SOHOÁt is veszem a szót. Szóval amiről nem beszéltünk még többek között azok a SOHO routerek vagy home routerek, ki, hogy ismeri. A soho routerek azok, amiket az ember megtalálhat a saját otthonában, beállíthat rajta 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 fajta titkosítással. Tehát ezekből a routerekből raktunk le hármat a hálózatban, 1-et a motelbe és 2-t a kávéházba, azon belül az egyiket a bárba másikat az étkező helyre, hiszen azt számoltuk, hogy nem lesz több vendég egyszerre mint 250, a bárban főleg. A harmadik soho pedig a motelben található. A biztonsági beállításukról is beszélnék egy keveset. 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 jelszót azért állítottuk be, hogy csak a fogyasztásra esedékes vendégek tudják a WiFi-t használni. Azért is a PSK verziót állítottuk be, mert legalább 8 karakter hosszú kell lennie, kis- és nagy betűket, számokat és speciális karaktereket is kell tartalmaznia, tehát nehezebb a hálózat feltörése. Ezek mellett a PSK kapcsolat megtartásához egy eszköznek meg kell ismernie egy dinamikus kulcsot, amely a hálózat generál és ezzel együtt küldi csak titkosítva a csomagokat az adott eszközökre.

Spanning tree  
Spanning tree protokollt állítottunk be a New York hotel terület switchei közt és a kávéház routerei között. Ezzel a protokollal akadályozzuk meg többek között, hogy ne legyen üzenetszórási vihar, ha egymással kommunikálnának az eszközök. Na de hogyan is működik az STP protokoll? A hálózatban kiválaszt egy gyökérponti hidat, amelyhez minden kapcsoló egy útvonalon csatlakozik, a többi kapcsoló portjai közül néhányat lezár, hogy azok ne továbbítsanak forgalmat (kivéve, ha esetleg több switchen van VLAN priority és secondary-ság beállítva, olyankor egyes forgalmaknak megnyit más útvonalat is) de ha egy útvonal meghibásodik, tegyük fel a kábel megszűnik működni, akkor automatikusan átkapcsolja a forgalmat egy másik útvonalra. Ez a protokoll számos előnyt biztosít, például ahogy azt már mondtam, megelőzi az üzenetszórási vihart (azaz hurkokat), redundanciát növeli és nem utolsó sorban, csökkenti a forgalom terhelését. Az STP-nek is több verziója létezik már, például az IEEE 802.1D vagy 802.1w stb. Ezek újabb és újabb megvalósítások melyek egyre gyorsabbá és megbízhatóbbá varázsolják az STP protokollt.

Show spanning-tree interface  
show spanning-tree summary

GRE

Mint ahogy látható a topológián, állítottunk GRE (Generic Routing Encapsulation) alagutat is. A protokoll működése igen egyszerű, hiszen 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. Tehát az üzemeltetők router és a kávézó router között egy virtuális alagutat hoz létre két pont között, amellyel, ha nincsenek is egy hálózatba, akkor is azt érzékelik mintha egy lenne, persze ehhez az kell, hogy a fizikai interface-en át tudjon menni a csomag. Az alagutak segítségével tehát olyan protokollok adatait tudjuk szállítani két forgalomirányító között, melyeket a közvetítő hálózat nem támogat.

Show interface tunnel

OSPF  
Nem utolsó sorban OSPF-et állítottunk be a 4 fő router között, azaz a terület elválasztó routerjeink között, ezzel biztosítva, hogy a hálózatot dinamikusan és gyorsan megismerik egymástól, plusz saját magunk munkájának gyorsításának érdekében. Szóval mi is az az OSPF? Az OSPF vagy OSPFv2 (Open Shortest Path First version 2) egy link-állapotú útválasztási protokoll, amelyet kis- és közepes méretű hálózatokhoz terveztek. Az OSPFv2 útválasztási algoritmusa a legrövidebb út algoritmus, amely a hálózatban lévő linkek súlyai alapján határozza meg a legrövidebb útvonalakat a forgalom számára. Az hálózatokat egységekre, úgynevezett területekre osztja fel. A területek lehetővé teszik a hálózat adminisztratív felosztását, és segítenek megvédeni a hálózatot a rosszindulatú támadásoktól. Egyik legfőbb eleme a 10 másodpercenként küldött „hello-csomagok” (ezt tudjuk változtatni, ez az alap értéke), 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 az forgalom továbbítására.

show ip ospf interface  
show ip ospf neighbour

Köszönjük, hogy meghallgattak minket!