**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.

**Port-aggregation**

A Hotelben és a kávézóban a switcheken portösszefogást alkalmaztunk PAgP protokoll (Port Aggregation Protocol) segítségével. Ennek célja nagyobb sávszélesség elérése, a terhelés eloszlatása, illetve redundancia bisztosítása. A PagP egy Cisco által fejlesztett protokoll, az általuk támogatott eszközök között müködik 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

Máté első része

**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

**CHAP**

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

**HSRP**

A New York hotel területén HSRP protokolt 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

**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 utásait 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.

**PAT**

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.

Át adom Máténak a szót, aki a Vlanokról, illetve a VTPről fog beszélni.