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**

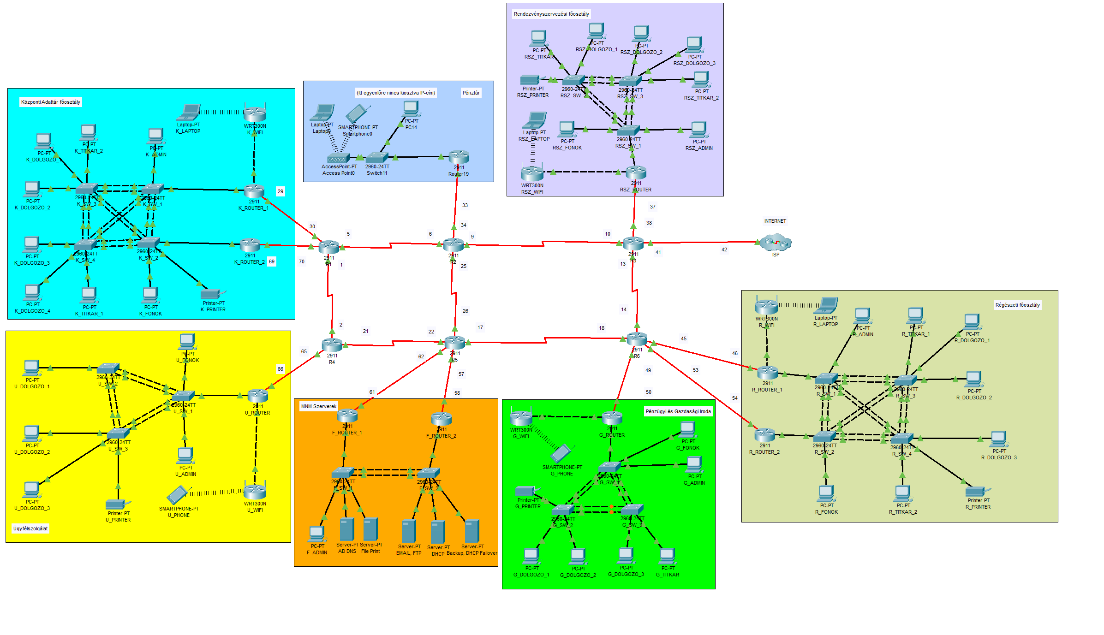
Jelenovszki Mihály, Király Ákos, Tankó Erik Péter  
2/14.B

Budapest, 2023.

# 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.

1. ábra A hálózat topológiája

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

- világos kék terület: Központi Adattár Főosztály

- halványzöld terület: Régészeti Főosztály

- lila terület: Rendezvényszervezési Főosztály

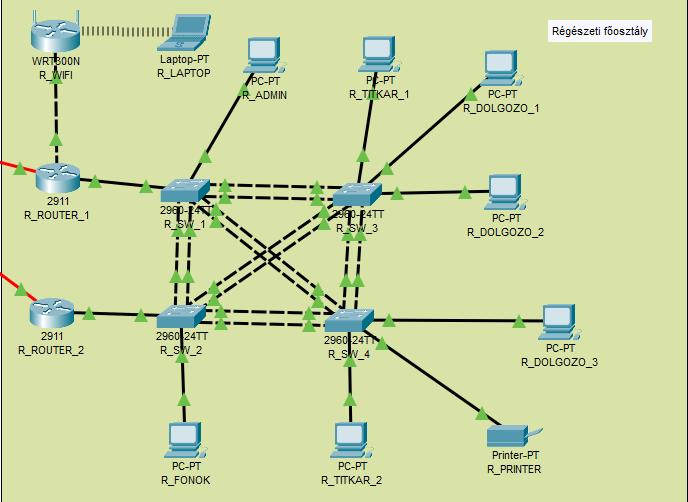
- sárga terület: Ügyfélszolgálat

- sötét kék terület: Pénztár

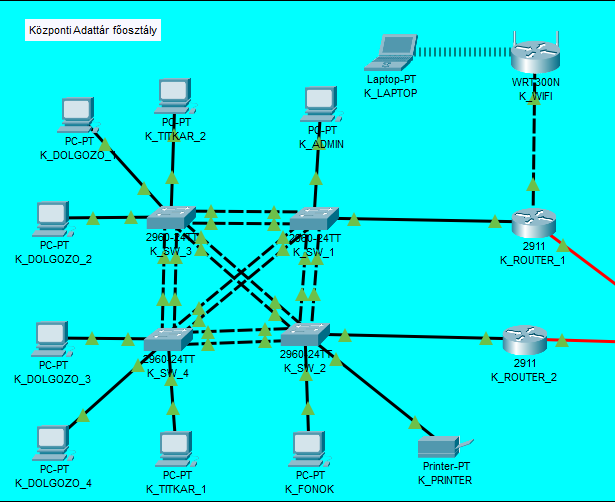
- narancssárga terület: MNM Szerverek

- zöld terület: Pénzügyi és Gazdasági Iroda

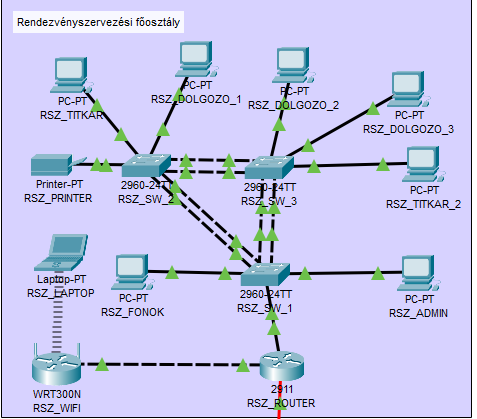
## Régészeti Főosztály

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

## Központi Adattár Főosztály

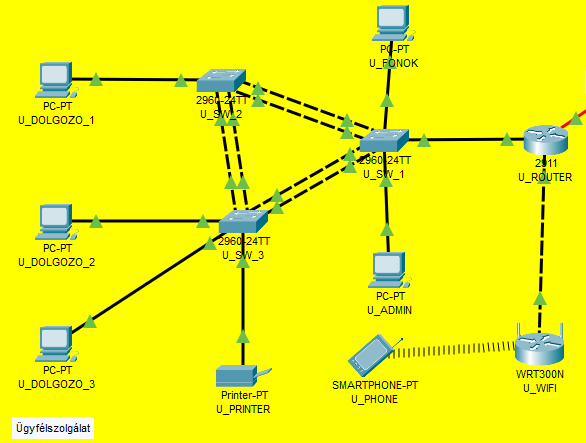
A Központi Adattár főosztály a Magyar Nemzeti Múzeum által bérelt irodában végzik napi feladataikat. Feladatuk a Régészeti főosztállyal való kapcsolattartás és az onnan kapott dokumentálásoknak, fotóknak, információknak a gyűjtése, megőrzése és feldolgozása.

## Rendezvényszervezési Főosztály

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

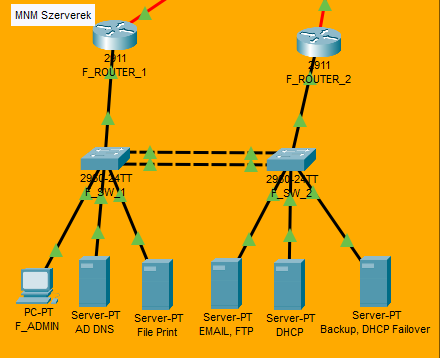
## Ügyfélszolgálat

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

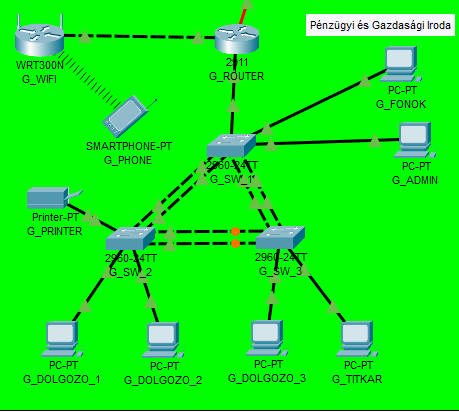


## MNM Szerverek

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



## Pénzügyi és Gazdasági Iroda



# 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 jelszó**t, 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.

Hálózatunkban használt protokollok:

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

## 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.

Úgy működik, hogy engedélyezi a megbízható forrásból érkező DHCP-kiszolgáló üzeneteket, mint például a DHCPOFFER és a DHCPACK. Ha a DHCP-kiszolgáló üzenetei nem megbízható portokról érkeznek, a DHCP-forgalmat elveti. A switch létrehoz egy DHCP Snooping Binding Database nevű táblát, amiben regisztrálja a nem megbízható porthoz csatlakozó gazdagépek forrás MAC-címét és IP-címét.

### Parancsok

Először be kell állítanunk az alábbi parancsot:

* *ip dhcp snooping*

Majd belépni az általunk megadott interfészekbe:

* *ip dhcp snooping trust*

## Port security

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

### Parancsok

Első sorban 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*

## 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.

## 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. Rosszab esetekben ezek a viharok és hurkok a hálózat leállásához is vezethetnek.

## SSH

## STP

## VLAN

# Cisco Packet Tracer szerverek

## DHCP

## DNS

## FTP

## TFTP

## EMAIL

## WEB

# Szerverek dokumentáció