DIPLOMAMUNKA

Lefkánics Szabolcs

Debrecen
2009

Debreceni Egyetem
Informatikai Kar

Egy működő kommunikációs hálózat elemzése és fejlesztése

Témavezető:
Dr. Almási Béla
Egyetemi Docens

Készítette:
Lefkánics Szabolcs
Programtervező Informatikus Msc.

Debrecen
2009

1. Bevezetés

Az informatikai hálózatok fejlődése, terjeszkedése megállíthatatlan. A fejlődő országokban lassan minden ember kapcsolatba kerül velük valamilyen módon, úgy tűnik, a kommunikáció minden formájában teret hódít. Ha belegondolunk abba, milyen szerepe volt néhány tíz évvel ezelőtt – még csak épület méretű hálózatok léteztek – és milyen szerepe van most – már az egész világot behálózza (Internet), melyet gyakorlatilag a Föld bármely pontjáról elérhetünk – rájövünk, mennyire komfortossá is teszi életünket, és bizony az is igaz, hogy a legtöbb világméretű cég gyakorlatilag létezni sem tudna e „közeg" nélkül.

Azt, hogy hálózatainkat folyamatosan fejlesztenünk kell, könnyen beláthatjuk. Mint minden más területen, itt is igaz az állítás, miszerint az embereknek a technika fejlődésével egyre nagyobbak az elvárásaik. Ha hozzászokunk egy adott szolgáltatási szinthez, többet akarunk, még jobb minőségű, még gyorsabb adatátvitelt. Ez az igény késztet minket – informatikusokat – arra, hogy folyamatosan fejlesszük, jobbá tegyük az irányításunk alatt működő rendszereket. Hogy hol van a fejlődés vége, senki sem tudja. Manapság már bőven túlnőttünk azon, hogy csak a hétköznapi értelemben vett adat megosztására, továbbítására használjuk a hálózatokat. E közeg segítségével telefonálhatunk (VOIP), vagy akár televíziót nézhetünk – ezen IP alapú szolgáltatások, lássuk be, előbb-utóbb teljesen átveszik az analóg rendszerek szerepét. Az ilyen és hasonló igények persze folyamatos fejlesztést vonnak maguk után, kiszolgálásuk – és ami a legfontosabb, jó minőségű kiszolgálásuk – nem lehetséges egy elavult hálózattal. A gyártók folyamatosan új termékekkel jelennek meg, új, gyorsabban működő és megbízhatóbb útválasztó protokollokat fejlesztenek. A fejlesztések azonban sokszor nem csak a megnövekedett igények kielégítését hivatottak ellátni, de sokszor költséghatékonyabb megoldásokat is kínálnak, mint elődjük. Gondoljunk például a videó telefonálásra, mely egy már ma is létező, a cégvilágban igen elterjedt kommunikációs forma. Segítségével rengeteg pénzt és időt spórolhatunk, az utazás során bekövetkező környezetszennyezés elkerüléséről már nem is beszélve.

Az általam választott számítógépes hálózat fejlesztésénél is hasonlóak a motivációk. A hálózat egy 300 fős céget szolgál ki (HSBC Credit Zrt.), mely közvetve része egy sokkal nagyobb, szó szerint az egész világot behálózó rendszernek (HSBC Bank Plc). A szervezet,

melynek részei vagyunk, 87 országban van jelen. Magyarország az európai régió közvetlen tagja. A magyarországi vállalat egy viszonylag egyszerű, bérelt vonali hálózatból áll, két központi telephellyel, valamint kilenc fiókkal. A hálózat fejlesztés során ezt a bérelt vonali rendszert migráljuk MPLS technológia alá, amit főleg későbbi fejlesztések (IP Telefónia), valamint egy országok közötti (International) MPLS felhő kialakítása motivál.

A dolgozat folyamán elemző stílusban mutatom be a cég számítógépes hálózatát. Az első részben elemzem a meglévő rendszer felépítését, működését, néhány technikai részletet bővebben is kifejtve. A második rész elejében a fejlesztést motiváló tényezők bemutatása után magát a bevezetni kívánt technológia működését tárgyalom, rávilágítva ezzel az MPLS legfőbb előnyeire. Ezt követően a migráció lépéseit, tervezést, implementációt részletezem, végül pedig a szinte kötelezőnek mondható tesztelés kap némi teret dolgozatomban.

2. Elemzés

Az elemzés során a meglévő, fejleszteni kívánt hálózat részletes bemutatása következik. A fejezet során kitérek mind a fizikai felépítésre (eszközök, topológia), mind a működésre (útválasztó protokoll elemzése, routok elemzése, redundancia). Ezek után egy rövid kitérőt teszünk a LAN oldalon, megvizsgáljuk a központi iroda lokális hálózatát. Ezen fejezet célja, hogy jobban megértsük és átlássuk a teljes rendszer működését, ugyanis sok részlete az új rendszernek is szerves részét képezi majd.

2.1 Routing (WAN oldal)

Első lépésként vizsgáljuk meg a WAN oldali felépítést, valamint a routing-ért felelős protokoll általános tulajdonságait, működését a HSBC hálózatában.

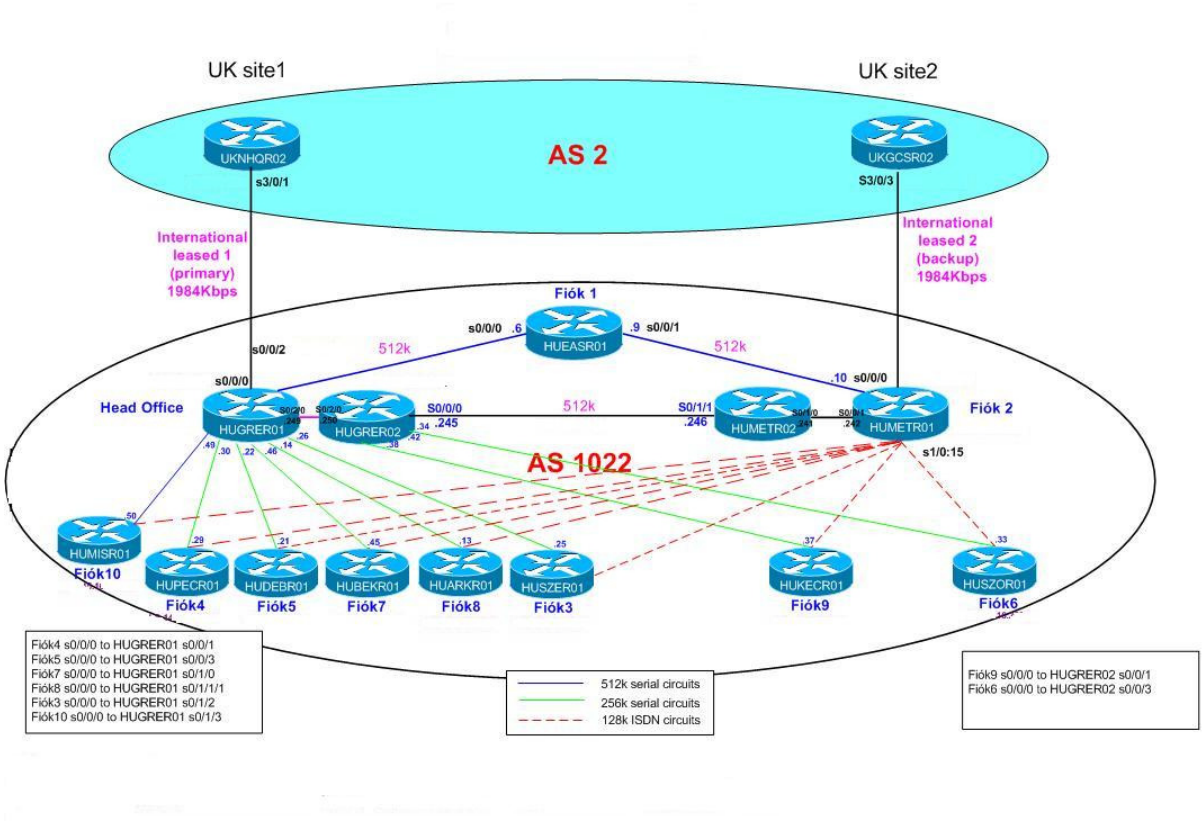
2.1.1 Eszközpark

A routing megvalósításáért felelős eszközpark homogén, kizárólag Cisco 2821-es útválasztókat használunk.

1. Cisco 2821

Ebből minden telephelyen egy darab található, kivétel ez alól a központi iroda (Head Office), valamint a 2-es fióktelep, ahol kettőt helyeztünk el. Ennek egyik oka, hogy a bérelt vonali szolgáltatás X.21 interfészen érkezik és problémás lett volna 10 db ilyen interfészt egy router-ben elhelyezni. Másik nem elhanyagolható ok pedig egy hibatűrő hálózat kialakítása, aminek működését később kifejtem.
Az eszközök nagyon megbízhatóan működnek már 7 éve, egy ventillátor leálláson kívül más problémánk még nem volt velük.

2.1.2 Hálózati topológia bemutatása, elemzése



2. Bérelt vonali topológia

A hálózat viszonylag egyszerűen épül fel. Mint az a 2-es ábrából is látszik, csillagpontos topológia, melynek a Head Office a középpontja (az ábrán bal oldalon, HUGRER01 és HUGRER02 eszközök). Ennek előnyeit könnyen beláthatjuk, ha feltételezzük valamelyik fiók leszakadását a hálózatról. Ezen esemény ugyanis a topológia jellegéből adódóan nem érinti a többi telephely működését, azok elérhetősége továbbra is biztosított.

A WAN linkeken /30-as alhálózatokat használunk, melyek biztosítják a szükséges két IP címet linkenként.

Az egyes végpontok 256Kb/s sávszélességű bérelt vonallal kapcsolódnak a központi telephelyhez, melynek végét a szolgáltató x.21 interfészen biztosítja. Ez a sebesség manapság már kevésnek tűnhet - többek között ez az egyik érv a fejlesztés mellett. A fióktelepek egyáltalán nem kommunikálnak egymással, adatforgalmukat tekintve egyrészről a Head Office-ban lévő fájl és nyomtató szervereket címzik, másrészről pedig az egyes applikációk (banki rendszerek, levelező program) szerverei az Egyesült Királyságban találhatóak, melyek

elérése alapesetben a Head Office-on keresztül történik, egy 2Mb-es nemzetközi bérelt vonalon keresztül.

Mint az a topológiából is látszik, a redundanciának jelentős szerep jutott a hálózat kialakításakor. A fióktelepeken a bérelt vonalon kívül egy ISDN2 kapcsolat is készenlétben áll (2x64k, a képen ------ jelöli). A router az esetleges bérelt vonali útvonal elvesztése esetén néhány másodperc alatt átáll a másodlagos irányra és betárcsáz az ISDN2 másik végén található 2-es fióktelepre, ahol egy ISDN30 várja a bérelt vonalról leszakadt telephelyek hívásait. Mivel a 2-es fióktelep is redundánsan kapcsolódik a Head Office-ra, ezért szinte biztosra vehető, hogy az ISDN kapcsolaton kommunikáló telephelyek elérik a központi irodát és tudnak kommunikálni mind a lokális szerverekkel, mint a UK-ben lévő applikáció szerverekkel. Ez a két irány egy közvetlen 512Kb-es bérelt vonal a 2-es fiók és a Head Office között, valamint egy másik 512Kb-es link a 2-es fiók és 1-es fiók között. Ez a „háromszög" redundanciát biztosít az ISDN kapcsolat nélkül maradt 1-es fiók számára is, ami a topológiából is jól látszik.

A redundancia kapcsán meg kell említeni a nemzetközi bérelt vonal elvesztésének lehetőségét. Ebben az esetben a központi routerek másodlagos útvonala a 2-es fióktelep felé mutatnak, amely szintén rendelkezik egy 2Mb-es nemzetközi bérelt vonallal Anglia felé. Ez így még jónak is tűnhet, a hálózatban azonban – ha éppen a 2-es telephelyet használjuk nemzetközi gateway[1]-ként - van egy bottleneck[2], ami nem más, mint a Head Office és a 2-es fiók közötti, mindösszesen 512Kb-es bérelt vonal. Ugyanis hiába a másodlagos 2Mb, ha az adat a két központi telephely között csak 512Kb-et használhat.

Szót kell még ejteni a központi irodában, a két útválasztó (HUGRER01 és HUGRER02) közötti Hot Standby Router Protocol[3]-ról. Ez ethernet linken van megvalósítva, szerepét tekintve pedig csak a Head Office LAN-jában dolgozók számára van jelentősége, ugyanis ha az egyik router meghibásodik, annak fizikai kapcsolataival a másik nem rendelkezik, kivéve a központ LAN linkjét (a LAN topológia bemutatásánál fogjuk látni miért). Így egy esetleges R1 hiba esetén a központ nem szakad le a hálózatról, mind a fióktelepekkel, mind Angliával képes kommunikálni a 2-es telephelyen keresztül.

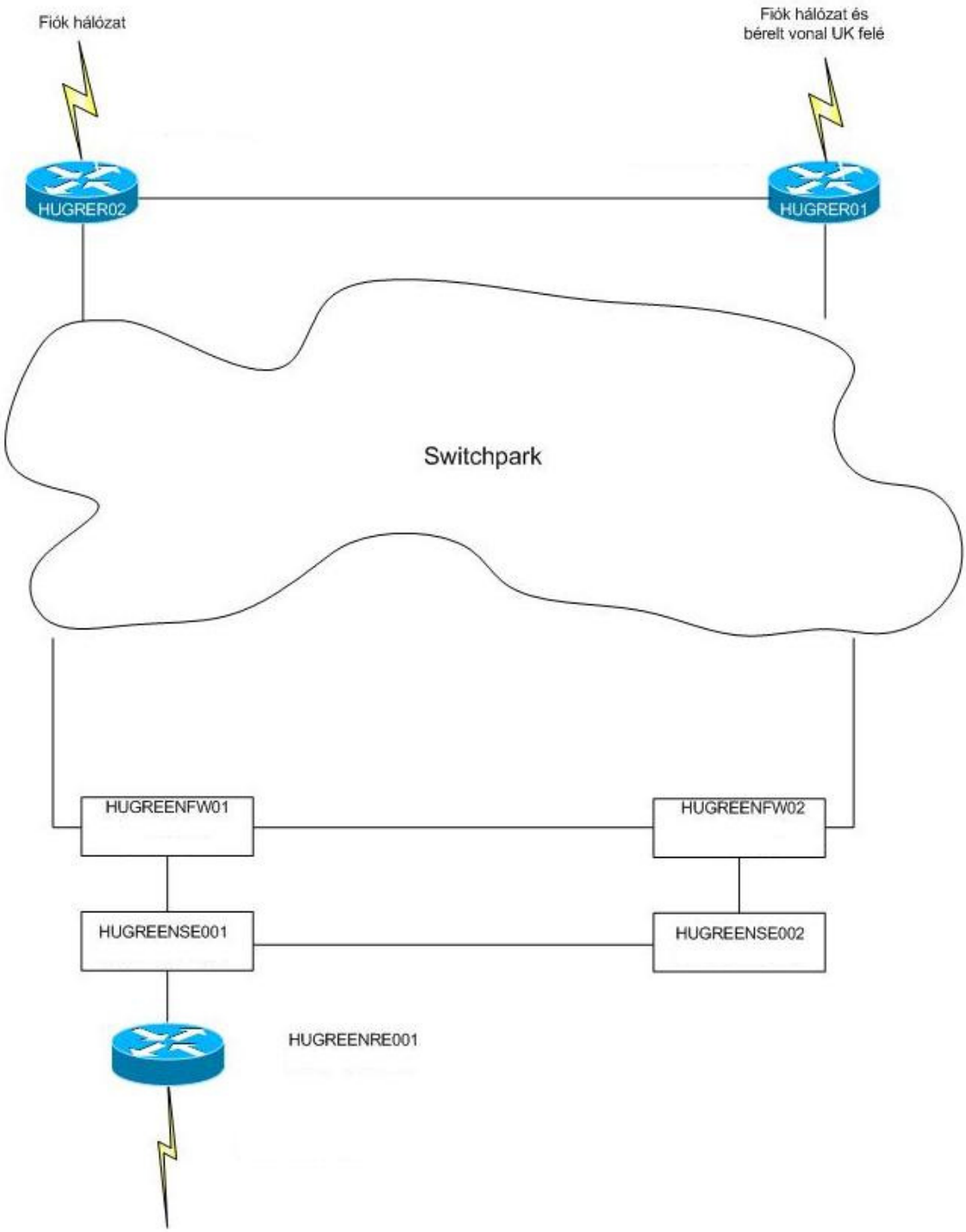
---

[1] egy alhálózat ki/belépési pontja. Ha egy hálózaton lévő eszköz kommunikálni szeretne egy másik eszközzel, amely nem ugyan abban az alhálózatban van, akkor a gateway-t címzi.

[2] egy hálózati topológiában szereplő linkek közül a legkisebb sávszélességgel rendelkező

[3] HSRP Cisco Systems által kidolgozott megoldás, segítségével hibatűrő hálózatok építhetőek. A protokoll megvéd az alapértelmezett átjáró (gateway) elvesztésétől azon hostoknál is, amelyek nem képesek azt dinamikusan megtanulni.

Ami a fenti topológiából kimaradt az a lokális hálózat egyetlen kilépési pontja, egy redundáns tűzfal (3-as ábra).



3. A hálózat egyetlen kilépési pontja

A HUGREENFW01 és HUGREENFW02 is közvetlenül kapcsolódik egy-egy layer 3-as switch-hez a hálózat 'belső' oldalán, (a switch parkot egy későbbi fejezetben fogom részletezni), a külső oldalon pedig két access switch biztosítja a későbbi bővíthetőséget (HUGREENSE001 és 002). Csak a szemléltetés kedvéért hagytam egy routert a HUGREENSE001-es switchen, ami egyébként egy, a nyomtatás kiszervezéshez, a központi irodánk és egy nyomda közötti bérelt vonalon hivatott az útválasztást végezni.

2.1.3 Általános router beállítások bemutatása

Ebben a részben az útválasztók alap beállításait tárgyalom (csak az érdekesebb parancsokkal foglalkozom, a teljesség igénye nélkül).
A következő startup konfig[1] mondhatni alapnak, minden router ezen beállítással működik – természetesen az interfészek azonosítója, IP címe eltér.

A startup config néhány alap beállítással kezdődik:

```
!
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
```

Az első két sor biztosítja azt, hogy a debug és a log információk időbélyegzővel együtt kerüljenek tárolásra, méghozzá a helyi idővel. A harmadik service beállítás bekapcsolja az access és ena jelszó titkosítását a konfigurációs fájlokban, így ezek egy sima konfigurációs fájl megjelenítéssel nem láthatóak.

[1] a router összes konfigurációját tartalmazó fájl. Az eszköz kikapcsolás vagy újraindítás alkalmával ennek segítségével jegyzi meg beállításait.

```
!
clock timezone GMT 0
no network-clock-participate wic 0
no network-clock-participate wic 1
!
```

A clock timezone parancs magától értetődő, beállítja az időzónát. A no network clock participate parancs megtiltja az utána írt interfésznek, hogy a hálózatból kapott órajelet használja.

```
!
ip cef
!
```

Az ip cef egy érdekes utasítás. Ha bekapcsoljuk, akkor a router az első routed interfészen kapott csomagról eltávolítja a layer 2 réteget, és a lecsupaszított layer 3 réteget eltárolja. Az ezután kapott csomagokat ezen információ alapján routolja, anélkül, hogy a CPU-t használná, így jelentősen felgyorsítva az útválasztást. Ezt Cisco's Express Forwarding (CEF)-nek hívják. Hátránya csupán annyi lehet, hogy a debug funkció nem működik a „gyorsan küldött" csomagokra.

```
!
interface Serial0/0/1
 description 512K link to Metrotech
 bandwidth 512
 ip address 145.16.0.1 255.255.255.252
 no shutdown
 clock rate 2016000
 dce-terminal-timing-enable
!
```

A serial0/0/1 interfész konfigurációja is mondhatni ’átlagosnak’. Ami viszont érdekes és tanulságos lehet, az a bandwith érték megadása. Ugyanis az EIGRP protokoll az itt beállított értékkel számolja a metrikát, és ha rossz érték van megadva (vagy kimarad ez a beállítás) akkor megeshet, hogy a hálózatválasztó protokoll rossz, esetleg nem a leggyorsabb routot fogja használni, mint elsődleges irányt.
A dce-terminal-timing-enable arra kényszeríti az interfészt, hogy a DTE eszköztől kapott időzítést használja, és ne a sajátját.

```
!
interface GigabitEthernet0/0
 ip address 145.17.1.252 255.255.255.0
 ip helper-address 128.9.49.71
 ip helper-address 128.8.117.71
 duplex full
 speed 100
 standby 20 ip 145.17.1.254
 standby 20 priority 105
 standby 20 preempt
!
```

A fenti Gi interfész a LAN oldal felé néz. Érdekessége lehet a speed és duplex beállítás, ugyanis mi minden ethernet portot – legyen szó akár router-ről akár switch-ről – fixen full 100 ra konfigurálunk. (van, aki az auto beállításokra esküszik, később részletezem, miért).
Fentebb már szót ejtettem a HSRP (Hot Standby Router Protocol) beállításról. Ez az interfész a primary (145.17.1.254). A HUGRER02-ben van konfigurálva a „másodlagos gateway” amelyen természetesen magasabb prioritás van beállítva.

2.1.4 Routing protocol elemzése

A router alap beállításai után a hálózatban működő útválasztó protokoll elemzésével foglalkozunk. Először néhány szót ejtünk a protokoll működéséről általában, ezután pedig megnézzük, hogyan használható ez a gyakorlatban, milyen konfigurációt alkalmazunk a HSBC hálózatában.

2.1.4.1 EIGRP működése

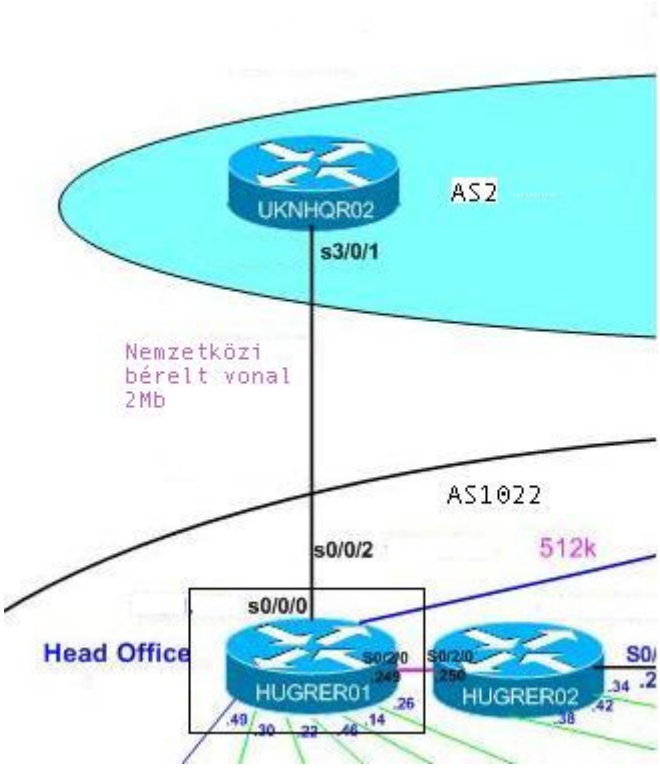
Az EIGRP napjaink egyik legelterjedtebb útválasztó protokollja egy AS-en belül (Cisco hálózatokban). Működését tekintve 3 fő lépést különíthetünk el a routok meghatározásánál:

- Szomszédos eszközök felfedezése: az EIGRP-t használó routerek hello üzeneteket küldenek, hogy felfedezzék a szomszédos, szintén EIGRP protocol-t használó útválasztókat, amelyekkel potencionálisan „szomszédok" lehetnek.
- Topológia csere: a szomszédok egymással a teljes topológiát kicserélik, amikor egy szomszéd viszony létrejön, aztán csak részleges topológia csere történik, az is csak akkor, ha valamilyen változás történik a hálózatban.
  Itt fontos még megjegyezni, hogy az egyes routerek természetesen nem tárolják az egész hálózatra vonatkozó routing bejegyzéseket, csak a számukra fontosakat. Ilyenek például a közvetlenül hozzájuk csatlakozó alhálózatok, vagy egy szomszéd eszköz által jelentésre került másodlagos útvonal, amit használni tud egy távolabbi alhálózat elérésére, az elsődleges útvonal elvesztése esetén.
- Útválasztás: a routing bejegyzések elemzése során a protokoll kiválasztja a legkisebb metrikával rendelkező útvonalat, hogy elérje a címzett alhálózatot.

A fenti három lépés eredményeként a routernek három EIGRP táblát kell fenntartania. Az EIGRP szomszéd lista a potencionális EIGRP protocol-t futtató routereket tartalmazza.
Az EIGRP topológia tábla az összes routing bejegyzést tartalmazza, amelyeket a router a szomszédaitól tanult. Végül pedig az IP routing tábla csak a kiválasztott, legjobb metrikával rendelkező útvonalakat foglalja magába.

2.1.4.2 Az EIGRP működése a hálózatban

Az EIGRP a legnagyobb szerepet nyílván a központi (a csillagpont közepén lévő) útválasztókban kapta. Nézzük most meg az egyik központi node-ban (HUGRER01) konfigurált EIGRP beállításokat.



4. HUGRER01 forgalomirányító kapcsolatai

Mivel ez a csomópont 2 AS-el van kapcsolatban, így az EIGRP-t mindkét irányba be kell kapcsolni. Először a távoli AS rendszer felé történő disztribúciót elemezzük:

```
!
router eigrp 2
 redistribute eigrp 1022 route-map HUDRN
 passive-interface default
 no passive-interface Serial0/0/0
 network 172.1.0.0
 distribute-list prefix HU_TOUK out Serial0/0/0
 distribute-list prefix HU_FROMUK in Serial0/0/0
 no auto-summary
```

```
 no eigrp log-neighbor-changes
!
```

Mint az látszik, először egy route redisztribúció van beállítva egy route map alapján. Ez a route map a HUDRN:

```
!
route-map HUDRN permit 10
 match ip address 10
 set metric 200000 10 255 1 1500
!
```

Ahol a parancs megenged minden olyan route redisztributálást, ami a 10-es ACL-ben engedélyezve van, valamint beállítja a redisztribútált routok metrikáját a fenti értékeke szerint, ezzel mintegy testre szabva a 2-es AS-be bekerülő routokat.
A továbbiakban látunk egy passive iterface default parancsot, ami tulajdonképpen a routerben lévő összes interfészt passzív módba rakja – természetesen csak az EIGRP által generált forgalom tekintetében - , megakadályozva ezzel azt, hogy a routing protocol túl nagy forgalmat generáljon, vagy esetleg olyan irányba is küldjön routing információkat, amerre nem szabad.
A passive interface parancs azonban egy kicsit másképpen működik az EIGRP protokollnál használva, mint azt már megszokhattuk más protokollok esetében. Ugyanis míg más routing protokolloknál a parancs csak a kifelé menő forgalmat tiltja, itt sem a kimenő, sem a bejövő EIGRP üzeneteknek nem enged szabad utat. Így a router természetesen elveszti a passzív interfész irányában lévő, esetleg EIGRP protokollt használó routerekkel a szomszéd kapcsolatot.
A no-passive-interface [interface] parancs kiadásával nyílván deaktiválhatjuk a parancs hatását egy meghatározott interfészre, így mintegy „elérhetővé” téve az EIGRP-t az érintett interfészen.
Mit is jelent ez a mi hálózatunk esetében? A no-passive-interace parancs aktív módba rakja a serial0/0/0 irányt. Mivel AS 2-ben lévő router csak ebben az irányban van, így felesleges is lenne folyamatos hello üzenetekkel terhelni a többi interfészt.

```
!
network 172.1.0.0
!
```

A network parancs az EIGRP egyik „alap” konfigurációs parancsa, tulajdonképpen ezzel engedélyezzük az EIGRP működését az egyes irányokba. Itt minden olyan interfészen bekapcsoltuk az EIGRP-t, amin a 172.1.0.0 hálózat van konfigurálva. Mivel a hálózat wildcard mask[1] nélkül van megadva, ezért a router természetesen classful-ként értelmezi azt.

```
!
distribute-list prefix HU_TOUK out Serial0/0/0
distribute-list prefix HU_FROMUK in Serial0/0/0
!
```

A fenti két parancs segítségével megakadályozzuk, hogy a két AS határon lévő útválasztó minden EIGRP routing információt kicseréljen. A parancsok alkalmazásával kifelé irányban csak a HU_TOUK prefix listában meghatározott, befelé jövő irányban pedig a HU_FROMUK által definiált routok cseréje engedélyezett.

```
!
no auto-summary
no eigrp log-neighbor-changes
!
```

Alapesetben az auto summary parancs szummarizálja a routokat, így csökkentve a routing információkat, tehermentesítve ezzel a hálózatot illetve az eszközöket. Itt viszont nincs rá szükség, ugyanis csak a prefix listában meghatározott routoknak engedünk utat, nem kapunk „felesleges” routing információkat.
Hogy tovább csökkentsük a forgalmat az amúgy sem túl nagy sebességű nemzetközi bérelt vonalon, az eigrp logok cseréjét is kikapcsoltuk a no eigrp log-neighbor-changes paranccsal.

[1] cisco wildcard mask az ip cím azon részét írja le, amelyet vizsgálni kell. Például Access Control List-eknél használják, ahol azt mutatja meg, hogy a listában szereplő ip cím mely részét kell összehasonlítani a csomagon lévő ip azonos részletével.

```
!
router eigrp 1022
 redistribute eigrp 2 route-map HUGRN
 passive-interface default
 no passive-interface GigabitEthernet0/0
 no passive-interface GigabitEthernet0/1
 no passive-interface Serial0/0/1
 no passive-interface Serial0/0/2
 no passive-interface Serial0/0/3
 no passive-interface Serial0/1/0
 no passive-interface Serial0/1/1
 no passive-interface Serial0/1/2
 no passive-interface Serial0/1/3
 network 145.16.0.0 0.7.255.255
 no auto-summary
 no eigrp log-neighbor-changes
!
```

A teljesség kedvéért a routing protocol konfigurációját megadom a 1022-es AS-re is. A konfiguráció lényege tulajdonképpen azonos az AS 2-ével. A 1022-es AS-ben lévő routerek nyílván az „ellenkező oldalon” vannak, így a csak ebben az irányba néző interfészek lesznek nem passzív-ok. A wildcard mask használata a network parancsnál biztosítja, hogy az EIGRP csak azokon az interfészeken legyen aktív, amelyek a 145.16.0.0 és a 145.23.255.255 közötti alhálózatban vannak.

2.2 Switching (LAN oldal)

Ebben a fejezetben a fiókirodák és a központi iroda lokális hálózatának bemutatása következik. A teljes rendszer átlátásához lényeges, hogy megismerjük a lokális hálózatok működését, ip címkiosztási metódusát, valamint a hálózati hurkok elkerülésének módját, a Spanning Tree Protocol-t (STP). Ez utóbbi szerepének megértéséhez szükséges egy rövidebb technikai fejezet, amely az STP működésének részleteit ismerteti. Említés szinten megjelenik néhány lehetséges LAN oldali fejlesztés a fejezetben. Ezen „ötletek" függetlenek a dolgozat tárgyától, nem részei a tárgyalt MPLS migrációnak.

2.2.1 Használt eszközök bemutatása, főbb tulajdonságok

Az eszközpark routing oldalon teljesen homogén volt. Switching oldalon viszont nem mondható el ugyan ez. Igaz, hogy a legtöbb telephelyen ugyan azt a típust – cisco catalyst 2950 – használjuk, de akad fiókiroda ahol Alcatel omnistack 6124 , cisco catalyst 2960 , vagy éppen a már IP telefónia bevezetésére alkalmas cisco catalyst 3560 végzi a switching-et.
Ezeken kívül a Head Office-ban található 2 db catalyst 3550 layer 3-as switch.

2.2.2 Néhány szó a spanning tree protocol-ról

A spanning tree portocol lényege, hogy elkerüljük hurkok képződését redundáns hálózatokban, megakadályozva ezzel broadcast stormok[1] kialakulását, valamint a hálózati hurkok másik „eredményét" a MAC tábla instabilitást[2]. Ezt a protokoll úgy éri el, hogy míg egyes portokon szabad adatforgalmat engedélyez (forwarding state) addig másokon blokkolja azt (blocking state). Azt, hogy mely portokat blokkolja és melyeket engedélyezi, a Spanning Tree Algorythm (STA) segítségével dönti el. Ehhez első lépésbe az algoritmus kiválaszt az

[1] Ha egy hálózaton lévő eszköz üzenetet szeretne küldeni a vele egy alhálózaton lévő összes többi eszköznek, akkor úgynevezett broadcast (üzenetszórási címmel ellátott csomag) üzenetet küld. Az aktív hálózati eszközök tudják, hogy a broadcast címmel ellátott csomagot mindenkinek küldeni kell, így minden interfészükön küldik azt. Hurok esetén egy ilyen csomag a végtelenségig keringhetne a hálózatban.
[2] Hurok esetén egy broadcast üzenet többször (több interfészen) is visszatérhet egy switch-ez, olyan irányból is, amerről nem lenne szabad neki. Mivel a csomag tartalmazza az eredeti küldő MAC címét, ezért a switch-nek folyamatosan más interfészt kell beregisztrálnia a MAC cím mellé.

adott LAN szegmensben egy úgynevezett root switchet (minden switch kap egy BID id-t MAC alapján, és a legalacsonyabb BID-el rendelkező switch lesz a root switch) , majd ennek a switchnek minden port-ját forwarding state-be rakja. A BID információkat egyébként – mint minden más STP-vel kapcsolatos információt – a switchek a BPDU üzenetekkel cserélik egymás között. A root switch kiválasztását követően, minden más switch meghatározza a saját Root Portját (RP), amely a legkisebb adminisztratív távolságra van a root switch-től, majd ezt a portot forwarding state-be rakja. Ezután már csak azt kell eldönteni, mely portok lesznek Designated Portok (DP).

A kialakult topológiában történő változás hatására az STP újra konvergál, ami 50 másodpercig tart. Ez az érték a max age paraméter (10x2 másodperc hello) és a forward delay összegéből (a listening és learning state időtartama) jön össze.

A Spanning Tree Protocol-nak van újabb változata is, amely a Rapid Spanning Tree nevet viseli. Mint az a nevéből is kiderül, ez a protokoll gyorsabban konvergál elődjénél. Ezt egyrészről azzal éri el, hogy csak 3x2 másodperc hello üzenetet vár mire újra konvergál, valamint eltávolították a forward delay-t, ami nagyban lerövidítette a várakozási időt.

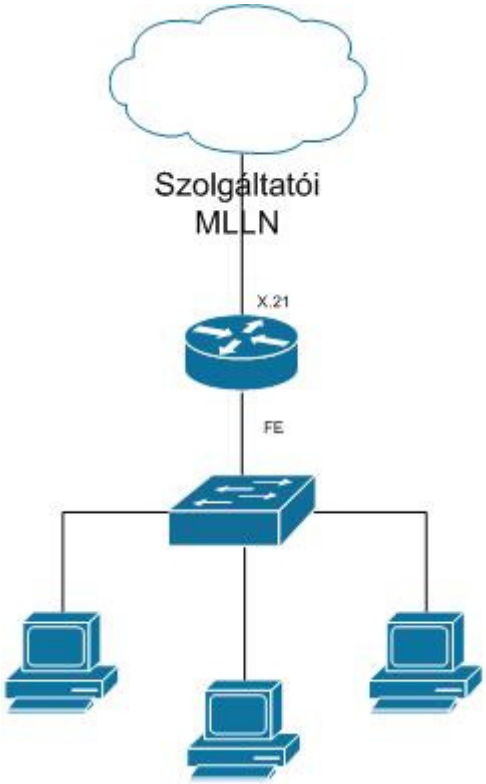
Az RSTP egyébként rendelkezik néhány plusz funkcióval is, például, megkülönböztet különböző link státuszokat, mint:

- link type point to point: switchek közötti kapcsolat
- link type shared: switch és hub közötti kapcsolat
- edge type: switch és végberendezés (például PC) közötti kapcsolat

Ezen plusz „képességével” az RSTP protokoll különbséget tud tenni kapcsolatai között, így a link type vagy az edge type linkeken le tudja csökkenteni a konvergencia idejét, amely több időt vesz igénybe egy shared típusú kapcsolaton.

2.2.3 LAN topológia bemutatása

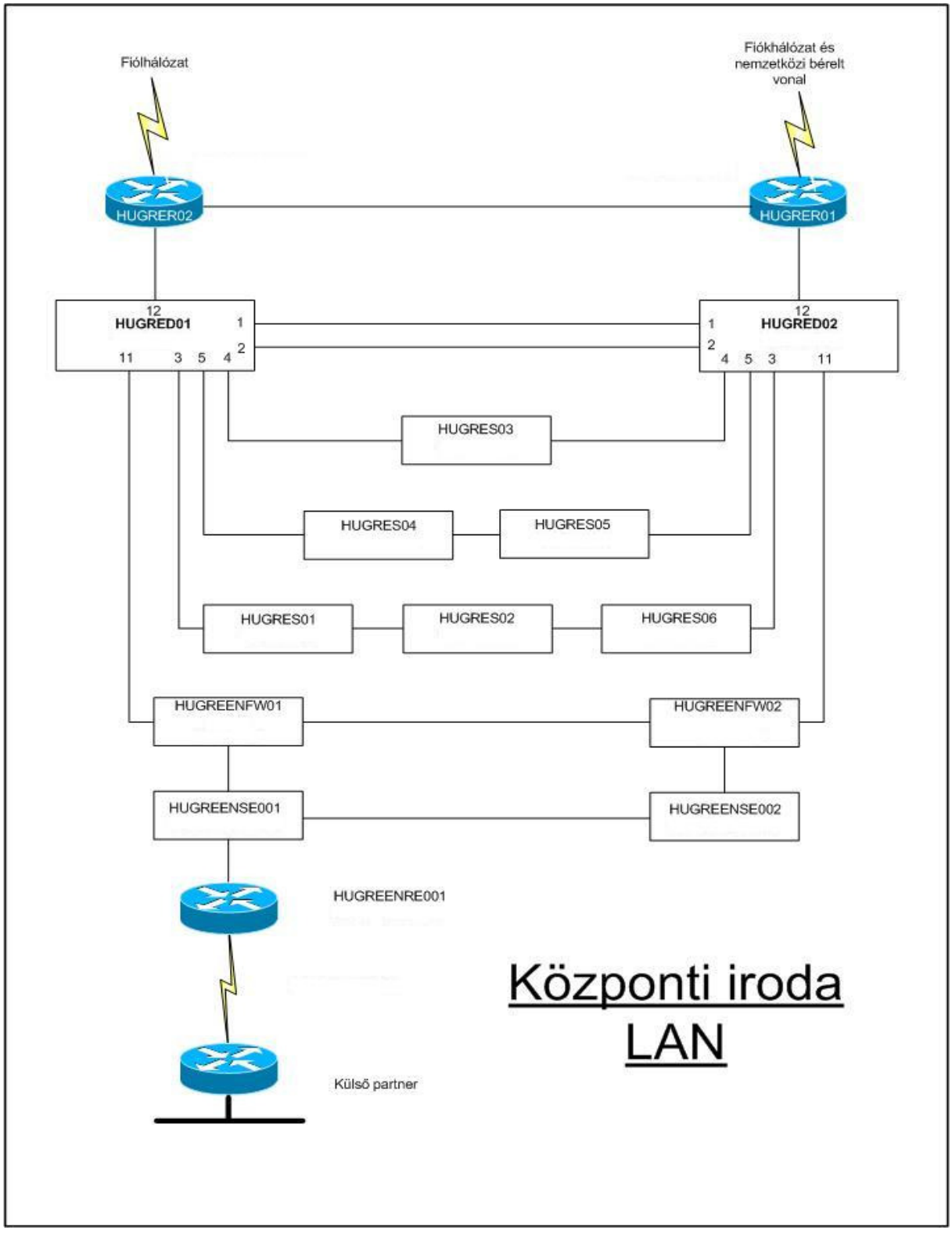
A fiókirodákban egyszerű a helyzet: a router mögött közvetlenül helyezkedik el a switch (általában egy, de van ahol kettő), a switch-en pedig közvetlenül a PC-k (5-ös ábra).



5. Fiókiroda LAN topológia

A switch és router között 100Mbit/s –os fast ethernet kapcsolatot alakítottunk ki. A nagyobb létszámmal rendelkező telephelyeken, ahol két 24 portos switch található a switch-ek közötti kapcsolatot (Gigabit ethernet interfész híján) Etherchannel konfigurációval oldottam meg. Ezzel ugyanis biztosítani lehet a két switch közötti folyamatos kommunikációt arra az esetre is, ha az egyik link inaktívvá válik.

A központi irodát viszont érdemes közelebbről megvizsgálni:



6. Head Office LAN topológia

Mint az már bevett szokás – és Cisco ajánlás - a topológiában a routerek alatt közvetlenül a layer 3-as switch-ek foglalnak helyett. Tulajdonképpen ezek fogják össze az access switch-eket, amelyekkel optikai kábellel vannak összekötve. A layer 3-as switch-ek (amelyek itt egyben core és distribution switchek is) aggregációs pontot létesítenek az access switch-ek számára, melyek így optimalizált kábelmennyiség mellett, redundáns topológiába rendezhetőek. A fent látható elrendezés azonban nem optimális. Ugyanis redundancia és sebesség szempontjából csupán a HUGRES03 kapcsoló van ideálisan bekötve. Minden access switch 2 uplink-kel kellene, hogy kapcsolódjon a layer 3-as switch-ekhez: eggyel a HUGRED01-hez, egy másikkal pedig a HUGRED02-höz, így biztosítva teljes redundanciát és optimális sebességet a broadcast domain[1]-ben.
Ha belegondolunk, hogy egy, a HUGRES02-re csatlakozó számítógép egy csomagot szeretne küldeni a HUGRES03-om mögött lévő végpontra, a csomagnak át kellene mennie vagy a HUGRES01 vagy a HUGRES04 switch-eken –attól függően, hogy a Spanning Tree melyik linket blokkolta - , terhelve ezzel ezen eszközöket. Ennek függvényében ideális LAN fejlesztés lehetne a core switch-ek bővítése GBIC kártyákkal, minden access switch-nek helyett biztosítva ezzel egy fent vázolt topológia kialakításához.

Nézzük meg most a LAN-ban lévő eszközök beállításait, természetesen a teljesség igénye nélkül, csak az érdekesebb részeket kiemelve.

A PC-k dinamikusan kapják az IP címet, egy, az Egyesült Királyságban lévő DHCP szervertől[2]. A számítógép első, hálózaton történő bekapcsolásával kéréssel fordul a DHCP szerverhez IP címért, subnet mask-ért és gateway információkért. Ezeket a szerver természetesen kiosztja – feltéve, hogy van még szabad, kiosztható dinamikus IP a tartományba – és ezzel egy időben a kérő kliens gép MAC címét is regisztrálja a kiosztott IP cím mellé. Ezzel biztosítjuk azt, hogy az IP címkiosztás ugyan dinamikus, a gépek azonban napról napra ugyan azt az IP-t kapják, megkönnyítve ezzel az adminisztrációt, és az esetleges hibajavítást.

[1] azon eszközök csoportját írja le, amelyek közül ha az egyik küld egy broadcast üzenetet, akkor a többi megkapja. Tipikusan az a hálózatrész, ahol az üzenetszórási célcímmel ellátott csomag megjelenik.
[2] olyan szerver, amely azért felelős, hogy a hálózatra kapcsolódó eszközök (node-ok) kapjanak IP címet, és a kiosztott IP cím egyedi legyen.

Természetesen vannak olyan eszközök, amelyeknél statikus IP címeket használunk. Ezek azon berendezések, amelyekhez folyamatosan kéréssel fordulnak más node-okhoz, mint például: nyomtatók, szerverek, hálózati végberendezések.
A számítógépekben lévő NIC kártyák beállítása mondhatni általánosnak, egy dolgot kivéve: minden kártyán kötelező a 100Mbps/Full duplex beállítás, amelynek segítségével a PC és switch között az információátvitel egy időpillanatban mindkét irányban lehetséges. Igaz ugyan, hogy a legtöbb NIC auto beállításon is ezt az értéket veszi fel (feltéve, hogy a switch port konfigurációban is ez a beállítás szerepel), azonban mint tapasztalatom mutatja, vannak kivételek. Nem egyszer fordult elő, hogy a PC és switch egyezkedés vége 10Mbps/Half Duplex beállítás lett, ami jelentősen megnövelte a CRC-k számát a collision domain[1]-ben, teljesen lelassítva ezzel a hálózati kommunikációt az adott switch-porton. Ezt elkerülendő konfigurálunk minden NIC kártyát és Switch access portot 100Mbps/Full Duplex-re.
Ezzel át is ugrottunk az access switch-ekre. Ezen eszközök beállításai mondhatni szokványosak.

```
!
interface FastEthernet0/24
duplex full
speed 100
spanning-tree portfast
!
```

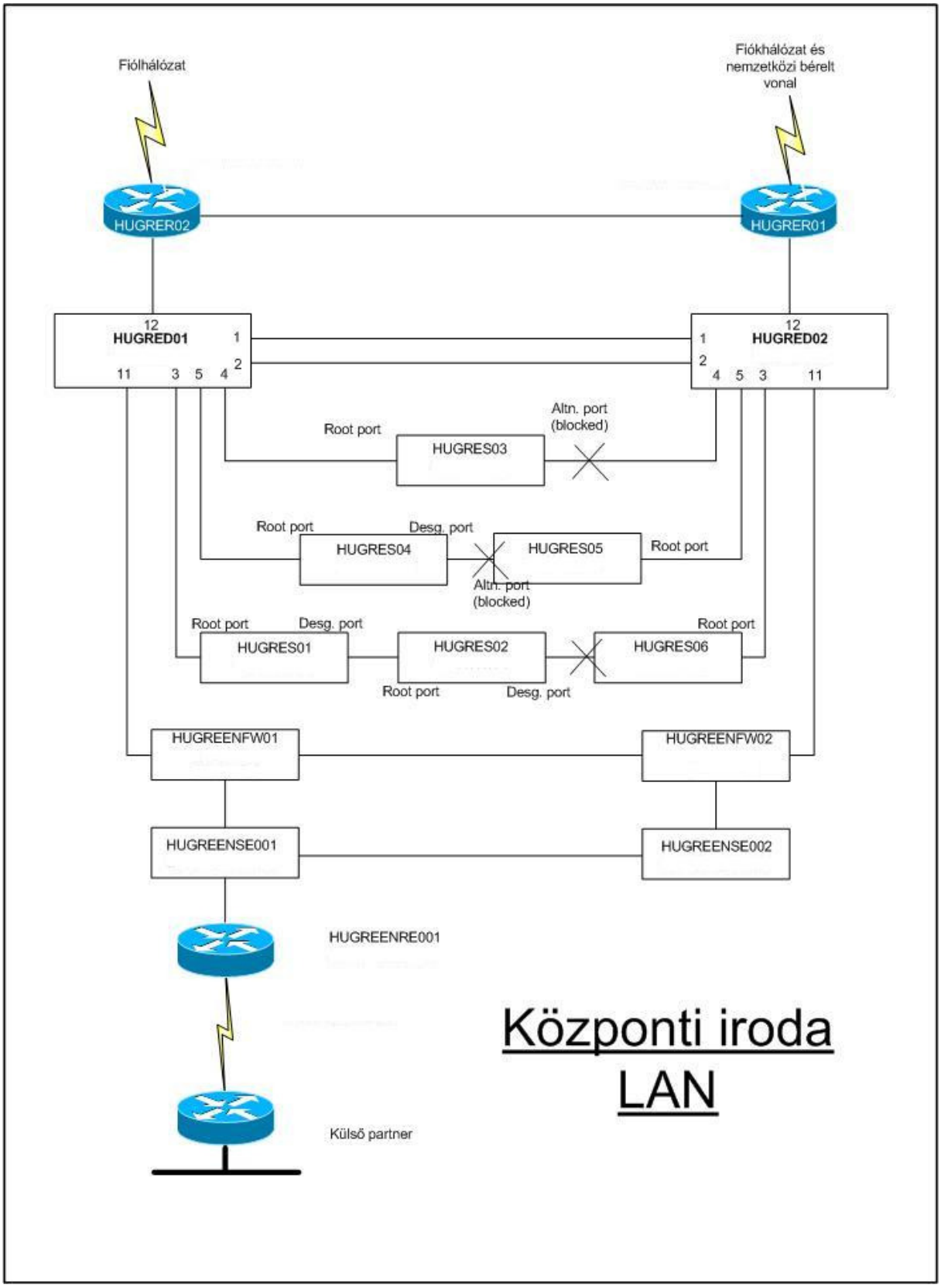
A duplexitás és sebesség fix értékre való konfigurálásán kívül még a spanning tree portfast beállítás található meg az access portokon. Ez a parancsot kötelezőnek is tekinthetjük az olyan hálózatokban, ahol redundánsan alakítjuk ki a topológiát, STP alkalmazásával. A parancs ugyanis minden olyan switch porton alkalmazni kell, amely végberendezéssel, és nem egy másik switch-el vagy bridge-el van kapcsolatban. Alkalmazását követően, a port azonnal forwarding státuszba kerül bármilyen aktivitás hatására. A parancs nélkül a switch-nek először muszáj lenne meggyőződnie arról, hogy a port Designated Port (DP), majd

[1] azon eszközök csoportja, amelyek által generált hálózati forgalom ütközhet egymással. Tipikusan az egy hub-ra kapcsolt, vagy az egy switch port-hoz csatlakoztatott eszközök tartoznak egy collision domain-be, ahol egy időpillanatban csak egy információ átvitel folyhat.

ideiglenesen listening majd learning státuszba kellene azt raknia, blokkolva ezzel a forgalmat hosszú másodpercekig.
A HUGRES05 switch beüzemelése után elfelejtettük beállítani a portfast-ot az access portokon, amely így minden egyes – hozzá közvetlenül kapcsolódó – PC bekapcsolása után több másodpercig blokkolta a forgalmat, megállítva ezzel majdnem egy egész osztály munkáját, ugyanis a hálózatra érzékenyebb applikációk timeout-ra hivatkozva hibaüzeneteket adtak. Azóta tudom, milyen nagy problémát tud okozni ezen beállítás hiánya az Edge Type[1] linkeken.

Mint az már a fenti néhány sorból kiderülhetett, a hálózatban a hurkok képződésének megakadályozására Rapid Spanning Tree protocol-t használunk. A root switch a HUGRED01 amelynek root switch révén minden interfésze root port, azaz küld és fogad adat csomagokat.
A 7-es ábrából jól látszik, mely portok vannak blokkolt státuszban, melyek a backup portok, és hol történik adat továbbítás. Port cost és switch priority nincs manuálisan konfigurálva, a protokoll a default értékeket használja.

[1] a PC (hálózati „végfelhasználó”) és switch közötti kapcsolat.



7. RSTP port státuszok a Head Office-ban

2.2.3 LAN Security

Lan security szempontból tulajdonképpen semmilyen beállítást nem alkalmazunk. Port security-t egyáltalán nem használunk. Tervezem, hogy az Edge Type linkeken BPDU Guardot állítok be, amely megakadályozza, hogy egy esetleges behatoló idegen switch-et rakjon a hálózatra. Ha a switch BPDU üzeneteket kap BPDU Guard-al ellátott porton, azt azonnal letiltott állapotba rakja.

Ezen kívül tervezem port security bevezetését is, biztosítva ezzel azt, hogy ne kerülhessen ellenőrizetlenül semmilyen eszköz a hálózatra. A beállítás részleteit tekintve, egy MAC címet konfigurálunk majd, a port-security violation default módban hagyjuk (idegen MAC érzékelésekor „kikapcsolja” az interfészt), és sticky learning-et állítunk be (a switchek kihasználtsága pillanatnyilag majdnem maximális, rengeteg energia és idő lenne egyenként MAC címeket konfigurálni a portokon).

3. Fejlesztést motiváló tényezők

Az eddigiekben vázolt bérelt vonali hálózat mellett kissé elszaladt az idő. Strukturálisan, redundancia szempontból – egy-két hibától eltekintve – jónak mondható, szinte minden más szempontból viszont fejlesztésre szorul.

Az első és legnagyobb probléma a sebesség. 256Kbps sávszélességen ugyan még a kisebb hálózati forgalmat generáló applikációk – mint például a banki rendszerek, amelyek telnet alkalmazások, és AS400 szerverrel kommunikálnak– viszonylag jól elfutnak, azonban egy sokkal nagyobb forgalmat generáló levelező kliens már igencsak nehézkesen kommunikál még a fiókokban átlagosnak mondható 4-6 fős felhasználói szám mellett is. A leginkább kritikus alkalmazás azonban a Microsoft Excel. Mivel a felhasználók dokumentumaikat a központban lévő szervereken tárolják, ezért azok olvasása és írása is hálózatot igényel. Nagyobb Excel fájlok esetén nem volt ritka az 5-8 perces várakozási idő, elég nagy elégedetlenséget kiváltva ezzel a felhasználók körében.

De nem csak ebből a szempontból volt kevés a 256Kbps. Mivel a Windows-t System Management környezetben üzemeltetjük, és az applikációkat hálózaton terjesztjük a munkaállomások között – önkicsomagoló formában – ezért a 256Kbps igencsak korlátolta lehetőségeinket. Ha éppen rossz időpontban küldtünk ki egy McAfee engine-t, amely nem a legújabb vírus definíciós fájlal rendelkezett, akkor egy fiókban lévő összes gép egyszerre kezdte el azt tölteni a központban lévő EPO szerverről, szinte használhatatlanná téve ezzel a fiókiroda linkjét.

Másik nagyon fontos motiváló tényező a közeljövőre tervezett IP Telefónia rendszer bevezetése. Ehhez a nagyobb sebességen kívül egy olyan rendszerben kellett gondolkodnunk, amely egy sokkal jobban konfigurálható, skálázható Quality of Service-el rendelkezik. Azáltal, hogy egy IP-VPN hálózatban a QoS sokkal jobban skálázható, sokkal jobb minőségű hang vagy videó átvitel valósítható meg. És akkor még nem szóltunk a nagyobb rendelkezésre állásról, bár e tekintetben a bérelt vonalnál sem volt különösen nagy probléma.

Végül de nem utolsó sorban pedig egy Ip VPN hálózat üzemeltetése olcsóbb, így a meglévőnél jóval gyorsabb hálózatot kapunk kevesebb pénzért.

A fentieket figyelembe véve az MPLS hálózat kialakítása logikus lépés. A következő részben a fent részletezett hálózatot migráljuk át MPLS technológia alá. A fejezet a technológia

bemutatásával kezdődik, ahol a teljesség igénye nélkül szó lesz az MPLS gerinchálózat működéséről (szolgáltatói oldal), valamint használatának előnyeiről.

4. Választott fejlesztési irány (MPLS) részletes bemutatása

A Multiprotocol Label Switching (MPLS) nagyon népszerű napjainkban, nem véletlenül. Kialakításakor egy, az ATM pozitív tulajdonságaival rendelkező (skálázhatóság, Quality of Service), valamint az IP egyszerűségét, rugalmasságát is magában hordozó technológia kialakítása volt az elsődleges cél. Ezen tulajdonságok tették ezt a technológiát elterjedté az első időkben csak nagyobb hálózatok kialakításánál, majd a későbbiekben – az MPLS VPN megjelenésével – kisebb rendszereknél is. Az MPLS VPN[1] megjelenése biztosította ugyanis azt, hogy változó layer 2 fölött (Ethernet, PPP, ATM stb.) hozzanak létre virtuális magánhálózatokat. Ezen hálózatok rendelkeznek a LAN technológiában már megszokott VLAN tulajdonságokkal, úgy, mint flexibilitás és kiterjeszthetőség, mindezek mellet azonban még egységesen kezelt QoS-t és közös erőforrás elérést is képesek biztosítani. (A VPN technológiát e dolgozat keretei között nem részletezem)

Az MPLS technológia

Az MPLS megszületésének egyik legfőbb oka a routing egyszerűbbé tétele volt. A már korábban létező multiservice hálózatokban is használtak viszonylag gyors konvergenciájú protokollokat, és QoS-t (queuing, traffic-shaping), ezek azonban nagy erőforrás igényűek, jelentősen terhelik a processzort, viszonylag nagy szakértelem és körültekintéssel használhatóak. Hogy miért? Gondoljuk végig, a router minden egyes csomagnál véghez viszi a következő műveletsort:

1. Fogadja a bejövő csomagot, és esetleg elő feldolgozást (pl. IP precedencia átállítás, policy routing), végez.

[1] VPN: Virtual Private Network, vagy virtuális privát hálózat.Egy „hordozó” (akár publikus) hálózaton működő virtuális, titkosított csatorna, amely csak a VPN tagjai számára látható, a hálózaton jelen lévő többi felhasználó számára nem.

2. Meghozza a routing döntést

3. Elvégzi a klasszifikációt, azaz a megfelelő forgalmi osztályokba sorolja a beérkező csomagot. Ennek során, a cél címen kívül a forrás címet, az IP-be ágyazott protokoll típusát (TCP/UDP/RTP), annak protokoll portjait vizsgálja. Ez egy elég komplex feladat, hardware-rel nem támogatható.

4. Elvégzi a kimenő interfészen a megfelelő sorba állítást a kívánt QoS megvalósítása érdekében.

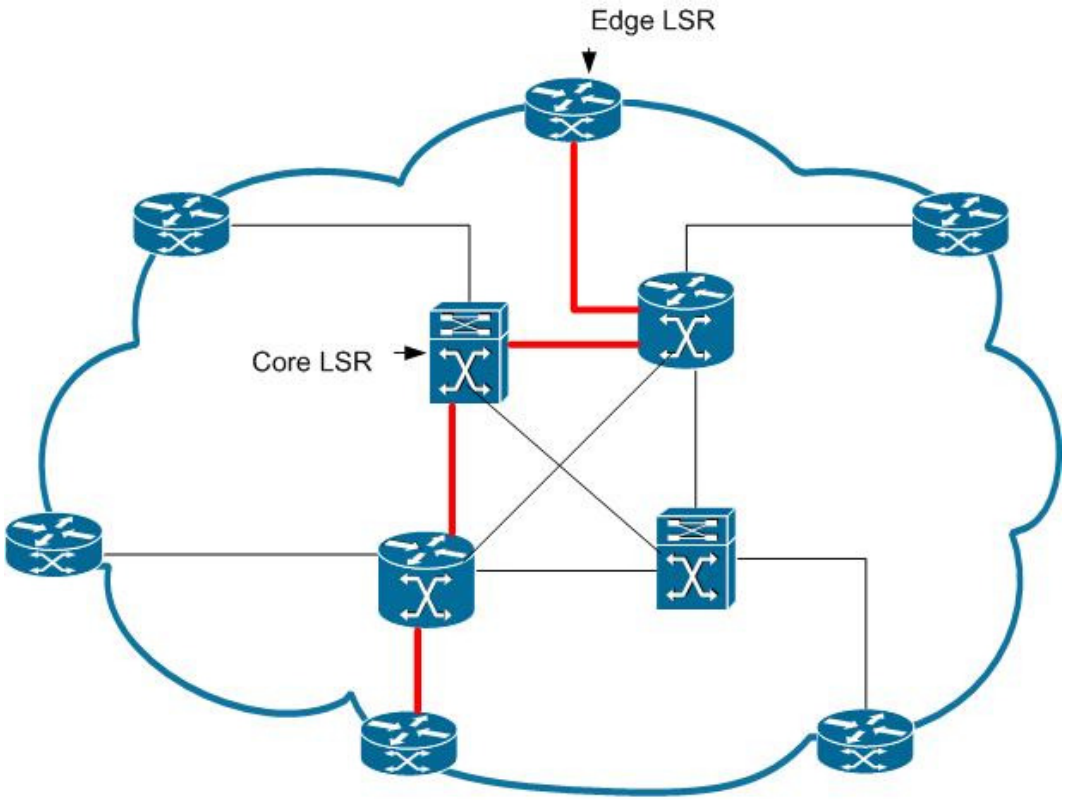
A fentiek átgondolásával beláthatjuk, hogy nagyobb méretű hálózatokban a nagy routing csomópontokban az útválasztó eszközök túlterheltek, esetenként nem is létezik akkora kapacitású eszköz, ami alkalmas lenne a feladatra.

Ezen probléma kiküszöbölése céljából, azaz a skálázhatóság megteremtése miatt hozta létre a Cisco a tag switching-et, amely mára MPLS néven szabványos protokollá vált. Az MPLS kialakítás céljai:

- Egy nagy kiterjedésű, sok kapcsolattal rendelkező IP gerinchálózatban ne kelljen nagy routing táblák alapján továbbítani a csomagokat, mivel ez nagy CPU igénybevétellel jár
- Gyors re-routing hiba esetén
- Egyszerű konfiguráció
- Minél többfajta hordozó hálózaton működjön
- VPN lehetőségek

A kialakítás lényege az, hogy a hálózatunkat alkotó, immáron label switch routernek (LSR-nek) nevezett eszközöket két csoportba soroljuk:

- a hálózat szélén elhelyezkedő edge LSR-ek végzik a klasszifikációt,
- a hálózat belsejében lévő core LSR-ek pedig már csak a csomagok továbbítását végzik



8. példa egy MPLS gerinchálózatra

A gyors routing szempontjából az edge LSR felcímkézi a csomagokat, amely címke a gerinchálózatban lévő core LSR-ek számára iránymutató mind QoS, mind továbbítási szempontból. A core LSR kizárólag ezen fix hosszúságú szám alapján hozza meg a routing döntést. Mivel a csomagot a címke a teljes core hálózaton elkíséri, és kizárólag ez azonosítja, ezért nagyon fontos az egyediség, amelyért a Label Distribution Protocol (LDP) felelős (a címkék kiosztását is ez végzi).

Jól megfigyelhető az ATM-el való hasonlóság:

- Az MPLS LSP-ket (Label Switch Path) állít fel, amelyek tulajdonképpen olyan virtuális csatornák, amelyeket már az ATM hálózatoknál is megfigyelhettünk. Az ábrán jól látszik, hogy ezen virtuális csatorna két Edge LSR „külső” interfésze között helyezkedik el, és az LSP-k továbbítási tábláinak bejegyzéseiből áll össze.

- A csomag továbbítás az MPLS-nél is a felépített csomagtovábbítási tábla (label switch table) alapján történik, ahogy az ATM esetén is. A tábla csak az input és output interfészt és címkét tartalmazza (az ATM-mel ellentétben azonban a címkének itt nem csak lokális jelentősége van).

A fenti ábrán háromfajta eszközt látunk:

- router alapú edge LSR-t
- router alapú core LSR-t
- ATM switch alapú core LSR-t. Az utóbbiban a kapcsolást a tag switch controller végzi

Ezen eszközöknél a csomagok továbbítása a label switching tábla alapján történik, így az LSP is áthalad rajtuk.

A gerinchálózatban, vagy éppen a szolgáltatói és a felhasználó autonóm rendszerek közötti útvonal információk cseréjére az egyik legelterjedtebb protokoll, a Border Gateway Protocol (BGP).

BGP

A Border Gateway Protocol-t főleg autonóm rendszerek határán használják olyan információk cseréjére, amelyek segítségével az útválasztó eszközök felépíthetik routing tábláikat. A protokoll ezen formáját external BGP-nek nevezik, és habár ez a protokoll legfőbb alkalmazási területe, néhány nagy hálózatban IGP[1]-ként is használják.
A BGP egy TCP[2] alapú protokoll, ahol a célport a 179-es, a helyi port pedig véletlenszerűen kerül kiosztásra. A TCP biztonságosabbá tétele érdekében használhatunk MD5 autentikációt, amely megakadályozza, hogy egy, a két forgalomirányító közzé elhelyezett idegen eszköz esetleg hamis routing információkat terjesszen, vagy információkhoz jusson.

[1] Interior Gateway Protocol: egy autonóm rendszeren belül elhelyezkedő útválasztó eszközök közötti routing információ cseréért felelős protokoll.
[2] Transmission Control Protocol: szállításért felelős protokoll. Egyik fontos tulajdonsága a megsérült csomagok érzékelése és azok javítása.

Az internet protokolljaként is ismert BGP-nek manapság a 4-es verziója használatos. A BGP-t használó útválasztók Path Vector routing algoritmust használva nem csak az alhálózat helyét ismerik, de azon AS-ek számát is, amelyeken keresztül a cél a legideálisabb költséggel megközelíthető. Ez nagyon fontos tényező a routing hurkok kiküszöbölése szempontjából, ugyanis a protokoll úgy segít elkerülni ezek kialakulását, hogy minden olyan bejövő routing információt eldob, amely a saját, lokális AS számát tartalmazza.
A protokoll útvonal információk megszerzéséhez és továbbításához ún. update üzeneteket használ, amelyek segítségével csak a topológiában bekövetkező változásokat kommunikálja. Ilyenkor egyfelől bejelenti milyen új útvonalat ismert meg, másfelől pedig közli, milyen általa ismert útvonalat von vissza. Ezek után kiválasztja a legjobb útvonalat egy alhálózat elérésére, és ezt teszi bele a routing táblába. Ahhoz, hogy biztosan a legjobb route kerüljön a táblába, a routing információknak meglehetősen sok attribútumot kell tartalmaznia. Ezek a következők:

- AS Path: azon AS-ek listáját tartalmazza, amelyeken a routing információ keresztül haladt. A route továbbküldése előtt az eszköz saját AS-e is bekerül a listába.
- Community: autonóm rendszerek csoportját foglalhatja egységbe, amelyek azonos tulajdonságokkal rendelkeznek, például hálózat, vagy bármilyen fizikai tulajdonság tekintetében.
- Local_Pref: az egy AS-hez tartozó szomszédok által küldött routing információkból melyiket tartja a legjobbnak a router, azaz melyik a legjobb útvonal egy alhálózat eléréséhez a helyi AS-ből.
- Multi_Exit Discriminator: az mondja meg, hogy egy AS-nek melyik a preferált belépési pontja.
- Next Hop: azon BGP router-nek az interfész IP címét tartalmazza, amelytől az üzenet származik.
- Origin: azt mondja meg, hogy egy route hogy került be a BGP routing táblába. Ez lehet: IGP, EGP vagy Incomplete. A preferált az IGP, ezután pedig az EGP.

A fenti attribútumok segítségével könnyen kiválasztható a legjobb útvonal.
A BGP router alapértelmezésben minden 60 másodpercben szkenneli a next-hop routert, annak elérhetőségét és állapotát, hogy validálhassa vagy éppen megváltoztathassa az ideális

útvonalait. Ennek nagy hátránya lehet, hogy két szkennelési idő között bármilyen IGP instabilitás vagy hálózati hiba hurkokat okozhat a hálózatban.

5. A tárgyalt hálózat migrálása MPLS környezetbe

Most, hogy tisztában vagyunk az MPLS fogalmával, működésének hátterével, valamint a használni kívánt útválasztó protokoll legfontosabb tulajdonságaival, elkezdhetjük a migrációt. A következőkben a rendszerterven keresztül eljutunk a megvalósításig, kiemelve a migráció és az új rendszer fontosabb elemeit.

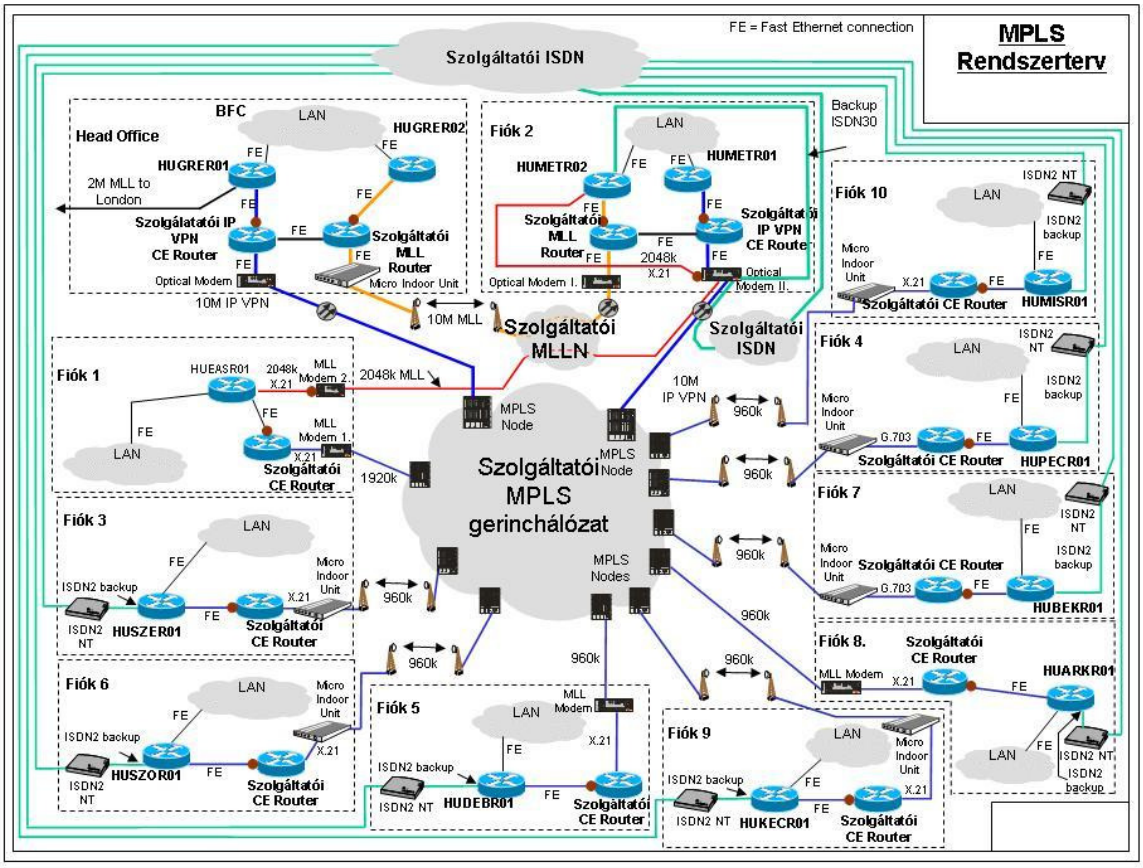
5.1 Rendszerterv

A rendszerterv segítségével bepillantást nyerhetünk az új hálózati struktúra kialakításába, másodlagos útvonalak tervezésébe, valamint felületesen a rendszer működésébe.

5.1.1 Topológia

Mint azt már fentebb részleteztem, az új technológiára való átállás elsődleges célja a sávszélesség növelése, valamint felkészülés egy IP telefónia rendszer bevezetésére, amely szempontból az új technológia által kínált jobb QoS szinte elengedhetetlenül fontos.

A rendszerterv elkészítésénél egyik fő szempont maradt a redundancia megtartása, sőt ha lehet, fokozása. A 9-es ábrán látható rendszerterv már a végleges topológiát mutatja, amely számos változtatáson esett át az eredeti elgondoláshoz képest.



9. MPLS Rendszerterv

Első lépésben fel kellett vázolnunk a vezetőségnek néhány lehetőséget mind sebesség, mind redundancia szempontból. Nyílván az ár a sebesség és a redundancia megbízhatóságának növelésével arányosan nő. Végül – mint az a topológiából is látszik – 1Mb-es access linkeknél maradtunk. Mivel alapesetben minden forgalom a Head Office-on megy keresztül (vagy közvetlenül az itt található szervereket címzi) ezért ez a végpont 10Mb-el csatlakozik az MPLS felhőhöz. Ugyancsak 10Mb-et kapott a 2-es fiókiroda, amelynek optikai access linkje backup-ként szolgál abban az estben, ha a Head Office elvesztené az optikai linkjét. Ekkor a fiókirodák és Head Office, vagy a fiókirodák, és Anglia közötti kommunikáció a 2-es telephelyen keresztül valósul meg, egy közvetlen, 10Mb-es bérelt vonal segítségével a két központi iroda között. A backup vonalakat tekintve a fiókirodáknál megmaradt az eredeti ISDN2 vonal, amely két csatornájával 128Kbit/s sebességet biztosít arra az esetre, ha a telephely elvesztené a kapcsolatot az MPLS felhővel. Felmerült egy esetleges fejlesztés ezen a téren is – az ISDN technológiát ADSL-re cseréltük volna – azonban mivel eddig nem volt

gond az ISDN technológiával, és a legfontosabb applikációk (banki rendszerek) 128Kbit/s sebességen is működő képesek, ezért ezen a téren nem változtattunk.

Az access linkek kiépítésénél – a technológia jellegéből adódóan – egy új 2811-es, szolgáltató által kihelyezett és üzemeltett, úgynevezett CE (Costumer Edge) router is helyett kapott a telephelyek rack-szekrényeiben. A két CE router ethernet interfészen kapcsolódik, és a linken természetesen /30-as IP tartományt alakítunk ki. A két központi telephelyen, a végponti CE routerek hibájából eredő esetleges leállásokat elkerülendő, a szolgáltató kérésünkre 2 routert telepít, és a két router között fastethernet kapcsolaton keresztül Hot Standby Routing Protocol-t implementál. A HSRP biztosítja azt, hogy a két router tulajdonképpen egy IP cím alatt látszódik majd a helyi hálózatból (gateway), így a plusz router miatt nem kell konfigurációt módosítani.

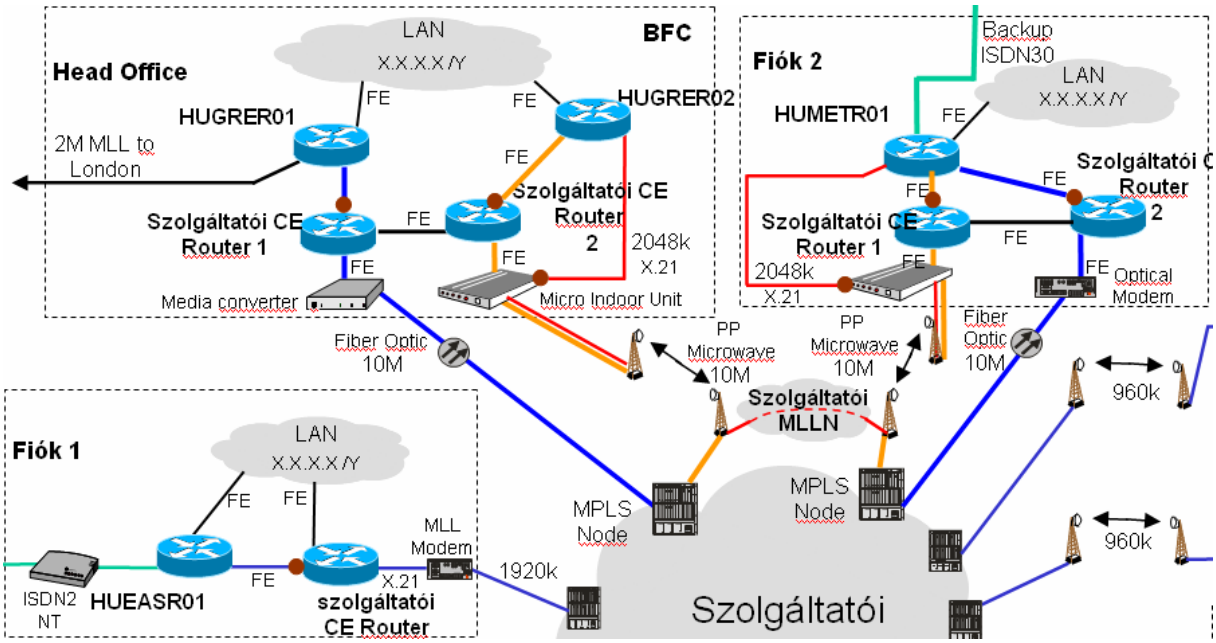
A CE és PE (Provider Edge Router) közötti link viszont X.21 felületen érhető el. Az Access link típusa nagyban függ a telephely földrajzi elhelyezkedésétől. Ahol a szolgáltató nem tud kábeles technológiát biztosítani, ott mikrohullám segítségével oldja meg a CE és PE forgalomirányítók közötti nagy sebességű kommunikációt.

Alapesetben a telephelyenkénti két Costumer Edge router-re nem lenne szükség, a HSBC viszont nem szerette volna átengedni – az esetlegesen világméretű hálózatába is betekintést engedő – végponti útválasztóinak felügyeletét a szolgáltatónak. Ennek természetesen vannak előnyei és hátrányai. Nagy előnye, hogy egy esetlegesen felmerülő probléma esetén nem kell várnunk a szolgáltatóra, a probléma elhárítását mi magunk is megkezdhetjük (ha az eszközben van a hiba). Ezzel szoros összefüggésben van, hogy bármilyen konfiguráció módosítást is késlekedés nélkül képesek vagyunk eszközölni (természetesen csak abban az esetben, ha az a szolgáltató felé, vagy felől jövő routingot, kommunikációt nem érinti).

Hátránya viszont, hogy plusz eszközként növeli a hibafaktort, valamint az implementációt is nagyban megnehezíti (a későbbiekben kiderül, miért).

Külön szót kell ejtenünk a két központi telephely, valamint a bérelt vonali hálózatnál is kiemelt szereppel rendelkező 1-es fióktelep kapcsolatáról. Mint azt már fentebb említettem a Head Office és a 2-es fiókiroda is 10Mb sávszélességű optikai technológiára épülő kapcsolattal rendelkeznek a szolgáltatói gerinchálózat felé. Az eredeti terv itt két 10Mb adatátviteli sebességű linket tartalmazott (10-es ábra), a második azonban (ami a fenti ábráról már hiányzik), mint a későbbi tesztjeink során kiderült, nem tudták biztosítani a várt szintű

redundanciát. Ez a másodlagos link mikrohullámú kapcsolaton volt biztosítva, és mintegy másodlagos access link-ként erősítette volna a redundáns kapcsolatot a gerinchálózat felé.



10. Az átalakított topológia

Ez az elgondolás azonban megbukott a tesztek során, ugyanis a redundancia tesztnél kiderült, hogy az optikai link elvesztése esetén a használt (később részletezett) routing protokoll nagyon lassan konvergál át a mikrohullámú kapcsolatra (mintegy 5 perc), így ezen link megtartása tulajdonképpen értelmetlenné vált. (A lassú konvergencia okára egy későbbi fejezetben visszatérek.)

A teszt eredményeképpen hoztuk meg azt a döntést, hogy a mikrohullámú kapcsolatot átalakítjuk a gerinchálózattól teljesen független bérelt vonali technológiává, direkt kapcsolatot kialakítva ezzel a két központi telephely között.

A topológiára pillantva kiderül, hogy az 1-es fiókiroda kapcsolódása is eltér a többi telephelyen megszokottétól. Mivel ez a végpont már a bérelt vonali hálózat idejében is különleges pozícióban volt – ez volt a központi telephelyek közötti redundancia „háromszögnek” az egyik csúcspontja – így nem rendelkezett ISDN2 kapcsolattal (így az itt

található router-ben BRA kártya sem volt). Ezért úgy döntöttem, hogy mivel ez egy nagyobb létszámmal rendelkező fióktelep, így az eredetileg a Head Office és a 2-es fióktelep közötti 2Mb-es bérelt vonalat a Head Office-ból áthelyezem ide, így biztosítva redundaciát.

5.1.2 QoS (Quality Of Service)

Az adatforgalom priorizálása DSCP bitek segítségével történik, és a mi eszközeink végzik. A szolgáltatói router minden esetben a mi eszközeinktől kapott DSCP paraméter alapján kezeli le a priorizálást, és gondoskodik annak megfelelő érvényesítéséről a teljes MPLS IP hálózaton keresztül.

5.1.3 IP Címzési struktúra

A bérelt vonali LAN IP cím tartományok megtarthatóak, ami azt jelenti, hogy a bérelt vonali hálózatnál használt, publikus IP cím tartományba eső címek maradhatnak. Mint azt már fent említettem, a szolgáltató és a HSBC útválasztói között /30-as tartományok kerülnek kialakításra.
Természetesen itt célszerű a már meglévő WAN tartományoktól eltérő címeket választani, az átállás (párhuzamos üzem) könnyebb kivitelezhetőségének érdekében.

5.1.4 Routing Protocol

A routing protocol a szolgáltató és a HSBC router-ek között Border Gateway Protocol (BGP). A protokollhoz konfigurált AS-számot egy, a HSBC központban működő hálózat támogató csoporttól kapjuk. Itt tartják nyílván a HSBC világméretű hálózatában a használt és használaton kívüli autonóm rendszerek azonosítóit. HSBC elvárás továbbá, hogy a BGP scan-time paraméter a legkisebb értékre, azaz 5 másodpercre legyen állítva, a lehető legkevesebb esélyt adva ezzel ideiglenes routing hurkok kialakulásának.

A protokoll mellé MD5 autentikációt implemetálunk, ami azt jelenti, hogy a BPG által használt bármilyen TCP üzenet csak akkor cserélődhet ki a két router között, ha az autentikáció sikeres volt.

5.2 Megvalósítás

A terv felállítása után következik a megvalósítás. A fejezet célja, hogy bemutassa milyen intézkedésekre van szükség ahhoz, hogy az implementáció gördülékenyen menjen, valamint, hogy az esetlegesen felmerülő problémákra – amennyire lehet – felkészüljünk. A fizikai megvalósításon túl szó lesz a BGP implementálásáról kiemelve a fontosabb részleteket.

5.2.1 Fizikai implementáció

A megvalósítás során az egyik fő szempont a folyamatosság. Mivel a fiókirodák munkáját nem szeretnénk megszakítani, ezért az implementáció éjszakánként zajlik. Felállítottam egy sorrendet, amelyben a központi telephelyek állnak az első helyen – természetesen ezeket kell először implementálni – ezután éjszakánként két fióktelepet állítunk át az új technológiára. A Head Office-ban lévő központi router-ekben ez alatt az idő alatt biztosítani kell a két technológia közötti átjárhatóságot, ugyanis míg néhány fióktelep már az új MPLS gerinchálózatot használja, addig a többiek még a régi, bérelt vonali technológiával érik el a központi telephelyet. Mivel az esetleges, új hálózatnál fellépő hibák miatti üzletmenetben bekövetkező megszakításokat szeretnénk elkerülni, ezért az implementáció teljes befejezéséig, valamint egy sikeres redundancia teszt elvégzéséig a bérelt vonali kapcsolat minden fiókban meghagyjuk. Ezt könnyedén megtehetjük, mivel a telephelyek ethernet interfészen kapcsolódnak a szolgáltatói CE routerekhez, ezért a serial linkek a helyükön maradhatnak. Így az új MPLS linken történő bármilyen hiba esetén percek alatt visszaállhatunk a bérelt vonalra. Annak érdekében, hogy a reziliencia 100%-os biztonsággal fenntartható legyen, az utolsó telephely amelyet implementálunk az 1-es fióktelep. Ugyanis mindaddig, amíg egyetlen fiók is bérelt vonalon kapcsolódik a Head Office-hoz, ez egy alterantív irány az elsődleges 2Mb-es nemzetközi bérelt vonal elvesztésekor.
Az implementáció során az első lépés a központi routerek IOS upgrade-je. Ezeket még az új hálózat konfigurálása előtt kell megtenni, csak ezek után lehet BGP routingot konfigurálni.

Az upgrade-re minden telephelyen szükség van (a régi verzió nem támogatja a BGP protokollt), ezeket az implementáció estéjén, közvetlenül az új routing konfiguráció elkészítése előtt hajtjuk végre.
Az upgrade után a két CE router közötti kapcsolat felépítése következik. Itt figyelni kell, hogy a szolgáltató minden telephelyen implementálja CE routereinek ethernet interfészén a 100Mb Full Duplex beállítást, különben a két router közötti kapcsolat nem épül ki. A szolgáltató preferált beállítása egyébként az auto negotiation, és azt az elvet vallja, hogy így mindig létrejön a kapcsolat, és az egyezkedés vége 100Mb Full Duplex. Erre én sok ellenpéldát láttam már, éppen ezért kértük a fix 100 full beállítást.
Gondoskodni kell továbbá arról, hogy a két CE router közötti MD5 autentikáció azonos paraméterekkel be legyen állítva (jelszóra különös tekintettel), ugyanis ennek hiányában sem alakul ki szomszéd viszony a két eszköz között.

Ezután következhet a tényleges BGP konfiguráció.

5.2.2 BGP implementálása

A routing protocol konfigurálása a központi telephelyen a leghangsúlyosabb, ugyanis nagyon lényeges, hogy mely routokkal rendelkeznek a központi forgalomirányító eszközök.
A HUGRER01 router-en végrehajtandó BGP konfiguráció:

```
!
router bgp 64758
 no synchronization
 bgp log-neighbor-changes
 bgp scan-time 5
 network 145.16.1.0 mask 255.255.255.252
 network 145.16.255.1 mask 255.255.255.255
 redistribute eigrp 2
 neighbor 145.16.1.2 remote-as 65077
 neighbor 145.16.1.2 password 7 082318795A1F06234F5903023D
 neighbor 145.16.1.2 timers 15 45
 neighbor 145.16.1.2 allowas-in
```

```
 neighbor 145.16.1.2 soft-reconfiguration inbound
 neighbor 145.16.1.2 route-map Out-To-MPLS out
 no auto-summary
!
```

A router bgp 64758 paranccsal aktiváljuk a BGP routing protokollt a 64758-as azonosítóval rendelkező autonóm rendszerre, amelynek ezzel a HUGRER01 eszköz „tagjává" válik. Nagyon fontos, hogy ez a szám egyedi legyen, és a HSBC hálózatában sehol máshol ne legyen ugyan ezzel az azonosítóval rendelkező AS.

A no synchronization megakadályozza, hogy a BGP és az Interior Gateway Protocol (jelen esetben EIGRP) szinkronizáljon egymással, vagyis a BGP router-nek nem kell megvárnia, hogy egy belső route validálást kapjon az IGP-től mielőtt használ/hirdet egy routot. Tulajdonképpen szinkronizációra a két útválasztó között csak abban az esetben lenne szükség, ha lenne egy belső router, amely csak IGP protokollt használ, és alapesetben nem ismeri a BGP routjait. Ez a mi esetünkben nem áll fent, ugyanis a hálózatunkban nincs olyan forgalomirányító (a HUGRER01-nek sincs olyan szomszédja) amely ne futtatna BGP protokollt, így ne ismerné a BGP által hirdetett útvonalakat. Ezáltal szinkronizációra sincs szükség.

Míg az EIGRP protokollnál a szomszéd viszony változásokat nem jegyeztük (no eigrp log neightor changes) addig itt készítünk ezen változásokról bejegyzéseket a log fájlban. Bekapcsolásának oka, hogy BGP routereink főleg a szolgáltató által felügyelt és menedzselt eszközökkel állnak szomszéd viszonyban, így a legbiztonságosabb az, ha feljegyzéseket készítünk minden változásról, ami a két CE router között történik.

A BGP scan time beállításról már volt szó fentebb. Ez az érték alapértelmezésben 15 másodperc, ami azt jelenti, hogy a router 15 másodpercenként validálja a next-hop routereket. Ezt a mi esetünkben csökkentettük 5 másodpercre a bgp scan-time 5 paranccsal, ezzel lecsökkentve annak esélyét, hogy ideiglenes routing hurkok alakuljanak ki két szkennelési periódus között.

A két network parancsal engedélyezzük a BGP-t azon interfészeken, amelyek a 145.16.1.0 /30 és a 145.16.255.1 /32 –es hálózatban vannak. Az első a szolgáltató CE forgalomirányító felé néző ethernet interfész, a második pedig egy loopback interfész.

A redistribute eigrp 2 paranccsal redisztributáljuk a routokat a 2-es AS-ből. Ez elengedhetetlenül fontos, ugyanis a helyi BGP routerek így tanulják meg a távoli (UK-ban lévő) alhálózatokhoz vezető útvonalat, amelyet a parancs segítségével a 2-es AS-ben futó IGP (jelen esetben EIGRP)-ből redisztributálunk.
A következő néhány sorban a HUGRER01 router BGP szomszédjára (szolgáltatói CE) vonatkozó parancsokat találunk.

```
!
neighbor 145.16.1.2 remote-as 65077
neighbor 145.16.1.2 password 7 082318795A1F06234F5903023D
neighbor 145.16.1.2 timers 15 45
neighbor 145.16.1.2 allowas-in
neighbor 145.16.1.2 soft-reconfiguration inbound
neighbor 145.16.1.2 route-map Out-To-MPLS out
!
```

A remote-as parancs segítségével a 145.16.1.2 IP címmel rendelkező, 65077-es AS-hez tartozó eszközt regisztráljuk a BGP szomszéd táblában. Mivel az AS szám nem a router sajátja, ezért ez az eszköz egy külső BGP szomszéd-ként kerül bejegyzésre:

```
„
HUGRER01>show ip bgp neighbors
BGP neighbor is 145.16.1.2,  remote AS 65077, external link
”
```

A fentebb már szintén részletezett MD5 autentikációt a neightbor password parancs segítségével állíthatjuk be. A parancs és a jelszó közzé írt hetes paraméterrel titkosítjuk a jelszót, így az a running vagy startup konfigból nem olvasható ki.
A BGP peer-ek elérhetőségét ellenőrző keepalive[1] és holdtime[1] értékeke beállítására szolgál a neighbor timers parancs. Az első érték a keepalive, a második pedig a holdtime. Az

[1] Keepalive: a Cisco eszközök keepalive üzenetekkel ellenőrzik, hogy a velük közvetlen kapcsolatban lévő Cisco eszközök elérhetőek e. Ezen érték beállítása mondja meg, hogy milyen gyakran küldjön az eszköz keepalive üzeneteket.

alapértelmezett értékek keepalive-nál 60, holdtime-nál pedig 180 másodperc. Ezt kicsit soknak találtuk, ezért csökkentettük 15 és 45 másodpercre.

Alapesetben a routing hurkok elkerülése érdekében a BGP router-ek elvetik az olyan útvonal információkat, amelyek tartalmazzák a saját AS számukat. A neighbor allowas-in parancs segítségével azonban ez a „viselkedés" megszüntethető, és a parancs után megadhatjuk, hogy hányszor fogadja el az eszköz a saját AS számát is tartalmazó routot.

Hasznosnak tartottam implementálni a soft-reconfiguration inboud parancsot, ugyanis ezen parancs alkalmazásával egy BGP újra konfiguráció esetén sem vesznek el a jelenlegi routing frissítések. Alapesetben ugyanis, ha változtatjuk a BGP szabályrendszert, akkor az összes bejövő (jelenlegi) frissítés elvész. Annak érdekében, hogy ún. dinamikus BGP konfigurációt hajthassunk végre egy BGP routeren, tárolnunk kell az összes, szomszédtól érkező BGP információt, amelyeket az eszköz használni tud egy esetleges újra konfiguráció alatt és után. Az új beállítások implementálását követően, ezen tárolt adatok feldolgozásra kerülnek az új szabályrendszer szerint. Mivel ezen információk az eszköz memóriájában tárolódnak, ezért a parancs hatására szignifikánsan megnő a memóriahasználat. A HUGRER01 routeren tehát elméletileg van lehetőség ún. „soft reconfiguration"-re.

Route map-ekről már volt szó az EIGRP konfiguráció kapcsán. Hatását tekintve itt is ugyan azt az eredményt kapjuk: kontrollálják vagy módosítják a routing információkat azon irányba/interfészen, amelyre a route map-et alkalmaztuk. A mi esetünkben az „Out-to-MPLS" route map-et alkalmazzuk a 145.16.1.2-es szomszéd irányába küldött, routing információkat tartalmazó üzenetekre. A route map egy prefix listára mutat:

```
!
route-map Out-To-MPLS permit 10
 match ip address prefix-list GLOBALNETWORKS
!
```

Ahol a parancs megenged minden olyan útvonal információ cserét, amely a „GLOBALNETWORKS" prefix listában engedélyezve van.

[1] Holdtime: ez a paraméter határozza meg, hogy egy eszköz hány másodpercig várjon miután nem kapott választ egy keepalive üzenetre.

```
!
ip prefix-list GLOBALNETWORKS seq 10 permit 128.0.0.0/2
ip prefix-list GLOBALNETWORKS seq 20 permit 10.0.0.0/8
ip prefix-list GLOBALNETWORKS seq 30 permit 145.17.0.0/20
ip prefix-list GLOBALNETWORKS seq 40 permit 145.16.0.0/13
ip prefix-list GLOBALNETWORKS seq 50 permit 145.16.1.0/30
ip prefix-list GLOBALNETWORKS seq 60 permit 145.16.255.1/32
!
```

A legfontosabb, hogy minden telephely rendelkezzen a 128.0.0.0/2 és a 10.0.0.0/8 –as hálózatok elérési információival, ugyanis ezek biztosítják a legfontosabb applikációk Angliában lévő szervereinek elérhetőségét. A 145-el kezdődő címek lokálisak, és tulajdonképpen az összes HSBC Credit által használt alhálózatot lefedik. Ezen hálózatok hirdetésén kívül másra nincs szükség, ezért elég, ha a BGP csak ezeket az információkat adja át az MPLS gerinchálózatnak.
A fiókhálózatokban található útválasztók tulajdonképpen nem is rendelkeznek más hálózatok elérési útvonalával:

```
„
    145.17.0.0/25 is subnetted, 1 subnets
C    145.17.11.0 is directly connected, GigabitEthernet0/0
     145.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    145.16.255.7/32 is directly connected, Loopback0
C    145.16.1.120/30 is directly connected, GigabitEthernet0/1
B    10.0.0.0/8 [20/0] via 145.16.1.122, 1w1d
B*   0.0.0.0/0 [20/0] via 145.16.1.122, 4w2d
B    128.0.0.0/2 [20/0] via 145.16.1.122, 1w0d
”
```

Az itt látható routing tábla segítségével a fiókok minden számukra fontos szervert elérnek. Ebből is jól látszik, hogy a végponti routereknek a szolgáltatói gerinchálózatból tulajdonképpen semmit sem kell látniuk, routing táblájuk nagyon egyszerű.

A routing konfiguráció után következhet a tesztelés.

6. Tesztelés

A tesztelés az implementáció egyik legfontosabb lépése. Ennek segítségével bizonyosodhatunk meg arról, hogy a routing jól működik, valamint egy vonalprobléma esetén az útválasztók a meghatározott időn belül átkonvergálnak a másodlagos routokra.
Miután az implementáció befejeződött, el kell végezni egy teljes reziliencia tesztet. Ez tulajdonképpen a szolgáltatói CE router irányába néző ethernet interfész lekapcsolását jelenti, egyenként a fiókirodákban, valamint a központi telephelyen. Ez utóbbi kiemelten fontos, ugyanis alaphelyzetben minden forgalom áthalad az itt található útválasztókon. Fontos elem továbbá a szolgáltató által biztosított, a gerinchálózathoz hozzáféréssel rendelkező hálózati mérnök elérhetősége a tesztelés ideje alatt, ugyanis sok esetben csak a szolgáltató által üzemeltetett eszközök konfigurálásával oldható meg egy routing probléma.

A fiókokban a lekapcsolást követően ellenőrizni kell a routing táblát, amelyben a BGP által megtanult útvonalak a dialer interfész irányába kell, hogy mutassanak. Ezután egy tracert paranccsal ellenőrizni kell a tényleges routingot, mind a Head Office-ban lévő szerverek irányába, mind az Egyesült Királyságban található applikáció szerverek felé.

A központi iroda redundacia tesztje során több link meghibásodását is szimulálni kell. Az elsődleges link lekapcsolása után a központi iroda közvetlenül elérhetetlenné válik a fiókok számára az MPLS gerinchálózaton keresztül. Ebben az esetben a szolgáltatói, MPLS felhőben lévő útválasztóknak reagálni kell a változásra, és a forgalmat a 2-es fióktelep irányába kell terelni. Itt különösen fontos a szolgáltató jelenléte, ugyanis hiba esetén csak a szolgáltatónak van lehetősége azt felülvizsgálni és kijavítani.
Az elsődleges nemzetközi bérelt vonal elérhetetlensége esetén, a Head Office központi (HUGRER01) forgalomirányítójának az EIGRP által megtanult 128-al és 10-el kezdődő route-jai a két központi telephely (Head Office és Fiók2) közötti bérelt vonal irányába kell,

hogy mutassanak. Ezt, egy, a fiókhálózatból UK célcímmel indított trace-el is meg kell erősíteni.

Az 1-es fióktelepen az MPLS access link lekapcsolását követően, az 1-es és 2-es fiók közötti bérelt vonalnak kell aktívvá válnia. A routing helyes működését természetesen ebben az irodában is ellenőrizni kell trace-routok segítségével.
A tesztelés befejezésével a teszteredményeket dokumentálni kell.

7. Összefoglalás

A sikeres tesztelés befejeztével megállapíthatjuk, hogy egy, korunk elvárásainak megfelelő, mind sebességben, mind technológia fejlettségben előremutató kommunikációs hálózat került kialakításra.
A tervezés során kitűzött célokat ugyan nem sikerült teljes mértékben megvalósítani – gondolok itt a másodlagos, mikrohullámú access linkre való lassú konvergálásra - , viszont az ezt kiváltó 10Mb-es bérelt vonali megoldás is kielégítőnek bizonyult. A lassú konvergencia oka – mint később kiderült – a szolgáltatói gerinchálózatban lévő autonóm rendszerek mennyisége volt, ugyanis útvonal változás esetén a protokoll minden AS határán újrakonvergál, ami megsokszorozza a várakozási időt. Ezt leszámítva viszont az új technológia bevezetése probléma nélkül lezajlott. A HSBC magyarországi leányvállalata ezáltal egy olyan naprakész kommunikációs technológia birtokába jutott, ami a jövőben nagyban megkönnyíti majd az esetleges fejlesztések megvalósítását. Gondolok itt például az új szervizekre, amelyek lehetővé teszik olyan adatforgalom problémamentes irányítását, amely nagy mennyiségű „késleltetésre érzékeny csomagot” generál. Ilyen például az IP telefónia, vagy a videó konferencia, melyek lassan teljesen felváltják a jelenlegi megoldásokat. Az, hogy az MPLS technológiának köszönhetően kevesebb adatcsomagot vesztünk el nem csak az IP alapú kommunikáció minőségét javítjuk, de minden más applikáció is gyorsabb hálózati kommunikációt valósíthat meg. Ez hatványozottan igaz lesz a nemzetközi 2Mb-es bérelt vonal fejlesztésekor, ekkor ugyanis az Egyesült Királyságban található host-ok is gyorsabban elérhetőek lesznek.

Külön kihívást jelentett a szolgáltatóval való együttműködés a migráció ideje alatt.
Mivel a végfelasználói CE útválasztó eszközök a mi tulajdonunkban vannak, és a karbantartásukat nem szerettük volna kiengedni a kezünkből, így az implementációhoz szükséges konfigurációt is nekünk kellett elkészíteni, természetesen szoros együttműködésben a szolgáltatóval. Itt akadtak nehézségek (főleg szolgáltatói mulasztások történtek – nem megfelelő MD5 és interfész konfiguráció, stb), de ezen problémák megfelelő kommunikációval könnyedén orvosolhatóak voltak.

Összességében elmondhatjuk, hogy a migráció elsődleges célja, valamint várt eredménye realizálódott. A sebesség 4 szeresére nőtt, amit a felhasználók is érzékelnek, és pozitívan értékelnek. IP telefóniát ugyan még nem használunk a hálózaton, viszont az új technológia birtokában biztos hátteret tudhatunk egy jövőbeli telekommunikációs fejlesztés mögött. Továbbá amellett, hogy jelentős növekedést értünk el mind sebesség, mind megbízhatóság terén, a cég számítógépes hálózatokra fordított havi kiadásait is csökkentettük 40%-al, ezzel valós, kézzel fogható megtakarítást is felmutatva.

8. Irodalomjegyzék:

Wendell Odom: CCENT/CCNA ICND1 Official Exam Certification Guide, Cisco Press 2007

Wendell Odom: CCNA ICND2 Official Exam Certification Guide, Cisco Press 2007

Dr. Almási Béla: Számítógép hálózatok előadás –
http://irh.inf.unideb.hu/oktanyag.htm

MPLS/Tag Switching –
http://www.cisco.com/en/US/docs/internetworking/technology/handbook/MPLS_Tag-Switching.html

MPLS and MPLS VPNs for Beginners by Christopher Brandon Johnson:
http://www.infosecwriters.com/text_resources/pdf/CJohnson_MPLS_VS_MPLS_VPN.pdf

Border Gateway Protocol –
http://www.cisco.com/en/US/tech/tk365/tk80/tsd_technology_support_sub-protocol_home.html

Route Maps for IP routing protocol –
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008047915d.shtml