



Budapesti Műszaki Szakképzési Centrum  
Neumann János Informatikai Technikum

***Szakképesítés neve:*** Informatikai rendszer- és alkalmazás-  
üzemeltető technikus  
***száma:*** 5-0612-12-02

# **VIZSGAREMEK**

## **Gandhiegyszálse**

### **Tesztelési dokumentáció**

Dombi-Hejcsér Bence, Necek Dániel Milán, Veres Kolos  
13IRAÜ1

Budapest, 2025.



# TARTALOMJEGYZÉK

TARTALOMJEGYZÉK .....	2
VLAN-ok.....	3
Vlanok létrehozása .....	3
VTP (VLAN trónk protokoll).....	3
Inter-Vlan routing.....	4
Második rétegbeli megvalósítások.....	5
EtherChannel (port összevonás) .....	5
Portbiztonság .....	7
STP (Spanning Tree Protocol).....	9
Harmadik rétegbeli megvalósítások.....	11
HSRP .....	11
OSPF .....	14
OSPF Hitelesítés .....	15
NAT .....	16
Tűzfalak.....	18
Port Továbbítás .....	19
SSH (Secure Shell Protokoll).....	21
Tunnel.....	22
IP telefonok.....	24
WEB-VPN .....	25
BGP.....	28
WLC .....	29
Windows és Linux Szerverek.....	31
Active Directory.....	31
DHCP.....	32
MAIL .....	32
Web és DNS .....	33
FTP.....	33
RSYNC és szerverek közti SSH.....	34
Hálózat Programozás .....	36



# VLAN-ok

## Vlanok létrehozása

A megtervezett vlanokat statikusan létrehozzuk a kapcsolókon, a 2. Telephelyen (G1SS2) kizárólag a vtp szervernek beállított kapcsolón hozzuk létre a vlanokat.

```
G1SS2-SW1#show vlan brief
```

VLAN	Name	Status
-----	-----	-----
1	default	active
10	Dolgozok_Data	active
30	management	active
40	VOICE	active
50	wireless	active

A show parancs kimenetéből látszik, hogy a kívánt vlanok létrejöttek a kapcsolón.

## VTP (VLAN trönk protokoll)

A 2. telephelyen (G1SS2) a vtp kliensként beállított kapcsolókra a vlanokat a vtp protokollal juttatjuk el. Először ellenőrizzük, hogy a kapcsolónk vtp módja kliensre van-e állítva, és hogy a tartomány név helyes-e.

```
G1SS2-SW2#show vtp status
```

```
VTP version running : 1
VTP Domain Name : G1SS.com

Feature VLAN :
-----
VTP Operating Mode : Client
Number of existing VLANs : 9
```

A beállítások ellenőrzését követően nézzük meg, hogy a kapcsoló megkapta-e a vlanokat.

```
G1SS2-SW2#show vlan brief
```

VLAN	Name	Status
-----	-----	-----
1	default	active
10	Dolgozok_Data	active
30	management	active
40	VOICE	active
50	wireless	active

A kliensként beállított SW2 kapcsolón kiadott show parancs kimenetéből látszik, hogy a vlanok sikeresen átkerültek a kapcsolóra.



## Inter-Vlan routing

Az inter-vlan routing tesztelése azzal kezdődik, hogy a forgalomirányító alinterfészeinek ellenőrizzük, hogy a címei és az interfészek utáni vlan azonosító helyes-e.

```
G1SS2-R2#show ip interface brief
```

Interface	IP-Address	Status
FastEthernet0/0	unassigned	up
FastEthernet0/0.10	192.168.2.2	up
FastEthernet0/0.30	192.168.2.130	up
FastEthernet0/0.40	192.168.2.34	up
FastEthernet0/0.50	192.168.2.66	up

Miután a forgalomirányító interfészeinek helyes beállítása megtörténik, a hálózatban amint lesz IP címe a berendezéseknek, kommunikálni tudnak egymással. Az IP címek kiosztása később kerül bemutatásra.

A vlanok közötti forgalom tesztelésére az 1. telephelyen (G1SS1) kerül sor, a VLAN 10-ben levő PC és VLAN 30-ban levő kapcsoló között. Először ellenőrizzük a VLAN 10-ben levő PC-n, hogy melyik hálózatban van.

```
C:\>ipconfig
```

```
FastEthernet0 Connection: (default port)
```

```

Connection-specific DNS Suffix...:
Link-local IPv6 Address . . . . .: FE80::201:97FF:FEC0:1284
IPv6 Address . . . . .: ::
IPv4 Address . . . . .: 192.168.1.103
Subnet Mask . . . . .: 255.255.255.240
Default Gateway . . . . .: ::
                          192.168.1.97

```

Ezt követően a Kapcsolón ellenőrizzük, a hálózatot.

```
G1SS1-SW1#show running-config | include default-gateway
```

```
ip default-gateway 192.168.1.169
```

```
G1SS1-SW1#show ip interface brief | include Vlan30
```

```
Vlan30          192.168.1.170    up
```

Mivel ezek látszik, hogy külön hálózatban vannak, PING paranccsal teszteljük a kapcsolatot a két eszköz között.

```
Pinging 192.168.1.170 with 32 bytes of data:

Reply from 192.168.1.170: bytes=32 time<1ms TTL=254
Reply from 192.168.1.170: bytes=32 time<1ms TTL=254
Reply from 192.168.1.170: bytes=32 time=1ms TTL=254
Reply from 192.168.1.170: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.1.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Látszik, hogy a csomagok sikeresen elérték a kapcsolóhoz, ez azt jelenti, hogy működik a vlanok közötti forgalomirányítás.

## Második rétegbeli megvalósítások

### EtherChannel (port összevonás)

Az EtherChannel tesztelése úgy fog történni, hogy ellenőrizzük az összevont csatornák létezését, az összevont portok egyikét lekapcsoljuk, és ellenőrizzük, hogy a forgalom továbbra is sikeresen halad át az összevont csatornán.

Az első lépés a létezés ellenőrzése, amire a „*show etherchannel summary*” parancsot használtuk.

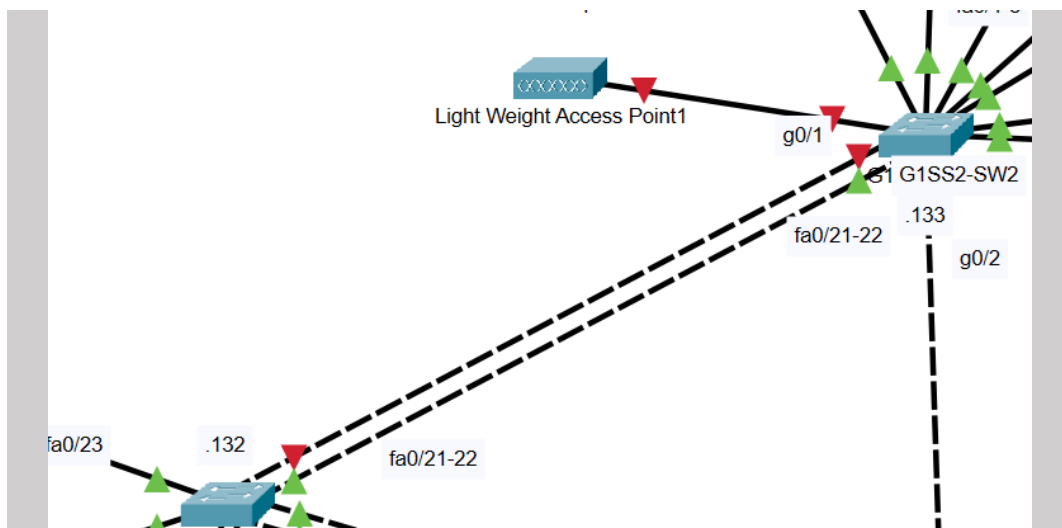
```
G1SS2-SW1#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        LACP       Fa0/21(P) Fa0/22(P)
2      Po2(SU)        LACP       Fa0/18(P) Fa0/19(P)
G1SS2-SW1#
```

Látszik, hogy a Po1-ben a FastEthernet 0/21 és 22-es portok vannak, a Po2-ben pedig a FastEthernet 0/18 és 19-es portok.

Miután meggyőződünk róla, hogy az összevont csatornák léteznek, a csatornában levő egyik portot manuálisan lekapcsoljuk.



Ezt követően teszteljük, hogy a bal oldali kapcsoló (G1SS2-SW1) a PING paranccsal elér-e a jobb oldali (G1SS2-SW2) kapcsolót. (A jobb oldali kapcsoló VLAN 30-as virtuális IP címe 192.168.2.133).

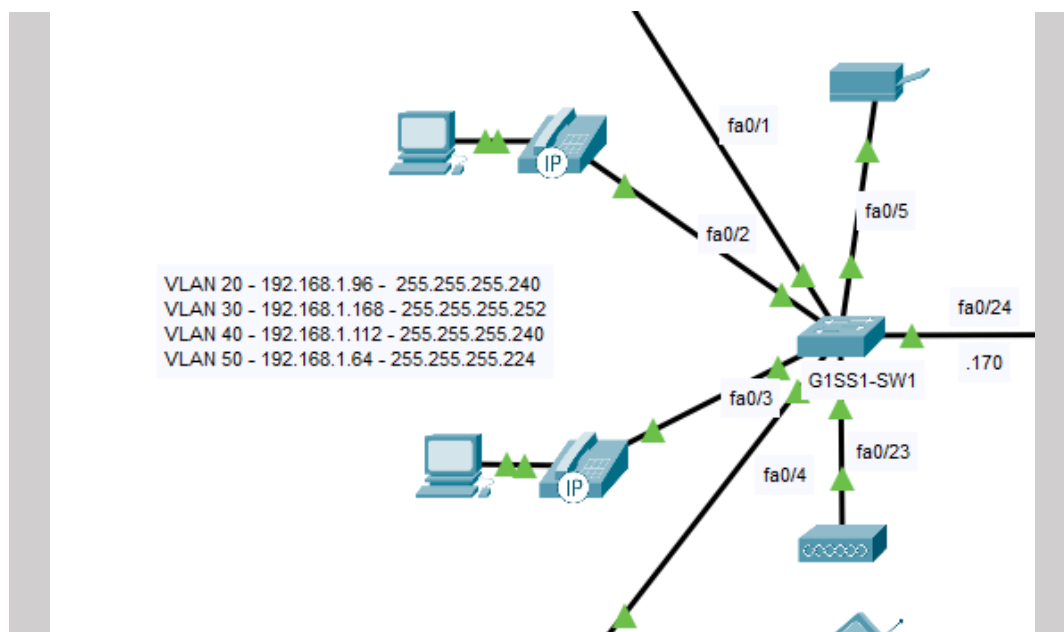
```
G1SS2-SW1#ping 192.168.2.133

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.133, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Látjuk, hogy a kapcsoló sikeresen elér a .133-as címet annak ellenére, hogy az egyik portot lekapcsoltuk. Ebből arra következtetünk, hogy a port összevonásunk működik hiba nélkül.

## Portbiztonság

A portbiztonság tesztelésénél először bemutatjuk a hálózati szegmenst ahol a támadást szimuláljuk, bemutatjuk a portvédelem állapotát, végrehajtjuk a támadást, aztán pedig ellenőrizzük a portvédelem állapotát.

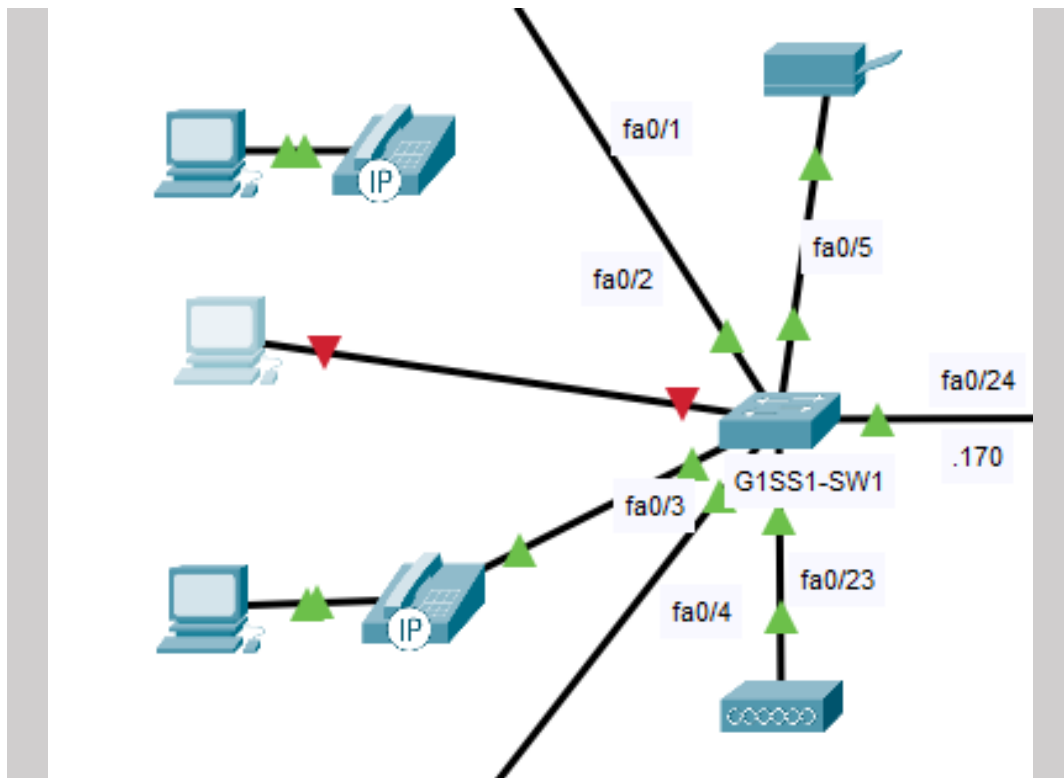


A fenti hálózat részen fogunk port sértést szimulálni. A kapcsoló használatban levő portjain, amire telefonok vannak csatlakoztatva, 2 MAC cím megtanulása volt engedélyezve, illetve ezeket a MAC címeket a kapcsoló meg is tanulta, és hogyha másik eszköz másik fizikai címmel csatlakozna, a portot letiltja.

```
G1SS1-SW1(config)#do show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	2	2	0	Shutdown
Fa0/2	2	2	0	Shutdown
Fa0/3	2	2	0	Shutdown
Fa0/4	2	2	0	Shutdown

A parancs kimenetén látszik, hogy a beállított 2 címet a kapcsoló meg is tanulta.



Az FastEthernet0/2 port kábelét kihúzzuk a kapcsolóból, és egy idegen számítógépre csatlakoztatjuk, és kérünk DHCP-vel címet a gépen.

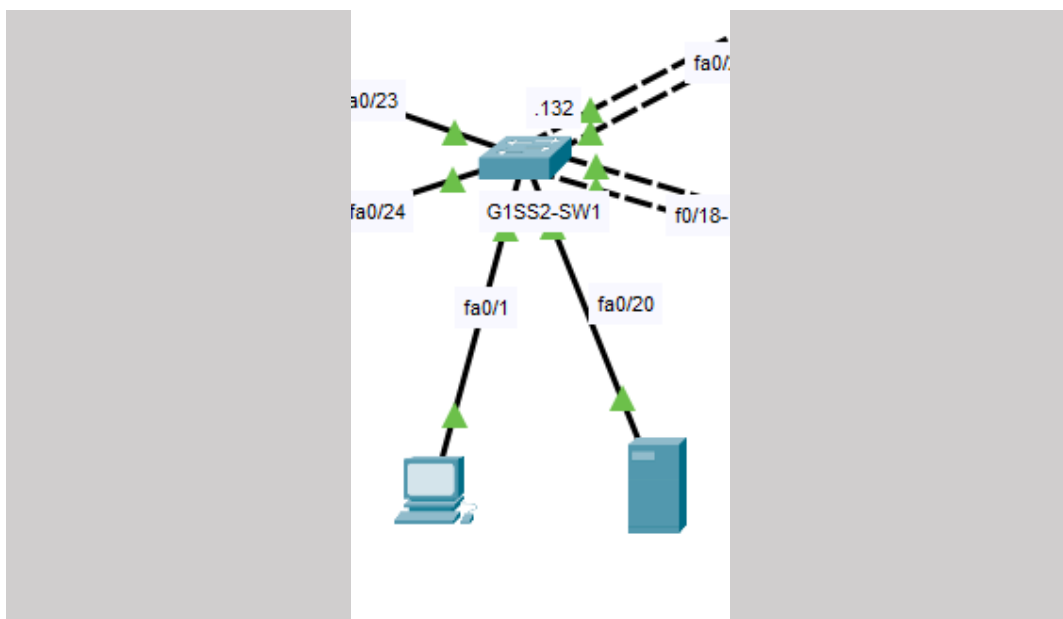
```
G1SS1-SW1#show port-security interface fa0/2
Port Security                : Enabled
Port Status                   : Secure-shutdown
Violation Mode                 : Shutdown
Aging Time                     : 0 mins
Aging Type                     : Absolute
SecureStatic Address Aging    : Disabled
Maximum MAC Addresses         : 2
Total MAC Addresses           : 2
Configured MAC Addresses      : 0
Sticky MAC Addresses          : 2
Last Source Address:Vlan      : 0001.97C0.1284:20
Security Violation Count      : 1
```

Mint látható a port automatikusan lekapcsolódik, hiszen ez a MAC cím nem volt a megtanultak listájában.



## STP (Spanning Tree Protocol)

Az STP tesztelésénél először bemutatjuk a hálózati szegmenst ahol a támadást szimuláljuk, bemutatjuk az STP állapotát, végrehajtjuk a támadást, aztán pedig ellenőrizzük a portvédelem állapotát.



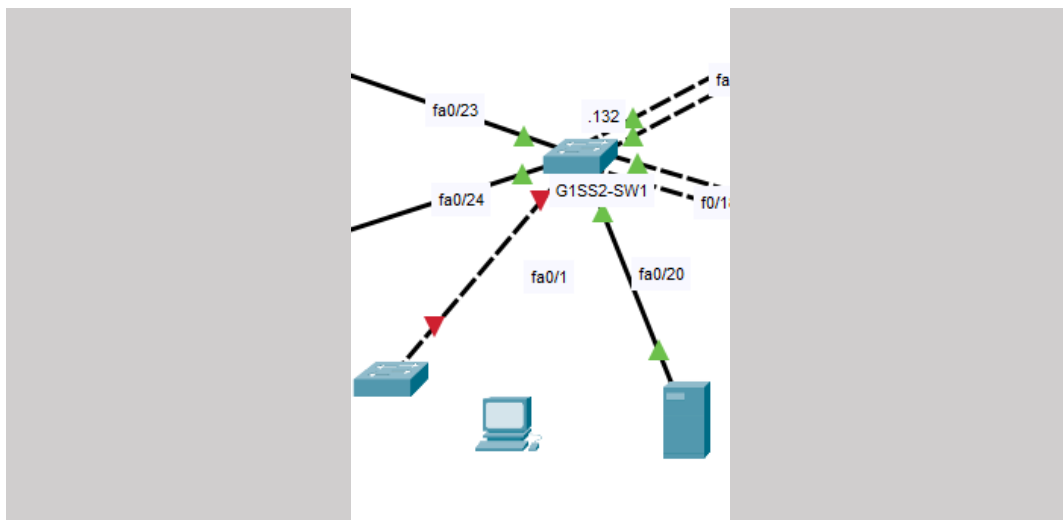
A képen látható hálózat részen fogjuk a támadást szimulálni. A kapcsoló használatban levő Fast Ethernet 0/1 -es portján, amire egy gép van csatlakoztatva.

```
G1SS2-SW1(config)#do show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: Dolgozok_Data management VOICE wireless
Extended system ID      is enabled
Portfast Default         is enabled
Portfast BPDU Guard Default is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default        is disabled
EtherChannel misconfig guard is disabled
UplinkFast               is disabled
BackboneFast              is disabled
Configured Pathcost method used is short
```

Name	Blocking	Listening	Learning	Forwarding	STP Active
VLAN0001	9	0	0	1	10
VLAN0010	7	0	0	3	10
VLAN0030	4	0	0	6	10
VLAN0040	6	0	0	4	10
VLAN0050	6	0	0	4	10
5 vlans	32	0	0	18	50

A kapcsolón a kiadott parancs megmutatja a kapcsoló mostani STP állapotát, amely mutatja, hogy az eszköz rapid-pvst módot használ, amely gyors konvergenciát biztosít, továbbá az is látható, hogy az eszköz a Root Bridge szerepet tölti be az összes VLAN esetében (Dolgozok\_Data, management, VOICE, wireless).

Az eszközön a Portfast engedélyezve van így az eszközhöz csatlakozó portok gyorsan továbbító állapotba kerülnek, továbbá a BPDU Guard is bekapcsolt állapotban van így, ha egy új kapcsolót csatlakoztatnak az eszközhöz az azonnal letiltja azt a portját, ahol összeköttették őket. Az utóbbit teszteljük is le.



A képen látható módon a Fast Ethernet 0/1-es portjából eltávolítjuk a számítógépet és összeköttetjük egy másik kapcsolóval.

```
G1SS2-SW1(config)#do show interface status
Port      Name      Status      Vlan      Duplex  Speed Type
Po1        Po1        connected   trunk     auto    auto
Po2        Po2        connected   trunk     auto    auto
Fa0/1      Fa0/1      err-disabled 30        auto    auto  10/100BaseTX

G1SS2-SW1(config)#do show interface fa0/1
FastEthernet0/1 is down, line protocol is down (err-disabled)
```

A képeken látható parancsok kiadásával megbizonyosodhatunk, hogy a port egyből le is tiltódik.

# Harmadik rétegbeli megvalósítások

## HSRP

A HSRP tesztelésénél először bemutatjuk a hálózati szegmenst ahol a kiesést szimuláljuk, bemutatjuk az HSRP állapotát, végrehajtjuk a meghibásodást, aztán pedig ellenőrizzük, hogy sikeresen átvette-e az R3 az R1 től az active szerepet.

```
G1SS1-R1#show standby
FastEthernet0/1.10 - Group 1
  State is Active
  Virtual IP address is 192.168.1.3
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.2
  Priority 150 (configured 150)
FastEthernet0/1.30 - Group 2
  State is Active
  Virtual IP address is 192.168.1.163
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.162
  Priority 150 (configured 150)
FastEthernet0/1.40 - Group 3
  State is Active
  Virtual IP address is 192.168.1.35
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.34
  Priority 150 (configured 150)
FastEthernet0/1.50 - Group 4
  State is Active
  Virtual IP address is 192.168.1.147
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.146
  Priority 150 (configured 150)
G1SS1-R1#
```

A képen látható a HSRP állapota az R1 -n. Látszik hogy az R1 az active forgalomirányító.



```
FastEthernet0/0.10 - Group 1
  State is Standby
  Virtual IP address is 192.168.1.3
  Preemption disabled
  Active router is 192.168.1.1
  Priority 100 (default 100)
FastEthernet0/0.30 - Group 2
  State is Standby
  Virtual IP address is 192.168.1.163
  Preemption disabled
  Active router is 192.168.1.161
  Priority 100 (default 100)
FastEthernet0/0.40 - Group 3
  State is Standby
  Virtual IP address is 192.168.1.35
  Preemption disabled
  Active router is 192.168.1.33
  Priority 100 (default 100)
FastEthernet0/0.50 - Group 4
  State is Standby
  Virtual IP address is 192.168.1.147
  Preemption disabled
  Active router is 192.168.1.145, priority 150
  Priority 100 (default 100)
```

A képen látható a HSRP állapota az R2 -n. Látszik hogy R2 a standby forgalomirányító.

```
C:\>tracert 192.168.1.131

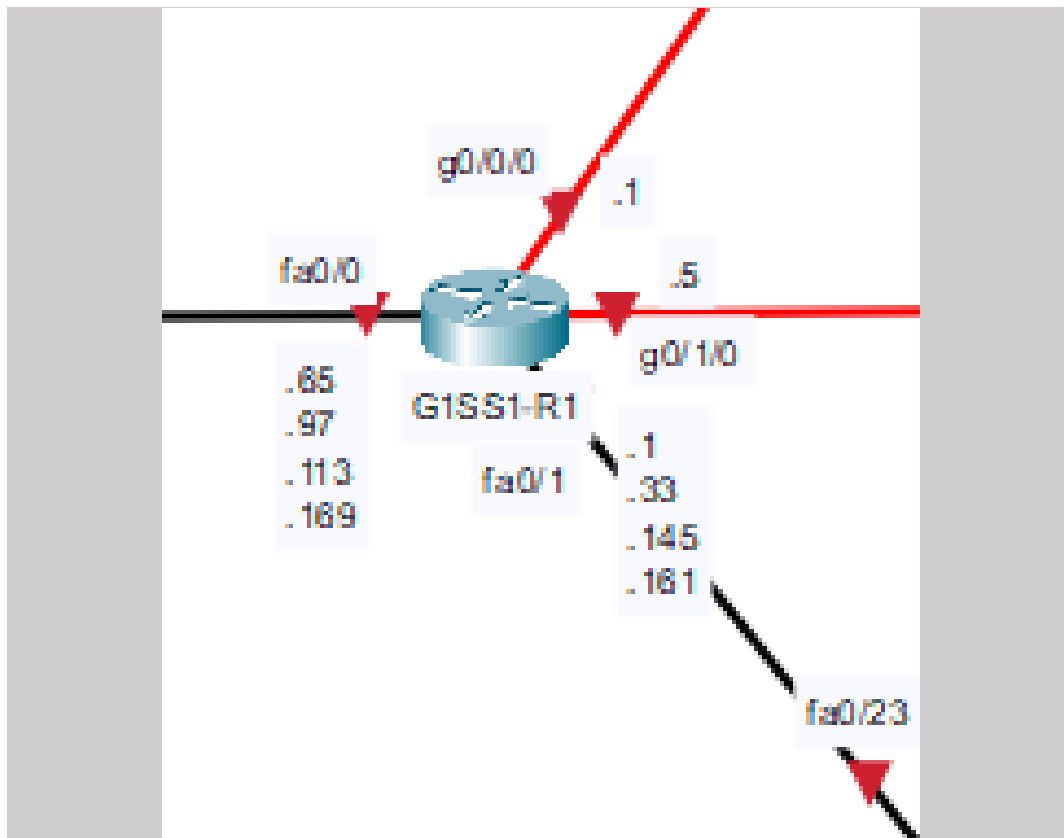
Tracing route to 192.168.1.131 over a maximum of 30 hops:

  1  0 ms      0 ms      0 ms      192.168.1.1
  2  0 ms      0 ms      0 ms      10.0.0.2
  3  7 ms      0 ms      0 ms      192.168.1.131

Trace complete.

C:\>
```

A hálózat egyik gépéről küldünk egy pinget a belső szervernek, mint látszik a tracert parancsnak köszönhetően a csomag az R1 (192.168.1.1) felé távozott.



Az R1 forgalomirányítót lekapcsolt állapotba tesszük és megismételjük az előző folyamatot.

```
C:\>tracert 192.168.1.131

Tracing route to 192.168.1.131 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.1.2
  2  0 ms    0 ms    0 ms    10.0.0.9
  3  0 ms    0 ms    0 ms    192.168.1.131

Trace complete.

C:\>
```

Az előzőekben használt gépről küldünk egy pinget a belső szervernek, mint látszik a csomag az R3 (192.168.1.2) felé távozott és az R3 átvette az R1 től az active szerpet.

## OSPF

A forgalomirányítók között OSPF protokollt használtunk, hogy az üzenetek mindig a leggyorsabb útvonalon jussanak célba. A protokoll mellett szól az is, hogy dinamikusan tanítják meg egymásnak a betanult hálózatokat, ezzel skálázhatóvá teszi az egész hálózatot.

A forgalomirányítók konfigurálása után kialakultak a szomszédsági kapcsolatok minden nem passzív interfészen.

```
G1SS1-R3#sh ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.1.1	1	FULL/BDR	00:00:32	192.168.1.1	FastEthernet0/0.10
1.1.1.1	1	FULL/BDR	00:00:33	10.0.0.5	GigabitEthernet0/1/0
1.1.1.1	1	FULL/BDR	00:00:32	192.168.1.161	FastEthernet0/0.30
1.1.1.1	1	FULL/BDR	00:00:33	192.168.1.33	FastEthernet0/0.40
1.1.1.1	1	FULL/BDR	00:00:32	192.168.1.145	FastEthernet0/0.50

A forgalomirányítók miután egyeztették az interfészeken a szomszédokat „Hello” üzenetekkel, elkezdtek hirdetni a kapcsolt hálózataikat, majd megtanulni a másik által osztottat.

Minden határforgalomirányítón statikusan állítottuk be az útvonalat az Internet felé. Ezt is hirdetik a többi felé, hogy tudják, ha ki akarnak menni az ISP felé, akkor rajtuk át vezet az út.

```
Gateway of last resort is 22.22.22.2 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O   10.0.0.0/30 [110/2] via 10.0.0.5, 00:43:13, GigabitEthernet0/1/0
C   10.0.0.4/30 is directly connected, GigabitEthernet0/1/0
L   10.0.0.6/32 is directly connected, GigabitEthernet0/1/0
C   10.0.0.8/30 is directly connected, GigabitEthernet0/0/0
L   10.0.0.10/32 is directly connected, GigabitEthernet0/0/0
 22.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   22.22.22.0/30 is directly connected, GigabitEthernet0/2/0
L   22.22.22.1/32 is directly connected, GigabitEthernet0/2/0
 192.168.1.0/24 is variably subnetted, 13 subnets, 5 masks
C   192.168.1.0/27 is directly connected, FastEthernet0/0.10
L   192.168.1.2/32 is directly connected, FastEthernet0/0.10
C   192.168.1.32/27 is directly connected, FastEthernet0/0.40
L   192.168.1.34/32 is directly connected, FastEthernet0/0.40
O   192.168.1.64/27 [110/11] via 10.0.0.5, 00:43:13, GigabitEthernet0/1/0
O   192.168.1.96/28 [110/11] via 10.0.0.5, 00:43:13, GigabitEthernet0/1/0
O   192.168.1.112/28 [110/11] via 10.0.0.5, 00:43:13, GigabitEthernet0/1/0
O   192.168.1.128/28 [110/12] via 10.0.0.5, 00:43:03, GigabitEthernet0/1/0
C   192.168.1.144/28 is directly connected, FastEthernet0/0.50
L   192.168.1.146/32 is directly connected, FastEthernet0/0.50
C   192.168.1.160/29 is directly connected, FastEthernet0/0.30
L   192.168.1.162/32 is directly connected, FastEthernet0/0.30
O   192.168.1.168/30 [110/11] via 10.0.0.5, 00:43:13, GigabitEthernet0/1/0
S*  0.0.0.0/0 [1/0] via 22.22.22.2
```

## OSPF Hitelesítés

Hitelesítéssel védjük az OSPF által használt hirdető interfészeket, hogy a jelszavakat kódolva lássa a hálózatba illetéktelenül behatoló. Az alábbi show parancsok utolsó sorai írják, hogy a hitelesítés be van kapcsolva és jelszó kell hozzá.

```
GlSSL-R1#sh ip ospf interface g0/1/0

GigabitEthernet0/1/0 is up, line protocol is up
 Internet address is 10.0.0.5/30, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State BDR, Priority 1
 Designated Router (ID) 3.3.3.3, Interface address 10.0.0.6
 Backup Designated Router (ID) 1.1.1.1, Interface address 10.0.0.5
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:07
 Index 2/2, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
   Adjacent with neighbor 3.3.3.3 (Designated Router)
 Suppress hello for 0 neighbor(s)
 Message digest authentication enabled
   Youngest key id is 1
GlSSL-R1#sh ip ospf interface g0/0/0

GigabitEthernet0/0/0 is up, line protocol is up
 Internet address is 10.0.0.1/30, Area 0
 Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State BDR, Priority 1
 Designated Router (ID) 2.2.2.2, Interface address 10.0.0.2
 Backup Designated Router (ID) 1.1.1.1, Interface address 10.0.0.1
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:02
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1, Adjacent neighbor count is 1
   Adjacent with neighbor 2.2.2.2 (Designated Router)
 Suppress hello for 0 neighbor(s)
 Message digest authentication enabled
   Youngest key id is 1
```

## NAT

A NAT tesztelésénél először bemutatjuk a forgalomirányító alap NAT statisztikáit, ahol a tesztet szimuláljuk, bemutatjuk az NAT állapotát, végrehajtjuk a csomagküldést, aztán pedig ellenőrizzük, hogy sikeres lett-e a címfordítás, viszont mindennek előtt nézzük meg a hozzáférési listát, amely a címeket tartalmazza, amiket a forgalomirányító átfordít.

```
G1SS1-R3(config)#do show access-lists
Standard IP access list 1
 10 permit 192.168.1.0 0.0.0.31
 20 permit 192.168.1.32 0.0.0.31 (2 match(es))
 30 permit 192.168.1.144 0.0.0.15 (2 match(es))
 40 permit 192.168.1.160 0.0.0.7
 50 permit 192.168.1.64 0.0.0.31
 60 permit 192.168.1.96 0.0.0.15 (8 match(es))
 70 permit 192.168.1.112 0.0.0.15
 80 permit 192.168.1.168 0.0.0.7
 90 permit 192.168.1.128 0.0.0.15
100 permit 10.0.0.8 0.0.0.3
110 permit 10.0.0.4 0.0.0.3
120 permit 10.0.0.0 0.0.0.3
130 deny any (58 match(es))
```

```
Gateway of last resort is 22.22.22.2 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O   10.0.0.0/30 [110/2] via 10.0.0.9, 00:04:23, GigabitEthernet0/2/0
    [110/2] via 10.0.0.5, 00:04:23, GigabitEthernet0/1/0
C   10.0.0.4/30 is directly connected, GigabitEthernet0/1/0
L   10.0.0.6/32 is directly connected, GigabitEthernet0/1/0
C   10.0.0.8/30 is directly connected, GigabitEthernet0/2/0
L   10.0.0.10/32 is directly connected, GigabitEthernet0/2/0
 22.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   22.22.22.0/30 is directly connected, GigabitEthernet0/0/0
L   22.22.22.1/32 is directly connected, GigabitEthernet0/0/0
192.168.1.0/24 is variably subnetted, 13 subnets, 5 masks
C   192.168.1.0/27 is directly connected, FastEthernet0/0.10
L   192.168.1.2/32 is directly connected, FastEthernet0/0.10
C   192.168.1.32/27 is directly connected, FastEthernet0/0.40
L   192.168.1.34/32 is directly connected, FastEthernet0/0.40
O   192.168.1.64/27 [110/11] via 10.0.0.5, 00:04:23, GigabitEthernet0/1/0
O   192.168.1.96/28 [110/11] via 10.0.0.5, 00:04:23, GigabitEthernet0/1/0
O   192.168.1.112/28 [110/11] via 10.0.0.5, 00:04:23, GigabitEthernet0/1/0
O   192.168.1.128/28 [110/11] via 10.0.0.9, 00:04:23, GigabitEthernet0/2/0
C   192.168.1.144/28 is directly connected, FastEthernet0/0.50
L   192.168.1.146/32 is directly connected, FastEthernet0/0.50
C   192.168.1.160/29 is directly connected, FastEthernet0/0.30
L   192.168.1.162/32 is directly connected, FastEthernet0/0.30
O   192.168.1.168/30 [110/11] via 10.0.0.5, 00:04:23, GigabitEthernet0/1/0
S*  0.0.0.0/0 [1/0] via 22.22.22.2
```

```
G1SS1-R3(config)#do show ip nat statistics
Total translations: 2 (2 static, 0 dynamic, 1 extended)
Outside Interfaces: GigabitEthernet0/0/0
Inside Interfaces: FastEthernet0/0 , GigabitEthernet0/1/0 , GigabitEthernet0/2/0 ,
FastEthernet0/0.10 , FastEthernet0/0.30 , FastEthernet0/0.40 , FastEthernet0/0.50
Hits: 0 Misses: 6
Expired translations: 0
```



A képeken látható a G1SS1-R3 forgalomirányítónak a routing táblája illetve a NAT statisztikái

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 22.22.22.6

Pinging 22.22.22.6 with 32 bytes of data:

Reply from 22.22.22.6: bytes=32 time=2ms TTL=252
Reply from 22.22.22.6: bytes=32 time=2ms TTL=252
Reply from 22.22.22.6: bytes=32 time=2ms TTL=252
Reply from 22.22.22.6: bytes=32 time=2ms TTL=252

Ping statistics for 22.22.22.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

Küldünk egy ping csomagot egy külső címre, az egyik eszközünkről.

```
G1SS1-R3(config)#do show ip nat statistics
Total translations: 4 (2 static, 2 dynamic, 3 extended)
Outside Interfaces: GigabitEthernet0/0/0
Inside Interfaces: FastEthernet0/0 , GigabitEthernet0/1/0 , GigabitEthernet0/2/0 ,
FastEthernet0/0.10 , FastEthernet0/0.30 , FastEthernet0/0.40 , FastEthernet0/0.50
Hits: 7 Misses: 79
Expired translations: 4
Dynamic mappings:
```

At Device: G1SS1-R3	
Source: PC5(2)	
Destination: ISP2	
In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.1.98, Dest. IP: 22.22.22.6 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 22.22.22.1, Dest. IP: 22.22.22.6 ICMP Message Type: 8
Layer 2: Ethernet II Header 00D0.17A0.226D >> 00D0.BA45.2348	Layer 2: Ethernet II Header 00D0.BCC9.1663 >> 0001.9791.4D5A
Layer 1: Port GigabitEthernet0/1/0	Layer 1: Port(s): GigabitEthernet0/0/0

Újra megnézzük a NAT statisztikákat és láthatjuk hogy a csomag sikeresen átment és a forgalomirányító átfordította a belső címet külső címmé.

## Tűzfalak

A tűzfalunk lényege, hogy a Vendég hálózatba tartozók ne tudják elérni a belső szervereket, csakis IP címet kapjanak a DHCP-től.

Ennek a tesztelésnek az első lépése, hogy megnézzük a gép kap-e DHCP-vel címet.

```
C:\>ipconfig /release

IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway...: 0.0.0.0
DNS Server.....: 0.0.0.0

C:\>ipconfig /renew

IP Address.....: 192.168.1.148
Subnet Mask.....: 255.255.255.240
Default Gateway...: 192.168.1.145
DNS Server.....: 192.168.1.131
```

Látjuk, hogy a DHCP-vel kapott cím eldobása és újra kérése után is kap címet, így arra következtetünk, hogy a tűzfalunknak ez a beállítása helyesen működik. Mostmár csak azt kell tesztelnünk, hogy a PING parancs elér-e a szervert, illetve WEB-en elér-e a szervert.

```
C:\>ping 192.168.1.131

Pinging 192.168.1.131 with 32 bytes of data:

Reply from 192.168.1.145: Destination host unreachable.
Reply from 192.168.1.145: Destination host unreachable.
Reply from 192.168.1.145: Destination host unreachable.
Reply from 192.168.1.145: Destination host unreachable.

Ping statistics for 192.168.1.131:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



Látjuk, hogy sem a PING, sem a WEB kérés nem éri el a szervert. A működés érdekében teszteljünk ezt egy nem tiltott gépről.



```
C:\>ping 192.168.1.131

Pinging 192.168.1.131 with 32 bytes of data:

Reply from 192.168.1.131: bytes=32 time=65ms TTL=128
Reply from 192.168.1.131: bytes=32 time=7ms TTL=128
Reply from 192.168.1.131: bytes=32 time=9ms TTL=128
Reply from 192.168.1.131: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.1.131:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```



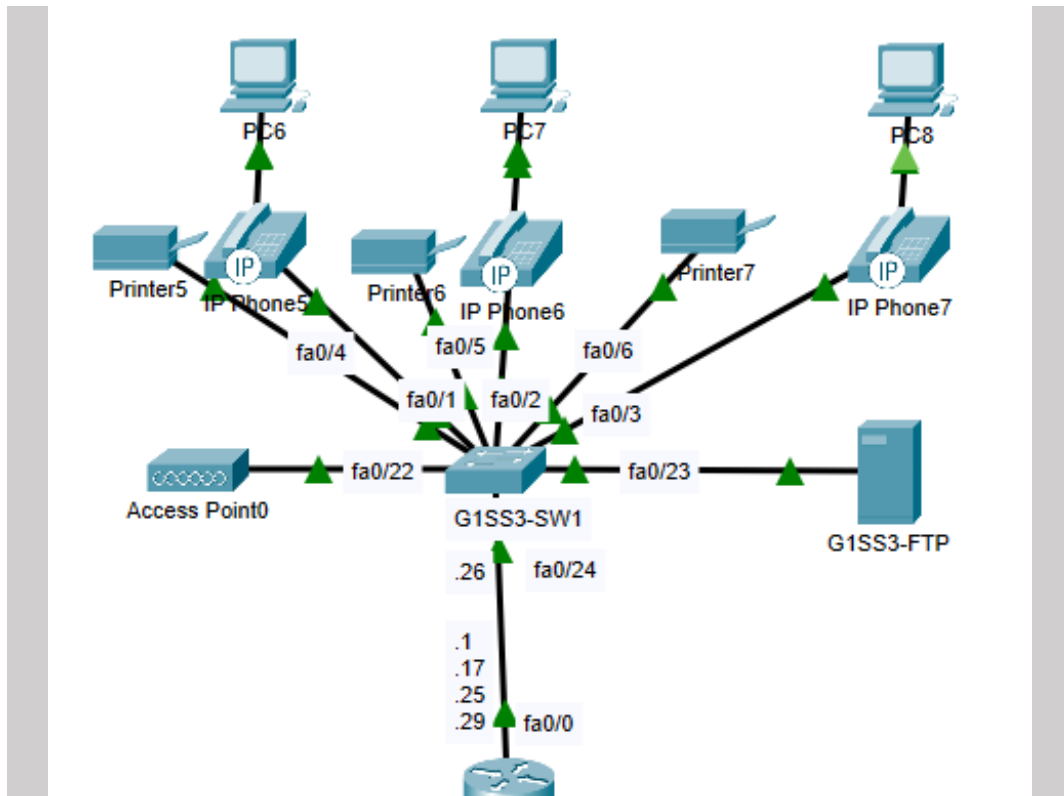
Végezetül látszik, hogy egy másik hálózatban levő gépről ezek a kérések működnek.

## Port Továbbítás

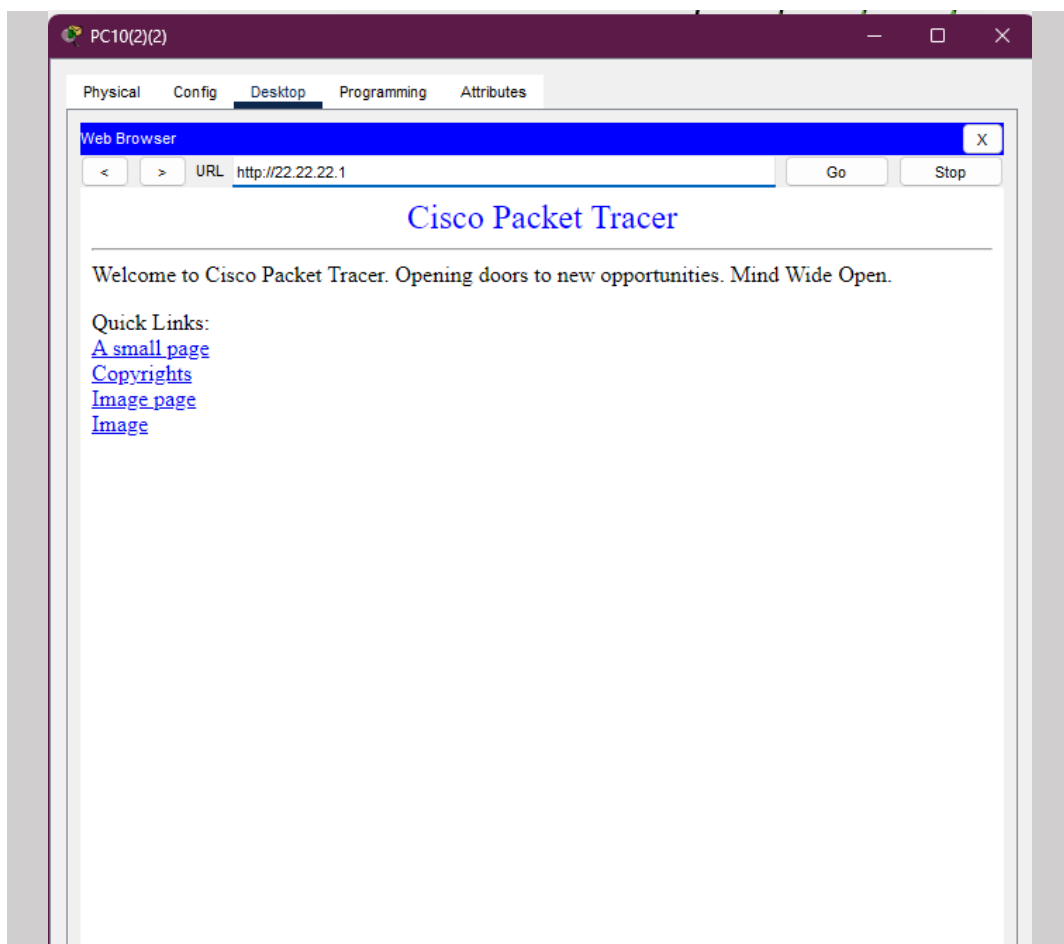
A Port továbbítás tesztelésénél egy külső hálózathoz (G1SS3) megpróbáljuk elérni a belső hálózat (G1SS1) webszerverét a G1SS1-R3 külső címének lekérdezésével.

```
ip nat inside source static tcp 192.168.1.132 80 22.22.22.1 80
ip nat inside source static tcp 192.168.1.132 443 22.22.22.1 443
```

Először is nézzük meg a beállított statikus nat-ot, amely a forgalomirányító külső címére érkező kéréseket a 80 és 443-as porton továbbítja a szerver megfelelő portjára.



Utána a külső siteon bejelentkezünk a PC-be és belemegyünk a web browserbe.



Majd beírjuk a G1SS1-R3 külső címet jelen esetben a 22.22.22.1 -es címet és megjelenik az 1-es sítón lévő webszerver weboldala.

```
G1SS1-R3#sh ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
tcp  22.22.22.1:443      192.168.1.132:443 ---                ---
tcp  22.22.22.1:443      192.168.1.132:443 22.22.22.10:1033   22.22.22.10:1033
tcp  22.22.22.1:80       192.168.1.132:80   ---                ---
tcp  22.22.22.1:80       192.168.1.132:80   22.22.22.10:1025   22.22.22.10:1025
tcp  22.22.22.1:80       192.168.1.132:80   22.22.22.10:1026   22.22.22.10:1026
```

Lekérdezzük a fordítótábláját a G1SS1-R3 -nak és láthatjuk, hogy a beérkező kérést továbbította a forgalomirányító a szervernek.

## SSH (Secure Shell Protokoll)

Az SSH tesztelésének egyetlen lépése van, a konfigurációt követően egy számítógép Parancssorából indítunk egy SSH csatlakozást az adott eszköz felé a következő paranccsal:

```
C:\>ssh -l admin 192.168.1.1
```

Ezt követően a megfelelő jelszóval bejelentkezünk, és hogyha minden sikerült, a hálózati eszközt promt-ját kell lássuk a számítógépen levő „C:\>” helyett.

```
Password:
```

```
G1SS1-R1>
```

Ezt követően hogyha elvégeztük a dolgunkat az eszközön csak egy exit paranccsal kilépünk.

```
G1SS1-R1>exit
```

```
[Connection to 192.168.1.1 closed by foreign host]
C:\>
```

A tesztelésből látszik, hogy a konfigurált SSH protokoll működik.

## Tunnel

Az Ipv6 os alagút tesztelésénél először megnézzük a az ipv6 os interface-einket továbbá az alagutat és az ipv6 os routing táblát. Utána megpróbáljuk elérni a másik telephelyen található ipv6 os címmel rendelkező számítógépet, majd ellenőrizzük hogy hogy történt a címfordítás.

```
G1SS1-R3(config)#do show ipv6 interface brief
FastEthernet0/1          [up/up]
    FE80::1
    2011::1
GigabitEthernet0/0/0     [up/up]
    unassigned
GigabitEthernet0/1/0     [up/up]
    unassigned
GigabitEthernet0/2/0     [up/up]
    unassigned
GigabitEthernet0/3/0     [administratively down/down]
    unassigned
FastEthernet1/0          [administratively down/down]
    unassigned
FastEthernet1/1          [administratively down/down]
    unassigned
Tunnell                  [up/up]
    FE80::230:F2FF:FE76:1A1C
    2001::1
```

A képen látható a G1SS1-R3 határ forgalomirányító ipv6 os interface-ei. A FastEthernet0/1 és a Tunnell. Leolvasható az interface-ek ip címei és link local címei.

```
G1SS1-R3(config)#do show ipv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C    2001::/126 [0/0]
    via Tunnell, directly connected
L    2001::1/128 [0/0]
    via Tunnell, receive
C    2011::/64 [0/0]
    via FastEthernet0/1, directly connected
L    2011::1/128 [0/0]
    via FastEthernet0/1, receive
R    2012::/64 [120/2]
    via FE80::2E0:8FFF:FE8D:ED15, Tunnell
L    FF00::/8 [0/0]
    via Null0, receive
```

A képen a forgalomirányító ipv6-os routing táblája látható jól leolvasható hogy a Lokális (L), hozzacsatlakoztatott (C), illetve RIP (R) által megtanult útvonalak vannak.

```
G1SS1-R3(config)#do show ipv6 interface Tunnell
Tunnell is up, line protocol is up
IPv6 is enabled, link-local address is FE80::230:F2FF:FE76:1A1C
Global unicast address(es):
  2001::1, subnet is 2001::/126
```

A képen a Tunnell interface-t láthatjuk. Leolvasható az ipv6 os címe illetve a link local címe.

```
C:\>ping 2012::2

Pinging 2012::2 with 32 bytes of data:

Reply from 2012::2: bytes=32 time=2ms TTL=126
Reply from 2012::2: bytes=32 time=1ms TTL=126
Reply from 2012::2: bytes=32 time=8ms TTL=126
Reply from 2012::2: bytes=32 time=1ms TTL=126

Ping statistics for 2012::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 3ms
```

Most megpróbáljuk elérni az első telephely Ipv6 -os hálózat számítógépéről a második telephely számítógépét és mint láthatjuk az eléérés sikeres.

PDU Information at Device: G1SS1-R3

OSI Model    Inbound PDU Details    Outbound PDU Details

At Device: G1SS1-R3  
Source: PC9  
Destination: PC10

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IPv6 Header Src. IP: 2011::2, Dest. IP: 2012::2 ICMPv6 Echo Message Type: 128	Layer 3: IP Header Src. IP: 22.22.22.1, Dest. IP: 22.22.22.5 IPv6 Header Src. IP: 2011::2, Dest. IP: 2012::2 ICMPv6 Echo Message Type: 128
Layer 2: Ethernet II Header 00E0.8F04.599C >> 00D0.FF90.9C48	Layer 2: Ethernet II Header 00D0.BCC9.1663 >> 0001.9791.4D5A
Layer 1: Port FastEthernet0/1	Layer 1: Port(s): GigabitEthernet0/0/0

Ezen a képen a címfordítást láthatjuk hogy a határ forgalomírányító a belső ipv6 -os címet egy ipv4 es csomagban szállítja át a másik telephely számítógépe felé.

## IP telefonok

Az IP telefonok tesztelése azzal kezdődik, hogy ellenőrizzük, hogy a telefonok kaptak IP címet a DHCP szervertől. Látszik hogy a helyes beállításokkal megkapja az IP címet, és a telefon beállított számát is.

```
Device Name: IP Phone4(1)
Device Model: 7960

Port      Link      IP Address      MAC Address
Vlan1     Down     <not set>       0001.4363.A876
Switch    Up       <not set>       0030.F2B3.76D4
PC         Up       <not set>       000C.8553.7AC1
Vlan40     Up       192.168.1.114/28 0001.4363.A876

Gateway: 192.168.1.113
Line Number: 100
```

A következő lépés, hogy felhívjuk a másik hálózatban levő 200-as számú telefont.

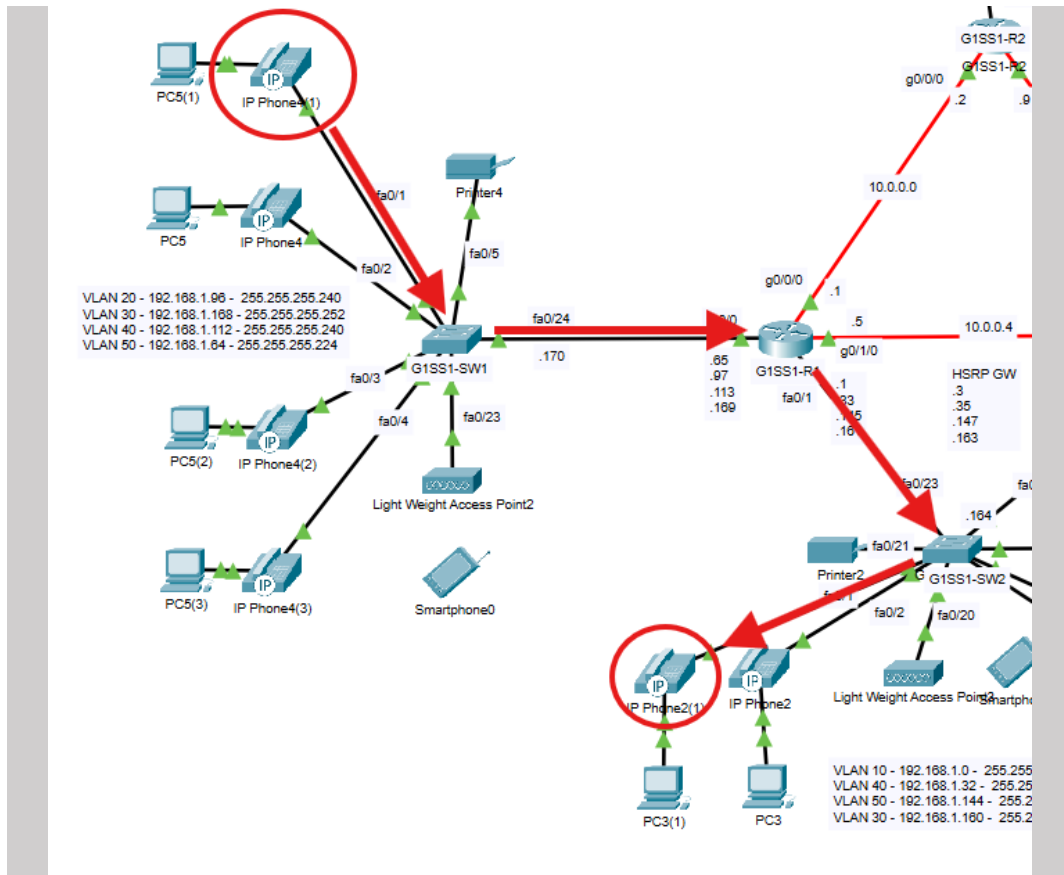


Látszik, hogy a 100-as hívja a 200-ast, a 200-on kiírja, hogy hívás érkezik a 100-as telefonról, és csörög.



Látszik, hogy ha felvesszük, a két telefon csatlakozik. Az utolsó képen pedig látszik, hogy ez a két telefon valóban külön hálózatokban van, és a kijelölt útvonalon el is éri egymást.





## WEB-VPN

Az ASA eszközön kialakított WEB-VPN szolgáltatás teszteléséhez először ellenőrizzük az ASÁN létrehozott Bookmark Managert, és hozzá rendelt User Managert.

Bookmark Title	URL
web	http://192.168.1.2

User Manager

Username

admin

Bookmark

web

Profile Name

adminprofil

Group Policy

admingroup

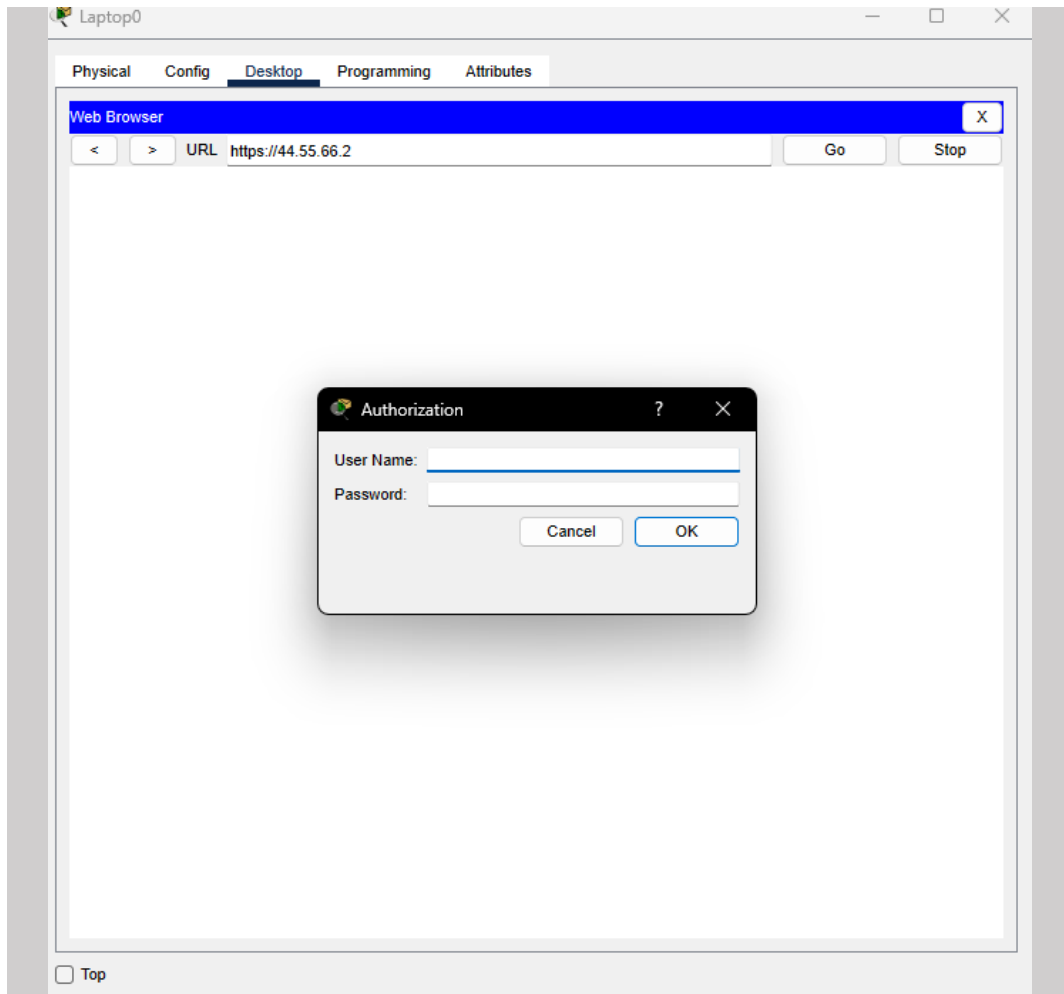
Set

Users

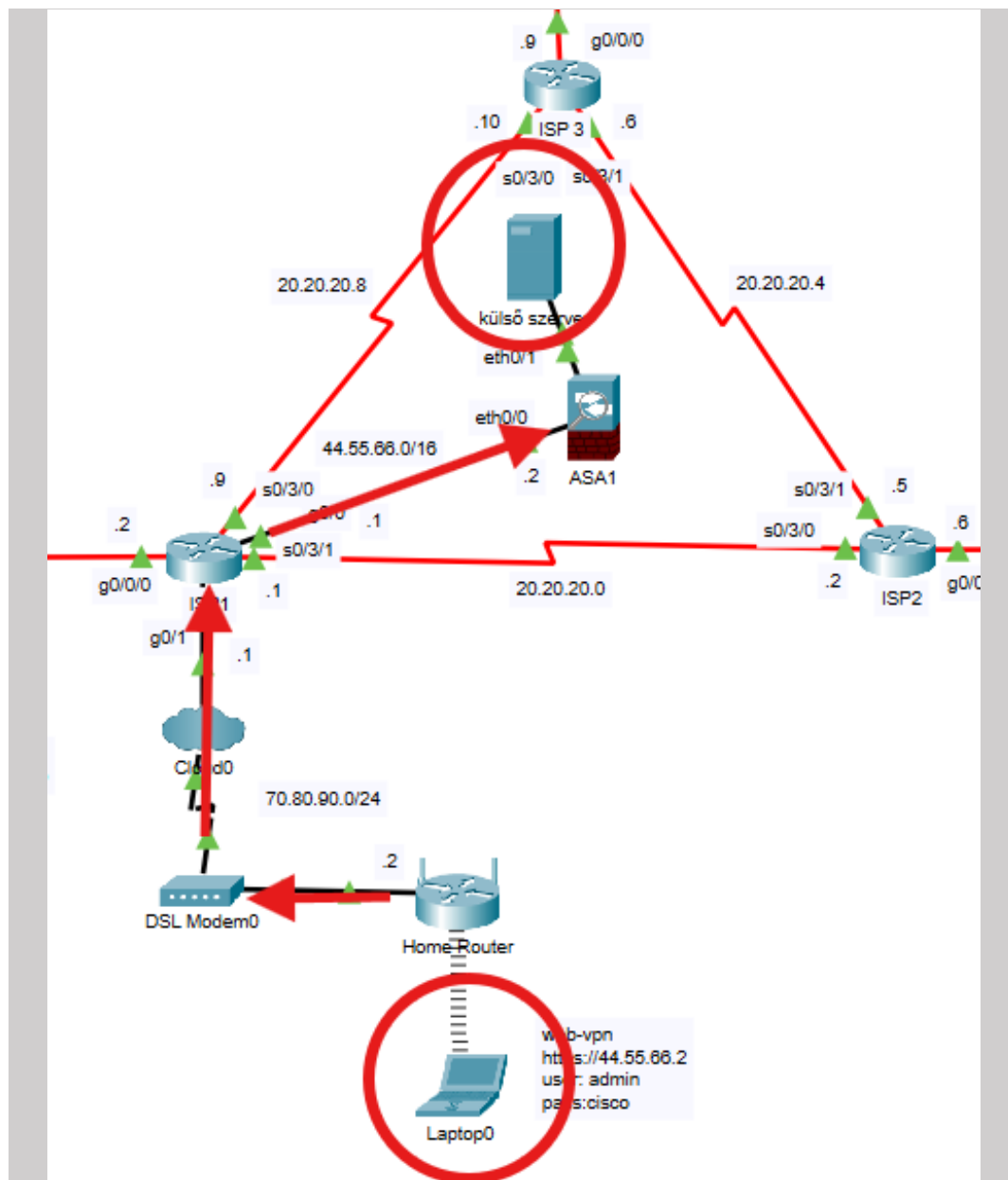
Username	Bookmark	Profile Name	Group Policy
admin	web	adminprofil	admingroup

Miután ezt ellenőriztük és helyes, az otthoni gépről beírjuk az ASA külső interfészének az IP címét a böngészőbe, és az ASÁN megadott bejelentkezési adatokkal bejelentkezünk.



Ezek után látszik, hogy sikeresen bejelentkeztünk az ASA WEB-VPN segítségével.





A fenti képen látható az útvonal, amit bejártunk a klienstől a belső ASA által védett szerverig.

# BGP

A BGP tesztelése egyúttal az internet szimulálásának a tesztelése. A lényeg, hogy sikeresen szimuláljuk a szolgáltató hálózatát, hogy pontosan tudjuk bemutatni a belső hálózatok közti kommunikációt.

Az alábbi paranccsal először megnézzük az egyes ISP BGP szomszédait. Látszik, hogy ott van a két másik ISP, illetve a pontos szimuláció érdekében, akár csak a szolgáltatómál, másik AS-be kerültek.

```
ISP-1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 65001

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
20.20.20.2    4 65002   72     63     14    0   0 01:01:34      4
20.20.20.10   4 65003   72     62     14    0   0 01:00:41      4
```

A következő parancsban látszik a BGP által hirdetett, és más ISP-től kapott hálózatok, illetve útvonalak. A nyíl mutatja, hogy melyik hálózat felé melyik a legjobb Next Hop.

```
ISP-1#show ip bgp
BGP table version is 21, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Next Hop        Metric LocPrf Weight Path
*> 20.20.20.0/30   0.0.0.0          0         0 32768 i
*                  20.20.20.2          0         0   0 65002 i
*                  20.20.20.10         0         0   0 65003 65002 i
* 20.20.20.4/30    20.20.20.2          0         0   0 65002 i
*>                  20.20.20.10         0         0   0 65003 i
*> 20.20.20.8/30   0.0.0.0          0         0 32768 i
*                  20.20.20.2          0         0   0 65002 65003 i
*                  20.20.20.10         0         0   0 65003 i
*                  20.20.20.10         0         0   0 65003 i
*> 22.22.22.0/30   0.0.0.0          0         0 32768 i
*> 22.22.22.4/30    20.20.20.2          0         0   0 65002 i
*                  20.20.20.10         0         0   0 65003 65002 i
*> 22.22.22.8/30    20.20.20.10         0         0   0 65003 i
*                  20.20.20.2          0         0   0 65002 65003 i
```

A végső lépés a működés tesztelése, ezt egy **traceroute** paranccsal tesszük meg.

```
ISP-3#traceroute 22.22.22.1
Type escape sequence to abort.
Tracing the route to 22.22.22.1

 1 20.20.20.9 228 msec 943 msec 957 msec
 2 22.22.22.1 976 msec 929 msec 954 msec
ISP-3#
```

Látszik, hogy a traceroute elmegy az egyes ISP-hez, majd az ISP továbbítja az egyes telephely határ forgalomirányítójának.

# WLC

A WLC teszteléséhez először megnézzük, hogy az alap beállítások után „https://” -el be tudunk-e jelentkezni az eszközbe.



Bejelentkezés után a WLAN fülön ellenőrizzük a vezeték nélküli hálózatok meglétét.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK						
WLANs						
Current Filter: <a href="#">[Change Filter]</a> <a href="#">[Clear Filter]</a> <span>Create New</span> <span>Go</span>						
<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/>	1	WLAN	VLAN 10 Dolgozok	Dolgozok	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	2	WLAN	VLAN 20 Vezetoseg	Vezetoseg	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	3	WLAN	VLAN 30 management	Management	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	4	WLAN	VLAN 40 Guest	Vendég	Enabled	[WPA2][Auth(PSK)]

A következő a hálózatokhoz létrehozott interfészek meglétének tesztelése.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMA			
Interfaces			
Interface Name	VLAN Identifier	IP Address	Interface Type
<a href="#">VLAN 10</a>	10	192.168.1.66	Dynamic
<a href="#">VLAN 20</a>	20	192.168.1.82	Dynamic
<a href="#">VLAN 40</a>	40	192.168.1.146	Dynamic
<a href="#">management</a>	30	192.168.1.133	Static

Ellenőrizzük, hogy a DHCP szerveren a Pool beállításai helyesek-e, és a WLC címét szórja-e. Ez fontos az Access Pointok miatt, hogy tudjanak a WLC-re csatlakozni és szórni a hálózatok azonosítóját.

**DHCP**

Interface	FastEthernet0	Service	<input checked="" type="radio"/> On	<input type="radio"/> Off
Pool Name	VLAN 30-management			
Default Gateway	192.168.1.129			
DNS Server	192.168.1.131			
Start IP Address :	192	168	1	135
Subnet Mask:	255	255	255	240
Maximum Number of Users :	8			
TFTP Server:	0.0.0.0			
WLC Address:	192.168.1.133			

A WLC Wireless fülén látszik, hogy mind a négy AP csatlakozott a WLC-hez.

MONITOR <u>WLANS</u> <u>CONTROLLER</u> <b>WIRELESS</b> SECURITY   MANAGEMENT	
<b>All APs</b>	
Current Filter <span style="float: right;">[Change Filter] [Clear Filter]</span>	
Number of APs 4	
AP Name	IP Address(Ipv4/Ipv6)
<a href="#">Management AP</a>	192.168.1.137
<a href="#">Vezetoseg AP</a>	192.168.1.139
<a href="#">Guest AP</a>	192.168.1.138
<a href="#">Dolgozok AP</a>	192.168.1.136

Az utolsó lépés, a Vendég hálózatra csatlakozó Gépen ellenőrizzük, hogy a DHCP szerver osztott-e neki IP címet.

```
C:\>ipconfig

Wireless0 Connection:(default port)

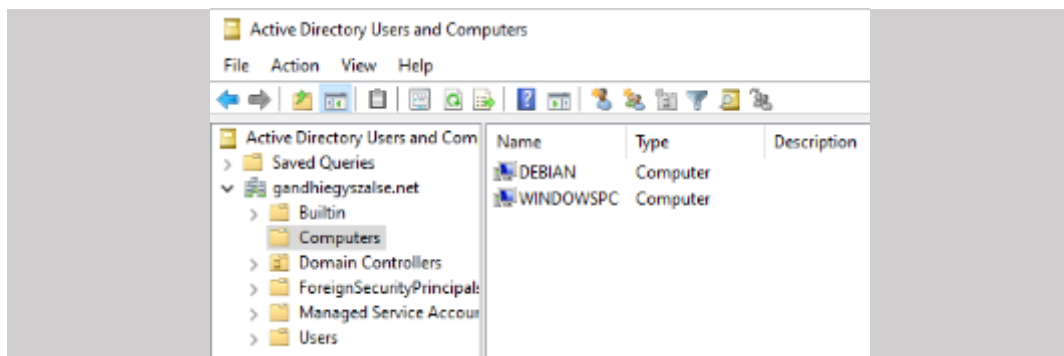
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::201:63FF:FE12:AA73
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.147
Subnet Mask.....: 255.255.255.240
Default Gateway.....: ::
                        192.168.1.145
```

Mint látszik a parancs kimenetéből, a gép kapott IP címet a megfelelő DHCP Pool-ból.

# Windows és Linux Szerverek

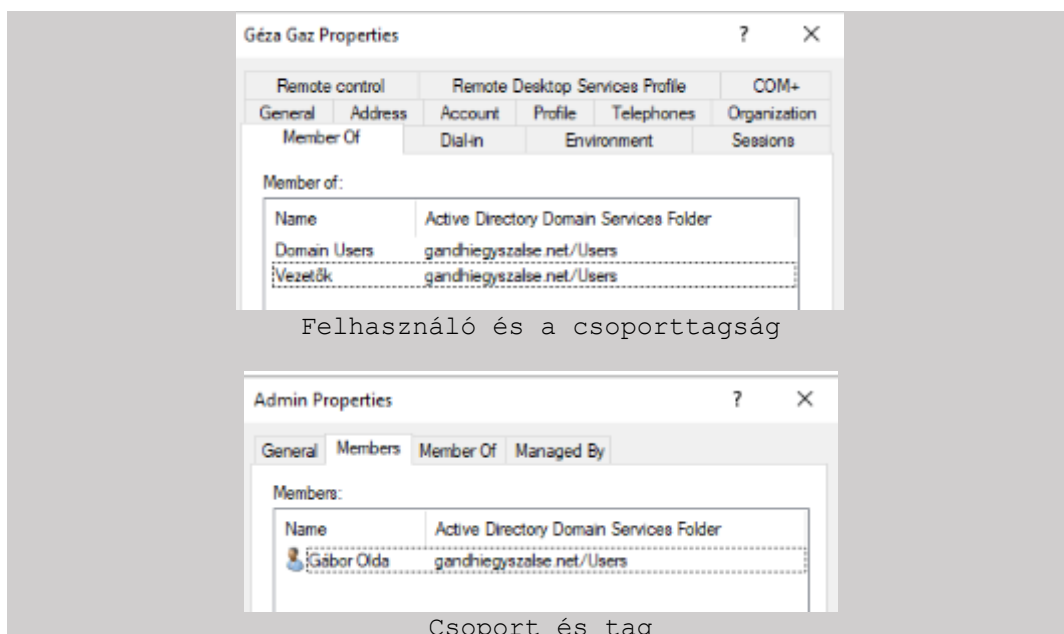
## Active Directory

Felcsatlakoztattunk egy Windows gépet, illetve a Debian gépet, ami a Linux alapú szerverünk szerepét tölti be. A tartományban megnézzük, hogy látja-e a gépet, mint vezérlő.



A Windows gépen is leellenőriztük, többféle módon a tartományt létezését, kezdve a ping paranccsal, utána az nslookup paranccsal megnéztük, hogy érzékeli a Windows szerveren működő DNS szolgáltatás. Miután mindenről megbizonyosodtunk, a beléptetését grafikusán intéztük el a rendszeren belül.

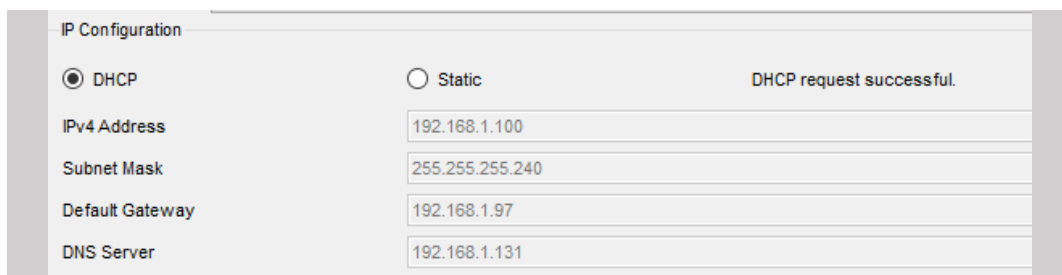
A felhasználókat és a csoportokat is leellenőriztük, hogy sikeresen létrehoztuk-e, ezt kétféleképp is megnéztük. A felhasználót nézzük és melyik csoportnak a tagja, a másik pedig pont fordítva, megnyitjuk a csoportot és megnézzük ki a tagja.



## DHCP

Miután megcsináltuk a DHCP pool-okat a szerveren, illetve a Cisco Packet Tracer-ben, leteszteltük ott, hogy a hálózatban minden működjön és tudjunk tovább haladni.

Miután a gépeken átállítottuk az IP konfigurációban, hogy ne statikusan, hanem DHCP-vel kapjon címet, vártunk egy kicsit és sikeresen meg is kapta azt.



IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address	192.168.1.100
Subnet Mask	255.255.255.240
Default Gateway	192.168.1.97
DNS Server	192.168.1.131

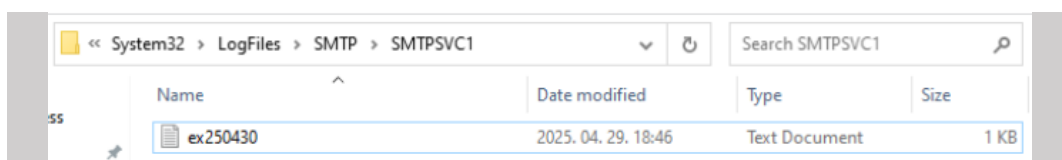
## MAIL

A MAIL szolgáltatás működését a tartományvezérlőből néztük meg, hogy sikeresen kimegy-e az üzenet, amit küldtünk.

Az üzenetet az Admin küldte Munka Misinek, teszt témával, „Ez egy tesztüzenet” tartalommal. Az üzenet megfelelően elment.

```
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2025-04-30 00:01:42
#Fields: time c-ip cs-method cs-uri-stem sc-status
00:01:42 127.0.0.1 HELO - 250
00:03:32 127.0.0.1 MAIL - 250
00:05:21 127.0.0.1 RCPT - 250
00:05:59 127.0.0.1 DATA - 250
```

Emellett azt is leteszteltük, hogy a kimenő levélről kap-e log üzenetet a szerver az erre készített mappába, amit beállítottunk neki.



Name	Date modified	Type	Size
ex250430	2025. 04. 29. 18:46	Text Document	1 KB

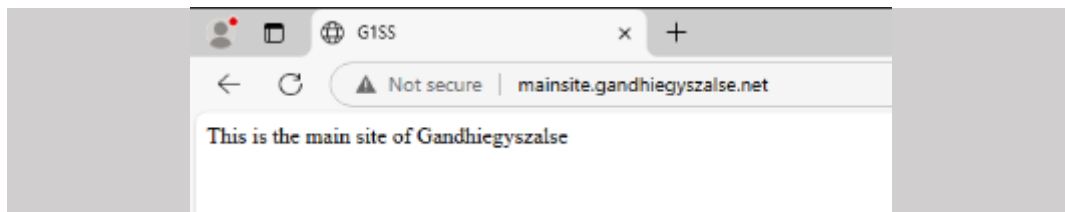


## Web és DNS

A web és a DNS működését egybevontuk, hiszen DNS nélkül nem is lehetne rákeresni a weboldalra.

Tesztelést a Windows gépen egy böngészőben végeztünk, ahol rákerestünk a weboldal nevére, „mainsite.gandhiegyzalse.net”.

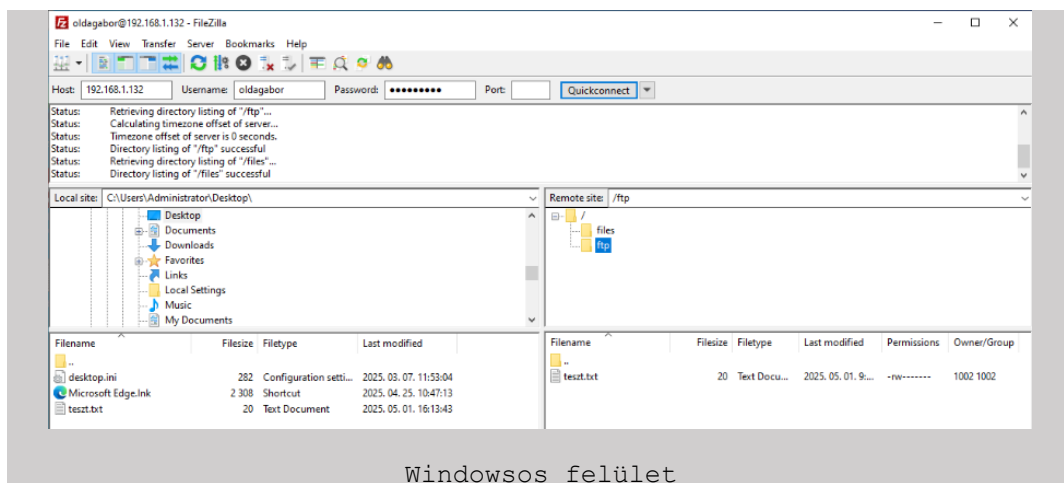
Mindkét szolgáltatás sikeresen működik, jó oldalra mutat rá a link.



## FTP

A FileZilla rendkívül megkönnyítette a dolgunkat a tesztelés folyamatán, hiszen minden le van egyszerűsítve, ezért arra a következtetésre jutottunk, hogy az összes gépre feltelepítjük majd és általa tudnak hozzáférni a Linuxon található fájlokhoz, amik nekik szólnak, illetve fel tudják tölteni az adatokat ide.

Beléptünk Olda Gábor fiókjába, onnan néztük a tesztelést. Gábor látja az összes mappát, illetve a mappában lévő fájlokat, ami a Linuxon elérhető és a felhasználóhoz tartozik. Ezeket le tudja tölteni és fel is tud tölteni rá. Ezt mindkét úton leteszteltük. Mindkét esetben sikerrel jártunk el.



Windowsos felület



```
root@G1SSLinux:~# ls /oldagabor
files  ftp
root@G1SSLinux:~# ls /oldagabor/ftp
teszt.txt
root@G1SSLinux:~# _
```

Linuxos felület

## RSYNC és szerverek közti SSH

Az rsync tesztelése előtt leellenőriztük, hogy az SSH működik-e mindkét gépen, el tudják-e érni egymást.

```
C:\Users\Administrator>ssh oldagabor@192.168.1.132
oldagabor@192.168.1.132's password: _
Linux G1SSLinux 6.1.0-30-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.124-1 (2025-01-12) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
oldagabor@G1SSLinux:~$ _
```

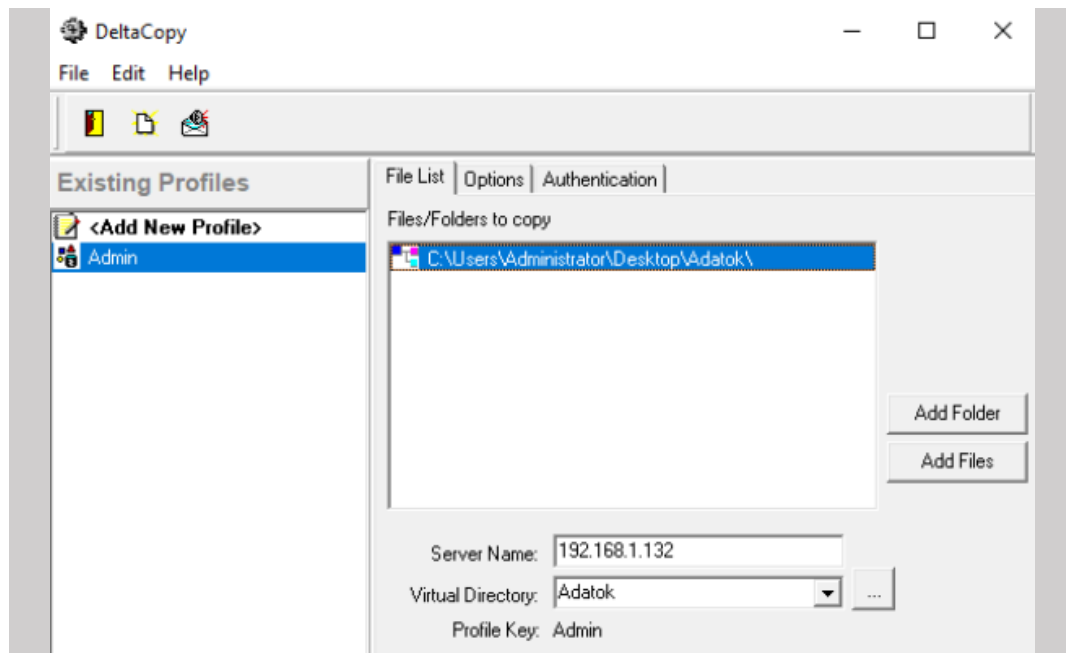
Windows

```
Microsoft Windows [version 10.0.20348.567]
(c) Microsoft Corporation. All rights reserved.

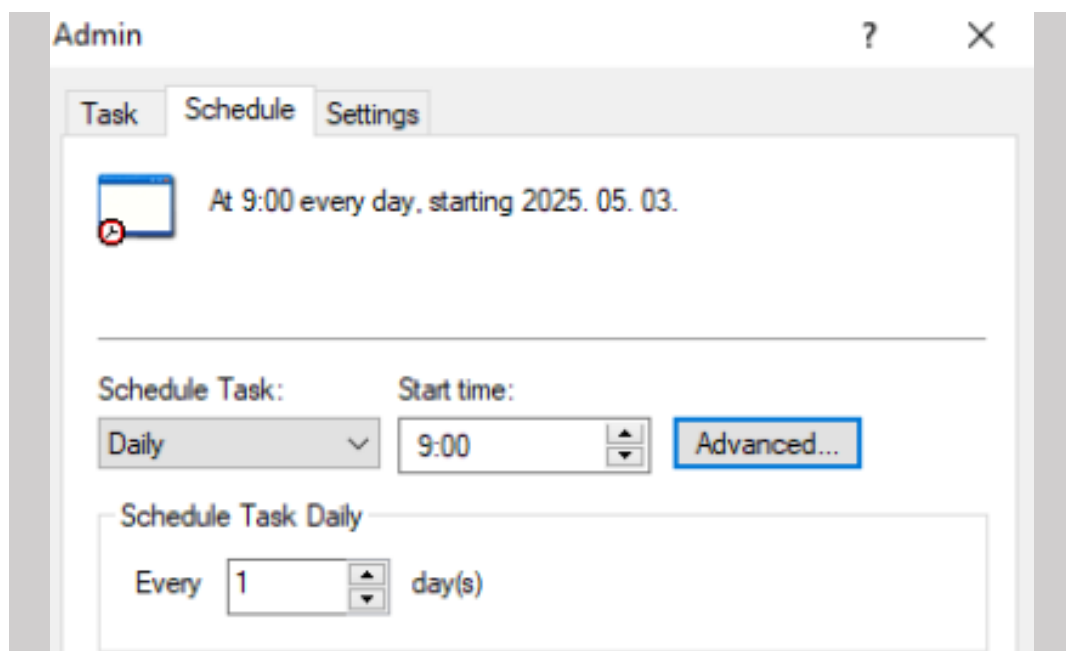
gandhiegyszalse\oldagabor@G1SS1-WS C:\Users\oldagabor>
```

Debian

Miután sikeresen leteszteltük az SSH működését, beléptetjük a Windows-t az rsync-be a DeltaCopy segítségével. Itt létrehoztunk neki egy új profilt és megadtuk neki a szerver elérhetőségét.



Majd beállítottunk neki egy menetrendet, hogy mikor másoljon át a fájlokat.





## Hálózat Programozás

A tesztet egy azonos forgalomirányítón végeztük el, hogy a hálózatunk működését ne zavarjuk be.

A szkript lefuttatása előtt beleírtuk a forgalomirányítót, amiben szeretnénk konfigurálni. Ezután lefuttatjuk a programot. Ez sikeresen bedob a forgalomirányítóba, itt pedig a Cisco követelményeinek megfelelően tudjuk variálni a konfigurációt. Jelen esetben a négyes interfészen adtunk IP címet az eszköznek.

A sikerességét egy másik szkript segítségével ellenőriztük, amivel meg tudjuk nézni az átkonfigurált forgalomirányító interfészeit.

```
(nc) bence@vz-lxc103:~/python/nc$ python3 nmwrite.py
Password:
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
r1(config)#interface GigabitEthernet0/4
r1(config-if)#ip address 192.168.10.10 255.255.255.0
r1(config-if)#no shutdown
r1(config-if)#end
r1#
(nc) bence@vz-lxc103:~/python/nc$ python3 nm.py
Password:
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet1	172.17.255.210	YES	DHCP	up	up
GigabitEthernet2	192.168.1.10	YES	manual	down	down
GigabitEthernet3	unassigned	YES	unset	down	down
GigabitEthernet4	192.168.10.10	YES	manual	down	down

```
(nc) bence@vz-lxc103:~/python/nc$
(nc) bence@vz-lxc103:~/python/nc$
```