Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

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

***száma:*** 5-0612-12-02

**VIZSGAREMEK**

**General Logistics Systems Hungary  
(GLS)**

Pozsonyi Zsombor István, Mazács Levente, Zgyerka Máté  
2/14.B

Budapest, 2022.

Tartalomjegyzék

[**Forgalomirányítás:** 4](#_Toc133947330)

[**Hálózat rövid leírása:** 5](#_Toc133947331)

[**Budapest Központi Telephely** 5](#_Toc133947332)

[**Győri Telephely** 8](#_Toc133947333)

[**Debreceni Telephely** 10](#_Toc133947334)

[**DHCP:** 12](#_Toc133947335)

[**DHCP a hálózatunkban:** 12](#_Toc133947336)

[**DHCP snooping:** 14](#_Toc133947337)

[**DHCP snooping a hálózatunkban:** 15](#_Toc133947338)

[**HSRP:** 16](#_Toc133947339)

[**HSRP a hálózatunkban:** 16](#_Toc133947340)

[**Spanning-Tree:** 20](#_Toc133947341)

[**Spanning-tree a hálózatunkban:** 22](#_Toc133947342)

[**VTP:** 23](#_Toc133947343)

[**VTP a hálózatunkban:** 24](#_Toc133947344)

[**TFTP:** 26](#_Toc133947345)

[**TFTP a hálózatunkban:** 27](#_Toc133947346)

[**IPSEC:** 28](#_Toc133947347)

[**SYSLOG:** 31](#_Toc133947348)

[**SYSLOG a hálózatunkban:** 31](#_Toc133947349)

[**ETHERCHANNEL:** 32](#_Toc133947350)

[**ETHERCHANNEL a hálózatunkban:** 32](#_Toc133947351)

[**FTP:** 34](#_Toc133947352)

[**FTP a hálózatunkban:** 35](#_Toc133947353)

[**Hálózat programozás:** 36](#_Toc133947354)

[**Budapesti Szerverkörnyezet:** 37](#_Toc133947355)

[**DHCP/DHCP Failover:** 37](#_Toc133947356)

[**DNS:** 38](#_Toc133947357)

[**Debreceni Szerverkörnyezet:** 41](#_Toc133947358)

[**Mikrotik router:** 41](#_Toc133947359)

[**DHCP/DHCP Failover:** 41](#_Toc133947360)

[**DNS:** 43](#_Toc133947361)

[**Active Directory:** 45](#_Toc133947362)

[**Győri Szerverkörnyezet:** 46](#_Toc133947363)

# **Forgalomirányítás:**

A forgalomirányításhoz OSPF protokollt használunk. Az OSPF az Open Shortest Path Frist rövidítése, magyarul legrövidebb út először. Az OSPF egy kapcsolat alapú forgalomirányító protokoll.  
Jellemzői:

* gyors konvergencia
* osztály nélküli
* skálázható
* támogatja a VLSM és a CIDR
* hitelesített
  + MD5(Massage Digest) alapú hitelesítés

Az OSPF három adatbázist használ:

* adjacency database
* link-state database
* forwarding database

# **Hálózat rövid leírása:**

A General Logistics Systems Hungary központi telephelye Budapesten helyezkedik el, ezen felül két kisebb telephelye van Győrbe és Debrecenbe.

## **Budapest Központi Telephely**



Budapest Központi Telephelyen található egy ügyfélszolgálati rész, ahol 3 számítógép és 3 vonalas telefon található, ezek mellett egy közös hálózati nyomtató, ami az ügyfélszolgálaton dolgozók számára van fenntartva.



Ügyfélszolgálat mellett található egy Logisztikai rész, ahol 8 darab számítógép található, plusz egy hálózati nyomtató, ami a Logisztika részen dolgozók számára van fenntartva. Ezen a részen történnek a csomagszállítással kapcsolatos

logisztikai munkák, mint például a csomagok kézbesítéséhez szükséges útvonalak megtervezése.



Mint minden munkahelyen, itt is található egy külön főnöki iroda, ahol elhelyezkedik egy a főnöknek fenntartott számítógép, összekötve egy vezetékes telefonnal, és egy hálózati nyomtatóval.

Az adminnak, azaz a rendszergazdának fenntartott részen található 2 darab szerver, ez a két szerver felel a Budapesti Telephelyen elhelyezett eszközök IP-címzéséért, amit DHCP protokoll segítségével megy végbe. A fő szerver mellett elhelyezkedik egy Failover szerver, ami akkor lép életbe, ha esetleg a fő szerver meghibásodik, ekkor a Failover szerver teljes mértékben átveszi a feladatot a fő szervertől, amíg a hiba nincs elhárítva. A szerverek a DHCP kívül még egy fájl print szolgáltatást is ellátnak. Még található egy Admin számítógép, amiről a rendszergazda végzi a munkáját.

## **Győri Telephely**

Győri telephelyünk szintén 3 részre van felosztva, amely áll egy Győri ügyfélszolgálatból, egy Győri logisztikai részből, és egy Győri Admin szobából.



Győri Ügyfélszolgálaton található egy nyomtató és egy darab hálózati vezetékes telefon, amihez csatlakoztatva van Ethernet kábellel, egy dolgozói számítógép.

A Győri Logisztika helységben, található 3 darab dolgozói gép, amelyek Ethernet kábellel vannak csatlakoztatva a Switchez, ezen felül egy közös hálózati nyomtató is van telepítve, amit mind a három számítógépről ellehet érni.



Győri főnöki irodában, el lett helyezve egy hálózati vezetékes telefon, amely egy Ethernet kábelen keresztül csatlakozik a Switchbe, ehhez a vezetékes telefonhoz, csatlakoztatva van Ethernet kábellel egy főnöki számítógép, emellett még található egy hálózati nyomtató is.

A Győri Admin szobában, van 2 darab szerver, melyek a Győri telephelyet látják el megfelő IP címekkel DHCP protokoll segítségével. A két szerver közül az egyik egy Failover szerver, ami akkor lép életbe, ha esetlegesen a fő szerver meghibásodik, és leáll a működése. A szerverek a DHCP kívül még egy fájl print szolgáltatást is ellátnak. Ezek mellet természetesen elvan helyezve egy Admin számítógép, amiről a rendszergazda végzi a munkáját.

## **Debreceni Telephely**

Debreceni Ügyfélszolgálatunk szintén áll egy nyomtatóból és egy hálózati vezetékes telefonból, ami össze van kötve egy dolgozói számitógéppel.

Debreceni Logisztikai részen részen el lett helyezve 3 darab dolgozói számítógép, amelyek Ethernet kábellel vannak csatlakoztatva egy Switchez, és található egy közös hálózati nyomtató is.

A Debreceni Admin részen, található a már megszokott 2 darab szerver, melyek ellátják a Debreceni Telephelyet a megfelelő IP címekkel DHCP protokoll segítségével. A két darab szerver közül az egyik egy Failover szerver, mely azt a célt szolgálja, ha esetleges hiba folytán a Fő szerver meghibásodás miatt leáll, akkor ez a szerver veszi át a feladatait, amíg a hiba nincs elhárítva. A szerverek a DHCP kívül még egy fájl print szolgáltatást is ellátnak. El lett helyezve még egy Admin számítógép, amiről a rendszergazda tudja végezni a feladatait.

A Debreceni főnöki irodában szintén található egy hálózati vezetékes telefon, amely a már említett módon van csatlkaoztatva a Switchez, továbbá egy főnöki számítógép van Ethernet kábellel csatlakoztatva a vezetékes telefonhoz. Itt is el lett helyezve egy hálózati nyomtató.

# **DHCP:**

A DHCP (Dynamic Host Configuration Protocol) egy hálózati protokoll és szolgáltatás, amely lehetővé teszi a hálózati eszközöknek (például számítógépeknek, okostelefonoknak, nyomtatóknak) a hálózatba történő automatikus bekapcsolódását és az IP cím, a hálózati maszk és az alapértelmezett átjáró dinamikus hozzárendelését. A DHCP szerverek lehetővé teszik a hálózati eszközök számára az automatikus IP cím-kiosztást és az IP-cím konfliktusok elkerülését a hálózatban.

A DHCP szolgáltatás megkönnyíti a hálózati eszközök hozzáadását és konfigurálását, különösen a nagyobb hálózatok esetén. A DHCP szerver a hálózati eszközöknek automatikusan hozzárendel egy IP címet, amely a hálózat konfigurációjától függően átmeneti vagy statikus lehet. Az átmeneti IP címek általában csak ideiglenesen érvényesek, míg a statikus IP címek hosszabb távra szólnak, és általában az állandó eszközök (például szerverek) számára használatosak.

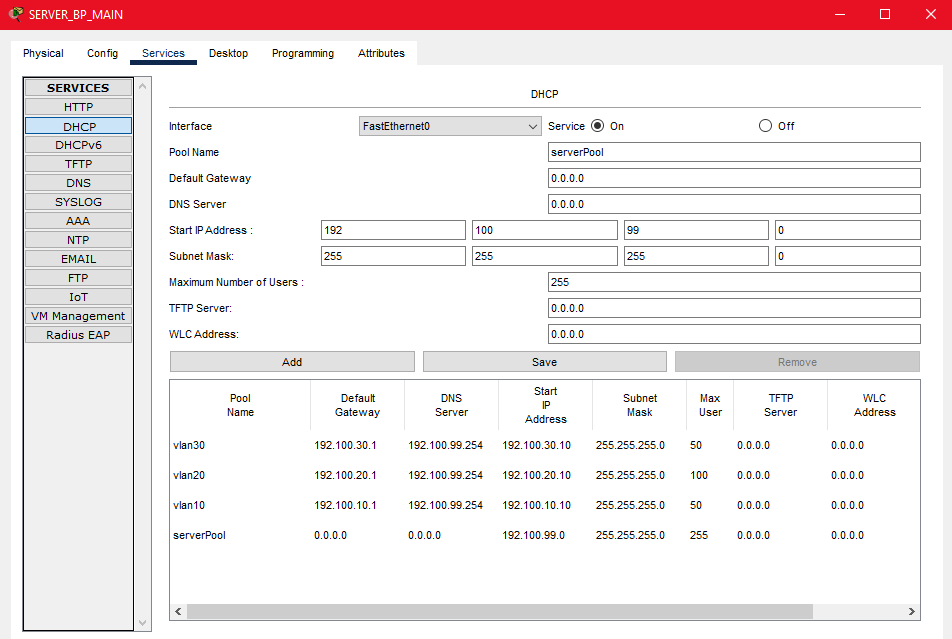
Használata lehetővé teszi a hálózati eszközök számára az automatikus beállítást és az egyszerűbb hálózatkezelést, miközben minimalizálja az IP-cím konfliktusokat és az emberi hibákat.

## **DHCP a hálózatunkban:**

Mindegyik telephelyen DHCP szolgáltatással osztottunk IP címeket a hálózati eszközeinknek (pl.: számítógép, telefon) a szerverek segítségével. Mind a három telephelyen külön VLAN-okra vannak osztva a helyek ezért mindegyik VLAN-nak külön-külön POOL-t kellet létrehozni.

A DHCP beállítások láthatóak a képeken, a Main és a Backup szervereken is van DHCP szolgáltatás, hogy ha leállna a Main szerver akkor ugyanúgy meglegyen az eszközök számára ez a szolgáltatás a Backup szerver részéről.

A képen asztal látható

Automatikusan generált leírás

# **DHCP snooping:**

A DHCP egy protokoll, amelyet a DHCP-kiszolgálók használnak IP-hálózatokban a hálózati konfigurációs adatok dinamikus kiosztására az ügyféleszközökhöz (DHCP-kliensekhez). A lehetséges hálózati konfigurációs adatok közé tartozik a felhasználói IP-cím, az alhálózati maszk, az alapértelmezett átjáró IP-címe, a DNS-kiszolgáló IP-címe és a bérlet időtartama. A DHCP protokoll lehetővé teszi a DHCP kliensek dinamikus konfigurálását az ilyen hálózati konfigurációs adatokkal, manuális beállítási folyamat nélkül.

A DHCP snooping egy biztonsági funkció, amely segít elkerülni a hálózaton lévő jogosulatlan DHCP-kiszolgálók által okozott problémákat, amelyek érvénytelen konfigurációs adatokat szolgáltatnak a DHCP-klienseknek. Egy rosszindulatú felhasználó akkor okozhatja ezt a problémát, ha tudtunk kívül olyan kapcsolót vagy más eszközt ad a hálózathoz, amely alapértelmezés szerint engedélyezve van a DHCP-kiszolgálóval. Egyes esetekben egy rosszindulatú felhasználó a szolgáltatásmegtagadás vagy a Man in the Middle támadás részeként DHCP-kiszolgálót ad a hálózathoz.

A DHCP snooping segít megelőzni az ilyen problémákat azáltal, hogy különbséget tesz a legitim DHCP-kiszolgálókhoz csatlakoztatott megbízható és az általános felhasználókhoz csatlakoztatott nem megbízható portok között. A DHCP-csomagok ellenőrzés nélkül továbbításra kerülnek a megbízható portok között. A más kapcsolóportokon érkező DHCP-csomagok továbbítás előtt ellenőrzésre kerülnek. A nem megbízható forrásból érkező DHCP-csomagokat a rendszer eldobja.

Mit csinál a DHCP Snooping?

* érvénytelen, nem megbízható DHCP üzenetek szűrése
* határértékek figyelése, megbízható és nem megbízható forrás esetén
* DHCP snooping adatbázist épít a megbízható állomásokról

## **DHCP snooping a hálózatunkban:**

Hálózatunkban DHCP snooping-ot alkalmaztunk, az esetleges támadások megakadályozása érdekében.

A DHCP snooping lehetővé teszi, hogy szűrjük a nem általunk szándékozott DHCP szolgáltatás használatát.

Ezt a szolgáltatást a switcheken a megfelelő portokon állítottuk be, annak érdekében, hogy ismeretlen DHCP offer és DHCP apk csomagok ne juthassanak el a hálózatunkban található számítógépeinkhez.

Ehhez használt parancsok:

# **HSRP:**

A HSRP (Hot Standby Router Protocol) működése nagyon egyszerű. A protokol egy virtuális IP címet kínál fel a LAN hálózatunk számára alapértelmezett átjáróként. Ezt a virtuális IP címet fogjuk alapértelmezett átjáróként beállítani a LAN állomásain. A virtuális IP címen több forgalomirányító is osztozik, egymás között megbeszélve, hogy melyikük fogja az alapértelmezett átjáró feladatát ellátni, vagyis a tényleges adatforgalmat közvetíteni. A virtuális IP cím mellé egy virtuális MAC címet is rendel a HSRP.

Azt a forgalomirányítót, amelyik a tényleges adatforgalmat közvetíti, **aktív (active)** forgalomirányítónak nevezzük. Az, hogy melyik lesz az aktív, egy választás eredménye. Minden forgalomirányítóhoz rendelünk egy prioritást, és amelyiké a legnagyobb, az kapja meg az aktív szerepet. A második legmagasabb prioritású forgalomirányító kapja meg a **tartalék (standby)** szerepet, míg a többiek **figyelő (lsiten)** állapotba kerülnek. Ha az aktív kiesik, akkor a tartalék forgalomirányítónak van egy beállított, alapértelmezett HSRP prioritása, melynek értéke 100. Amennyiben a két forgalomirányítónak azonos a prioritása, akkor a LAN-hoz kapcsolódó interfész IP címe alapján döntik el, hogy melyik legyen a sorban elől.

## **HSRP a hálózatunkban:**

Minden egyes telephelyünkön alkalmaztunk HSRP protokollt, az esetleges meghibásodások esetén kialakuló hibák megellőzése érdekében.

Mind a három telephelyünkön 4 VLAN található, ebből kifolyólag mindegyik telephelyünkön 4 darab virtuális IP címet kellet bekonfigurálnunk, melyek az adott VLAN-ok alapértelmezett átjáróijuk lesznek.

**A Budapesti telephelyen az alábbi módon néz ki:**

A Main router kapta az adott IP cím tartományban a második IP címet, a Backup router pedig a harmadik IP címet. A virtuális IP cím az adott cím tartományban az első IP-t kapta.

**A Main Router címei (ROUTER\_BP\_MAIN):**

A képen szöveg látható

Automatikusan generált leírás

**A Backup Router címei (ROUTER\_BP\_BACKUP):**

A képen szöveg látható

Automatikusan generált leírás

**Konfiguráció:**

A képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírás **Main Router konfigurációja:**

A képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírás

Mint ahogy a konfigurációban is látszik, előszőr az adott alinterfésznek az IP címét adtuk meg, ami minden esetben a második kiosztható cím, majd ezután a HSRP verzióját állítottuk be. Megadtunk a HSRP-nek az azonosítóját és a hozzá tartozó virtuális IP címet. Ezek után, mivel ez a Main Router konfigurációja, állítottunk prioritást, melynek értéke 110 lett, hogy ez a Router kapja meg az aktív szerepet.

**A képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírásBack Router konfigurációja:**

A képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírás

A Backup router konfigurációjában annyi eltérés található, hogy az adott IP cím tartományban a harmadik IP címet kapta minden esetben. Itt prioritást hagytuk az alapértelmezett értéken, ami 100-as, ezáltal ez a router kapta a tartalék szerepet.

Ugyanezen a módon csináltuk a másik két telephelyen is.

**A Győri telephelyen az alábbi módon néz ki:**

**A Main Router címei (ROUTER\_GY\_MAIN):**

A képen szöveg látható

Automatikusan generált leírás

**A Backup Router címei (ROUTER\_GY\_BACKUP):**

A képen szöveg látható

Automatikusan generált leírás

**Konfiguráció:**

A képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírás **Main Router konfigurációja:**

A képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírás

A képen szöveg látható

Automatikusan generált leírás**Backup Router konfigurációja:**

A képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírás

# **Spanning-Tree:**

A Spanning-tree-t, azaz feszítőfa protokolt a redundánsan kiépített LAN eszközök esetén használt algoritmus, amely a hurkok kialakulását képes megakadályozni.

**A redundancia:**

A redundanciát a hálózatok terén azért alkalmazzuk mert ezzel növeljük a megbízhatóságot. Az eszközök között így alternatív útvonalak állnak rendelkezésre. Az alternatív útvonalak viszont problémához vezethetnek, ha egy-egy csomag körbe jár a redundáns útvonalakon.

Ha redundánsan kötünk össze kapcsolókat, azok automatikus tanulási és továbbítási működése miatt, természetes módon alakulnak ki a hurkok. Ehhez hozzájárul az is, hogy a második rétegben működő kereteknek nincs lejárati ideje, azaz Time To Live számlálójuk.

A feszítőfa protokoll biztosítja, hurkok elkerülését. A protokoll két járható port közül az egyiket mindig zárva tartja, tartaléknak. Az így lezárt porton csak akkor enged forgalmat, ha az elsődleges útvonal meghibásodik.

A lezárt portokat az STP saját céljaira használja, úgynevezett BPDU-keretek küldésére. A **BPDU**, a **Bridge Protocol Data Unit**, rövidítése, magyarul hídprotokoll adategységnek fordítható. Egy BPDU üzenet portokról, címekről, prioritásokról és költségekről tartalmaz információkat, amelyek biztosítják a hurkok felismerését.

A feszítőfa protokollnak többféle megvalósítása létezik:

* RSTP - Rapid Spanning Tree Protocol
* MSTP - Multiple Spanning Tree Protocol

Az STP protokoll az **STA**, azaz **Spanning Tree Algorithm**, magyarul feszítőfa algoritmust használja. Az algoritmus kiválaszt egy kapcsolót, amelyet referenciaként használ. A kiválasztott kapcsolót nevezzük gyökérponti hídnak, angolosan root bridge. Az STA algoritmus ezt a híd azonosító alapján dönti el. Akinek a legkisebb a hídazonosítója, az lesz a gyökérponti híd.

A hídazonosító több érték összetevője:

* prioritás
* a küldő MAC címe
* opcionálisan egy kiterjesztett rendszer azonosító is

Az STA tehát megállapítja, melyik kapcsolónak legalacsonyabb a hídazonosítója. Ezek után az algoritmus kiszámolja a gyökéri ponti hídhoz vezető legrövidebb útvonalakat, a portok és útvonalak költségét is beleszámolva. Ha több útvonal van, a legkisebb költségű útvonalon engedi a forgalmat.

Ha minden kapcsoló számára kiszámította a gyökérponti hídhoz képest előnyben részesített utakat, az STA minden porthoz egy szerepet rendel. Ezek a szerepek a következő lehetnek:

* RP – gyökér port
* DP – kijelölt port – designated port
* AP – tartalék port – backup port
* letiltott port – shut down port
* szélső port – edge port

## **Spanning-tree a hálózatunkban:**

# **VTP:**

A VTP vagy VLAN Trunking Protocol egy 2. szintű protokoll, amelyet a VLAN konfigurálásához és kezeléséhez használnak a Cisco eszközökön.

A VTP lehetővé teszi egy vagy több VLAN hozzáadását, átnevezését vagy törlését egyetlen kapcsolón (a szerveren), amely ezt az új konfigurációt továbbítja a hálózat összes többi kapcsolójára (kliensekre). A VTP így elkerüli az esetleges következetlenségeket a VLAN-ok konfigurációjában az egész helyi hálózaton.

A VTP a Cisco kapcsolókon működik a következő 3 mód egyikében:

* client
* server
* transparent

**SERVER:** A switchet VTP szerver módba állítja. Ebben a módban a switch hirdeti a VLAN információkat. Engedélyezve van a Vlan konfigurálása. A switch vissza tudja állítani a VLAN információkat a VTP adatbázisból (VTP database), amely a nem felejtő memóriában van, újraindítás után is.

**CLIENT:** A switchet VTP kliens módba állítja. A VTP engedélyezve van, és hirdetéseket tud küldeni, de nincs elég nemfelejtő memóriája a VLAN konfiguráció tárolására. Ebben a módban VLAN konfigurálására nincs mód. Ameddig a VTP kliens el nem indul, nem hirdet VTP információt, amíg a fogadott hirdetésekből fel nem építi a switch, a saját VLAN adatbázisát.

**TRANSPARENT:** A switchet VTP transzparens módba állítja. A switchben ilyenkor a VTP le van tiltva. Nem küld hirdetéseket, és nem is tanul a kapott hirdetésekből, nincs hatása a VLAN konfigurációjának más, a hálózatban lévő eszközre. A switch a vett VTP hirdetéseket minden trönk portjára kiadja, kivéve azt a portot, amelyen a hirdetést fogadta. A multi-VLAN portok a switchet automatikusan transzparens módba állítja.

## **VTP a hálózatunkban:**

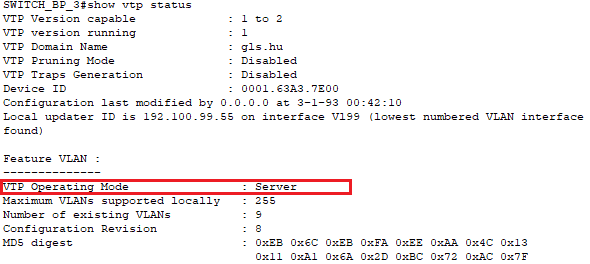
A képen diagram, sematikus rajz látható

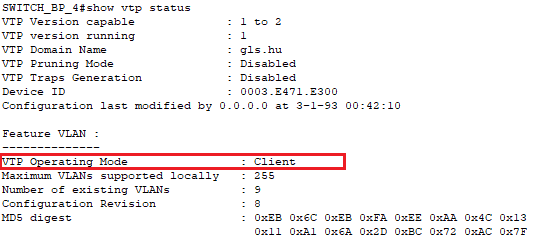
Automatikusan generált leírásA VTP bekonfigurálása a következőképpen nézett ki, kiválasztottunk egy adott swicthet a telephelyeken, amelyek a Szerver switch szerepét fogják betölteni. A Budapesti telephely esetében ez a SWITCH\_BP\_3 nevű switch lett. Ezen a switchen létrehoztunk egy vtp domain címet, ami **gls.hu** lett.

Ezután létrehoztunk egy egy vtp passwordot, ami **gls123**(csak a dokumentálás céljából) lett.

Majd ezek után a képen látható parancssal megadtuk, hogy ez a switch lesz a szerver switch.

Ezeket a beállításokat megtettük az adott telephelyen lévő összes switchen, természetesen ezeket már kliens módba állítottuk.

**SWICTH\_BP\_3 státusza:**

**SWICTH\_BP\_4 státusza:**

# **TFTP:**

A TFTP (Trivial File Transfer Protocol) egy egyszerű és minimális funkciókat biztosító hálózati protokoll és szolgáltatás, amely lehetővé teszi fájlok gyors és hatékony átvitelét a hálózatban. A TFTP protokollt általában olyan környezetekben használják, ahol a teljes FTP (File Transfer Protocol) rendszer túl bonyolult vagy túl nagy méretű. A TFTP különösen hasznos lehet például a hálózati berendezések konfigurálásához, frissítéséhez vagy helyreállításához, ahol a rendszer távoli helyen van vagy csak korlátozott hozzáférés áll rendelkezésre.

A TFTP szolgáltatás alapvetően egy kliens-szerver alapú rendszer, ahol a kliens kérheti a szervertől a fájlokat, és a szerver továbbítja a kért fájlt a kliensnek. A TFTP protokoll nagyon egyszerű, csak minimális biztonsági funkciókkal és hibakezeléssel rendelkezik. Ennek eredményeként a TFTP fájlok átvitele nagyon gyors és hatékony, de a fájlok megsérülhetnek vagy elveszhetnek, ha valamilyen hiba merül fel a folyamat során.

Gyakran használják a hálózati eszközök (például router, kapcsolók, tűzfalak) konfigurálásához és frissítéséhez, valamint az operációs rendszerek telepítéséhez és frissítéséhez. Emellett a TFTP-t használják a hálózati hibakereséshez és a helyreállítási folyamatokhoz, például a meghibásodott rendszerek helyreállításához.

## **TFTP a hálózatunkban:**

Hálózatunkban a TFTP szolgáltatást leginkább az eszközök konfigurációjának mentésére használtunk, amelyeket feltöltöttünk a szerverekre.

A képen szöveg látható

Automatikusan generált leírásEzzel a paranccsal lehet feltölteni a TFTP szerverre az adott eszköz konfigurációját.

A képen szöveg látható

Automatikusan generált leírásItt látszódik, hogy a szerverre felvannak töltve az adott telephely eszközeinek a konfigurációik.

# **IPSEC:**

Az IPSec protokoll a TCP/IP architektúra hálózati rétegének szabványosított biztonsági protokollja. Ez azt jelenti, hogy az IP és minden fölötte található protokoll (TCP, UDP, ICMP stb.) számára védelmet biztosít.

Két alprotokollja van, az AH (**Authentication Header**) és az ESP (**Encapsulated Security Payload**). Az AH és az ESP protokollok kombinálhatók az IP csomagok teljeskörű védelme érdekében.

Az IPSec protokollhoz tartoznak még az ISAKMP (Internet Security Association and Key ManagementProtocol) és az IKE (Internet Key Exchange) protokollok. Mindkettő kulcscserével kapcsolatos feladatokat lát el.

**AH protokoll**

Az AH protokoll

* integritásvédelmet,
* eredethitelesítést
* visszajátszás elleni védelmet

biztosít az IP csomagok számára.

**AH fejléc**

|  |  |  |
| --- | --- | --- |
| Köv. fejléc | hossz | foglalat |
| Security Parameters Index (SPI) | | |
| sorszám | | |
| MAC | | |

Az integritásvédelmet és az eredethitelesítést úgy éri el, hogy az IP fejléc és az azt követő felsőbb szintű protokoll fejléce közé beszúr egy AH fejlécet, mely egy, a teljes IP csomagra számolt üzenethitelesítő kódot (MAC) tartalmaz.

A visszajátszások detektálásának érdekében, az IP csomagokat sorszámozza.

Az AH fejlécben található MAC érték a sorszámot is védi.

* **Következő fejléc**: Ez a mező az AH fejlécet követő fejléc típusát adja meg, azaz az IP csomag tartalmára utal.
* **Hossz:** Ez a mező az AH fejléc 32 bites szavakban mért hosszára utal.
* **Security Parameter Index (SPI):** Ez egy azonosító, mellyel a küldő azt jelzi a vevő számára, hogy milyen módon és mely kulcsokat használva kell az AH fejlécét feldolgozni. Az AH protokoll feltételezi, hogy a küldő és a vevő korábban már megegyezett az alkalmazható algoritmusokban és kulcsokban, tipikusan az ISAKMP/IKE protokollokat használva.
* **sorszám:** Ez a mező az aktuális IP csomag sorszámát tartalmazza.

**ESP protokoll**

Az ESP protokoll feladata

* IP csomag tartalmának rejtése
* a tartalom integritásának védelme

Az előbbit az IP csomag tartalmának rejtjelezésével oldja meg a protokoll, az utóbbit pedig úgy, hogy az ESP fejlécre és a csomag tartalmára számít MAC kódot és azt a csomaghoz csatolja.

Az AH-val ellentétben az ESP MAC nem védi az IP fejléc mezőit.

**ESP-vel védett csomag felépítése**



**IPSEC üzemmódok**

Mind az AH, mind az ESP protokollt két üzemmódban lehet használni. Ezeket szállítási (transport) és alagút (tunnel) módoknak nevezzük. Szállítási módban az AH vagy az ESP fejléc a csomag eredeti IP fejléce és a felsőbb szintű protokoll (például TCP, UDP) fejléce közé kerül. Alagút módban azonban az eredeti IP csomagot teljes egészében beágyazzuk egy másik IP csomagba (IP tunneling), és az AH vagy az ESP fejléc az új, és az eredeti IP fejléc közé kerül.

# **VPN:**

A tunnel alapú VPN (Virtual Private Network) egy olyan technológia, amely lehetővé teszi a felhasználók számára, hogy biztonságosan és titkosítottan csatlakozzanak a hálózathoz vagy az internethez egy virtuális "tunnel" (alagút) segítségével.

A létrehozása során az adatok egy titkosított "alagútban" utaznak az interneten keresztül, így védelmet nyújtanak a kibertámadások és az adathalászat ellen. Az alagút létrehozásához a VPN protokoll (például az IPsec, SSL vagy TLS) biztonsági funkcióit használják.

Két fő típusa van: a szerver oldali és a kliens oldali. A szerver oldali VPN-t a vállalatok és szervezetek használják, hogy távoli munkatársaik biztonságosan és titkosítottan csatlakozhassanak a vállalati hálózathoz. A kliens oldali VPN-t pedig az egyéni felhasználók használják, hogy biztonságosan csatlakozzanak az internethez, és védelmet nyújtsanak a nyilvános Wi-Fi hálózatokon való internetezés során.

A képen szöveg látható

Automatikusan generált leírásSok előnnyel rendelkezik, beleértve a biztonságot, az adatvédelmet, a titkosítást, a hálózati elérhetőséget és az internetes korlátozások áthidalását. Ezért a VPN technológia egyre elterjedtebbé válik a vállalatok és az egyéni felhasználók körében is.

# **SYSLOG:**

A SYSLOG egy szabványosított protokoll és szolgáltatás a hálózati eszközök és rendszerek által generált naplóbejegyzések küldéséhez, gyűjtéséhez és feldolgozásához. A SYSLOG lehetővé teszi a rendszergazdák számára, hogy figyelemmel kísérjék és ellenőrizzék a hálózati eszközök és alkalmazások teljesítményét, állapotát és biztonságát, valamint az esetleges hibák és problémák időben történő felismerését és kezelését. A SYSLOG rendszerek általában egy központi naplószerverre küldik a naplóbejegyzéseket, ahol a rendszergazdák könnyen áttekintést kaphatnak az összes eszköz és alkalmazás aktivitásáról. A SYSLOG protokoll számos implementációval rendelkezik, és általában széles körben elérhető a legtöbb hálózati eszközön és szerveren.

## **SYSLOG a hálózatunkban:**

A routereken a „logging” parancs segítségével adtuk meg, hogy mely szerverekre küldjön SYSLOG logokat a hálózat eszközeinek aktivitásáról.

A képen szöveg látható

Automatikusan generált leírásA main és backup szerverekre is megy a SYSLOG logolás.

A szervereken a SYSLOG szolgáltatást bekapcsoltuk, innentől fogva látszódnak a hálózat különböző logolásai.

# **ETHERCHANNEL:**

Az EtherChannel egy hálózati technológia, amely lehetővé teszi, hogy több Ethernet interfész összevonása után nagyobb sávszélességet és redundanciát biztosítson a hálózati kapcsolatokban. Az EtherChannelt gyakran használják a nagyobb hálózatokban, ahol a magas rendelkezésre állás és a megbízhatóság elengedhetetlen.

Lehetővé teszi a hálózati eszközök (például switchek) összekapcsolását, hogy egyetlen logikai csatornát hozzanak létre, amely magasabb sávszélességet és redundanciát biztosít a hálózati forgalom számára. Az EtherChannel használatával a hálózati eszközök képesek elosztani a forgalmat a többi csatorna között, ami javítja a teljesítményt és a megbízhatóságot.

Alkalmazása előnyös lehet olyan esetekben, amikor a hálózati forgalom magas, és nagyobb sávszélesség szükséges. Emellett az EtherChannel lehetővé teszi a hálózati eszközök redundanciájának növelését, így ha egy interfész meghibásodik, a hálózat még mindig működik, mivel az átviteli kapacitásokat az EtherChannel más interfészei veszik át. Az EtherChannel további előnye, hogy csökkenti a hálózati eszközök adminisztrációs terheit, mivel egyetlen logikai csatornát kezel, nem pedig külön-külön az interfészeket.

## **ETHERCHANNEL a hálózatunkban:**

Az etherchannel technológiát a swictheink között alkalmaztunk, hogy nagyobb sávszélességet és redundanciát biztosítson.

A képen diagram látható

Automatikusan generált leírásA képen látható swicthek-nél 6 különböző channelt hoztunk létre ezzel is növelve a biztonságot.

Ezen a képen a SWICTH\_BP\_3 swicth „show etherchannel summary” parancs kimenetelét láthatjuk, amely megmutatja, hogy hány darab channel-t használ, hogy melyek azok a channel-ek pontosan és hogy mely portokat használja ezekhez.

A képen asztal látható

Automatikusan generált leírás

# **FTP:**

Az FTP (File Transfer Protocol) egy protokoll és szolgáltatás, amely lehetővé teszi a fájlok átvitelét az interneten keresztül. Az FTP egy kliens-szerver alapú rendszer, ahol a kliens számítógép kapcsolódik a szerverhez, majd fájlokat tölthet le a szerverről, vagy feltöltheti a szerverre. Az FTP rendszer általában a hálózati szolgáltatók és a szerverek számára biztosított szolgáltatás, amely lehetővé teszi az ügyfelek számára a fájlok tárolását és megosztását az interneten keresztül.

Egyértelmű utasításokat tartalmaz a fájlok átvitelére, és lehetővé teszi a fájlok másolását és mozgatását a kliens és a szerver között. Az FTP szolgáltatás segítségével lehetőség van fájlok letöltésére és feltöltésére, fájlok másolására, törlésére és áthelyezésére. Az FTP-t gyakran használják weboldalakat és fájlokat tároló szerverek kezeléséhez, valamint az internetes fájlcserékhez és a tartalom megosztásához.

## **FTP a hálózatunkban:**

A képen szöveg látható

Automatikusan generált leírásAz FTP szolgáltatásunkba felvettük mind a négy résznek egy saját felhasználóját, amellyel könnyedén feltudnak tölteni fájlokat a szerverre és könnyedén le is tudjak tölteni azokat. Ezzel könnyítve a fájlok és adatok mozgatását az irodák között.

# **Hálózat programozás:**

Program kód:

A képen szöveg látható

Automatikusan generált leírás

A program célja hogy megkönnyítse a rendszer gazdák munkáját, hogy gyorsabban lehessen a port security esetleges hibáit elhárítani. A script ip címmel, ssh username és jelszót kér el a felhasználótól futás közben majd csatlakozik a kívánt switchre ssh keresztül. A program helyes futása után egy log fájlba kiírja a show port-security parancs kimenetelét.

# **Budapesti Szerverkörnyezet:**

A mikrotik routerünket az alábbi módon konfiguráltuk be.

Itt látható **az ip address print** és **az ip firewall nat** print kimenetele:

A 192.168.99.254-es IP címet és az 50000-es port számot a PDC szerverünknek tartjuk fent.

A képen szöveg látható

Automatikusan generált leírásA 192.168.99.253-as IP címet és az 50001-es port számot pedig a BDC szerverünknek tarjuk fent.

## **DHCP/DHCP Failover:**

A DHCP-t a fő szerverünkön keresztül konfiguráltuk be, amelyen több pool-t is létrehoztunk a különböző helységek és VLAN-ok számára.

A képen szöveg látható

Automatikusan generált leírásA képen látható IP-cím felosztásba lettek megadva a DHCP paraméterei:

A képen jól látható, hogy DHCP Failover szervernek a BDC szerverünk lett beállítva, ez a szolgáltatás abban az esetben lép működésbe, ha valamilyen hiba folytán a PDC azaz a fő szerverünk leáll, ekkor a BDC szerver veszi át a DHCP cím osztás szerepét.

A kép demonstrálja, hogy a BDC szerverre sikeresen átmentek a DHCP beállítások.

A képen szöveg látható

Automatikusan generált leírás

DNS szervernek megvan adva természetesen a PDC szerverünk és a BDC szerverünk IP címe.

A képen szöveg látható

Automatikusan generált leírás

## **DNS:**

DNS domain name-nek **debrecengls.kft** lett beállítva.

Forward Lookip Zones paraméterei:

A képen szöveg látható

Automatikusan generált leírásReverse Lookup Zones paraméterei:

Users and Computers:

A képen asztal látható

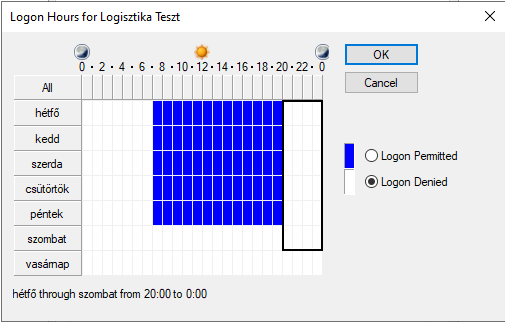
Automatikusan generált leírásItt látható, hogy milyen beosztások szerint vannak a felhasználók/dolgozók felosztva.

A képen szöveg látható

Automatikusan generált leírás

Ezek alapján hoztunk létre Groupokat, amibe az adott pozíción dolgozókat felvesszük, ezáltal tudjuk az ők által használt felhasználókat konfigurálni (pl.: milyen szolgáltatásokhoz férjenek hozzá a saját profiljukkal).

Mindegyik itt dolgozónak beállítottuk, hogy csak a munka idejében legyen képes bejelentkezi a felhasználójával a gépre.



# **Debreceni Szerverkörnyezet:**

## **Mikrotik router:**

A mikrotik routerünket az alábbi módon konfiguráltuk be.

Itt látható **az ip address print** és **az ip firewall nat** print kimenetele:

A 192.200.99.254-es IP címet és az 50000-es port számot a PDC szerverünknek tartjuk fent.

A 192.200.99.253-as IP címet és az 50001-es port számot pedig a BDC szerverünknek tarjuk fent.

A képen szöveg látható

Automatikusan generált leírás

## **DHCP/DHCP Failover:**

A DHCP-t a fő szerverünkön keresztül konfiguráltuk be, amelyen több pool-t is létrehoztunk a különböző helységek és VLAN-ok számára.

A képen látható IP-cím felosztásba lettek megadva a DHCP paraméterei:



A képen jól látható, hogy DHCP Failover szervernek a BDC szerverünk lett beállítva, ez a szolgáltatás abban az esetben lép működésbe, ha valamilyen hiba folytán a PDC azaz a fő szerverünk leáll, ekkor a BDC szerver veszi át a DHCP cím osztás szerepét.

A kép demonstrálja, hogy a BDC szerverre sikeresen átmentek a DHCP beállítások.

A képen szöveg látható

Automatikusan generált leírás

A képen az Ügyfélszolgálatos helység DHCP paraméterei láthatóak:

Az alapértelmezett átjáró a cím tartomány legelső címe, a többi pool-ba is e szerint jártunk el.

DNS szervernek megvan adva természetesen a PDC szerverünk és a BDC szerverünk IP címe.

A képen szöveg látható

Automatikusan generált leírás

Egy windows kliens-el jól lehet szemléltetni a DHCP Failover működését.

Amint leáll a PDC szerver, onnantól kezdve a BDC szerver veszi át a feladatot.

**PDC szerver működése közben:**



**PDC szerver leállása után:**

****

## **DNS:**

DNS domain name-nek **debrecengls.kft** lett beállítva.

Forward Lookip Zones paraméterei:

A képen asztal látható

Automatikusan generált leírás

Reverse Lookup Zones paraméterei:

A képen szöveg látható

Automatikusan generált leírás

## **Active Directory:**

Users and Computers:

Itt látható, hogy milyen beosztások szerint vannak a felhasználók/dolgozók felosztva.



Ezek alapján hoztunk létre Groupokat, amibe az adott pozíción dolgozókat felvesszük, ezáltal tudjuk az ők által használt felhasználókat konfigurálni (pl.: milyen szolgáltatásokhoz férjenek hozzá a saját profiljukkal).

Mindegyik itt dolgozónak beállítottuk, hogy csak a munka idejében legyen képes bejelentkezi a felhasználójával a gépre.



# **Győri Szerverkörnyezet:**

# **Kép Források:**

https://support.huawei.com/enterprise/en/doc/EDOC1100041799/f2298f86/using-ipsec-vpn-to-implement-secure-interconnection-between-lans