****Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

***Szakképesítés neve:*** Informatikai rendszer- és   
alkalmazás-üzemeltető technikus

***száma:*** 5-0612-12-02

**Vizsgaremek**

**Metropolitan Transportation Authority**

Bodnár Martin, Huszár Bence, Mokos Márk  
2/14.A

Budapest, 2023.

Tartalom

[A hálózat tesztelési dokumentációja 3](#_Toc127782458)

[Sárga elipszis terület: Wall Street-i metro megálló 3](#_Toc127782459)

[DHCP 3](#_Toc127782460)

[Kizárt címek 3](#_Toc127782461)

[VLAN 10 – Kék terület (Jegy nyomtató autómaták) 3](#_Toc127782462)

[VLAN 20 – Narancs terület (Beléptető rendszer) 4](#_Toc127782463)

[VLAN 30 – Magenta terület (Privát WIFI) 4](#_Toc127782464)

[VLAN 40 – Sárga terület (Pékség) 5](#_Toc127782465)

[VLAN 50 – Zöld terület (Admin szoba) 6](#_Toc127782466)

[VTP 7](#_Toc127782467)

[VTP beállítások: 7](#_Toc127782468)

[Wall\_St\_SW\_Main: 7](#_Toc127782469)

[Wall\_St\_SW\_F0: 7](#_Toc127782470)

[Wall\_St\_SW\_F-1: 8](#_Toc127782471)

[Link-aggregation 10](#_Toc127782472)

[Wall\_St\_SW\_Main: 10](#_Toc127782473)

[Wall\_St\_SW\_F0: 10](#_Toc127782474)

[Wall\_St\_SW\_F-1: 11](#_Toc127782475)

[Portsecurity 12](#_Toc127782476)

[Wall\_St\_SW\_Main: 12](#_Toc127782477)

[Wall\_St\_SW\_F0: 12](#_Toc127782478)

[Wall\_St\_SW\_F-1: 13](#_Toc127782479)

[STP 14](#_Toc127782480)

[Wall\_St\_SW\_Main: 14](#_Toc127782481)

[Wall\_St\_SW\_F0: 14](#_Toc127782482)

[Wall\_St\_SW\_F-1: 15](#_Toc127782483)

# A hálózat tesztelési dokumentációja

A hálózat teszteléséhez a Cisco Packet tracer szimulációs és EVE-NG virtualizációs programokat választottuk

# Sárga elipszis terület: Wall Street-i metro megálló

# DHCP

A megálló területén a jegy automaták, a beléptető rendszer, a vezeték nélküli forgalomirányító, a pékség és az admin számára az automatikus IPv4 címkiosztást a határ forgalomirányítón konfigurált DHCP szolgáltatással biztosítottuk.

### Kizárt címek

**(Részlet)**

show running-config

ip dhcp excluded-address 193.200.10.1

ip dhcp excluded-address 193.200.20.1

ip dhcp excluded-address 193.200.30.1

ip dhcp excluded-address 193.200.40.1

ip dhcp excluded-address 193.200.50.1

### VLAN 10 – Kék terület (Jegy nyomtató autómaták)

show ip dhcp pool VLAN10

Pool VLAN10 :

Utilization mark (high/low) : 100 / 0

Subnet size (first/next) : 0 / 0

Total addresses : 254

Leased addresses : 2

Excluded addresses : 5

Pending event : none

1 subnet is currently in the pool

Current index IP address range Leased/Excluded/Total

193.200.10.1 193.200.10.1 - 193.200.10.254 0 / 5 / 254

### VLAN 20 – Narancs terület (Beléptető rendszer)

1. ábra – VLAN 10 – Wireshark DORA üzenetek

show ip dhcp pool VLAN20

Pool VLAN20 :

Utilization mark (high/low) : 100 / 0

Subnet size (first/next) : 0 / 0

Total addresses : 254

Leased addresses : 2

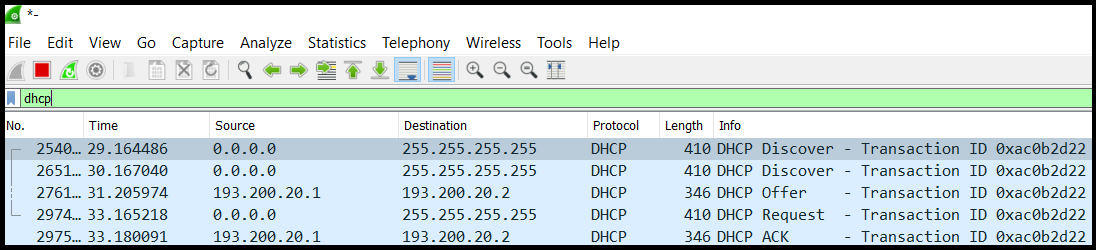
Excluded addresses : 5

Pending event : none

1 subnet is currently in the pool

Current index IP address range Leased/Excluded/Total

193.200.20.1 193.200.20.1 - 193.200.20.254 2 / 5 / 254



2. ábra – VLAN 20 – Wireshark DORA üzenetek

### VLAN 30 – Magenta terület (Privát WIFI)

show ip dhcp pool VLAN30

Pool VLAN30 :

Utilization mark (high/low) : 100 / 0

Subnet size (first/next) : 0 / 0

Total addresses : 254

Leased addresses : 1

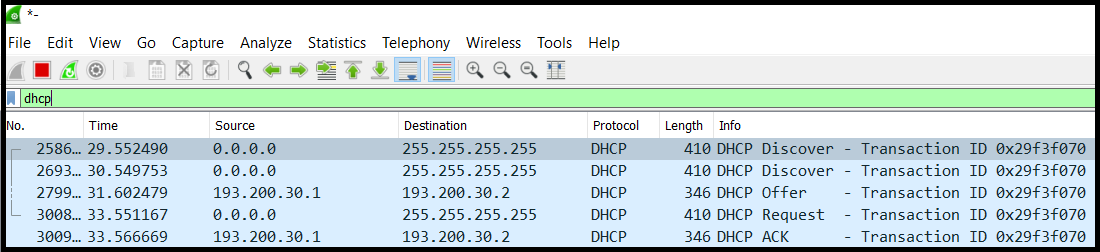
Excluded addresses : 5

Pending event : none

1 subnet is currently in the pool

Current index IP address range Leased/Excluded/Total

193.200.30.1 193.200.30.1 - 193.200.30.254 1 / 5 / 254



3. ábra – VLAN 30 – Wireshark DORA üzenetek

### VLAN 40 – Sárga terület (Pékség)

show ip dhcp pool VLAN40

Pool VLAN40 :

Utilization mark (high/low) : 100 / 0

Subnet size (first/next) : 0 / 0

Total addresses : 254

Leased addresses : 2

Excluded addresses : 5

Pending event : none

1 subnet is currently in the pool

Current index IP address range Leased/Excluded/Total

193.200.40.1 193.200.40.1 - 193.200.40.254 2 / 5 / 254

### VLAN 50 – Zöld terület (Admin szoba)

4. ábra – VLAN 40 – Wireshark DORA üzenetek

show ip dhcp pool VLAN50

Pool VLAN50 :

Utilization mark (high/low) : 100 / 0

Subnet size (first/next) : 0 / 0

Total addresses : 254

Leased addresses : 1

Excluded addresses : 5

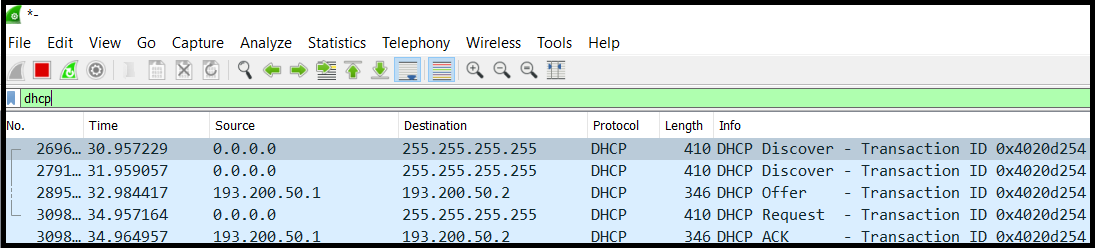
Pending event : none

1 subnet is currently in the pool

Current index IP address range Leased/Excluded/Total

193.200.50.1 193.200.50.1 - 193.200.50.254 1 / 5 / 254

5. ábra – VLAN 50 – Wireshark DORA üzenetek

A DHCP kérésekben Wireshark-kal megfigyelhetők (lásd 1-5. ábra) a DORA üzenetek. Az első üzenet a ***DHCP Discover*** a hálózatban keresi/felderíti a DHCP szervert. A második üzenet a ***DHCP Offer***, amit a DHCP szerver küld válaszként egy megajánlott IPv4 címmel. A harmadik üzenetet ***DHCP Request***, a kliens küldi válaszként a szervernek, hogy kéri a megajánlott IPv4 címet. Utoljára a szerver válaszként küldi a ***DHCP Acknowledge*** üzenetet, amely után a kliens megkapja a megajánlott IPv4 címét a bérleti idő lejártáig.

*A többi site DHCP tesztelése is ugyanezen módon megtörtént.*

# VTP

A megálló területét VLAN-okra bontottuk fel, ezek létrehozására pedig VTP-t használtunk, így elég a VTP szerverként beállított kapcsolón létrehozni a VLAN-okat, majd a kapcsoló szinkronizálja a VLAN adatbázisát a trunk portjaihoz kapcsolt VTP kliens kapcsolókkal.

## VTP beállítások:

* Wall\_St\_SW\_Main – VTP szerver
* Wall\_St\_SW\_F0 – VTP kliens
* Wall\_St\_SW\_F-1 – VTP Kliens
* VTP jelszó: cisco
* VTP domain: cisco.com

Illetve a klienseken jól látszik , hogy megtanulták a VLAN-okat:

### Wall\_St\_SW\_Main:

SW\_Main#show vtp status

VTP Version capable : 1 to 2

VTP version running : 1

VTP Domain Name : cisco.com

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 0007.EC29.0410

Configuration last modified by 0.0.0.0 at 3-1-93 00:25:24

Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :

--------------

VTP Operating Mode : Server

Maximum VLANs supported locally : 255

Number of existing VLANs : 12

Configuration Revision : 40

MD5 digest : 0x36 0xC3 0x9B 0x97 0x11 0xBF 0x69 0x9A

0xF5 0x03 0xB3 0x7C 0xE1 0x3C 0x80 0x93

### Wall\_St\_SW\_F0:

SW\_F0#show vlan brief

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active

10 Tickets active Fa0/3, Fa0/4

20 Admission active Fa0/1, Fa0/2

30 Wifi active

40 Bakery active

50 Admin active

60 VOID active 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, Fa0/23, Fa0/24,

Gig0/1, Gig0/2

99 Native active

1002 fddi-default active

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active

SW\_F0#show vtp status

VTP Version capable : 1 to 2

VTP version running : 1

VTP Domain Name : cisco.com

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 0005.5E96.2460

Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :

--------------

VTP Operating Mode : Client

Maximum VLANs supported locally : 255

Number of existing VLANs : 12

Configuration Revision : 38

MD5 digest : 0x1E 0x5C 0x7E 0x5A 0xEA 0x67 0x21 0xA0

0x31 0xF6 0x56 0x3E 0xBD 0xE1 0xC2 0x23

SW\_F0#show vtp password

VTP Password: cisco

### Wall\_St\_SW\_F-1:

SW\_F-1#show vlan brief

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active

10 Tickets active

20 Admission active

30 Wifi active Fa0/5

40 Bakery active Fa0/1, Fa0/2, Fa0/3, Fa0/4

50 Admin active

60 VOID active 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, Fa0/21, Fa0/22, Gig0/1

Gig0/2

99 Native active

1002 fddi-default active

1003 token-ring-default active

1004 fddinet-default active

1005 trnet-default active

SW\_F-1#show vtp status

VTP Version capable : 1 to 2

VTP version running : 1

VTP Domain Name : cisco.com

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 0009.7C8C.84E0

Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00

Feature VLAN :

--------------

VTP Operating Mode : Client

Maximum VLANs supported locally : 255

Number of existing VLANs : 12

Configuration Revision : 38

MD5 digest : 0x1E 0x5C 0x7E 0x5A 0xEA 0x67 0x21 0xA0

0x31 0xF6 0x56 0x3E 0xBD 0xE1 0xC2 0x23

SW\_F-1#show vtp password

VTP Password: cisco

*A többi site VTP tesztelése is ugyanezen módon megtörtént.*

# Link-aggregation

LACP segítségével 2 fizikai portot “összevonunk” 1 logikai porttá, ezzel növelve port sávszélességét és a redundanciát a hálózatban.

### Wall\_St\_SW\_Main:

SW\_Main#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 Fa0/23(P) Fa0/24(P)

2 Po2(SU) LACP Fa0/21(P) Fa0/22(P)

### Wall\_St\_SW\_F0:

SW\_F0#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

------+-------------+-----------+----------------------------------------------

2 Po2(SU) LACP Fa0/21(P) Fa0/22(P)

3 Po3(SU) LACP Fa0/19(P) Fa0/20(P)

### Wall\_St\_SW\_F-1:

SW\_F-1#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 Fa0/23(P) Fa0/24(P)

3 Po3(SU) LACP Fa0/19(P) Fa0/20(P)

Látható az is, ha a 2 port közül az egyik port nem működik, akkor a másik még működni fog:

SW\_F0#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

------+-------------+-----------+----------------------------------------------

2 Po2(SU) LACP Fa0/21(D) Fa0/22(P)

3 Po3(SU) LACP Fa0/19(D) Fa0/20(P)

*A többi site Ether-channel tesztelése is ugyanezen módon megtörtént.*

# Portsecurity

Portvédelmet konfiguráltunk a kapcsolókon a második rétegen így maximum 1 címet írnak be a MAC cím táblájukba portonként, sticky módban így a következő alkalommal a porton csatlakozó gép MAC címét jegyzi meg és shutdown violation móddal. Portsértés esetén a port lekapcsol és manuálisan kell felkapcsolnunk plusz a sértés számlálót növeli.

### Wall\_St\_SW\_Main:

SW\_Main#show port-security

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

--------------------------------------------------------------------

Fa0/1 1 1 0 Shutdown

----------------------------------------------------------------------

SW\_Main#show port-security interface fa0/1

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

Last Source Address:Vlan : 00D0.FFE3.152C:50

Security Violation Count : 0

### Wall\_St\_SW\_F0:

SW\_F0#show port-security

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

--------------------------------------------------------------------

Fa0/1 1 1 0 Shutdown

Fa0/2 1 1 0 Shutdown

Fa0/3 1 1 0 Shutdown

Fa0/4 1 1 0 Shutdown

----------------------------------------------------------------------

SW\_F0#show port-security interface fa0/1

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

Last Source Address:Vlan : 00D0.BC06.8CB7:20

Security Violation Count : 0

### Wall\_St\_SW\_F-1:

SW\_F-1#show port-security

Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action

(Count) (Count) (Count)

--------------------------------------------------------------------

Fa0/1 1 1 0 Shutdown

Fa0/2 1 1 0 Shutdown

Fa0/4 1 1 0 Shutdown

----------------------------------------------------------------------

SW\_F-1#show port-security interface fa0/1

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Shutdown

Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 1

Last Source Address:Vlan : 0030.F240.46D0:40

Security Violation Count : 0

# STP

A hurkok elkerülése miatt spanning-tree protokollt alkalmaztunk a megállóban

### Wall\_St\_SW\_Main:

(Primary root)

SW\_Main#show spanning-tree summary

Switch is in rapid-pvst mode

Root bridge for: default Tickets Admission Wifi Bakery Admin Native

Extended system ID is enabled

Portfast Default is disabled

PortFast BPDU Guard Default is disabled

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 5 0 0 3 8

VLAN0010 5 0 0 3 8

VLAN0020 5 0 0 3 8

VLAN0030 5 0 0 3 8

VLAN0040 5 0 0 3 8

VLAN0050 4 0 0 4 8

VLAN0099 5 0 0 3 8

---------------------- -------- --------- -------- ---------- ----------

7 vlans 34 0 0 22 56

### Wall\_St\_SW\_F0:

SW\_F0#show spanning-tree summary

Switch is in rapid-pvst mode

Root bridge for:

Extended system ID is enabled

Portfast Default is disabled

PortFast BPDU Guard Default is disabled

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 8 0 0 2 10

VLAN0010 6 0 0 4 10

VLAN0020 6 0 0 4 10

VLAN0030 8 0 0 2 10

VLAN0040 8 0 0 2 10

VLAN0050 8 0 0 2 10

VLAN0099 8 0 0 2 10

---------------------- -------- --------- -------- ---------- ----------

7 vlans 52 0 0 18 70

### Wall\_St\_SW\_F-1:

SW\_F-1#show spanning-tree summary

Switch is in rapid-pvst mode

Root bridge for:

Extended system ID is enabled

Portfast Default is disabled

PortFast BPDU Guard Default is disabled

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 10 0 0 1 11

VLAN0010 10 0 0 1 11

VLAN0020 10 0 0 1 11

VLAN0030 9 0 0 2 11

VLAN0040 6 0 0 5 11

VLAN0050 10 0 0 1 11

VLAN0099 10 0 0 1 11

---------------------- -------- --------- -------- ---------- ----------

7 vlans 65 0 0 12 77

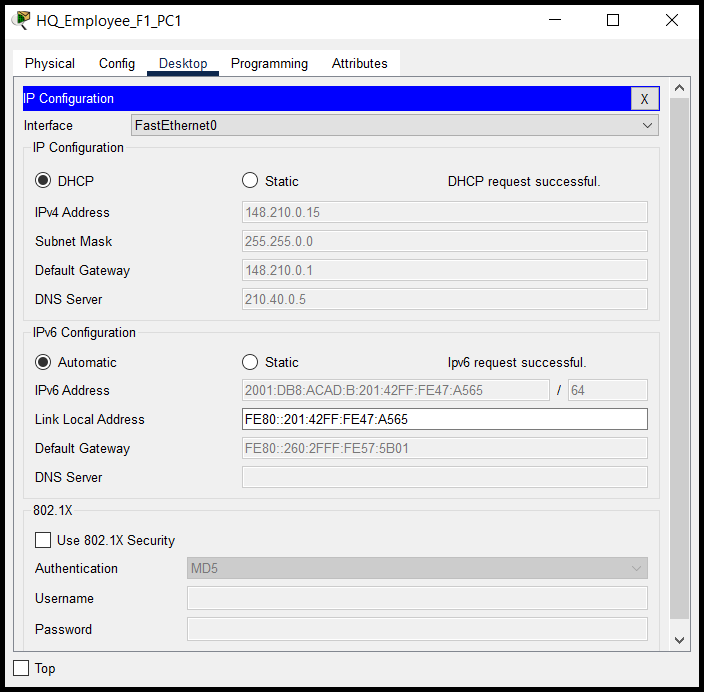
*A többi site STP tesztelése is ugyanezen módon megtörtént.*

# NAT/PAT

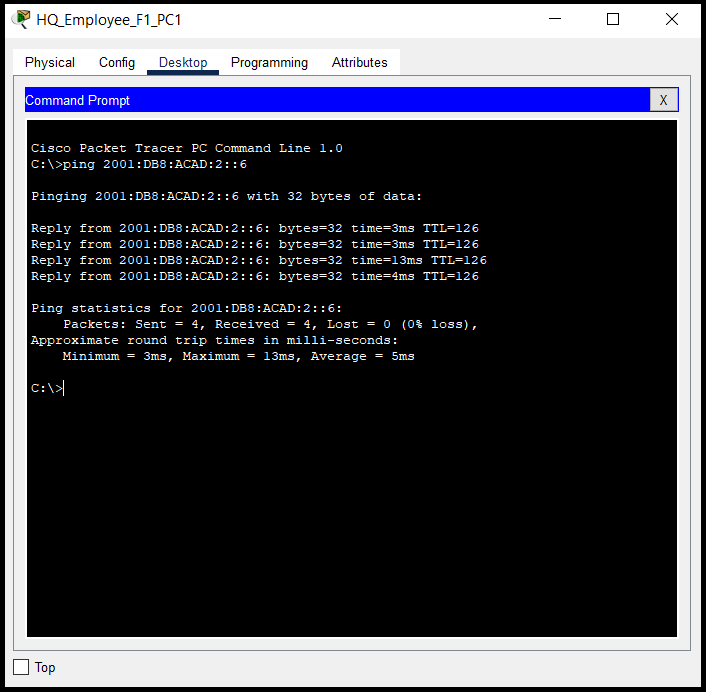
# Zöld elipszis terület: MTA Headquarters

## GRE Tunnel

Az irodában található állomások a távoli siteon lévő DHCP szervertől kapják dinamikusan az IPv4 címeiket. Ehhez egy GRE alagutat konfiguráltunk a kettő site között és egy forgalomirányítási területté vontuk össze a két siteot. Ezen felül konfiguráltunk egy második IPv6 over IPv4 GRE alagutat így az állomások IPv6-tal is elérik a szervereket.

Az ábrából jól látható, hogy az irodában lévő PC sikeresen kap IPv4 címet a távoli siteon lévő DHCP szervertől.

6. ábra – DHCP request over GRE



7. ábra – Sikeres pingv6 a távoli szerverekhez

Az ábrán látható, hogy az irodából a PC meg tudja pingelni a távoli siteon lévő szervert IPv6 címmel. A határ forgalomirányítóig ICMPv6 csomagként kerül továbbításra a ping, ahol a forgalomirányító ezt becsomagolja egy IPv4 csomagba és így kerül kiküldésre az internet-szolgáltatónk felé.

## IPSec Tunnel

IPSec policy beállításai:

HQ\_Border\_R#show crypto isakmp policy

Global IKE policy

Protection suite of priority 1

encryption algorithm: DES - Data Encryption Standard (56 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Pre-Shared Key

Diffie-Hellman group: #1 (768 bit)

lifetime: 86400 seconds, no volume limit

IPSec transform-set beállításai:

HQ\_Border\_R#show crypto ipsec transform-set

Transform set SITE2TSET: { { esp-aes esp-sha-hmac }

will negotiate = { Tunnel, },

Transform set #$!default\_transform\_set\_1: { esp-aes esp-sha-hmac }

will negotiate = { Transport, },

Transform set #$!default\_transform\_set\_0: { esp-3des esp-sha-hmac }

will negotiate = { Transport, },

IPSec crypto map beállításai:

HQ\_Border\_R#show crypto map

Crypto Map SITE2CMAP 1 ipsec-isakmp

Peer = 40.0.0.2

Extended IP access list VPN

access-list VPN permit ip host 20.0.0.2 host 40.0.0.2

Current peer: 40.0.0.2

Security association lifetime: 4608000 kilobytes/3600 seconds

PFS (Y/N): N

Transform sets={

SITE2TSET,

}

Interfaces using crypto map SITE2CMAP:

Serial0/1/0

HQ\_Border\_R#show crypto ipsec sa

interface: Serial0/1/0

Crypto map tag: SITE2CMAP, local addr 20.0.0.2

protected vrf: (none)

local ident (addr/mask/prot/port): (20.0.0.2/255.255.255.255/0/0)

remote ident (addr/mask/prot/port): (40.0.0.2/255.255.255.255/0/0)

current\_peer 40.0.0.2 port 500

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 46, #pkts encrypt: 46, #pkts digest: 0

#pkts decaps: 42, #pkts decrypt: 42, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

local crypto endpt.: 20.0.0.2, remote crypto endpt.:40.0.0.2

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0x9049B568(2420749672)

inbound esp sas:

spi: 0x4751CB9B(1196542875)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2002, flow\_id: FPGA:1, crypto map: SITE2CMAP

sa timing: remaining key lifetime (k/sec): (4525504/3561)

IV size: 16 bytes

replay detection support: N

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x9049B568(2420749672)

transform: esp-aes esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2003, flow\_id: FPGA:1, crypto map: SITE2CMAP

sa timing: remaining key lifetime (k/sec): (4525504/3561)

IV size: 16 bytes

replay detection support: N

Status: ACTIVE

outbound ah sas:

outbound pcp sas:

## DHCPv6 Stateless

## EIGRP

## IPv6 EIGRP

# Rózsaszín elipszis terület: MTA Garázs/Szervíz

## HSRP