Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

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

***száma:*** 5-0612-12-02

**VIZSGAREMEK**  
**Szász Tamás István korház bemutatása**

Fazekas Gábor János, Hrazdyra Norbert Krisztián, Kun Leon

2/14B

Budapest, 2024.

Tartalom

[Cégleírás 3](#_Toc152673117)

[A hálózat dokumentációja 4](#_Toc152673118)

[Kék terület 4](#_Toc152673119)

[VLAN (Virutal Local Area Network) 6](#_Toc152673120)

[VTP (VLAN Trunk Protocol) 7](#_Toc152673121)

[PAgP (Port Aggregation Protocol) 7](#_Toc152673122)

[Feszitőfa protokoll (Spanning Tree Protocol) 8](#_Toc152673123)

[DHCP (Dynamic Host Configuration Protocol) 9](#_Toc152673124)

[HSRP (Hot Standby Router Protocol) 10](#_Toc152673125)

[FTP (File Transfer Protocol) 11](#_Toc152673126)

# Cégleírás

Az InnoTech Networks kft. a hálózati megoldások szakértője, aki magas színvonalú informatikai szolgáltatást nyújt a különböző iparágak számára. A cég több mint 100 elégedett ügyféllel rendelkezik Magyarországon és külföldön, akiknek a legújabb technológiákat és innovációkat alkalmazza a hálózati tervezés, kivitelezés és üzemeltetés területén. Az InnoTech Networks kft. rugalmasan és hatékonyan alkalmazkodik az ügyfelei igényeihez, és olyan hálózati megoldásokat kínál, amelyek növelik a vállalati folyamatok sebességét, stabilitását és eredményességét. Az InnoTech Networks kft. széles körű tapasztalattal rendelkezik a hálózati megoldások területén, és kiszolgálja a különböző iparágak hálózati igényeit, mint például egészségügy, oktatás, kereskedelem, szolgáltatás..

# A hálózat dokumentációja

A kiépítendő hálózatot a Packet Tracer nevű szimulációs programban terveztük meg. A tervezetet az 1.

1. ábra - A hálózat topológiája

## Kék terület

A kék színnel jelölt területe a kórház igazgatóságának telephelye.

Ezen a telephelyen 30 fő részére kellett biztosítanunk egy zökkenőmentes hálózatot.

A kék területen az alábbi eszközöket használtuk:

* 2db 2911-es Forgalomirányító
* 4db 2960 Switch
* Szerver
* Számítógépek
* Nyomtatók

Az alábbi protokollokat alkalmaztuk a telephelyen:

* VTP
  + Elkerüljük az esetleges következetlenségeket a VLAN-ok konfigurációjában az egész kék területen (Vlanok közötti információ csere)
* STP
  + Annak érdekében, hogy ne alakuljanak ki hurkok illetve szórási viharok
* FTP
* EMAIL
* PAGP

A forgalomirányítókon az alábbiakat alkalmaztuk:

* Vlan-ok létrehozása
  + Vlan 15: Orvosi igazgatóság
  + Vlan 8: Gazdasági igazgatóság
  + Vlan 7: Főigazgatóság

### VLAN (Virutal Local Area Network)

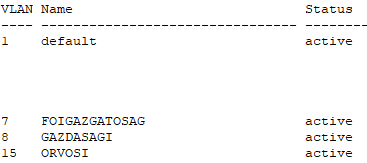
Egy LAN-hoz a hozzáférést biztosítani normál esetben egy hozzáférési rétegbeli kapcsoló feladata. Egy második rétegbeli (Layer 2) kapcsolón virtuális helyi hálózatok (**VLAN, Virtual Local Area Network**) hozhatók létre a szórási tartományok méretének csökkentésére, harmadik rétegbeli (Layer 3) eszközhöz hasonló funkcióval. A hálózatot rendszerint eleve VLAN-ok használatával tervezik meg, ami megkönnyíti, hogy a hálózat kiszolgálja egy szervezet céljait.  
Az igazgatóság telephelyén vlanokat alkalmaztunk a könnyebb kezelés érdekében.

Virtuális Helyi Hálózatokat nagyon egyszerűen hozhatunk létre.

A globális konfigurációs módba lépve, a vlan <vlan\_azonosító> parancs kiadásával már létre is hoztuk az alkalmazni kívánt vlan-t, a könnyebb azonosítás érdekében pedig, a   
name <vlan\_neve> parancs adható ki. Miután mindennel megvagyunk, ezt a folyamatot minden használni kívánt switchen ki kell adnunk, hacsak nem alkalmazunk **VTP**-t a hálózatban. Ezután az adott **interface**hez hozzá kell rendelni, a megfelelő vlan-t, amit úgy tehetünk meg, hogy a portot hozzáférhető állapotba tesszük a switchport mode <access/trunk> parancs kiadásával, majd a switchport access vlan <vlan\_azonosító> paranccsal hozzá is rendeltük a kívánt vlan-t.

A **natív** **VLAN** egy olyan VLAN, amelyre a **trunk** portokon érkező tageletlen csomagok kerülnek. A tageletlen csomagokat a trunk portok a natív VLAN-ba helyezik, így lehetővé teszik a nem tagelt csomagok kezelését is. A trunk egy olyan kapcsolat, amelyen több VLAN forgalma haladhat át. A trunk portokat általában switchek kötik össze, és a trunk kapcsolatokat használják a VLAN-ok közötti forgalom továbbítására.

A Kék színnel jelölt telephelyen három különböző **VLANT** hoztunk létre, hogy a különböző igazgatóságok tagjai, zavartalanul végezhessék munkájukat.



2. ábra - show vlan brief parancs kimenetele

### VTP (VLAN Trunk Protocol)

A **VLAN Trunking Protocol** (VTP) segítségével a Cisco eszközök automatikusan cserélik a VLAN konfigurációs információkat a hálózaton keresztül. Ez megkönnyíti a VLAN-ok kezelését a hálózaton, mivel a változásokat elegendő egy, az ún. **szerver** switchen elvégezni, majd ezek a változások automatikusan szétterjednek az összes VTP-t támogató eszközre.

A VTP-nek két módja van. A szerver, és a kliens. Ezt a vtp mode <server/client> parancs kiadásával állíthatjuk be.

**Szerver:** Ebben a módban a szervernek beállított switch hirdeti a VLAN információkat. Engedélyezve van a **vlanok** konfigurálása. A switch vissza tudja állítani a VLAN információkat a VTP adatbázisból (VTP database), amely a nem felejtő memóriában van, újraindítás után is.

**Kliens:** 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.

3. ábra - show vtp status parancs kimenetele

### PAgP (Port Aggregation Protocol)

A PAgP a Cisco saját fejlesztésű protokollja, mely az EtherChannel kapcsolatok automatikus létrehozását segíti. Használata esetén a kapcsolók PAgP-csomagokkal egyeztetnek a portok között az EtherChannel kialakításához. Ha a PAgP megfelelő Ethernet portokat talál, összefogja azokat egy EtherChannel-be, amely ezután egyedi portként vesz részt a feszítőfában.

Cégünk cisco routereket alkalmaz, ezért a PAgP-t választottuk. A PAgP csak cisco routereken működik, cserébe viszont sokkal egyszerűbb beüzemelni, illetve menedzselni.

A portösszefogás beüzemelése nagyon egyszerű. Első lépésként létrehozzuk a szükséges Port-Channeleket. Ezt az interface port-channel <csatorna\_azonosító> parancs kiadásával tehetjük meg. Ezután az adott switchen, belépünk az interface range <int,int> paranccsal az összevonni kívánt interfacekbe és a channel-group <azonosító> mode <active/passive/desirable/on> parancsot kiadva, beállítjuk, hogy milyen módon fusson a Link Aggregation. Az utolsó paraméter attól függ, hogy LACP-t, vagy PAgP-t használunk. Cégünk esetében, a desirable paramétert kellett megadni.

Fontos, hogy ezen parancsok kiadása alatt, le kell kapcsolni azon interfaceket, amelyeket éppen konfigurálunk.

4. ábra - show etherchannel parancs kimenetele, S1\_SWITCHEN

### Feszitőfa protokoll (Spanning Tree Protocol)

A redundanciát a hálózatok terén azért alkalmazzuk, hogy növeljük a megbízhatóságot, és alternatív útvonalak álljanak 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 redundáns kapcsolatok még veszélyesebbek szórásos üzenetek esetén. Ha a szórásos üzenetek továbbítása során a teljes sávszélességet elfoglalják a keretek, akkor szórási viharról beszélünk, angolul broadcast storm. Az ilyen viharok kialakulásához néhány másodperc is elég.

A feszítőfa protokoll biztosítja, hogy elkerüljük a hurkokat. 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 **Per VLAN Spanning Tree** (**PVST**) egy olyan Cisco-specifikus implementáció, amely lehetővé teszi a hálózati eszközök számára, hogy minden VLAN-hoz külön fa-topológiát hozzanak létre. Az STP működésének alapja az útvonalválasztás fa kialakítása, amelynek célja a hálózat topológiájának optimalizálása. A PVST működése során minden VLAN-hoz külön fa készül, amelynek célja a hálózati forgalom optimalizálása.

A redundanciát a hálózatok terén azért alkalmazzuk, hogy növeljük a megbízhatóságot, és alternatív útvonalak álljanak rendelkezésre. Az alternatív útvonalak viszont problémához vezethetnek, ha egy-egy csomag körbe jár a redundáns útvonalakon.

### DHCP (Dynamic Host Configuration Protocol)

A **DHCP**, vagyis a Dynamic Host Configuration Protocol, egy olyan hálózati protokoll, amely automatikusan biztosítja a hálózati végpontok (kliensek) számára a szükséges IP címeket és egyéb hálózati beállításokat anélkül, hogy manuális beavatkozásra lenne szükség.

A DHCP alkalmazásához szükségünk van egy DHCP-Poolra, amelyet az   
ip dhcp pool <pool\_név> parancs kiadásával hozhatunk létre, a globális konfigurációs szinten. Ha megvan a pool, meg kell adnunk, hogy mely hálózat számára osszon IP címeket a szerver/router, illetve a hálózat alapértelmezett átjáróját. Ehhez a   
network <cím\_tartomány> <alhálózati\_maszk> illetve a   
default-router <alapértelmezett\_átjáró> parancsot szükséges kiadni.

Vannak olyan esetek, amikor nem szeretnénk, hogy bizonyos IP címek kiosztásra kerüljenek, mint például a forgalomirányító IP címe, vagy esetleg egy területen alkalmazott szerveré. Ehhez ki kell adnunk globális konfigurációs szinten, az   
ip dhcp excluded-address <kezdeti\_IP-cím> <vég\_IP-cím>  
A fontosabb parancsok ezzel meg is vannak.

Ha szükséges, a a dns-server <DNS\_szerver\_cím> parancsot kiadva, beállíthatjuk, hogy milyen **DNS** címet adjon a DHCP a klienseknek. A KÉK területen, az igazgatóság tagjait rendeltük hozzá az ftp-hez, hogy a fontosabb iratok, adatokat, együttesen tudják kezelni, egy közös tárhelyen.

Ha mindennel készen vagyunk, a privilegizált EXEC szinten a   
show ip dhcp pool kiadásával megtekinthetjük, az aktuális beállításokat.

. ábra - A kék területen routerén alkalmazott DHCP beállításai

### HSRP (Hot Standby Router Protocol)

A Cisco saját feljesztésű FHRP-je, az alapátjáró IPv4-eszköz hibatűrő működtetésére. A HSRP magas szintű hálózati elérhetőséget biztosít, az IPv4 alapértelmezett átjárót használó állomások számára ad első ugrás forgalomirányító redundanciát. A HSRP a forgalomirányítók egy csoportjából választ ki aktív és készenléti (standby, tartalék) eszközt. Az aktív eszköz végzi a csomagok továbbítását, a készenléti vagy tartalék eszköz pedig, megfelelő feltételek teljesülése esetén, átveszi a kiesett aktív eszköz szerepét. A HSRP tartalék forgalomirányítójának feladata figyelni a HSRP-csoport működését és gyorsan átvenni a csomagtovábbítás feladatát az aktív eszköz hibájakor.

HSRP IPv6-verzió - A Cisco saját fejlesztésű FHRP-je, ugyanaz a feladata, mint a HSRP-nek, csak IPv6 környezetben. Egy HSRP IPv6 csoport virtuális MAC-címe a HSRP-csoport számából, virtuális IPv6 link-local címe pedig a HSRP virtuális MAC-címből képződik. Amíg aktív a HSRP-csoport, tagjai rendszeresen küldenek forgalomirányító hirdetés (RA) üzeneteket a HSRP virtuális IPv6 link-local címére. Amikor a csoport inaktívvá válik, nem érkezik több ilyen hirdetés.

Beállítása igen egyszerű. Először ki kell választanunk, hogy melyik az aktív, és melyik a tartalék forgalomirányító. A mi esetünkben az aktív forgalomirányító a FOEPULET\_R, a tartalék pedig a IGAZGATOSAG\_BACKUP. Beállításához az aktív routeren be kell lépnünk a szükséges interface(ek)be, majd a standby <azonosító> ip <virtualis\_forg\_ip> parancsot kiadva, meg kell adnunk a virtuális IP címet ( A KÉK területen, ez a 192.168.99.254), majd beállítjuk a forgalomirányító prioritását, ezzel jelezve, hogy melyik legyen az aktív. Ezt a standby 1 priority <prioritás> paranccsal tehetjük. Minél kisebb a prioritás, annál nagyobb elsőbséget élvez a forgalomirányító, tehát az lesz az aktív. Emellett az aktív routeren, ki kell adnunk a standby 1 preempt parancsot, mely megmondja, hogy a router, kerekedjen felül, a többi aktív routeren.

### FTP (File Transfer Protocol)

Az **FTP** (File Transfer Protocol) egy szabványos kommunikációs protokoll, amely lehetővé teszi a számítógépes fájlok átvitelét egy hálózaton keresztül. Az FTP külön vezérlő- és adatkapcsolatokat használ, és támogatja a különböző adattípusokat, módokat és biztonsági lehetőségeket. Az FTP-t gyakran használják a weboldalak tartalmának feltöltésére és letöltésére, valamint a számítógépek közötti fájlmegosztásra.