** használatával. A NAT-nak 3 fő típusát különböztetjük meg amik a következők: Statikus -, Dinamikus NAT és Port Address Translation *(PAT)*. Utóbbi fontos számunkra, ugyanis mi a **PAT**-ot konfiguráltuk be a routeren. A PAT egy **speciális típusú dinamikus NAT**, amely egyetlen nyilvános IP-címet használ több privát IP-cím leképezéséhez. A PAT a forrásport száma alapján különbözteti meg a különböző privát IP-címeket.

**GRE Tunnelt** alkalmazunk az adatforgalom beágyazódásáért és a kapcsolat lebonyolítása érdekében, hogy a harmadik fél az egymás közti kulcsot ne tudja megsérteni. A GRE (*Generic Routing Encapsulation*) lehetővé teszi, hogy adatcsomagokat egy **másik protokollba ágyazzunk be**, és ezen protokoll hálózatán keresztül továbbítsuk őket. Ez a technika hasznos lehet a **VPN-ek, a tűzfalak áthidalása** és a különböző típusú hálózatok összekapcsolása terén. Példának okáért, a *PNETLab-ban* szimuláltuk, hogy a **„center”** területen IPv6-os címekkel dolgoztunk a 4 router között, viszont a **GRE Tunnel** IPv4-es címmel továbbítja az *„Üzemeltetőkből”* a *„Kávézóba”* a hálózati csomagokat.

A hálózatban egy területű **ospf** *(Open Shortest Path Frist)* **-et** konfiguráltunk annak érdekében, hogy a hálózat területei egymást közt tudjanak kommunikálni. Ez egy olyan útválasztási protokoll, amely az **IP-hálózatokon belül** működik a csomagok továbbításának legjobb útvonalainak meghatározásához. Az OSPF a *továbbítási protokollok* közé tartozik, ami azt jelenti, hogy a hálózat összes routere megosztja egymással a saját csatlakozásaival kapcsolatos információkat. Ez az információ lehetővé teszi az egyes routerek számára, hogy **dinamikusan** létrehozzanak egy **topológiai térképet** a **teljes hálózatról**. Az OSPF előnye a távolságvektoros protokollokkal [például *RIP (Routing Information Protocol)*] szemben, hogy **gyorsabban konvergál**, azaz gyorsabban tud alkalmazkodni a hálózati változásokhoz. Ez azért van, mert az OSPF minden router *rendelkezik a teljes hálózati topológia ismeretével,* míg a távolságvektoros protokollok csak a szomszédos routerektől kapott információkra támaszkodnak. Az *„Üzemeltetők”*, illetve a *„Laguna Motel”* routert ezen felül **OSPFv3** funkcióval is ellátuk. Ez az IPv6-os címek továbbítása szolgál.

A *„Hotel”* felé telepítettük a **Backup** routert, amely **HSRP** protokollal működik. A HSRP (*Hot Standby Router Protocol)* a Cisco által kifejlesztett, első ugrás *(first hop)* redundanciát biztosító protokoll, amely IPv4-es hálózatokban használható. A HSRP célja, hogy automatikusan **átvegye az alapértelmezett átjáró szerepét** egy meghibásodott forgalomirányítótól. Ez biztosítja a hálózat folyamatos működését, és minimalizálja a kiesési időt. A mi topológiánkban a *New York Hotel* az **aktív** forgalomírányító míg a *Backup* **designated** forgalomírányítoként üzemel, amely átveszi az aktív szerepet, ha az **aktív** forgalomírányítóval valami meghibásodás lenne.

Annak érdekében, hogy az internet szolgáltatást bárhonnan el lehessen érni a hálózaton belül, az „*Üzemeltetők”* router-én biztosítottunk egy **alapértelmezett statikus routolást** mindkét végen.

A **CHAP** a **PPP** *(Point-to-Point Protocol)* protokoll egy kiterjesztése, amelyet a routerek közötti hitelesítéshez használnak. Ez egy biztonságosabb alternatíva a régebbi **PAP** *(Password Authentication Protocol)* protokollal szemben, mivel nem továbbítja a jelszavakat nyílt szöveges formában. Ezt ahitelesítést a *„center”* hálózaton belül végeztünk minden router közt, ahol a **felhasználónevet „Uzemeltetok”** -re a **jelszavat** pedig **„cisco” -**ra állítottuk.

Az „*Üzemeltetők”* hálózatához csatlakozó felhasználók számára egy olyan ACL *(Access Control List)* konfiguráltunk, amely **megakadályozza** a bejövő **pingeléseket** a területen lévő **szerverek felé**, ugyanakkor **lehetővé teszi a kimenő** forgalmat, azaz a felhasználók elérhetik a szolgáltatásokat, és bármilyen külső forrásból elérhetőek maradnak.

### 2.1.1 *Üzemeltetők* konfigurációja

**Hostname:**

hostname Uzemeltetok

**Static route:**

ip route 0.0.0.0 0.0.0.0 gig0/0/0

**OSPF**

router ospf 1

router-id 1.1.1.1

passive-interface gig0/0

passive-interface gig0/0/0

network 35.125.55.0 0.0.0.127 area 0

network 100.100.100.28 0.0.0.3 area 0

network 100.100.100.16 0.0.0.3 area 0

network 100.100.100.20 0.0.0.3 area 0

default-information originate

**OSPFv3**

ipv6 router ospf 2

passive-interface gig0/0

passive-interface gig0/0/0

default-information originate

int gig0/0

ipv6 ospf 2 area 0

int se0/1/0

ipv6 ospf 2 area 0

**PPP**

int se0/1/0

encap ppp

ppp authentication chap

exit

username Laguna secret cisco

**GRE**

int t1

ip address 200.200.200.1 255.255.255.252

tunnel source se0/1/0

tunnel destination 100.100.100.22

**ACL**

ip access-list extended noping

deny icmp any host 35.125.55.126 echo

deny icmp any host 35.125.55.125 echo

deny icmp any host 35.125.55.124 echo

deny icmp any host 35.125.55.123 echo

int g0/0

ip access-group noping out

**PAT**

int gig0/0

ip nat inside

int se0/1/0

ip nat inside

int se0/1/1

ip nat inside

int se0/2/0

ip nat inside

int gig0/0/0

ip nat outside

ip access-list standard 60

permit 35.125.55.0 0.0.0.127

permit 192.168.54.0 0.0.0.31

permit 192.168.54.32 0.0.0.7

permit 192.168.31.0 0.0.0.127

permit 192.168.31.248 0.0.0.7

permit 192.168.31.128 0.0.0.63

permit 172.16.0.80 0.0.0.7

permit 172.16.0.88 0.0.0.7

permit 172.16.0.0 0.0.0.31

permit 172.16.0.64 0.0.0.15

permit 172.16.0.32 0.0.0.31

ip nat pool PATPOOL1 50.50.50.50 50.50.50.50 netmask 255.255.255.0

ip nat inside source list 60 pool PATPOOL1 overload

**NTP/SYSLOG**

logging 35.125.55.126

ntp server 35.125.55.123

service timestamps log datetime msec

ntp update-calendar

**IPv6**

ipv6 unicast-routing

int gig0/0

ipv6 enable

ipv6 address 2001:A1A1:B1B1:C1C1::/64

ipv6 address FE80::1 link-local

int se0/1/0

ipv6 enable

ipv6 address 2001:A3A3:B3B3:C3C3::/64

ipv6 address FE80::1 link-local

### 2.1.2 *New York Hotel* konfigurációja

**Hostname:**

hostname NewYorkHotel

**Interface gig0/0.11**

encapsulation dot1q 11

ip add 172.16.0.81 255.255.255.248

**Interface gig0/0.12**

encapsulation dot1q 12

ip add 172.16.0.89 255.255.255.248

**Interface gig0/0.21**

encapsulation dot1q 21

ip add 172.16.0.1 255.255.255.224

**Interface gig0/0.22**

encapsulation dot1q 22

ip add 172.16.0.65 255.255.255.248

**Interface gig0/0.31**

encapsulation dot1q 31

ip add 172.16.0.33 255.255.255.224

**Interface gig0/0**

no sh

**Router OSPF 1:**

router-id 2.2.2.2

passive-inerface gig0/0

passive-inerface gig0/0.11

passive-inerface gig0/0.12

passive-inerface gig0/0.21

passive-inerface gig0/0.22

passive-inerface gig0/0.31

network 172.16.0.0 0.0.0.31 area 0

network 172.16.0.32 0.0.0.31 area 0

network 172.16.0.64 0.0.0.7 area 0

network 172.16.0.80 0.0.0.7 area 0

network 172.16.0.88 0.0.0.7 area 0

network 100.100.100.28 0.0.0.3 area 0

**HSRP**

int g0/0.11

standby ver 2

standby 11 ip 172.16.0.86

standby 11 priority 150

standby 11 preempt

int g0/0.12

standby ver 2

standby 12 ip 172.16.0.94

standby 12 priority 150

standby 12 preempt

int g0/0.21

standby ver 2

standby 21 ip 172.16.0.30

standby 21 priority 150

standby 21 preempt

int g0/0.22

standby ver 2

standby 22 ip 172.16.0.78

standby 22 priority 150

standby 22 preempt

int g0/0.31

standby ver 2

standby 31 ip 172.16.0.62

standby 31 priority 150

standby 31 preempt

**NTP/SYSLOG**

logging 35.125.55.126

ntp server 35.125.55.123

service timestamps log datetime msec

ntp update-calendar

**DHCP**

ip dhcp pool VLAN21

network 172.16.0.0 255.255.255.224

default-router 172.16.0.30

ip dhcp pool VLAN31

network 172.16.0.32 255.255.255.224

default-router 172.16.0.62

ip dhcp excluded-address 172.16.0.81

ip dhcp excluded-address 172.16.0.89

ip dhcp excluded-address 172.16.0.1

ip dhcp excluded-address 172.16.0.2

ip dhcp excluded-address 172.16.0.82

ip dhcp excluded-address 172.16.0.90

ip dhcp excluded-address 172.16.0.33

ip dhcp excluded-address 172.16.0.34

ip dhcp excluded-address 172.16.0.65

ip dhcp excluded-address 172.16.0.66

ip dhcp excluded-address 172.16.0.86

ip dhcp excluded-address 172.16.0.94

ip dhcp excluded-address 172.16.0.30

ip dhcp excluded-address 172.16.0.62

ip dhcp excluded-address 172.16.0.78

### 2.1.3 *Backup* konfigurációja

**Hostname:**

hostname Backup

**VLAN:**

interface gig0/0.11

encapsulation dot1q 11

ip add 172.16.0.81 255.255.255.248

interface gig0/0.12

encapsulation dot1q 12

ip add 172.16.0.89 255.255.255.248

interface gig0/0.21

encapsulation dot1q 21

ip add 172.16.0.1 255.255.255.224

interface gig0/0.22

encapsulation dot1q 22

ip add 172.16.0.65 255.255.255.248

interface gig0/0.31

encapsulation dot1q 31

ip add 172.16.0.33 255.255.255.224

interface gig0/0

no sh

**Static route:**

ip route 0.0.0.0 0.0.0.0 gig0/2/0

**NTP/SYSLOG:**

logging 35.125.55.126

ntp server 35.125.55.123

service timestamps log datetime msec

ntp update-calendar

**OSPF:**

router ospf 1

router-id 5.5.5.5

network 100.100.100.36 0.0.0.3 area 0

network 100.100.100.32 0.0.0.3 area 0

network 100.100.100.40 0.0.0.3 area 0

network 172.16.0.0 0.0.0.31 area 0

network 172.16.0.32 0.0.0.31 area 0

network 172.16.0.64 0.0.0.7 area 0

network 172.16.0.80 0.0.0.7 area 0

network 172.16.0.88 0.0.0.7 area 0

network 100.100.100.28 0.0.0.3 area 0

network 100.100.100.20 0.0.0.3 area 0

passive-interface gig0/0

passive-interface gig0/0.11

passive-interface gig0/0.12

passive-interface gig0/0.21

passive-interface gig0/0.22

passive-interface gig0/0.31

passive-interface gig0/2/0

default-information originate

**HSRP:**

int g0/0.11

standby ver 2

standby 11 ip 172.16.0.86

int g0/0.12

standby ver 2

standby 12 ip 172.16.0.94

int g0/0.21

standby ver 2

standby 21 ip 172.16.0.30

int g0/0.22

standby ver 2

standby 22 ip 172.16.0.78

int g0/0.31

standby ver 2

standby 31 ip 172.16.0.62

**DHCP:**

ip dhcp pool VLAN21

network 172.16.0.0 255.255.255.224

default-router 172.16.0.30

ip dhcp pool VLAN31

network 172.16.0.32 255.255.255.224

default-router 172.16.0.62

ip dhcp excluded-address 172.16.0.81

ip dhcp excluded-address 172.16.0.89

ip dhcp excluded-address 172.16.0.1

ip dhcp excluded-address 172.16.0.2

ip dhcp excluded-address 172.16.0.82

ip dhcp excluded-address 172.16.0.90

ip dhcp excluded-address 172.16.0.33

ip dhcp excluded-address 172.16.0.34

ip dhcp excluded-address 172.16.0.65

ip dhcp excluded-address 172.16.0.66

ip dhcp excluded-address 172.16.0.86

ip dhcp excluded-address 172.16.0.94

ip dhcp excluded-address 172.16.0.30

ip dhcp excluded-address 172.16.0.62

ip dhcp excluded-address 172.16.0.78

**PAT:**

int gig0/2/0

ip nat outside

int gig0/0

ip nat inside

int se0/1/0

ip nat inside

int se0/0/0

ip nat inside

ip access-list standard 60

permit 35.125.55.0 0.0.0.127

permit 192.168.54.0 0.0.0.31

permit 192.168.54.32 0.0.0.7

permit 192.168.31.0 0.0.0.127

permit 192.168.31.248 0.0.0.7

permit 192.168.31.128 0.0.0.63

permit 172.16.0.80 0.0.0.7

permit 172.16.0.88 0.0.0.7

permit 172.16.0.0 0.0.0.31

permit 172.16.0.64 0.0.0.15

permit 172.16.0.32 0.0.0.31

ip nat pool PATPOOL2 51.51.51.51 51.51.51.51 netmask 255.255.255.0

ip nat inside source list 60 pool PATPOOL2 overload

### 2.1.4 *Laguna Motel* konfigurációja

**Hostname:**

hostname LagunaMotel

**OSPF:**

router ospf 1

router-id 4.4.4.4

passive-interface gig0/0

passive-interface gig0/1

network 192.168.54.40 0.0.0.3 area 0

network 192.168.54.32 0.0.0.7 area 0

network 100.100.100.16 0.0.0.3 area 0

network 100.100.100.12 0.0.0.3 area 0

**OSPFv3:**

ipv6 router ospf 2

router-id 4.4.4.4

passive-interface gig0/0

passive-interface gig0/1

int gig0/1

ipv6 ospf 2 area 0

int se0/0/0

ipv6 ospf 2 area 0

**PPP:**

int se0/0/0

encap ppp

ppp authentication chap

exit

username Uzemeltetok secret cisco

**NTP/SYSLOG:**

logging 35.125.55.126

ntp server 35.125.55.123

service timestamps log datetime msec

ntp update-calendar

**IPv6:**

ipv6 unicast-routing

int range gig0/0-1

ipv6 enable

int gig0/1

ipv6 address 2001:A2A2:B2B2:C2C2::/64

ipv6 address FE80::1 link-local

int se0/0/0

ipv6 enable

ipv6 address 2001:A3A3:B3B3:C3C3::1/64

ipv6 address FE80::1 link-local

### 2.1.5 *Kávézó* konfigurációja

**Hostname:**

hostname kavezo

**VLAN:**

int gig0/0.10

encap dot1q 10

ip add 192.168.31.1 255.255.255.128

int gig0/0.20

encap dot1q 20

ip add 192.168.31.129 255.255.255.192

int gig0/0.30

encap dot1q 30

ip add 192.168.31.193 255.255.255.248

**OSPF:**

router ospf 1

router-id 3.3.3.3

passive-interface gig0/0

network 192.168.31.0 0.0.0.127 area 0

network 192.168.31.128 0.0.0.63 area 0

network 192.168.31.192 0.0.0.7 area 0

network 100.100.100.12 0.0.0.3 area 0

network 100.100.100.20 0.0.0.3 area 0

**GRE:**

int t1

ip address 200.200.200.2 255.255.255.252

tunnel source se0/0/1

tunnel destination 100.100.100.18

**NTP/SYSLOG:**

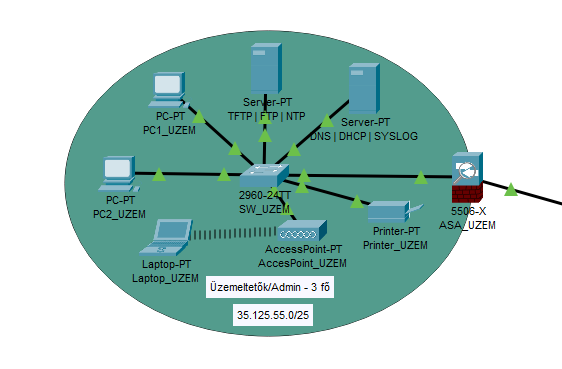
logging 35.125.55.126

ntp server 35.125.55.123

service timestamps log datetime msec

ntp update-calendar

## 2.2 Üzemeltetők



Az **üzemeltetők/admin** területen találhatóak meg a hálózat működésének legmérvadóbb szolgáltatásai. Ez működteti a felhasználók között az dns, web, FTP és Tftp szolgáltatásokat, amelyeken keresztül a hotel komplexum a saját weboldalát érik el.

Ezeken felül egy megosztott nyomtató is található a hivatalos dokumentumok előállítása érdekében.

Biztonság tekintetében **SYSLOG** szerveren monitorozzuk és naplózzuk az eseményeket a hálózatban, így könnyen detektálhatjuk, hogy a sértés melyik irányból jött és mikor.

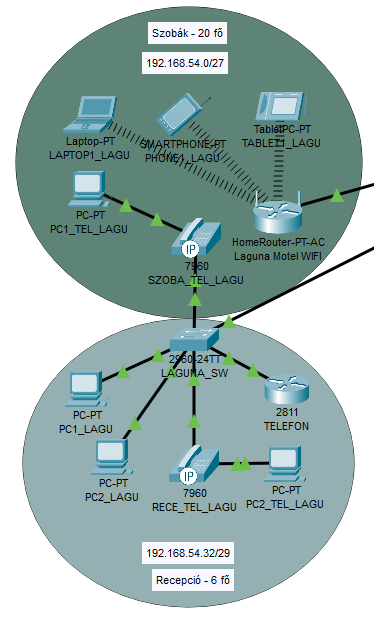
Ezen a területen egy **Cisco Adaptive Security Applience** *(ASA)* hardveres tűzfal biztosítja a védelmet az itt található érzékeny adatok számára.

DNS cím: **lwsolutions.hu**

TFTP-FTP-NTP szerver ip: 35.125.55.123

DHCP-DNS-SYSLOG szerver ip: 35.125.55.126

## 2.3 Motel

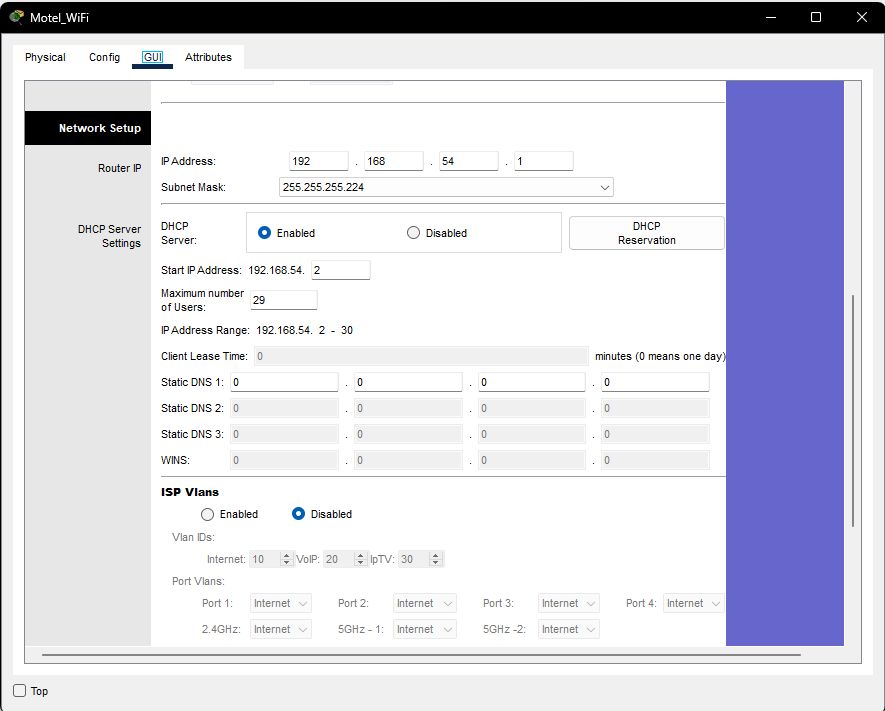
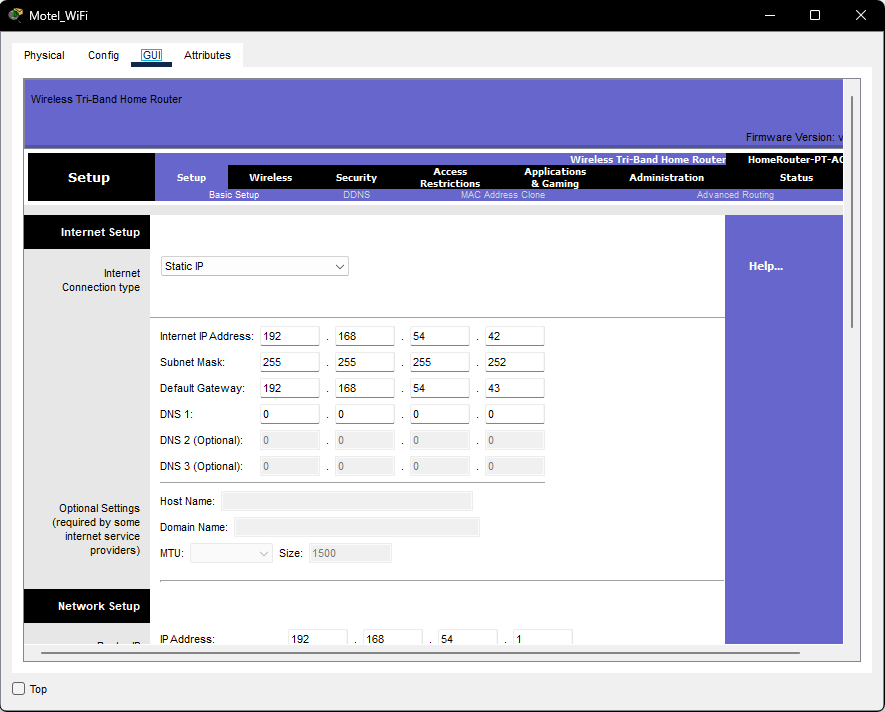


Ezen a területen IPv4 és IPv6-os címek egyaránt megtalálhatóak a hálózat korszerű kialakításából eredően.

A **SOHO** router **Motelen** belüli vendégeknek fenntartott vezetéknélküli hálózatot biztosít, *WPA2-PSK* titkosítással ellátva, ezáltal biztosítja azt, hogy más ne férhessen hozzá a belső hálózathoz és generáljon fölösleges forgalmat a megfelelő belépési adatok hiányában.

Az SSID **Laguna\_Motel\_WiFi,** a jelszó pedig **Laguna123** *AES* titkosítású.

Statikusan kapta a SOHO router az IP-címét (**192.168.54.42/30**), a dinamikusan kiosztott címként pedig a felhasználók **192.168.54.1/24**-es címeket kapják meg max .5-es címmel kezdve max 29 főnek.



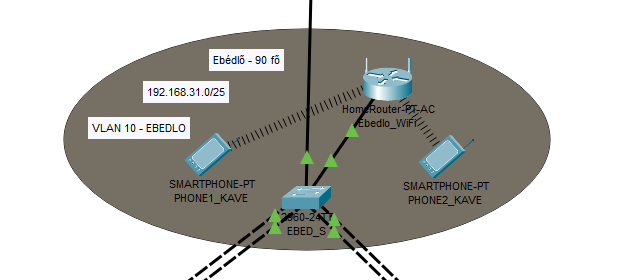
A képen szöveg, képernyőkép, szoftver, Számítógépes ikon látható

Automatikusan generált leírás

A képen szöveg, képernyőkép, szoftver, Számítógépes ikon látható

Automatikusan generált leírás

## 2.4 Kávézó



Az **Ebédlő** terültet a VLAN 10-be helyeztük el elkülönítve a VLAN 20 és 30-tól. A VLAN-ba 90 személyt tettünk be, akik a területen tartózkodhatnak és kaphatnak IP címet DHCP szolgáltatás segítségével. Mindezt pedig az **EBED\_S**-hez kötöttük.

A kapcsolón belül az STP (**Spanning Tree Protocol**), illetve VTP (**VLAN Trunk Protocol**) protokollt konfiguráltuk. A VTP protokoll azt biztosítja számunkra, hogy a VLAN konfiguráció a teljes hálózat területén egységes. Az STP-n belül a **rapid-spanning tree** protokollt használtuk, mivel a második rétegbeli hurkok megelőzésére preferált protokoll és aktívan képes megerősíteni, hogy egy port biztonságosan továbbító állapotba kerülhet, nem hagyatkozik időzítőkre.

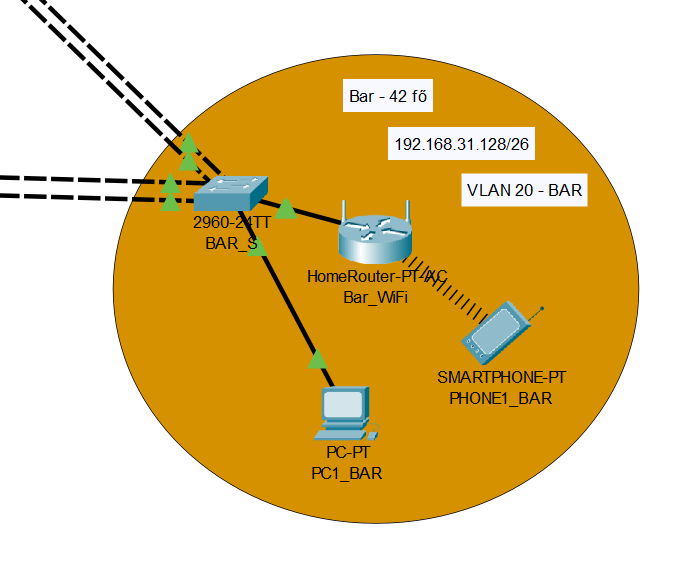
A VTP konfigurációban a következőket ejtettük meg. Az **EBED\_S** lett a szerver switch, amely a kliensekre (**BAR\_S**, **IRODA\_S**) fogja küldeni a VLAN információkat. Domain névnek a „*kavezo*” -t adtunk, jelszónak pedig a „*kave123*” -at. A verziót pedig átkapcsoltuk 2-esre.

A router felé néző interfészekre a *switchport access* mellett megadtuk a *spanning-tree portfast*, és *spanning-tree bpduguard enable* parancsokat. A portfast parancs kiadásánál zökkenőmentessé teszi az STP-ről az RSTP-re váltást. A bpduguard pedig egy úgymond életben tartó mechanizmusként működik, ami 2 másodpercenként küldi ki a “*Hello*” csomagokat. Három egymás utáni BPDU kimaradása után megszakítja a szomszéddal a kapcsolatot. Az információt a viszonylag gyors elévülése miatt nagyon hamar észlelhetők a hibák a hálózaton belül.

Minden kapcsolón megadtunk egy hídazonosítót. Ez a hídazonosító az adott VLAN száma. Ezért az **EBED\_S** kapcsolón a *spanning-tree vlan vlan-szám root primary* a 10,20 és 30 VLAN számot kapta.

**IROD\_S** és **BAR\_S** kapcsolók irányába az interfészeket **PAgP** port összefogással kapcsoltuk össze. Majd őket az int port-channel channel-group szám paranccsal trunk állapotba kapcsoltuk, így a VLAN-ok a kapcsolókon keresztül tudnak kommunikálni. Az **EBED\_S** interfészeken az desirable állapotot állítottuk be mindkét irány felé.

A kapcsolón a védelem értelmében portbiztonságot (port-security-t) alkalmaztunk, amivel a belépő és sértő felhasználók esetén megtagadjuk a hálózati hozzáférést azzal, hogy az adott portot azonnal lekapcsoljuk (restrict állapot – *switchport port-security violation restrict*), és egy syslog üzenetet küld a konzolnak/syslog szervernek. Így látva, hogy mikor, és hol történt a sértés.

Ezenfelül korlátoztuk az engedélyezett mac-címek számát (*switchport port-security mac-address <szám>, switchport port-security max <szám>, switchport port-security mac-address sticky*).

A **Bar** területet a VLAN 20-be helyeztük el elkülönítve a VLAN 10 és 30-tól. A VLAN-ba 42 személyt tettünk be, akik a területen tartózkodhatnak és kaphatnak IP címet DHCP szolgáltatás segítségével. Mindezt pedig a **BAR\_S**-hez kötöttük.

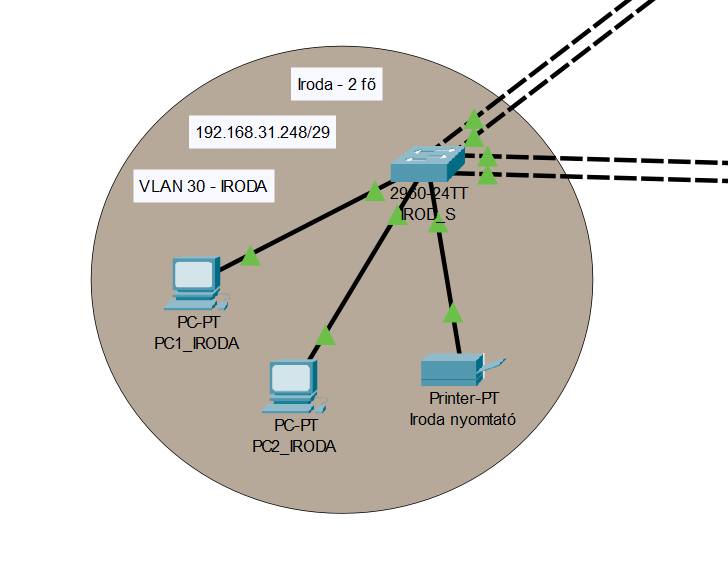
Itt a VTP beállítás annyiban különbözik, hogy ez már egy kliens switch lett. Ez azt fogja eredményezni, hogy ha a megfelelő domain és jelsző kombinációt beírjuk, akkor a szerver switchről (**EBED\_S**), automatikusan megkapja a VLAN információkat.

A kapcsolón belül szintén ugyanazt az STP protokollt konfiguráltuk, mint az **EBED\_S** kapcsolón. A *secondary root* a VLAN 10, 20, 30.

A gép, illetve a SOHO Router felé néző interfészekre úgyszint a *switchport access* mellett megadtuk a *spanning-tree portfast*, és *spanning-tree bpduguard enable* parancsokat.

**PAgP** tekintetében az **EBED\_S** kapcsoló irányába a saját oldalát, valamint az **IRODA\_S** kapcsoló irányába újonnan külön létrehozott etherchannel állapotát *desirable*-ra állítottuk, majd pedig a kapcsolatot *trunk* állapotra kapcsoltuk.

Végezetül az **Iroda** területünk az **IRODA\_S** kapcsolójának konfigurációja nem sokkal tér el az előzőektől.



### 2.4.1 *EBED\_S* konfigurációja:

**VLAN-ok:**

vlan 10

name EBEDLO

vlan 20

name BAR

vlan 30

name IRODA

int gig0/1

sw mo trunk

int range fa0/1-6

sw mo trunk

**VTP:**

vtp mode server

vtp domain kavezo

vtp password kave123

vtp version 2

**Portvédelem:**

int range f0/5-24

sh

int range gig0/1-2, f0/1-4

switchport port-security mac-address sticky

switchport port-security violation restrict

switchport port-security maximum 1

**PortösszeFOGÁS:**

int range f0/1-2

channel-group 1 mode desirable

int range f0/3-4

channel-group 2 mode desirable

**Feszítőfa:**

spanning-tree mode rapid-pvst

spanning-tree vlan 10,20,30 root primary

int gig0/2

spanning-tree portfast

spanning-tree bpduguard enable

### 2.4.2 *BAR\_S* konfigurációja:

**VTP:**

int range fa0/1-6

sw mo trunk

vtp mode client

vtp domain kavezo

vtp password kave123

**VLAN:**

int range fa0/2

sw mode acc

sw acc vlan 20

**Portvédelem:**

int range f0/1, f0/7-24, gig0/1

sh

int range f0/2-6, gig0/2

switchport port-security mac-address sticky

switchport port-security violation restrict

switchport port-security maximum 1

**ETHERCHANNEL:**

int range f0/3-4

channel-group 2 mode desirable

int range f0/5-6

channel-group 3 mode desirable

**Feszítőfa:**

spanning-tree mode rapid-pvst

int range gig0/2, f0/2

spanning-tree portfast

spanning-tree bpduguard enable

### 2.4.3 *IRODA\_S* konfigurációja:

**VTP:**

int range fa0/1-6

sw mo trunk

vtp mode client

vtp domain kavezo

vtp password kave123

**VLAN:**

int range fa0/3-4, fa0/24

sw mode acc

sw acc vlan 30

**Portvédelem:**

int range f0/7-23

sh

int range f0/1-6, f0/24

switchport port-security mac-address sticky

switchport port-security violation restrict

switchport port-security maximum 1

**ETHERCHANNEL:**

int range f0/1-2

channel-group 1 mode desirable

int range f0/5-6

channel-group 3 mode desirable

**Feszítőfa:**

spanning-tree mode rapid-pvst

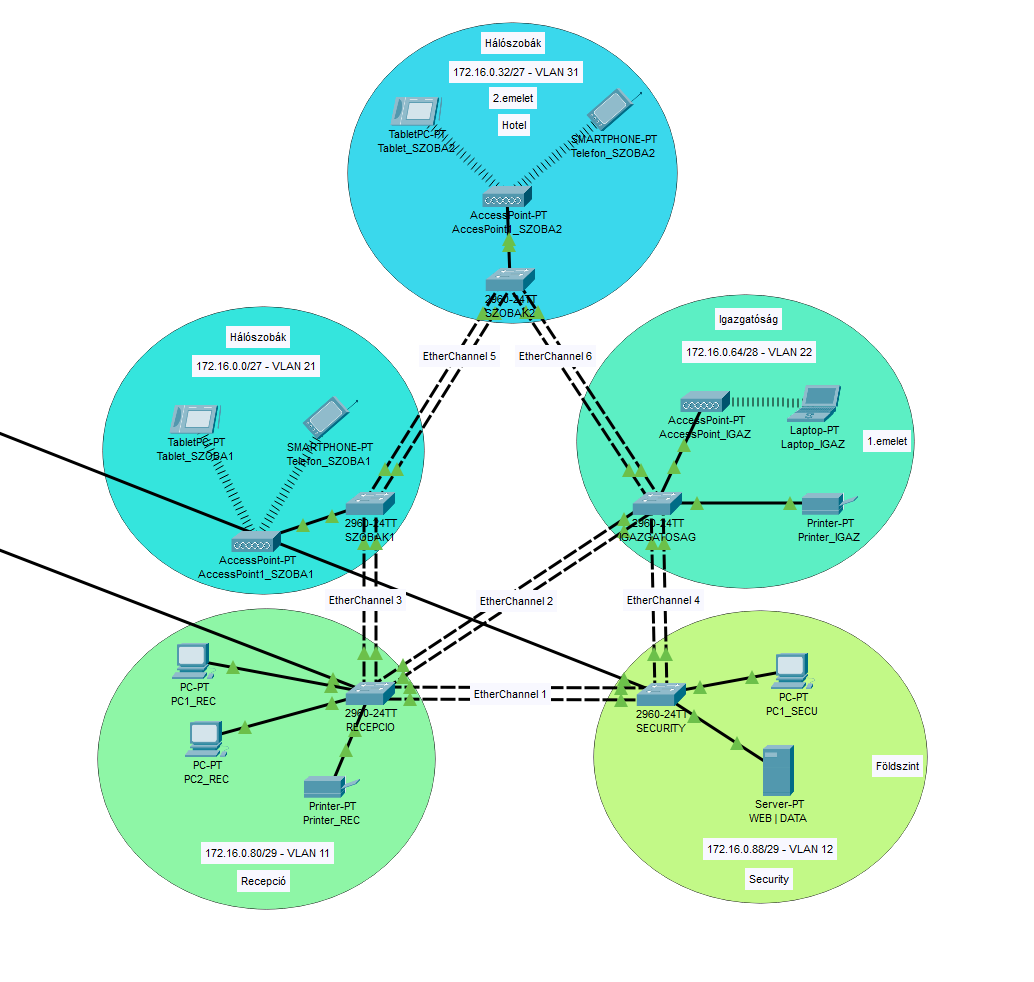
spanning-tree vlan 10,20,30 root secondary

int range f0/3-4, f0/24

spanning-tree portfast

spanning-tree bpduguard enable

## 2.5 New York Hotel



A hotel hálózati felépítése nagyjából a kávézó alapjaira épül annyi különbséggel, hogy itt egy sokkal nagyobb mennyiségű felhasználóval dolgoztunk, illetve a hálózat biztonságra nagyobb hangsúlyt fektettünk. Több különféle protokollt alkalmaztunk, amely a hálózat redundáns működéséhez nagyban hozzájárul.

Az egyik legfontosabb funkció a hotel hálózatában, hogy egy ***BACKUP*** routert elhelyeztük HSRP protokollal ellátva. A **HSRP** *(Hot Standby Router Protocol)* egy Cisco fejlesztésű protokoll, ami redundáns alapértelmezett átjárót biztosít a hálózat számára.

A HSRP lehetővé teszi, hogy két vagy több router közül mindig legyen egy aktív, amely továbbítja a forgalmat. Ha az aktív router meghibásodik, a másik router automatikusan átveszi a feladatát, így a vendégek nem érzékelik a kiesést.

Itt is alkalmaztunk *VLAN*-okat, amiket 5 fő részre lehet bontani. **VLAN 11, 12, 21, 22, 31.** Az első szám az emelet számát indikálja, a második pedig a szobát. Fontos kiemelni, hogy a *VLAN*-ok egymástól elkülönítve vannak jelen.

*VLAN 11:* Recepció *VLAN 12:* Security  *VLAN 21:* Hálószobák (itt a 2. emeleten lévő összes hálószoba van) *VLAN 22:* Igazgatóság *VLAN 31:* Hálószobák (itt a 3. emeleten lévő összes hálószoba van)

A switchek között a redundancia érdekében itt is alkalmaztunk 2. rétegbeli protokolokat, amik a **Spanning-tree**, **EtherChannel és VTP.**

Minden *switch* között megtalálható **PAgP** (*Port Aggregation Protocol*)**,** amely lehetővé teszi, hogy több fizikai portot összevonjunk egyetlen logikai porttá. Ez a technológia növeli a sávszélességet és a redundanciát a switchek között. A portösszefogás működése során a switchek trunköket hoznak létre, amelyek több fizikai portból állnak. A trunkökben lévő portokat úgy konfiguráltuk, hogy együttműködjenek, és egyetlen logikai portként viselkedjenek. Ez azt jelenti, hogy a forgalom a trunkben lévő összes porton eloszlik.

A *Recepció*, a *Security* és az *Igazgatóság* között **Spanning-tree** (*feszítőfa*) protokollt is konfiguráltunk. Ez megakadályozza, hogy ne legyen üzenetszórási vihar, ha egymással kommunikálnának az eszközök. A hálózatban kiválaszt egy gyökérponti hidat, amelyhez minden switch egy útvonalon csatlakozik, a többi switch portjai közül néhányat lezár, hogy azok ne továbbítsanak forgalmat, de ha egy útvonal meghibásodik, akkor automatikusan átkapcsolja a forgalmat egy másik útvonalra.

A VLAN-ok switcheken történő biztos és egységesen frissülő konfigurációja érdekében a **VTP** (*VLAN Trunking Protocol*) protokollt alkalmaztuk. Ez egy olyan szabványosított hálózati protokoll, amelyet a Cisco rendszerek használnak a Virtuális LAN-ok (*VLAN-ok*) konfigurációjának automatikus terjesztésére és karbantartására egy Ethernet hálózaton belül. A VTP célja a hálózati adminisztráció egyszerűsítése és a konzisztencia biztosítása a VLAN konfigurációk között. **VTP szervernek** a *Recepción* lévő switchetállítottuk be, az épületben található többi eszköz *Client módban* üzemel, amik a *„NYHOTEL”* domain névvel, illetve a *„NYHOTEL”* jelszóval csatlakoznak a szerver switchhez és figyelik a változtatásokat.

A hotel egész területén **DHCP** segítségével dinamikusan IP címeket osztunk, mely segít az új eszközök beállításában a hálózatban, hiszen elég rácsatlakozniuk a hálózatra és a megfelelő helyről és a megfelelő VLAN IP tartományból már kap is IP-címet, illetve takarékoskodik az IP címekkel, mert csak akkor használ egy IP-t egy adott PC amikor hozzá van csatlakozva.

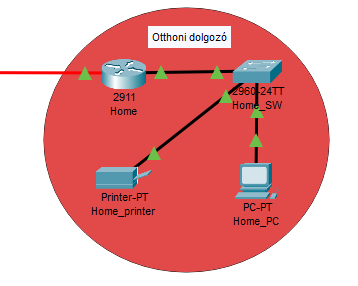
A könnyű kommunikáció érdekében **IP telefonokat** helyeztünk el az összes szobában, illetve a 3 fő szobában, ami a *Recepció*, a *Security* és az *Igazgatóság*. Ezek azt a célt szolgálják, hogy az épületen belül direktbe el tudnak érni egyes szolgáltatásokat a vendégek a hálószobákból, a többi helyiségben pedig a kollegák tudják megkeresni egymást.

A *Security*-ben található meg a hotel **helyi WEB és DATA szervere**, amin fut a weboldal, illetve tárolva vannak foglalások/vendégek adatai. A legnagyobb biztonság érdekében ehhez csak adott emberek férhetnek hozzá fizikálisan, illetve különféle tűzfalas beállítások biztosítják a szerveren a maximális védelmet. Ebből a helyiségből monitorozhatóak a hotelben megtalálható biztonsági kamerák is.

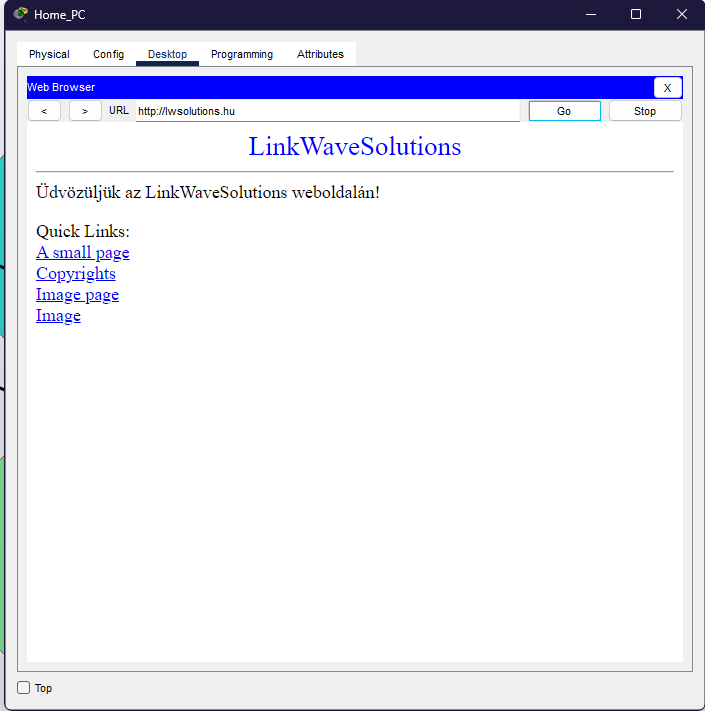
Annak érdekében, hogy a vezeték nélküli kapcsolat az épületen belül megbízható legyen és biztosan bírja a terhelést az emeletekre különálló **Access Pointokat** helyeztünk el, amelyeket *DHCP* segítségével dinamikusan osztanak IP címet az eszközöknek.

Több fizikai **fix és mobil eszközt** is elhelyeztünk a topológián, hogy szemléltessük ezeknek elhelyezkedését, illetve azt, hogy hol lesznek ezek használatban. A **hálózati nyomtatókat** a bármelyik dolgozó el tudja érni a megfelelő felhasználóval belépve.

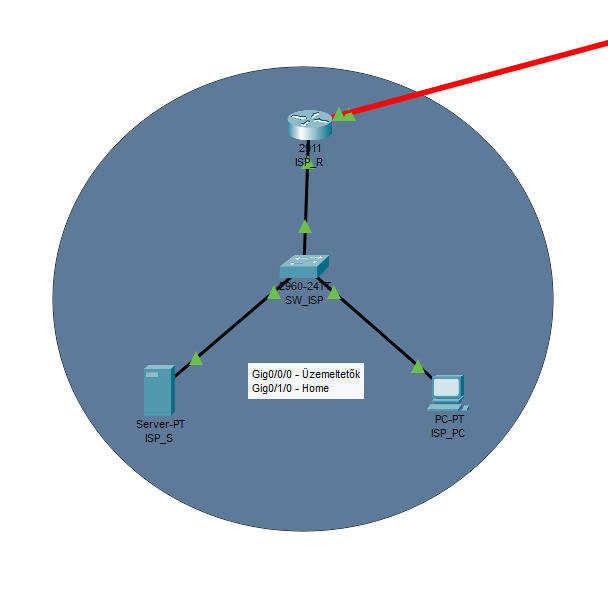
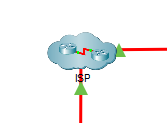
## 2.6 Otthoni dolgozó



Az otthoni dolgozó lényegében a *„Hotel”* dokumentálási és foglalási ügyeit tudja távolról könnyedén intézni. A Hotel weboldalát elérni, amire egy speciális jogosultságokkal rendelkező felhasználóval be tud lépni. Egy nyomtatót is elhelyeztünk annak érdekében, hogyha esetleg valami fontos dokumentumot kellene aláírni.



## 2.7 ISP



Ezen a részen szimuláltuk le az internetszolgáltatót. A területet dns szerverrel láttuk el, a kapcsolat tesztelésének érdekében.

ACL segítségével a felhasználók csak a weboldalt érik el, pingelni viszont nem képesek. A saját hálózatbeli kliens pedig a hálózaton belül csak az **Admin** szervereket éri el.

A **center** felé szintén statikus route-tal kommunikál és ezt úgynevezett *„clusterbe”* helyeztük el.

### 2.7.1 ISP Konfigurációja:

**Hostname**

hostname ISP\_R

**Interface GIG0/0**

ip address 100.100.100.1 255.255.255.248

**Interface GIG0/0/0**

ip address 100.100.100.25 255.255.255.252

**Interface GIG0/1/0**

ip address 100.100.100.9 255.255.255.252

**Static route**

ip route 50.50.50.0 255.255.255.0 100.100.100.26

ip route 51.51.51.0 255.255.255.0 100.100.100.41

ip route 60.60.60.0 255.255.255.0 100.100.100.10

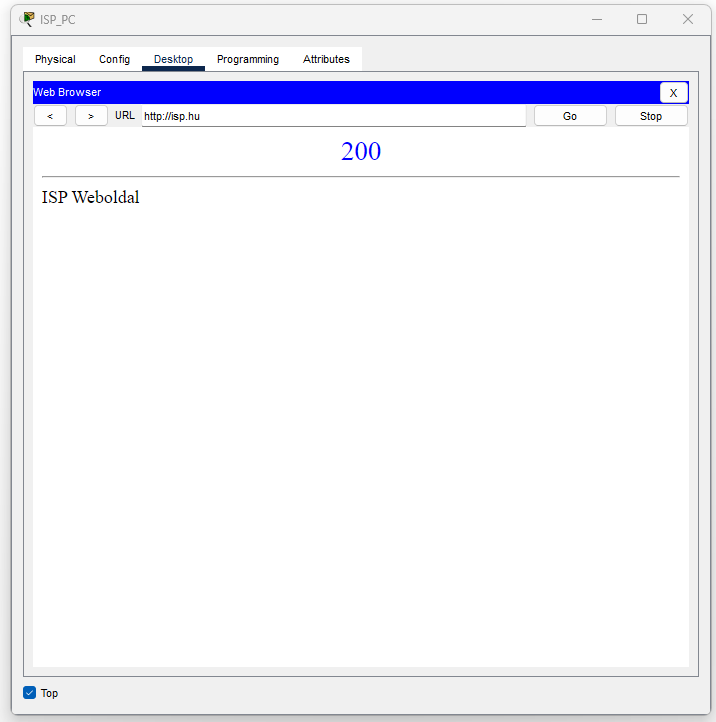
ip route 70.70.70.0 255.255.255.0 g0/0/0

ip route 61.61.61.0 255.255.255.0 100.100.100.10

A képen szöveg, képernyőkép, képernyő, szoftver látható

Automatikusan generált leírás

# 



# 3. Hálózat programozás

*import time*

*from netmiko import ConnectHandler*

*router\_parameter ={*

*'device\_type': 'cisco\_ios',*

*'host': '192.168.14.134',*

*'username': 'admin',*

*'password': 'admin',*

*'secret': input("Current Password: ")*

*}*

*def get\_new\_enable\_pwd():*

*new\_enable\_password = input("Enter a new enable password: ")*

*return new\_enable\_password*

*def change\_enable\_pwd(router\_parameter, new\_enable\_password):*

*try:*

*with ConnectHandler(\*\*router\_parameter) as ssh:*

*ssh.enable()*

*ssh.send\_config\_set([f'enable secret {new\_enable\_password}'])*

*print(f"Enable password changed successfully to: @{new\_enable\_password}")*

*except Exception as e:*

*print(f"Error: {str(e)}")*

*if \_\_name\_\_=="\_\_main\_\_":*

*while True:*

*new\_enable\_password = get\_new\_enable\_pwd()*

*change\_enable\_pwd(router\_parameter, new\_enable\_password)*

*print("Waiting for a week before changing the enable password again...")*

*time.sleep(604800)*

Ez a Python-kód automatizálja a Cisco IOS router engedélyezési jelszavának rendszeres   
(***7 naponta****)* időközönként történő módosítását.

A képen szöveg, képernyőkép látható

Automatikusan generált leírásA képen szöveg, képernyőkép, szoftver, Multimédiás szoftver látható

Automatikusan generált leírás

# 4. Szerverek és felhőszolgáltatás

**Cég név:** LinkWave Solutions

**Dolgozók száma:** 40 fő

**Feltelepített szervereink:**

1. ***Mikrotik Router***

**Adatok a szerverről:**

-Mikrotik 7.12

-Internet megosztása

-*Ethernet 1*: DHCP cím

-*Ethernet 2*: 35.125.55.1

1. ***Windows GUI – AD | PDC | DNS | DHCP***

**Adatok a szerverről:**

-Windows Server 2022

-50GB belső tárhely

**Konfiguráció:**

-*Domain*: lwsolutions.hu

-*Hostname*: winserverpdc

-*Felhasználónév*: LINKWAVE\administrator

-*Jelszó*: Asd123

-*IP cím*: 35.125.55.126/25

-*DNS címek*: 8.8.8.8

**Szerver feladata(i), és letelepített szolgáltatásai**:

-Active Directory

-Domain Controller

-DNS

-DHCP

***3. Windows GUI – BDC | DHCP FAILOVER***

**Adatok a szerverről:**

-Windows Server 2022

-50GB belső tárhely

**Konfiguráció:**

-*Domain*: lwsolutions.hu

-*Hostname*: winseverbdc

-*Felhasználónév*: LINKWAVE\administrator

-*Jelszó*: Asd123

-*IP cím*: 35.125.55.125/25

-*DNS címek*: 35.125.55.126

-*DHCP* (Failover)

***4. Linux Server – Webserver | Fileserver | Print***

**Adatok a szerverről:**

-Debian 12.2.0

-50GB belső tárhely (system)

-10GB shared

-50GB backup

**Konfiguráció:**

-*Domain*: lwsolutions.hu

-*Hostname*: linuxserverweb

-*Felhasználónév*: linuxserverwebadmin

-*Jelszó*: Asd123

-*IP cím*: 35.125.55.124

-*DNS címek*: 35.125.55.126, 35.125.55.125

**Szerver feladata(i), és letelepített szolgáltatásai**:

-MySQL

-Web (Apache)

-Domain admin jogosultságok

-SSL Tanúsítvány

-Automatizált mentés

-URL Rewrite

-Közös mappák

-Mappák kvótázásai

-Group Policy beállítások

**Linkek:**

-*WEB elérhetősége*: <http://lwsolutions.hu> -> (Átirányítás *https*-re)

***5. Windows 10 Kliens***

**Adatok a szerverről:**

-Windows 10 (64 bit)

-50GB belső tárhely

**Konfigurációk:**

-*Felhasználónév*: winadmin

-*Felhasználó jelszó*: Asd123

-*Gép neve*: winclient

-*Domain*: lwsolutions.hu

-*IP cím*: 29.124.58.11 (255.255.255.128)

-*DNS címek*: 35.125.55.126, 35.125.55.125

**Belépési adatok:**

Tartomány vezérlői fiók:

-*Név*: LWSOLUTIONS\administrator

-*Jelszó*: Asd123

TOVÁBBI FELHASZNÁLÓI FIÓK BELÉPÉSI ADATAI LENTEBB.

**Szerver feladata(i), és letelepített szolgáltatásai:**

-RSAT (Server Manager)

-DNS

-Reverse Lookup Zone

-Forward Lookup Zone

-DHCP

-Group Policy Management

-Users and Computers

-Computer Management

**Szervezeti egységek:**

**-**LWSOLUTIONS

-Uzemeltetok

-Laguna\_Motel

-New\_York

-Kavezo

**Linkwave Solutions** cégünk azt a feladatot kapta, hogy a **Hotel Komplexum** számára a szervertelepet kiépítse különböző biztonságos működő szerverekkel. Mi ezt meg is valósítottuk a kért paraméterek alapján és ügyeltünk a korszerű megoldásokra is.   
  
Mikrotik router segítségével kiosztottuk a címeket, amelyek a *35.125.55.0*-ös hálózatot ölelik körbe. Az alapértelmezett átjáró így a .*1* lett.

Az **Hotel Komplexum** kért egy domain controller-es szervert DNS, DHCP, active directory-val, egy backup domain controller szervert dhcp failover konfigurációval hogyha bármi történik az elsődleges **AD** szerverrel, a telephelyek kaphasson továbbra is internet elérést. Kértek ezen felül egy file szervert, egy webszervert, print és FTP szervert, egy MySQL alapú szervert az adatok tárolására és szűrésére, és egy email szolgáltatást.

Mi az AD és a BDC szervert Windows GUI 2022-ben valósítottuk meg. Beállítottunk nekik ip címeket maszkkal, valamint egy elsődleges DNS-címet, és a szerverek nevének elérhetőségét. Az AD szerver IP címe a *35.125.55.126*, az BDC szervernek pedig *35.125.55.125* IP címet adtuk. Az elsődleges domain controller DNS-címének a 8.8.8.8 címet adtuk meg, a másodlagosnak meg az elsődleges DC IP címét kapta meg.   
  
A továbbiakat a server managerben konfiguráltuk fel, ahol a DNS, DHCP, Active Directory, és a BDC esetében a DHCP failovert feltelepítettük. A felhasználók a **LWSOLUTIONS\administrator** felhasználónévvel tudnak fellépni, a jelszó pedig *Asd123* lett. Mindkét szerver esetén a domain-név a **lwsolutions.hu**-n lesz elérhető.

Az IP címzést a 35.125.55.10-től adtuk meg a 35.125.55.120-ig.

Felkonfigurálva mindkét Windows GUI szervert, a továbbiakat egy Windows 10 kliensen keresztül folytattuk.

A Windows-t feltelepítve és partícionálva az LWSOLUTIONS tartományba léptettük be *winclient* gépnévvel együtt. Ezután tartományvezérlőként (**LWSOLUTIONS\administrator**) RSAT-on keresztül tudjuk konfigurálni a szerverrel kapcsolatos teendőket.  
  
Server Manager-ben megadtuk a két GUI szerver IP címét (*35.125.55.125, .126*), hogy felvegyük a szerverlistákba őket. Ezután az elsődleges DC-n keresztül a DNS Reverse és Forward Lookup beállításain keresztül zónákat, pointereket, és a hostot, ahol a további szerverek elérhetőségét szerver névvel együtt fel tudtuk venni.

Ezután az active directoryban felvettük az **Hotel Komplexum** szervezeti egységeit, felhasználókkal és csoportokkal együtt.

## A képen szöveg, képernyőkép, Betűtípus, sor látható Automatikusan generált leírásA képen szöveg, képernyőkép, szám, Párhuzamos látható Automatikusan generált leírás4.1 Felvett felhasználók és belépési adatok területenként