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. ábrán látható:

1. ábra - A hálózat topológiája

## Kék terület

A kék színnel jelölt terület 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:

* Harmadik rétegbeli redundáns megoldás:
  + HSRP
    - A fő router (**FOEPULET\_R**) leállása esetén, az **IGAZGATOSAG\_BACKUP** átveszi a router irányítási szerepkörét.
* Második rétegbeli redundáns megoldások:
  + STP
    - Hurkok és szórási viharok kialakulásának meggátolásának érdekében
  + Link Aggregáció
    - Port összefogás

Forgalomirányítók:

* SSH
  + Titkosított távoli hozzáférést biztosít.
* EIGRP
  + Dinamikus forgalomirányítást biztosít telephelyek és VLAN-ok között

Kapcsolók (Switchek)

* Vlan Trunk Protocol
  + Kapcsolók közötti **VLAN** információ csere
* Port-security
  + Az interfészek 1 címet tanulhatnak meg maximum, ismeretlen cím esetén, eldobják a nem ismert címet, és logolják, a „sértést”
* DHCP Snooping
  + Csak ismert interfészeknek oszt címet a DHCP
* jelszó titkosítás
  + SECRET jelszavak
  + service password-encryption
* SSH
  + Titkosított távoli hozzáférést biztosít az adminnak.

### 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 802.1Q trönk porthoz van hozzárendelve. A trönk portok azok a kapcsolók közötti linkek, amelyek egynél több VLAN forgalmának a továbbítását is lehetővé teszik. Egy 802.1Q trönk port a különböző VLAN-okból érkező forgalmat valamint a nem VLAN-ból származó forgalmat egyaránt továbbítja.

A Kék színnel jelölt telephelyen öt különböző **VLANT** hoztunk létre. Hármat, hogy az igazgatóság tagjai zavartalanul végezhessék munkájukat, egy alapértelmezett (default) VLAN-t, illetve egy **NATÍV VLAN-**t, hogy a nem VLAN-ból érkező információk is továbbításra kerüljenek.

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:** Lehetővé teszi, hogy létrehozzon, eltávolítson és módosítson VLAN-okat az egész hálózaton. Beállíthat más konfigurációs opciókat is, mint például a VTP verzió, és be- vagy kikapcsolhatja a VTP pruninget az egész VTP domain számára. A VTP szerverek hirdetik a VLAN konfigurációjukat a többi, ugyanabban a VTP domainben lévő switch felé, és szinkronizálják a VLAN konfigurációjukat a trunk linkeken érkező üzenetek alapján.

**Kliens:** Lehetővé teszi, hogy létrehozzon, megváltoztasson és töröljön VLAN-okat a helyi eszközön. A VTP kliens módban egy switch tárolja a legutóbb ismert VTP információkat.

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 PortFast a Cisco PVST+ környezetben használt funkciója. A PortFast beállítás a kapcsolóportot lezárt állapotból azonnal továbbító állapotba váltja, amellyel megkerüli a szokásos figyelő és a tanuló állapotokat. A PortFast arra szolgál, hogy a hozzáférési portok eszközei azonnal elérjék a hálózatot, ne kelljen megvárniuk konvergálását minden egyes VLAN-on. Hozzáférési porton az egyetlen munkaállomást vagy szervert csatlakoztató portot értjük.

Szabályos PortFast beállítások esetén sosem érkezhetnek BPDU-k, mert ez azt jelentené, hogy a portra másik híd vagy kapcsoló csatlakozik, ami feszítőfa hurokhoz vezethetne.

A Rapid Per-VLAN Spanning Tree Plus (PVST+)

biztosítja a kapcsolat gyors helyreállítását egy eszköz, egy eszközport vagy egy LAN meghibásodása után. Emellett gyors konvergenciát biztosít a szélső portok, az új gyökérportok és a pont-pont kapcsolatokon keresztül csatlakoztatott portok számára.

A Rapid PVST+ minden egyes virtuális helyi hálózathoz (VLAN) külön feszítőfa példányt futtat. Ez lehetővé teszi a port számára, hogy egyes VLAN-okat továbbítson, miközben más VLAN-okat blokkol. A PVST+ biztosítja a VLAN-ok terheléselosztását több porton, ami a hálózati erőforrások optimális kihasználását eredményezi.

A gyors PVST+ segítségével a konvergencia gyorsan történik. Alapértelmezés szerint a feszítőfa protokollban minden kijelölt port 2 másodpercenként küld egy BPDU-t (Bridge Protocol Data Unit). A topológiában egy kijelölt porton, ha három egymást követő alkalommal kimaradnak a hello üzenetek, vagy ha lejár a maximális életkor, a port azonnal törli az összes protokollinformációt a táblából. Egy port úgy tekinti, hogy elveszíti a kapcsolatot a közvetlen szomszédos kijelölt porttal, ha három BPDU-t kihagy, vagy ha a maximális kor lejár. A protokollinformációk ilyen gyors öregedése lehetővé teszi a hibák gyors észlelését.

### Port-Security (Portbiztonság)

A portbiztonság megvédi a hálózatot az ismeretlen **MAC**-címek elárasztásától azáltal, hogy korlátozza a portonként megtanult **MAC**-címek számát.

Az adott interfészen 3 beállítást végezhetünk el. Megadhatjunk, hogy miként ismerje fel a hozzá csatlakozó eszköz/eszközök **MAC**-címét, emellett megadhatjuk, a maximum **MAC-**címek számát, illetve, hogy sértés esetén, hogy reagáljon a kapcsoló.

A **MAC**-cím beállítását kétféleképpen tehetjük meg. Megathatjuk statikusan, vagy bekapcsolhatjuk a „sticky” nevű funckiót, amivel felismeri és eltárolja, az akkor hozzá csatlakozó eszköz **MAC**-címét. Cégünk az utóbbi beállítást alkalmazta a hálózaton.

Sértés esetén, három funkció közül válaszhatunk.

* protect
  + A switch eldobja a keretet.
* restrict
  + Amellett, hogy eldobja a keretet, naplózza az eszköz **MAC-**címét, illetve, a behatolási kísérletek számát.
* shutdown
  + Tulajdonságai alapján megegyezik az előzővel, viszont, sértés esetén a portot disabled állapotba helyezi, amit csak manuálisan tud visszakapcsolni a rendszergazda.

A telephelyen a restrict állapotot alkalmaztuk, ugyanis tulajdonságait tekintve ez a legbiztonságosabb, illetve, nem szükséges manuális beavatkozás, hiszen a folyamat megy tovább, nem kapcsol le a sértett port.

### 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

### DHCP-Snooping

A DHCP snooping egy DHCP biztonsági funkció, amely a nem megbízható DHCP-üzenetek szűrésével, valamint a DHCP snooping kötési táblázat létrehozásával és karbantartásával nyújt biztonságot. A nem megbízható üzenet olyan üzenet, amely a hálózaton vagy tűzfalon kívülről érkezik, és a hálózaton belül forgalmi támadásokat okozhat.

A DHCP snooping kötési tábla tartalmazza a MAC-címet, az IP-címet, a bérleti időt, a kötés típusát, a VLAN-számot és a kapcsoló helyi, nem megbízható interfészeinek megfelelő interfészinformációkat; a megbízható interfésszel összekapcsolt állomáshelyekre vonatkozó információkat nem tartalmazza. A nem megbízható interfész olyan interfész, amely úgy van konfigurálva, hogy a hálózaton vagy tűzfalon kívülről érkező üzeneteket fogadjon. A megbízható interfész olyan interfész, amely úgy van konfigurálva, hogy csak a hálózaton belülről érkező üzeneteket fogadjon.

A DHCP-snooping tűzfalként működik a nem megbízható állomás és a DHCP-kiszolgálók között. Emellett lehetőséget ad a végfelhasználóhoz csatlakozó nem megbízható és a DHCP-kiszolgálóhoz vagy egy másik kapcsolóhoz csatlakozó megbízható interfészek megkülönböztetésére.

### 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.

6. ábra - FTP felhasználók, jogosultságok

### EMAIL

Az igazgatóság szerverén alkalmazunk levelező klienst, egyedi domain címmel, így könnyebben elérik egymást a dolgozók. Az email két protokollt használ, az **SMTP**-t és a **POP3**-at.

A **POP3** (Post Office Protocol version 3) egy olyan email protokoll, amely hozzáférést biztosít egy email szerveren tárolt beérkező üzenetekhez1. A protokoll letölti és törli az üzeneteket1. Amikor egy POP3 kliens csatlakozik a levelező szerverhez, az összes üzenetet letölti a postafiókból. Ezután a kliens a helyi számítógépen tárolja az üzeneteket és törli azokat a távoli szerverről. Ennek köszönhetően a felhasználók helyben, offline módban is hozzáférhetnek az üzenetekhez.

Az email protokollok között található még az SMTP (Simple Mail Transfer Protocol), amely az email üzenetek küldéséért felelős, és az IMAP (Internet Message Access Protocol), amely lehetővé teszi a felhasználó számára, hogy hozzáférjen és kezelje az email szerveren tárolt üzeneteit

### DNS (Domain Name System)

A DNS lefordítja a domain neveket IP címekké, hogy a böngészők betölthessék az internetes erőforrásokat.

A DNS szerverek lehetővé teszik, hogy az embereknek ne kelljen megjegyezniük az IP címeket, mint például a 192.168.1.1 (IPv4-ben), vagy a bonyolultabb, újabb alfanumerikus IP címeket, mint például a 2400:cb00:2048:1::c629:d7a2 (IPv6-ban).

Amikor egy felhasználó egy weboldalt szeretne betölteni, egy fordításnak kell történnie a felhasználó által a webböngészőbe beírt (például pelda.com) és a gépbarát cím között, ami szükséges a valami.com weboldalának eléréséhez.

7. ábra - KÉK területen alkalmazott DNS címfordítás

### SSH (Secure Shell)

Az SSH olyan hálózati protokoll, mely segítségével titkosított hálózati kapcsolattal jelentkezhetünk be egy távoli gépre. Az SSH gyakorlatilag lehetővé teszi a biztonságos kommunikációt két távoli számítógép között még egy nem biztonságos hálózaton keresztül is. Ugyanakkor nem csak távoli elérésre alkalmas, hanem fájlok másolására, titkosított csatornák létrehozására (stunnel) és parancsok kiadására is a távoli gépen.

## Rózsaszín terület

A rózsaszínnel jelölt terület, az otthoni dolgozó telephelye. Ő felel a betegek felvételéért, egyeztet időpontot az orvosokkal, illetve felviszi a kórház rendszerébe az adatokat.

A rózsaszín területen az alábbi eszközök, protokollok megtalálhatóak:

* WRT300N Vezeték nélküli forgalomirányító
  + DHCP
  + Jelszótitkosítás
* Laptop
* Nyomtató
* Okostelefon

### DHCP

A forgalomirányító DHCP-vel oszt IP címet az otthoni dolgozónak.

8. ábra - Otthoni dolgozó DHCP konfiguráció