Márk - Vanyek - Zoli

# Bevezetés

Üdvözlök mindenkit! A mai előadásban bemutatásra kerül a LinkWave Solutions által üzemeltetett, Magyarországon fővárosának belvárosában elhelyezkedő Hotel, Motel és az ezekhez tartozó kávézó. A csoport tagjai Görhöny Márk, Vanyek Máté és Vigh Zoltán, akik a hálózat kialakításáért, zavartalan működéséért felelnek.

A mai bemutatóban körbejárjuk a topológia egyes részeit, felépítésüket, működésüket.

A kivetített packet tracer állományban látható a kiépített hálózatban megtalálható Hotel, Kávézó, Motel és az Üzemeltetők irodájának topológiája. Emellett megtalálható egy otthoni dolgozó is.

A hálózat biztonságos és zökkenőmentes működéséért második- és harmadik rétegbeli megoldásokat alkalmaztunk, melyeket ilyen sorrendben fogunk bemutatni.

# VLANOK

A VLAN (Virtuális LAN-ok) egy olyan hálózati tervezési és konfigurációs elrendezés, amely lehetővé teszi, hogy egy fizikai hálózatot virtuális csoportokra osszunk, mintha különálló hálózatok lennének. Ez a hálózat könnyebb kezelését, skálázhatóságát és biztonságát biztosítja. Hálózatunkban több helyen is alkalmaztunk VLAN-okat, a megfelelő biztonság és hatékonyság érdekében.

A kávézóban a VLAN 10, 20 és 30-as, míg a Hotelben a VLAN 11, 12, 20, 22, 31 hálózatot találhatjuk meg. A Hotel VLAN rendszere könnyen értelmezhető. Az első számból kiolvashatjuk, hogy melyik emeleten helyezkedik el, a második pedig egyszerűen a helyiségek elkülönítése miatt lényeges.

*RECEPCIO\_S:* #show vlan brief

*EBED\_S:* #show vlan brief

# VTP

Ezek zavartalan működése érdekében VTP protokollt alkalmaztunk a switchek között, amely a következőt jelenti pontosabban:

A VLAN Trunking Protocol (VTP) egy olyan szabványosított hálózati protokoll, amelyet a Cisco rendszerek használnak a Virtuális LAN-ok (VLAN-ok) konfigurációjának automatikus terjesztésére és karbantartására egy Ethernet hálózaton belül. A VTP célja a hálózati adminisztráció egyszerűsítése és a konzisztencia biztosítása a VLAN konfigurációk között.

A VTP segítségével a hálózati eszközök, például kapcsolók, automatikusan cserélik és frissítik a VLAN információkat. Ez azt jelenti, hogy ha egy VLAN-t egy kapcsolón hoznak létre, módosítanak vagy törölnek, a változások automatikusan más kapcsolókon is végrehajtódnak, így egy egységes VLAN konfigurációt biztosítva a teljes hálózaton.

A VTP egy trunk nevű kapcsolóporton keresztül kommunikál. A trunk portok olyan Ethernet portok, amelyeken több VLAN forgalom is áthaladhat. A VTP üzeneteket a hálózati eszközök küldik és fogadják a trunk portokon keresztül, és ezek az üzenetek tartalmazzák a VLAN konfigurációs információkat. Fontos megjegyezni, hogy a VTP csak Cisco eszközök között működik, és nem interoperál más gyártók hálózati eszközeivel, amelyek más VLAN kezelési protokollokat használnak.

RECEPCIO\_S:#show vtp status

EBED\_S:#show vtp status (vtp version 2 -> 1 teszt kedvéért)

# Portsecurity

A hotel és a kávézó switchein a biztonság érdekében portbiztonság beállításokat állítottunk be. A nem használt portokat lekapcsoltuk. Portonként egyetlen mac-address jogosult hozzáférni a hálózathoz. Emellett, ha megszegi valaki a feltételeket, a port megszakítja az adatátvitelt, és egy notepad logban kijelzi a megsértés körülményeit.

Show parancsok: show port-security

# Ether channel

A Hotelben és a kávézóban a switcheken portösszefogást alkalmaztunk PAgP protokoll (Port Aggregation Protocol) segítségével. Ennek célja nagyobb sávszélesség elérése és redundancia biztosítása. A PagP egy Cisco által fejlesztett protokoll, az általuk támogatott eszközök között működik és segít egyszerűsíteni az Etherchannel konfigurációját, karbantartását. Fontos megjegyezni, hogy az IEEE is szabványosított egy hasonló technológiát, melyet LACP-nak (Link Aggregation Control Protocol) neveznek. Ez egy nyílt szabványú protokoll és nem csak Cisco eszközökkel, hanem más gyártók hálózati eszközeivel is kompatibilis. A két protokoll közötti választás a környezettől és az alkalmazott eszközök típusától függ.

show parancsok: show etherchannel summary

# ASA

Tűzfalat raktunk az üzemeltetők területhez, ahova külső eszközök a beállításunk miatt csak a szervereket tudják megpingelni vagy a szerverek szolgáltatásait igénybe venni. Más forgalmat be nem engedünk vele, csak a válasz csomagokat. A tűzfalak persze még jók számos más dologra, például NAT beállításra vagy VLAN-ok kezelésére, de akár az IPS felől érkező csomagok átellenőrzésére, esetekben letiltására.

# **Spanning tree**

Spanning tree protokollt állítottunk be a New York hotel terület switchei közt és a kávéház switchei között. Megakadályozza, hogy ne legyen üzenetszórási vihar, ha egymással kommunikálnának az eszközök. A hálózatban kiválaszt egy gyökérponti hidat, amelyhez minden switch egy útvonalon csatlakozik, a többi switch portjai közül néhányat lezár, hogy azok ne továbbítsanak forgalmat, de ha egy útvonal meghibásodik, akkor automatikusan átkapcsolja a forgalmat egy másik útvonalra.

Show spanning-tree interface

Show spanning-tree summary

SOHO

A soho routeren beállíthatunk különböző hálózatokat, gondolok itt a privát, akár jelszóval elzárható hálózatra, vagy a guest hálózatra amire akár időkorlátot és sebességi korlátot is rakhat az ember, különböző titkosításokkal. Ezekből a routerekből raktunk le hármat a hálózatban, 1-et a motelbe és 2-t a kávéházba. Mindegyik routeren a hálózathoz megfelelő SSID-t állítottunk be annak érdekében, hogy a vendégek könnyen megtalálhassák azt, és ezeket a hálózatok WPA2-PSK AES jelszó titkosítóval láttuk el. A PSK kapcsolat megtartásához egy eszköznek meg kell ismernie egy dinamikus kulcsot, amelyet a hálózat generál és ezzel együtt küldi csak titkosítva a csomagokat az adott eszközökre.

IP Phone

Állítottunk be IP telefonokat a Laguna motelbe, hogy a vendégek tudják a recepciót hívni, ha bármilyen kérdésük van. Működésük gyakorlatilag ahogy a nevében benne van, IP címen keresztül kapnak kapcsolatot a hálózaton belül, így kommunikálva egymással.

# **DHCP**

Dinamikusan ip címeket a New York területen osztunk, mely segít az új eszközök beállításában a hálózatban, hiszen elég rácsatlakozniuk a hálózatra és a megfelelő helyről és a megfelelő VLAN ip tartományból már kap is IP-címet, illetve takarékoskodik az IP címekkel, mert csak akkor használ egy ip-t egy adott PC amikor hozzá van csatlakozva. Emellett az üzemeltetők és a Laguna motel dinamikusan kapnak IPv6 címeket. Ezek mellett a SOHO routereken is DHCP-vel osztjuk az IP címeket a hostok számára.

# SSH

A megfelelő és gyors karbantartás érdekében kialakítottunk SSH kapcsolatot a központi routereken. Hogy mi az az SSH és miért jó nekünk? Az SSH a **Secure Shell** (**biztonságos parancsértelmező)** rövidítése. Ez egy hálózati protokoll, ami titkosított csatornát hoz létre két számítógép között, amely a 22-es TCP porton fut és lehetővé teszi a **biztonságos kommunikációt még a nem biztonságos hálózaton** keresztül is. Működése egyszerű alapokra épül. Az SSH **titkosítási technikákat** alkalmaz a kommunikáció védelme érdekében. A számítógép és a router először egy **kulcscserét** hajt végre, amely során titkos kulcsokat hoznak létre a kommunikáció titkosításához. A kulcscsere után a két eszköz titkosított formában kommunikál egymással. Esetünkben 1024 karakter hosszú kulcsot hoztunk létre, 2-es verziójú SSH-val a nagyobb biztonság miatt.

SSH teszt:üzemről vmelyik routerre

# SYSLOG/NTP

Mindezen felül a további monitorozás érdekében üzemeltetünk egy SYSLOG szervert, amely naplóüzeneteket gyűjt össze a hálózaton lévő eszközökről. A Syslog kliensek (jelenesetben a routerek) naplóüzeneteket küldenek a szerverünknek a SYSLOG protokoll segítségével. A szerver tárolja a naplóüzeneteket, és szükség esetén továbbítja őket más rendszereknek, például egy SIEM (Security Information and Event Management) rendszernek.

Ezzel párhuzamosan működik az NTP szerverünk, amely pontos időt biztosít a hálózaton lévő számítógépek számára. Ez egy hierarchikus rendszert használ a pontos idő biztosításához. A hierarchia legfelső szintjén az atomórák találhatók, amelyek a legpontosabb időforrások. A hierarchia következő szintjén az NTP szerverek találhatók, amelyek szinkronizálják óráikat az atomórákkal. A hierarchia alsó szintjén a hálózaton lévő számítógépek találhatók, amelyek szinkronizálják óráikat az NTP szerverünkkel, amit az NTP protokoll segítségével visznek véghez.

SYSLOG bemutatás:routeren vmi updatet kiadunk, majd a szerveren megmutatjuk

NTP bemutatás: #show ntp associations

# HSRP

A New York hotel területén HSRP protokollt alkalmaztunk magasabb szintű hálózati elérhetőség érdekében, az IPv4 alapértelmezett átjárót használó állomások számára ad első ugrás forgalomirányító redundanciát. A HSRP a forgalomirányítók egy csoportjából választ ki aktív és készenléti eszközt. Az aktív eszköz végzi a csomagok továbbítását, a készenléti vagy tartalék eszköz pedig, megfelelő feltételek teljesülése esetén, átveszi a kiesett aktív eszköz szerepét. A HSRP tartalék forgalomirányítójának feladata figyelni a HSRP-csoport működését és gyorsan átvenni a csomagtovábbítás feladatát az aktív eszköz hibájakor.

Show: show standby

# CHAP(PPP)

A központi routereink között PPP kapcsolatot és CHAP hitelesítést is konfiguráltunk a nagyobb biztonság érdekében. A PPP (Point-to-Point Protocol) eredetileg a pont-pont kapcsolatokon továbbított IPv4 forgalom számára jött létre beágyazási protokollként. A PPP használatának számos előnye van többek között az is, hogy a protokoll nincs gyártói tulajdonban. Számos olyan jellemzővel bír, amelyekkel a HDLC nem rendelkezik, például ügyel a kapcsolat minőségére, túl sok hiba esetén a PPP leállítja a kapcsolatot. Emellett a PPP támogatja a PAP és a CHAP hitelesítést is, melyekből az utóbbit konfiguráltuk a hálózatunkba, mivel nagyobb biztonságot nyújt. A PAP hitelesítés létrejötte után nincs szükség az újbóli azonosításra. Ezáltal a hálózat sebezhetővé válik a támadásokkal szemben. Az egyszeri hitelesítést végző PAP protokollal ellentétben a CHAP ismétlődő kihívásokat intézve ellenőrzi, hogy a távoli állomás valóban érvényes jelszót ismer-e. A jelszó értéke változó, és az összeköttetés fennállása alatt előre nem megjósolhatóan módosul.

Show: show interface

OSPF

OSPF-et állítottunk be a 4 fő router között, a terület elválasztó routerjeink között, ezzel biztosítva, hogy a hálózatot dinamikusan és gyorsan megismerik egymástól, plusz saját magunk munkájának gyorsításának érdekében. Az OSPF link-állapotú útválasztási protokoll, amelyet kis- és közepes méretű hálózatokhoz terveztek így számunkra megfelelő protokoll. A hálózatokat területekre osztja fel, amik lehetővé teszik a hálózat adminisztratív felosztását, és segítenek megvédeni a hálózatot a rosszindulatú támadásoktól. Egyik legfőbb eleme a 10 másodpercenként küldött „hello-csomagok”, ami a hálózat linkjeinek állapotáról ad visszajelzést. Ezek után összegyűjtik ezeket az üzeneteket, és létrehoznak egy táblázatot a hálózat linkjeiről és azok állapotáról, majd ezt a táblázatot használják a forgalom továbbítására. Ezek mellett OSPFv3-at is állítottunk be a Laguna motel és üzemeltetők terület között, ahol használunk ipv6 címeket is, de erről majd később Máté beszélne.

show ip ospf interface

show ip ospf neighbour

# GRE

A topológián, állítottunk be GRE (Generic Routing Encapsulation) alagutat is. A protokollban a beágyazott csomagok egy GRE fejlécet kapnak, amely tartalmazza a forrás, a cél és az alagút típusát. Amint ez a GRE fejléc megérkezik a forráshoz, az információkat a rendeltetési helyére továbbítja és a fejlécet törli. Az üzemeltetők router és a kávézó router között egy virtuális alagutat hoztunk így létre, amellyel, ha nincsenek is egy hálózatba, akkor is azt érzékelik mintha egy lenne, de ehhez az kell, hogy a fizikai interface-en össze legyenek kötve és át tudjon menni a csomag. Az alagutak segítségével olyan protokollok adatait tudjuk szállítani két forgalomirányító között, melyeket a közvetítő hálózat nem támogat.

Show interface tunnel

# ACL

Az ACL engedélyező és tiltó utasítások sorozata. Ezek a listák határozzák meg a forgalomirányítók számára, hogy mely csomagokat fogadják el és melyeket utasítsák vissza. Két nagyobb részre lehet bontani az ACL-eket. Ezek a „standard” - és a „extended”. A standard, azaz normál ACL-ek csak a forráscímekre vonatkozóan tudnak tiltást, illetve engedélyezést alkalmazni, míg az extended vagyis kiterjesztett képes cél címeket, portokat és felsőbb rétegbeli protokollokat is figyelembe venni. A normál ACL-ek utasításait a listák sorszámtól függően 1-99 között tudjuk használni, míg a kiterjesztett listák utasításait 100-199 között vagy szavakkal elnevezve tudjuk alkalmazni. Utóbbi rendkívül hasznosnak bizonyul, ha sok ACL-t használunk a hálózatunkban, mivel a lista nevével utalhatunk az ellátott funkciójára. Jelenleg 2 ACL-t használ a hálózatunk. Az egyik a PAT működéséhez szükséges, ebben beállítottuk az engedélyezett belső hálózatokat. A másik ACL-ben azt állítottuk be, hogy a szervereket a túlterhelés elkerülése érdekében ne lehessen pingelni. A pingelhetőségen ívűl minden funkció tökéletesen működik a szervereken.

# PAT/NAT

Az Internet elterjedésével a rendelkezésre álló IPv4 címek száma rohamosan csökkeni kezdett. Erre a problémára nyújt megoldást a PAT (Port Address Translation), más néven NAT overload, a NAT egyik fajtája, melynek fő célja a privát IP címeinket nyilvános IP címre fordítani. Lényege, hogy több privát IP címet egyetlen nyilvános IP címhez rendel egyedi portszámok segítségével. A PAT rejtve tartja a privát hálózatban lévő eszközök IP-címeit az internettől, ezáltal javítva a hálózat biztonságát. A PAT a forgalomirányítókon valósul meg. Amikor a privát hálózatban lévő eszköz kimenő kapcsolatot létesít az internettel, a forgalomirányító lefordítja a privát IP-címet egy nyilvános IP-címre és portra, majd eltárolja a lefordítást egy fordítási táblázatban. NAT: Emellett statikus NAT-ot állítottunk a szervereknek az üzemeltető helységben a könnyebb elérhetőség érdekében, illetve az otthoni dolgozó számára is statikus natolást állítottunk.

# IPv6

Az üzemeltetők, illetve a Motel részére konfiguráltunk IPv6 címeket, amelyeket az adott területen DHCP protokoll segítségével automatikusan kapnak meg az eszközök. Az IPv6 ugyanazokat az alapvető elveket követi, mint az IPv4, azonban az IPv6 számos új funkciót is bevezet. Az IPv6 címek 128 bitesek, ami hatalmas címtartományt biztosít. Ez a címtartomány elegendő ahhoz, hogy minden internethez kapcsolódó eszköz egyedi címet kapjon. Az IPv6 fejléce egyszerűbb, mint az IPv4 fejléce, ezáltal hatékonyabb adatátvitelt tesz lehetővé. Az IPv6 támogatja a mobil eszközöket. A mobil IPv6 egy olyan protokoll, amely lehetővé teszi a mobil eszközök számára, hogy hálózatváltáskor is megőrizzék IP-címüket.

# Szerverek

A hálózatunkban megtalálható az üzemeltető részleg is, amely a topológia azon része, ahol mi tartjuk szemmel a hálózat működését. Ezen a részlegen megtalálhatóak a hálózat szerverei, egy IP telefon a direkt kommunikáció érdekében, az Admin PC-k és egy AP. A szerverek funkcionalitása az itt látható topológián belül működik, viszont a megfelelő szemléltetés érdekében megcsináltuk őket valós virtuális számítógépként a VitualBox nevű szoftver segítségével.

Mikrotik router segítségével kiosztottuk a címeket, amelyek a 35.125.55.0/25-ös hálózatot ölelik körbe. Illetve különféle tűzfal beállításokat alkalmaztunk a szerverek számára.

Van egy primary domain controller-es szerver DNS, DHCP, active directory-val, secondary domain controller szerver dhcp failover konfigurációval hogyha bármi történik az elsődleges ad szerverrel, a hotel, motel és a kávézó kaphasson továbbra is internet elérést. Ezen felül megtalálható egy Linux alapú file, web és print szerver, illetve a későbbiekben kialakításra kerül egy MySQL alapú szerver az adatok tárolására és szűrésére, és egy email szolgáltatást.

Az PDC és az BDC szervert Windows GUI 2019-ben valósítottuk meg.   
A server managerben konfiguráltuk fel, a DNS, DHCP, Active Directory szolgáltatást, és az SDC esetében a DHCP failovert feltelepítettük. A felhasználók a saját felhasználónévükkel tudnak fellépni. Mindkét szerver esetén a domain-név a lwsolutions.hu-n lesz elérhető. Ezenfelül korlátozva a felhasználók bejelentkezési ideje és egyes dolgokhoz való hozzáférése is.

Felkonfigurálva mindkét Windows GUI szervert, a továbbiakat egy Windows 10 kliensen keresztül folytattuk.

A Windows-t feltelepítve és partícionálva a LINKWAVESOLUTIONS tartományba léptettük be.

Server manager-ben megadtuk a két GUI szerver ip címét, hogy felvegyük a szerverlistákba őket. Ezután az elsődleges DC-n keresztül a dns reverse és forward lookup beállításain keresztül zónákat, pointereket, és A hostot, ahol a további szerverek elérhetőségét szerver névvel együtt fel tudtuk venni.

Ezután az active directoryban felvettük a Hotel szervezeti egységeit, felhasználókkal és csoportokkal együtt.

A kollegák felhasználójának állítottunk be alapértelmezett hátteret, amely minden cégen belüli dolgozónak egységes, alapvetően telepítve van a Firefox böngésző és ilyen szintű felhasználókkal a biztonság érdekeben nem férnek hozzá a CMD-hez és a Control Panelhez. Ha fájlkezelőbe belépünk, láthatjuk, hogy több megosztott hálózati mappát és lát a felhasználó. Az egyik egy X GB-os személyes mappa, amit az adott felhasználó lát csak és egy másik X GB-os közös mappa, amihez minden felhasználó hozzáfér. A böngészőt megnyitva láthatjuk cégünk weboldalát is.

# Programozás

Kódunk automatizálja a Cisco forgalomirányítók enable jelszavának frissítési folyamatát, biztosítva a biztonságot és a rendszeres jelszócserét. A kód két modul importálásával kezdődik: time és netmiko. Az idő modult arra használtuk, hogy késleltetést állítsunk a jelszóváltoztatások között. A Netmiko kényelmes felületet biztosít a hálózati eszközökkel való interakcióhoz. A szükséges modulok importálása után megadtuk a kívánt útválasztó paramétereit: az IP-címet, az eszköztípust, az azonosításhoz szükséges hitelesítő adatokat és az aktuális engedélyjelszót. Ezután a „get\_new\_enable\_pwd()” függvény arra kéri a felhasználót hogy adjon meg egy új jelszót. A következő függvény „change\_enable\_pwd()” SSH-kapcsolatot hoz létre a routerrel a megadott paraméterekkel, és megváltoztatja a jelszót az új megadott jelszóra, ezután kiírja a felhsználónak az új jelszót. Majd a script egy végtelen ciklusba lép, hogy ismét megváltoztassa a jelszót. Minden jelszóváltoztatás után egy hétig vár „time.sleep(604800)”, mielőtt újabb változtatást kérne.