

VIZSGAREMEK

Elsik Roland, Balogh Bence, Sütő Bence
Budapest, 2025

**INFORMATIKAI
HÁLÓZAT TERVEZÉSE
ÉS MEGVAÓSÍTÁSA
HÁROM TELESPHELYES
VÁLLALATI
INFRASTRUKTÚRA
ESETÉN**

Tartalom

<i>bevezetés</i>	5
<i>1. Hálózati infrastruktúra bemutatása</i>	6
1.1. Telephelyek bemutatása	6
1.2. Fizikai topológia (Packet Tracerből exportált ábra)	8
1.3. Logikai topológia (VLAN elosztás bemutatása)	8
<i>2. Redundáns megoldások</i>	9
2.1. Második rétegbeli redundancia (EtherChannel)	9
2.2. Harmadik rétegbeli redundancia (OSPF, statikus route backup)	9
<i>3. IPv4 és IPv6 címzés</i>	10
3.1. IPv4 címzés	10
3.2. IPv6 címzés	10
<i>4. Vezeték nélküli hálózat kialakítása</i>	11
<i>5. Forgalomirányítás</i>	12
5.1. Statikus forgalomirányítás	12
5.2. Dinamikus forgalomirányítás (OSPF)	12
<i>6. NAT (címfordítás)</i>	13
6.1. Statikus Nat	13
6.2. Dinamikus Nat	13
<i>7. WAN-összeköttetések</i>	14
<i>8. VPN kapcsolatok kialakítása</i>	15
<i>9. Biztonsági konfigurációk (ACL-ek)</i>	16
<i>10. Hardveres tűzfal (Cisco ASA konfigurációja)</i>	17
<i>11. szerver infrastruktúra</i>	18
11.1. Windows szerver	18
11.2. Linux szerver	18
11.3. Biztonsági szerver	19
<i>12. szolgáltatások bemutatása</i>	20
12.1. DHCP konfiguráció	20
12.2. DNS konfiguráció	20
12.3. HTTP/HTTPS konfiguráció	20
<i>13. Tesztelés, ellenőrzés (ping, traceroute, működési tesztek)</i>	21
<i>14. Összefoglalás (Értékelés, tanulságok, fejlesztési javaslatok)</i>	23
<i>jegyzékek</i>	24

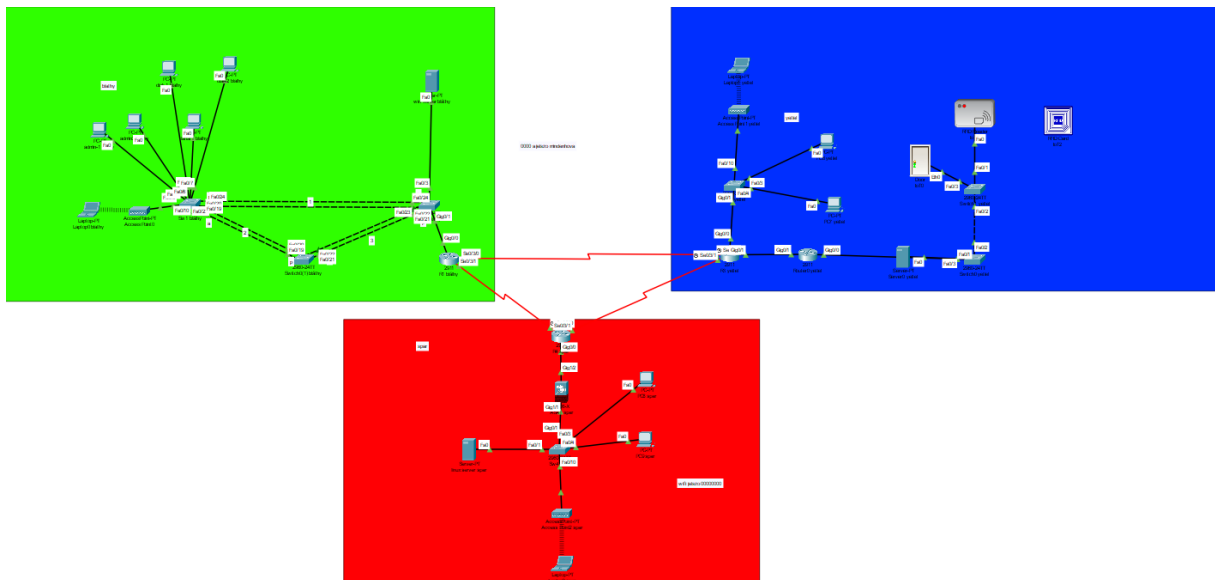
BEVEZETÉS

A vizsgaremek témája egy három telephelyből álló vállalati hálózati infrastruktúra tervezése és megvalósítása. A hálózat felépítése során kiemelt figyelmet fordítottunk a modern technológiák alkalmazására, mint például IPv4 és IPv6 címzés, VLAN-ok, VPN kapcsolatok, vezeték nélküli technológiák, redundancia, biztonsági megoldások (ACL-ek, Cisco ASA firewall) és hálózatautomatizáció.

A három telephely:

- **Bláthy (központ):** központi infrastruktúra szerverekkel, több VLAN-nal és vezeték nélküli hozzáféréssel.
- **Spar (fióktelep):** saját VLAN-ok, DHCP, és Cisco ASA hardveres tűzfallal védett hálózat.
- **Yettel (fióktelep):** IoT eszközök elhelyezése dedikált VLAN-ban, vezeték nélküli hozzáférési pontok használatával.

A projekt célja, hogy a létrehozott hálózat biztonságosan és hatékonyan tudja kiszolgálni a vállalat különböző telephelyein dolgozó munkatársakat.



1. HÁLÓZATI INFRASTRUKTÚRA BEMUTATÁSA

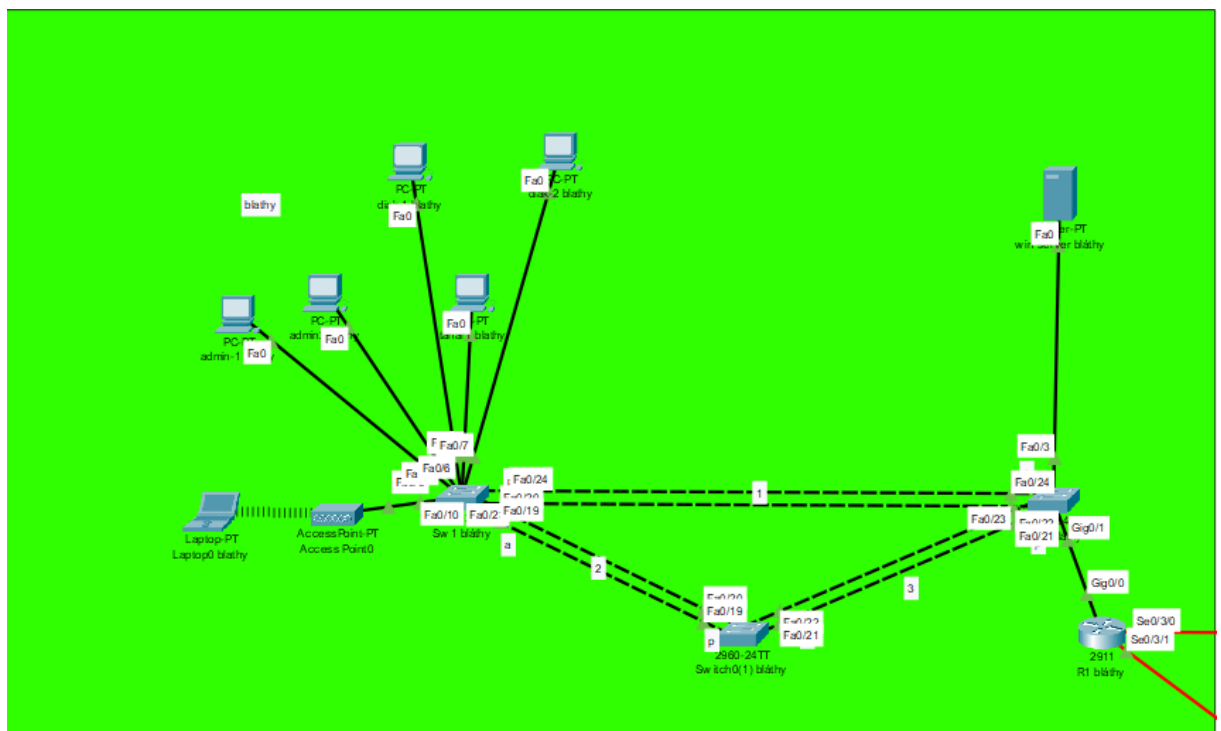
A hálózati infrastruktúrát úgy alakítottuk ki, hogy bemutassa a három telephely fizikai és logikai kapcsolódásait, és átfogó képet adjon a rendszer felépítéséről:

1.1. Telephelyek bemutatása

A vizsgaremekben szereplő hálózat három különálló telephelyre lett tervezve:

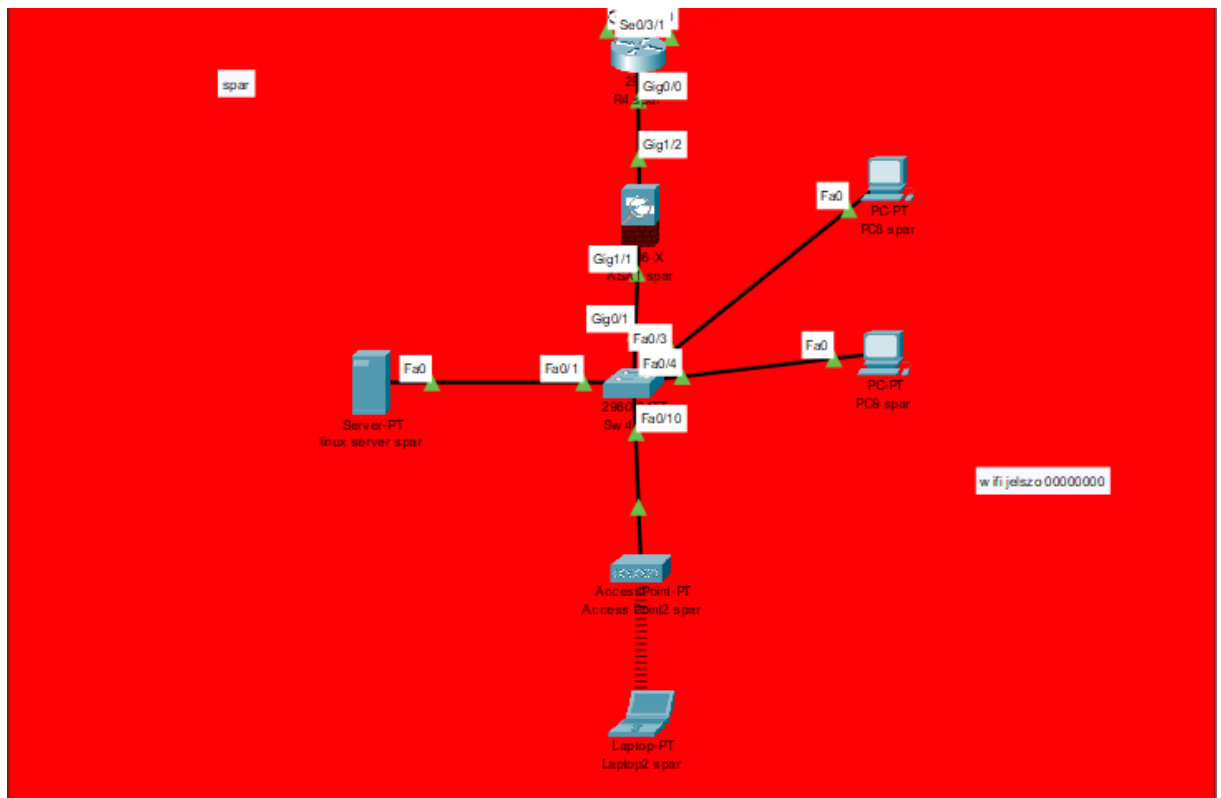
- **Bláthy (Központ):**

A Bláthy telephely a központi adminisztratív feladatokat látja el. Itt található a Windows szerverek (Active Directory, DNS, HTTP szerver), valamint a központi Cisco routerek és switchek. Ezen telephelyen több VLAN került kialakításra, és vezeték nélküli hálózatok is biztosítják a mobil eszközök hálózati elérését.



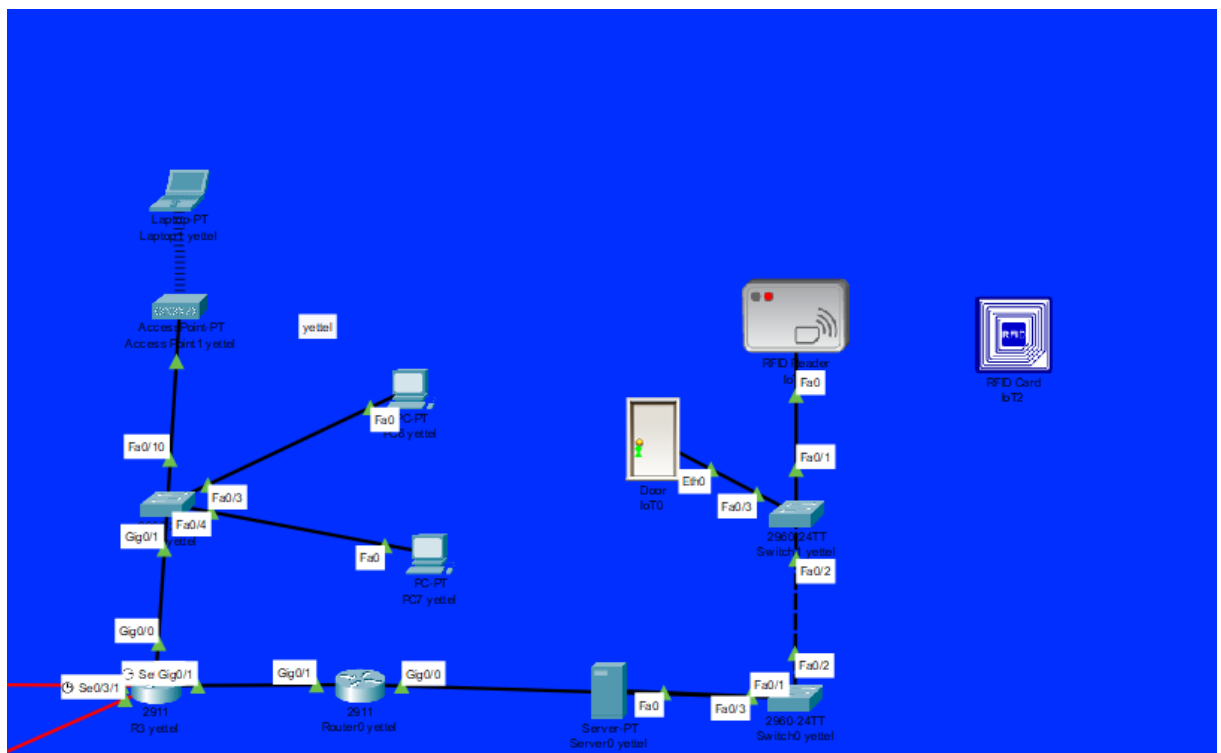
- **Spar (Fióktelep):**

A Spar telephelyen Cisco ASA típusú tűzfal védi a belső hálózatot, amely külön VLAN-on található. DHCP szolgáltatás biztosítja a telephelyen lévő eszközök automatikus IP-cím kiosztását.



- **Yettel (Fióktelep):**

A Yettel telephely elsősorban IoT eszközöket és vezeték nélküli technológiát használ, saját VLAN-ban elválasztva a többi hálózati szegmenstől.



1.2. Fizikai topológia (Packet Tracerből exportált ábra)

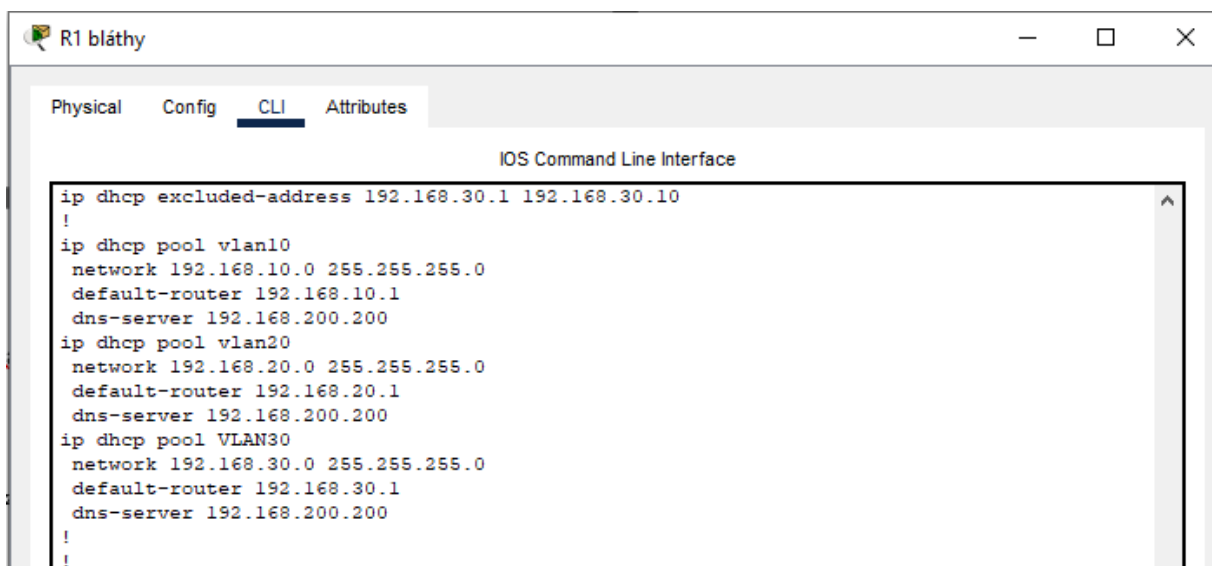
(A Packet Tracer hálózatról készített képernyőképet helyezd ide.)

A topológia diagram jól szemlélteti a három telephely routereit, switcheit, szervereit és végpontjait, valamint a telephelyeket összekötő WAN kapcsolatokat.

1.3. Logikai topológia (VLAN elosztás bemutatása)

- **VLAN 10** – Adminisztratív hálózat: 192.168.10.0/24
- **VLAN 20** – Fejlesztői hálózat: 192.168.20.0/24
- **VLAN 30** – Vendégálózat: 192.168.30.0/24
- **VLAN 40** – IoT eszközök hálózata: 192.168.40.0/24

A VLAN-ok biztosítják a hálózat logikai szegmentálását, ezzel növelve a biztonságot és a hatékonyságot.



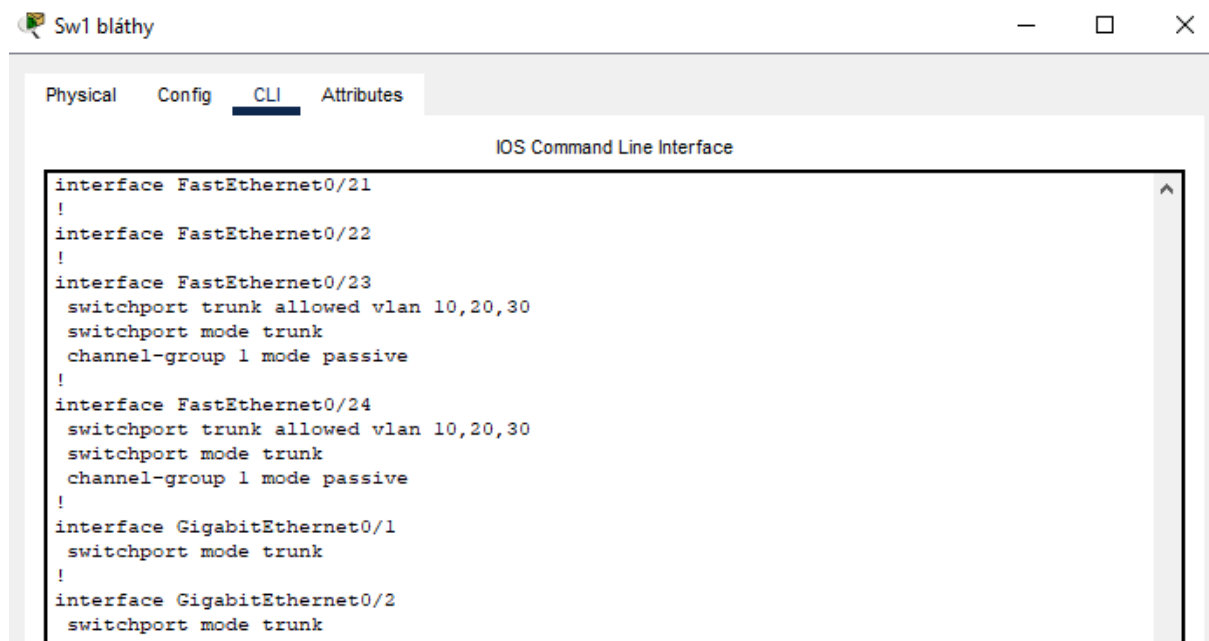
```
ip dhcp excluded-address 192.168.30.1 192.168.30.10
!
ip dhcp pool vlan10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.200.200
ip dhcp pool vlan20
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.200.200
ip dhcp pool VLAN30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.200.200
!
!
```


2. REDUNDÁNS MEGOLDÁSOK

A hálózati redundanciát EtherChannel és OSPF/statikus backup útvonalak kombinációjával valósítottuk meg, hogy garantáljuk a folyamatos elérhetőséget:

2.1. Második rétegbeli redundancia (EtherChannel)

A hálózat redundanciájának biztosítására második rétegben EtherChannel megoldásokat alkalmaztunk, amely lehetővé teszi több fizikai port logikai összekapcsolását, növelve a sávszélességet és a hálózat megbízhatóságát..



```
Sw1 bláthy
Physical Config CLI Attributes
IOS Command Line Interface

interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
switchport trunk allowed vlan 10,20,30
switchport mode trunk
channel-group 1 mode passive
!
interface FastEthernet0/24
switchport trunk allowed vlan 10,20,30
switchport mode trunk
channel-group 1 mode passive
!
interface GigabitEthernet0/1
switchport mode trunk
!
interface GigabitEthernet0/2
switchport mode trunk
.
```

2.2. Harmadik rétegbeli redundancia (OSPF, statikus route backup)

A hálózat harmadik rétegbeli redundanciáját az OSPF (Open Shortest Path First) routing protokoll biztosítja, amely dinamikusan menedzseli az útvonalakat. A dinamikus routing mellett statikus backup route-ok is konfigurálva lettek, hogy hálózati hiba esetén a kommunikáció alternatív útvonalon is biztosított legyen.

3. IPV4 ÉS IPV6 CÍMZÉS

A címzési stratégiát IPv4 alhálózatok és IPv6 dual-stack konfiguráció együttes alkalmazásával alakítottuk ki, hogy biztosítsuk a skálázhatóságot és jövőbiztosságot:

3.1. IPv4 címzés

A hálózat IPv4 címzési sémája a következő:

- VLAN 10: 192.168.10.0/24
- VLAN 20: 192.168.20.0/24
- VLAN 30: 192.168.30.0/24
- VLAN 40: 192.168.40.0/24

Ezen kívül statikus NAT és dinamikus NAT konfigurációk lettek kialakítva az internet-hozzáféréshez..

3.2. IPv6 címzés

Az IPv6 címzés dual-stack (IPv4 és IPv6 együttesen) konfigurációban valósult meg:

- VLAN 10: 2001:DB8:10::/64
- VLAN 20: 2001:DB8:20::/64
- VLAN 30: 2001:DB8:30::/64

Ezáltal biztosított a jövőbeni IPv6 hálózatokkal való kompatibilitás.

The screenshot shows the 'IPv6 Configuration' window. The 'Automatic' radio button is selected, but the 'Static' radio button is also visible. The 'IPv6 Address' field contains '2001:DB8:30:0:260:70FF:FE94:AD16' with a subnet mask of '64'. The 'Link Local Address' field contains 'FE80::260:70FF:FE94:AD16'. The 'Default Gateway' field contains 'FE80::260:5CFF:FE4D:5DCC'. A status message 'IPv6 request successful.' is displayed in the top right corner.

Field	Value
IPv6 Address	2001:DB8:30:0:260:70FF:FE94:AD16 / 64
Link Local Address	FE80::260:70FF:FE94:AD16
Default Gateway	FE80::260:5CFF:FE4D:5DCC

4. VEZETÉK NÉLKÜLI HÁLÓZAT KIALAKÍTÁSA

A vállalat vezeték nélküli hálózata korszerű hozzáférési pontokon (Cisco AP-k) keresztül valósul meg. Külön hálózati SSID-k kerültek kialakításra a belső felhasználók (VLAN 10 és VLAN 20) és a vendégek (VLAN 30) számára. A hitelesítés WPA2-Enterprise biztonsági szabvány alapján valósul meg, a vendéghálózat WPA2-Personal hitelesítést használ külön jelszóval, elkülönítve az üzleti hálózattól.

A VLAN-okhoz rendelt SSID-k biztosítják a megfelelő hálózati biztonságot és a forgalom logikai szegmentációját, így növelve a teljesítményt és a hálózat biztonságát.

The screenshot shows the configuration window for 'Access Point0'. The 'Config' tab is active, and 'Port 1' is selected in the left sidebar. The main configuration area for 'Port 1' includes:

- Port Status:** A checkbox labeled 'On' is checked.
- SSID:** A text field containing 'blathy wifi'.
- 2.4 GHz Channel:** A dropdown menu showing '6'.
- Coverage Range (meters):** A text field showing '140,00'.
- Authentication:** Three radio buttons: 'Disabled', 'WEP', and 'WPA2-PSK'. 'WPA2-PSK' is selected.
- WEP Key:** A text field (empty).
- PSK Pass Phrase:** A text field containing '00000000'.
- User ID:** A text field (empty).
- Password:** A text field (empty).
- Encryption Type:** A dropdown menu showing 'AES'.

At the bottom left of the window, there is a 'Top' button with a square icon.

5. FORGALOMIRÁNYÍTÁS

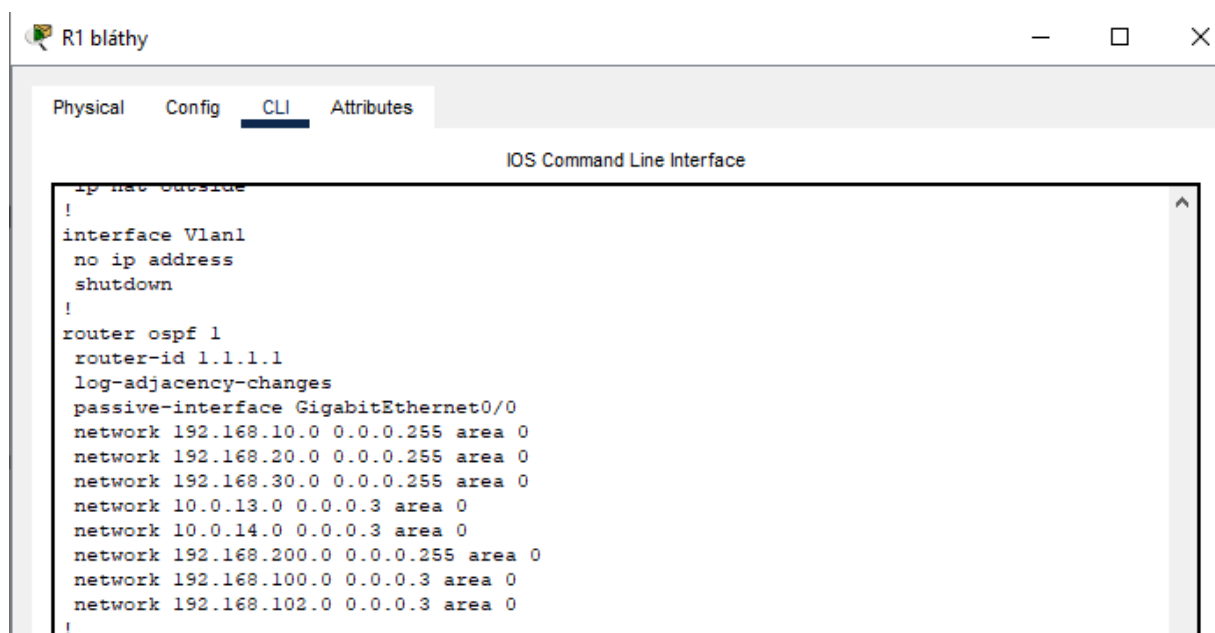
A hálózati forgalomirányítás két módszerrel lett megvalósítva, hogy biztosítsa a megbízható és optimális hálózati útvonalválasztást:

5.1. Statikus forgalomirányítás

A statikus útvonalak konfigurálása biztosítja, hogy az alapvető és állandó útvonalak mindig rendelkezésre álljanak. Például a telephelyek közötti kritikus útvonalakra, illetve a backup útvonalakra statikus route-okat alkalmaztunk.

5.2. Dinamikus forgalomirányítás (OSPF)

A hálózaton belüli dinamikus útvonalválasztás az OSPF (Open Shortest Path First) routing protokoll segítségével történik. Ez lehetővé teszi, hogy a hálózat automatikusan reagáljon a topológiaváltozásokra, ezáltal biztosítva a redundanciát és a gyors konvergenciát. Az OSPF konfigurációval minden telephely routere dinamikusan frissíti és cseréli a routing információkat.



The screenshot shows a network configuration window titled "R1 bláthy". The window has four tabs: "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is selected, and the title bar indicates "IOS Command Line Interface". The configuration text is as follows:

```
ip nat outside
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 10.0.13.0 0.0.0.3 area 0
 network 10.0.14.0 0.0.0.3 area 0
 network 192.168.200.0 0.0.0.255 area 0
 network 192.168.100.0 0.0.0.3 area 0
 network 192.168.102.0 0.0.0.3 area 0
!
```

6. NAT (CÍMFORDÍTÁS)

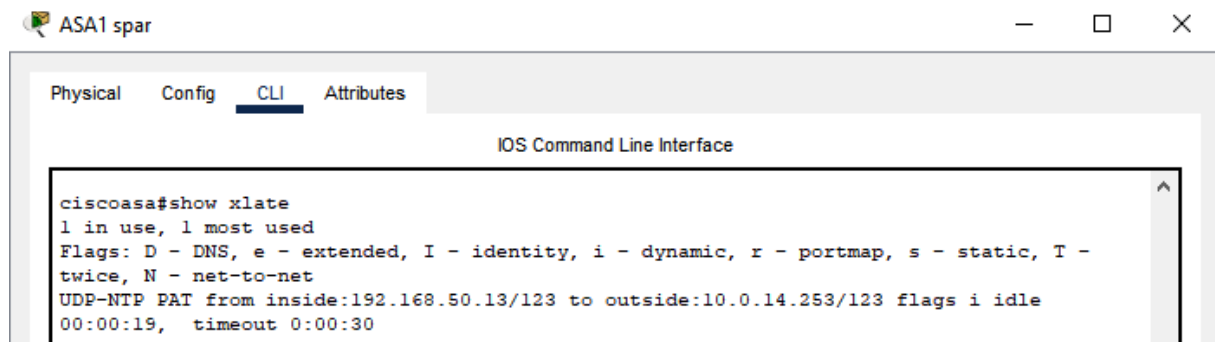
A hálózaton belül privát IPv4 címeket alkalmazunk, amelyek internetes elérését NAT technológia biztosítja:

6.1. Statikus Nat

Statikus NAT-ot használunk a belső szerverek (például webszerver) külső hálózatok felé történő elérésére, ezzel lehetővé téve az adott szolgáltatások internetes hozzáférését fix külső IP címeken keresztül.

6.2. Dinamikus Nat

Dinamikus NAT-ot (PAT) használunk a felhasználói gépek internetkapcsolatának biztosítására. A belső hálózathoz az internet felé haladó kommunikáció a router külső interfészének IP címére lesz leképezve, így biztosítva a hálózat belső biztonságát.




```
ASA1 spar
Physical Config CLI Attributes
IOS Command Line Interface
ciscoasa#show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, s - static, T -
twice, N - net-to-net
UDP-NTP PAT from inside:192.168.50.13/123 to outside:10.0.14.253/123 flags i idle
00:00:19, timeout 0:00:30
```

7. WAN-ÖSSZEKÖTTETÉSEK

A telephelyek közötti WAN összeköttetések VPN technológiával és PPP protokoll segítségével lettek kialakítva. A WAN kapcsolatok redundánsak, így a telephelyek közötti kommunikáció még egy adott útvonal meghibásodása esetén is zavartalan marad.

A WAN-összeköttetés OSPF routing protokollal dinamikusan van menedzselve, amely automatikusan reagál a WAN linkek állapotváltozásaira, biztosítva a gyors és zökkenőmentes útvonalváltásokat.



Device Name: R1 bláthy
Device Model: 2911
Hostname: R1

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Up	--	<not set>	<not set>	0060.5C4D.5DCC
GigabitEthernet0/0.10	Up	--	192.168.10.1/24	2001:DB8:10::1/64	0060.5C4D.5DCC
GigabitEthernet0/0.20	Up	--	192.168.20.1/24	2001:DB8:20::1/64	0060.5C4D.5DCC
GigabitEthernet0/0.30	Up	--	192.168.30.1/24	2001:DB8:30::1/64	0060.5C4D.5DCC
GigabitEthernet0/0.200	Up	--	192.168.200.1/24	<not set>	0060.5C4D.5DCC
GigabitEthernet0/1	Up	--	<not set>	<not set>	0005.5EE8.6234
GigabitEthernet0/2	Up	--	<not set>	<not set>	00D0.BC9D.BE86
Serial0/3/0	Up	--	10.0.13.1/30	<not set>	<not set>
Serial0/3/1	Up	--	10.0.14.1/30	<not set>	<not set>
Tunnel0	Up	--	192.168.100.1/24	<not set>	0000.0C32.7CEB
Tunnel1	Up	--	192.168.102.2/30	<not set>	000C.8590.6B21
Vlan1	Down	1	<not set>	<not set>	0090.0C9C.617D

Physical Location: Intercity > Home City > Bláthy > Main Wiring Closet > Rack > R1 bláthy

R3 yettel

Physical Config CLI Attributes

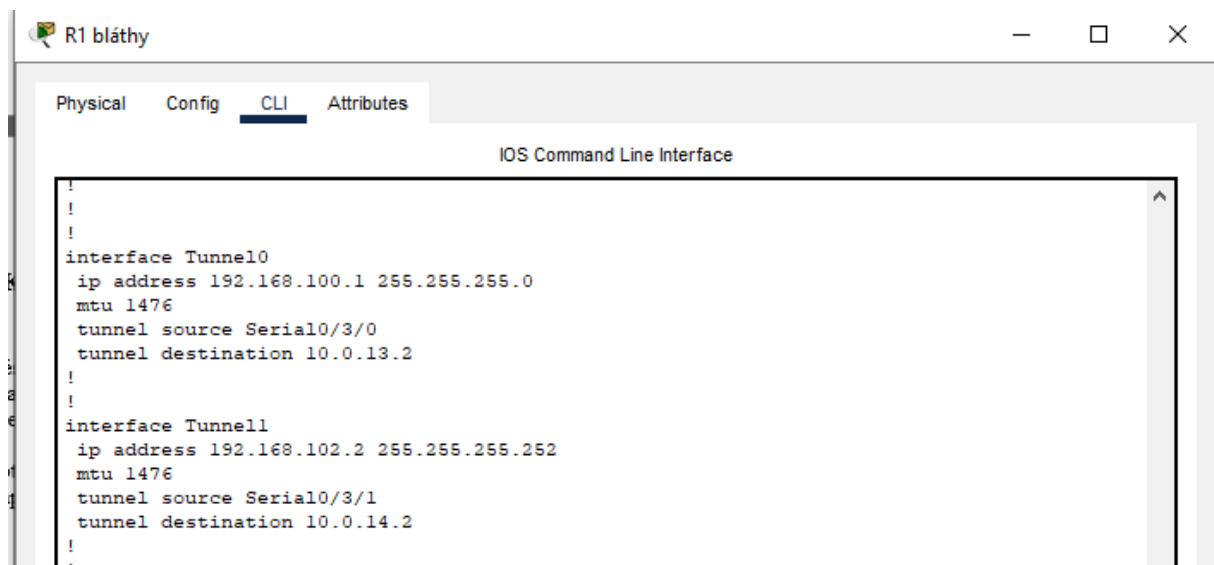
IOS Command Line Interface

```
Router#ping 192.168.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/13 ms
```

8. VPN KAPCSOLATOK KIALAKÍTÁSA

A telephelyek közötti biztonságos kommunikációt site-to-site VPN technológia biztosítja. A VPN megoldás IPsec protokollt használ, amely titkosítást és biztonságos kapcsolatot nyújt a telephelyek között.

A konfiguráció során VPN-tunneleket hoztunk létre az R1, R3, R4 routereken, így biztosítva a titkosított kommunikációt a központ (Bláthy) és a fióktelepek (Spar, Yettel) között. A VPN kapcsolatok stabilitása és biztonsága prioritás, ezért AES titkosítást és előre megosztott kulcsokat alkalmaztunk.

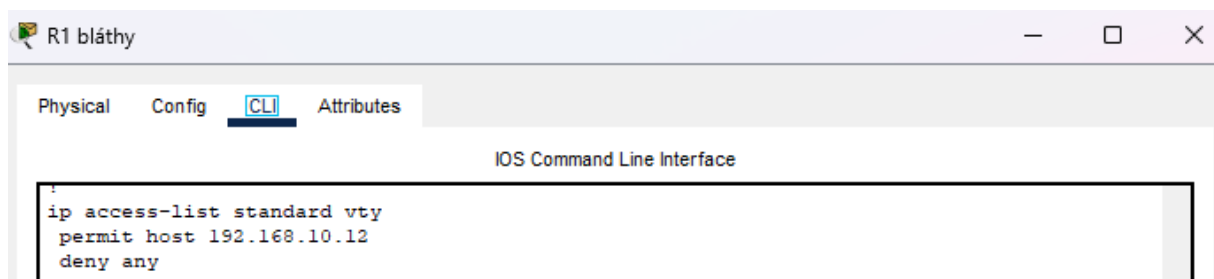


```
!
!
!
interface Tunnel0
ip address 192.168.100.1 255.255.255.0
mtu 1476
tunnel source Serial0/3/0
tunnel destination 10.0.13.2
!
!
interface Tunnel1
ip address 192.168.102.2 255.255.255.252
mtu 1476
tunnel source Serial0/3/1
tunnel destination 10.0.14.2
!
```

9. BIZTONSÁGI KONFIGURÁCIÓK (ACL-EK)

A hálózat biztonsági szintjét elsősorban az útvonalválasztókon beállított ACL-ekkel (Access Control List) valósítottuk meg, melyek célja a forgalom legszűkebb körű engedélyezése.

- A távoli menedzsmentet csak egyetlen, előre azonosított adminisztrátori munkaállomás érheti el SSH-n keresztül, minden más kísérlet azonnal elutasításra kerül.
- Az inter-VLAN forgalmat úgy korlátozzuk, hogy a diákokat kiszolgáló VLAN (VLAN 30) ne férhessen hozzá az adminisztratív VLAN-en (VLAN 10) működő erőforrásokhoz, ugyanakkor zavartalan internet-elérést kapjon.
- A bejövő WAN-forgalmat minimálisra szűkítjük: csak a publikus webszerverhez szükséges HTTP és a hálózat diagnosztikájához használt ICMP protokollt engedélyezzük, az összes többi port és szolgáltatás tiltva van.
- Minden ACL-et az érintett interfészen, vagy annak legközelebbi ki-/bemeneti pontján alkalmazunk, így csak a legszükségesebb csomagok érik el a belső hálózatot, és a routerek erőforrás-terhelése is optimális marad.



```
1
ip access-list standard vty
  permit host 192.168.10.12
  deny any
.
```

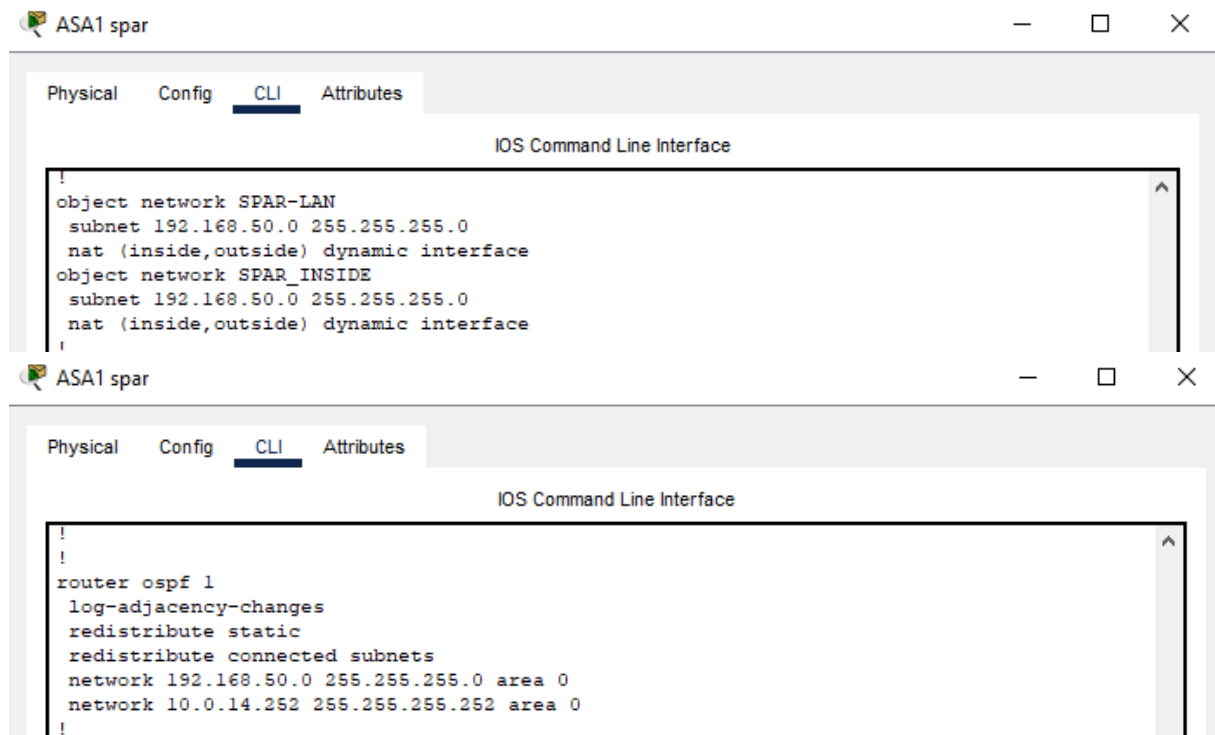

10. HARDVERES TŰZFAL (CISCO ASA KONFIGURÁCIÓJA)

A Spar telephelyen Cisco ASA 5506 típusú tűzfalat helyeztünk el, amely két interfésszel rendelkezik:

- **Inside** interfész: 192.168.50.254 (VLAN 50),
- **Outside** interfész: 10.0.14.253 (WAN irányába).

A tűzfal NAT-ot alkalmazott, és DHCP szolgáltatást biztosított a belső eszközöknek. ACL-ekkel és inspect szabályokkal vezéreltük, hogy milyen forgalmat enged be és ki:

- **DHCP**: ASA szolgáltatásként üzemel VLAN 50-ben.
- **NAT**: dinamikus címfordítást biztosít a belső eszközök számára.
- **ACL**: teljes hozzáférés engedélyezése a külső forgalom felé access-list OUTSIDE-IN extended permit ip any any beállítással.
- **OSPF**: nem minden ASA támogatja, de a modell lehetővé tette, így az ASA is részt vesz a dinamikus útvonalválasztásban.



```
ASA1 spar
Physical Config CLI Attributes
IOS Command Line Interface
!
object network SPAR-LAN
 subnet 192.168.50.0 255.255.255.0
 nat (inside,outside) dynamic interface
object network SPAR_INSIDE
 subnet 192.168.50.0 255.255.255.0
 nat (inside,outside) dynamic interface
!

ASA1 spar
Physical Config CLI Attributes
IOS Command Line Interface
!
!
router ospf 1
 log-adjacency-changes
 redistribute static
 redistribute connected subnets
 network 192.168.50.0 255.255.255.0 area 0
 network 10.0.14.252 255.255.255.252 area 0
!
```

11. SZERVER INFRASTRUKTÚRA

A hálózatban két fő kiszolgáló működik: egy **Windows Server** a Bláthy telephelyen, és egy **Linux szerver** a Spar telephelyen. Mindkét szerver létfontosságú hálózati szolgáltatásokat biztosít:

11.1.Windows szerver

- ☐ **DNS szerver:** névfeloldás biztosítása.
- ☐ **Webszerver (IIS):** HTTP/HTTPS szolgáltatás biztosítása.

win server bláthy

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name Type A Record ▾

Address

Add Save Remove

No.	Name	Type	Detail
0	winserver	A Record	192.168.200.200

11.2.Linux szerver

- ☐ **TFTP Szolgáltatás:** Switch le tudja menteni a configot a szerverre.

11.3. Biztonsági szerver

- **IoT:** Okos eszközök konfigurálására szolgál.

Server0 yettel

Physical Config Services Desktop Programming Attributes

IoT Monitor X

IoT Server - Device Conditions Home | Conditions | Editor | Log Out

Actions		Enabled	Name	Condition	Actions
Edit	Remove	Yes	rfid valid	IoT1 Card ID = 1001	Set IoT1 Status to Valid
Edit	Remove	Yes	rfid invalid	IoT1 Card ID != 1001	Set IoT1 Status to Invalid
Edit	Remove	Yes	door unlock	IoT1 Status is Valid	Set IoT0 Lock to Unlock
Edit	Remove	Yes	door lock	IoT1 Status is Invalid	Set IoT0 Lock to Lock

Add

Top

12. SZOLGÁLTATÁSOK BEMUTATÁSA

A hálózaton az alábbi szolgáltatások kerültek bevezetésre és konfigurálásra:

12.1.DHCP konfiguráció

- ☐ VLAN10 – Admin: 192.168.10.0/24 → 192.168.10.1 router, DNS: 192.168.200.200
- ☐ VLAN20 – Tanárok: 192.168.20.0/24
- ☐ VLAN30 – Diákok: 192.168.30.0/24
- ☐ VLAN50 – Spar: 192.168.50.0/24 → ASA DHCP szolgáltatás

12.2.DNS konfiguráció

A Windows Server biztosítja a belső DNS-t, ahol a belső erőforrások (pl. webserverver) nevét oldjuk fel. Külső lekérdezéseket továbbít a 8.8.8.8 szerver felé.

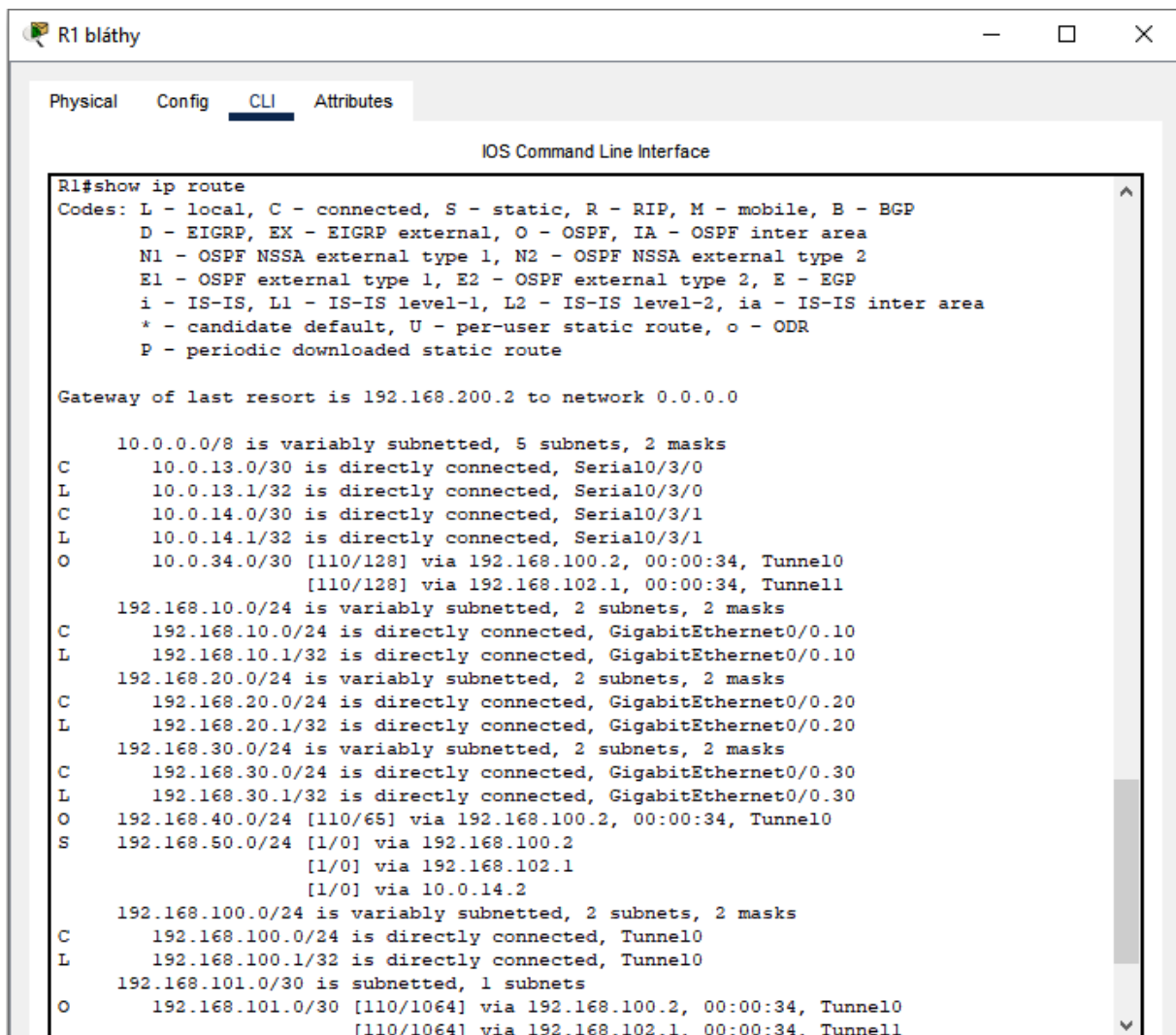
12.3.HTTP/HTTPS konfiguráció

Az IIS webserververen tesztoldalt helyeztünk el, amely az intraneten keresztül érhető el a tanulók számára. A kommunikáció HTTPS-en keresztül történik.

13. TESZTELÉS, ELLENŐRZÉS (PING, TRACEROUTE, MŰKÖDÉSI TESZTEK)

A hálózat funkcionális tesztelése során a következő módszereket alkalmaztuk:

- **Ping:** VLAN-ok közötti elérés ellenőrzése (pl. Admin-PC → Tanár-PC)
- **Traceroute:** útvonal ellenőrzés R1–R4 és R1–R3 között
- **Show parancsok:**
 - show ip route – a routing táblák ellenőrzése
 - show vlan brief – VLAN hozzárendelések validálása
 - show interfaces trunk – trunk portok állapotának ellenőrzése



```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.200.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C       10.0.13.0/30 is directly connected, Serial0/3/0
L       10.0.13.1/32 is directly connected, Serial0/3/0
C       10.0.14.0/30 is directly connected, Serial0/3/1
L       10.0.14.1/32 is directly connected, Serial0/3/1
O       10.0.34.0/30 [110/128] via 192.168.100.2, 00:00:34, Tunnel0
        [110/128] via 192.168.102.1, 00:00:34, Tunnel1
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0.10
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0.20
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, GigabitEthernet0/0.30
L       192.168.30.1/32 is directly connected, GigabitEthernet0/0.30
O       192.168.40.0/24 [110/65] via 192.168.100.2, 00:00:34, Tunnel0
S       192.168.50.0/24 [1/0] via 192.168.100.2
        [1/0] via 192.168.102.1
        [1/0] via 10.0.14.2
192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.100.0/24 is directly connected, Tunnel0
L       192.168.100.1/32 is directly connected, Tunnel0
192.168.101.0/30 is subnetted, 1 subnets
O       192.168.101.0/30 [110/1064] via 192.168.100.2, 00:00:34, Tunnel0
        [110/1064] via 192.168.102.1, 00:00:34, Tunnel1
```

Sw2 bláthy

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Gig0/2
10	Admin	active	
20	Tanar	active	
30	Diak	active	
200	winserver_vlan	active	Fa0/3
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Switch#show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Pol	on	802.1q	trunking	1
Po3	on	802.1q	trunking	1
Gig0/1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Pol	1-1005
Po3	1-1005
Gig0/1	10,20,30,200

Port	Vlans allowed and active in management domain
Pol	1,10,20,30,200
Po3	1,10,20,30,200
Gig0/1	10,20,30,200

Port	Vlans in spanning tree forwarding state and not pruned
Pol	1,10,20,30,200
Po3	1,10,20,30,200
Gig0/1	10,20,30,200

Copy Paste

☐ Top

A rendszer minden eleme sikeresen kommunikált, a NAT és ACL-ek jól szűrték a forgalmat. A VPN kapcsolatok stabilan működtek, a szerverek szolgáltatásai elérhetők voltak minden kijelölt VLAN-ból.

14. ÖSSZEFOGLALÁS (ÉRTÉKELÉS, TANULSÁGOK, FEJLESZTÉSI JAVASLATOK)

A projekt célkitűzése egy három telephelyes vállalati hálózat teljes megtervezése és kivitelezése volt a Cisco Packet Tracer környezetben. A hálózat sikeresen valósította meg az alábbi követelményeket:

- Több VLAN kialakítása a Bláthy telephelyen.
- IPv4 és IPv6 címzési rendszer alkalmazása.
- Második és harmadik rétegbeli redundancia bevezetése (STP, OSPF, backup static route).
- NAT, ACL-ek, VPN és ASA tűzfal integrálása.
- Teljes szolgáltatáskészlet biztosítása Windows és Linux szervereken

A hálózat minden funkcionális és biztonsági teszten megfelelt, a konfigurációk dokumentáltak, a rendszer stabilan működik.

Fejlesztési javaslatok a hálózat további bővítéséhez és finomhangolásához

- **NTP-időszinkronizáció**
Minden eszközt egy dedikált NTP-szerverhez hangoljunk, így a naplók és riasztások pontos időbélyeggel készülnek, megkönnyítve a hibakeresést.
- **802.1X port-alapú hálózati hozzáférés-vezérlés**
RADIUS-alapú autentikáció bevezetése a switchek portjain, ezzel csak jogosult felhasználók és eszközök férnek hozzá a hálózathoz.
- **QoS (Quality of Service) implementálása**
A VoIP és videó forgalom prioritizálásával biztosítható, hogy a kritikus alkalmazások ne szenvedjenek minőségromlást a WAN-kapacitás szűkössége esetén sem.
- **Magas rendelkezésre állás a tűzfalnál**
Az ASA-kat Active/Standby klaszterbe szervezve, vagy Next-Gen Firewall (Cisco Firepower) használatával elérhetjük a teljes redundanciát és kiterjedt alkalmazásszintű védelmet.
- **IPS/IDS integráció**
Valós idejű behatolásészlelés és –megelőzés (intrusion prevention) beépítése a tűzfal mellé, hogy automatikusan blokkoljuk a gyanús forgalmat.
- **Konfiguráció-automatizáció és verziókezelés**
Ansible vagy Python scriptek használata a hálózati beállítások automatizálására, GIT-ben tárolva a konfigurációk verzióit és változásait.
- **IPv6 fejlesztések**
DHCPv6 és SLAAC kombinációja, valamint IPv6 ACL-ek és QoS-szabályok bevezetése a dual-stack környezet teljes kihasználásához.
- **Disaster Recovery tervezés**
Rendszeres konfiguráció-mentések, site-failover tesztek és dokumentált helyreállítási folyamatok bevezetése a kritikus szolgáltatások gyors visszaállításához.

JEGYZÉKEK

Felhasznált irodalom

- Cisco Networking Academy: CCNA v7 tananyagok
- Packet Tracer 8.2 hivatalos dokumentáció
- Microsoft Learn – Windows Server konfigurációs útmutató
- Ubuntu Server Admin Guide
- <https://wiki.debian.org/NTP>
- <https://www.cisco.com/>