**Miskolci SZC**

**Kandó Kálmán Informatikai Technikum**

**Informatikai rendszer- és alkalmazás-üzemeltető**

**technikus projektfeladat**

**Hálózattervezési és kivitelezési vizsgaremek**

Készítette: Lajka Kristóf (13.A)

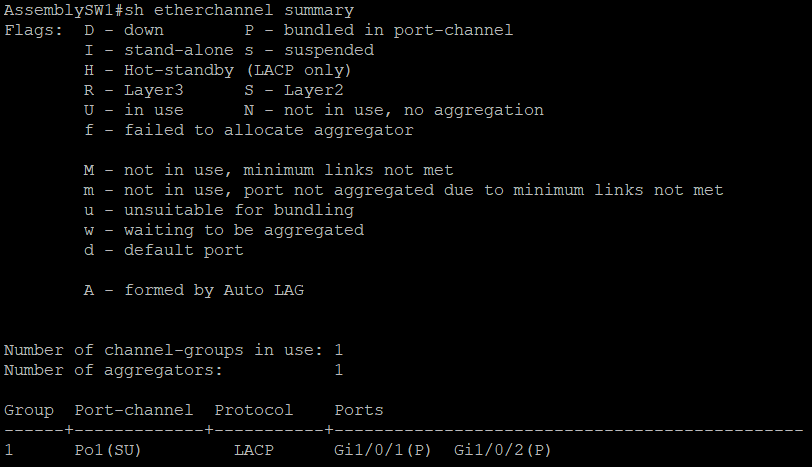
Váradi Ádám (13.A)

Enyedi Sándor (13.A)

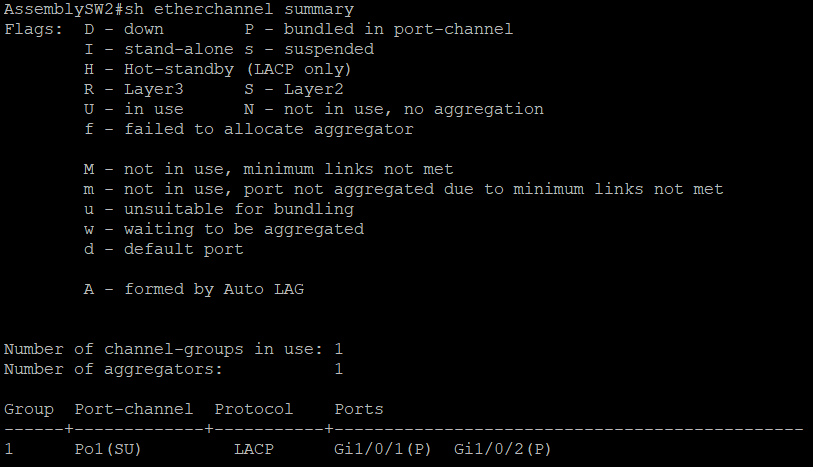
Miskolc, 2025.04.10.

# Etherchannel

AssemblySW1-en az 1-es számú port-channel-en az LACP protokoll helyes működése látható.



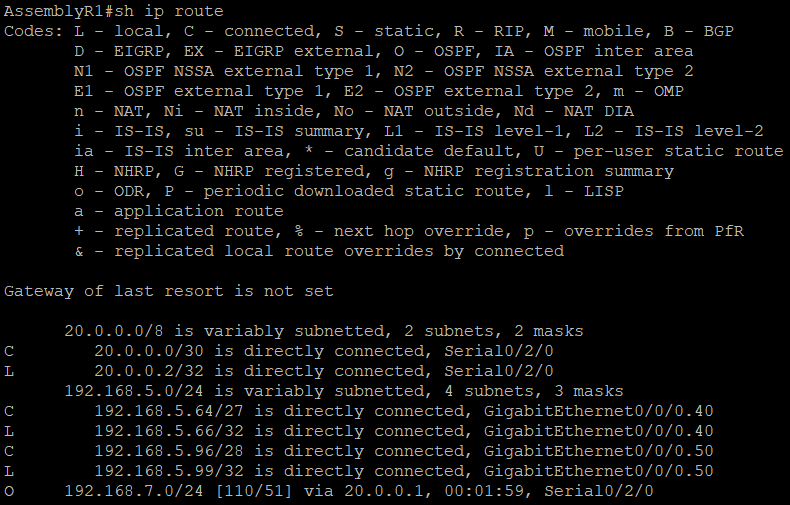
AssemblySW1 LACP tesztelése



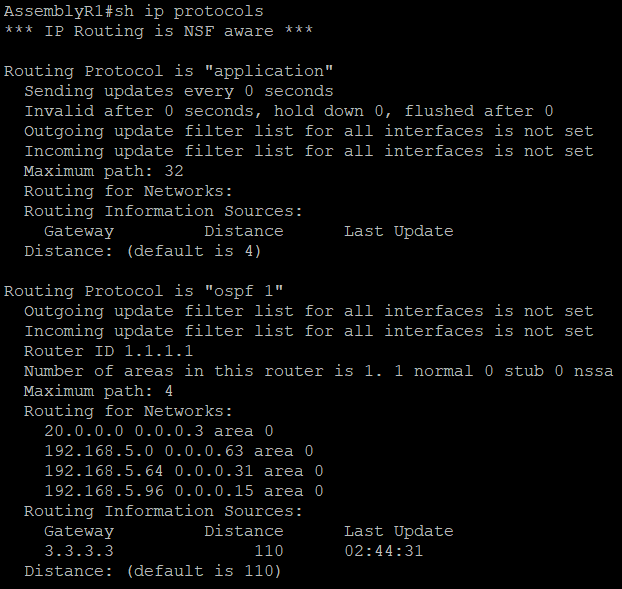
AssemblySW2 LACP tesztelése

# OSPF

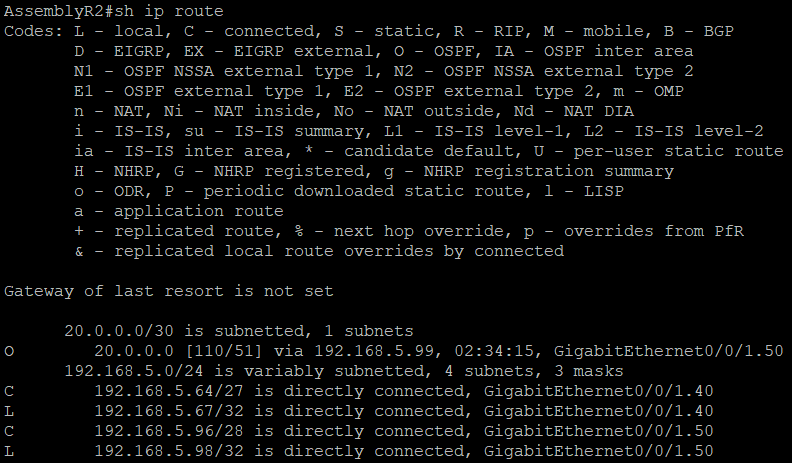
AssemblyR1 és AssemblyR2 irányítótáblája látható. Az alábbi ábrákon látható, hogy az OSPF irányító protokoll működik, ezt a legalsó sorban látható „O” betű jelzi, ami mellett látható a távoli hálózat.



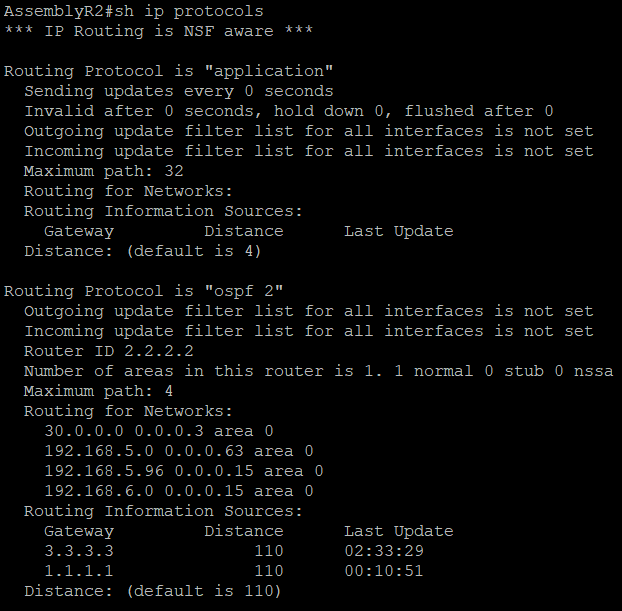
AssemblyR1 irányítótáblája



AssemblyR1 OSPF beállításai



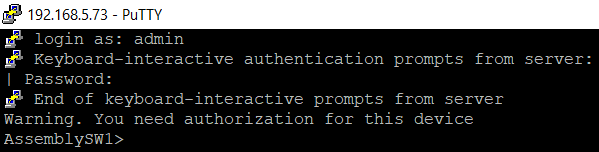
AssemblyR2 irányítótáblája



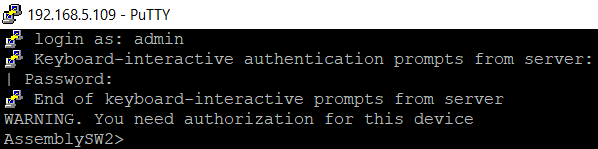
AssemblyR2 OSPF beállításai

# SSH tesztek

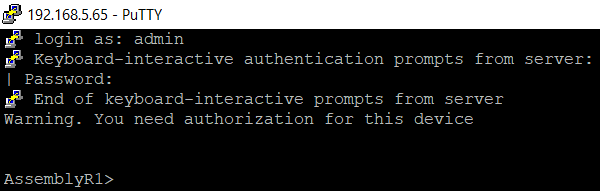
Az alábbi képeken a biztonságos távoli elérést teszteltük a routereken és a switcheken.



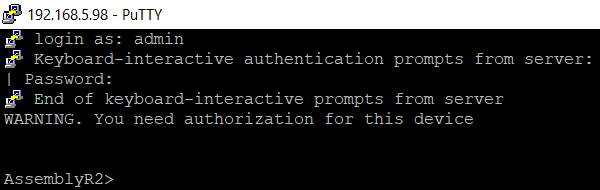
AssemblySW1 IP címen keresztüli biztonságos távoli elérése



AssemblySW2 IP címen keresztüli biztonságos távoli elérése



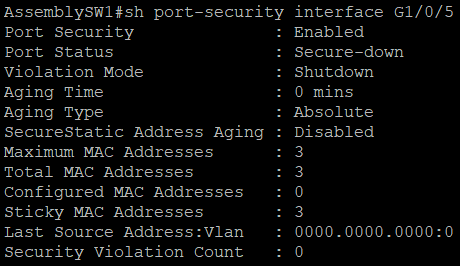
AssemblyR1 IP címen keresztüli biztonságos távoli elérése



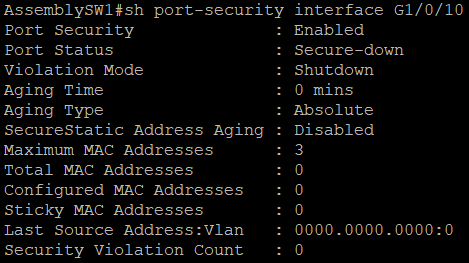
AssemblyR2 IP címen keresztüli biztonságos távoli elérése

# Port-security

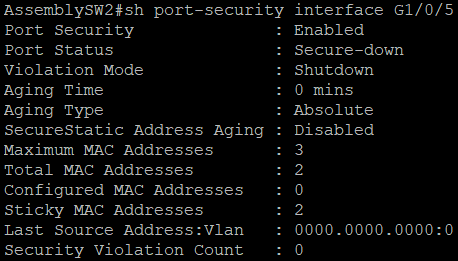
A képen a switchek PC és Webszerver felé irányuló portjai láthatók, biztonságossá téve port-security beállítással. Maximum 3 (Webszervernél 4) eszköz csatlakozhat a switchekhez, a mac-address címeket megjegyeztetjük, aki pedig 4. (Webszervernél 5.) eszközként akar csatlakozni, letiltjuk.



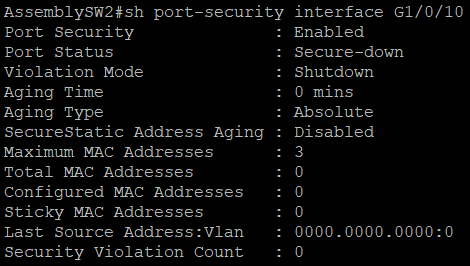
AssemblySW1 G1/0/5 Port-security beállítása



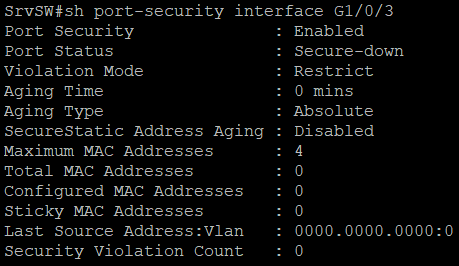
AssemblySW1 G1/0/10 Port-security beállítása



AssemblySW2 G1/0/5 Port-security beállítása



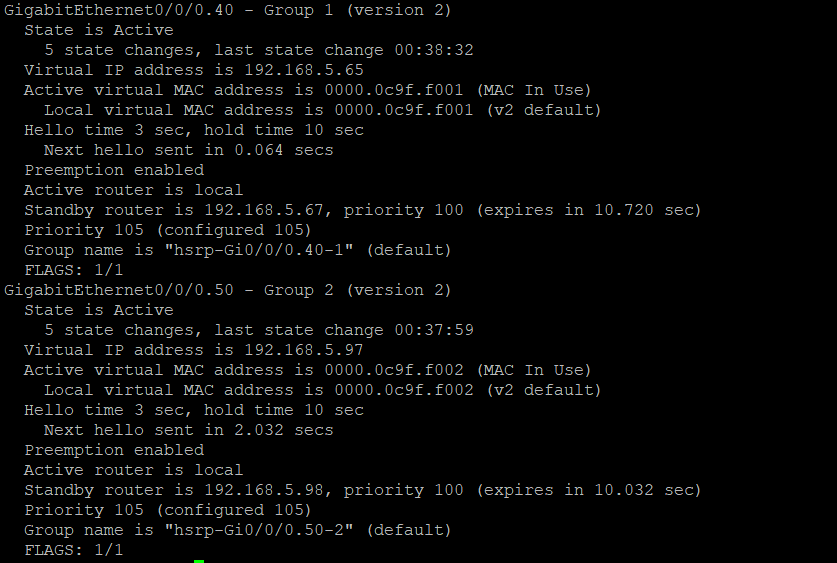
AssemblySW2 G1/0/10 Port-security beállítása



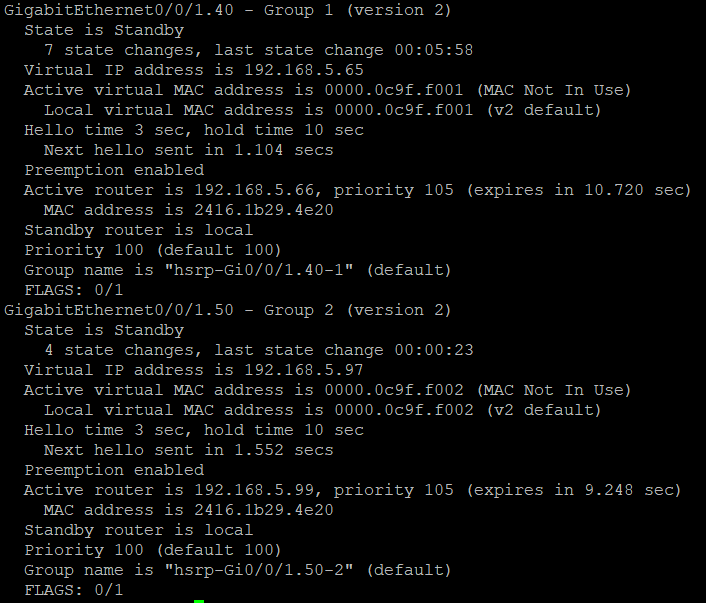
SrvSW G1/0/3 Port-security beállítása

# HSRP

Az alábbi képeken az AssemblyR1 és az AssemblyR2 HSRP beállítását láthatjuk. Lehetővé teszi, hogy két vagy több router egy virtuális routerként működjön, így ha az egyik router meghibásodik, a forgalom automatikusan az aktív másik routerre irányul, biztosítva a folyamatos kapcsolódást és a hálózati redundanciát.



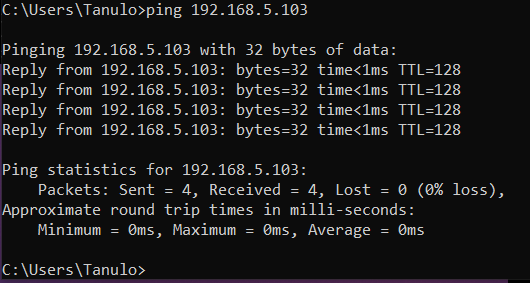
AssemblyR1 az Active router



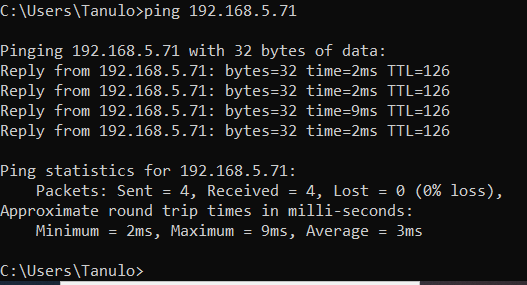
AssemblyR2 a Standby router

# Pingek

Teszteltük az eszközök közötti kapcsolatelérést többféle módon.



Két külön VLAN-ban lévő PC eléri egymást (PC1 pingeli a PC3-at)



Két azonos VLAN-ban lévő PC eléri egymást (PC1 pingeli a PC2-t)

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

Bármelyik PC eléri a Windows Servert

# DHCP Server (Windows)

A képen szöveg, képernyőkép, Betűtípus, sor látható

Lehet, hogy a mesterséges intelligencia által generált tartalom helytelen.

A képen szöveg, képernyőkép, képernyő, szoftver látható

Lehet, hogy a mesterséges intelligencia által generált tartalom helytelen.

# FTP Server (Windows)

Az FTP (File Transfer Protocol) egy fájl szerver szolgáltatás, amit arra használtunk, hogy a hálózati eszközeink (routerek, switchek) konfigurációs állományait kimásoljuk és tároljuk ezen a szerveren. A running configokat másoltuk ki.

A képen szöveg, képernyőkép, képernyő, szoftver látható

Lehet, hogy a mesterséges intelligencia által generált tartalom helytelen.

# Webserver (Windows)

Az alábbi képeken a Windows Webszerver tesztelése látható, amely könnyen integrálható a Windows-alapú környezetekkel, biztosítja a stabil és biztonságos működést, valamint széleskörű támogatást nyújt különböző webalkalmazásokhoz és szolgáltatásokhoz. Rugalmas konfigurálhatósága és fejlesztői eszközei révén egyszerűen kezelhető és skálázható.

A képen szöveg, képernyőkép, képernyő, szoftver látható

Lehet, hogy a mesterséges intelligencia által generált tartalom helytelen.

A képen szöveg, elektronika, képernyőkép, szoftver látható

Lehet, hogy a mesterséges intelligencia által generált tartalom helytelen.

# DNS Server (Ubuntu)

Az Ubuntu-s DNS Server szolgáltatást azért választottuk, mert megbízható és nyílt forráskódú megoldás, amely költséghatékonyan biztosítja a gyors és biztonságos névfeloldást a hálózaton belül. Ezen kívül jól integrálható más Ubuntu alapú rendszerekkel és könnyen skálázható a jövőbeni igényekhez. Egyetlen hátránya, hogy nehezen tudtuk bekonfigurálni, mivel beállítása körülményes, és 4-5 config fájlban is szerkesztenünk kellett.

A képen szöveg, képernyőkép, Betűtípus látható

Lehet, hogy a mesterséges intelligencia által generált tartalom helytelen.

# ACL

Az ACL-t azért állítottuk be, hogy pontosan szabályozhassuk, ki és milyen jogosultságokkal férhet hozzá a rendszer erőforrásaihoz, ezzel biztosítva a biztonságot és a jogosulatlan hozzáférés megakadályozását.



AssemblyR1 ACL beállítása

A képen szöveg, Betűtípus, képernyőkép, tipográfia látható

Lehet, hogy a mesterséges intelligencia által generált tartalom helytelen.

AssemblyR2 ACL beállítása

A képen szöveg, Betűtípus, képernyőkép, tipográfia látható

Lehet, hogy a mesterséges intelligencia által generált tartalom helytelen.

CENTER ACL beállítása

A képen szöveg, képernyőkép, Betűtípus látható

Lehet, hogy a mesterséges intelligencia által generált tartalom helytelen.

SrvR ACL beállítása

# Trace route

A Trace route-ot azért használjuk, hogy nyomon követhessük az adatforgalom útját a hálózaton, és azonosíthassuk a kapcsolat lassulásának vagy hibájának helyét.

A képen szöveg, képernyőkép, Betűtípus látható

Lehet, hogy a mesterséges intelligencia által generált tartalom helytelen.

# NAT (Network Address Translation)

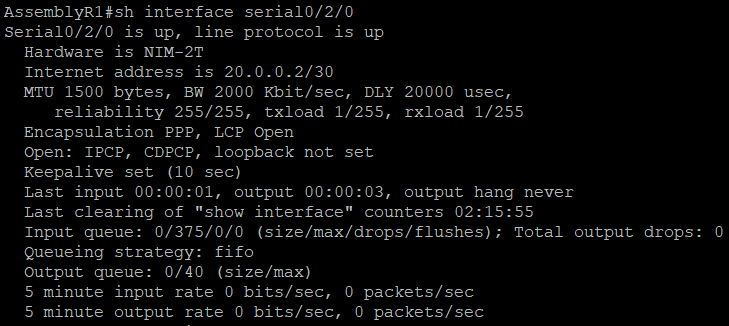
A NAT-ot (Network Address Translation) abból a célból használtuk, hogy a helyi hálózatunk eszközei egyetlen nyilvános IP-címen keresztül kommunikálhassanak az interneten, ezáltal növelve a hálózat biztonságát és hatékonyabban kihasználva az IP-címek korlátozott számát.

A képen szöveg, képernyőkép, Betűtípus látható

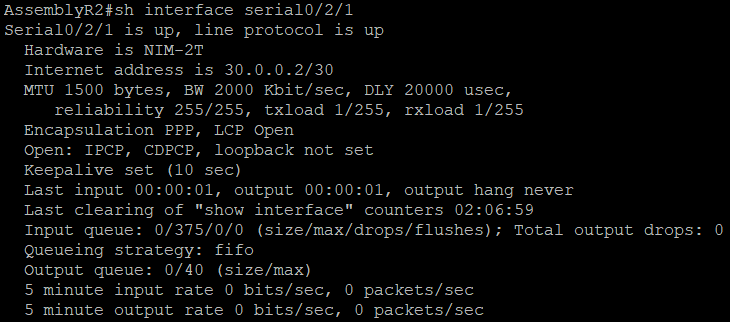
Automatikusan generált leírás

# PPP (Point-to-Point Protocol)

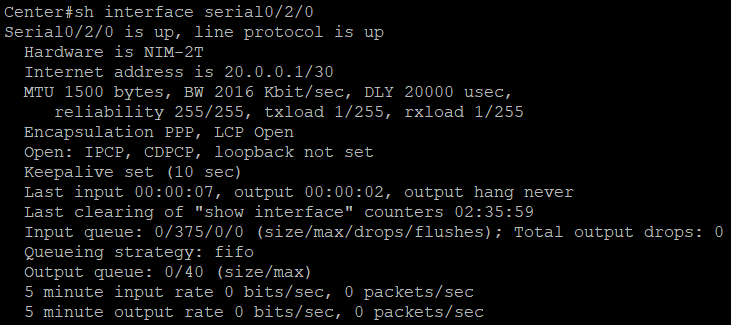
A PPP-t (Point-to-Point Protocol) azért alkalmaztuk, hogy biztosítsuk a hálózati kapcsolatok hitelesítését és a kommunikáció biztonságát. Ezáltal védelmet nyújtottunk az illetéktelen hozzáférés ellen, és garantáltuk, hogy csak a jogosult felhasználók férhessenek hozzá a rendszerhez.



AssemblyR1 PPP tesztelése



AssemblyR2 PPP tesztelése



CENTER PPP tesztelése