Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

***Szakképesítés neve:*** Informatikai rendszer- és

alkalmazás-üzemeltető technikus

***száma:*** 5-0612-12-02

**VIZSGAREMEK**

**Vajda-Papír Kft. bemutatása**

Kiss Levente Magor, Győri Péter, Fekete Attila  
2/14B

Budapest, 2023.

**Tartalomjegyzék**

[Cégleírás 1](#_Toc132563834)

[Használt protokollok 2](#_Toc132563835)

[STP (Spanning Tree Protocol) 2](#_Toc132563836)

[HSRP (Hot Standby Router Protocol) 3](#_Toc132563837)

[DHCP (Dynamic Host Configuration Protocol) 4](#_Toc132563838)

[OSPF (Open Shortest Path First) 5](#_Toc132563839)

[VTP (Vlan Trunking Protocol) 6](#_Toc132563840)

[Link Aggregation 7](#_Toc132563841)

[Vezeték nélküli hálózatok 8](#_Toc132563842)

[IPv4 cím 9](#_Toc132563843)

[IPv6 cím 9](#_Toc132563844)

[Site-to-site VPN 10](#_Toc132563845)

[ASA (Adaptive Security Appliance) 11](#_Toc132563846)

[ACL (Access-List) 12](#_Toc132563847)

[IPSec (Internet Protocol Security) 13](#_Toc132563848)

[Port Security 14](#_Toc132563849)

[Dunaföldvári telephely 16](#_Toc132563850)

[**Irodaház (Piros szín)** 16](#_Toc132563851)

[**A épületrész (Kék szín)** 16](#_Toc132563852)

[**B épületrész (Narancssárga szín)** 16](#_Toc132563853)

[**C épületrész (Zöld szín)** 16](#_Toc132563854)

[**D épületrész (Lime szín)** 17](#_Toc132563855)

[**E épületrész (Lila szín)** 17](#_Toc132563856)

[**F épületrész (Rózsaszín szín)** 17](#_Toc132563857)

[**Logisztika (Narancssárga szín)** 18](#_Toc132563858)

[**Szerverszoba** 18](#_Toc132563859)

[Amazon Web Services (Webszerver) 19](#_Toc132563860)

[**Object Network** 19](#_Toc132563861)

[Székesfehérvár Ügyfélközpont 21](#_Toc132563862)

[**Székesfehérvár ügyfélszolgálat 1. épület** 21](#_Toc132563863)

[**Székesfehérvár ügyfélszolgálat 2. épület** 21](#_Toc132563864)

[Budapesti telephely 22](#_Toc132563865)

[Vajda Papír Kft. szerverkörnyezeti dokumentáció 23](#_Toc132563866)

[**Szolgáltatások** 23](#_Toc132563867)

[**Active Directory** 24](#_Toc132563868)

[**Domain Controller** 24](#_Toc132563869)

[**DHCP (Dynamic Host Configuration Protocol)** 24](#_Toc132563870)

[**DHCP Failover** 24](#_Toc132563871)

[**Fileserver** 24](#_Toc132563872)

[**Group Policy Object** 24](#_Toc132563873)

[**Mail Server** 24](#_Toc132563874)

[**Backup** 24](#_Toc132563875)

[**Vajda-Papír Kft. szerverinek beállításai** 25](#_Toc132563876)

[**Dunaföldvári telephely szerverei** 25](#_Toc132563877)

[Mikrotik Router 25](#_Toc132563878)

[Windows Server Gui Primary 25](#_Toc132563879)

[Windows Server Gui Failover 25](#_Toc132563880)

[Linux Server Mail 26](#_Toc132563881)

[Windows Client 26](#_Toc132563882)

[**Budapesti telephely szerverei** 26](#_Toc132563883)

[Mikrotik Router 26](#_Toc132563884)

[Windows Server Gui RODC 27](#_Toc132563885)

[Windows Client 27](#_Toc132563886)

[**Székesfehérvári telephely szerverei** 28](#_Toc132563887)

[Mikrotik Router 28](#_Toc132563888)

[Windows Server Gui Primary 28](#_Toc132563889)

[Windows Server Gui Failover 28](#_Toc132563890)

[Windows Client 29](#_Toc132563891)

[**Adatközpont szerverei** 29](#_Toc132563892)

[Mikrotik Router 29](#_Toc132563893)

[Linux Server WEB FTP 29](#_Toc132563894)

[Windows Client 30](#_Toc132563895)

[**A felhasználókra vonatkozó általános szabályok (Group Policy Obejcts)** 31](#_Toc132563896)

[**EVE-NG (Enterprise Virtual Environment-Next Generation)** 34](#_Toc132563897)

[Vajda-Papír site-to-site VPN 35](#_Toc132563898)

[**Hálózat programozás** 36](#_Toc132563899)

[Forrásjegyzék 38](#_Toc132563900)

# **Cégleírás**

A Vajda-Papír Kft. egy papírgyártással foglalkozó cég, amely korszerű technológiájának köszönhetően a legújabb innovációkat használja, emellett teljesen megfelel a környezetvédelem által támasztott elvárásoknak. Magas szintűen automatizált, ezért hatékony és eredményes, egészen 1999-től, napjainkig. A cégbe számtalan világhírű márka fektette bizalmát, ezért a garázsból induló vállalkozás az évek során óriási gyártelepekké nőtte ki magát.

Csapatunk meghívást kapott a Dunaföldvári Vajda-Papír telephelyre, ahol részletes betekintést nyerhettünk a cég hálózati felépítésébe. Ezt követően arra törekedtünk, hogy minél pontosabban szimuláljuk a digitális térben a telephelyek hálózatát. Ennek célja pedig, a jövőbeli fejlesztések és frissítések tesztelése virtuálisan.

# **Használt protokollok**

### **STP (Spanning Tree Protocol)**

A Feszítőfa egy automatikusan működő protokoll. Minden feszítőfa célja, hogy a 2. rétegbeli hurkot megelőzze, ehhez a switchek egy Spanning Tree algoritmust hívnak segítségül, aminek mindig az a célja, hogy az adott feszítő fában megállapítsa, hogy hol és ki lesz a root bridge, és hol jönnek létre designated portok, root portok és alternate portok. Ennek a folyamatnak a lejátszódása addig tart, amíg minden hurokban megállapításra nem kerül, hogy ki lesz a root bridge (amit a többiek elismernek root bridge-nek, és hirdetik), és kialakításra kerül a hurok megszakítása egy alternate port segítségével.

A Rapid Spanning Tree Protocol -t használjuk a gyorsabb konvergencia végett, amely külön kezeli a VLAN -okat.

Minden switchen beállítjuk a BPDU támadások elleni védelmet, így megakadályozzuk, hogy bizonyos portokon BPDU keretek haladhassanak át.

Az SW\_IRODA1 az elsődleges kapcsoló, a vlan10 -nél, SW\_IRODA2 pedig a másodlagos kapcsoló. SW\_IRODA2 az elsődleges kapcsoló a vlan20 és a vlan99 -nél a Dunaföldvári telephelyen.

### **HSRP (Hot Standby Router Protocol)**

Az egyik módszer arra, hogy megszüntessük a forgalomirányító kritikus meghibásodási pont szerepét az, hogy virtuális forgalomirányítót valósítunk meg. Ekkor több forgalomirányítót olyan módon konfigurálunk, hogy együttesen egyetlen forgalomirányító látszatát keltsék a LAN állomásainak számára. Egy IP-cím és egy MAC-cím közös használatával kettő vagy több forgalomirányító egyetlen virtuális forgalomirányítóként működhet.

A HSRP magas szintű hálózati elérhetőséget biztosít, az IPv4 alapértelmezett átjárót használó állomások számára ad first hop 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.

### **DHCP (Dynamic Host Configuration Protocol)**

A DHCP egy hálózati menedzsment protokoll, amely az alkalmazás rétegben található. Nagy szerepet játszik a nagyobb hálózatok IP-cím kiosztásában, ugyanis segítségével dinamikusan rendelhetünk hálózatunk végeszközeihez IP-címeket, ezzel rengeteg időt megspórolva. A DHCP protokollt szolgáltató eszközünk lehet egy forgalomirányító vagy egy szerver. Ez az eszköz felé kell jeleznie a kliensünknek, egy szórásos üzenet formájában (DHCP Discover), hogy IP-címet szeretne magának. Ezt követően a protokollt futtató eszköz egy válaszban (DHCP Poffer) leírja a kliensnek szánt IP-Címet, ehhez tartozó maszkot, átjárót, a DNS szerver IP-Címét illetve a bérlet időt. Ezt követően a kliensünk visszajelez (DHCP Request), hogy számára megfelelnek a kapott címek, illetve a bérleti időt szintúgy ezzel a módszerrel tudja meghosszabbítani. Végezetül pedig egy visszajelzést kap kliensünk a szervertől (DHCP Pack), hogy bejegyzésre kerültek az IP-Címek.

Emellett vannak különböző kimenetelei az IP-Cím kérésnek. A DHCP jelzi, ha nem tud megvalósulni a kliens kérése (DHCP Nak), illetve a kliens is tudja jelezni, hogyha a mellékel IP-Cím már használatban van (DHCP Decline). Ha pedig az idő letelte előtt szeretne a kliens lemondani a bérletéről, azt is jelezheti a szerver felé (DHCP Release).

A mi hálózatunkban is nagy szerepet játszik ez a protokoll, ugyanis a legtöbb hálózati végeszköz így kapja az IP-címét. Ezzel nem csak időt takarítunk meg, hanem a hibalehetőségeket is redukáljuk.

### **OSPF (Open Shortest Path First)**

Az OSPF egy linkállapotú nyíltszabványos irányítási protokoll, amely a hálózati rétegben helyezkedik el. Főleg a nagyvállalati hálózatokban elterjedt, de bárhol használható. Tervezéséből eredően osztály nélküli, azaz támogatja a VLSM -et és a CIDR -t. Az OSPF nem a legegyszerűbb forgalomirányítási protokoll, ám sokkal kifinomultabb, kevesebb sávszélességet foglal, emellett hurokmentes és számos más előnnyel rendelkezik a RIP-hez képest.

A linkállapotú irányítási protokoll működése két részre bontható. Először felderíti a hálózat topológiáját, majd a kapott gráfban megkeresi a legrövidebb útvonalat. Három táblával dolgozik, a forgalomirányítási táblával, a szomszédsági táblával és a topológiai táblával.

Hatékonyságát annak köszönheti, hogy a forgalomirányítás változásai váltják ki az útvonal frissítéseket, egyébként csak Hello csomagok küldésével felügyeli a szomszédságot. Tehát nem terheli folyamatosan a hálózatot nagyobb méretű csomagokkal. Skálázható, lehet finom hangolni, illetve többterületű OSPF -et is alkalmazhatunk.

A protokoll támogatja az Message Digest 5 alapú hitelesítést. Az MD5 alkalmazásakor az OSPF forgalomirányítók a társaiktól csak olyan kódolt irányítási frissítéseket fogadnak el, ahol megegyezik az előre megosztott kulcs.

### **VTP (Vlan Trunking Protocol)**

A VTP protokoll egy kényelmi protokoll aminek a célja, hogy a switchek számára engedélyezi, hogy dinamikusan osszanak meg Vlan információt egymás között. Négy módot különböztetünk meg a protokollnál, szerver, client, transparent és off. Ki kell jelölnünk egy szerver switchet aki a client switcheket fogja megtanítani. A transparent mód pedig értelmezi és fogadja a VTP által küldött információkat, viszont nem menti el, csak továbbítja.

### **Link Aggregation**

A Link Aggregation protocol több fizikai kapcsolatot egy logikai kapcsolatként kezel. Ezzel az adatátviteli sebesség és a biztonság nő, illetve a terhelés megosztás valósul meg. Egymás melletti portokat szokás összefogni, illetve mindkét oldalt ugyan azokat a portokat. Emellett a portok típusának és duplexitásának is ugyanolyannak kell lennie mindkét oldalon.

A PAgP, az-az port egyesítő protokoll a Cisco saját fejlesztésű protokollja, amit teljes Ciscos környezetben érdemes használni. Három módja van, az On, a Desirable és az Auto.

### **Vezeték nélküli hálózatok**

A vezeték nélküli hálózatok mobilitást, könnyebb hálózati elérést biztosítanak felhasználóiknak. Egészen a kis, akár otthoni hálózatoktól, az ipari nagyságú hálózatokig, mindenhol használatos. A mobilitásból fakadóan számos előnye van még a vezeték nélküli hálózatoknak, mint például a költséghatékonyság. Sokszor egyszerűbb egy vállalatnak az embereit költöztetni, mint az eszközeit.

A vezeték nélküli kliensnek csatlakoznia kell egy vezeték nélküli forgalomirányítóhoz, hogy kommunikálni tudjanak a hálózaton. Ennek a folyamatnak három lépése van.

* A vezeték nélküli forgalomirányító felderítése
* A vezeték nélküli forgalomirányító hitelesítése
* A vezeték nélküli forgalomirányítóval való társulás

A csatlakozáskor megkell adnunk egyes paramétereket. Az SSID egy minimum 2 maximum 32 karakter hosszú egyedi azonosító a vezeték nélküli kliens számára. A csatorna beállításakor automatikusan vagy statikusan tudunk megadni frekvenciasávokat, amit az adattovábbításhoz fog használni a forgalomirányító. A Security mode a biztonsági beállításokat jelenti az eszközön, mint például WEP, WPA és a legelterjedtebb a WPA2. WPA2 -nél Encryption -t az-az titkosítást is kell választanunk. Illetve egy jelszót is kell megadnunk, amivel a klienst hitelesíti a forgalomirányító.

### **IPv4 cím**

Az IPv4 cím volt az IP első változata. Az OSI Modell hálózati rétegében kapott helyet. Feladata, hogy adatot továbbítson a hálózat végpontjai között.

Három fő típusba sorolhatóak, unicast, multicast illetve broadcast. 32 bit hosszú, amit 4 oktettre lehet bontani. 4 darab 1 bájtos, az-az 0 és 255 közé eső, ponttal elválaszott számmal írjuk le az IPv4 -es címet.

Fő problémája volt, hogy nem számoltak a végességével. Hiába fejlesztettek ki több protokollt, mint például a VLSM, vagy a NAT, az elfogyását nem tudták megakadályozni. IPv6 cím befutása lett a végleges megoldás.

### **IPv6 cím**

Az IPv6 cím az IPv4 címek elfogyása miatt jött létre. 128 bit hosszú, amit 8 részre tagolhatunk, ezek a hextetek, amik egyenként 16 bitből állnak. Tagolására kettőspontot használunk. 16 os számrendszert használ, amiből kifolyólag a hextetek 0-9 közötti illetve A-F közötti értéket vehetnel fel.

Mivel elődéhez képest sokkal hosszabb, így két rövidítési módszer jött létre.

* I. A teljes, nullákból álló hextetek elhagyása, amit kettő darab kettősponttal jelölünk.

**2001:0DB8:0000:FE01** esetén **2001:0DB8::FE01**

* II. A vezető nullák elhagyása.

**2001:00DB:AC10:FE01** esetén **2001:DB:AC10:FE01**

Az első módszer egy cím esetén csak egyszer használható, míg a második a módszer egy cím esetén többször is használható.

Három fő címtípusa van, az unicast, a multicast illetve az anycast.

### **Site-to-site VPN**

A site-to-site VPN (Virtual Private Network) egy olyan megoldás, amely lehetővé teszi két vagy több távoli hely összekapcsolását egy biztonságos hálózaton keresztül. Ez a megoldás lehetővé teszi a számítógépek és az eszközök közötti biztonságos kommunikációt az interneten keresztül.

A Cisco routerek használata lehetővé teszi a site-to-site VPN konfigurálását. Ezek routerek általában támogatják az IPsec (Internet Protocol Security) protokollt, amely a VPN kapcsolatok létrehozásához használatos. Az IPsec protokoll az adatok titkosítását és a hálózatok közötti biztonságos adatátvitelt teszi lehetővé.

A Cisco routerrel rendelkező két hely közötti site-to-site VPN konfigurálásához először be kell állítani az IPsec-t a routeren, majd létre kell hozni az IPsec-tunnel-t. Az IPsec-tunnel lehetővé teszi a két hely közötti biztonságos adatátvitelt az interneten keresztül.

A site-to-site VPN segítségével a két hely közötti adatátvitel biztonságosabbá válik, és lehetővé teszi a dolgozók számára, hogy biztonságosan kapcsolódjanak a távoli hálózathoz. A site-to-site VPN használata különösen hasznos lehet azoknak a vállalatoknak, amelyeknek több irodája vagy telephelye van, és biztonságos kommunikációt kell fenntartaniuk azok között.

### **ASA (Adaptive Security Appliance)**

A Cisco ASA egy olyan tűzfal- és biztonsági eszköz, amelyet a Cisco Systems fejlesztett ki az adatközpontok és a nagyvállalati hálózatok védelmére. Az ASA lehetővé teszi a hálózati forgalom ellenőrzését és az esetleges fenyegetések blokkolását.

Ennek az eszköznek a biztonsági funkciói közé tartozik többek között a tűzfal, a VPN, az antivirus védelem, az URL szűrés és a kiterjesztett hozzáférési szabályok. Az ASA támogatja a VLAN-okat is.

Az ASA lehetővé teszi a felhasználók számára a hálózati forgalom részletes ellenőrzését és nyomon követését, valamint az átvitt adatok biztonságos és titkosított továbbítását a VPN-n keresztül. Az ASA-nak többféle konfigurációs lehetősége is van, így lehetővé teszi a felhasználók számára az egyéni igényekre szabott beállításokat.

### **ACL (Access-List)**

Az Access List egy olyan eszköz a Cisco hálózati eszközein, amely lehetővé teszi a forgalom irányítását és korlátozását a hálózaton. Az Access List egy lista, amely különböző szabályokat tartalmaz, amelyeket az eszközök alkalmaznak a hálózati forgalom kezelése érdekében.

Az Access List segítségével a hálózat adminisztrátora meghatározhatja, milyen típusú forgalom engedélyezett vagy tiltott a hálózaton belül vagy a hálózattól kívül. Az Access List szabályai meghatározhatják a forrás- és a cél IP-címeket, a protokollokat, az adatportokat, valamint a forgalom további paramétereit. Az Access List használatával az adminisztrátorok meghatározhatják a hálózat biztonsági szintjét, optimalizálhatják a hálózati forgalmat, és kezelhetik a hálózati erőforrásokat.

### **IPSec (Internet Protocol Security)**

Az IPSec (Internet Protocol Security) egy protokoll-szabvány, amely lehetővé teszi a virtuális magánhálózatok (VPN) biztonságos kapcsolatát az interneten keresztül. A Cisco eszközei is támogatják az IPSec-et, amely a hálózati adatok titkosítását, hitelesítését és integritását biztosítja a küldésük és fogadásuk során.

Az IPSec alapvetően két fő komponensből áll: az Authentication Header (AH) és az Encapsulating Security Payload (ESP). Az AH az adatok hitelesítéséért felelős, míg az ESP az adatok titkosításáért és integritásáért felelős.

Az IPSec használata biztonságosabbá teszi a VPN-kapcsolatot azzal, hogy megakadályozza a külső felek által a hálózati adatok megfigyelését vagy manipulálását. Az IPSec további előnye, hogy kompatibilis számos platformmal, és lehetővé teszi a távoli hozzáférést a vállalati erőforrásokhoz anélkül, hogy az adatokat kockáztatnánk.

### **Port Security**

A Port-Security egy olyan biztonsági funkció a Cisco hálózati eszközein, amely lehetővé teszi a hálózati adminisztrátor számára, hogy korlátozza a hálózati eszközökhöz csatlakozó eszközök számát, és megakadályozza a nem kívánt hálózati eszközök csatlakozását.

Az eszközök a hálózati eszközökbe egy adott fizikai porton keresztül csatlakoznak, és a Port-Security funkció lehetővé teszi az adminisztrátorok számára, hogy meghatározzák, hogy hány eszköz csatlakozhat egy adott portra. Az eszközök MAC-címeit rögzítik, és azokat az adott porttal társítják, és így a hálózati eszközök csak akkor képesek csatlakozni a portra, ha azok MAC-címei előre engedélyezettek a Port-Security szabályai szerint.

A Port-Security használata segít megakadályozni a hálózati támadásokat, amelyek a hálózati eszközökön keresztül történhetnek, például az adathalászat vagy a rosszindulatú programok terjesztése. A Port-Security funkció további előnye, hogy segít csökkenteni a hálózati forgalmat és optimalizálni a hálózatot.

**NAT (Network Address Translation)**

A Network Address Translation (NAT) egy olyan eljárás a Cisco hálózati eszközein, amely lehetővé teszi, hogy a privát IP-címeket publikus IP-címekkel helyettesítsék a hálózatok közötti kommunikáció során. A NAT funkció általában akkor hasznos, ha egy vállalati hálózatnak nincs elegendő publikus IP-címe, vagy ha egy hálózati eszköz számára nincs publikus IP-cím rendelve.

A NAT funkció lehetővé teszi, hogy a privát IP-címeket átalakítsuk publikus IP-címekké a hálózat határain. Az IP-cím átalakítás során a NAT funkció a privát IP-címeket publikus IP-címekké alakítja át, és a publikus IP-címeket használja a hálózatok közötti kommunikációhoz.

A NAT funkció további előnye, hogy segít megvédeni a privát hálózatokat a külső támadásoktól, mivel a publikus IP-címek használata álcázza a privát hálózatok belső struktúráját. A NAT használatának egyik hátránya azonban, hogy bizonyos alkalmazások, például a VoIP (Voice over IP) vagy a video konferencia alkalmazások számára problémákat okozhat.

# **Dunaföldvári telephely**

## **Irodaház (Piros szín)**

Itt helyezkednek el az alkalmazottak, akik irodai munkát végeznek a mindennapokban, ezért itt található a legtöbb végeszköz a hálózatban.

## **A épületrész (Kék szín)**

Az épület ezen része a papírgyár első állomása, itt történik a papíralapanyag érkeztetése, illetve a szállításból való kicsomagolás, majd külön, a telephely raktárával kompatibilis tekercsekre való felhelyezés és tárolása. A beérkezett alapanyagot külön kóddal ellátott címkét kapnak és ez alapján tudják beazonosítani, hogy mikor és hová helyezték el a tekercseket.

## **B épületrész (Narancssárga szín)**

A B épületrészben találhatóak azok a gépek, amelyek a papíralapanyagot átalakítják felhasználható papírrá, amiből a következő állomásokon különböző termékek készülnek. Fontos a rendszerezés fenntartása, illetve a minőség-ellenőrzés is, amit különféle manuálisan és automatikusan vezérelt gépek végeznek.

## **C épületrész (Zöld szín)**

A telephely C épületrészében található a gyár egyik legfontosabb állomása, az elkészített papíranyagok rendszerezése, illetve azok tekercselése, majd ezek után megfelelő címkével való ellátása. Fontos, hogy pontosan nevezzék meg a különböző papírfajtákat, hiszen többféle papírterméket is gyártanak ezen alapanyagokból.

## **D épületrész (Lime szín)**

A feltekercselt elkészített papír anyagokat itt tárolják el. A sok tekercs, illetve fém gép miatt, sok az jel elől elárnyékolt rész, ezért jelerősítőket alkalmaznak sorokra, illetve folyosókra felosztva. Mellőzhetetlen a kiváló jel, hiszen a rendszerezés megköveteli, hogy a tekercsek a megfelelő helyre legyenek regisztrálva a későbbi elérés érdekében.

## **E épületrész (Lila szín)**

Az gyár ezen része felel a papírtermékek elkészítéséért, számtalan gép található ezen csarnokban, amik akár Toalett papírt, zsebkendőt, vagy akár egészségügyi maszkot gyártanak a hét minden napján. Esetleges leállás komoly kockázatot jelenthet az egész telehelynek, ezért ezt az épületrészt nagyobb figyelemmel követik az említett minőségellenőrök, esetleges hibás termék esetén azonnal közbe tudjanak lépni és az adott problémát elhárítani.

## **F épületrész (Rózsaszín szín)**

Az elkészített, majd becsomagolt késztermékeket itt tárolják el, raklapokon targoncás segítséggel, ameddig azokért nem érkeznek meg a szállítással megbízott kamionok. A csomagolt termékek kapnak egy egyéni kódot, ami alapján be lehet azonosítani őket, illetve egyesével átesnek egy minőség-ellenőrzésen, amivel a cég felelősséget vállal a termékeire.

## **Logisztika (Narancssárga szín)**

A logisztikai épületben dolgozók felügyelik a gördülékeny gyártást, fejlesztik, hogy még precízebben és hatékonyabban haladjon az előállítás, mint például a raktári berendezések útvonal-optimalizált elrendezésével. Emellett a felmerülő gondokat, hibákat javítják.

## **Szerverszoba**

A képen diagram látható

Automatikusan generált leírásA szerverszoba az egész telephelyet ellátó helyiség. A szerverszobában helyet kapott kettő darab grafikus felületű Windows 2019 szerver, amelyeknek lényegében ugyan az a feladatuk viszont, ha a fő szerver valamilyen oknál fogva nem üzemel, a tartalék szerver lép életbe, ezért is vannak más-más kapcsolókra kötve. Számos szolgáltatást nyújtanak ezek a szerverek az egész Dunaföldvári telephelynek, mint például DHCP, DNS, AD, TFTP, FTP, Fileserver. Ezek mellett még a Printszerver is az irodaházban kapott helyet, amely összeköti a hálózatban a nyomtatókat az itt dolgozók számítógépeivel.

A primary domain controller az SRV\_IRODA\_PRIMARY. A backup domain controller pedig az SRV\_IRODA\_BACKUP. Több szervezeti egységre bontjuk az itt dolgozókat,

* Dolgozók
* Főnökség
* Üzem
* Logisztika
* FTP Felhasználó

Ezeken a szervezeti egységeken belül adjuk meg az itt dolgozók adatait, mint például az email címüket, felhasználónevüket, jelszavukat és itt csatoljuk fel a hálózati meghajtókat. Illetve a szervezeti egységek segítségével adhatjuk meg a felhasználók jogosultságait.

# **Amazon Web Services (Webszerver)**

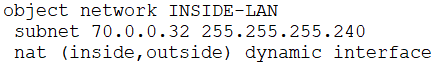
Az Amazon Web Services területünk egy felhőben elhelyezett hálózat, amely az ISP1 hálózattal van kapcsolatban. Itt kapott helyet a Linux Debian alapú WEB szerverünk.

Itt kapott helyet egy Cisco 5505-ös ASA, ami három VLAN-al dolgozik, egy OUTSIDE, egy INSIDE és egy DMZ területtel.

* Az OUTSIDE terület 0-s biztonsági szinttel működik, így senki sem tudja elérni a belső részt.
* Az INSIDE terület 100-as biztonsági szinttel működik.
* A DMZ terület 70-es biztonsági szinttel működik.

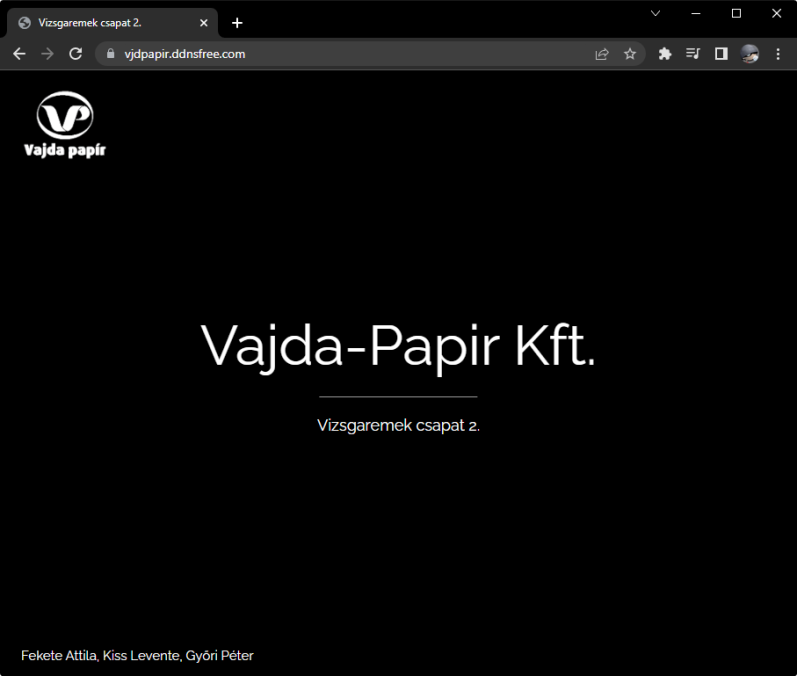
## **Object Network**

A webszerverünk a DMZ területen kapott helyet és egy statikus NAT segítségével kapta meg a 70.0.0.10 -es címet.

Az INSIDE területen kaptak helyet a dolgozók, akik dinamikus NAT segítségével tudnak kimenni az internetre.

Az INSIDE területen lévő dolgozók a tűzfaltól kapnak IP-címet.

Statikus forgalomirányítást használtunk (alapértelmezett) az ISP felé.



# **Székesfehérvár Ügyfélközpont**

A Vajda Papír Székesfehérvári Ügyfélközpontja felel a beszállítókkal, illetve a viszonteladókkal való kommunikációért. Az két épületben elhelyezett laptopok hozzáférési ponton keresztül kapják az internet elérést. Emellett egy-egy irodai nyomtató is helyet kapott az épületekben. Az itt dolgozók bejelentkezési adataik, email címük az épületekben elhelyezett AD szervereken lettek eltárolva. A Primary szerver az 1. épületben míg a Backup szerver a 2. épületben kapott helyet.

## A képen diagram látható Automatikusan generált leírás**Székesfehérvár ügyfélszolgálat 1. épület**

Az egyes számmal ellátott épület foglalkozik a beszállítókkal való kapcsolattartástért. Bármilyen import vagy export tevékenységet az itt dolgozók egyeztetnek és beszélnek meg a külsős cégekkel.

## A képen diagram látható Automatikusan generált leírás**Székesfehérvár ügyfélszolgálat 2. épület**

A kettes számmal ellátott épület felel a viszonteladókkal, partnerekkel való kapcsolattartásért. Az itt dolgozóknak az üzleti megkeresések továbbítása, kezelése, illetve a meglévő partnerekkel való kommunikáció lebonyolítása a feladatuk.

# **Budapesti telephely**

A Vajda Papír Budapesti telephelye felel a külföldi exportálás lebonyolításáért. A területen két épület található, egy irodaház, illetve egy központi raktár, ahová a gyártósorról kigördülő kész termékek kerülnek elraktározásra.

A képen diagram látható

Automatikusan generált leírás**Irodaház**

Az irodaház blbalbalba

**Raktár**

Az raktár blbalbalba

# **Vajda Papír Kft. szerverkörnyezeti dokumentáció**

A cég hálózatának tervezése közben arra törekedtünk, hogy a legbiztonságosabb és legstabilabb szerverkörnyezetet építhessük ki. A legtöbb hálózati területen a főszerverek mellett megtalálható tartalék szerver is, amely bármilyen meghibásodás esetén képes azonnal átvenni a főszerver feladatát. Az irodai területeken szünetmentes tápegység biztosítja az áramot a számítógépek, nyomtatók és telefonok számára esetleges áramkimaradás, feszültségingadozás esetén. A szerverszobák, minden telephelyen, jól klimatizált, külön elzárt helyiségek, ahová a belépés kizárólag a hozzá jogosultak ujjlenyomatával történik meg. Emellett számos nagyfelbontású kamera figyeli a folyosót és a helyiséget.

## **Szolgáltatások**

Vajda-Papír Dunaföldvári telephely

* Windows Server Gui Primary – AD, DNS, DHCP, FILESERVER, RAID5 BACKUP
* Windows Server Gui Backup – FAILOVER
* Linux Server – MAIL

Vajda-Papír Székesfehérvári telephely

* Windows Server Gui Primary – AD, DNS, DHCP, FILESERVER, RAID5 BACKUP
* Windows Server Gui Backup – FAILOVER

Vajda-Papír Budapesti telephely

* Windows Server Gui Primary – RODC

Vajda-Papír Adatközpont

* Linux Server – WEB, MAIL

## **Active Directory**

Az Active Directory címtár az adatbázisból és az azt futtató szolgáltatásból áll. Autentikációs és autorizációs szolgáltatásokat nyújt a Windowst futtató számítógépek részére, lehetővé téve a hálózat adatbázisai, felhasználói, csoportjai egységes adminisztrálását.

## **Domain Controller**

A Domain Controller, másnéven tartományvezérlő, autentikációs és autorizációs szolgáltatást nyújt.

## **DHCP (Dynamic Host Configuration Protocol)**

A DHCP protokoll feladata, hogy automatikusan ellássa a végeszközöket IP címmel.

## **DHCP Failover**

A főszerver DHCP szolgáltatásának leállása esetén a Failover veszi át a szerepét.

## **Fileserver**

A Fileserver biztosít a felhasználók számára másokkal közös vagy esetlegesen saját területet, ahol tárolni, menteni tudják fájljaikat.

## **Group Policy Object**

A Group Policy segítségével lehetőségünk van a felhasználók jogköreinek személyre szabására.

## **Mail Server**

A Mail Server egy levelező rendszer szolgáltatásait nyújtja a felhasználók számára.

## **Backup**

A Backup szolgáltatás lehetővé teszi a szerver számára az automatizált, ütemezett biztonsági mentéseket.

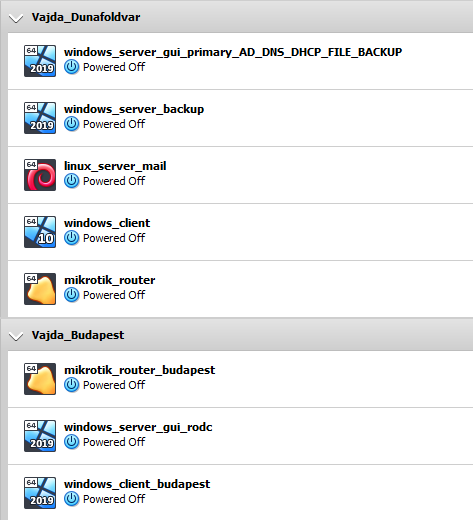
## **Vajda-Papír Kft. szerverinek beállításai**

## **Dunaföldvári telephely szerverei**

### **Mikrotik Router**

Típus – Linux  
Verzió – Other Linux (64-bit)  
Memória – 512 MB  
Tárhely – 500 MB  
Processzor magok száma – 1  
Felhasználónév – admin  
Jelszó – mikrotik123

### **Windows Server Gui Primary**

**Típus – Microsoft Windows  
Verzió – Windows 2019 (64-bit)  
Memória – 2 GB  
Tárhely – 50 GB  
*- shares.vdi – 100 GB  
- raid5\_backup1.vdi – 50 GB  
- raid5\_backup2.vdi – 50 GB  
- raid5\_backup3.vdi – 50 GB  
- raid5\_backup4.vdi – 50 GB  
- raid5\_backup5.vdi – 50 GB*   
Processzor magok száma – 2  
Domain – vjdpapir.hu  
Felhasználónév – administrator  
Jelszó – #Aa123456789@  
AD Felhasználók jelszava - #Cc123456789@

### **Windows Server Gui Failover**

Típus – Microsoft Windows  
Verzió – Windows 2019 (64-bit)  
Memória – 2 GB  
Tárhely – 50 GB  
Processzor magok száma – 2  
Domain – vjdpapir.hu  
Felhasználónév – administrator  
Jelszó – #Aa123456789@

### **Linux Server Mail**

Típus – Linux  
Verzió – Debian (64-bit)  
Memória – 1 GB  
Tárhely – 50 GB  
Processzor magok száma – 2  
Domain – mail.vjdpapir.hu  
Felhasználónév – root  
Jelszó – #Aa123456789@

### **Windows Client**

Típus – Microsoft Windows  
Verzió – Windows 10 (64-bit)  
Memória – 2 GB  
Tárhely – 50 GB  
Processzor magok száma – 2  
Domain – vjdpapir.hu  
Felhasználónév – administrator  
Jelszó – #Aa123456789@

## **Budapesti telephely szerverei**

### **Mikrotik Router**

Típus – Linux  
Verzió – Other Linux (64-bit)  
Memória – 512 MB  
Tárhely – 500 MB  
Processzor magok száma – 1  
Felhasználónév – admin  
Jelszó – #Aa123456789@

### **Windows Server Gui RODC**

Típus – Microsoft Windows  
Verzió – Windows 2019 (64-bit)  
Memória – 2 GB  
Tárhely – 50 GB  
Processzor magok száma – 2  
Domain – vjdpapir.hu  
Felhasználónév – administrator  
Jelszó – #Aa123456789@

### **Windows Client**

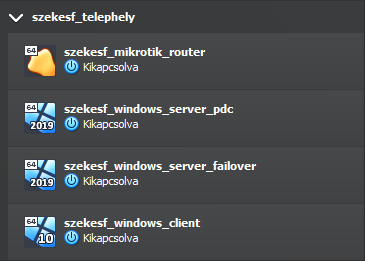
Típus – Microsoft Windows  
Verzió – Windows 10 (64-bit)  
Memória – 2 GB  
Tárhely – 50 GB  
Processzor magok száma – 2  
Domain – vjdpapir.hu  
Felhasználónév – administrator  
Jelszó – #Aa123456789@

## **Székesfehérvári telephely szerverei**

### **Mikrotik Router**

Típus – Linux  
Verzió – Other Linux (64-bit)  
Memória – 512 MB  
Tárhely – 500 MB  
Processzor magok száma – 1  
Felhasználónév – admin  
Jelszó – mikrotik123

### **Windows Server Gui Primary**

**Típus – Microsoft Windows  
Verzió – Windows 2019 (64-bit)  
Memória – 2 GB  
Tárhely – 50 GB  
*- shares.vdi – 100 GB  
- raid5\_backup1.vdi – 50 GB  
- raid5\_backup2.vdi – 50 GB*  *- raid5\_backup3.vdi – 50 GB  
- raid5\_backup4.vdi – 50 GB  
- raid5\_backup5.vdi – 50 GB*  
Processzor magok száma – 2  
Domain – szekesf.vp  
Felhasználónév – administrator  
Jelszó - #server123  
AD Felhasználók jelszava - #user123

### **Windows Server Gui Failover**

Típus – Microsoft Windows  
Verzió – Windows 2019 (64-bit)  
Memória – 2 GB  
Tárhely – 50 GB  
Processzor magok száma – 2  
Domain – szekesf.vp  
Felhasználónév – administrator  
Jelszó - #server123

### **Windows Client**

Típus – Microsoft Windows  
Verzió – Windows 10 (64-bit)  
Memória – 2 GB  
Tárhely – 50 GB  
Processzor magok száma – 2  
Domain – szekesf.vp  
Felhasználónév – administrator  
Jelszó - #client123

## **Adatközpont szerverei**

### **Mikrotik Router**

Típus – Linux  
Verzió – Other Linux (64-bit)  
Memória – 512 MB  
Tárhely – 500 MB  
Processzor magok száma – 1  
Felhasználónév – admin  
Jelszó - #Aa123456789@

### **Linux Server WEB FTP**

Típus – Linux  
Verzió – Debian (64-bit)  
Memória – 2 GB  
Tárhely – 20 GB  
Processzor magok száma – 2  
Felhasználónév – root  
Jelszó - #Aa123456789@

### **Windows Client**

Típus – Microsoft Windows  
Verzió – Windows 10 (64-bit)  
Memória – 2 GB  
Tárhely – 50 GB  
Processzor magok száma – 2  
Domain – szekesf.vp  
Felhasználónév – administrator  
Jelszó - #Aa123456789@

## **A felhasználókra vonatkozó általános szabályok (Group Policy Obejcts)**

**A vezérlőpanelhez való hozzáférés megtiltása**

A felhasználók a vezérlőpanel segítségével széleskörűen módosíthatják a rendszerbeállításokat, és ezek a módosítások biztonsági problémákhoz vezethetnek. A biztonságosabb üzleti környezet érdekében korlátozza a vezérlőpanelhez való hozzáférést csak a kiváltságos felhasználókra. A vezérlőpanelhez való hozzáférés korlátozható a Vezérlőpult és a számítógép beállításaihoz való hozzáférés tiltása házirend engedélyezésével.

User Configuration > Administrative Templates > Control Panels

**A parancssorhoz való hozzáférés megakadályozása**

A parancssor a Windowsban olyan parancsok futtatására szolgál, amelyek fejlett rendszergazdai funkciókat hajtanak végre. Rosszindulatú felhasználók kezében azonban a parancssor a rendszer integritásának veszélyeztetésére használható. A hálózatot érő károk megelőzése érdekében korlátozza a parancssorhoz való hozzáférést a Parancssorhoz való hozzáférés megakadályozása házirend segítségével.

User Configuration > Administrative Templates > System

**Minden cserélhető tárolóhoz való hozzáférés megtagadása**

Az eltávolítható eszközök fogékonyak a vírusokra és rosszindulatú szoftverekre, és ha a felhasználóknak lehetővé teszik, hogy csatlakoztassák őket a számítógépükhöz, az egész hálózatot megfertőzhetik. Az eltávolítható eszközök lehetővé teszik a rosszfiúk számára azt is, hogy rövid idő alatt nagy mennyiségű adatot távolítsanak el. A Minden eltávolítható tároló osztály engedélyezésével megtilthatja az eltávolítható eszközök használatát: Minden hozzáférés megtagadása házirend.

User Configuration > Administrative Templates > Removable Storage Access

**Nem kívánt szoftverek telepítésének tiltása a felhasználóknak**

Ha a felhasználók nem kívánt szoftvereket telepítenek a rendszereikre, akkor a takarítás és az informatikai rendszergazdák számára bonyolult karbantartási folyamatok következnek. Ha meg akarja tiltani a felhasználóknak a szoftverek telepítését, engedélyezze a Felhasználói telepítés tiltása házirendet.

User Configuration > Administrative Templates > Windows Components > Windows Installer

**Ne tárolja a LAN Manager hash-értékeit a következő jelszóváltoztatáskor**

A Windows a LAN-kezelő (LM) jelszók hash-értékeit a helyi Biztonsági fiókkezelő (SAM) adatbázisában tárolja. Ezek az LM hash-ek gyengék, és a támadók könnyen visszafejthetik a tiszta szöveges formátumukat. Ennek elkerülése érdekében a hálózati biztonság engedélyezésével akadályozza meg, hogy a Windows tárolja az LM hash-okat: LAN-kezelő hash-értékét ne tárolja a következő jelszóváltoztatási házirendnél.

User Configuration > Windows Settings > Security Settings > Local Policies > Security Options

**Az automatikus újraindítás megakadályozása a bejelentkezett felhasználókkal az ütemezett frissítések telepítése során**

A Windows-frissítések során a rendszer kényszerű újraindítása fájdalmas lehet. Az újraindítások megszakítják a munkát, és a nem mentett elemek elveszhetnek. A Windows automatikus újraindításának megakadályozásához engedélyezze a Bejelentkezett felhasználók automatikus újraindításának tilalma az automatikus frissítések ütemezett telepítésekor házirendet.

User Configuration > Administrative Templates > Windows Component > Windows Update

**A Group Policy Object beállítások változtatásainak nyomon követése**

A csoportházirend-objektum (GPO) beállításaihoz csak az IT-adminisztrátorok férhetnek hozzá. A beállítások illetéktelen megváltoztatása a biztonság megsértését jelzi. A GPO-beállítások minden módosításának nyomon követése a címtárszolgáltatáshoz való hozzáférés és a címtárszolgáltatás módosításainak ellenőrzése házirendek meghatározásával biztonságosabb hálózatot eredményez.

User Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies/DS Access

## **EVE-NG (Enterprise Virtual Environment-Next Generation)**

Az EVE-NG egy olyan szoftverplatform, amely lehetővé teszi a hálózati topológiák és eszközök szimulálását és tesztelését virtuális környezetben.

A szoftver támogatja a különböző hálózati eszközöket, például switcheket, router-eket, valamint lehetővé teszi a hálózati protokollok és technológiák, például OSPF, HSRP és VPN konfigurálását és tesztelését.



A csapatunk a topológiánk egyes részeit az EVE-NG segítségével tesztelte és szimulálta le, ezeket a megoldásokat a dokumentáció következő részében részletesebben bemutatjuk.

### **Vajda-Papír site-to-site VPN**

A Vajda Papir Kft. dunaföldvári és budapesti telephelyét két VPN kapcsolat köti össze.

Erre azért van szükség, hogy a budapesti dolgozók biztonságosan elérjék az email szervert, és könnyedén tudjanak fájlokat megosztani a dunaföldvári dolgozókkal.

A képen szöveg, térkép, beltéri látható

Automatikusan generált leírásA tartalék VPN kapcsolat akkor lép életbe, hogyha az elsődleges VPN útvonal meghibásodik. Így rendelkezésre áll egy biztonsági tartalékkapcsolat.

**R\_AB – R\_BUDA1 - (CMAP 10)  
R\_LOGISZTIKA\_KULSO – R\_BUDA2 – (CHMAP 20)**

A VPN beállításánál az alábbi paramétereket adtuk meg.

|  |  |
| --- | --- |
| **Paraméterek** | **Használt** |
| Kulcsosztási módszer | ISAKMP |
| Titkosító algoritmus | AES256 |
| Hash algoritmus | SHA |
| Hitelesítési módszer | Pre-Share |
| Kulcscsere | DH Group 24 |
| ISAKMP kulcs | vajdavpnpa55 |

## **Hálózat programozás**

A program célja, hogy kapcsolódjon a két Cisco eszközhöz, majd futtasson két parancsot, amelyek kimenetelét külön fájlokba menti.

Az alábbi bemenő adatokkal dolgozik  
 - Két Ciscos eszköz IP-címe  
 - Az eszközök bejelentkezési adatai (felhasználónév, jelszó)  
 - A futtatni kívánt parancsok listája

Helyes működés esetén a program létrehoz két fájt, az eszközök nevében, a saját IP-címeivel, amelyek tartalmazzák az eszközökről lekérdezett adatokat. Ha hiba történik, akkor a program hibaüzenetet ad ki a kapcsolódási hibáról.

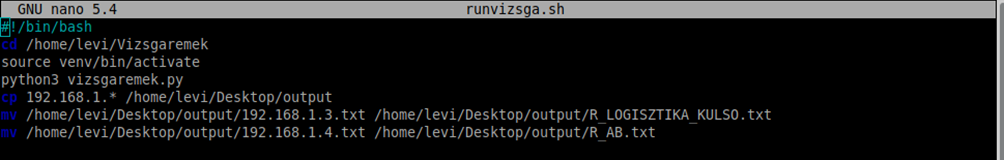
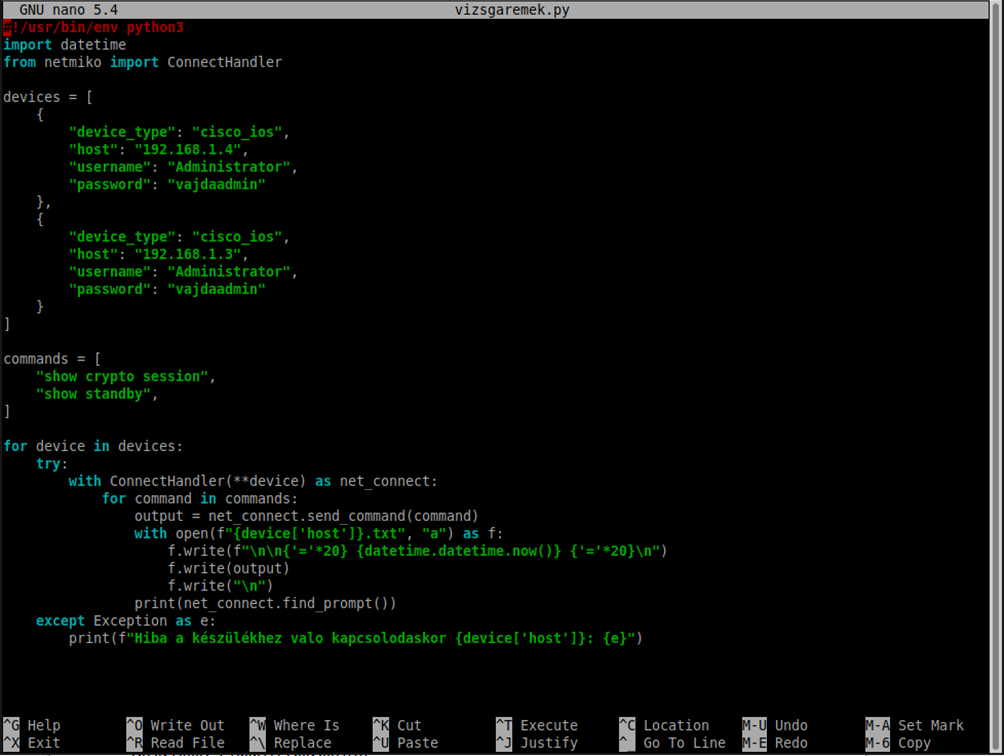
A program az alábbi lépéseket hajtja végre:

* Beimportálja a szükséges modulokat.
* Megadja a csatlakoztatni kívánt eszközök adatait.
* Létrehoz egy listát a futtatni kívánt parancsokkal.
* Végigmegy a csatlakoztatni kívánt eszközökön, és kapcsolódik hozzájuk.
* Minden eszközön csatlakozás után végrehajtja a parancsokat, majd az eredményeket fájlokba írja.
* Bezárja a kapcsolatot minden eszközzel.

A program a try-except szerkezetet használja a kapcsolódási hibák kezelésére, és with szerkezetet a fájlok automatikus bezárására.

Contrab használatával a program automatikusan lefut óránként, és hozzáírja az új kimenetet a már meglévő fájlokhoz. A contrab-nak egy shell scriptet adunk meg, amely megadja a megfelelő parancsokat a program működéséhez.

  
 *A contrab óránként futtatja a shell scriptet.*

*A shell script.*

*A python program*

# **Forrásjegyzék**

[PAgP Kép](https://networkustad.com/2019/11/08/etherchannel-protocols-pagp-and-lacp/)

[Felhasználókra vonatkozó általános szabályok (GPO)](https://www.manageengine.com/products/active-directory-audit/kb/best-practices/best-group-policy-settings.html)

[EVE-NG logó](https://www.eve-ng.net/)