Vizsgaremek Dokumentáció

A képen sor, diagram látható

Automatikusan generált leíráskészült a 2023/24-es tanév SzKTV verseny szóbeli vizsgarészre.

Tartalom

[Bevezetés 4](#_Toc160963238)

[Limitációk 4](#_Toc160963239)

[Hálózat Megvalósítása 5](#_Toc160963240)

[A Hálózat Logikai Topológiája 5](#_Toc160963241)

[Telephelyek Hálózati Infrastruktúrája 5](#_Toc160963242)

[Kőbánya 5](#_Toc160963243)

[Miskolc 5](#_Toc160963244)

[Csepel és Pécel 5](#_Toc160963245)

[Felhasznált Hálózati Technológiák 6](#_Toc160963246)

[TCP/IP 6](#_Toc160963247)

[Etherchannel 6](#_Toc160963248)

[VLAN 6](#_Toc160963249)

[STP 6](#_Toc160963250)

[SSH 6](#_Toc160963251)

[VPN 6](#_Toc160963252)

[Hálózati Alkalmazások 6](#_Toc160963253)

[Radius 6](#_Toc160963254)

[SFTP és TFTP 7](#_Toc160963255)

[Rsyslog 7](#_Toc160963256)

[NTP 7](#_Toc160963257)

[Microsoft Active Directory 7](#_Toc160963258)

[DHCP 7](#_Toc160963259)

[SLAAC 7](#_Toc160963260)

[DNS 7](#_Toc160963261)

[Beállítások - Hálózati Eszközök 8](#_Toc160963262)

[Routerek 8](#_Toc160963263)

[Switchek 8](#_Toc160963264)

[Beállítások - Szerverek 9](#_Toc160963265)

[Windows szerver 9](#_Toc160963266)

[Active Directory Domain Controller 9](#_Toc160963267)

[DNS 9](#_Toc160963268)

[DHCP 9](#_Toc160963269)

[Biztonsági mentés 9](#_Toc160963270)

[Szervezeti Egységek 10](#_Toc160963271)

[Csoport beállítások 10](#_Toc160963272)

[Fájlmegosztás 10](#_Toc160963273)

[Linux szerver 10](#_Toc160963274)

[Hálózati eszközök Interfész beállításai 12](#_Toc160963275)

[Minta Konfiguráció - Router 15](#_Toc160963276)

[Eszköz neve, valamint alap adatok beállítása 15](#_Toc160963277)

[Alinterfészek létrehozása és VLAN-hoz rendelése (ha szükséges) 15](#_Toc160963278)

[Interfészek és alinterfészek IP címeinek és leírásainak beállítása 15](#_Toc160963279)

[Rendszeridő NTP-n keresztüli szinkronizálása a fő telephelyi Linux szerverről 15](#_Toc160963280)

[Hozzáférési listák konfigurálása 15](#_Toc160963281)

[Túlterheléses, port alapú hálózati címfordítás beállítása 15](#_Toc160963282)

[Statikus NAT 16](#_Toc160963283)

[GRE Tunnel létrehozása és konfigurálása 16](#_Toc160963284)

[Bejelentkezések fő telephelyi radius szerverrel való hitelesítése (hiányában lokális kis-nagybetü érzékenységgel) 16](#_Toc160963285)

[Távoli Hozzáférés beállítása csak SSH-n keresztüli módra 16](#_Toc160963286)

[Syslog naplózás beállítása a Linux szerverre 16](#_Toc160963287)

[A helyi Kliens hálózatok számára DHCP szolgáltatás konfigurálása 16](#_Toc160963288)

[IPv6 forgalomirányítás 16](#_Toc160963289)

[Minta konfiguráció - Switch 17](#_Toc160963290)

[Eszköz neve, valamint alap adatok beállítása 17](#_Toc160963291)

[VLAN-ok létrehozása és a megfelelő SVI-k konfigurálása (management IP, stb) 17](#_Toc160963292)

[VLAN-ok interfészhez rendelése, nemhasznált interfészek lekapcsolása 17](#_Toc160963293)

[Router felé irányuló interfész Trunk konfigurációjának beállítása (csak adott VLAN-ok, nativ vlan) 17](#_Toc160963294)

[Portok beállítása gyors továbbító módba (spanning-tree portfast) 18](#_Toc160963295)

[Portbiztonsági beállítások konfigurálása 18](#_Toc160963296)

[Távoli Hozzáférés beállítása csak SSH-n keresztüli módra 18](#_Toc160963297)

[Etherchannel létrehozása 18](#_Toc160963298)

[Forgalomiránytás bekapcsolása 19](#_Toc160963299)

[Projekt szervezési eszközök 20](#_Toc160963300)

# Bevezetés

Jelen dokumentáció egy fiktív számítógép szervíz és bolthálózat, a Computerceg Kft. informatikai hálózatát, illetve szerver szolgáltatásait mutatja be.

A cégről és telephelyeiről a következőket érdemes tudni: 4 telephellyel rendelkeznek, ebből a kőbányai telephely funkcionál fő telephelyként - itt találhatóak meg a cég szerverei, illetve itt egy magasabb létszámmal folyik a munka (kb. 20 fő, a többi telephelyen kb. 10 fő). A telephelyek mindegyikén zajlik számítástechnikai eszközök eladása, illetve javításra alkalmas eszközök szervizelése.

A fő telephelyen található szerverek főbb funkcionalitásai, szolgáltatásai közé tartozik a boltok raktárkészletének követését végző adatbázis szerver; az ezt, és az esetleges céges Weboldalt kiszolgáló webszerver; központi, közös fájltárolási megoldás; utóbbi hitelesítéséhez használt tartomány vezérlés és tartományi felhasználók kezelése; hálózati névfeloldás és annak szűrése; illetve a helyi (kőbányai) hálózatok dinamikus IP cím kiosztását kezelő DHCP szerver.

Jelen projekt mivel nem éles környezetbe készül, felhasználónevek és jelszók tekintetében az „admin” „Passw0rd” kombináció van hasznosítva. Valós környezetben lehetőség szerint minden alkalmazási helyen, felhasználónként külön jelszót érdemes használni a nagyobb biztonság érdekében. Természetesen a felhasználók jogosultsági szintjeivel is lehet egy külön dokumentációt megtölteni, de itt - mivel nem éles környezetbe megy a projekt - nem volt lényeges.

A telephelyek közötti kapcsolat VPN-ekkel van megoldva, mivel a cég méretéből és forgalmából kifolyólag nem igényel bérelt vonalat, vagy akár saját telephely-közi infrastruktúra kiépítését és üzemeltetését. A VPN kapcsolatokat akár különböző internet szolgáltatók hálózatán keresztül is be lehet üzemelni, ezzel is tovább biztosítva a gyors és gazdaságos telepítést.

A külső telephelyek hálózati kialakítása mind funkcionalitásuk egyezősége, mind egyfajta szabályosság, szabványosság megteremtés miatt hasonlítanak egymásra, ezzel is későbbi hibakeresések, illetve hálózat fejlesztési lehetőségek egyszerűbb kivitelezéséhez alkalmas közeg megteremtése volt a cél.

A dokumentáció igyekszik a technológiákat laikus szinten is megmagyarázni. További nem megválaszolt kérdések, illetve nem teljesen érthető kifejtések esetén keresse fel az alkotót ( elérhetőség a dokumentum végén.)

# Limitációk

Jelen dokumentáció nem szimulálja le különböző hálózati szolgáltatók jelenlétét (lásd Redundáns internet elérés), így a kőbányai hálózat mind két kijárata jelenleg ugyan arra a szolgáltatói eszközre csatlakozik fel, de ezek hálózati szempontból különválasztottnak tekintett. Egy valós helyzetben érdemes ezen internet felé vezető kapcsolatokat két, egymástól független szolgáltatóhoz beköttetni, ezzel is csökkentve a távolról elérendő eszközök szolgáltatás kiesésével járó események esélyét.

Másik probléma, hogy az alkotó számára nem állt rendelkezésre olyan router, ami kettőnél több hálózati interfésszel rendelkezett volna. A kőbányai kijáratok ezáltal egy kicsit érdekes módszerrel, egy harmadik switch bevonásával lettek bekötve. Egyik fizikai interfész felel a két switch felől érkező forgalmak összesítéséért (Trunk), illetve a másik interfész felel a szolgáltató hálózataiért (két külön IP tartomány, a switchig Trunk-ölve, utána már nincs címke). Ezzel egy ugyan elég torz szülött hálózati infrastruktúra alakult ki, de így tudta az alkotó a legkevesebb eszköz használatával megoldani a feladatot. Mindez kiváltható lenne egy legalább 3 csatlakozóval rendelkező routerrel, de sajnos az alkotónak ilyen nem állt rendelkezésére.

# Hálózat Megvalósítása

## A Hálózat Logikai Topológiája

A cég hálózata 4 telephelyet tartalmaz, a külső telephelyek a fő telephellyel site-to-site GRE Tunnel VPN-el, hálózatfejlesztés esetén GRE over IPsec VPN-el lesznek összeköttetve, előbbi egy egyszerűsített technológiájú, utóbbi pedig egy robusztusabb megvalósítása az interneten átívelő helyi hálózatok összeköttetésének.

Mindegyik telephely fel van bontva virtuális alhálózatokra, amik segítségével a hálózati forgalmakat lehet korlátozni. A korlátozás fő lényege, hogy például jogosulatlan eszközökről ne lehessen hozzáférni a telephelyi hálózatok gerincét képező 2. és 3. rétegbeli eszközökhöz, illetve nyomtatókhoz.

A szabványosság érdekében a különböző telephelyek IP címzési sémája szinte teljesen azonos. A telephelyek hálózatait egymástól az IP címük 3. octetje alapján lehet megkülönböztetni - a kőbányai hálózatok a 192.168.100.x címeket használják, a péceli hálózatok a 192.168.101.x címeket használják, stb. A szabványosság másik megnyilvánulása, hogy az azonos VLAN-okban azonos IP cím tartományok találhatók, például a 10-es VLAN (KLIENSEK) minden hálózatban az első 128 címet tartalmazza, az 50-es VLAN a következő 8 címet, és így tovább. Ezen alhálózatok tartományainak eloszlása a VLSM módszerrel lett megállapítva. A tényleges IP tartományokról egy későbbi fejezetben lesz szó.

Kivételes eset, hogy az egyik telephely egy már meglévő eszköz miatt a többi (külső) telephelyen megszokot hálózati infrastruktúra helyett (1 forgalomiránytó és 1 kapcsoló) egy ASA tűzfal eszközt tartalmaz, illetve a helyi VLAN-ok kezelése okán egy több rétegű kapcsoló kapott helyt.

## Telephelyek Hálózati Infrastruktúrája

### Kőbánya

A kőbányai telephely a cég központja, itt található szerverek szolgáltatásait az összes külső telephelyen dolgozó alkalmazott használja. A magasabb elérhetőségi szint érdekében a kőbányai hálózat két internet szolgáltatással is rendelkezik, melyek valós esetben két külön szolgáltatónál lennének bekötve. Emellett a belső hálózati szegmensben két switch található, amik egymással is összeköttetésben álnak Etherchannel technológiával. Ez mind kábel hibák, mind hálózati eszköz kieséséből adódó helyzeteket is képes áthidalni. Ez a két megoldás valósítja meg a második és harmadik rétegbeli redundanciát a kőbányai hálózatban. A Szerverek hálózata rendelkezik IPv6 címzéssel is, mivel az egyik szolgáltatói irány már dual-stack -kel működik, melynek címeit az eszközök SLAAC segítségével kapnak meg az átjárótól.

Az itt található szerverekről egy későbbi fejezetben lesz szó.

### Miskolc

A miskolci telephelyen egy már birtokolt eszköz miatt egy ASA, illetve egy több rétegű switch található, mint gerinc hálózati eszközök. Az ASA látja el az átjáró szerepét a miskolci nagy hálózat számára, tűzfal funkcionalitást, hálózati címfordítást, valamint a kőbányai szerverekhez való hozzáférés alapját, a VPN kapcsolatot szolgáltatja. A több rétegű switch az ASA liszenszének limitációja miatt vált szükségessé, ugyanis alap esetben ez a Liszensz csak 2 VLAN-t képes teljes értékűen kezelni, hármat már csak megszorításokkal, többet pedig egyáltalán nem. A több rétegű switch valósítja meg a VLAN-ok kezelését, a közöttük, illetve az ASA felé elérhető külső hálózatok felé történő forgalmak irányítását.

A miskolci hálózat minden más paraméterében megegyezik a másik két telephely paramétereivel.

### Csepel és Pécel

A csepeli és péceli hálózatok szinte teljesen megegyeznek egymással. Ezekben a hálózatokban egy router és egy switch található, mint gerinc hálózati eszközök. A router szolgáltatja a címfordítást, a kőbányai szerverek VPN-es elérését, valamint általánosságban a forgalomirányítást. A switch alapvetően csak csatlakozó többszörözés és VLAN szétválasztási funkciókat lát el.

## Felhasznált Hálózati Technológiák

### TCP/IP

A dokumentáció összes hálózata a TCP/IP protokoll szövetet alkalmazza. Fontos megjegyezni, hogy a kőbányai hálózatban nem csak IPv4, hanem IPv6 címzés is történik, így az ottani routernek képesnek kell lennie a dual-stack üzemre. Az IPv6-os címeket a VPN-es hálózatok nem hasznosítják, NAT64-et a Szerverek dual-stack-essége révén nem kell hasznosítani. Az alkalmazott beállítások egy későbbi fejezetben leesznek kifejtve.

### Etherchannel

A kőbányai hálózatban a két switch között Etherchannel technológiával több fizikai vonalat egy logikai vonalként használunk, ezzel az egyes kábelek esetleges hibája esetén is képesek vagyunk a switchek közötti adattovábbításra, illetve ezen csatlakozások sávszélessége össze is adódik. Mivel csak Cisco eszközök vannak használatban, így a PAgP protokoll részesült előnyben. Az alkalmazott beállítások egy későbbi fejezetben lesznek kifejtve.

### VLAN

Mindegyik telephely rendelkezik VLAN alhálózatokkal. A VLAN szabványok közül a 802.1q szabvány került alkalmazásra. Fontos szabályok:

A Trunk vonalakon csak a használatos VLAN-ok (10,20,30,50) lehetnek engedélyezve, natív VLAN-nak a 99-et (NEMHASZNALT) kell használni.

A nem használt interfészeket a 99-es VLAN-ba (NEMHASZNALT) kell rendelni, valamint azokat le kell kapcsolni.

Az alkalmazott beállítások egy későbbi fejezetben lesznek kifejtve.

### STP

A kőbányai harmadik switch miatt elengedhetetlennél vált a Spanning Tree Protocol használata, mely a második rétegbeli hálózati hurkokat szünteti meg. Nélküle szórási viharok alakulhatnának ki a hálózaton, ami akár teljes sávszélesség elvesztését is okozhatná. Beállítását csak a switchek általános beállításainál említi meg a dokumentáció, minden más beállítása alapértelmezetten megfelelően működik.

### SSH

A hálózati eszközök a VPN-ből bármikor elérhetőek, távoli konfigurálásuk SSH protokollon keresztül lehetséges. Az SSH protokoll beállításait, illetve beállításának előfeltételét jelentő beállításokat (domain név, kulcsok, stb.) egy későbbi fejezet fejti ki.

### VPN

A külső telephelyekről történő szerver elérés VPN-ek keresztül zajlik. Az alap forgalmakra a hálózatok átjárói között megvalósított site-to-site GRE Tunnel VPN lesz fenntartva. Hogy az ezen a kapcsolaton átmenő csomagok egy magasabb biztonsági szintet képviselve titkosított állományként kerüljenek az internetre, ahhoz más (újabb/frissebb) eszközöket kell beszerezni, amihez a projekt elkészítésekor az alkotónak nem volt hozzáférése. Minden olyan forgalom, ami nem a szerver felé megy, azok az internet irányába hagyják el a külső telephelyek hálózatát. Az olyan forgalmak, melyek egy külső telephelyről a főtelephely szervereire irányulnak, a VPN tunnelen keresztül fogják elhagyni a hálózatot, amin keresztül jutnak át a főtelephely hálózatába. A VPN beállításait egy későbbi fejezet fejti ki.

## Hálózati Alkalmazások

### Radius

A hálózati eszközök konfiguráláshoz megfelelő jogosultsággal kell rendelkezni. A Radius segítségével egy központi listában tudjuk tárolni a jogosult felhasználókat (hálózati rendszergazdákat), melynek szolgáltatása a Linux szerverről fog történni. Természetes a Radius szerver elérhetetlensége esetén egy lokális hitelesítés is elérhető marad, de azt csak és kizárólag Radius szerver mentes időkben lehet kihasználni. A beállítások egy későbbi fejezetben lesznek kifejtve.

### SFTP és TFTP

Ezen szolgáltatások elsődlegesen a hálózati eszközök biztonsági mentéseire van fenntartva. A két protokoll a hálózati eszközöknél nagyobb toleráló képességet gyakorol, mivel vannak olyan eszközök, amik csak ftp, vagy csak tftp-n keresztül képesek fájlátvitelt lebonyolítani. A beállításokat egy későbbi fejezet fejti ki.

### Rsyslog

A hálózati eszközök naplófájljait a Linux szerver gyűjti. Ezen szolgáltatás teszi lehetővé a naplófájlok fogadását és tárolását. Beállításait egy későbbi fejezet fejti ki.

### NTP

A hálózati eszközök és akár a végberendezések rendszer idejét érdemes szinkronban tartani. Ezt a célt szolgálja az NTP, ami a rendszeridőt hálózaton keresztül állítja be. NTP szolgáltatás a Linux szerveren fut, mely egy magyarországi időszerverről kéri le a pontos időt. A beállításokat egy későbbi fejezet fejti ki.

### Microsoft Active Directory

A központi fájlmegosztást, illetve az ehhez hozzáférő felhasználók azonosítását a Windows szerveren futó Active Directory Domain System szolgáltatás teszi lehetővé. A felhasználók a hálózat nagymértékű terhelésének elkerülése érdekében lokális felhasználókat használnak ugyan, de a központi fájlmegosztáskor egy, a szerveren megtalálható domain felhasználóval kell azonosítaniuk magukat jogosultságuk megszerzéséhez.

### DHCP

A Kliensek számára a külső hálózatokban a helyi átjárók, Miskolcon a több rétegű switch, kőbányán pedig a Windows szerver lát el DHCP, azaz dinamikus IP konfigurációs kiszolgáló szerepet. Ezek tényleges konfigurációját egy későbbi fejezet fejti ki.

### SLAAC

A kőbányai hálózat az egyik szolgáltatói linken rendelkezik IPv6 lehetőséggel, így a kőbányai router SLAAC-en keresztül kap IPv6 címet, valamint a Szerverek részére SLAAC-kel biztosítja a GUA IPV6-os címek létrehozását. A beállításokat egy későbbi fejezet fejti ki.

### DNS

A cég szervereinek egyszerűsített elérését a Domain neveket kezelő DNS szolgáltatás fogja garantálni, ami a Windows szerveren fut. Ebbe jelenleg a két céges szerver rekordjai szerepelnek, valamint ez kérdezi tovább a számára ismeretlen domain nevek mi létét. Későbbi fejlesztésként ezt a szolgáltatást akár a Linux szerver is elláthatja, melyen ezen címek szűrésére is lehetőség nyílik, hogy rosszindulatú szolgáltatások domain nevei, illetve nem munkához kapcsolódó oldalak domain nevei ne legyenek elérhetőek.

# Beállítások - Hálózati Eszközök

Ez a fejezet elsődlegesen a feladatok megnevezésével foglalkozik. A tényleges beállításokat a dokumentum végén, parancs szerinti kiírásban találhatók meg.

## Routerek

A külső telephelyeken található Routerek elsődlegesen a következő beállításokat kell elvégezni:

* Eszköz neve, valamint alap adatok beállítása (domain, lokális felhasználók, jelszavak, stb.),
* Alinterfészek létrehozása és VLAN-hoz rendelése (ha szükséges),
* Interfészek és alinterfészek IP címeinek beállítása (a megfelelő címek a dokumentum végén található táblázatban megtalálhatók),
* Rendszeridő NTP-n keresztüli szinkronizálása a fő telephelyi Linux szerverről,
* Hozzáférési listák konfigurálása (Internet hozzáférés (NAT) és a VPN egymásból való kizárása),
* Túlterheléses, port alapú hálózati címfordítás beállítása,
* GRE Tunnel létrehozása és konfigurálása,
* Bejelentkezések fő telephelyi radius szerverrel való hitelesítése (hiányában lokális kis-nagybetű érzékenységgel),
* Távoli Hozzáférés beállítása csak SSH-n keresztüli módra,
* Syslog naplózás beállítása a Linux szerverre,
* A helyi Kliens hálózatok számára DHCP szolgáltatás konfigurálása.

A miskolci ASA beállítása parancsokat tekintve másabb, de mindezen funkciókat ő is maradéktalanul ellátja.

A kőbányai router annyiban különbözik, hogy ezen a web szerver távoli elérése érdekében két cím lesz ki NAT-olva, egy statikusan a Linux szervernek, egy pedig minden más eszköznek mely nem a VPN irányába folytat kommunikációt.

## Switchek

A Péceli és Csepeli hálózatok switch-ein a következő beállításokat kell elvégezni:

* Eszköz neve, valamint alap adatok beállítása (lokális felhasználók, jelszavak, átjáró, stb.),
* VLAN-ok létrehozása és a megfelelő SVI-k konfigurálása (management IP, stb.),
* VLAN-ok interfészhez rendelése, nemhasznált interfészek lekapcsolása,
* Router felé irányuló interfész Trunk konfigurációjának beállítása (csak adott VLAN-ok, natív vlan),
* Portok beállítása gyors továbbító módba (*spanning-tree portfast*),
* Port biztonsági beállítások konfigurálása (*port-security*, *bpduguard*, *rootguard*, stb.),
* Távoli Hozzáférés beállítása csak SSH-n keresztüli módra.

A kőbányai eszközök kiegészülnek az Etherchannel beállításával, illetve itt az Etherchannelen keresztül is Trunk vonal valósul meg. Emellett a kiegészítő harmadik switch miatt az olyan portokat, amik mögött switch található, ne állítsa gyors továbbító módba (spanning-tree portfast).

A miskolci eszköznek a VLAN-ok között forgalomirányítási feladati is vannak, illetve ezen az eszközön nincs szükség Trunk vonal beállítására. Az ASA felé menő vonal a hálózati eszközök számára fenntartott alhálózatott használja, a rajta keresztül menő forgalmak gond nélkül továbbíthatóak az internet/VPN felé, míg a hálózati eszközöket célzó csomagok kiszűrhetőek maradnak, ezzel továbbra is fenntartva a hálózati eszközök hozzáférésének korlátozott módját.

# Beállítások - Szerverek

A következő fejezetek nagy vonalakban írják le a beállítások lépéseit. A köztes lépéseket/részeket az eszközöket konfiguráló rendszergazdának kompetenciáira hagyatkozva kell megoldania.

## Windows szerver

A projekt előkészülete alatt a Windows Server 2019 operációs rendszer állt rendelkezésre, így ennek beállításait és azok módszereit írja le a dokumentáció. Más Windows Server verzió esetén előfordulhat, hogy adott beállításokat nem úgy, vagy akár egyáltalán nem lehet beállítani, ezért az alkotó megkérné a dokumentációt olvasó és az eszköz konfigurálását végző rendszergazdát, hogy amennyiben lehetséges, a Windows Server 2019-es verzióját használja.

Telepítésre használt verzió**: Windows Server 2019 Standard Evaluation Desktop Experience (x64)**

* Legalább két merevlemez használata szükséges (egy fő, illetve egy a biztonsági mentések számára)
* Administrator jelszavának használja a "Passw0rd" kulcsszót
* Az eszköz nevét módosítsa computercegWIN-re
* Az eszköz IPv4 címét állítsa 192.168.100.146-ra, maszkot 255.255.255.248-ra (/29)
* Az eszköz IPv6 link-local címét állítsa fe80::2-re, GUA címét SLAAC-re
* Telepítse a következő szerepköröket:
  + Active Directory Domain Controller
  + DNS Server
  + DHCP Server
* Telepítse a következő funkcionalitásokat:
  + Windows Server Backup
* Minden nem említett beállítást alkalmazzon legjobb belátása szerint (dokumentálás erősen ajánlott).

### Active Directory Domain Controller

* Típusa: új erdő,
* Domain neve: computerceg.lan,
* Jelszónak használja a "Passw0rd" kulcsszót,
* Minden más beállítást legjobb belátása szerint állítson be.

### DNS

* A computerceg.lan domain-ben létre kell hozni a következő rekordokat:
* A Windows szerver részére egy WINSERVER (IP címe 192.168.100.146)
* A Linux szerver részére egy LINUXSERVER (IP címe 192.168.100.147)

### DHCP

* Scope neve: Kliensek
* IP tartomány: 192.168.100.3 - 192.168.100.126
* Maszk: /25, avagy 255.255.255.128
* Kizárt címek: nincs (csak a tartomány eleje lehetne (.1 - .2))
* Válassza az azonnali konfigurálást
* Alapértelmezett átjáró: 192.168.100.1
* DNS szerver: 192.168.100.146
* Aktiválja a scope-ot.

### Biztonsági mentés

A jelenlegi mentési rendszer csak a felhasználók által a Windows szerveren létrehozott központi, közös fájlmegosztásban megtalálható fájlokat menti el.

* Mentéseket a Windows szerveren, külön meghajtón tároljuk.
* Beállításai:
* Mentés ideje: 22:00 minden nap
* Mentés célja: Fizikai meghajtó
* Minden más beállítás az éppen használt eszközöktől függően kell beállítani (konkrét eszköz megnevezése, közös fájlmegosztás tényleges helye, stb.)

### Szervezeti Egységek

Hozzon létre egy Felhasznalok nevű szervezeti egységet a céges felhasználók profiljainak rendszerezése érdekében.

### Csoport beállítások

A fájlmegosztás korlátozása érdekében hozza létre a g\_felhasznalok csoportot és rendelje hozzá a megfelelő felhasználókat.

### Fájlmegosztás

A közös fájlmegosztás számára hozzon létre egy mappát a Windows szerveren, amit utána osszon meg a g\_felhasznalok csoport számára. Ajánlott megosztási név: Dokumentumok.

## Linux szerver

A projekt előkészülete alatt a Debian GNU/Linux 12 (bookworm) operációs rendszer lett kiválasztva, így ennek a beállításait és azok módszereit írja le a dokumentáció. Más Linux verzió esetén előfordulhat, hogy adott beállításokat nem úgy, vagy akár egyáltalán nem lehet beállítani, ezért az alkotó megkérné a dokumentációt olvasó és az eszköz konfigurálását végző rendszergazdát, hogy amennyiben lehetséges, a Debian GNU/Linux 12-es verzióját használja.

Telepítésre használt verzió: **Debian 12.5.0 amd64**

Az operációs rendszer telepítésénél vegye figyelembe a következőket:

* Az eszköz neve LinuxServer, tartománya computerceg.lan, root és admin felhasználója legyen Passw0rd jelszóval ellátva.
* Az operációs rendszert csak parancssoros felülettel és csak a szükséges rendszereszközökkel telepítse,
* A meghajtók partícionálásában és minden egyéb felmerülő kérdésben legjobb belátása szerint cselekedjen (dokumentálás erősen ajánlott).
* Telepítés után az apt részére állítson be hálózati tükröt legalább egy magyarországi debian szerverre (pl. [ftp.bme.hu](ftp://ftp.bme.hu))
* Az eszköz IPv4-es címét állítsa 192.168.100.147-re, maszkot 255.255.255.248-ra (/29)
* Az eszköz IPv6-os címét állítsa fe80::3-ra, GUA címét SLAAC-re
* Frissítse az apt listáját és utána töltse le a következő csomagokat: smbclient vsftpd tftpd-hpa tftp-hpa apache2 libapache2-mod-php mariadb-server phpmyadmin cockpit rsyslog ntp ufw ssh freeradius
* Állítsa be, hogy a vsftpd lokális felhasználókkal működjön, valamint a /home/ftp mappát használja adattárolásra
* Állítsa be, hogy a tftpd-hpa nem létező fájl esetén hozza létre azt, valamint a /configok mappát használja adattárolásra.
* Adja hozzá a Helyi rendszergazdákat (root és admin) a mariadb szerkesztésére jogosultak adatbázisához "Passw0rd" azonosítással.
* Hangolja össze a phpmyadmin működését a web és adatbázis szolgáltatásokkal és tesztelje, hogy a felület működőképes.
* Konfigurálja a rsyslog szervert az összes hálózati eszköz syslog üzenetének fogadására.
* Állítsa be az ntp időszervereket legalább egy magyar időszerverre (pl. 0.hu.pool.ntp.org) és szinkronizálja az eszköz rendszer-idejét.
* Konfigurálja be az ssh szervert a következők alapján:
* Ne engedje a root közvetlen bejelentkezését
* Figyelje 64422-es portot.
* Minden más beállítás tegyen legjobb belátása szerint (dokumentálás erősen ajánlott).
* A hálózati eszközök hitelesítése érdekében vegye fel az eszközöket a clients.conf állomány végére.
* Tesztelje egy már beállított hálózati eszköz segítségével a syslog szerver működését.
* Minden más beállítás tegyen legjobb belátása szerint (dokumentálás erősen ajánlott).

# Hálózati eszközök Interfész beállításai

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Eszköz** | **Interfész** | **VLAN** | **IP** | **Maszk** | **Prefix** | **Leírás (description)** |
| **RKobanya** | G0/0.70 | vlan70 | 10.0.0.2 | 255.255.255.248 | /29 | Kobanya1 ISP fele |
| G0/0.80 | vlan80 | 10.0.0.10 | 255.255.255.248 | /29 | Kobanya2 ISP fele |
| G0/1.10 | vlan10 | 192.168.100.1 | 255.255.255.128 | /25 | Kliensek |
| G0/1.20 | vlan20 | 192.168.100.145 | 255.255.255.248 | /29 | Szerverek |
| FE/0::1 |  |  |
| G0/1.30 | vlan30 | 192.168.100.137 | 255.255.255.248 | /29 | Nyomtatok |
| G0/1.50 | vlan50 | 192.168.100.129 | 255.255.255.248 | /29 | Halozati Eszkozok |
| Tunnel1 | - | 172.16.1.1 | 255.255.255.252 | /30 | Kobanya1 Miskolc VPN |
| Tunnel2 | - | 172.16.1.5 | 255.255.255.252 | /30 | Kobanya2 Miskolc VPN |
| Tunnel3 | - | 172.16.1.9 | 255.255.255.252 | /30 | Kobanya1 Pecel VPN |
| Tunnel4 | - | 172.16.1.13 | 255.255.255.252 | /30 | Kobanya2 Csepel VPN |
| **S1Kobanya** | VLAN50 | - | 192.168.100.130 | 255.255.255.248 | /29 | Management interface |
| F0/1-5 | - | - | - | - | port channel 1 |
| port-channel 1 | - | - | - | - | Trunk S1 es S2 kozott |
| F0/6 | vlan10 | - | - | - | Kliensek |
| F0/22 | vlan10 | - | - | - | WifiAP |
| F0/23 | vlan30 | - | - | - | Nyomtato1 |
| F0/24 | vlan30 | - | - | - | Nyomtato2 |
| G0/1 | - | - | - | - | Trunk S1 es S3 kozott |
| F0/7-21, G0/2 | vlan99 | - | - | - | Nem hasznalt |
| **S2Kobanya** | VLAN50 | - | 192.168.100.131 | 255.255.255.248 | /29 | Management interface |
| F0/1-5 | - | - | - | - | port channel 1 |
| port-channel 1 | - | - | - | - | Trunk S1 es S2 kozott |
| F0/6 | vlan20 | - | - | - | Windows server |
| F0/7 | vlan20 | - | - | - | Linux server |
| G0/1 | - | - | - | - | Trunk S2 es S3 kozott |
| F0/8-24, G0/2 | vlan99 | - | - | - | Nem hasznalt |
| **S3Kobanya** | VLAN50 | - | 192.168.100.132 | 255.255.255.248 | /29 | Management interface |
| F0/1 | - | - | - | - | RKobanya belso Trunk |
| F0/2 | - | - | - | - | RKobanya kulso Trunk |
| F0/3 | vlan70 | - | - | - | Kobanya1 ISP fele |
| F0/4 | vlan80 | - | - | - | Kobanya2 ISP fele |
| G0/1 | - | - | - | - | Trunk S1 es S3 kozott |
| G0/2 | - | - | - | - | Trunk S2 es S3 kozott |
| F0/5-24 | vlan99 | - | - | - | Nem hasznalt |
| **WINSERVER** | LAN | - | 192.168.100.146 | 255.255.255.248 | /29 | Windows server |
| FE80::2 |  |  |
| **LINUXSERVER** | LAN | - | 192.168.100.147 | 255.255.255.248 | /29 | Linux server |
| FE80::3 |  |  |
| **AMiskolc** | E1/1 | vlan2 | 10.0.0.18 | 255.255.255.248 | /29 | Miskolc ISP fele |
| E1/2 | vlan1 | 192.168.103.129 | 255.255.255.248 | /29 | Halozati Eszkozok |
| **SMiskolc** | VLAN1 | - | 192.168.103.130 | 255.255.255.248 | /29 | Management interface |
| VLAN10 | - | 192.168.103.1 | 255.255.255.128 | /25 | Kliensek |
| VLAN30 | - | 192.168.103.137 | 255.255.255.248 | /29 | Nyomtatok |
| F0/1 | vlan1 | - | - | - | Halozati Eszkozok |
| F0/2 | vlan10 | - | - | - | Kliensek |
| F0/22 | vlan10 | - | - | - | WifiAP |
| F0/23 | vlan30 | - | - | - | Nyomtato1 |
| F0/24 | vlan30 | - | - | - | Nyomtato2 |
| Tunnel1 | - | 172.16.1.2 | 255.255.255.252 | /30 | Kobanya1 Miskolc VPN |
| Tunnel2 | - | 172.16.1.6 | 255.255.255.252 | /30 | Kobanya2 Miskolc VPN |
| F0/3-21, G0/1-2 | vlan99 | - | - | - | Nem hasznalt |
| **RPecel** | G0/0 | - | 10.0.0.26 | 255.255.255.252 | /30 | Pecel ISP fele |
| G0/1.10 | vlan10 | 192.168.101.1 | 255.255.255.128 | /25 | Kliensek |
| G0/1.30 | vlan30 | 192.168.101.137 | 255.255.255.248 | /29 | Nyomtatok |
| G0/1.50 | vlan50 | 192.168.101.129 | 255.255.255.248 | /29 | Halozati Eszkozok |
| Tunnel1 | - | 172.16.1.10 | 255.255.255.252 | /30 | Kobanya1 Pecel VPN |
| Tunnel2 | - | 172.16.1.17 | 255.255.255.252 | /30 | Pecel Csepel VPN |
| **SPecel** | VLAN50 | - | 192.168.101.130 | 255.255.255.248 | /29 | Management interface |
| G0/1 | - | - | - | - | Trunk RPecel es SPecel kozott |
| F0/1 | vlan10 | - | - | - | Kliensek |
| F0/22 | vlan10 | - | - | - | WifiAP |
| F0/23 | vlan30 | - | - | - | Nyomtato1 |
| F0/24 | vlan30 | - | - | - | Nyomtato2 |
| F0/2-21, G0/2 | vlan99 | - | - | - | Nem hasznalt |
| **RCsepel** | G0/0 | - | 10.0.0.30 | 255.255.255.252 | /30 | Csepel ISP fele |
| G0/1.10 | vlan10 | 192.168.102.1 | 255.255.255.128 | /25 | Kliensek |
| G0/1.30 | vlan30 | 192.168.102.137 | 255.255.255.248 | /29 | Nyomtatok |
| G0/1.50 | vlan50 | 192.168.102.129 | 255.255.255.248 | /29 | Halozati Eszkozok |
| Tunnel1 | - | 172.16.1.14 | 255.255.255.252 | /30 | Kobanya2 Csepel VPN |
| Tunnel2 | - | 172.16.1.18 | 255.255.255.252 | /30 | Pecel Csepel VPN |
| **SCsepel** | VLAN50 | - | 192.168.102.130 | 255.255.255.248 | /29 | Management interface |
| G0/1 | - | - | - | - | Trunk RCsepel es SCsepel kozott |
| F0/1 | vlan10 | - | - | - | Kliensek |
| F0/22 | vlan10 | - | - | - | WifiAP |
| F0/23 | vlan30 | - | - | - | Nyomtato1 |
| F0/24 | vlan30 | - | - | - | Nyomtato2 |
| F0/2-21, G0/2 | vlan99 | - | - | - | Nem hasznalt |
| **Kliens számítógépek** | LAN | - | DHCP | DHCP | DHCP | Kliens számítógépek |

# Minta Konfiguráció - Router

Ebben a fejezetben a routerekkel kapcsolatos konfigurációk találhatóak meg. Mivel több router beállítási palettája csak minimális dolgokban tér el egymástól, ezek nincsenek megismételve. Minden beállítási típus csak egyszer fordul elő, melyek bemutatásához a kőbányai, valamint a péceli routerek konfigurációi lettek felhasználva.

### Eszköz neve, valamint alap adatok beállítása

*hostname RPecel  
username admin privilege level 15 password Passw0rd  
enable password Passw0rd  
ip domain-name computerceg.hu  
line console 0  
 logging synchronous  
 exit*

### Alinterfészek létrehozása és VLAN-hoz rendelése (ha szükséges)

*interface G0/1.10  
 encapsulation dot1q 10  
 exit  
interface G0/1  
 no shutdown  
 exit*

### Interfészek és alinterfészek IP címeinek és leírásainak beállítása

*interface G0/0  
 description ISP\_Fele  
 ip address 10.0.0.26 255.255.255.252  
 no shutdown  
 exit  
interface G0/1.10  
 description Kliensek  
 ip address 192.168.101.1 255.255.255.128  
 exit*

### Rendszeridő NTP-n keresztüli szinkronizálása a fő telephelyi Linux szerverről

*ntp server 192.168.100.147  
service timestamps log datetime msec  
!Ha hitelesiteni szeretnenk az ntp kiszolgalot:  
ntp authenticate  
ntp authentication-key 1 md5 Passw0rd*

### Hozzáférési listák konfigurálása

*ip access-list extended NAT-ACL  
 deny ip 192.168.101.0 0.0.0.255 192.168.100.0 0.0.0.255  
 permit ip 192.168.101.0 0.0.0.127 any  
 exit*

### Túlterheléses, port alapú hálózati címfordítás beállítása

*interface G0/0  
 ip nat outside  
 exit  
interface G0/1.10  
 ip nat inside  
 exit  
ip nat inside source list NAT-ACL interface G0/0 overload*

### Statikus NAT

*ip nat inside source static 192.168.100.147 10.0.0.3*

### GRE Tunnel létrehozása és konfigurálása

*interface tunnel1  
 ip address 172.16.1.10 255.255.255.252  
 tunnel source G0/0  
 tunnel destination 10.0.0.2  
 no shutdown  
 exit*

### Bejelentkezések fő telephelyi radius szerverrel való hitelesítése (hiányában lokális kis-nagybetü érzékenységgel)

*aaa new-model  
aaa authentication login Bejelentkezes group radius local-case  
radius-server host 192.168.100.147 key Passw0rd  
line vty 0 15  
 login authentication Bejelentkezes  
 exit*

### Távoli Hozzáférés beállítása csak SSH-n keresztüli módra

*crypto key generate rsa general-keys modulus 1024  
ip ssh version 2  
ip ssh time-out 120  
ip ssh authentication-retries 3  
line vty 0 15  
 transport input ssh  
 exit*

### Syslog naplózás beállítása a Linux szerverre

*logging on  
logging trap  
logging host 192.168.100.147*

### A helyi Kliens hálózatok számára DHCP szolgáltatás konfigurálása

*ip dhcp excluded-address 192.168.101.1 192.168.101.2  
ip dhcp pool Kliensek  
 default-router 192.168.101.1  
 dns-server 192.168.100.146  
 network 192.168.101.0 255.255.255.128  
 exit*

### IPv6 forgalomirányítás

*ipv6 unicast-routing  
interface G0/1.20  
 ipv6 enable  
 ipv6 address fe80::1 link-local  
 exit*

# Minta konfiguráció - Switch

A Péceli és Csepeli hálózatok switchein a következő beállítások a jellemzőek.

### Eszköz neve, valamint alap adatok beállítása

*hostname SPecel  
username admin privilege 15 passwor Passw0rd  
enable password Passw0rd  
ip domain-name computerceg.hu  
ip default-gateway 192.168.101.129  
line console 0  
 logging synchronous  
 exit*

### VLAN-ok létrehozása és a megfelelő SVI-k konfigurálása (management IP, stb)

*vlan 10  
 name KLIENSEK  
vlan 30  
 name NYOMTATOK  
vlan 50  
 name HALOZATIESZKOZOK  
vlan 99  
 name NEMHASZNALT  
 exit  
interface vlan50  
 description Management interface  
 ip add 192.168.101.130 255.255.255.248  
 no shutdown  
 exit*

### VLAN-ok interfészhez rendelése, nemhasznált interfészek lekapcsolása

*interface F0/1  
 description Kliensek  
 switchport mode access  
 switchport access vlan 10  
 no shutdown  
 exit  
interface range f0/2-21,G0/2  
 description Nem hasznalt  
 switchport mode access  
 switchport access vlan 99  
 shutdown  
 exit*

### Router felé irányuló interfész Trunk konfigurációjának beállítása (csak adott VLAN-ok, nativ vlan)

*interface G0/1  
 description Trunk RPecel es SPecel kozott  
 switchport mode trunk  
 switchport trunk native vlan 99  
 switchport trunk allowed vlan 10,30,50  
 no shutdown  
 exit*

### Portok beállítása gyors továbbító módba (spanning-tree portfast)

*!Mivel ezekben a halozat tipusokban csak egy switch talalhato, ezert az osszes portot gyorstovabbitonak tekinthetjuk  
interface range F0/1-24,G0/1-2  
 spanning-tree portfast  
 exit*

### Portbiztonsági beállítások konfigurálása

*!Az elozo gondolatmenettel harmoniaban  
interface range F0/1-24,G0/1-2  
 switchport port-security  
 spanning-tree bpduguard enable  
 spanning-tree guard root  
 exit*

### Távoli Hozzáférés beállítása csak SSH-n keresztüli módra

*crypto key generate rsa general-keys modulus 1024  
ip ssh version 2  
ip ssh time-out 120  
ip ssh authentication-retries 3  
aaa new-model  
aaa authentication login Bejelentkezes group radius local-case  
radius-server host 192.168.100.147 key Passw0rd  
line vty 0 15  
 transport input ssh  
 login authentication Bejelentkezes  
 exit*

A kőbányai eszközök kiegészülnek az Etherchannel beállításával, illetve itt az Etherchannelen keresztül is Trunk vonal valósul meg. Emellett a kiegészítő harmadik switch miatt az olyan portokat, amik mögött switch található, ne állítsa gyors továbbító módba (*spanning-tree portfast*).

### Etherchannel létrehozása

*interface range F0/1-5  
 shutdown  
 channel-group 1 mode desirable  
 no shutdown  
 exit  
interface port-channel 1  
 no shutdown  
 exit  
!Innentol kezdve a port-channel 1 kezelheto ugy, mint egy darab interfesz, az eddig ismertetett beallitasok alkalmazhatoak ra.*

A miskolci eszköznek a VLAN-ok között forgalomirányítási feladati is vannak, illetve ezen az eszközön nincs szükség Trunk vonal beállítására. Az ASA felé menő vonal a hálózati eszközök számára fenntartott alhálózatott használja, a rajta keresztül menő forgalmak gond nélkül továbbíthatóak az internet/VPN felé, míg a hálózati eszközöket célzó csomagok kiszürhetőek maradnak, ezzel továbbra is fenntartva a hálózati eszközök hozzáférésének korlátozott módját.

A miskolci többrétegű switch egyszerűbb kezelése érdekében érdemes továbbra is az interfészeket vlan-okba rendezni és ezen VLAN-ok SVI-inek ip-címet addni.

### Forgalomiránytás bekapcsolása

*ip routing*

# Projekt szervezési eszközök

A kkk-ban meghatározott feltételek alapján érinteni kell a projekt szervezése alatt használt, projekt elkészülését segítő technológiák és alkalmazások bemutatását. Az év végére készülő projektben az ottani csapattársakkal a kapcsolatot több felületen tartjuk. Elsődleges kommunikációs felület a Discord nevű, szöveges és hang alapú kommunikációt támogató chat-program. Ezen elsősorban a felmerülő problémák megvitatása, valamint probléma megoldására irányuló megvalósítások (például hogyan legyen megoldva a szolgáltató szimulálása) céljából van hasznosítva.

A projekt másik két hasznos alkalmazása a Trello, mely egy Projekt menedzsment megoldás, elsődlegesen a mérföldkövek követésére van hasznosítva. Másik fontos alkalmazás a Git verziókezelő szoftvert felhőben megvalósító GitHub, amit a konfigurációs, dokumentációs, valamint a projekt szabályozásával kapcsolatos segítő fájlok (jó szokások, nevezési szabályok, stb.) tárolására, valamint azok verzió követésére hasznosítunk.

Készítette a 2023/24-es  
SzKTV versenyre: Nagy István  
([isti.nagy03[kukac]gmail.com](mailto:isti.nagy03@gmail.com?subject=Vizsgaremek%20dokumentáció%20kérdés))