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: 3](#_Toc118924191)

[DHCP snooping: 7](#_Toc118924192)

[Spanning-Tree: 8](#_Toc118924193)

[Spanning-tree a hálózatunkban: 10](#_Toc118924194)

# 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

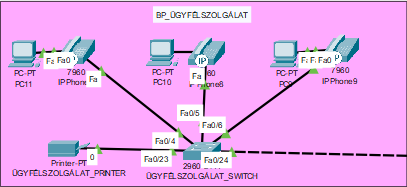
A General Logistics Systems Hungary központi telephelye Budapesten helyezkedik el, ezen felül két kisebb telephelye van Győrbe és Debrecenbe.

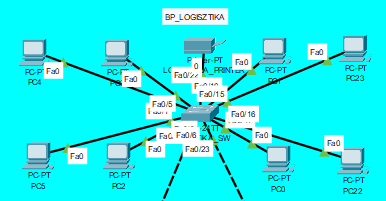
**Budapest Központi Telephely**

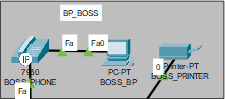
A képen térkép látható

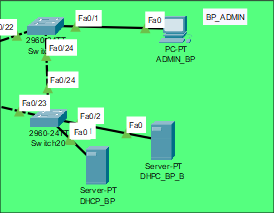
Automatikusan generált leírás

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 segítségével visz végbe. A szerver mellett elhelyezkedik egy úgynevezett 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. Még található egy Admin számítógép, amiről a rendszergazda végzi a munkáját.

# DHCP snooping:

Egy biztonsági megoldás a megbízható DHCP szerverek és a nem megbízható állomások között.

Mit csinál a DHCP Snooping?

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

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:

A 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: