Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

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

***száma:*** 5-0612-12-02

**VIZSGAREMEK**

**Gandhi egy szál se**

**Tesztelési dokumentáció**

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

Budapest, 2025.

TARTALOMJEGYZÉK

[TARTALOMJEGYZÉK 2](#_Toc197006645)

[Szolgáltatások meg minden (mégse xd) 2](#_Toc197006646)

[VLAN-ok 3](#_Toc197006647)

[Vlanok létrehozása 3](#_Toc197006648)

[VTP (VLAN trönk protokoll) 3](#_Toc197006649)

[Inter-VLAN routing 4](#_Toc197006650)

[Második rétegbeli megvalósítások (L2) 5](#_Toc197006651)

[EtherChannel (port összevonás) 5](#_Toc197006652)

[Portbiztonság 6](#_Toc197006653)

[STP (Spanning Tree Protocol) 8](#_Toc197006654)

[HSRP 9](#_Toc197006655)

[OSPF 12](#_Toc197006656)

[OSPF Auth 13](#_Toc197006657)

[NAT 14](#_Toc197006658)

[Access-List 15](#_Toc197006659)

[Port Forward 16](#_Toc197006660)

[Ip telefonok 17](#_Toc197006661)

[WEB-VPN 19](#_Toc197006662)

[BGP 22](#_Toc197006663)

[WLC 22](#_Toc197006664)

Szolgáltatások meg minden (mégse xd)

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 router 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

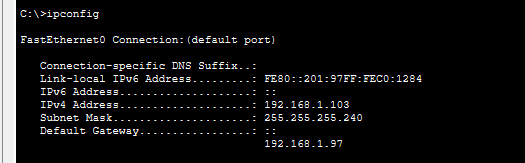
FastEthernet0/0.30 192.168.2.130 up

FastEthernet0/0.40 192.168.2.34 up

FastEthernet0/0.50 192.168.2.66 up

Miután a router 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.



Ezt követően a Kapcsolón ellenőrizzük, a hálózatot.

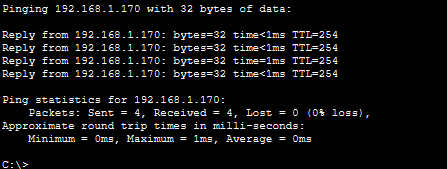
G1SS1-SW1#show running-config | include default-gateway

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.



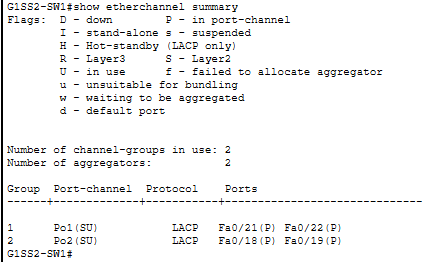
Látszik, hogy a csomagok sikeresen elértek a kapcsolóhoz, ez azt jelenti, hogy működik a vlanok közötti forgalomirányítás.

Második rétegbeli megvalósítások (L2)

EtherChannel (port összevonás)

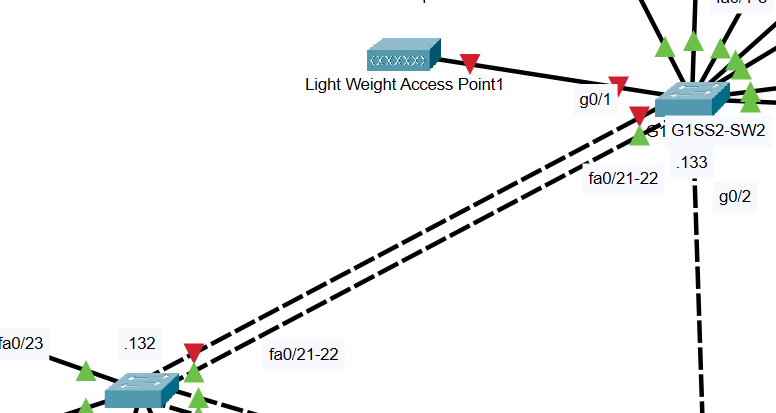
Az EtherChannel tesztelése úgy fog történni, hogy ellenőrizzük az összevont csatornák létezését, az összevont portok egyikét lekapcsoljuk, és ellenőrizzük, hogy a forgalom továbbra is sikeresen halad át az összevont csatornán.

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

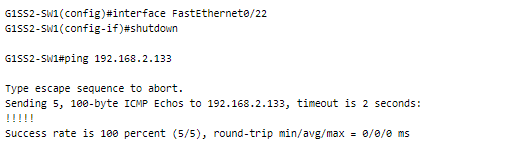


Látszik, hogy a Po1-ben a FastEthernet 0/21 és 22-es portok vannak, a Po2-ben pedig a FastEthernet 0/18 és 19-es portok.

Miután meggyőződtünk 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 eléri-e a jobb oldali (G1SS2-SW2) kapcsolót. (A jobb oldali kapcsoló VLAN 30-as virtuális IP címe 192.168.2.133).



Látjuk, hogy a kapcsoló sikeresen eléri 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 képen szöveg, diagram, képernyőkép, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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.

A képen szöveg, képernyőkép, Betűtípus, szám látható

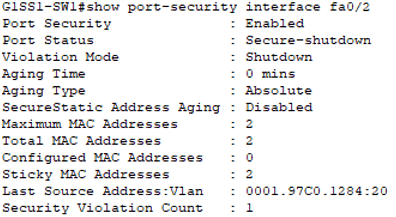
Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

A képen diagram, sor, képernyőkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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



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 képernyőkép, tervezés látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A switchen a kiadott parancs megmutatja a switch 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 switchet csatlakoztatnak az eszközhöz az azonnal letiltja azt a portját, ahol összekötötték őket. Az utóbbit teszteljük is le.

A képen képernyőkép, diagram, sor, szöveg látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen látható módon a Fast Ethernet 0/1 es portjából eltávolítjuk a számítógépet és összekötjük egy másik switchel.

A képen szöveg, képernyőkép, Betűtípus, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.



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

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.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

A képen képernyőkép, szöveg látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

A képen szöveg, sor, képernyőkép, diagram látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Az R1 router-t lekapcsolt állapotba tesszük és megismételjük az előző folyamatot.

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Az előzőekben hasznát gépről küldünk egy pinget a belső szervernek, mint látszik a 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.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A forgalomirányítók miután egyeztették az interfészeken a szomszédokat „Hello” üzenetekkel, elkezdték 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.

A képen szöveg, Betűtípus, képernyőkép, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

OSPF Auth

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.

A képen szöveg, képernyőkép, Betűtípus, dokumentum látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus, dokumentum látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

NAT

A NAT tesztelésénél először bemutatjuk a router alap NAT statisztikáit, ahol a tesztet szimuláljuk, bemutatjuk az HSRP állapotát, végrehajtjuk a csomagküldést, aztán pedig ellenőrizzük, hogy sikeresen lett e a címfordítás.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, Betűtípus, képernyőkép, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

A képen szöveg, képernyőkép, Betűtípus, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

A képen szöveg, képernyőkép, Betűtípus, dokumentum látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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 helyesn működik. Mostmár csak azt kell tesztetljük, hogy a PING parancs eléri-e a szervert, illetve WEB-en eléri-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 teszteljül 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

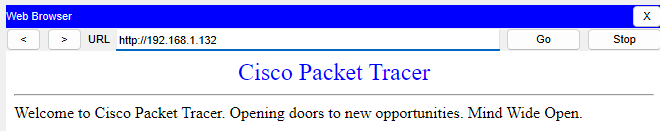
Reply from 192.168.1.131: bytes=32 time=7ms TTL=128

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 Forward

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

A képen szöveg, képernyőkép, Betűtípus, dokumentum látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen képernyőkép, diagram, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

Először a külső siteon bejelentkezünk a PC-be és belemegyünk a web browserbe

A képen szöveg, elektronika, képernyőkép, képernyő látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

A képen szöveg, képernyőkép, Betűtípus, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

Ip telefonok

(work in progress)

A képen Elektronikus eszköz, telefon, elektronika látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen telefon, Elektronikus eszköz, elektronika, kütyü látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

konfiguráció után, a telefonok különböző hálózatban elérik egymást

A képen szöveg, diagram, sor, képernyőkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, diagram, sor, képernyőkép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

WEB-VPN

(work in progress)

A képen szöveg, szoftver, Betűtípus, Weblap látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen szöveg, képernyőkép, szoftver, számítógép látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

A képen diagram, sor, kör, szöveg látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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.

A képen szöveg, képernyőkép, Betűtípus, sor látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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

WLC

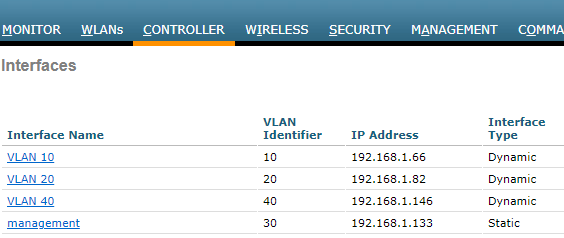
A WLC teszteléséhez először megnézzük, hogy az alap beállítások után „https://” -el be tudunk-e jelentkezni az eszközbe.



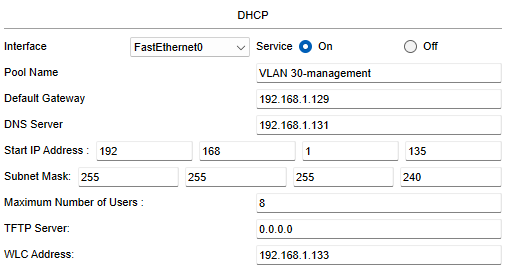
Bejelentkezés után a WLAN fülön ellenörizzük a vezeték nélküli hálózatok meglétét.



A következő a hálózatokhoz létrehozott interfészek meglétének tesztelése.



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.



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



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.