# Script

## Hálózat

A Metropolitan Transportation Authority megbízására készült a tervezetünk. Mint a videóban is elhangzott az MTA a legnagyobb tömegközlekedést biztosító cég New York Metropolitan területén és így rendelkezniük kell egy megbízható redundáns hálózattal.

A cég a következő feladatokat szánta nekünk:

* A metro megállóknak a hálózatát megterverzni és konfiguráni valamint a megállókban az MTA-tól bérelt üzlethelységeknek biztosítani a hálózati szolgáltatást.
* A cég headquarters épületében a hálózat kiépítése az irodák, szerverszoba, admin szoba, kiadott üzlethelység figyelembe vételével. Vezeték nélküli hálózat kiépítése a dolgozók számára. A cég távoli szerverei és a headquarter épülete közötti VPN konfigurálása.
* A cég garázsának egyben metro, busz és vonat szerelő állomásnak a hálózatát megtervezni, hogy minden áron elérhető legyen a telephely mert fontos diagnosztikai adatokat küldenek az irodában dolgozó munkatársaiknak, ami alapján tudják kalkulálni az esetleges kimaradásokat és minél elöbb tájékoztatni erről az embereket.
* A cég távoli szervereinek a telepítése a Sziklás-hegységben és a szolgáltatások biztosítása.
* A távoli munkás kapcsolatának biztosítása.

A hálózat 5 telephelyből épül fel, ezek a Wallstreet metró megálló, az MTA irodaház, a Garázs és szerviz, a Szikláshegységi szerverterem, és a távmunkás. Ezek különböző logikai szegmensekre lettek felosztva funkció alapján. Példaként a Wallstreet-i telephelyben található jegyautómaták, beléptető rendszer, privát wifi, pékség és az admin szoba számára létrehozott vlan.

A vlanok könnyebb konfigurálásához vtp-t alkalmaztunk. A Wall\_St\_SW\_Main kapcsoló lett kinevezve vtp szervernek, a többi kapcsoló kliensnek van beállítva. Jelszóval van ellátva ami a „cisco”, a domain név pedig „cisco.com” és természetesen 2-es verzióval van felkonfigurálva.

Hogy megakadályozzuk az illetéktelen eszközök becsatlakozását a hálózatba, a kapcsolókon port security-t konfiguráltunk. A kapcsolók az első felcsatlakozó eszköz címét tanulják meg, ismeretlen eszköz esetén a shutdown mód értelmében a port lekapcsol. Minden használaton kívüli portot lekapcsoltunk, és külön vlan-ba raktuk így, ha valaki mégis felkapcsolná a portot nem fog tudni kommunikálni senkivel mert nincs beállítva a forgalomirányítás

A többi protokollt a továbbiakban Bence fogja ismertetni:

(Martin)

A Link Aggregation használatával a fizikai portokat összevontuk logikailag. Ez azért szerencsés, mert egyrészt növeli a sávszélességet úgy, hogy nem kell drágább kábelekre költeni és ha esetleg az egyik fizikai kábel kiesne, akkor a hálózat tovább tud működni a másik kábeleken.

Protokollnak az LACP-t választottuk, mert az LACP nem csak a Cisco-s, hanem bármelyik más gyártótól származó switch-et is elfogad. A port-channelek mindkét fele „active” módba lettek állítva.

Forgalomirányító protokollnak az EIGRP protokollt választottuk, mert ez egy „vegyes” protokoll, tartalmaz részeket a távolságvektor és a kapcsolatállapot alapú protokollokból is. A router-hirdetéseket nem periodikusan küldi, hanem csak akkor, amikor topológiai változás történik a hálózatban és ezeket a hirdetéseket nem az összes eszköznek küldi el, hanem csak azoknak, akik közvetlenül érintettek a változásban. Emiatt sokkal kevésbé terheli a hálózatot, mint egy OSPF és gyorsabban konvergál is.

A protokoll azonosító számának a 50-es számot választottuk, az automatikus útvonalösszevonást kikapcsoltuk és a forgalomirányító hirdeti az alapértelmezett kijáratot. Az alapértelmezett kijáratot statikus útvonal segítségével határoztuk meg.

(Bence)

És legvégül azért

Hogy megakadályozzuk a hurkok és szórási viharok létrejöttét STP protokollt konfiguráltunk. Az STP biztosítja, hogy bármely két eszköz között csak egy logikai útvonal létezzen, a többit pedig lezárja Az STP fajtákból a Rapid-PVST-t használjuk, mert ez az egyik leggyorsabban konvergáló. Sok erőforrást igényel, viszont a topológiába használt kapcsolók ezt bőven tudják futtatni. A Root Bridge-t úgy választottunk, hogy a Wall\_St\_SW\_Main switch legyen a Root Bridge. Ahhoz, hogy az STP zavartalanul működjön, több biztonsági funkciót is bevezettünk. Ez a kettő a PortFast és BPDU Guard

## Szerverek

A hálózat szerverei a Sziklás-hegységben lévő szerverszobában találhatók, így a szoba hűtésére nem kell külön költenie a cégnek, mert a 4000 méteres magasságban található szerverszoba az ottani hideg körülményeknek köszönhetően természetesen hűthető, hogy a szerverek ne hibásodjanak meg egy túlmelegedést követően. Ezzel egyhuzamban fizikai védelmet is biztosítunk a szervereknek, ha egy rossz indulatú alkalmazottja a cégnek netalán adatokat szeretne lopni vagy vírusokkal szeretné megfertőzni a szervereket először meg kéne találnia és bejutni a szerverszobába ami így körülbelül lehetetlen lenne.

Bence, kérlek fejtsd ki kicsit a szervereket

(Martin)

Az ADDS, DNS, DHCP, backup szolgaltatasokat egy windows alapú, amíg a WEB, FTP szolgáltatásokat pedíg egy linux alapú szerver biztosítja. Letreghoztunk felhasználókat amiket kulonboszo jogosultsagokkal rendelkezo security groupokba osztottunk, így a cég különböző osztályairól be tudnak lépni az active directoryba a megfelelő jogosultságaikkal. A felhasználók gépén autómatikusan települ egy firefox böngésző a beállított group policynak köszönhetően. Illetve a nap végén automatikusan készít egy biztonsági mentést a szerver. A windows szerveren található egy print szerver is, hogy az alkalmazottak tudjanak nyomtatni.

A web szerverhez azért választottunk docker-composet mert így könnyen skálázható a weboldalunk a késöbbiekben ugyanis nagy terheltségre számít a cég és ezzel a megoldással könnyen átvihető a web szolgáltatásunk docker swarm-ra. Ezzel a megoldással egyszerre több szerveren futtathatjuk a containereinket úgy mintha csak egyetlen szerveren futnának, akár futási időben növelhetjük a szerverek számát és a docker swarm gondoskodik a terhelés elosztásról.

(Bence)

## Angol

We were given the task of building a well functioning network for the Metropolitan Transportation Authority with multiple sites like the subway stations, the bakery and such. In order to complete this task we had to perform the following:

* Providing internet connection and layer 2 redundancy for the parlor and the network infrastructure at the subway station.
* Installing a network for the offices, the server room, the admin room, the parlor, and the reception inside the headquarter building of the company.
* Providing a private wireless internet access for the employees.
* Build a VPN connection between the HQ and the remote server farm therefore merging the two routing areas into one.
* Designing the network with layer 3 redundancy for the garage/repair station so it may be available at all times, because it is crucial to send diagnostic data to their colleagues at HQ which may be used to calculate and notify the passengers of the down time of transportation vehicles.
* Installing the remote servers in the Rocky Mountains and configuring the services on them.
* Ensure the connection of the remote worker.

To develop the network we have used Cisco Packet Tracer it consists of 5 sites:

* Wall Street Subway Station
* MTA Headquarters
* Garage/Repair Station
* Rocky Mountains Server Room
* Remote Worker

(Bence)

The yellow site represents the subway stations, given the minimal difference between each station it is sufficient to present only one. This area just like all the others is divided into multiple VLAN’s.

The green site represents the Headquarters where the employees mainly perform office work with computers. The building has two levels, on the first floor the lower ranked employees, on the second the higher ones.

The pink site is where diagnostics data is processed, and maintenance is performed on vehicles.

We store our main servers in the Rocky Mountains, the servers use a lot of power, thus generating high heat, there is also need for power to operate the cooling for these systems, the chill air of the mountain side offers a great help in managing cooling

We developed the remote worker site for the employee who works from their home, this site does not feature VLANs, we have provided a cable modem, a switch, and pc for them.

(Martin)