Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

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

***száma:*** 5-0612-12-02

**VIZSGAREMEK**

**Magyar Nemzeti Múzeum**

Jelenovszki Mihály, Király Ákos, Tankó Erik Péter  
2/14.B

Budapest, 2023.

**Tartalomjegyzék**

[Magyar Nemzeti Múzeum megbízása 5](#_Toc134329944)

[A hálózat bemutatása 5](#_Toc134329945)

[Régészeti Főosztály 6](#_Toc134329946)

[Cisco Packet Tracer eszközök 6](#_Toc134329947)

[Használt protokollok 6](#_Toc134329948)

[Központi Adattár 7](#_Toc134329949)

[Cisco Packet Tracer eszközök 7](#_Toc134329950)

[Használt protokollok 7](#_Toc134329951)

[Rendezvényszervezési Főosztály 8](#_Toc134329952)

[Cisco Packet Tracer eszközök 8](#_Toc134329953)

[Használt protokollok 8](#_Toc134329954)

[Ügyfélszolgálat 9](#_Toc134329955)

[Cisco Packet Tracer eszközök 9](#_Toc134329956)

[Használt protokollok 9](#_Toc134329957)

[MNM Szerverek 10](#_Toc134329958)

[Cisco Packet Tracer eszközök 10](#_Toc134329959)

[Szerverek és szolgáltatások 10](#_Toc134329960)

[Pénzügyi és Gazdasági Iroda 11](#_Toc134329961)

[Cisco Packet Tracer eszközök: 11](#_Toc134329962)

[Használt protokollok: 11](#_Toc134329963)

[Pénztár 12](#_Toc134329964)

[Cisco Packet Tracer eszközök: 12](#_Toc134329965)

[Használt protokollok: 12](#_Toc134329966)

[Gerinchálózat 13](#_Toc134329967)

[Cisco Packet Tracer eszközök: 13](#_Toc134329968)

[Használt protokollok: 13](#_Toc134329969)

[Hálózat dokumentáció 14](#_Toc134329970)

[HSRP 14](#_Toc134329971)

[Parancsok 14](#_Toc134329972)

[VTP 15](#_Toc134329973)

[Parancsok 15](#_Toc134329974)

[Link Aggregation 16](#_Toc134329975)

[Parancsok 16](#_Toc134329976)

[DHCP Snooping 17](#_Toc134329977)

[Parancsok 17](#_Toc134329978)

[VOIP 18](#_Toc134329979)

[Port security 19](#_Toc134329980)

[Parancsok 19](#_Toc134329981)

[Dinamikus Forgalomirányítás 20](#_Toc134329982)

[Előnyök 20](#_Toc134329983)

[Hátrányok 20](#_Toc134329984)

[EIGRP 20](#_Toc134329985)

[Statikus Forgalomirányítás 21](#_Toc134329986)

[Előnyök 21](#_Toc134329987)

[Hátrányok 21](#_Toc134329988)

[Alapértelmezett statikus útvonal 21](#_Toc134329989)

[STP 22](#_Toc134329990)

[Parancsok 22](#_Toc134329991)

[SSH 23](#_Toc134329992)

[Parancsok 23](#_Toc134329993)

[VLAN 24](#_Toc134329994)

[Parancsok 24](#_Toc134329995)

[ACL 25](#_Toc134329996)

[NAT 26](#_Toc134329997)

[Statikus NAT 26](#_Toc134329998)

[PAT 26](#_Toc134329999)

[Jelszó titkosítás 27](#_Toc134330000)

[WAN 27](#_Toc134330001)

[IPsec 28](#_Toc134330002)

[ASA 29](#_Toc134330003)

[Policy-map 29](#_Toc134330004)

[Class-map 29](#_Toc134330005)

[Service-policy 29](#_Toc134330006)

[ACL 29](#_Toc134330007)

[Ip Route 30](#_Toc134330008)

[SSH 30](#_Toc134330009)

[VLAN 30](#_Toc134330010)

[IPv6 31](#_Toc134330011)

[Távmunkás 34](#_Toc134330012)

[Access Point 35](#_Toc134330013)

[Cisco Packet Tracer szerverek 36](#_Toc134330014)

[DHCP 36](#_Toc134330015)

[DNS 37](#_Toc134330016)

[FTP 38](#_Toc134330017)

[TFTP 38](#_Toc134330018)

[EMAIL 39](#_Toc134330019)

[WEB 39](#_Toc134330020)

[SYSLOG 40](#_Toc134330021)

[NTP 41](#_Toc134330022)

[Szerverek dokumentáció 42](#_Toc134330023)

[Szolgáltatások 42](#_Toc134330024)

[Active Directory 42](#_Toc134330025)

[Domain Controller 42](#_Toc134330026)

[Secondary Domain Controller 42](#_Toc134330027)

[Dynamic Host Configuration Protocol 42](#_Toc134330028)

[Domain Name System 42](#_Toc134330029)

[DHCP Failover 42](#_Toc134330030)

[Print server 42](#_Toc134330031)

[WEB szerver (IIS) 42](#_Toc134330032)

[File szerver 42](#_Toc134330033)

[Email szerver 43](#_Toc134330034)

[VPN 43](#_Toc134330035)

[Group Policy Object 43](#_Toc134330036)

[Mikrotik 46](#_Toc134330037)

[AD DC DNS DHCP 46](#_Toc134330038)

[DHCP 46](#_Toc134330039)

[AD DC 47](#_Toc134330040)

[DNS 48](#_Toc134330041)

[MAIL FTP File Print 49](#_Toc134330042)

[File Print 49](#_Toc134330043)

[WEB 49](#_Toc134330044)

[FTP 51](#_Toc134330045)

[MAIL 52](#_Toc134330046)

[Hálózatprogramozás 53](#_Toc134330047)

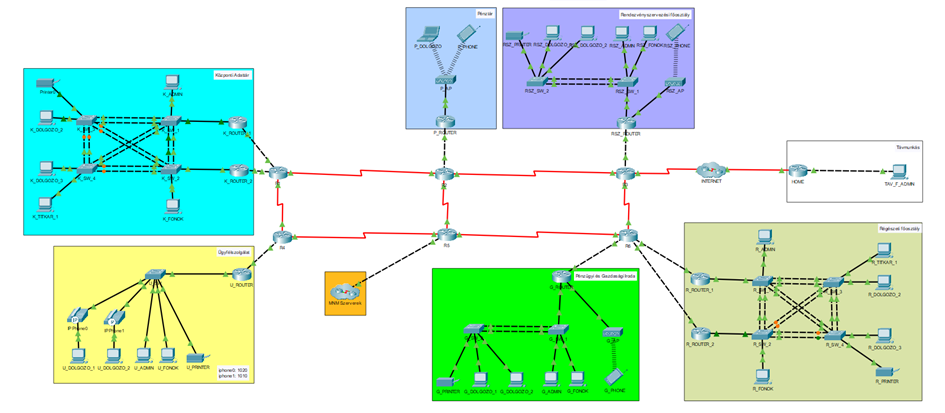
[PNET 53](#_Toc134330048)

[Python 54](#_Toc134330049)

# Magyar Nemzeti Múzeum megbízása

A Magyar Nemzeti Múzeum megbízott minket, hogy tervezzük meg és alakítsuk ki saját hálózatát, hogy a múzeumban és azon kívül dolgozó emberek számára a kommunikáció egyszerűbb legyen, az adatok biztonságos módon eljuthassanak a különböző főosztályokhoz és könnyedén eltudhassák végezni napi feladataikat.

# A hálózat bemutatása

A hálózat topológiai felépítését a Cisco Packet Tracer hálózat szimulációs programját használtuk. A teljes hálózat az alábbi képen látható.

. ábra A hálózat topológiája

A hálózat főosztályokból, szerverszobából, ügyfélszolgálatból, egy gazdasági irodából, illetve egy pénztárból áll.

- Türkiz terület: Központi Adattár Főosztály

- Szürke terület: Régészeti Főosztály

- Lila terület: Rendezvényszervezési Főosztály

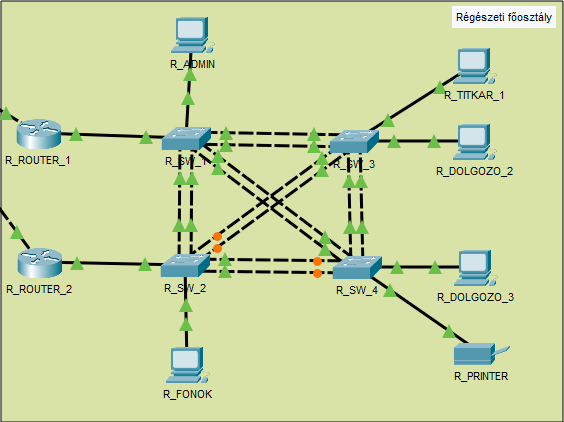
- Fehér terület: Ügyfélszolgálat

- Sötét kék terület: Pénztár

- Narancssárga terület: MNM Szerverek

- Zöld terület: Pénzügyi és Gazdasági Iroda

## Régészeti Főosztály

A Régészeti főosztály a Magyar Nemzeti Múzeum főépületén belül dolgozik, ahol a régi, múzeumi leletekről, tárgyakról szakmai dokumentálást készítenek, amelyeket továbbítanak a Központi Adattárhoz.

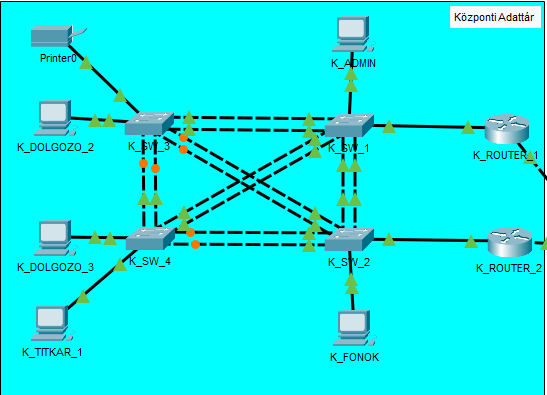
### Cisco Packet Tracer eszközök

* 2db Cisco 2911 router
* 4db Cisco 2960 switch
* printer
* PC-k

### Használt protokollok

* HSRP
* STP
* Link Aggregation
* VTP
* EIGRP
* Port Security
* SSH
* VLAN

## Központi Adattár

A Központi Adattár a feladatai a Régészeti főosztállyal való kapcsolattartás és az onnan kapott dokumentálásoknak, fotóknak, információknak a gyűjtése, megőrzése és feldolgozása.

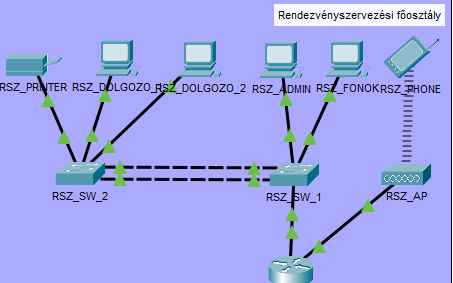
### Cisco Packet Tracer eszközök

* 2db Cisco 2911 router
* 4db Cisco 2960 switch
* printer
* PC-k

### Használt protokollok

* HSRP
* STP
* Link Aggregation
* VTP
* EIGRP
* Port Security
* SSH
* VLAN

## Rendezvényszervezési Főosztály

A Rendezvényszervezési főosztály, ahol a Magyar Nemzeti Múzeum rendezvényeinek, programjainak a megtervezése és annak a megszervezése a főbb feladatuk.

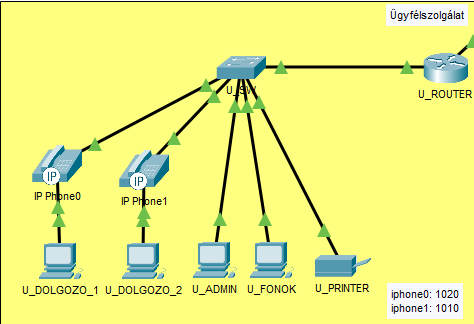
### Cisco Packet Tracer eszközök

* 1db Cisco 2911 router
* 2db Cisco 2960 switch
* printer
* PC-k
* 1db access point
* smartphone

### Használt protokollok

* DHCP (Router)
* VLAN
* Link Aggregation
* EIGRP
* Port Security
* ACL
* SSH

## Ügyfélszolgálat

Az ügyfélszolgálati részen a dolgozók kezelik, illetve fogadják az esetleges panaszokat, információval látják el az ügyfelet és segítenek minden esetleges kérdésben.

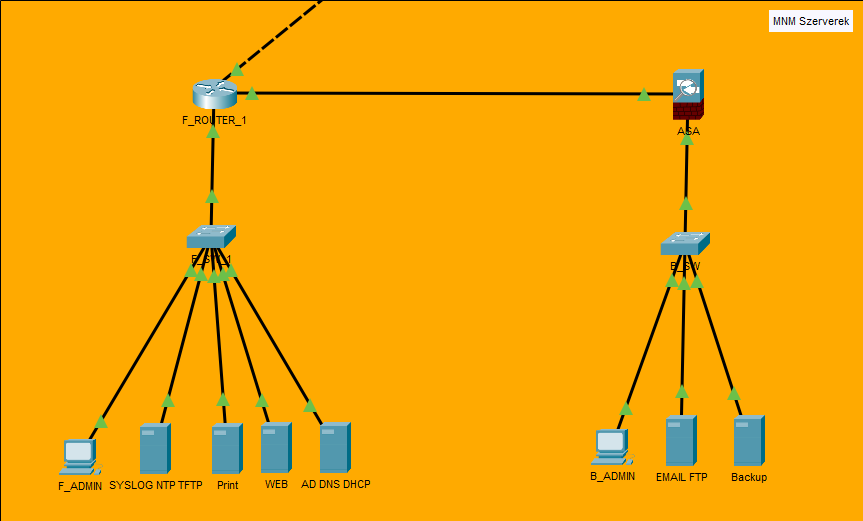
### Cisco Packet Tracer eszközök

* 1db Cisco 2911 router
* 1db Cisco 2960 switch
* printer
* PC-k
* IP phone

### Használt protokollok

* DHCP (Router)
* VLAN
* EIGRP
* Port Security
* ACL
* SSH

## MNM Szerverek

A Magyar Nemzeti Múzeum számára ki lett alakítva egy szerverszoba, ahol a szerverek különböző szolgáltatásokat nyújtanak dolgozók számára.

### Cisco Packet Tracer eszközök

* 1db Cisco 2911 router
* 2db Cisco 2960 switch
* Szerverek
* PC-k
* Cisco ASA 5505 tűzfal

### Szerverek és szolgáltatások

* AD
* DNS
* DHCP
* EMAIL
* FTP
* PRINT
* SYSLOG
* NTP
* TFTP
* Backup (DHCP Failover)

## Pénzügyi és Gazdasági Iroda

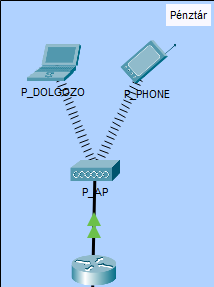
### Cisco Packet Tracer eszközök:

* 1db Cisco 2911 router
* 2db Cisco 2960 switch
* printer
* PC-k
* 1db access point
* smartphone

### Használt protokollok:

* DHCP (Router)
* VLAN
* Link Aggregation
* EIGRP
* Port Security
* ACL
* SSH

## Pénztár

A pénztár, ahol a vásárlók képesek a múzeummal kapcsolatos rendezvényekre jegyeket vásárolni.

### Cisco Packet Tracer eszközök:

* 1db Cisco 2911 router
* 1db access point
* laptop
* smartphone

### Használt protokollok:

* DHCP (Router)
* EIGRP
* ACL
* SSH

## Gerinchálózat

A hálózatok, irodák összeköttetése érdekében kialakítottunk egy gerinchálózatot.

### Cisco Packet Tracer eszközök:

* 6db Cisco 2911 router

### Használt protokollok:

* EIGRP
* SSH
* IPsec
* Static Route
* PPP CHAP

# Hálózat dokumentáció

## HSRP

Hot Standby Router Protocol (HSRP) egy harmadik rétegbeli redundáns megoldás. Ennek a segítségével, ha a hálózatban valamelyik router nem működne, akkor a másik router fogja átvenni a forgalomirányítás feladatát.

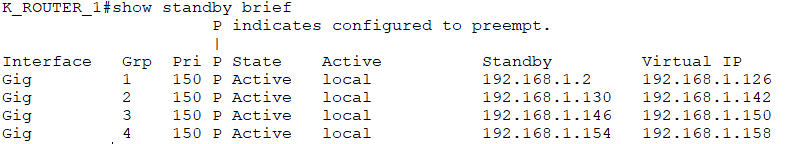
Ezt egy virtuális ip cím és prioritásérték megadásával lehetséges. A virtuális ip címen több router is osztozik, egymás között megbeszélve, hogy melyikük fogja az alapértelmezett átjáró feladatát ellátni. A legnagyobb prioritású router fogja megkapni az aktív (active) szerepet. A második legnagyobb prioritású router fogja megkapni a tartalék (standby) szerepet. Ha pedig egy hálózaton belül kettőnél több router osztozik a virtuális ip címen, akkor az aktív és tartalék routeren kívül többi router a figyelő (listen) állapotba fog kerülni. Ha az aktív kiesik, akkor a tartalék veszi át a feladatát, és a legmagasabb prioritású figyelő állapotú lesz a tartalék.

Minden routernek van egy alapértelmezett HSRP prioritása, melynek 100 az értéke. Amennyiben két router azonos prioritással rendelkezik, akkor LAN-hoz kapcsolódó interfész ip címe alapján döntik el az aktív szerepet.

### Parancsok

Először belépünk egy interfészbe, majd kiadjuk az alábbi parancsokat:

* *standby* <szám> *ip* <ip cím>
* *standby* <szám> *priority* <prioritási érték>



## VTP

A Vlan Trunking Protocol (VTP) segítségével nem kell manuálisan beállítani minden switch-nél a VLAN-okat, mivel az eszközök ezeket képesek egymástól megtanulni.

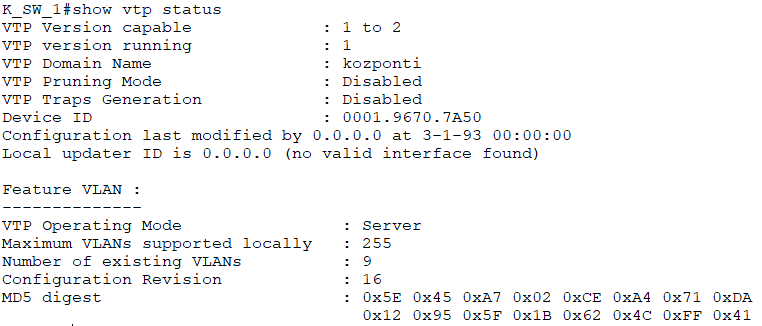
Ehhez szükségünk lesz megadni egy VTP domain nevet, egy VTP jelszót, illetve, hogy milyen módban legyen az adott switch.

VTP-nél két mód létezik. Az egyik a szerver (server) mód, ahol manuálisan beállítjuk a VLAN-okat, a domain nevet, illetve a jelszót. A másik a kliens (client) mód, aminek a beállításával a kliens módú switch-ek képesek a szerver módú switch-től megtanulni a VLAN-okat. Viszont ez csak akkor lehetséges, ha domain név, illetve a hozzátartozó jelszó megegyeznek a többi switch-nél is.

### Parancsok

A VTP beállításánál minden switch-nek az alapértelmezett módja a szerver. Tehát nem feltétlen kell megadni a szerver módot, hacsak nem szeretnénk kliensről szerverre átállítani.

* *vtp mode server/client*
* *vtp domain* <név>
* *vtp password* <jelszó>



## Link Aggregation

Link Aggregation, magyarul port összefogás megoldja, hogy a switch-eken több fizikai kábelt virtuálisan összekössünk, egy kábelként kezeljen.

Ezáltal növeli a sávszélességet, illetve, ha az egyik kábel megsérülne, akkor is működni fog a kapcsolat az összekötött eszközök között, tehát plusz védelmet is biztosít a hálózat számára.

Protokollok:

* Link Aggregation Control Protocol (LACP)
  + Bármely hálózati eszköznél használható
* Port Aggregation Protocol (PAGP)
  + Csak Cisco eszközöknél lehet használni

Mi hálózatunkban PAGP-t alkalmaztunk, mivel Cisco-s eszközöket használunk.

### Parancsok

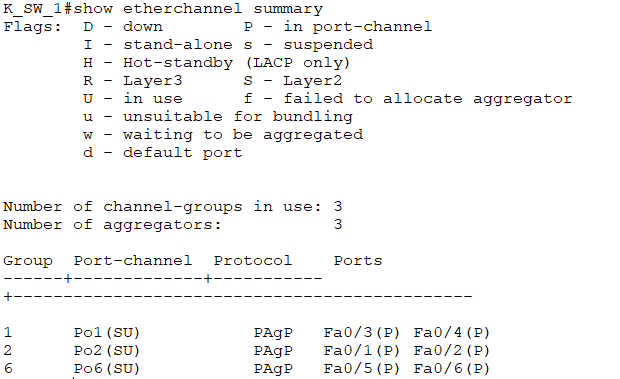
Először be kell lépnünk az általunk kiválasztott interfészekbe az *interface range* paranccsal.

PAGP:

* *channel-group* <szám> mode *on/desirable/auto*

LACP:

* *channel-group* <szám> mode *on/active/passive*



## 

## DHCP Snooping

A DHCP Snooping egy biztonsági technológia a 2. rétegű hálózati kapcsolón, amely megakadályozza, hogy illetéktelen DHCP kiszolgálók hozzáférjenek a hálózathoz. Ez egy védelem a nem megbízható gépekkel szemben, amelyek DHCP kiszolgálókká akarnak válni. A DHCP Snooping védelmet nyújt a köztes támadásokkal szemben. Maga a DHCP az OSI réteg 3. rétegén működik, míg a DHCP Snooping a 2. rétegű eszközökön működik a DHCP kliensektől érkező forgalom szűrésére.

A DHCP szerver létfontosságú szerepet tölt be minden szervezet hálózatában, mivel a legtöbb végfelhasználói eszköz, például a PC és a laptopok is DHCP-t használnak az IP-címek automatikus megtanulására. A szervezet hálózatán belüli eszközök védelme érdekében be kell állítanunk a DHCP Snooping-ot a 2. rétegbeli kapcsolón, ahol a megbízhatatlan eszközök csatlakoznak.

### Parancsok

Először be kell állítanunk az alábbi parancsot:

* *ip dhcp snooping*

Majd belépni az általunk megadott interfészekbe:

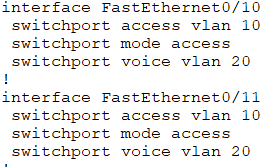
* *ip dhcp snooping trust*

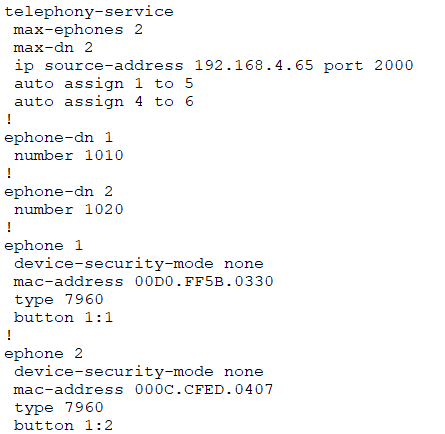
*A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás*

## VOIP

Az ügyfélszolgálatnál IP phone-okat alkalmaztunk, hogy hívásban tudják fogadni, kezelni az esetleges panaszokat.

A switch-en létrehoztunk egy VOICE nevű VLAN-t, amelyet a megfelelő interfészekhez hozzákapcsoltuk.



## Port security

A Port security, magyarul port védelem egy hasznos védelmi funkció. Ennek segítségével megakadályozzuk az illetéktelen behatolásokat.

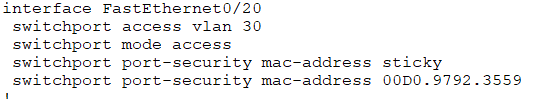
### Parancsok

Elsősorban a sticky parancsot használjuk, ezáltal a MAC címet dinamikusan megtanulja az eszköz, ahol kiadtuk a parancsot.

* *switchport port-security mac-address sticky*

Majd beállítjuk, hogy milyen műveletet hajtson végre, ha ismeretlen eszköz akarja használni a portot (általában az alapméretezett beállítását használjuk ennek a parancsnak, mert ez a legbiztonságosabb)

* *switchport port-security violation shutdown*



## Dinamikus Forgalomirányítás

Dinamikus forgalomirányítás protokoll feladatai közé tartozik a távoli hálózatok felderítése, információk karbantartása, a legjobb útvonal kiválasztása, valamint, ha egy útvonal elérhetetlenné válik, akkor egy újabb útvonal kiválasztása.

A router üzeneteket küld és fogad az interfészein, megosztják és cserélnek információkat a többi routerrel, amelyek ugyanazt a protokollt használják.

### Előnyök

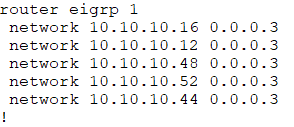
* könnyebb és gyorsabb konfigurálás nagyobb hálózatokban
* gyorsabb konvergencia
* alkalmazkodóképesség

### Hátrányok

* magasabb erőforrás igény
* kevésbé biztonságos a broadcast és a multicast frissítések miatt
* nagyobb sávszélességet használ

### EIGRP

Az Enhanced Interior Gateway Routing Protocol (EIGRP) egy Cisco által fejlesztett távolság vektor alapú dinamikus forgalomirányitási protokoll. DUAL algoritmus használatával hurok mentes útvonalakat biztosít.

Hálózatunkban ezt a megoldást használtuk, mivel gyorsabb konvergenciát biztosít és terhelésmegosztás szempontjából is jobb, mint az OSPF.

## Statikus Forgalomirányítás

### Előnyök

* könnyebb konfigurálás és menedzselés kisebb hálózatokban
* nem terheli a routert és a hálózatot
* biztonságosabb, mivel a statikus útvonalakat nem hirdetik a hálózaton

### Hátrányok

* megfelelő működéshez a teljes hálózat ismeretére van szükség
* nehéz és időigényes konfigurálás
* hiba vagy leállás esetén nem reagál automatikusan a hálózat

### Alapértelmezett statikus útvonal

Az alapértelmezett statikus útvonal egy olyan útvonal, amely minden csomagra illeszkedik. Ezen felül meghatározza azt az átjáró IP-címet is, ahova a router minden olyan csomagot elküldhet, amelyekhez nem tartozik sem megtanult, sem pedig statikus útvonal. Lényegében egy 0.0.0.0/0 IPv4 célcímmel megadott statikus útvonal. Beállítása egy végső átjárót hoz létre.

Mi hálózatunkba a gerinchálózat határ routere és az Internet közé lett alkalmazva.

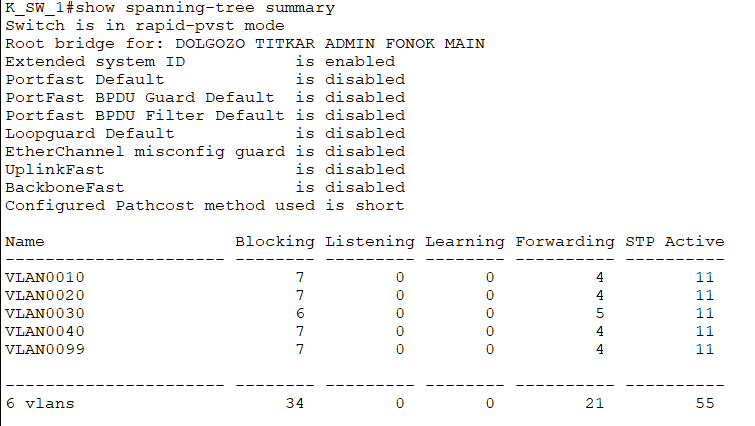


## STP

Mivel nagy hangsúlyt fektettünk arra, hogy a hálózat erőforrásai megfelelő módon legyenek kezelve és elkerüljünk minden olyan lehetséges esetet, ahol felesleges módon vagy a hálózat stabil, gyors működésnek a rovására legyenek felhasználva a rendelkezésre álló hardverek így Spanning Tree Protocolt konfiguráltunk minden olyan helyen, ahol egyszerre több alternatív útvonal is rendelkezésre áll, mivel PDU hurkok és broadcast viharok alakulhatnak ki ezeken a területeken amik jelentős mértékben befolyásolják a hálózat működésének a sebességet. Rosszabb esetekben ezek a viharok és hurkok a hálózat leállásához is vezethetnek.

### Parancsok

* *spanning-tree mode rapid-pvst*
* *spanning-tree vlan* <szám> *root primary/secondary*



## SSH

A Secure Shell (röviden: SSH) egy szabványcsalád, és egyben egy protokoll is, amit egy helyi és egy távoli számítógép közötti biztonságos csatorna kiépítésére fejlesztettek ki. Nyilvános kulcsú titkosítást használ a távoli számítógép hitelesítésére, és opcionálisan a távoli számítógép is hitelesítheti a felhasználót.

Az összes routeren és switchen 2-es verziójú SSH-t állítottunk be, 2048 bit hosszú kulccsal, felhasználónévvel és jelszóval.

### Parancsok

Először létrehozunk egy domain nevet.

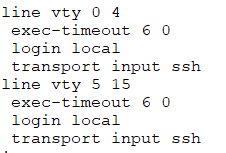
* *ip domain-name* <név>

Utána generálnunk kell egy crypto kulcsot.

* *crypto key generate rsa*

Majd megadjuk, hogy hány bites kulcs legyen. Utána létrehozunk egy felhasználónevet és egy jelszót és hozzáadjuk.

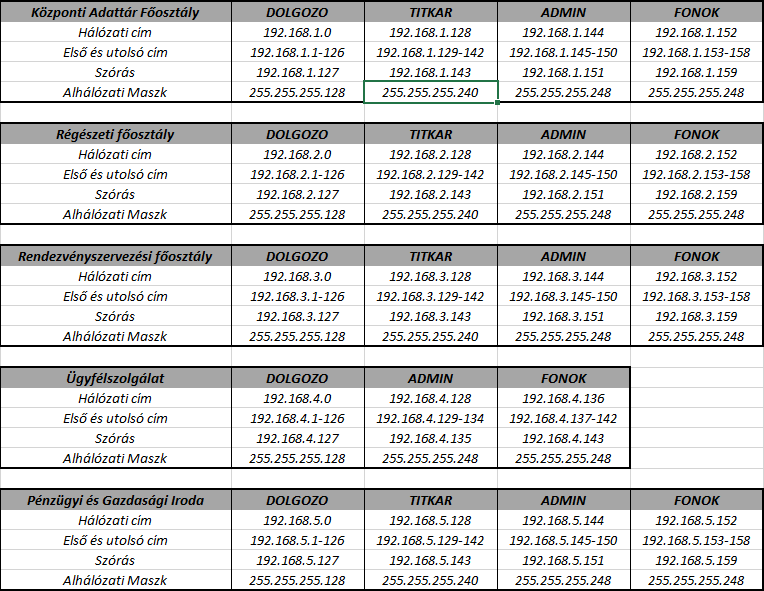
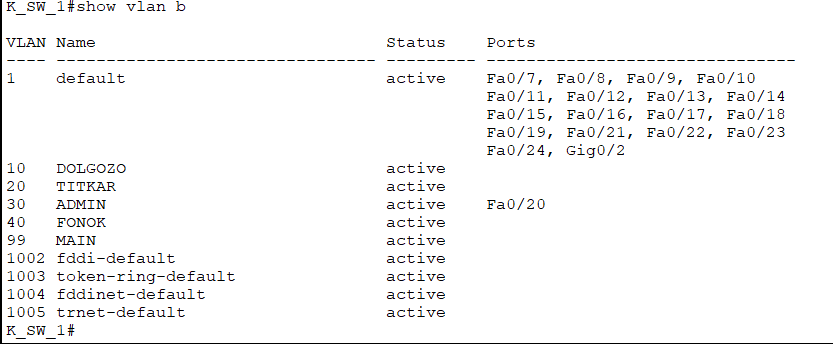
* *username* <név> *password* <jelszó>
* *line vty 0 15*
* *login local*



## VLAN

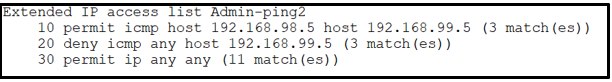
Hálózatunkban több helyen is kialakítottunk VLAN-okat a munkakörök számára, amikhez VLSM-mel számoltuk ki a megfelelő címtartományokat. VLAN-ok előnyei, hogy biztonságos, költségcsökkentő és a szórási tartományok is kisebbek.

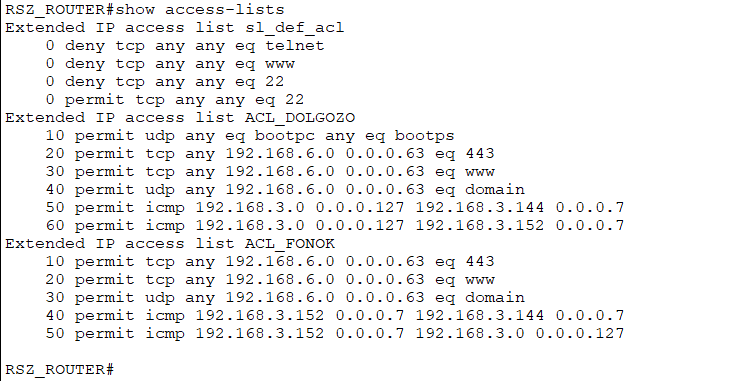
### Parancsok

* *vlan* <szám>
* *switchport mode access*
* *switchport access vlan* <szám>

## ACL

A hozzáférési jogosultság ellenőrzése (access control) valamilyen védett objektum, számítógép vagy számítógép-hálózat biztonságát szolgáló különböző védelmi eljárások összessége. Az informatikában a hozzáférési jogosultság feladata a számítógép erőforrásainak vagy magának a számítógépes hálózatnak a védelme illetéktelen felhasználástól. A hozzáférési jogosultság dönti el, hogy egy személynek, vagy egy a számítógépen futó eljárásnak (process) van-e lehetősége valamilyen objektum elérésére. Ez lehet egy fájl vagy valamilyen hardver eszköz stb.

Több ACL-t is alkalmaztunk hálózatunkon belül, mint pl. csak az adminok képesek a routerekhez és switchekhez való ssh elérést.



## NAT

A hálózati címfordítás (Network Address Translation) a címfordításra képes hálózati eszközök (pl. router) kiegészítő szolgáltatása, mely lehetővé teszi a belső hálózatra kötött gépek közvetlen kommunikációját tetszőleges protokollokon keresztül külső gépekkel anélkül, hogy azoknak saját nyilvános IP-címmel kellene rendelkezniük. A hálózati címfordító a belső gépekről érkező csomagokat az internetre továbbítás előtt úgy módosítja, hogy azok feladójaként saját magát tünteti fel, így az azokra érkező válaszcsomagok is hozzá kerülnek majd továbbításra, amiket – a célállomás címének módosítása után – a belső hálózaton elhelyezkedő eredeti feladó részére ad át.

Távmunkás résznél és a határ routernél (R3) PAT-ot (túlterheléses NAT-ot) alkalmaztunk.

### PAT

## Jelszó titkosítás

Minden eszközön be lett állítva privilegizált, vonali és konzoli jelszó, emellett egy üzenet fogad bejelentkezéskor, hogy illetékteleneknek tilos a belépés

Privilegizált jelszónál secret módba adtuk meg a jelszót, ami azt jelenti, hogy md5-tel van titkosítva így, ha valaki megnézi a konfigurációt szemmel nem értelmezhető jelszót fog találni. A második 2 helyen csak sima, nem titkosít jelszót tudunk megadni, de a service password-encryption parancs miatt titkosítja ezeket a jelszavakat is.



## WAN

Nagy kiterjedésű hálózat (Wide Area Network), ami két távoli területet kapcsol össze biztonságosan, pont-pont kapcsolati beágyazási módszerrel. Többféle protokollt támogat köztük a CHAP-et és PAP-et.

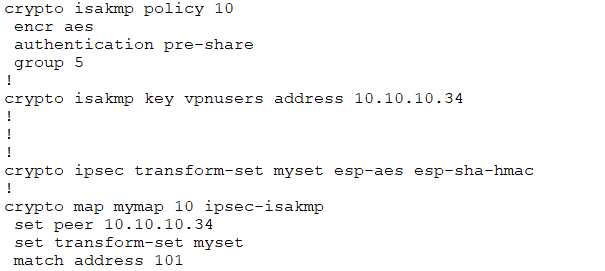
CHAP hitelesítést alkalmaztuk, hiszen biztonságosabb, megfigyeli a kapcsolatok minőségét és bármilyen típusú forgalomirányító eszközön támogatott.

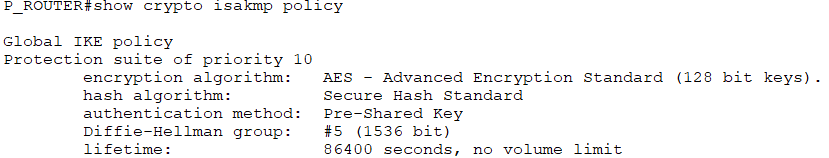
CHAP hitelesítés egy háromfázisú kézfogást használ és MD5-ös titkosítást. Előre meghatározott felhasználónév, jelszó párost hoztunk létre. Beállítás után titkos kulcsokat küldenek egymásnak a routerek.

## IPsec

Az **Internet Protocol Security** (**IPsec**) egy protokoll csomag az Internet Protokoll (IP) alapú kommunikáció biztonságosabbá tételére a kommunikációs viszony minden egyes csomagja hitelesítésével és titkosításával.

Az IPsec a hálózati rétegben működik, védi és hitelesíti az IP-csomagokat a résztvevő IPsec eszközök, más néven partnerek között. Az IPsec biztonságossá teszi az útvonalat két átjáró, két állomás, esetleg egy átjáró és egy állomás között.

A gerinchálózat és a pénztár között alkalmaztuk az IPsec-et a vásárlók adatai miatt.

Titkosításnál AES-t választottuk, integritásnál SHA. hiszen biztonságosabb, mint az MD5, hitelesítésnél pedig pre-share.

## ASA

A Cisco Adaptive Security Appliance (ASA) hardveres biztonsági tűzfalat használunk az MNM szerverek belüli részén, azon belül is a backup és az ftp szervernél.

### Policy-map

### Class-map

### Service-policy

### ACL

### Ip Route

Statikus forgalom irányítást alkalmaztunk a külső terület felől annak érdekében, hogy bárhonnan érkezhet a kérés a ftp szerver felé a kérés sikeres legyen

A belső admin gépünk DHCP-n keresztül kap IP címet az ASA-tól.

### SSH

Az ASA távoli kapcsolattal is elérhető, amelyet a belső admin képes elérni.

### VLAN

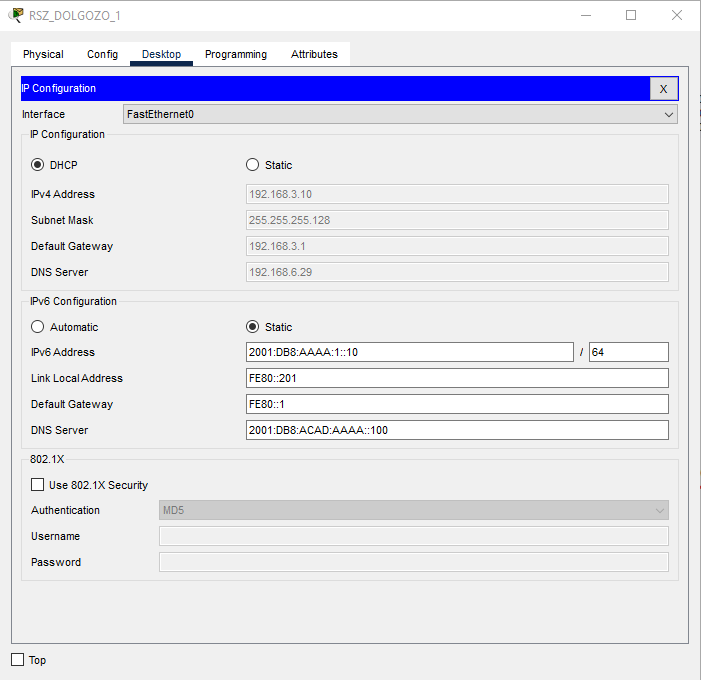
## IPv6

Az Internet Protocol version 6 (IPv6) az IPv4 utódja, amelyet arra terveztek, hogy az IPv4-es címzést leváltsa a kifogyóban lévő IPv4-es címek miatt, mivel míg az IPv4-el több mint 4 milliárd címzés lehetséges, az IPv6-os címzés több ezer milliárd eszköz számára biztosíthat IP-címet.

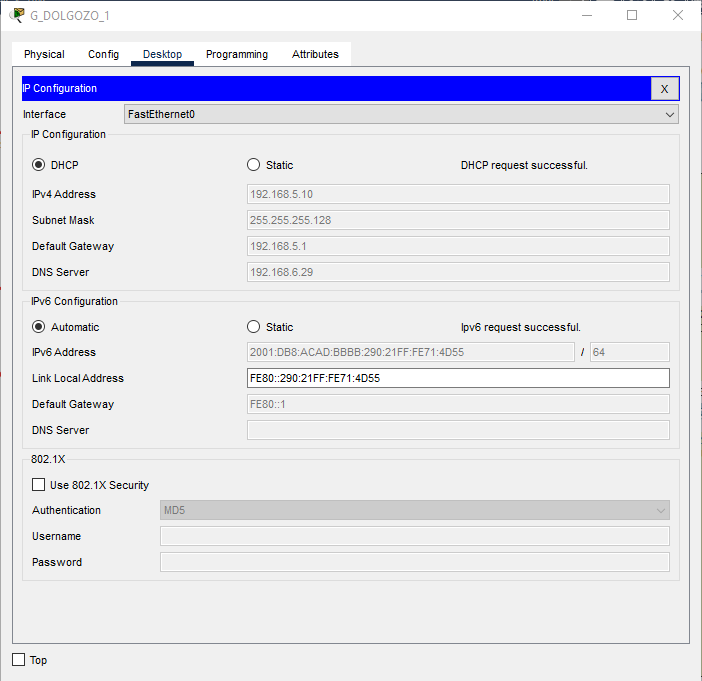
A Magyar Nemzeti Múzeum bizonyos részlegein, azaz a Pénzügyi és Gazdasági Irodában, a Rendezvényszervezési főosztályon, illetve a gerinchálózatban található IPv6-os címzés. A Múzeum IPv6-os címzésre szeretne átállni, viszont egyenlőre tesztelés alatt tart az átállás, ezért is található egyenlőre csak az előbb említett részlegeken IPv6-os címzés.

Az IPv6 címzést kétféleképen oldottuk meg, statikusan és dinamikusan (DHCPv6).

Statikusan a Rendezvényszervezési főosztályon található:



DHCPv6-tal kiadott címek a Pénzügyi és Gazdasági Irodában a dolgozók számára:



Ahhoz hogy az IPv6-os forgalomirányítás, illetve eleve az IPv6-os címek kiosztása lehetséges legyen, ki kellett adnunk minden IPv6-tal foglalkozó routeren a következő parancssort:



A IPv6-os forgalomirányítás EIGRP segítségével lett megoldva, ugyanúgy, mint az IPv4-es forgalomirányításnál, viszont hogy az eigrp 100 aktív legyen, a ki kell adnunk a no shutdown parancsot, máskülönben nem lehetséges a forgalomirányítás:

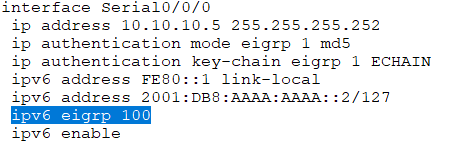
A képen szöveg, Betűtípus, fehér, képernyőkép látható

Automatikusan generált leírás

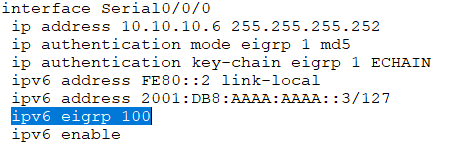
Az IPv4-es EIGRP-vel szemben, az IPv6-os EIGRP-n belül nem kell kiadnunk mely hálózatokat szeretnénk csatlakoztatni a forgalomirányításhoz, helyette az interface-en kiadjuk ip eigrp 100 parancsot.

Itt egy példa a gerinchálózatban lévő R1 és R2 routerek között:

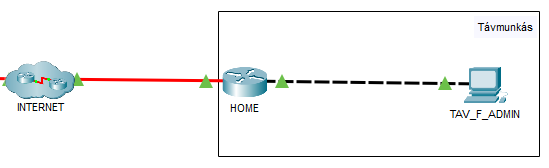
R1:



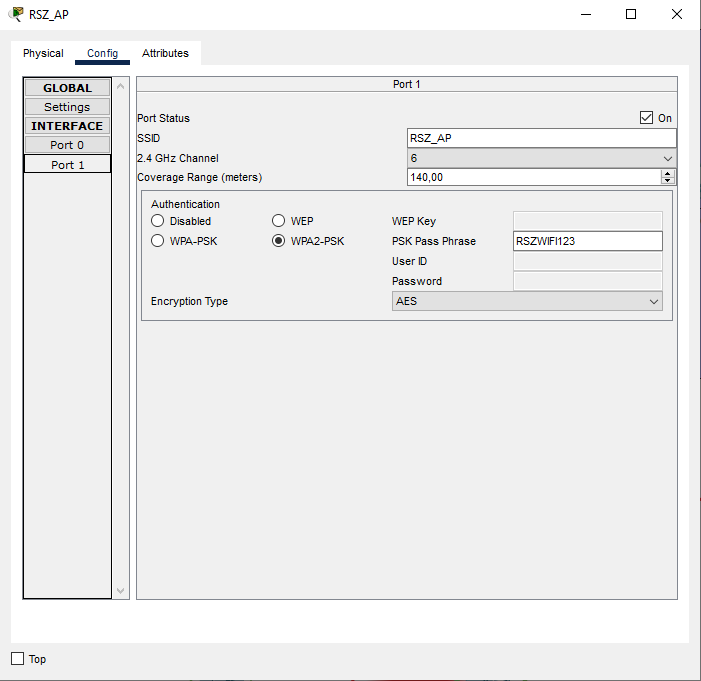
R2:

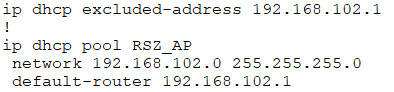


## Távmunkás

Ki lett alakítva egy távmunkás terület, így otthonról is képes dolgozni a távmunkás.

## Access Point

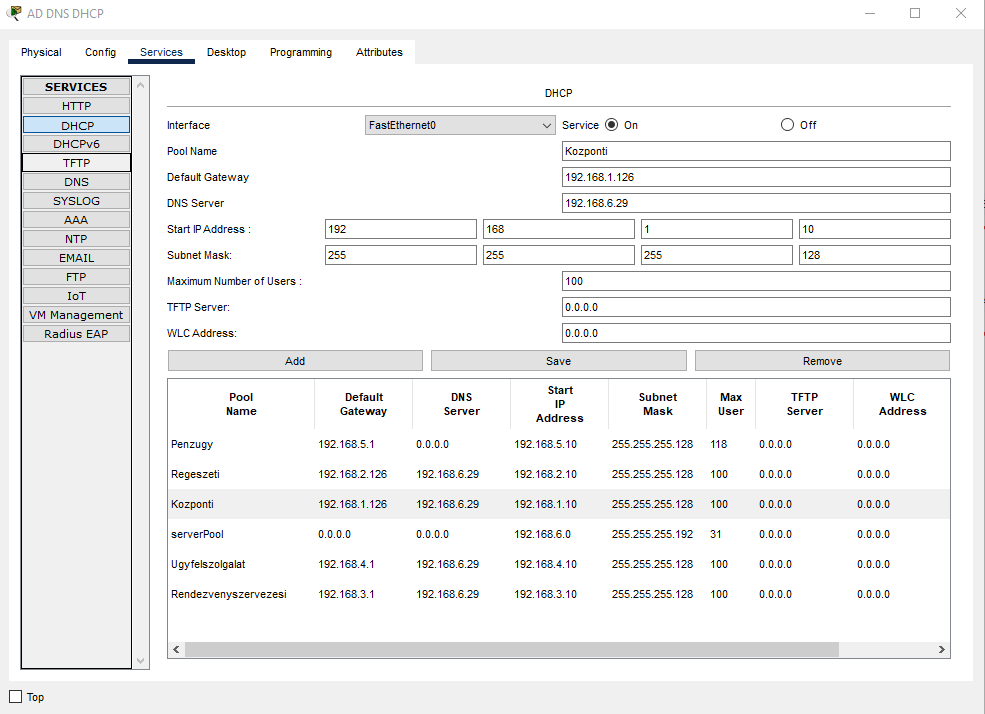
A rendezvényszervezési főosztálynál, gazdasági irodánál és a pénztárnál Access Point-okat helyeztünk el a vendégek számára, hogy vezeték nélkül is tudjanak csatlakozni a hálózathoz.

A routereken beállítottuk a dhcp működését, így az Access Point-ok képesek dinamikus ip címeket osztani az eszközöknek.

# Cisco Packet Tracer szerverek

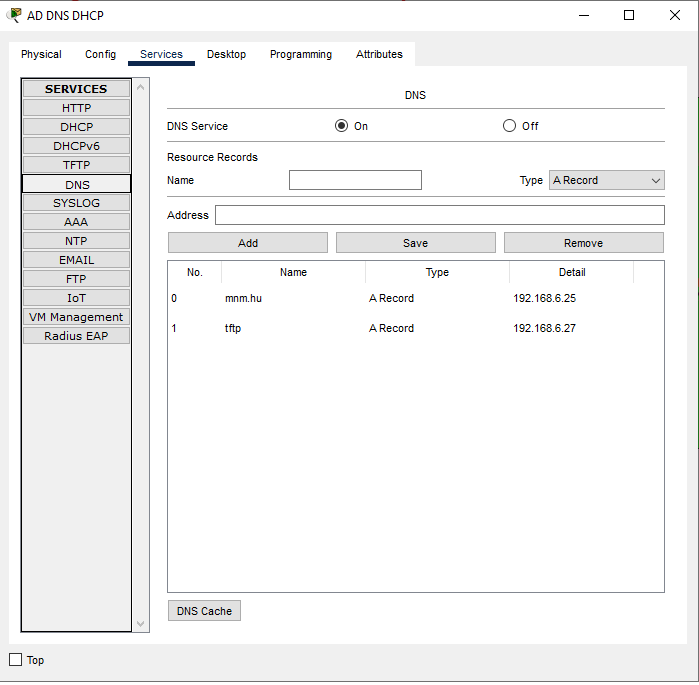
## DHCP

A dolgozók dinamikusan kapnak IPv4 címet a DHCP szervertől.

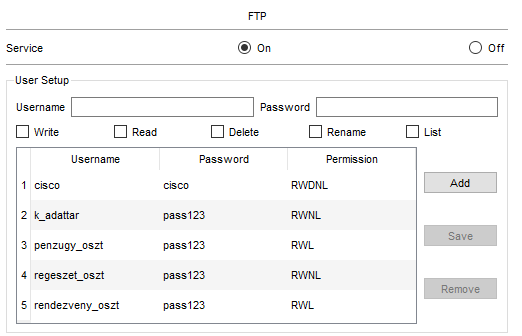


## DNS

A legtöbb szolgáltatásunk DNS-névvel van ellátva így a dolgozóknak nem kell tudniuk a fix ip címet. Így mindenkinek egyszerűbb és biztonságosabb.

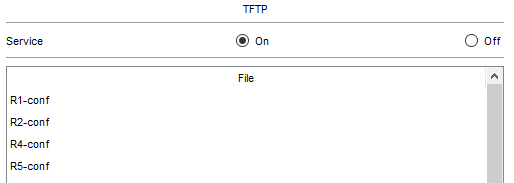


## FTP

Ki lett alakítva egy FTP szerver is, hogy gyorsan és biztonságos módon tudjanak fájlokat fel-le tölteni.

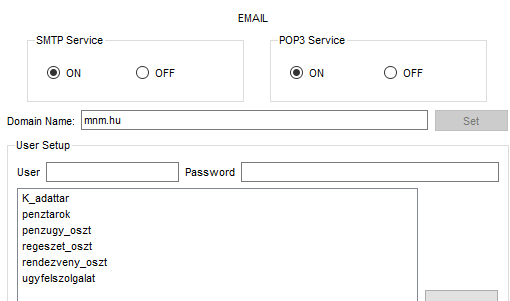
## TFTP

Naponta készítünk biztonsági mentést minden eszköz konfigurációjáról a szerverre így egy esetleges meghibásodás során azonnal vissza tudjuk tölteni a konfigurációkat.

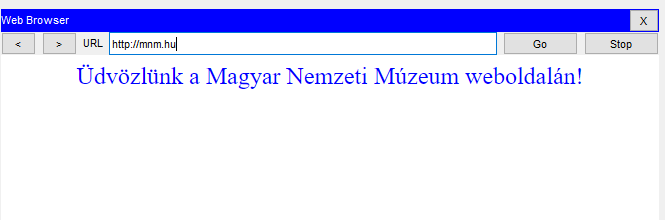


## EMAIL

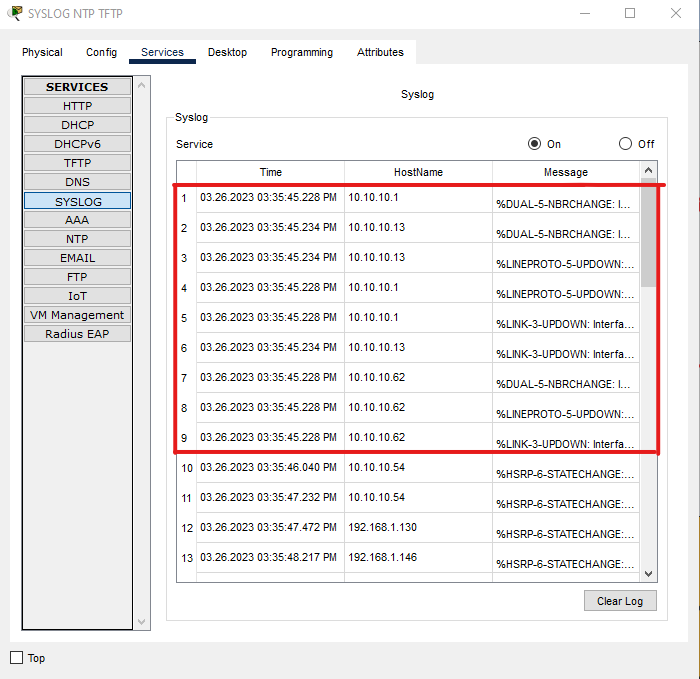
Saját belső levelező rendszert alakítottunk ki, mindenki saját felhasználónév és jelszó párossal rendelkezik, így minden dolgozó eléri a másikat.



## WEB

A Magyar Nemzeti Múzeum saját weboldallal is rendelkezik, amely az mnm.hu címen elérhető.

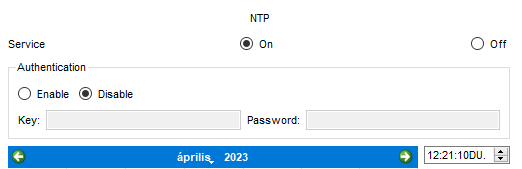
## SYSLOG

Az összes eszközünket monitorozzuk ezért minden egyes belépéskor egy üzenet érkezik a szerverre, ami a pontos dátum/időt mutat és hogy mit csináltak az adott eszközön, lekapcsoltak egy portot vagy átírtak egy ip címet.

## NTP

Az NTP szerver és a minden eszközökön beállított „*service timespan datetime msc*” parancs segítségével megjelenik a dátum-óra-perc-másodperc a syslog szerveren.





# Szerverek dokumentáció

## Szolgáltatások

### Active Directory

Az Active Directory egy Microsoft címtárszolgáltatás, tároló, amely adatobjektumokat tárol a helyi hálózati környezetben hierarchikus struktúrákban

### Domain Controller

A DC, magyarul tartományvezérlő autentikációs és autorizációs szolgáltatásokat nyújt tartományon belül

### Secondary Domain Controller

A fő Domain Controller meghibásodása során a másodlagos tartományvezérlő veszi át a szerepet, hogy a szolgáltatások továbbra is futhassanak.

### Dynamic Host Configuration Protocol

A DHCP egy olyan protokoll, amely automatikusan képes IP címeket osztani a végeszközöknek.

### Domain Name System

A DNS lényegében IP címekhez tartományneveket rendel hozzá, emiatt megkönnyíti a címalapú hozzáféréseket.

### DHCP Failover

A fő DHCP szolgáltató szerver leállása esetén átveszi a fő DHCP szerver szerepét.

### Print server

Hálózati nyomtatómegosztás, amit távolról is lehet működtetni.

### WEB szerver (IIS)

Elérhetővé teszi a weboldalakat http/HTTPS protokollon keresztül.

### File szerver

A felhasználok a belső hálózaton belül elerest kapnak egy közös, mindenki szamara látható es elérhető mappához ahova fileokat es adatokat tudnak feltölteni/letölteni es azt egymással megosztani. Emellett csak az administatoroknak elérhető privát mappa is rendelkezésre áll.

### Email szerver

Az IRedMail nevű szolgáltatást alkalmazzuk a felhasználok közötti levelező rendszer biztosítására.

### VPN

Egy virtuális privát hálózatot hoztunk létre, hogy növeljük a külső hálózat fele levő kommunikációnak a biztonságát azzal, hogy titkosítjük a VPN-en keresztül menő adatokat ezáltal nem láthatóak az eredeti hálózaton. Igy a távolról dolgozó munkasok biztonságosan férhetnek hozza a belső hálózathoz.

### Group Policy Object

A Group Policy Object segítségével tiltjuk a felhasználóknak a programok futtatását, a rendszer beállításának a módosításait es számos más jogkort ezáltal könnyen elkerülhető a kártékony programok futtatása vagy bármiféle idegen szoftver gépre kerülésé is.

**Windows server GUI**

* Hostname: winserver
* Adminstrator jelszó: Qwert123
* IP cím: 190.168.6.29
* Alhálózati maszk: 255.255.0.0
* Broadcast cím: 190.168.6.255
* Default gateway: 190.168.6.1
* Tartományi administator:
  + Felhasználó név: Adminstator
  + Jelszó: Qwert123
* Domain Controller
* Active Directory
  + adattarG (6 fo)
  + penztar (6 fo)
  + rendezvenyszervezi (6 fo)
  + ugyfelszolgalat (6 fo)
  + penzugy (6 fo)
* DNS
  + Forward Lookup zone:
    - Web.mnm.hu 190.168.6.29
    - [ftp.mnm.hu](ftp://ftp.mnm.hu) 190.169.6.29
    - Linuxmail.mnm.hu 190.168.6.51
  + Reverse Lookup zone:
    - Winserver.mnm.hu 190.168.6.29
    - Winserverbdc.mnm.hu 190.168.6.30
    - Linuxvp.mnm.hu 190.168.6.51
* DHCP
  + Address range: 190.168.6.100-190.168.6.150
  + Default gateway: 190.168.6.1
  + Leasing time: 2 nap
* Print szerver
* Webszerver
  + <https://mnm.hu> titkosított adatforgalom
* Fileserver
  + Közös 10Gb méretű mappa
  + Administatorok szamara létrehozott 10 Gb méretű mappa
* Ütemezett biztonsági mentes
* Group Policy beállítások
  + Egységes háttér minden eszközön
  + Letiltott programok (regedit,msc,cmd)
  + Programok távoli telepítése (Firefox)

**Linux Server (debian)**

* Hostname: Linuxserver
* Root jelszó: Qwert123
* IP cím: 190.168.6.51
* Alhálózati maszk: 255.255.255.0
* Broadcast cím: 190.168.6.255
* Default Gateway: 190.168.6.1
* OpenVPN
* IRedMail szolgáltatás
  + Minden AD-ben felvett felhasználó rendelkezik egy személyre szabott email címmel

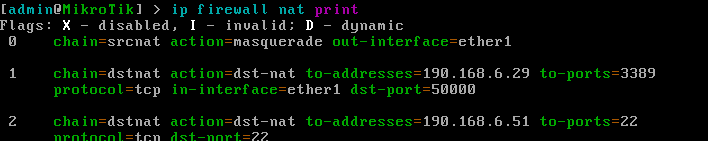
**Windows server GUI 2.**

* Hostname: winserverbdc
* IP cím: 190.168.6.30
* Alhálózati maszk: 255.255.255.0
* Broadcast cím: 190.168.6.255
* Default gateway: 190.168.6.1
* DHCP failover

**Windows Kliens**

* DHCP-n keresztül kap IP címet
* Hostname: winclient
* Jelszó: Qwert123
* RSAT

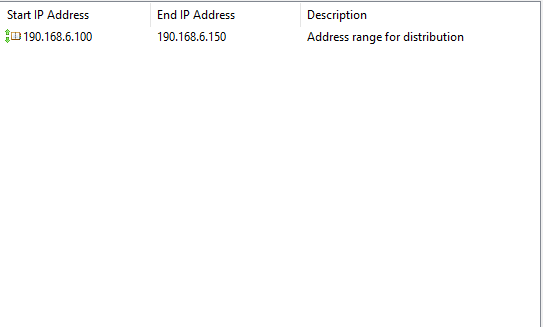
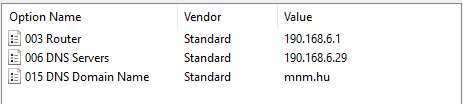
## Mikrotik



A távoli asztalkapcsolat es az ssh működéséhez szükséges parancsok

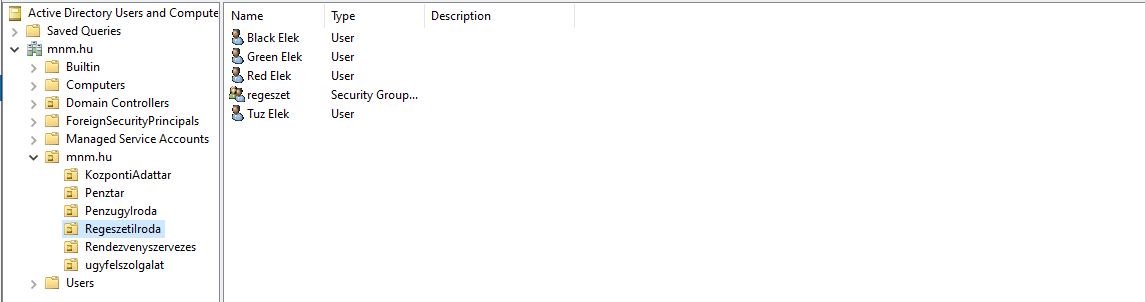
## AD DC DNS DHCP

### DHCP

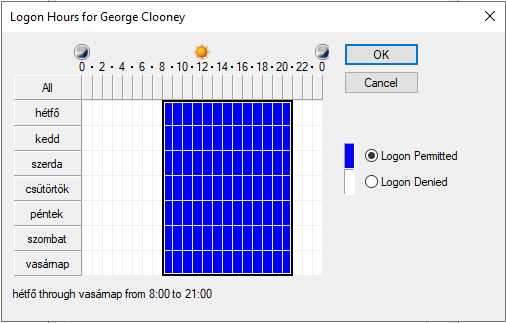


A szerver DHCP beállításai

### AD DC



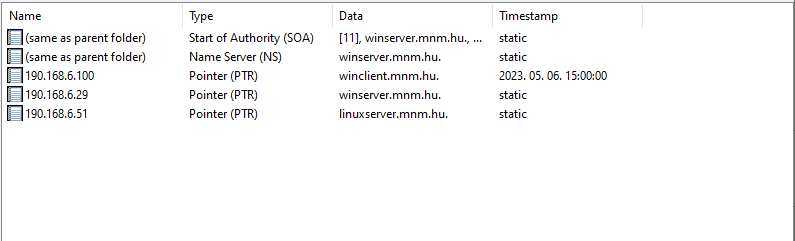
A felvett felhasználok es security groupok

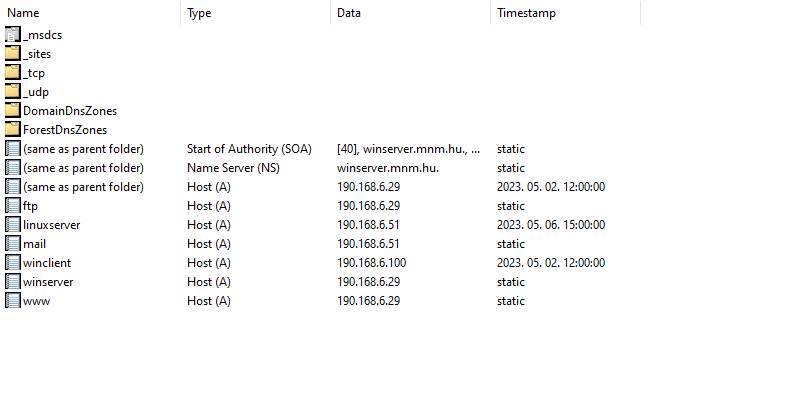


A felhasználóknak beállított bejelentkezési idő korlát

### 

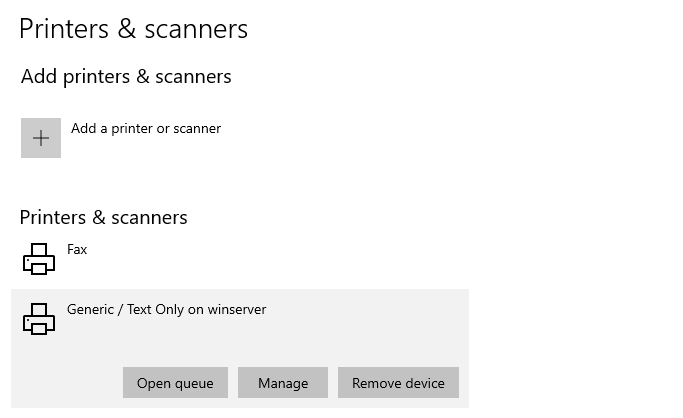
### DNS





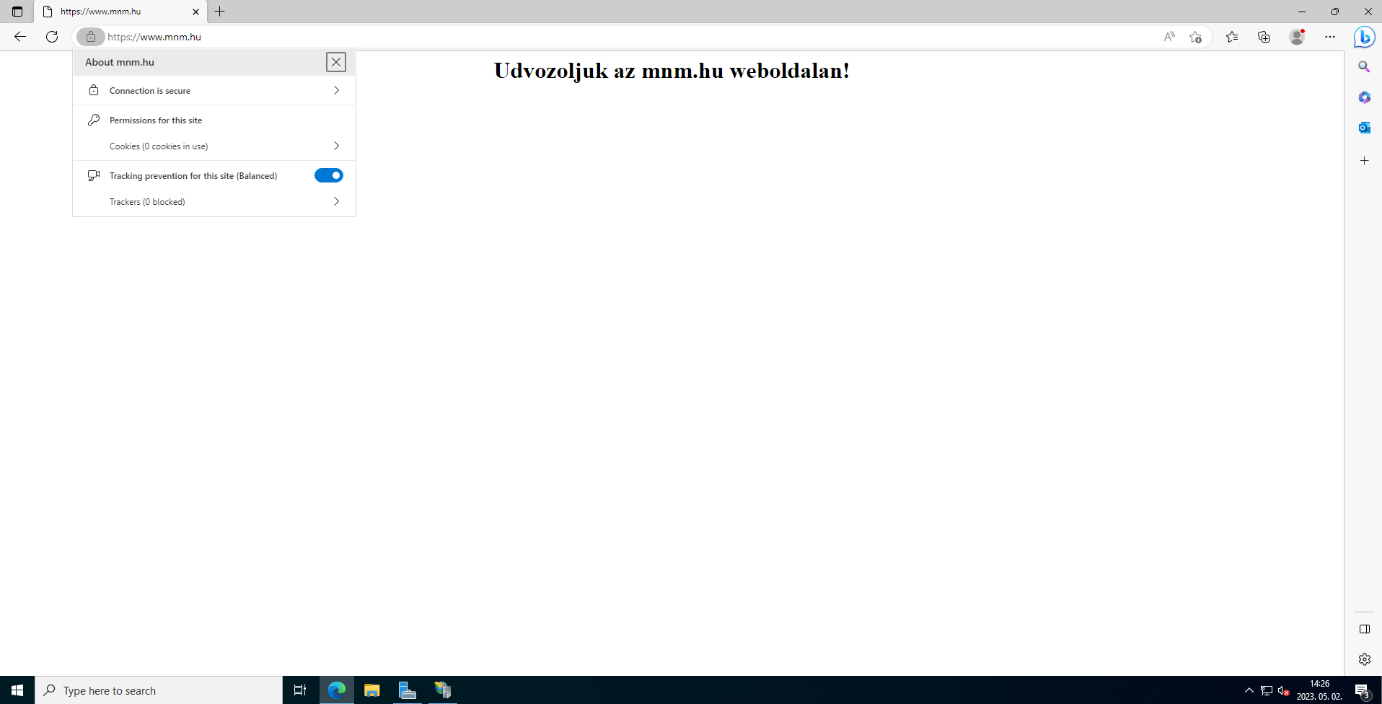
## MAIL FTP File Print

### File Print

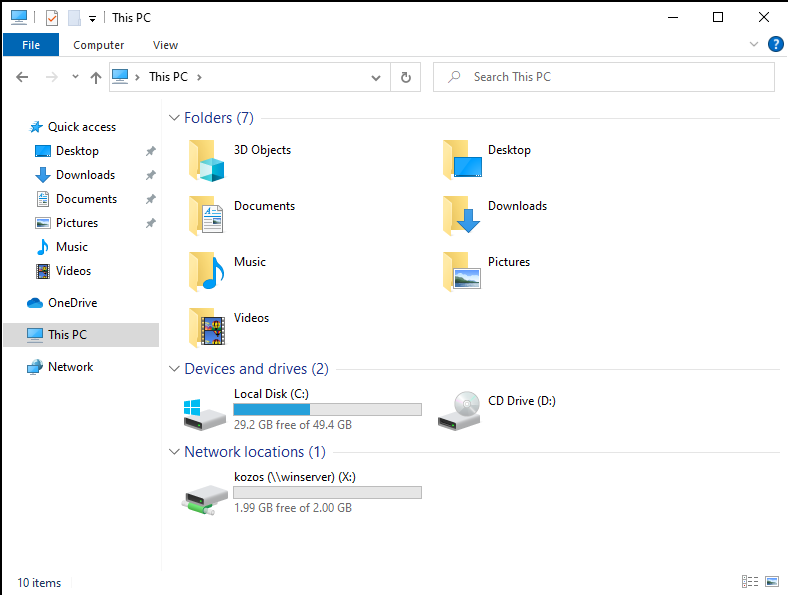


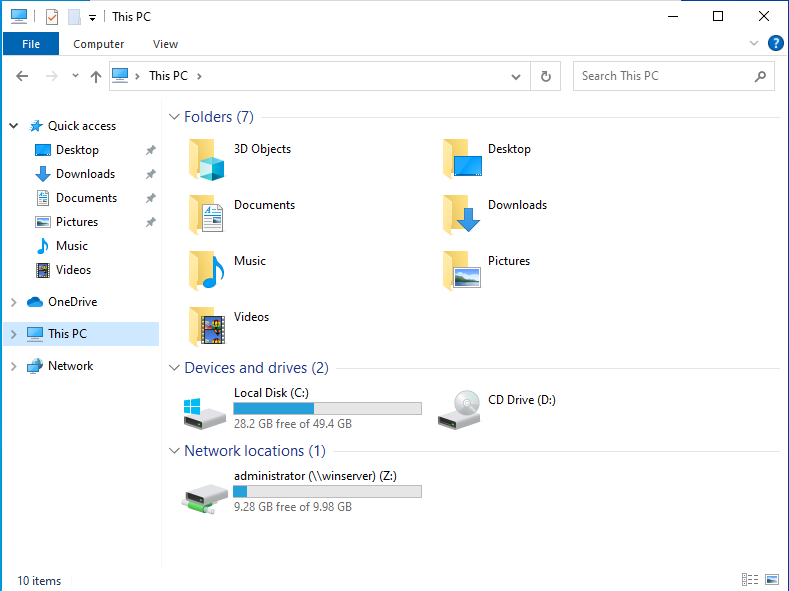
Print szervert eléri a kliens

### WEB

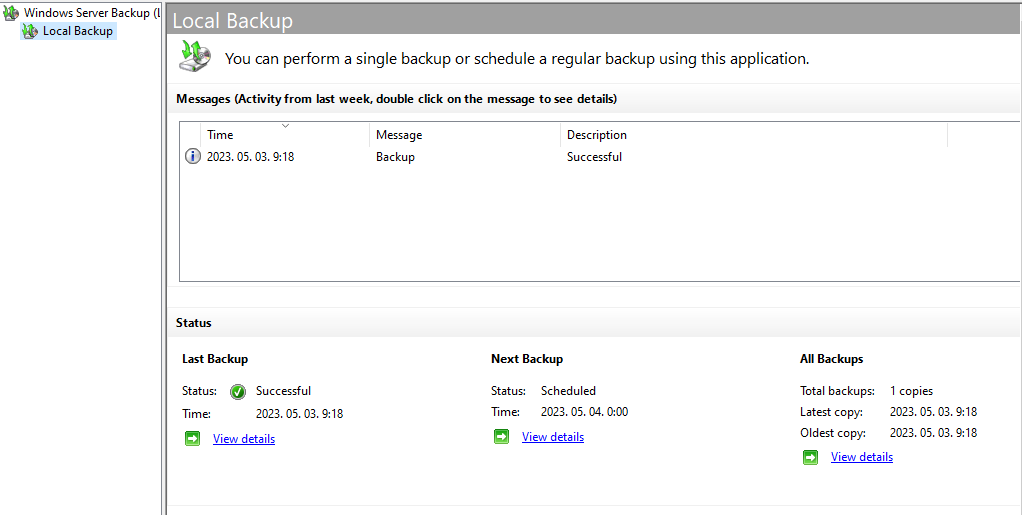


Weboldal biztonságos https kapcsolattal



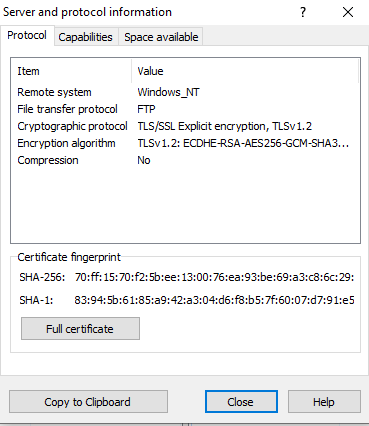
Közös mappa 2Gb feltöltési limittel

Csak az adminok szamara elérhető mappa 10Gb feltöltési limittel



Ütemezett biztonsági mentes

### FTP



Az ftp kapcsolathoz szükséges tanúsítvány

### MAIL

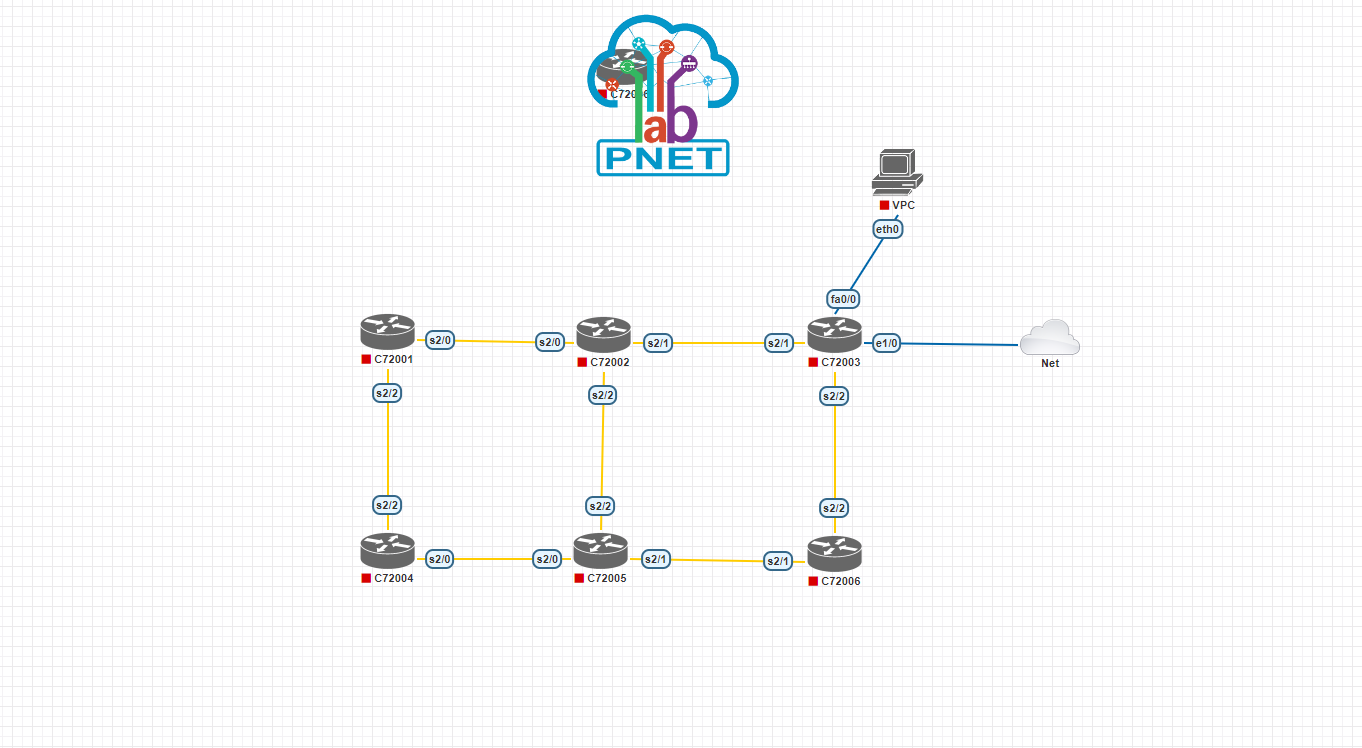
Sikeres email küldés két létrehozott felhasználói fiók között

# Hálózatprogramozás

## PNET

PNETLab (Packet Network Emulator Tool Lab) egy EVE-NG-n alapuló hálózat szimulációs program. A hálózatprogramozás részét ebben valósítottuk meg.

A program teszteléséhez felraktuk a gerinchálózatban található routereket.



## Python

A programot Python-ban írtuk meg. A program segítségével egyszerre tudjuk távolról elérni a routereket és megváltoztatni a privilegizált módhoz szükséges jelszót. A program működéséhez beimportáltuk a megfelelő modulokat. A routerek eléréséhez szükséges megadnunk a IP címet, felhasználónevet és a jelszót. Ezeket után belép a config módba, ahol ki fogja adni az általunk beírt jelszót és parancsot.

