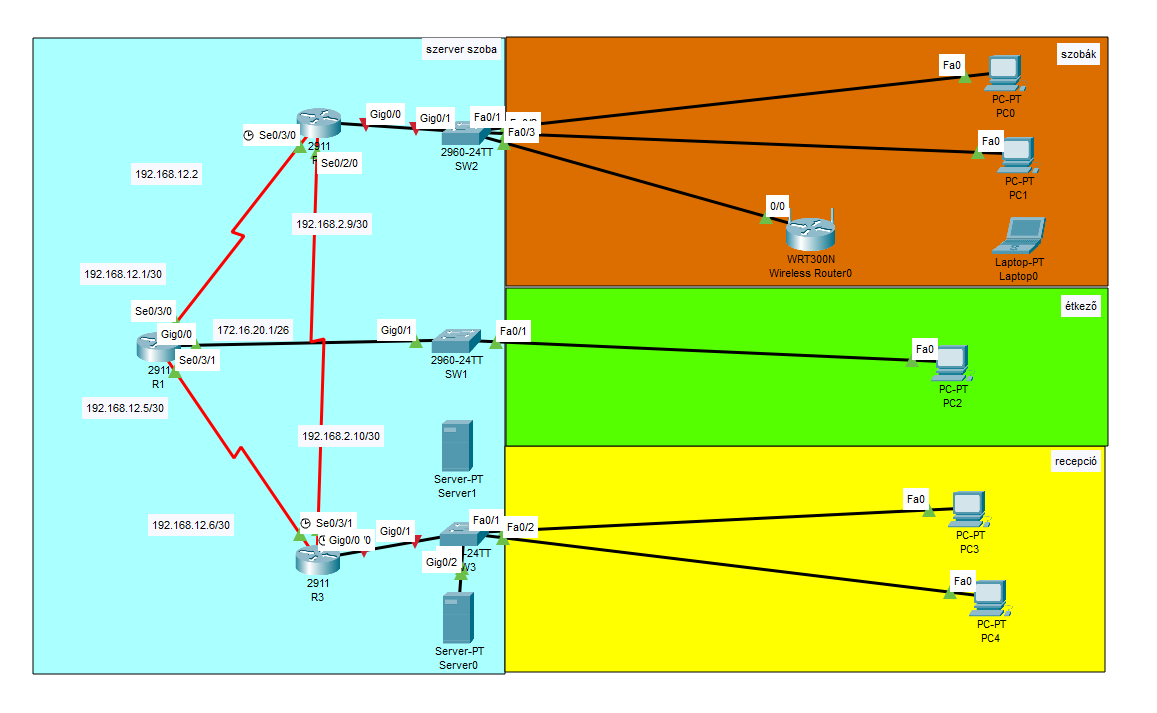
Vizsgaremek

Topográfia:Csapatunk egy képzeletbeli hotelt talált ki mely négy fő részre bontható. A hotelben található egy szerver szoba, hotel szobák az étkező valamint a recepció.

Szerver szoba:

A szerver szobában található a hotel összes hálózati eszköze. A szerverszobák olyan zárt terek, amelyek központi helyet biztosítanak a hálózati szerver erőforrásainak. Az ilyen szobák kulcsfontosságú szerepet játszanak az informatikai infrastruktúrában, különös figyelmet kell fordítani az eszközök hűtésére, az áramellátásra, a hálózati kapcsolatokra valamint a biztonságra. A mi hotelünk hálózata layer 3-as biztonsággal van ellátva. Ez lehetővé teszi azt ha a szálloda egyik routere meghibásodik akkor a másik két router segítségével akadálytalanul tovább tud működni a hálózat. A szerver szoba tartalmaz három routert, két switchet valamint egy windows szervert és egy linux szervert.

Hotel szobák:

A hotel szobák kaptak egy külön WRT300N névre hallgató vezetéknélküli routert melyhez egyéb informatikai eszközöket társítottunk számítógépek, laptopok, tabletek. Mindezeket hozzákötöttük a hotel szerverszobájához.

Étkező:

Az étkező nem igényel magához nagyobb informatikai struktúrát. Viszont a rendeléseket valahogy fel kell venni, így elhelyeztünk egy számítógépet az étkezőben is melyet csatlakoztattunk a hotel szerveréhez. Ez az egy számítógép hozzá van kötve egy 2960-24TT névre hallgató switchhez azon belül pedig a Vlan 10-hez van hozzárendelve a számítógép. A VLAN (Virtual Local Area Network) egy virtuális, logikailag elkülönített hálózati szegmens, amelyet egy fizikai hálózaton belül hoznak létre. A VLAN-ok között az adatforgalom alapértelmezetten nem látható. Az adatok szétválasztása csökkenti a biztonsági kockázatokat. Egyszerűvé teszi a hálózat átszervezését. Például egy VLAN-hoz tartozó eszközt fizikailag áthelyezhetünk, és a logikai tagságát megtarthatja.

Recepció:

A szálloda recepciójánál érkeznek be a szálloda foglalásai így oda is elhelyeztünk két számítógépet melyek szintén hozzá vannak rendelve a szálloda szerveréhez.

Parancsok amiket a switch beállításához használtunk:

**1. username admin password 1234**

1. Célja: Felhasználónév és jelszó létrehozása az eszköz eléréséhez.
2. Magyarázat:
   1. Egy admin nevű felhasználót hoz létre a 1234 jelszóval.
   2. Ezt a hitelesítést használhatják például SSH vagy Telnet hozzáféréshez.

**2. ip domain-name wmszki.hu**

1. Célja: A hálózati eszköz domain nevének beállítása.
2. Magyarázat: A domain név szükséges az SSH konfigurációhoz, mert a kulcsgenerálás során a rendszer ezt a nevet használja az eszköz azonosítására.

**3. enable secret cisco**

1. Célja: Egy titkosított jelszó beállítása az enable (privilegizált) módhoz.
2. Magyarázat:
   * A "cisco" lesz a privilegizált mód eléréséhez szükséges jelszó.

**4. line vty 0 15**

1. Célja: A virtuális terminálvonalak (VTY) konfigurációs módjának megnyitása.
2. Magyarázat:
   1. A 0 15 az eszközön elérhető összes VTY vonalat jelöli (általában 16 vonal).
   2. Ezeket a vonalakat távoli elérésre használják (pl. SSH vagy Telnet).

**5. login local**

1. Célja: Beállítja, hogy a VTY vonalakhoz történő hozzáféréshez a helyileg létrehozott felhasználói hitelesítés legyen szükséges.
2. Magyarázat: A felhasználónév és jelszó az előzőleg a username paranccsal létrehozott adatokból lesz ellenőrizve.

**6. transport input ssh**

1. Célja: Meghatározza, hogy a VTY vonalakhoz **csak** SSH protokollon keresztül lehessen hozzáférni.
2. Magyarázat: **Tiltja** a Telnet elérést, így biztonságosabbá teszi a távoli hozzáférést.

**7. password 1234**

1. Célja: Egy jelszó beállítása a vonalakhoz (például konzolhoz vagy VTY-hoz).
2. Magyarázat: Ez a jelszó lesz az alap hitelesítési adat, ha nincs login local használatban.

**8. crypto key generate rsa**

1. Célja: RSA kulcs generálása az SSH-hoz.
2. Magyarázat:
   1. Az SSH működéséhez szükséges titkosítási kulcsokat hozza létre.
   2. A parancs kiadása után meg kell adnod a kulcs hosszát (például 1024 vagy 2048 bit), amely meghatározza a biztonság erősségét.