

**ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM  
BOLYAI JÁNOS KATONAI MŰSZAKI KAR  
KATONAI MŰSZAKI DOKTORI ISKOLA**

**BLEIER ATTILA**

**A Magyar Honvédség állandó telepítésű  
hálózatának modernizációja**

---

Doktori (PhD) értekezés

**Témavezető: Prof. Dr. Rajnai Zoltán mk. ezredes, egyetemi tanár**

**2010, Budapest**

# Tartalomjegyzék

Bevezető.....	3
I. Magyar Honvédség elvárásai és a XXI század kihívásai.....	8
I.1 XXI sz. kihívásai a híradó és informatikai rendszerek szempontjából .....	8
I.2 A híradó és informatikai hálózatokkal szemben támasztott követelmények .....	12
I.3 A Magyar Honvédség állandó telepítésű hírendszere .....	18
I.4 A Magyar Honvédség állandó hírendszereinek vizsgálata .....	22
I.5 Összegzés.....	26
II. A Magyar Honvédség stacioner hálózatának forgalmi vizsgálata.....	28
II.1 Sáv szélességigény számítás 3D radar képekre .....	29
II.2 Forgalmi esetek szimulációja.....	31
II.3 Forgalmi esetek, forgalmi minták .....	34
II.4 Összegzés .....	45
III. A Magyar Honvédség stacioner hálózatának javasolt kialakítása .....	47
III.1 Hálózati rétegek.....	48
III.2 A stacioner hálózat kialakítása .....	53
III.3 A stacioner adatátviteli hálózat rendszerterve .....	58
III.4 A hálózat rendszerszintű mérése.....	77
III.5 Összegzés .....	79
IV. A vizsgálatok összegzése és az értekezés végkövetkeztetései .....	82
V. Jegyzékek .....	89
V.1 Ábrajegyzék .....	89
V.2 Táblázatjegyzék.....	90
V.3 Rövidítések jegyzéke.....	91
VI. Irodalomjegyzékek.....	94
VI.1 Hivatkozott Irodalom .....	94
VI.2 Felhasznált irodalom.....	97
VI.3 Publikációs jegyzék .....	104
VII. Mellékletek.....	105
VII.1 Gerinchálózati tesztelrendezés .....	105
VII.2 A stacioner hálózat forgalmi tervezésének eredményei .....	157

# Bevezető

## Tudományos probléma megfogalmazása

Kutatási témám a Magyar Honvédség híradó és informatikai hálózatának a stacioner (polgári megnevezésében gerinchálózati) rétegére vonatkozik, ezen belül elsősorban a stacioner hálózat forgalmi viszonyaival, valamint az egységes IP/MPLS (Internet Protokoll – Többprotokollos címkekapcsolás) hálózati technológia által nyújtott technológiai előnyöket kívánom vizsgálni.

A Magyar Honvédség stacioner hálózata a Magyar Honvédség transzport célú adatátviteli hálózata, amely a Magyar Honvédség telephelyeit köti össze időmultiplex átviteltechnikai hálózatokon keresztül. A stacioner hálózatot mikrohullámú hálózati eszközök alkotják, ezen mikrohullámú hálózati eszközök felújítása 2000-es évek elején történt meg. A stacioner hálózat jelenlegi felépítésével Fekete Károly disszertációja foglalkozik mélyebben [1], kutatásomat részben az ott szereplő kutatási eredményekre építettem.

A fentiek mellett a polgári távközlés technológiai oldalán végbement változások (az egységes IP (Internet Protokoll) alapú hálózatra való áttérés), a nagy-rendelkezésre állású IP alapú eszközök megjelenése, valamint azok polgári szolgáltatói gerinchálózatokban történő szélesebb körű elterjedése az, ami téma kutatására ösztönözött.

A szakirodalom tanulmányozása, a dokumentumok, a magyar és a külföldi tudományos igényű publikációk kutatása, feldolgozása és rendszerezése során a következő hipotézist állítottam fel:

- szükséges az informatikai hálózatok forgalmának a távközlési hálózatok forgalomelemzéséhez hasonló mélységű vizsgálata
- A Magyar Honvédség stacioner hálózatában szükséges ilyen forgalomelemzési módszerek használata
- A stacioner hálózat forgalmi viszonyai az elvárt hálózati kép, és hálózati viszony számítógéppel szoftveres úton modellezhető
- A forgalmi modell eredménye alapján, ill. a forgalmi modellezés módszerének használatával hosszabb távra meghatározható az elvárt hálózati technológia

Alapvető kutatási célként tűztem ki, hogy a fentiek alapján tanulmányozva a polgári távközlésben használt technológiákat, azokat adoptálva a speciális hálózati környezetre ajánlást adjak a jövőben stacioner hálózat elemeire.

### **A kutatási cél eléréséhez az alábbi részcélokat fogalmaztam meg:**

- megvizsgálni a speciális katonai híradó és informatikai követelményeket, amelyeket a stacioner hálózatnak teljesítenie kell
- Meghatározni olyan módszereket, amelyek segítségével a forgalmi viszonyok modellezhetőek
- Meghatározni a jelenlegi, és a várható jövőbeni forgalmi igényeket
- megvizsgálni egy egységes Ethernet/IP/MPLS alapú hálózati technológia modell használatának lehetőségét a Magyar Honvédség stacioner hálózatban
- Javaslatokat tenni a Magyar Honvédség stacioner hálózat fizikai és logikai kialakítására
- Meghatározni a javasolt hálózati szintű technológiai paramétereit
- Meghatározni egy migrációs utat a jelenlegi hálózati infrastruktúráról a kialakítandó hálózati struktúrára

### **A kitűzött célok megvalósítása érdekében:**

- *Tanulmányoztam* a Zrínyi Miklós Nemzetvédelmi Egyetem tudományos, tájékoztató és dokumentációs könyvtárában fellelhető, a témához kapcsolódó szabályzatokat, kandidátusi, egyetemi doktori és PhD értekezéseket, szakkönyveket, kiadványokat, cikkeket.
- *Áttekintettem* a IP/MPLS technológiára vonatkozó polgári, és a katonai kommunikációra vonatkozó katonai szabványosító intézetek fontosabb szabványait és ajánlásait.
- *Felkutattam és feldolgoztam* a témához kapcsolódó (többségében külföldi) tudományos közleményeket, szakkikkeket.
- *Konzultációkat folytattam* a kutatási területemhez tartozó rendszereket üzemeltető polgári és katonai szakemberekkel, így a stacioner hálózatot üzemeltető személyzettel, valamint a különböző polgári hálózatokat üzemeltető személyzettel.
- Hazai és nemzetközi *konferenciákon vettem részt*, ahol egyrészt a kutatási témám részeredményeit publikáltam előadások formájában, másrészt mélyebben megismertem a világban kialakult hálózati trendeket.

- Felhasználtam tapasztalataimat az *IP/MPLS gerinchálózat tervezésében/fejlesztésében* (Magyar Villamos Művek Zrt., Magyar Telekom Nyrt., Pannon GSM Zrt., Émász Kft.)

**A téma kidolgozása során kutatási területeim voltak:**

- A civil és katonai kommunikációs rendszerek, főbb rendszerelemek fejlődési-fejlesztési irányvonalai
- IP /MPLS hálózatok által nyújtott szolgáltatások és ezek fejlesztési irányvonalai
- Nagy rendelkezésre-állású IP/MPLS hálózatok kialakítása, azok eszközoldali, hálózatoldali és a szolgáltatásoldali vonatkozásai
- Távközlési átvitel-technikai és IP/MPLS hálózatok forgalmi modellezése, forgalmi tervezése
- Szolgáltatás-redundancia, hálózati topológiamodellek és technológiák vizsgálata nagy rendelkezésre állású szolgáltatások biztosításához
- A Magyar Honvédség stacioner hálózatának jelenlegi kialakítottsága

**Nem tekintetem kutatásom témájának:**

- Az egyes IP útválasztók technikai paramétereinek általános vizsgálatát, (csak olyan mértékben amely a stacioner hálózat kialakításában elfoglalt helyükhöz szükségesek, ezek a paraméterek NATO (North Atlantic Treaty Organization) STANAG (Standardization Agreement) és IETF (Internet Engineering Task Force), IEEE (Institute of Electrical and Electronics Engineers Inc ) szabványokban meghatározottak).
- Az Ethernet / IP /MPLS technológia alapvető bemutatását (civil és katonai hálózatokban egyaránt szélesebb körben használt technológia), a technológia ismertetése több helyen megjelent már a szakirodalomban így pl. [1].
- A javasolt technikai elképzeléseknek a Magyar Honvédség esetleges szervezeti vonatkozásait.
- Az értekezésben javasolt elvi megoldások konkrét gazdasági feltételeit, anyagi vonzatát.
- Az értekezésben javasolt elvi megoldások humán erőforrás igényét.

## Az alkalmazott kutatási módszerek:

A kutatási módszereim mind szekunder, mind primer kutatásokra épülnek.

- *Felkutattam és feldolgoztam* a témához kapcsolódó szakirodalmat, tudományos dolgozatokat, kandidátusi, egyetemi doktori és PhD értekezéseket.
- *Elemeztem és rendszereztem* a IP/MPLS hálózatok fejlődését az első generációs hálózati fejlesztésektől a mai második-harmadik generációs IP hálózatok fejlődéséig.
- *Tanulmányoztam* a jelenleg IP/MPLS hálózatokban használt hálózati szolgáltatásokat, ill. annak a működési viszonyait.
- *Tanulmányoztam* elsődlegesen az Egyesült Államok, Nagy Britannia, Franciaország és Németország civil és stacioner gerinchálózati technológiáit.
- *Következtetéseket vontam le* a vizsgált IP/MPLS gerinchálózatok, stacioner hálózatok jellemzőiről, alkalmazási sajátosságaiból.
- *Primer hálózattechnológiai kutatásokat és tervezési feladatokat* végeztem különböző polgári hálózatokon (Magyar Villamos Művek, Magyar Telekom Nyrt. és Pannon GSM Zrt, Émász Kft.) a tapasztalatokat a Magyar Honvédség stacioner hálózatának kialakításakor figyelembe vettem.
- A forgalmi eseteket számítástechnikai eszközökkel *modelleztem* és ahol lehetett *automatizáltam*.

A témával kapcsolatos dokumentumok kutatását, az adatok és információk gyűjtését, rendszerezését 2009. december végén fejeztem be.

Az értekezésem elkészítése során rengeteg tanácsot, segítséget kaptam, szeretném köszönetemet és hálámat kifejezni

- feleségemnek, Bleier-Cseke Lillának állhatatos türelmét, és segítségnyújtását az anyag elkészítése során
- A szüleimnek és testvéreimnek, a Bleier és Cseke családoknak a támogatását, akik segítségével nélkül ennek az anyagnak az elkészítésébe nem fogtam volna bele
- témavezetőmnek prof. dr. Rajnai Zoltán és a Zrínyi Miklós Nemzetvédelmi Egyetem híradó tanszékének segítségét
- Kapsch Kft-nek, kiemelten a Carrier Solutions részleg minden tagjának a segítségét, az ő aktív segítségük nélkül ez az anyag nem készülhetett volna el
- A Budai Református Egyházközösségnek segítő támogatását.

Az ő közvetett, vagy közvetlen segítségük nélkül az anyag nem készülhetett volna el.

A kutatási céljaim eléréséhez az értekezést három fejezetre tagoltam. Az *első fejezetben* az Összhaderőnemi Doktrína [2] alapján meghatároztam a követelményeket, valamint a stacioner hálózat jelenlegi kialakítása alapján meghatároztam a stacioner hálózat alkalmazásával szembeni követelményeket. A második fejezetben modelleztem a stacioner viselkedését három forgalmi modell alkalmazásával, szoftveres úton kialakítottam a hálózat modelljét. A harmadik fejezetben konkrét javaslatokat dolgoztam ki a hálózat kialakítására, a technológia meghatározásától a stacioner hálózaton alkalmazandó eszköztípusok, valamint hálózati szintű paraméterek és szolgáltatások meghatározásáig, és elvi ajánlásokat adtam a technológia alkalmazására a Magyar Honvédség stacioner hálózatában.

A mellékletekben azokat a témához kapcsolódó anyagokat csatoltam az értekezéshez, melyek a katonai híradás általam vizsgált területéhez kötődnek. Itt olyan részterületek kerültek ismertetésre, amelyeket az értékes egyes információinak precíz értékeléséhez célszerűnek ítélttem meg (így a IP/MPLS technológia ismertetése, az IP/MPLS hálózat forgalmi elemzése, az IP/MPLS szolgáltatások ismertetése, ill. egyes eszközparaméter beállítások amelyeket a primer alkalmazott kutatás során használtam).

## **Alaki és formai megfontolások**

A szakirodalomból felhasznált hivatkozott részeket az értekezés törzsrészében előfordulásuk sorrendjében [szögletes] zárójelben levő számmal jelöltem, majd a törzssanyag végén „Hivatkozott Irodalom” cím alatt soroltam fel, szintén előfordulásuk sorrendjében. Külön jegyzéket állítottam össze a „Felhasznált irodalom” számára.

Az értekezésben fontosnak ítélt gondolatokat és idézeteket *dőlt* betűkkel emeltem ki, míg a legfontosabb gondolatok kiemeléséhez a **vastagítást** alkalmaztam. Az ábráknál és a táblázatoknál igyekeztem a forrásokat feltüntetni, ezek szintén szögletes zárójelben szerepelnek, ugyanakkor a forrás nélküli ábrák és táblázatok a saját kutatási eredményeim, megfontolásaim alapján kerültek be a törzssanyagba.

Az értekezés témájához – jellegénél fogva – sok idegen, elsősorban angol kifejezés, szóösszetétel, betűszó vagy rövidítés kapcsolódik, ezért azokat lehetőleg első előfordulásuk alkalmával kifejtettem és a törzssanyag végén táblázatban foglaltam össze. A fogalom meghatározásoknál és a rövidítéseknel az AAP-6(2002), az AAP-15(2002) és az AAP-31(A) NATO dokumentumokat vettem elsődlegesen figyelembe.

## I. Magyar Honvédség elvárásai és a XXI század kihívásai

*„Változás` szeretete tart munkásságban és szül találmányokat; a régiek szeretése menti meg a már meglévőt, gonddal szerzettet, hamar eltűnésétől.”*

Wesselényi Miklós

A 90-es évektől kezdődően a hadviselés komoly változáson megy keresztül. A második hullámú anyagközpontú hadviselésből folyik az áttérés a harmadik hullámú (negyedik generációs) információs hadviselésre. Erre a váltásra a NATO komoly hangsúlyt fektet, ami megjelenik mint hangsúlyos kérdés a Magyar Honvédség Összhaderőnemi doktrínájában valamint a 2007-2016 közötti hosszú távú fejlesztési tervekben is.

Az első fejezetben arra keresem a választ, melyek azok a kihívások, amelyeknek a Magyar Honvédség hírendszere – kiemelten az állandó hírendszere – meg kell, hogy feleljen. Ezért a fejezet első felében ismertetem a kihívásokat, majd az állandó hírendszere definícióját azért, hogy pontosítsam a stacioner hálózat fogalmát. A fejezet további részében ismertetem az elvárásokat, fejlesztési irányokat. A fejezet végén ismertetem a stacioner hálózat jelenlegi képét, és a további fejezetek során javaslatot teszek annak továbbfejlesztésére.

### I.1 XXI sz. kihívásai a híradó és informatikai rendszerek szempontjából

Az ezredfordulóra a NATO a világ legnagyobb katonai szövetségi rendszerévé vált, ezzel együtt felvállalva azt is, hogy adekvát választ ad az ezredforduló katonai-politikai jellegű kihívásaira is. Ezen kihívások között a legfontosabbak a terrorizmusra adott megfelelő válasz, a természeti erőforrások kimerülése és a globális felmelegedés miatti katasztrófa és konfliktushelyzetek, ill. az infokommunikációs technológiák fejlődésével a hadviselés, és a hadseregek átalakítása mily módon történjen. Dolgozatomban az utóbbi kérdés magyar vonatkozásaival foglalkozom.

#### NATO és a terrorizmus

A NATO '99-es kibővítésével, és hazánk NATO csatlakozásával együtt a NATO képességalapú haderőre történő átállása is megkezdődött. Ennek első jele a prágai képességfelajánlási dokumentum (PCC - Prague Capabilities Commitment). A rigai 2006-os csúcson határozták meg az elkövetkezendő 10-15 év legfontosabb irányelveit. Ezek az irányelvek a Honvédelmi Minisztérium tolmácsolásában a következők: [3].

„Az irányelvek a biztonsági környezetet továbbra is folyamatosan változóknak írja le, amelyre a magas fokú komplexitás, a globalitás és a fejlemények megjósolhatatlansága a jellemző. A



dokumentum a legfontosabb fenyegetésekként az egyre agresszívabb terrorizmust és a tömegpusztító fegyverek terjedését jelöli meg, meghatározó kockázatként pedig a gyenge és működésképtelen államok jelentette problémát, valamint a regionális krízisek és konfliktusok okait és hatásait említi. Az átfogó politikai irányelvek szerint a szövetség a legveszélyesebb jövőbeni forgatókönyvnek a fenyegetések és kockázatok összekapcsolódását, ezen belül pedig a terroristák tömegpusztító fegyverekhez jutását tekinti. A komplex és gyorsan változó biztonsági környezetnek megfelelően a NATO továbbra is alapvető feladatának tekinti a biztonság garantálását, a konzultációt, az elrettentést és a védelmet, a válságkezelést és a partnerséget.”

## **NATO, természeti katasztrófák és az ezzel összefüggő erőforráskonfliktusok**

A természeti erőforrások kimerülése a XXI. század egyik meghatározó felismerése, melyet mind tudományos, mind gazdasági, mind politikai síkon kezelni kell [4]. Az anyag [5.] megállapítása szerint, a XXI. század meghatározó problémái lesznek a természeti erőforrások kimerülése miatt kialakuló politikai konfliktusok, ill. a globális felmelegedés okozta természeti katasztrófák kezelése. Ez utóbbiról sajnos nem jövő, hanem jelen időben kell, hogy beszéljünk, tragikus példa erre a 2010. májusi esőzések nyomán kialakult helyzet Miskolcon [6] a Katrina hurrikán nyomán kialakult katasztrófavhelyzet az Egyesült Államokban [7], vagy a Mexikói öbölben kialakult természeti katasztrófavhelyzet egy fűrótorony megsérülése miatt [8]. A Magyar Honvédségnek ilyen helyzetekben segítséget kell nyújtania a katasztrófavédelemnek. Az ilyen helyzetek során a gyors és pontos információeljuttatási képesség meghatározó.

## **A negyedik generációs hadviselés elterjedése**

A XX-sz. végén az Öböl-háborúkkal a hadviselés egy új formája jelent meg (az ún. negyedik generációs hadviselés), ahol kulcsfontosságú kérdés az információs fölény megszerzése lett. Az információs fölény megszerzése azért fontos, mert amennyiben az információs fölényben van az adott hadviselő fél, az előnyt jelent a döntéshozóknál – és döntési fölényben jelentkezik. A megfelelő információ birtokában, jobb döntéseket lehet hozni, és ez meghatározó jelentőségű lehet az ütközet kimenetelére.

Ezért elsődleges fontosságú az információs fölény megszerzése és fenntartása a jelen és a jövő háborúiban/válsághelyzeteiben. A kérdés az, hogy milyen módszerekkel, és eszközökkel tudjuk az információs fölényt kialakítani és fenntartani. Ez a kérdéskör, az információs hadviselés témaköre, amelynek egyik súlyponti oldala a kommunikációs célú információs fölény kiépítése és fenntartása, amely napjaink egyik leginkább kutatott területe.

## **A katonai informatikai alkalmazások elterjedése**

A NATO Network Enabled Capabilities doktrínájával hangsúlyossá válik a katonai informatikai és információs rendszerek alkalmazása. Ilyen rendszerek például az amerikai hadseregben a WWMCCS (World Wide Military Command and Control System), GCCS (Global Command and Control System), NMCS (National Military Command System) – vezetés irányítási rendszerek, ill. JOPEX (Joint Operation Planning and Execution System) Összhaderőnemi hadművelet-tervező rendszer; a brit hadseregben az IARCCIS (Interim ACE Rapid Reaction Corps) és THISTLE, a német haderőnél a HEROS (Heeres Führungsinformations System (für die rechnerunterstützte) Operationsführung in Staeben) vezetésirányítási rendszer, az ADLER (Artillerie-, Daten-, Lage- und Einsatz-Rechner) tüzérségi informatikai rendszer és az EIFEL a német légierő informatikai rendszere, a francia haderőnél a SGEA (Système de Guerre Électronique de l'Avant) és STRIDA (Système de Traitement et de Représentation des Informations de Défense Aérienne). [9 pp.131-164]

Ezek a rendszerek megkövetelik a híradó infrastruktúra felülvizsgálatát. A korábbi „hangbeszéd-központú” megközelítés az új informatikai és vezetésirányítási rendszerek igényeit nem elégítik ki, hiszen ezek nagy mennyiségű adatforgalmat generálnak. Új, információ központú megközelítés szükséges, és a híradó rendszereket is ebben a felfogásban szükséges felújítani, modernizálni. Ez természetesen nem jelenti, nem jelentheti azt, hogy a hagyományos rendszereket egyik napról a másikra szüntessük meg, hanem egy migrációs út szükséges a jelenlegi állapotból az elérendő végcél irányába.

A katonai információs rendszerben végbenő változások másik fontos irányvonala a különböző jellegű adatok és információs rendszerek integrációja, amely az egyes rendszerek között szorosabb együttműködést követel meg. Ezek természetesen együttműködési (szakszóval interoperabilitási) problémákat hoznak magukkal, amelyeket le kell küzdeni. Ez is abba az irányba mutat, hogy a különféle szolgáltatást biztosító rendszereket, így a hangátviteli rendszereket ill. informatikai rendszereket ne különálló rendszerekként kezeljük, hanem olyan rendszerelemekként, amelyek az erőforrások egy bizonyos halmazát képesek nyújtani. Ez egy új megközelítést igényel (ahol erőforrások adottak) és a híradórendszer (kommunikációs rendszer) szolgáltatásokat nyújt az (hálózati) erőforrásokon keresztül. Ez összhangban van a NATO Network Enabled Capabilities doktrínájában megfogalmazott elvekkel. [9 pp. 96-99], ill. [10]. Ez a megközelítés a Magyar Honvédségben jelenleg nem használt.

Hosszabb távon további kihívást jelent a Network Centric Warfare (Hálózatközpontú hadviselés) elterjedése – ami szintén része a NATO doktrínának. Itt megjelenik az a koncepció, hogy a katonai hálózatban egészen a végrehajtó egységekig minden egység, egy közös (IP alapú) kommunikációs hálózatba szervezett, így a különböző szintű döntéshozók, gyakorlatilag ugyanazokkal az információkkal rendelkeznek, mint a végrehajtó egységek. Ez komoly követelményeket ró, mind a harctéri, mind a tábori, mind pedig az állandó

hírrendszerre.

A harctéri hírrendszer alkalmazása sokkal szélesebb körű kell, hogy legyen, hiszen nagyon sokféle és különböző jellegű információkkal segítheti ez a csapatvezetést. Pl. a különböző életfunkciókat figyelő szenzorok folyamatos jelentést küldhetnek a katona állapotáról a döntéshozó, ill. az egészségügyi támogató csapatoknak, vagy a páncélozott járműveknél a különböző szenzorok küldhetnek állapotjelzéseket a jármű műszaki állapotáról a műszaki támogató alegységeknek. Megjelenhet az élő képi jelek küldése közvetlenül a végrehajtó csapatoktól. Ezek természetesen mind-mind különböző minőségi követelményeket rónak a hálózatra, a különböző adatokat különböző prioritással, különböző jellemzőkkel szükséges kezelni, mind a harctéri, mind a tábori, illetve az állandó hírrendszerben. Például az aggregált forgalmak, az állandó hírrendszerben a jelenleg használatos sáv szélességek, és technológiák többszörösét, és új megközelítésű kezelését igénylik.

A mobilitás növelése is kiemelt szerepet kap, elsősorban a tábori, és a harctéri hírrendszer esetében, ahol az új technológiák, mint pl. WiMAX (Worldwide Interoperability for Microwave Access) elterjedése várható, de várható bizonyos esetekben az EDR [11] ill. civil mobil technológiák veszélyhelyzeti alkalmazása [12], [13], így pl. a civil GSM hálózatok minősített helyzetben való alkalmazása kívánatos. Ezen technológiák közös előnye, hogy gyorsan, a helyzetnek megfelelően bevethetőek, hátrányuk, hogy – elsősorban az optikai szálal vezetékes technológiákkal szemben – nagyságrendekkel kisebb sáv szélességet biztosítanak.

További fontos követelmény a megbízhatóság, a rendelkezésre álló sáv szélesség, mind a stacioner mind a tábori hálózatban, illetve a hálózat tűrőképességének növelése. A fentiek azok a kihívások, amelyeknek egy jövőálló stacioner hálózat meg kell, hogy feleljen.

## I.2 A híradó és informatikai hálózatokkal szemben támasztott követelmények

A pontos kutatáshoz és tervezéshez szükséges a követelmények pontos meghatározása. A katonai, stacioner hálózattal szemben támasztott követelmények meghatározásához elsőként azt határozom meg, hogy mi tartozik a stacioner és informatikai hálózat alá. Ehhez elsőként a hírendszer fogalmát tisztázom, majd az Összhaderőnemi Doktrína alapján kiemelem azokat a követelményeket, amelyeket a hírendszerrel, ill. a híradó és informatikai rendszerrel szemben az Összhaderőnemi Doktrína támaszt.

### A hírendszer

A Magyar Honvédség híradó és informatikai rendszer vizsgálatakor fontos megfogalmazzunk azokat a határokat, amik definiálják ezt a rendszert. Dr. Sándor Miklós jegyzete a hírendszerrel így fogalmaz:

*a hírendszer:*

a csapatvezetési és fegyverirányítási rendszer alkotó része (alrendszere), amely egységes terv szerint telepített, hely és idő szerint összekapcsolt és illesztett, különböző rendeltetésű hírközpontok és híradó vonalak összessége és a személyzet.

A hírendszer a következő elemekből áll:

- vezetési pont hírközpontok;
- közvetlen összeköttetések híradó vonalai;
- alaphírhálózatok;
- futár- és tábori posta hírhálózat;
- híradás vezetés rendszere;
- híradás logisztikai rendszere;
- híradó tartalék.

Mint a felsorolásból is látszik a hírendszer egy szélesebb tevékenységkört rejt, mint pusztán a tradicionális hangalapú analóg, vagy digitális híradó (vagy polgári terminológiával távközlési) rendszer. Egyrészt tartalmaz olyan szolgáltatásokat, amik talán közelebb állnak a logisztikához (futár és tábori posta hálózat), és tartalmaz olyan fontos – a rendelkezésre állást növelő elemeket, mint a híradó tartalék.

Mára a hírendszer ill. híradó és informatikai rendszer az infokommunikáció kialakulásával egy egységes rendszert alkot, ahol a híradó rendszer hálózati/kommunikációs szolgáltatásokat nyújt az informatikai rendszer számára. Ez a szolgáltatás alapú modell vált általánossá a polgári életben, és véleményem szerint ezt a modellt lenne célszerű követni a Magyar

Honvédségnél is.

Milyen elvárásokat támaszt a Magyar Honvédség a hírendszerral szemben?

A hírendszert [9] rendelkezzen:

- magas fokú készenléttel
- szilárdsággal<sup>1</sup>
- mozgékonyssággal
- megfelelő áteresztőképességgel
- elégítse ki a híradó biztonság követelményeit

Úgy gondolom, hogy ezek az alapvető követelmények, amit a hírendszerral szemben támasztanunk kell. Ezt ki kell egészíteni szerintem néhány fontos további követelménnyel, amit én alkalmazás ill. szolgáltatás-specifikus követelményeknek nevezek. Azt kell vizsgálnunk, hogy a Magyar Honvédségnél használt alkalmazások, milyen követelményeket támasztanak a híradó (vagy kommunikációs) rendszerrel szemben.

A kommunikációs hálózatokkal szemben támasztott legfontosabb műszaki követelmények:

- rendelkezésreállítás
- szolgáltatás fizikai paraméterei (átadási pont jellege, interfész típusa)
- QoS (szolgáltatásminőség) paraméterek, mint például csomagvesztés, a késleltetés, a késleltetés ingadozás, az átlagos/csúcs/minimum átviteli sebesség stb.

Tehát amikor a hírendszert vizsgáljuk, mindenféleképpen tisztában kell lennünk azzal, hogy ez voltaképp egy kommunikációs rendszer, aminek a jósága<sup>2</sup> több elemből tevődik össze. Erről a véleményemet részletesebben a következő alfejezetekben fejtem ki.

A kommunikációs rendszer 'jósága' vagy a szolgáltatásminőség nem szubjektív, hanem mérhető paraméterekkel meghatározható. A hangrendszerek jóságának mérésével több anyag foglalkozik, pl. [36]. Az adathálózatok szolgáltatásminősége is hasonlóképpen jól kutatott terület pl. [37], azonban a gyakorlatban az adathálózatok mérése ritkán valósul meg.

A jövőállóság olyan meghatározó szempont amely nagyon nehezen mérhető, leginkább utólag állapítható meg egy rendszerről. Jelen értekezésben a jövőállóságot úgy tekintem, hogy a létrejött hálózat mennyire képes hosszútávon megfelelni a Magyar Honvédség rendszerei (ill. jövőbeli rendszerei) által támasztott követelményeknek, mennyire képes alkalmazkodni azokhoz. Folyamatszinten, a hálózat aprólékos és folyamatos javításával fenntartható egy olyan rendszer, amely jövőálló hosszabb távon is.

---

<sup>1</sup> A [9]-es irodalomban Munk S. szerző által használt kifejezés, mely valószínűleg az angol resiliency fogalom magyar megfeleltetése

<sup>2</sup> A rendszer jósága objektív vagy egyes esetekben szubjektív, mérhető paraméterekkel meghatározható minőségi kategória.

## Az Összhaderőnemi Doktrínában meghatározott követelmények

A Magyar Honvédség követendő irányvonalát az érvényben lévő Összhaderőnemi Doktrína határozza meg, mely 2003-ban lett elfogadva, jelenleg a felülvizsgálata folyik, a változások az év végére, jövő év elejére várhatóak. Az új doktrínában várhatóan hangsúlyosabb szerep jut a híradó és informatikai résznek, azonban ebben a fejezetben a várható módosítások még nem szerepelnek. Ebben a fejezetben azt fogom tárgyalni, hogy melyek azok az elvárások, ill. mi az az irányvonal, amelyet az érvényben lévő Összhaderőnemi Doktrína a kutatási területemre (a Magyar Honvédség állandó hírendszereinek modernizálására) vonatkozólag meghatároz.

Az Összhaderőnemi Doktrína definiálja, hogy melyek azok a feladatok, amire a Magyar Köztársaság fegyveres erőinek fel kell készülniük: „Az MK (Magyar Köztársaság) fegyveres erőinek készen kell állniuk mind a *hagyományos katonai védelemi feladatokra*, mind pedig azoknak a *konfliktusoknak a megoldására*, amelyek közvetten érintik országunk és szövetségeseink biztonságát és veszélyeztetik szűkebb vagy tágabb környezetünk stabilitását.” [2 pp.11] Ennek fényében kell vizsgálnunk a továbbiakban a Magyar Honvédség híradó és informatikai rendszerét, amely tehát két feladatra kell, hogy felkészüljön: „védelmi feladatokra” (elsősorban stacioner hálózat), ill. válságkezelő feladatokra (elsősorban tábori hálózat).

Az Összhaderőnemi Doktrína azt is meghatározza, hogy melyek azok a fenyegetések, ill. konfliktusok, amikre fel kell készülnünk. A doktrína elsődleges fenyegetésként nevezi meg a nemzetközi terrorizmus megerősödését, így mind a stacioner, mind a tábori hálózatot úgy kell kialakítani, hogy erre a fenyegetésre megfelelő választ tudjon adni.[2 pp.11] .

A doktrína a híradó és informatikai rendszert a harci támogató erők közé sorolja [2 pp. 17], melynek kapcsán két fogalmat tisztáz: a harci támogatás fogalmát, ill. a támogatott és támogatói viszonyt. Az előbbit így határozza meg: „A **harci támogatás** tartalma a harci erő támogatása, ami a támogatott harci egység feladata végrehajtásának felderítési adatokkal illetve tűzzel való támogatását, manővere végrehajtásának szabadságát és az ellenség mozgásának korlátozását, a szárazföldi erő légvédelmét, a tömegpusztító fegyverek elleni védelmet, az elektronikai-, információs-, a vezetési-irányítási-, lélektani hadviselést, valamint a polgári-katonai együttműködést, és a tömegtájékoztatást foglalja magában”[2 pp 27]. Mint láthatjuk az adattal való támogatást a doktrína kulcsfontosságúan kezeli közvetlenül és közvetetten is az elektronikai-, információs-, vezetés-irányítási-, ill. lélektani hadviselés kapcsán is, amelyekben az infokommunikációs rendszerek szintén fontos szerepet kapnak. Az adattal való támogatás szerepének felértékelődése, valamint az elektronikai-, információs-hadviselés megjelenése a korábbiakban megjelent információs fölény kialakításához szükséges. Ez a feladat komoly szerepet ró a Magyar Honvédség híradó és informatikai rendszerére.

A másik fontos dolog, amiről a harci támogatás kapcsán az Összhaderőnemi Doktrína említést tesz, az a Támogatott és támogatói viszony [2 pp. 28-29]. Az Összhaderőnemi Doktrína meghatározza az irányelveket – az „ún.” támogatási szolgáltatásra vonatkozóan. Ennek a továbbgondolása lehet a támogatási vagy szolgáltatási szintet definiáló megállapodás, amelyekre a további fejezetekben részletesen ki fogok térni.

Az Összhaderőnemi Doktrínában több helyen hangsúlyos szerepet kap a híradó és informatikai rendszer. Például a vezetési pont definíciójában is (értelemszerűen) fontos szerepet kap, amely szintén mutatja azt a kiemelt szerepet, amit a döntéshozatali folyamatban,

a döntési fölény kialakításakor játszik [2 pp.46], ill. felderítő információgyűjtő, feldolgozó és tájékoztató központ kapcsán is jelentős szerepet kap az információ továbbítása, amely elsősorban a híradó infrastruktúrán kell, hogy megtörténjen.

A doktrína 11. fejezete foglalkozik kiemelten a híradó és informatikai rendszerrel, amelyet így határoz meg: „a különböző vezetési szintek tevékenységéhez szükséges, rugalmasan változtatható, egységes elvek, módszerek és tervek alapján létrehozott; feladat, hely és idő szerint koordinált híradó és informatikai eszközök, eljárások, valamint az információs tevékenységeket végrehajtó szakállomány összessége.” [2 pp.87] A doktrína a híradó és informatikai rendszert, mint egységes egészet definiálja, összhangban a NATO elfogadott doktrínájával – ez egységes szervezeti felépítést sugall. Fontos észrevenni, hogy az információs tevékenységeket (tágabb értelemben az információs műveleteket) végrehajtó személyeket a híradó és informatikai rendszer részének tekinti.

A híradó és informatikai rendszerrel szemben az Összhaderőnemi Doktrínában az alábbi követelmények fogalmazódnak meg, amelyet három fő csoportban ismertettek:

- A működtetést, a fejlesztést, a meglévő rendszerekkel való integrációt támogató követelmények: szabványosság, kompatibilitás, interoperabilitás, felcserélhetőség, azonosság. Ezen követelmények azért fontosak, hogy a Magyar Honvédség rendszere egységes legyen, amely üzemeltetési és fejlesztési előnyökkel jár. (**Üzemeltetési előnyök** pl.: kisebb tartalékot kell képezni, kisebb a rendszerbeillesztés, a betanítás/oktatás költsége, könnyebb megoldani a támogató személyzet helyettesítését és a személyeknek is kevesebb gyártófüggő szabványt kell megtanulniuk, a rendszerek egymással való helyettesítése is könnyebb, a rendszerek cseréje, és fejlesztése szempontjából is ezek előremutató szempontok)
- A speciális katonai alkalmazásból eredő, **magas rendelkezésreállást és gyors bevetetőséget** segítő követelmények: reagáló képesség, megbízhatóság, szilárdság, időbeniség, rugalmasság, mobilitás. Ezen követelmények a katonai alkalmazás speciális igényei. Ehhez hasonló rendszerkövetelményeket a polgári infokommunikációs rendszerekben a távközlési szolgáltatóknál is találunk, ezért is fontos, hogy a polgári életben az infokommunikációs szolgáltatóknál használt elvek megjelenjenek a Magyar Honvédségnél is.
- **Információbiztonsággal** összefüggő követelmények: hitelesség, biztonság, rejtettség, elektronikus információvédelem. Ez a kormányzati ill. katonai szférában speciális követelmény, amelyre kiemelt figyelmet kell fordítani (és a Magyar Honvédség jelenleg is kiemelt figyelmet fordít).

Az Összhaderőnemi Doktrína meghatározza békében, minősített időszakban, ill. háborúban a híradó és informatikai rendszerét. Békében alapvetően békeállománnyal, a Magyar Honvédség állandó jellegű hálózatain üzemeltetett rendszer, amelynek képessége elégséges a békevezetés, irányítás, kiképzés és fenntartás teljesítéséhez. A rendszernek képesnek kell lennie minősített időszak, válságreakáló és katasztrófa helyzetek megoldására, ill. a készenlét fokozásával a tábori híradó és informatikai rendszerek csatlakoztatására. A válságreakáló műveletek és NATO kötelezettségeink kapcsán felmerülő fontos szempont a nemzetközi rendszerekhez való csatlakozás képessége. Háborúban, ugyanezen a bázison képesnek kell lennie az összhaderőnemi tervezés, vezetés támogatására, ill. a NATO védelmi erők

támogatására. [2 pp. 87-92]

Az Összhaderőnemi Doktrína legfontosabb vezérelvként említi, hogy az a felhasználó tevékenységének támogatására legyen megtervezve: polgári szóval élve, legyen felhasználóbarát, alkalmazási képesség szempontjából pedig az a legfontosabb irányelv, hogy háborús alkalmazásra legyen megtervezve. [2 pp. 87-92]

Korábban már említettük, hogy a Magyar Honvédség Összhaderőnemi Doktrínája az információs műveleteket végző személyeket a híradó és informatikai rendszer részének tekinti, így az információs műveletekként definiált feladatok a vezetés és információs rendszer részét kell, hogy képezzék, az információs műveletekkel a Doktrína 12. fejezete foglalkozik. [2 pp. 93-97]

Az infokommunikációs rendszer megjelenik (v. távközlési v. híradó és informatikai rendszerként) az információs műveletek, a védelmi és támadó információs műveletek fogalmának definíciójánál is. Ez az a területe a hadviselésnek amely dinamikusan fejlődik, és a NATO haderőknél egyre hangsúlyosabb szerepet kap. Az információs műveletek katonai tevékenységei és képességei meghatározásánál kiemelt rész foglalkozik a távközlési (híradó) és információs rendszerekkel, és hangsúlyozza a doktrína, hogy a vezetési és irányítási hadviselés alapelvei nagy mértékben függenek az időbeni és pontos információktól, kritikusak a hadműveletek sikeres végrehajtásánál. A híradóközpontokat a doktrína kritikus csomópontként definiálja, melynek elvesztése azonnal csökkentheti a vezetési irányítási képességet. [2 pp. 97]. Ennek megfelelően az állandó jellegű és tábori hírközpontok mindennemű támadástól való védelme elsődleges fontosságú.

A híradó és informatikai rendszerrel összefügg az Összhaderőnemi Doktrínában definiált elektronikai hadviselés is. [2 pp. 109-112] Az elektronikai hadviselés kiemelt célpontjai a híradó és informatikai rendszerek, ezért az elektronikai hadviseléssel szembeni védelem kiemelt fontosságú a híradó és informatikai rendszerek kialakításakor. A híradó és informatikai rendszer megjelenik még több más vonatkozásban is az Összhaderőnemi Doktrínában, erre azonban itt most nem térek ki.

Mint láthatjuk, az előző fejezetben vázolt alapelveket: a rendszerintegráció képességét, az információs műveleteket, a mobilitást a Magyar Honvédség érvényben lévő Összhaderőnemi Doktrínája is súlyponti kérdésekként kezeli. Ugyanakkor látnunk kell, hogy a NATO vezető katonai hatalmai fontosabb szerepet szánnak a híradó és informatikai rendszernek pl. az információs műveletek, vagy a stacioner, tábori és harctéri kommunikáció terén. Ezen változások remélhetőleg az új, átdolgozott doktrínába be fognak kerülni.

Az Összhaderőnemi Doktrínában megfogalmazott célokat a fejlesztési tervek támogatják, ültetik át a Magyar Honvédség rendszerébe. A tervekben szerepel az ágazati informatikai rendszerek összehangolására vonatkozó elgondolás kidolgozása (ez a korábban említett rendszerintegráció trendekkel összhangban van). Szerepel benne az informatikai rendszer fejlesztési irányainak meghatározása, ill. a különböző híradó és informatikai rendszerek fenntartása. Komolyabb rendszerfejlesztés nem szerepel benne, ez – a nemzetközi trendek, valamint a korábban említett kihívások figyelembe vételével – nem előremutató. Az egyetlen, fejlesztési feladatként definiálható rész benne a HM és MH objektumok



bekapcsolása a nemzeti védett INTRANET és a NATO védett információs rendszerébe. Nyilvánvaló, hogy a hosszú távú fejlesztési tervekben a híradó és informatikai rendszer felújítása hangsúlyosabb feladatként kell, hogy jelentkezzen.

A következő alfejezetekben a Magyar Honvédség stacioner hálózatának főbb problémáit összegzem, majd a második és harmadik fejezetekben az egyes problémákat mélyebben elemezve megoldás javaslatot teszek.

### I.3 A Magyar Honvédség állandó telepítésű hírendszere

A Magyar Honvédség jelenleg különálló híradó ill. informatikai rendszerrel rendelkezik, ahol a kommunikációs infrastruktúra egy része (csomagkapcsolt hálózati infrastruktúra) az informatikai szolgáltatásokat biztosító felelőségi körébe tartozik, a másik része (a tradicionális TDM (időmultiplex) infrastruktúra) pedig a híradó parancsnokság alá. Ennek a megközelítésnek történelmi okai vannak, mert korábban az IP protokoll térnyerése előtt, távközlési ill. híradó szakemberek foglalkoztak a kommunikációs infrastruktúrával, és informatikai szakemberek a számítógépes hálózatokkal.

Mára ez a megközelítés elavulttá vált, mert a kommunikációs infrastruktúra nagy része adathálózati alapú lett – amit kommunikációs szakemberek kell, hogy üzemeltessenek. Az előző fejezetben említett *hírendszert* definíciójából is látszik, hogy hír és az információ, technológia és módszerfüggetlen átviteléről van szó.

A számítógépes informatikai adatok átvitele, akár csak a hangátvitel pusztán egy a kommunikációs hálózat által nyújtott képességek között. Az IP csak egy új technológia, nem jelenti azt, hogy azok az alapelvek amik korábban érvényesek voltak a híradó/kommunikációs rendszerekre azok ma, egy új technológiai alapon nem lennének elvárások.

**Meglátásom szerint, jelen pillanatban a Magyar Honvédség a híradó és az informatikai rendszert, mint szolgáltatást nyújtja a többi csapategység számára.** Fontos, hogy a híradórendszert és informatikai rendszer és a híradó és informatikai csapatok által nyújtott támogató tevékenységet a többi csapategység, mint egy szolgáltatást kezelje. Amennyiben ez egy szolgáltatás, még hozzá kommunikációs szolgáltatás, akkor ennek a jóságát a polgári távközlésben megszokott SLA (Service Level Agreement – szolgáltatási szint szerződés) szolgáltatás paraméterekkel mérhetjük (előző alfejezetben megemlítettem néhányat, ezen szolgáltatás paraméterek közül), ehhez az infrastruktúra ma a Magyar Honvédség bizonyos szervezeti egységeiben rendelkezésre áll. Szintén fontos lenne (de ez egy messzebbre mutató kérdés), hogy az egyes alegységekkel, ezen kommunikációs szolgáltatás alapján az egyes szolgáltatásokra szolgáltatási paramétereket egyeztetni, ill. valamilyen módon betartani.

Jelen pillanatban ilyen szolgáltatási paraméterek az Egységes Kormányzat Gerinchálózat (röviden EKG) mint kormányzati szolgáltatás vonatkozásában vannak, ugyanakkor szükséges lenne, hogy a Magyar Honvédség saját hálózatát is, mint egy a Honvédség céljaira használt szolgáltató kommunikációs hálózatot kezelje. Ennek elengedhetetlen része, hogy a szolgáltatás-menedzsment része legyen a meglévő gyakorlatnak.

Szolgáltatás-menedzsment alatt a Magyar Honvédség hálózata által nyújtott szolgáltatások állandó és proaktív figyelését értjük, a szolgáltatási paraméterek betartása érdekében. Ennek egy része (hibamenedzsment) megvalósult már a Magyar Honvédségnél, azonban ez nem proaktív, mert nem megelőzi az esetleg előforduló hibát, hanem a hiba előfordulása után, felfedi, és elhárítja azt. Némi proaktív támogatásra, a forgalom megelőző vizsgálatára azonban van példa: a stacioner híradó hálózatban mérik a forgalom irányát és típusát, valamint működik egy forgalomelemző csoport, amely ebből von le következtetéseket, azonban ezeket nem használja minden csapategység, és nem működik hibameglévő célzattal,

elsődleges célja a kapacitástervezés (kihasználtság figyelés) ill. a távközlési szolgáltatókkal való elszámolás.

A szolgáltatási paraméterek betartását állandó mérésekkel, megfigyelésekkel végezhetjük el. A kommunikációs hálózatokban a technológia jellegétől függően különböző szolgáltatás paramétereket, a szolgáltatás jóságát más-más paraméterekkel, mérési módszerekkel mérhetjük. A TDM alapú transzport hálózatokban az elsődleges jellemző ebből a szempontból a bithibaarány (BER). A hang ill. kapcsolatorientált technológiáknál forgalom esetében a hangminőség (szubjektív jellemző), a hívásfelépítés sikerességének aránya, hívásbontás/megszakadás aránya azok a jellemzők amelyek alapján a kapcsolatorientált technológia vagy szolgáltatás jóságát megmondhatjuk.

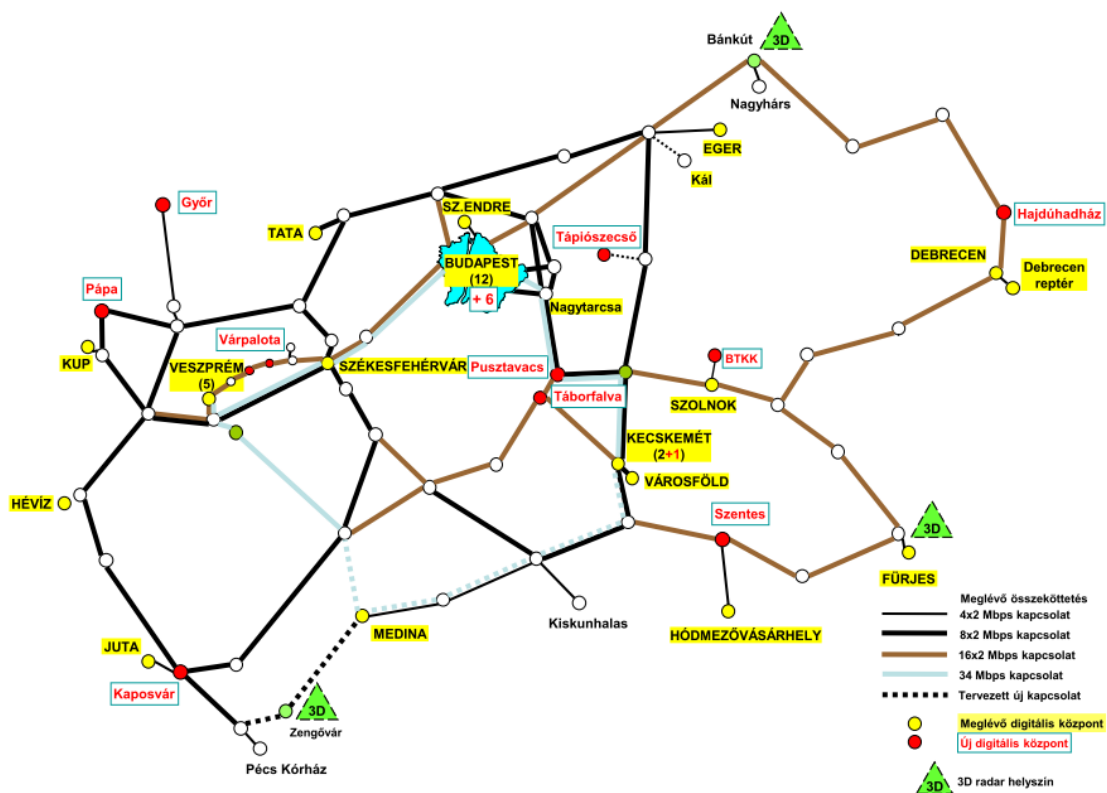
A csomagkapcsolt hálózatokban a QoS mérése napjaink egyik legfontosabb gyakorlati műszaki problémáját jelenti. A legtöbb hálózatban mérik a linkek jóságát különböző paraméterek mellett (hibás csomagok, hibás frame-k száma), azonban ez egy teljes hálózati szolgáltatás esetén nem elegendő. Ennek oka az, hogy ezen paraméterek adott fizikai kapcsolatra vonatkoznak, nem egy teljes útvonalra, ill. szolgáltatásra. Erre szintén léteznek technikák (round trip delay figyelése, ICMP (Internet Control Message Protocol) csomagok segítségével), amellyel a szolgáltatás alapvető rendelkezésre állását figyelhetjük, azonban ez nem árul el semmit arról, hogy az adott alkalmazás által megkövetelt különböző SLA-ban definiált szolgáltatás minőségi (QoS) paraméterek hogyan teljesülnek. Ehhez olyan jellegű adatra, ill. adatfeldolgozó rendszerre lenne szükség, amely a két szolgáltatás átadási pont között méri a szolgáltatás minőségi paramétereit.

A mai napig, a Magyar Honvédség hálózatában széleskörű, teljes hálózatra kiterjedő elemzés amely ilyen mérési eredményeken alapult volna – nem készült, ennek hiánya pedig a hosszú távú stratégiai tervezést, valamint a kapacitás és szolgáltatástervezést megnehezíti. **A kapacitás és szolgáltatástervezés hiánya azt eredményezi, hogy a szakembereknek nem áll a rendelkezésükre olyan részletes méréseken és elemzéseken alapuló anyag, amely alapján megalapozott fejlesztési tervekkel állhatnának elő. Másik fontos észrevétel, hogy a csomagkapcsolt hálózat megbízhatóságának mérésére jelenleg semmilyen módszer nem használt Magyar Honvédség hálózatában.** Ez azért lényeges, mert a szakirodalom szerint, a csomagkapcsolt hálózat útválasztó eszközök konfigurációs és szoftver problémái felelősek a hibák több, mint 50%-áért [14], és a biztonsági rések jelentős részéért is. A kilencvenes évek folyamán jelentős fejlesztések történtek ebben az irányban. Ebben az anyagban részletesen ezekre a technológiai fejlesztésekre nem térek ki, ezeket ismertnek feltételezem (a mellékletben található egy áttekintő fejezet erről, valamint az itt szereplő technológiai újdonságokról).

Nincsenek jelen pillanatban olyan statisztikák, amely azt mutatnák, hogy a hibák hány százaléka ered ilyen jellegű hibákból a Magyar Honvédség hálózatában. A problémát árnyalja, hogy ezen, IP alapú eszközök megfelelő konfigurációja egy nagyságrenddel bonyolultabb, mint a korábbi technológiát képviselő híradó transzport rendszereké, és a megfelelő emberek megtalálása, képzése komoly humán erőforrásbeli problémát jelent a Magyar Honvédség számára (ezért is alapvető fontosságú, hogy a Zrínyi Nemzetvédelmi

Egyetem, folytatva hagyományait kiváló híradó tiszteket képezzen, akik az új típusú rendszerek konfigurálásában gyakorlottak).

A fenti QoS szolgáltatásminőségi paraméterek, az előző alfejezetben említett, a hírrendszerrel szemben támasztott követelmények ismeretében válnak fontossá, hiszen semmilyen módon nem bizonyítható, vagy állapítható meg, hogy a hírrendszerrel szemben támasztott követelményeket a hírrendszer teljesíti-e. Jelen helyzet szerint, a mélyebb műszaki problémákat civil cégek oldják meg, akikkel támogató szerződést köt a Magyar Honvédség. A civil támogató cégek és a Magyar Honvédség elvárásai sokszor eltérnek egymástól, amint azt Magyarné Kucsera Erika is kiemeli a cikkében [15]. Az egyik fő problémát az okozza, hogy a civil támogatási szerződések a minősített helyzeteket Vis Maiornak minősítik, amire a szerződés hatálya nem terjed ki, a Magyar Honvédség híradórendszere pedig ilyen esetekben is természetesen működőképes kell, hogy legyen, sőt az ilyen esetek kiemelt fontosságúak! Az egyik megoldás a problémára a [85]-ban szereplő német példa lehet, hiszen egy kormányzati tulajdonú céggel már köthető olyan szerződés, amely nem zárja ki a minősített helyzeteket.



I-1. ÁBRA FIKTÍV HÁLÓZATI ÁBRA A 3D RADARKÉPEK TOVÁBBÍTÁSÁRA

A I-1. számú ábra a Magyar Honvédség jelenlegi stacioner transzport hálózatát mutatja, melyen látszik, hogy a honvédség stacioner transzport hálózata egy mikrohullámú PDH (Plesiochronouse Digital Hierarchy) nx2 Mbit/s összeköttetésekből álló TDM alapú transzport gerinchálózatból áll. Másrészt pedig egyes csomópontokon az EKG-re csatlakozva egy adatátviteli gerinchálózatból amely csomagkapcsolt IP/MPLS alapú és alapvetően

informatikai célokat szolgál. Az IP/MPLS hálózat az EKG IP/MPLS hálózatának LER/PE – routereihez kapcsolódik jelenleg 6 központi csomóponton 200 Mbit/s kapcsolattal, ill. további tizenhárom telephelyen 2Mbit/s-es kapcsolattal. A hangszolgáltatás nagy része digitális, ISDN (Integrated Services Digital Network) központokból áll, amelyeket a mikrohullámú transzport gerinc köt össze – többségében ISDN PRI/BRI (Primary Rate Interface/Basic Rate Interface), illetve néhány esetben analóg interfészekkel, mely az EDR-hez (Egységes Digitális Rádióhálózat) is kapcsolódik az ISDN központokon keresztül.

Az adott stacioner végponttal rendelkező telephelyen legtöbb helyen strukturált hálózat van kialakítva, ez a központi telephelyek esetében legalább a CAT5 (szabványformátum) szabványnak megfelel. Honvédségi felhasználásban gyakorlatilag nincsen vezeték nélküli szabványoknak (802.11a/b/g/n –WiFi (Wireless Fidelity), ill. 802.16e Wimax) megfelelő hálózat. Ezeknek az alkalmazási lehetőségeit a ZMNE (Zrínyi Miklós Nemzetvédelmi Egyetem) jelenleg is kutatja, illetve egyes híradó gyakorlatokon teszteli (COMMET 2007 – Wimax), ezek alkalmazása fontos lenne elsősorban a tábori hírendszerekben, azonban meg kell győződni ennek a biztonsági aspektusairól. Ez utóbbi a Wimaxban jobban támogatott, már csak azért is, mert védett frekvenciákon működik.

Az MH (Magyar Honvédség) zártcélú távközlő hálózatának gerincét az országot behálózó, 98 db mikrohullámú állomásból, 232 darab üzemelő mikrohullámú berendezésből álló, saját tulajdonú mikrohullámú hálózat, valamint az elmúlt időszak fejlesztéseinek eredményeképpen kialakult 51 darab (újak: Kecskemét SOF, Győr, Pápa, Kaposvár, Szentés, Hajdúhadháza, Pusztavacs, HIM, TH, BHP, Irinyi, Bánkút) (ISDN) digitális távbeszélőközpontot tartalmazó digitális távközlő hálózat alkotja. Működik még a rendszerbe integráltan 38 db – főleg kis kapacitású – elektronikus analóg központ is, melyek kiváltása még nem történt meg.

Az MH zártcélú távközlő hálózatának továbbfejlesztése érdekében 2004 évben az MH Mikrohullámú Hálózata, valamint az MH Digitális Távközlő Hálózata fejlesztésére közbeszerzési eljárás került lefolytatásra. 2005 év végéig olyan kapacitású hálózat jött létre, mely biztosítja a számítógépes rendszerek szükséges átviteli útjait. A haderőátalakítási folyamat során 4 már digitalizált helyszín került megszüntetésre, melynek során felszabaduló ISDN központok 2006 évben új helyszínekre (Tápiószecső, Táborfalva, Bp. Tünde utca, MH Központi Katonai Kórház) kerültek áttelepítésre. 2006 évben a fenti 4 helyszínen, Székesfehérváron és Nagytarcsán került sor strukturált hálózat kiépítésére.

A stacioner hálózat az átviteli kapacitást biztosítja az informatikai és beszédcélú kommunikációs hálózat számára. Szervezeti szempontból a beszédcélú kommunikációs hálózat a stacioner hálózat részét képezi.

## I.4 A Magyar Honvédség állandó hírrendszerének vizsgálata

A Magyar Honvédség hálózatának felépítését szekunder anyagokból nyilvánosan hozzáférhető anyagok alapján a híradó parancsnoksággal konzultálva vizsgáltam. Műszaki megállapításaimat 2009. év december 31-el zártam le, az akkor fennálló problémák, megállapítások képezik az értekezésem alapját. A hálózat technológiai fejlettségét a polgári alkalmazásban széles körben hozzáférhető rendszerekkel hasonlítottam össze, megállapításaimat a polgári távközlésben hozzáférhető megoldásokkal összevetve tettem meg.

### A Magyar Honvédség állandó hírrendszerében felmerülő technológiai jellegű problémák

Az előző fejezetben ismertetett állandó transzport hálózat nem felel meg a XXI században jelentkező technológiai igényeknek. A legfontosabb problémák a hálózati struktúrájával a következők:

1. **Inhomogén hálózati elemekből és technológiákból épül fel**, hiszen vegyes TDM és csomagkapcsolt alapú rendszerek alkotják, amelyek több humán erőforrást igényelnek az üzemeltetői oldalról (nem egységes technológia miatt). Másrésztől nem teszik lehetővé az egyes rendszerek hálózati integrációját (ezen integrációt egy egységes hálózati protokoll felett lehet elvégezni, ami az esetek legtöbbszörében – szinte kizárólag – az Internet Protokoll), a technológiai egyszerűsítés szempontjából célszerű a legköltséghatékonyabb Ethernet/IP protokollokat választani. Inhomogén hálózati technológiákból épül fel, hiszen párhuzamosan működik TDM és csomagkapcsolt alapú technológia a hálózatban, különböző fizikai és adatkapcsolati rétegbeli protokollokkal (pl. E1, soros, Ethernet interfészek párhuzamosan). Az a határozott megállapításom, hogy **költséghatékonyabb egységes Ethernet alapú interfészekre alapuló nagyrendelkezésre állású IP hálózatot** építeni, ezáltal csökkentve a hálózat komplexitását és egységesítve a hálózat által használt első, második és harmadik rétegbeli protokollokat. Ez összhangban van az Összhaderőnemi Doktrínában meghatározott **üzemeltetési előnyökként** megfogalmazott követelményekkel. A fenti problémára adott **javaslatom a harmadik fejezetben** szerepel.
2. Sok esetben a **hálózati erőforrások nincsenek megfelelően kihasználva, nem dinamikus a sáv szélesség kezelése**. A hangforgalom nem tölti meg a mikrohullámú hálózatban rendelkezésre álló kapacitásokat, így a kapcsolatok kihasználtsága alacsony. Az adatforgalom számára dedikált csatornák viszont túlterheltek, telítettek (Ez a probléma OIGH (Országos Internet Gerinc Hálózat) kialakulásával megoldódni látszik). A második fejezetben nyilvánosan hozzáférhető adatokon keresztül egy **új forgalomtervezési megoldást alkalmazva bizonyítom a probléma meglétét, és javaslatot teszek az erőforráskihasználtság javítására**. Ez könnyen belátható más

módon is, így pl. a hálózati forgalom elemzésével, azonban ilyen jellegű adatok nem nyilvánosan hozzáférhetőek, ezért itt adatvédelmi okok miatt nem szerepelnek.

3. **Nem teszi lehetővé** a katonai informatikai rendszerek által megkövetelt **nagyobb mennyiségű adatok gyors átvitelét** kapacitásproblémák miatt. A katonai informatikai rendszerek által generált sáv szélesség alkalmazásfüggő, azonban az adat jellegéből nagyságrendi becslés adható rá. **A második fejezetben részletesebben bizonyítom** ennek **a problémának a meglétét** is, és második és a harmadik fejezetben **megoldást adok az adatátvitel javítására a hálózati kapacitások hatékonyabb alkalmazásával.**
4. **Nincs megfelelő adatátviteli sebességű kapcsolat a stacioner és tábori kommunikációs rendszerek között**, ez is egyértelműen kapacitásprobléma. A két hálózat jellegéből adódóan más célokat szolgál, azonban a két hálózat megfelelő sáv szélességű összekötése szükséges. **A második fejezetben részletesebben bizonyítom** ennek **a problémának a meglétét** is, és a második és a harmadik fejezetben **megoldást adok az adatátvitel javítására Ethernet mikrohullámú eszközök alkalmazásával.**
5. Egyes helyeken elszigetelt LAN-okból (Local Area Network) áll a Magyar Honvédség stacioner hálózata. Ez egy strukturális probléma, ezért célszerű egységes, és minél inkább redundáns, szövevényes hálózatot kialakítani, mert ennek a rendelkezésreállása nagyságrendekkel jobb az elszigetelt hálózatokénál. A hálózati elszigeteltség abból adódik, hogy a hálózat inhomogén hálózati szegmensekből épül fel, így szükségszerűen az integráltságuk alacsony. **A probléma megoldására a javaslatom az egységesített hálózat kiépítése, amely a harmadik fejezetben szerepel.**
6. **Nincs egységes QoS (szolgáltatásminőség) bevezetve a hálózatban**, ami azt eredményezi, hogy jelenleg a hálózat best effort jellegű szolgáltatásokat nyújt (elindult ennek a bevezetése, az IP feletti hangátvitel kialakításával együtt). A hálózat best effort jellegű szolgáltatások mellett csak bizonyos jellegű alkalmazások forgalmát képes átvinni, valós idejű alkalmazások használata ilyen hálózaton nem lehetséges. Bár a jelenlegi informatikai hálózat best effort jellegű, ezen a hálózaton is bevezethető a szolgáltatásminőség, amennyiben a harmadik fejezetben ismertetett szolgáltatásminőségi elveket megtartjuk, de a szolgáltatásminőség tartós biztosítása csak olyan hálózati elemeken lehetséges, amelyek rendelkezésreállása nagy.
7. **A jelenlegi hálózatban nem használtak az IP/MPLS technológia nagyobb megbízhatóságot nyújtó védelmi mechanizmusai**, a jelenleg használt útvonalvédelmi mechanizmusok nem elégségesek ill. megfelelőek katonai gerinchálózat üzemeltetésére. A védelmi mechanizmusok alkalmazásának hiánya azt okozza, hogy a hálózat rendelkezésreállása relatíve alacsony. A probléma oka az, hogy az informatikai hálózatban legrövidebb út (SPF) algoritmust alkalmaznak alapértelmezett beállításokkal. A legrövidebb út (shortest path first – SPF) algoritmusok által biztosított áthidalási idők valósidejű szolgáltatások számára megfelelő finomhangolással alkalmazhatóak csak, erre az informatikai hálózatban használt útválasztók nem alkalmasak, mert ezeket nem támogatják. **A probléma megoldására**

**az informatikai hálózatra a harmadik fejezetben egy egységes IP/MPLS hálózatot javaslok.**

8. **Nincs adathálózati (forgalomtervezés) Traffic Engineering** a hálózatban. Ez azért probléma, mert még abban az esetben is, ha léteznek redundáns útvonalak a hálózatban, a hagyományos (Dijkstra algoritmusok) mindig a legrövidebb útvonalat választják, amely torlódást eredményezhet, még ha egy másik (hopszám szempontjából hosszabb) útvonalon szabad kapacitások állnak rendelkezésre vagy kisebb késleltetésű útvonal is rendelkezésre áll. **A probléma megoldására a második fejezetben egy eszközt adok a forgalomtervezéshez, a harmadik fejezetben pedig meghatározom azokat a hálózati beállításokat amelyek alkalmazásával ezek nagymértékben megkönnyíthetők.**
9. **Nincs releváns hálózati szintű mérés a hálózatban**, vagyis **nem áll rendelkezésre olyan hálózati szintű mérés**, amivel az adott szolgáltatás által megkövetelt paraméterek bizonyítottan rendelkezésre állnának. A Magyar Honvédség hálózatának a mérése a csapatok által adott visszajelzéseken alapul, azonban nincs olyan független minőségellenőrző módszer amely segítségével ez műszakilag mérhető lehet. **Ennek megoldására a harmadik fejezetben Ethernet tapeket használatot javaslom.**
10. A stacioner hálózat két meghatározó technológiából épül fel (TDM alapú átviteltechnikai, és kapcsolástechnikai elemekből) és kevert hálózati technológiát alkalmaz, ahol a kapacitások nagyobb részét az adatforgalom fedi le, ezek azonban az informatikai hálózathoz tartoznak. A jelenlegi állapot ilyen jellegű kialakulása történelmi okokra vezethető vissza. A korszerű hálózatokat az alábbi háromrétegű megközelítés jellemzi:
  - **átviteltechnikai hálózati réteg** (ennek célja az átviteli kapacitások biztosítása), a szóba jöhető technológiák vezetékes vagy vezeték nélküli első rétegben üzemelő átviteltechnikai berendezések (mikrohullámú eszközök, ill. hullámhosszmultiplex eszközök)
  - **kapcsoló hálózati elemek** (a modern hálózatokban ezek IP kapcsolóelemek; útválasztók vagy kapcsolók)
  - **szolgáltatást megvalósító hálózati rétegek** (ilyen pl. a beszédkommunikációt megvalósító IP-képes alközpontok, webserverek, ftp-szerverek stb.)

Ennek a megközelítésnek megfelelően szükséges a hálózatot felülvizsgálni, mert csak egy ilyen megközelítéssel lesz képes a közeljövő katonai informatikai alkalmazásait (szolgáltatást megvalósító rétegek elemei) – kellő biztonsággal és rendelkezésreállással megvalósítani. A hálózat átviteltechnikai és útválasztó hálózatelemeit harmadik fejezetben vizsgálom felül.

Röviden összefoglalva, a fenti okok miatt a Magyar Honvédség híradó rendszere elmarad a fejlettebb NATO tagállamokétól, és elmarad a magyar polgári távközlési gerinchálózatoktól is, a jelen fontosabb követelményeit kielégíti, azonban nincs felkészítve a közeljövő



kihívásaira.

A fenti problémákat két főbb csoportra osztanám, az egyik kapacitás jellegű probléma, erre a megoldási javaslatomat a második fejezetben ismertetem. Meglátásom szerint a fenti felsorolás 2., 3., 4., 8., problémája kapacitásproblémára vezethető vissza, amin hosszabb távon pedig tudatos kapacitástervezéssel (második fejezetben ismertetett megoldáson) keresztül, rövidebb távon megfelelően kiválasztott technológiával (harmadik fejezetben ismertetett megoldás) javíthatunk.

A felsorolásban szereplő többi probléma technológiai jellegű, amelyet a harmadik fejezetben ismertetett módon javaslok megoldani.

### **A Magyar Honvédség állandó telepítésű hálózatában felmerülő egyéb problémák**

A Magyar Honvédség stacioner hálózatában a technológiai és kapacitáskorlátok mellett, szervezeti, vagy üzemeltetési módszertani hiányosságok is vannak. A legfontosabb hiányosságokat az alábbiakban összegeztem:

A Magyar Honvédség infokommunikációs rendszere **különálló híradó és informatikai rendszerből áll** – szemben az 1999-es NATO csúcson elfogadott doktrínával, amely ezt egységes egészként kezeli. Ez egy kettős probléma, egyrészt szervezeti jellegű, másrészt műszaki jellegű. A műszaki jellegű problémát a tudatos tervezéssel hosszabb távon kiküszöbölhetjük, és egy egységes IP protokollon alapuló infokommunikációs rendszert hozhatunk létre. Ennek elvi akadálya nincs, gyakorlati akadálya is inkább pénzügyi vonatkozásai miatt van. A szervezeti átalakítás szükségessége az Összhaderőnemi Doktrínából következik, ennek a megoldásával ebben az értekezésben nem kívánok foglalkozni.

**Nincs szolgáltatásalapú megközelítés** a Magyar Honvédség hálózatában. A szolgáltatás alapú megközelítés hiánya elsősorban szemléletváltásbeli kérdés – amire úgy gondolom, hogy a híradó és informatikai szervek készen állnak. A korábbiakban leírt szolgáltatás alapú megközelítés a német hadseregben kiválóan bizonyított [17], ahol a privát szféra és a kormányzat közös cége [17] felel a C4I infrastruktúra üzemeltetéséért, és nyújtja ezt a szolgáltatást a német hadseregnek. Fontos megemlíteni, hogy a modell korábban több alkalommal bizonyított pl. a szovjet hadseregben a Nagy Honvédő Háborúban is [35]. Ez a modell több szempontból előnyös. A kormányzat képes a stratégiai és biztonsági kérdéseket a tulajdonosi viszonyából adódóan biztosítani, ill. a meglévő szakmai tudást, más – elsősorban kormányzati – ügyfeleknél hasznosítani.

A fontosabb változás, az egyes csapatokkal kötött szolgáltatási megállapodás lenne, amely definiálná az egyes csapategységek híradó igényeit és meghatározná az elvárásokat a híradó és informatikai szervek felé – így lehetne szavatolni azt, hogy a híradó rendszerrel szemben elvárt minőségi szint az egyes csapatok felé nyújtható legyen, ez az alapja a hírszolgáltatás megfelelő minőségbiztosításának.

**Nincs meghatározott szolgáltatási szint** az egyes csapatok felé. A szolgáltatási megállapodás

hiánya azt is jelenti, hogy nincs olyan paraméter, amit szavatolni kellene az egyes egységek felé, és nincs olyan paraméter, ami alapján bizonyítható lenne, hogy az adott paraméter, az adott körülmények között biztosított. Ez a kérdés a híradó és informatikai egységek számára fontos kérdés. Ezeknek bevezetése nem műszaki kérdés.

A fenti problémával összefügg, hogy nincs használatban semmilyen **SLA ellenőrző rendszer** a szolgáltatási szint figyelésére. Miután szolgáltatási megállapodás sincs, valamint a szolgáltatási szint sincs definiálva, ennek az ellenőrzése, és az ellenőrző rendszere is manuális úton megoldott. Ebből következik, ill. ezzel összefügg, hogy **nincs** olyan **módszer** amelyet a Magyar Honvédség általánosan használna a **szolgáltatásminőség mérésére**, ill. a hírszolgáltatás minőségének mérésére, és ezen módszerek hiánya hátráltatja a stratégiai, kapacitás és szolgáltatás tervezést. A mérés hiányára visszavezethető hibák, pontatlanságokat okoznak a stratégiai tervek készítésekor, amely hibák költségvonzattal járnak, hiszen hosszabb távon az optimálistól eltérő terv valósul meg.

Talán a legfontosabb probléma az, hogy ma a tervezési folyamat nem tud a mérés hiánya miatt megalapozott adatokon nyugodni. Erre rövid és közép- hosszú távú megoldás létezik, a rövid távú megoldás egy tanúsító szervvel elvégzett szolgáltatásminőségi „audit”, aminek az eredménye, egy a problémákra, hibaforrásokra, és potenciális megoldásokra rámutató összefoglaló elemzés lehet. (Nem minőségbiztosítás audit!). Közép és hosszú távú megoldása pedig a különböző mérési módszerek, ill. SLA menedzsment bevezetése.

A fenti viszonyokat tudomásul véve, a második fejezetben egy olyan lehetséges stratégiai és kapacitástervezési módszert ajánlok, amelyet a jövőben használni lehet forgalmi tervezéskor és technológiai tervezéskor.

A híradó és informatikai vezető szervek emberi erőforrás hiánnyal küzdenek. Ezt a problémát itt csak felvetem, a probléma részletes vizsgálata, megoldása nem tárgya értekezésemnek. Az emberi erőforráshiányok megoldása folyamatban van, itt inkább arra térnék ki, hogyan lehet, könnyíteni a helyzeten. Az egyik megoldás lehet a korábban már említett német modell alkalmazása. Tovább könnyíthet a helyzeten megfelelő ún. provisioning (létrehozási, felügyeleti) rendszer alkalmazása, ahol az alapvető üzemeltetési feladatokat grafikus felületen keresztül tudják elvégezni az üzemeltetők, és így a feladatokat több szintre – a szakemberek ismereti szintjének megfelelően – el lehet osztani. A fent vázolt problémák megoldására mind műszaki változtatások, mind szervezeti átalakítások szükségesek.

## **I.5 Összegzés**

Az új évezred új kihívásokat hozott mind a nemzetközi, mind a hazai katonai infokommunikációs rendszerek kialakításával kapcsolatban. Ezen legfontosabb kihívások között a harmadik generációs, **információ-központú hadviselésre történő áttérést**, az egyre szélesebb körben használt **katonai információs és kommunikációs rendszerek megfelelő kiszolgálását**, ill. az **új katonai infokommunikációs koncepciók támogatását** emeltem ki értekezésem bevezetést követő első fő fejezetében.

Ebben a fejezetben arra kerestem a választ, hogy az Összhaderőnemi Doktrína milyen követelményeket, milyen elvárásokat támaszt a szűkebb kutatási területem - Magyar Honvédség híradó és informatikai rendszerével kapcsolatban, ill. mennyire felel meg, tartalmazza a választ azon kihívásokra, amelyet megfogalmaztam.

A fejezetben kiemeltem, hogy **az Összhaderőnemi doktrína a Magyar Honvédség híradó és informatikai rendszerét, mint egy harci támogató rendszert** fogalmazza meg, és új megközelítés lehetőségét vettem fel a **támogató-támogatott viszonyt** illetően – mellyel részletesebben a következő fejezetben foglalkoztam. Meghatároztam a főbb irányvonalakat (rendszerintegrációs, katonai műszaki, és biztonsági, információvédelmi), amelynek mentén a **híradó és informatikai rendszerrel** szemben elvárt követelményeket kell teljesíteni. Az Összhaderőnemi Doktrína alapján bemutattam azon irányelveket, amelyek mentén a híradó és informatikai rendszert ki kell alakítani és felhívtam a figyelmet, hogy a doktrína az információs műveletek támogatását is a híradó és informatikai rendszer feladataként jellemzi.

Az Összhaderőnemi Doktrína meghatározta azon irányelveket, amelyek mentén a Magyar Honvédség híradó és informatikai rendszerét tervezni, kivitelezni és üzemeltetni szükséges. Ezen irányelvek lehetővé teszik a polgári életben használt nagy rendelkezésreállású hálózatok tervezéséhez, kivitelezéséhez és üzemeltetéséhez használt módszerek és eszközök használatát, amennyiben a katonai alkalmazásból adódó speciális követelményeket figyelembe lehet venni. A rendszerfejlesztési koncepció hiánya az, ami ennek az értekezésnek az elkészítésére sarkalt, hogy mutassak egy olyan lehetséges fejlesztési irányvonalat, amelyet a jövőben követni lehet.

**A jelenlegi hálózat technológiai szempontból elavult**, és műszaki problémákkal küzd, az időmultiplex (TDM) hálózati réteg már nem képes kiszolgálni az adathálózat sávszélességigényeit (ezt a második fejezetben részletesen fogom elemezni), ill. technológiailag sem megfelelő módon fedi le a csomagkapcsolt hálózat igényeit, hiszen a csomagkapcsolt hálózat protokollkonverziókon esik át. A hálózat csomagkapcsolt átviteltechnikára történő javasolt módosítását a harmadik fejezetben fogom bővebben kifejteni.

## II. A Magyar Honvédség stacioner hálózatának forgalmi vizsgálata

*„A háborúban minden egyes lépés előzetes ismereteket követel.”*

Sun Tzu, A háború művészete

Ebben a fejezetben azt vizsgáltam, hogy a Magyar Honvédség stacioner hálózata mennyire felel meg azoknak a sávszélesség követelményeknek, amiket a modern katonai informatikai alkalmazások támasztanak. Az első fejezetben bemutattam, hogy a stacioner hálózatban az alábbi erőforrási kapacitásproblémára visszavezethető technológiai jellegű hibák vannak:

1. Sok esetben a **hálózati erőforrások nincsenek megfelelően kihasználva** (a hangforgalom nem tölti meg a mikrohullámú hálózatban rendelkezésre álló kapacitásokat, így a kapcsolatok kihasználtsága alacsony, viszont adatforgalom telíti a hálózatot (Ez a probléma OIGH kialakulásával megoldódni látszik)
2. **Nem teszi lehetővé** a katonai informatikai rendszerek által megkövetelt **nagyobb mennyiségű adatok gyors átvitelét**, mely egyértelműen kapacitásproblémára vezethető vissza.
3. **Nincs megfelelő adatátviteli sebességű kapcsolat a stacioner és tábori kommunikációs rendszerek között.** Ez szintén kapacitásproblémát jelent.
4. Egyes helyeken **elszigetelt LAN-okból áll a Magyar Honvédség stacioner hálózata.** Ez egy strukturális probléma, célszerű egységes, és minél inkább összekötött hálózatot kialakítani, mert ennek a rendelkezésreállása és a kapacitásviszonyai is nagyságrendekkel jobbak az elszigetelt hálózatokénál.
5. **Nincs Traffic Engineering** a hálózatban.

A követelmények vizsgálatához a fejezet első felében egy mintaalkalmazás, egy katonai háromdimenziós radar **sávszélesség igényszámítását végeztem el.** Ilyen háromdimenziós katonai radart több telephelyen használnak Magyarországon. A fejezet második felében azt **elemzem, hogy** három forgalmi esetben a **stacioner hálózaton hogyan alakulnak a forgalmi viszonyok.** A fejezetben tudományos módszert alkalmazok arra, hogy:

- az adatkapcsolt hálózaton különböző végponti forgalmi eseteket figyelembe véve, a kapacitásviszonyok hogyan alakulnak
- az adatkapcsolt hálózaton, hogyan modellezhető egy forgalmi helyzet
- egy hálózati modellen milyen torlódási és túlterhelési problémák jelentkeznek
- ezek a túlterhelési problémák mit eredményeznek a valós hálózatban
- a stacioner hálózat hogyan reagál az alkalmazás réteg által megnövelt hálózati forgalomra

Ez a módszer gyakorlatban mind az oktatásban, mind az iparban hasznosítható. Oktatás területén jól modellezi az erőforrás problémák által okozott járulékos forgalmi problémákat, ezért **javaslom az alkalmazását mind a műszaki mind a katonai műszaki képzésben**. Az iparban az erőforrásmodellezés, a kapacitástervezés tudatosabb döntésekhez, pontosabb döntéshozói képhez vezet, így költséghatékonyabbá és kiszámíthatóbbá teszi az átviteltechnikai és IP hálózatok üzemeltetését és modellezését.

Az alábbiakban ismertetett módszer a Magyar Honvédség stacioner hálózatának tudatosabb forgalmi tervezését is elősegíti, a stacioner hálózat kapacitásproblémáit következőképpen segíti:

1. A módszer használatával **a hálózati erőforrások megfelelőbb kihasználtsága** érhető el
2. Adatforgalom növekedés esetén **a kiszolgáló hálózat szükséges kapacitásviszonyai meghatározhatóak** a módszer segítségével, így a hálózat szükséges sávszélességviszonyai pontosabban modellezhetőek
3. **Stacioner és tábori hálózatok közti adatforgalom kapacitástervezésére** használható a módszer
4. **A stacioner hálózat folyamatos és időszakos forgalmi modellezésére** alkalmas a módszer, segítségével megállapíthatóak a hálózat szűk keresztmetszetei és kritikus forgalmi helyei

## II.1 Sávszélességigény számítás 3D radar képekre

A katonai informatikai alkalmazások által felhasznált sávszélességek erősen függnek a katonai informatikai alkalmazás jellegétől. Ebben az alfejezetben egy becslési módszert mutatok be, a katonai informatikai alkalmazás sávszélességének a meghatározására, egy 3 dimenziós katonai radar sávszélességét alapul véve. Ezt a példabecslést (amely nem helyettesítheti a valós forgalmi viszonyok méréseken alapuló meghatározását) azért készítettem, hogy a katonai informatikai alkalmazások által használt sávszélesség mennyiségre egy nagyságrendi becslést tudjak meghatározni. A Magyar Honvédség által használt katonai informatikai alkalmazások sávszélesség viszonyai nem publikálható adatok, ezért a kutatáshoz ezt a mintaszámítást veszem alapul.

Az alábbi kalkuláció során az egyik legnagyobb adatforrásnak tekinthető 3D (három dimenziós) radarok sávszélességigényét számoltam ki. A kalkulációhoz ezeket az alapadatokat vettem figyelembe:

Paraméterek	Paraméter értékei
Radar hatótávolsága (km)	100
Pontosság (cm)	50
Tömörítési arány	1000000
Képfreállítás gyakorisága (s)	60

II-1. TÁBLÁZAT 3D RADAR PARAMÉTEREK

A radar hatótávolságát 100 km-re becsültem, ez alacsonyabb, mint ezen radarok valós képessége. A pontosságot úgy határoztam meg, hogy mennyi az egyes letapogatási pontok közt a távolság. A kettőnek a hányadosa megadja a képpontok számát, egy dimenzióban:

Képpontok száma 1 dimenzióban	200000
-------------------------------	--------

II-2. TÁBLÁZAT KÉPPONTOK SZÁMA 1 DIMENZIÓ

A 3D radar – nevéből is adódik – 3 dimenzióban működik, ezért a fenti képpont számok köbét kell vegyük a sávszélességigény számításához. Itt elhanyagolással élek, mert Descartes koordináta-rendszerben, egy kockát számolok, a valós eset pedig egy félgömb. Ez a képpontok darabszámát igen, a nagyságrendjét nem változtatja meg.

Képpontok száma 3 D-ban (Descartes kockát feltételezve)	8000000000000000
---	------------------

II-3. TÁBLÁZAT KÉPPONTOK SZÁMA 3D-BEN

Látható hogy a tömörítetlen képpontok száma  $8 \times 10^{15}$

Az információ átviteléhez meglehetősen jó tömörítést lehet alkalmazni, mert csak a statikus jellegű információknak kevés az információértéke, szinte kizárólag a delta - dinamikus információ mennyiség számít. Ezt úgy próbáltam szimulálni, hogy a tömörítési arányt meglehetősen nagyra, 1:1000000-ra vettem, így a tömörített adatmennyiség 1 GB-ra adódik (jelen számításban azt feltételeztem, hogy 1 képpont 1 bitnyi információnak felel meg). Ez egy önkényesen meghatározott szám, amely nagy valószínűséggel felülbecsüli a valós tömörítési arányt, ez azonban ebben az esetben megtehető. Amennyiben kisebb a tömörítési arány, azzal az átvendő adatmennyiség nő, amely még nagyobb sávszélességigényt jelent.

Tömörített adatmennyiség MB(megabájt)-ban	1000.00
---	---------

II-4. TÁBLÁZAT TÖMÖRÍTETT ADATMENNYISÉG

Hogyha azt feltételezzük, hogy minden 60 s-ben kell új teljes képet átvinni, ebből számíthatunk egy szükséges sávszélesség igényt.

Sávszélességigény Mbit/s	133.33
--------------------------	--------

II-5. TÁBLÁZAT SÁVSZÉLESSÉGIGÉNY

Látható, hogy a fenti paraméterek mellett, a 3D radarok adatainak sávszélességigénye 133Mbit/s-re jön ki.

Ezt összehasonlítva a fejezet további részében szereplő BANKUT, ZENGOVAR és FURJE telephelyeken alkalmazott mikrohullámú berendezésekkel a sávszélességeket az alábbi táblázatban (II-6. táblázat – 3d radarállomások rendelkezésre álló sávszélességei) tüntettem fel azt láthatjuk, hogy a **jelenleg használt mikrohullámú berendezések nem képesek ilyen sávszélesség igény kielégítésére.**

Élazonosító	Induló csomópont azonosítója	Végcsomópont azonosítója	Teljes Sávszélesség [Mbit/s]
<b>ZENGOVAR-B1</b>	ZENGOVAR	B1	32.00
<b>ZENGOVAR-MEDINA</b>	ZENGOVAR	MEDINA	32.00
<b>N3-N2</b>	BANKUT	N2	32.00
<b>BANKUT-BAZ2</b>	BANKUT	BAZ2	32.00
<b>FURJE-BE2</b>	FURJE	BE2	8.00

II-6. TÁBLÁZAT – 3D RADARÁLLOMÁSOK RENDELKEZÉSRE ÁLLÓ SÁVSZÉLESSÉGEI

A fentiekből megállapítható, hogy egy modern 3D radar adatátviteli sebességigényét nem képes kielégíteni a jelenlegi stacioner hálózat, már rögtön a belépő csomóponton nincs kellő mennyiségű sávszélesség.

A fenti kalkuláció is mutatja, hogy szükséges a stacioner hálózat forgalmi viszonyait, jövőállóságát vizsgálni. A fejezet további részében több sávszélesség minta mellett elemzem a kialakult forgalmi viszonyokat azért, hogy meg tudjam állapítani, hogy hol alakulnak ki forgalmi gócpontok, ill. milyen forgalommenyiségre kell a hálózatot méretezni. A fejezet további részében a teljes hálózatot veszem górcső alá, három forgalmi esetet alapul véve.

## II.2 Forgalmi esetek szimulációja

A fejezet ezen részében a Magyar Honvédség stacioner hálózatának forgalmi viszonyait vizsgáltam, 3 forgalmi esetet figyelembe véve. Az egyes forgalmi esetek megfelelnek a 90-es, a 2000-es és 2010-es évek múltbeli forgalmának.

A forgalmi viszonyok vizsgálatához a TOTEM Forgalmi szimulátort használtam [18]. A forgalmi szimulátor egy HP Proliant ML 150G2-s szerveren futott, 80GB (Gigabájt)os mirroring RAID -be szervezett merevlemezekkel, 1 GB-nyi memóriával, 2.6.24-26-generic SMP kernellel Ubuntu linux 8.04-es operációs rendszer alatt. A telepítési környezet megkívánta az ANT alkalmazáserver bizonyos komponenseinek a telepítését ill. TOTEM alkalmazást. Ezt a környezetet gyakorlatilag bármilyen végfelhasználói forgalomban kapható

számítógépen előállíthatjuk. A használt szoftverek licensz GPL (General Public License) tehát szabadon felhasználható kutatási, bizonyos feltételek teljesítése mellett pedig kereskedelmi célokra is. Az eredeti szoftveren konfigurációs módosításokat végeztem, magyarítottam, ill. speciális konfigurációs szoftvereket fejlesztettem hozzá azért, hogy a hálózatelemek felé történő automatizálást megkönnyítsem.

A szoftver részletesebb dokumentációja megtalálható a [19] irodalomban. A szoftver alkalmas arra, hogy a hálózaton a topológia megváltozásakor bekövetkező eseményeket szimuláljuk, akár él- (összeköttetés), akár csomópontkiesés (berendezés) esetén. A szoftver képes forgalmi eseteket szimulálni, számtalan útválasztó algoritmust ismer, a leggyakrabban használt Dijkstra (SPF) algoritmustól kezdve, a CSPF (Constrained Shortest Path First) algoritmuson át számtalan egyéb, jelenleg kutatási célokra használt algoritmuson, át ilyen pl. DAMOTE. Képes előre lefoglalt utak kezelésére, és a különböző tartalékolási technikák szimulálására.

A forgalmi szimulációs szoftverbe a forgalmi viszonyokat, valamint a hálózati topológiát a szoftver topológia szerkesztőjével vittem be. Bizonyos típusú hálózatelemekre, a topológia automatizált beolvasására egy automatizált megoldást dolgoztam ki, ezt azonban ebben az esetben nem használtam.

A topológia bevitelekor a végponti telephelyek kivételével az összes stationer telephely elnevezését megváltoztattam. Az egyes végponti helyszínek mindegyik példában megfelelnek a Magyar Honvédség digitális távbeszélő központokkal rendelkező állomásainak.

A csomópontok listáját az alábbi II-7. táblázat tartalmazza. A táblázat oszlopai sorrendben a következő információkat hordozzák.

- Csomópont azonosító: önkényesen választott csomópontazonosító
- Típus: CORE, vagy EDGE attól függően, hogy köztes csomópont, vagy forgalom indul is a csomóponttól. A nagyobb, ISDN központtal rendelkező telephelyeket tekintettem EDGE csomópontnak (a fejezet további részében részletezve szerepel ez)
- Státusz : lehetséges állapotai, UP (arra utal, hogy élő csomópont), vagy DOWN (nem működő csomópont). Jelentősége akkor van, ha olyan forgalmi eseteket kívánunk szimulálni, amely valamilyen csomópontkiesés esetén vizsgálja a forgalmak alakulását
- Belső azonosító – a szoftver által használt belső azonosítókód

Csomópont azonosítója	Típusa	Státusz	Belső azonosító
<b>K1</b>	CORE	UP	0
<b>K2</b>	CORE	UP	1
<b>TATA</b>	EDGE	UP	2
<b>V1</b>	CORE	UP	3
<b>GYOR</b>	EDGE	UP	4
<b>PAPA</b>	EDGE	UP	5
<b>V2</b>	CORE	UP	6
<b>V3</b>	CORE	UP	7
<b>V4</b>	CORE	UP	8
<b>SZEKESFEHERVAR</b>	EDGE	UP	9
<b>F1</b>	CORE	UP	10
<b>F2</b>	CORE	UP	11
<b>V5</b>	CORE	UP	12
<b>F3</b>	CORE	UP	13



Csomópont azonosítója	Típusa	Státusz	Belső azonosító
F4	CORE	UP	14
VARPALOTA	EDGE	UP	15
F6	CORE	UP	16
V6	CORE	UP	17
VESZPREM	EDGE	UP	18
V8	CORE	UP	19
F5	CORE	UP	20
KUP	CORE	UP	21
HEVIZ	EDGE	UP	22
Z1	CORE	UP	23
T1	CORE	UP	24
T2	CORE	UP	25
JUTA	EDGE	UP	26
T3	CORE	UP	27
F7	CORE	UP	28
F8	CORE	UP	29
B1	CORE	UP	30
ZENGOVAR	EDGE	UP	31
PECSKORHAZ	EDGE	UP	32
MEDINA	EDGE	UP	33
F9	CORE	UP	34
BK1	CORE	UP	35
BK2	CORE	UP	36
BK3	CORE	UP	37
TABORFALVA	EDGE	UP	38
PUSZTAVACS	EDGE	UP	39
SZENTENDRE	EDGE	UP	40
BUDAPEST	EDGE	UP	41
P1	CORE	UP	42
NAGYTARCSA	EDGE	UP	43
P2	CORE	UP	44
N2	CORE	UP	45
N1	CORE	UP	46
P3	CORE	UP	47
KAL	EDGE	UP	48
EGER	EDGE	UP	49
BANKUT	EDGE	UP	50
BAZ1	CORE	UP	51
BAZ2	CORE	UP	52
HAJDUHADHAZ	EDGE	UP	53
DEBRECEN	EDGE	UP	54
DEBRECEN REPTER	EDGE	UP	55
JNSZ3	CORE	UP	56
JNSZ1	CORE	UP	57
HB1	CORE	UP	58
SZOLNOK	EDGE	UP	59
BTKK	EDGE	UP	60
KISKUNHALAS	EDGE	UP	61
BK4	CORE	UP	62
KECSKEMET	CORE	UP	63
VAROSFOLD	EDGE	UP	64
P4	CORE	UP	65
P5	CORE	UP	66
BE1	CORE	UP	67
BE2	CORE	UP	68
BE3	CORE	UP	69
SZENTES	EDGE	UP	70
HODMEZOVASARHELY	EDGE	UP	71
FURJE	EDGE	UP	72

II-7. TÁBLÁZAT – FIKTIV HALÓZATI TOPOLOGIA, CSOMÓPONTOK TÁBLÁZATA

A táblázatban CORE csomópontokkal (II-7. táblázat) jelöltem azokat az állomásokat, amelyek nem rendelkeznek digitális távbeszélőközponttal, így közvetlenül feltételezhetően nem generálnak forgalmat, csak köztes ugrópontokként (ún. repeaterként) szerepelnek a mikrohullámú hálózati láncban. A végponti csomópontokat, amelyek digitális távbeszélőközponttal rendelkeznek EDGE csomópontként jelöltem. A fejezet további részében a hálózat forgalmi viszonyait ábrákon jelöltem. Az ábrákon, színekkel jelöltem, a hálózat éleinek a leterheltségét, a leterheltségeknek megfelelő színek a következők:

- 0-30 % telítettségig zöld
- a 30-60%-os telítettségig sárga
- a 60-100%-os telítettségig piros.

Ezek az ábrák az egyes élek terheltségét tartalmazzák. A numerikus értékek a mellékletben találhatóak meg, itt az érthetőség kedvéért csak kivonatolt formában utalok a mellékletben található részletes eredményekre.

A hálózati forgalmak szimulációja során a korlátokkal ellátott legrövidebb út (CSPF – Constraint Shortest Path First) algoritmust alkalmaztam. Ez az algoritmus arra készült, hogy a hálózati gráf élein állított korlátokat (pl. költségjellemző, fenntartott sávszélesség) figyelembe véve keresse meg a legrövidebb útvonalat. A használt szimulációs szoftver több algoritmust ismer, azonban ez az algoritmus használta a leggyakrabban a gyakorlati életben, ezért ettől az algoritmustól csak indokolt esetben érdemes eltérni. Ilyen indokolt eset egy gerinchálózat kialakítása lehet, mert itt szükséges és javasolt a végponttól végpontig a forgalmi tervezés (ún. Traffic Engineering). Az IP hálózatok túlnyomó többsége Dijkstra féle legrövidebb út algoritmust használ.

### **II.3 Forgalmi esetek, forgalmi minták**

Három hálózatszintű forgalmi esetet vettem figyelembe, 128 Kbps, 1 Mbps és 10 Mbps értékekkel, a fenti forgalmi esetek megválasztása az alábbi megfontoláson alapul. A 2000-es évek elején az adatforgalom a végpontokhoz zömmel ISDN technológián keresztül jutott el, 2 ISDN B csatorna sávszélesség 128 Kbps. A 2010-re években a szélessávú technológia általánossá vált, még a mobilhálózatokon hozzáférhető legalacsonyabb sávszélesség is legalább 1 Mbps. A fenti trendet követve megállapítható, hogy a civil életben a felhasználó által használt legkisebb sávszélesség legalább 10 Mbps lesz 2020-ra, és az Internet mindenhol elérhető lesz európai környezetben, vagyis infrastruktúra jellegű lesz. A szélessávú IP alapú alkalmazások terjedését [20] is ösztönzi.

A sávszélesség igények eloszlása az egyes végpontokon nem egyenletes, hanem normál, vagy Poisson eloszlású. Ennek az az oka, hogy így a forgalmi viszonyok jobban fedik a valós, nem egyenletes forgalmi viszonyokat. A felhasználók közvetlen interakciója is egyre inkább várható, ami azt eredményezi, hogy a forgalom jellege elosztottabb lesz. Ezzel párhuzamosan

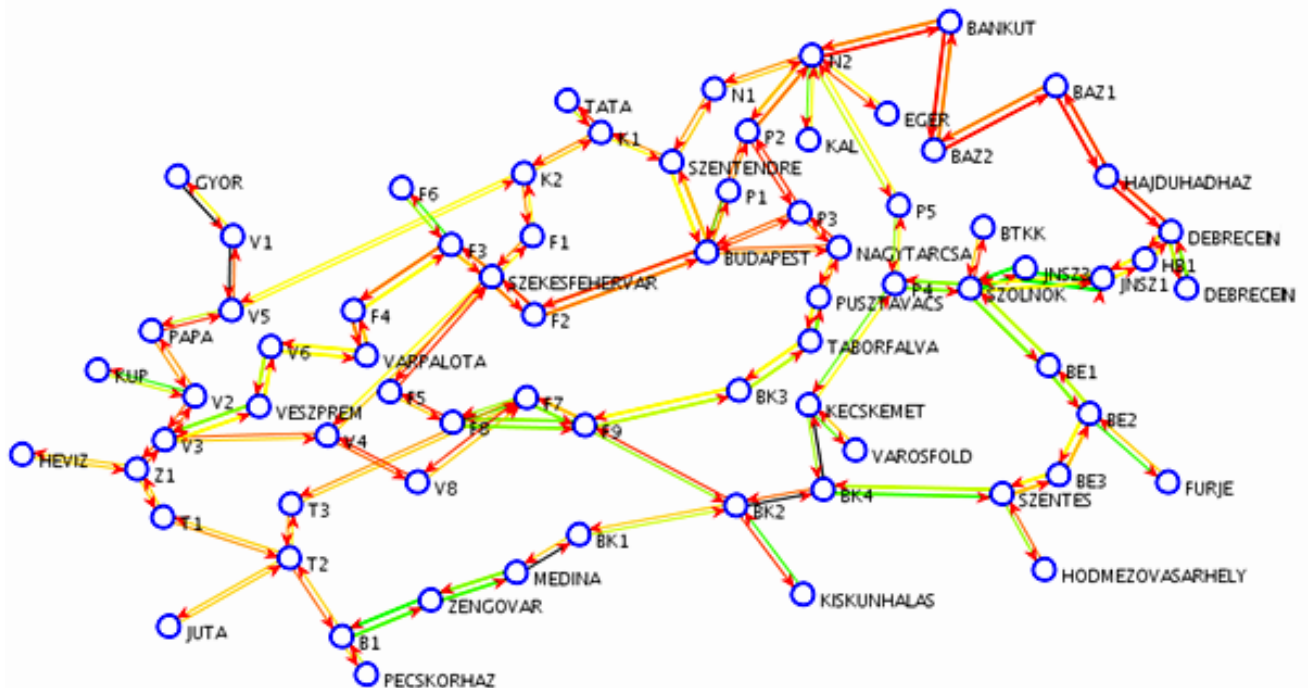
teljesen szövevényes csomóponti kapcsolatokat alakítottam ki az EDGE-el jelölt csomópontok között (tehát a digitális távbeszélőállomásokkal rendelkező telephelyek között).

A valós forgalmi minták természetesen nem pontosan ilyenek, a forgalom eloszlása, alkalmazás és helyszíntől függő, ezért az egyes forgalmi minták, az egyes alkalmazások igényeire jobban alakíthatóak. Az egyes helyszínek forgalma is jelentősen különbözik, azonban ahhoz, hogy azt vizsgálni tudjam, hogy jövőálló-e a Magyar Honvédség stacioner hálózata forgalmi szempontból, a fenti viszonyok megfelelőek.

### Kis sávszélességű adat, és hangforgalom szimulációja

Az első esetben példaforgalomként 1 Mbit/s körüli forgalmakat szimuláltam, az egyes végponti helyszínek forgalmát véletlenszám generátorral generáltam. A véletlenszám generátor normál eloszlású véletlenszámokat generált a végpontokra, 1 Mbit/s-os középértékkel és 0,5 Mbit/s-os szórással. Ezek a forgalmak minden végponti telephelyről, minden végponti telephelyre mennek. Ez a forgalom mennyiség, és eloszlás egy első generációs IP alapú hálózatra jellemző, a 2000 -2003 körüli állapotot jellemzi, azonban a mai igényeket már nem fedi le. Ez a forgalmi minta megfelel egy vegyes közepes méretű laktanya forgalmának, megfelel 16 db PCM (Pulse Code Multiplex) kódolású hangcsatornának, ill. vegyes adat és hangforgalomnak, amely nem tartalmaz valós idejű képátvitelt.

Ebben az esetben a forgalmi viszonyokat a (II-1. ábra) mutatja.



II-1. ÁBRA FORGALMI HÁLÓZATI VISZONYOK 1 MBIT/S MELLETT

Az ábrán jól követhető, hogy ilyen forgalmi helyzet esetén a Debrecen-Hajdúhadház-Bánkút viszonylat, ill. a Budapest-Szentendre-Nagytarcsa-Székesfehérvár viszonylatokon az élek terheltsége meghaladja a 90%-ot, tehát az élek közel teljesen telítettek. A fenti esetet vizsgálva az állapítható meg, hogy a Bánkút, Hajdúhadház, Debrecen ill. Bp. és Bp. környéki csomópontok körüli élek leterheltsége közelíti a 100%-ot. Ez ilyen forgalmi viszonyok esetén azt jelentené, hogy gyakorlatilag bizonyos viszonylatokban lehetetlenné vált a kommunikáció a végpontok között.

Az élek telítettségét a mellékletben szereplő táblázat tartalmazza részletesebben, kivonatosan a legtelítettebb éleket az alábbi táblázatban (II-8) foglaltam össze. A táblázat első oszlopában egy élazonosító található, ezt önkényesen állapítottam meg, célom egy olyan azonosítórendszer kialakítása volt, amely biztonsági szempontokat figyelembe vesz. A következő két oszlop az induló és végcsomópont azonosítója. Az egyes azonosítókhoz kapcsolódó sáv szélességeket a negyedik oszlop mutatja (Mbit/s-ban), ezek tulajdonképpen az élek kapacitásai. A szimuláció során a fenntartott sáv szélességet<sup>3</sup> (a maradék kapacitás az éleken) a hatodik oszlop mutatja, a hetedik oszlop pedig a telítettséget mutatja százalékban.

Az alábbi táblázatban összegyűjtöttem a legtelítettebb éleket ebben az esetben:

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sáv szélesség [Mbit/s]	Fenntartott sáv szélesség [Mbit/s]	Szabad <sup>4</sup> sáv szélesség [Mbit/s]	Telítettség
GYOR-V1	GYOR	V1	8.00	7.98	0.02	99.71%
V1-V5	V1	V5	8.00	7.98	0.02	99.71%
V5-V1	V5	V1	8.00	7.92	0.08	98.96%
Papa-V5	PAPA	V5	16.00	14.64	1.36	91.52%
V2-V3	V2	V3	16.00	16.00	0.00	99.99%
V3-V2	V3	V2	16.00	15.42	0.58	96.35%
V3-V4	V3	V4	16.0	15.87	0.13	99.19%
V4-V3	V4	V3	16.00	15.98	0.02	99.85%
F1-SZFVAR	F1	SZEKESFEHERVA R	16.0	14.80	1.20	92.47%
K2-F1	K2	F1	16.00	14.80	1.20	92.47%
V5-K2	V5	K2	16.00	15.95	0.05	99.66%
K2-K1	K2	K1	16.00	15.70	0.30	98.15%
K1-K2	K1	K2	16.0	15.84	0.16	99.03%
K1-TATA	K1	TATA	16.00	15.87	0.13	99.16%
V4-V8	V4	V8	16.00	16.00	0.00	99.98%
V3-Z1	V3	Z1	16.00	15.93	0.07	99.54%
Z1-V3	Z1	V3	16.00	15.96	0.04	99.76%
T2-T3	T2	T3	16.00	14.68	1.32	91.73%
T3-T2	T3	T2	16.00	15.33	0.67	95.79%
F5-SZFVAR	F5	SZEKESFEHERVA R	16.00	15.99	0.01	99.93%
SZFVAR-F5	SZEKESFEHERVAR	F5	16.00	15.91	0.09	99.45%

<sup>3</sup> Az angol reserved bandwidth terminológia magyar megfelelőjeként használom a fenntartott sáv szélesség fogalmat jelen disszertációban.

<sup>4</sup> Szabad sáv szélesség = Sáv szélesség – Fenntartott sáv szélesség. Angol megfelelője a free vagy available bandwidth.

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség [Mbit/s]	Szabad <sup>4</sup> sávszélesség [Mbit/s]	Telítettség
F8-F5	F8	F5	16.00	15.99	0.01	99.93%
JUTA-T2	JUTA	T2	8.00	7.78	0.22	97.28%
T3-F7	T3	F7	16.00	15.90	0.10	99.36%
F7-T3	F7	T3	16.00	15.33	0.67	95.79%
T2-B1	T2	B1	16.00	15.89	0.11	99.33%
B1-T2	B1	T2	16.00	15.44	0.56	96.48%
PECSKORHAZ-B1	PECSKORHAZ	B1	8.00	7.59	0.41	94.83%
B1-PECSKORHAZ	B1	PECSKORHAZ	8.00	7.46	0.54	93.29%
BK2-F9	BK2	F9	16.00	16.00	0.00	99.98%
BK2-BK1	BK2	BK1	8.00	8.00	0.00	99.99%
BK1-MEDINA	BK1	MEDINA	8.00	8.00	0.00	99.99%
SZFVAR-F2	SZEKESFEHERVAR	F2	32.00	31.37	0.63	98.04%
F2-SZFVAR	F2	SZEKESFEHERVAR	32.00	31.92	0.08	99.75%
K1-SZENTENDRE	K1	SZENTENDRE	16.00	15.69	0.31	98.05%
SZENTENDRE-K1	SZENTENDRE	K1	16.00	15.56	0.44	97.24%
F2-BUDAPEST	F2	BUDAPEST	32.00	31.65	0.35	98.90%
BUDAPEST-F2	BUDAPEST	F2	32.00	31.92	0.08	99.75%
BUDAPEST-NAGYTARCSA	BUDAPEST	NAGYTARCSA	16.00	15.72	0.28	98.23%
NAGYTARCSA-BUDAPEST	NAGYTARCSA	BUDAPEST	16.00	15.90	0.10	99.35%
BUDAPEST-P2	BUDAPEST	P2	16.00	16.00	0.00	99.97%
P2-BUDAPEST	P2	BUDAPEST	16.00	15.80	0.20	98.74%
SZENTENDRE-N1	SZENTENDRE	N1	16.00	15.99	0.01	99.94%
N1-SZENTENDRE	N1	SZENTENDRE	16.00	15.98	0.02	99.87%
N1-N2	N1	N2	16.00	15.09	0.91	94.32%
N2-N1	N2	N1	16.0	15.98	0.02	99.87%
NAGYTARCSA-PUSZTAVACS	NAGYTARCSA	PUSZTAVACS	16.00	15.98	0.02	99.85%
PUSZTAVACS-NAGYTARCSA	PUSZTAVACS	NAGYTARCSA	16.00	15.80	0.20	98.73%
NAGYTARCSA-P3	NAGYTARCSA	P3	16.00	15.82	0.18	98.88%
P3-P2	P3	P2	16.0	16.00	0.00	99.99%
P2-P3	P2	P3	16.00	15.77	0.23	98.54%
NAGYHARS-N2	KAL	N2	8.00	7.83	0.17	97.83%
N2-EGER	N2	EGER	16.00	15.86	0.14	99.12%
N2-N3	N2	BANKUT	32.00	30.74	1.26	96.07%
N3-N2	BANKUT	N2	32.00	32.00	0.00	99.98%
BANKUT-BAZ2	BANKUT	BAZ2	32.00	31.87	0.13	99.60%
BAZ2-BAZ1	BAZ2	BAZ1	32.00	31.87	0.13	99.60%
BAZ1-HAJDUHADHAZ	BAZ1	HAJDUHADHAZ	32.00	31.87	0.13	99.60%
BK2-KISKUNHALAS	BK2	KISKUNHALAS	8.00	7.98	0.02	99.72%
P4-P5	P4	P5	16.00	15.85	0.15	99.04%
P5-N2	P5	N2	16.00	16.00	0.00	99.99%
N2-P5	N2	P5	16.00	15.88	0.12	99.22%
DEBRECEN-HAJDUHADHAZ	DEBRECEN	HAJDUHADHAZ	34.00	33.95	0.05	99.85%
HAJDUHADHAZ-DEBRECEN	HAJDUHADHAZ	DEBRECEN	34.00	33.37	0.63	98.16%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség [Mbit/s]	Szabad <sup>4</sup> sávszélesség [Mbit/s]	Telítettség
SZOLNOK-BTKK	SZOLNOK	BTKK	8.00	7.73	0.27	96.66%
BTKK-SZOLNOK	BTKK	SZOLNOK	8.00	7.99	0.01	99.86%
HODMEZOVASARHELY-SZENTES	HODMEZOVASARHELY	SZENTES	8.00	7.71	0.29	96.35%
BE2-FURJE	BE2	FURJE	8.00	7.39	0.61	92.32%
FURJE-BE2	FURJE	BE2	8.00	7.84	0.16	98.04%

II-8. TÁBLÁZAT – ÉLTELÍTETTSÉG 1 MBIT/S FORGALOM MELLETT 1 MBIT/S

Mint a II-8 táblázatból látható, az élek jelentős része telítetté vált, pedig pusztán 1 Mbit/s-os végpont-végpont közti forgalmat szimuláltam (igaz, a végpontok közti forgalom nem egyenletes, de ezt a forgalmi mátrix normál eloszlása szimulálja).

Összegyűjtöttem a 10 legtöbb sávszélességet foglaló út listáját is (lásd II-9 táblázat) A VII-2. számú melléklet tartalmazza az útvonalak részletes leírását is, amelyben végigkövethető, hogy a szimulált algoritmus, hogyan választotta ki a legrövidebb utat.

Útvonal azonosító	Induló csomópont	Végződő csomópont	Lefoglalt sávszélesség [Mbit/s]
LSP-1327756693	BANKUT	SZOLNOK	4.12
LSP-2103831626	SZENTES	VARPALOTA	3.91
LSP-1052849489	PAPA	FURJE	3.77
LSP-388803609	VAROSFOLD	SZEKESFEHERVAR	3.75
LSP-642376298	SZENTES	ZENGOVAR	3.73
LSP-388884339	NAGYTARCSA	BUDAPEST	3.73
LSP-1244877144	SZENTES	VESZPREM	3.72
LSP-402688255	BUDAPEST	BANKUT	3.49
LSP-1320249276	HODMEZOVASARHELY	PECSKORHAZ	3.41
LSP-1911551397	SZEKESFEHERVAR	HEVIZ	3.40

II-9. TÁBLÁZAT - LEGTÖBB SÁVSZÉLESSÉGET FOGLALÓ UTAK – 1MBIT/S

A táblázatból jól látható, hogy sok esetben néhány nagyobb, az országot átszelő forgalmú útvonal lefoglalja a hálózati erőforrásokat (a példában az LSP-1327756693, ill. LSP-2103831626 azonosítójú viszonylatok). A technológia helyes megválasztásával, a hálózati eszközök pontos konfigurációjával elérhető, hogy az ilyen jellegű forgalmak a lehető legkevésbé terheljék a gyakrabban használt éleket. Ezt a jelenlegi statikus ill. pusztán a legrövidebb út algoritmusokon alapuló tervezés nem teszi lehetővé.

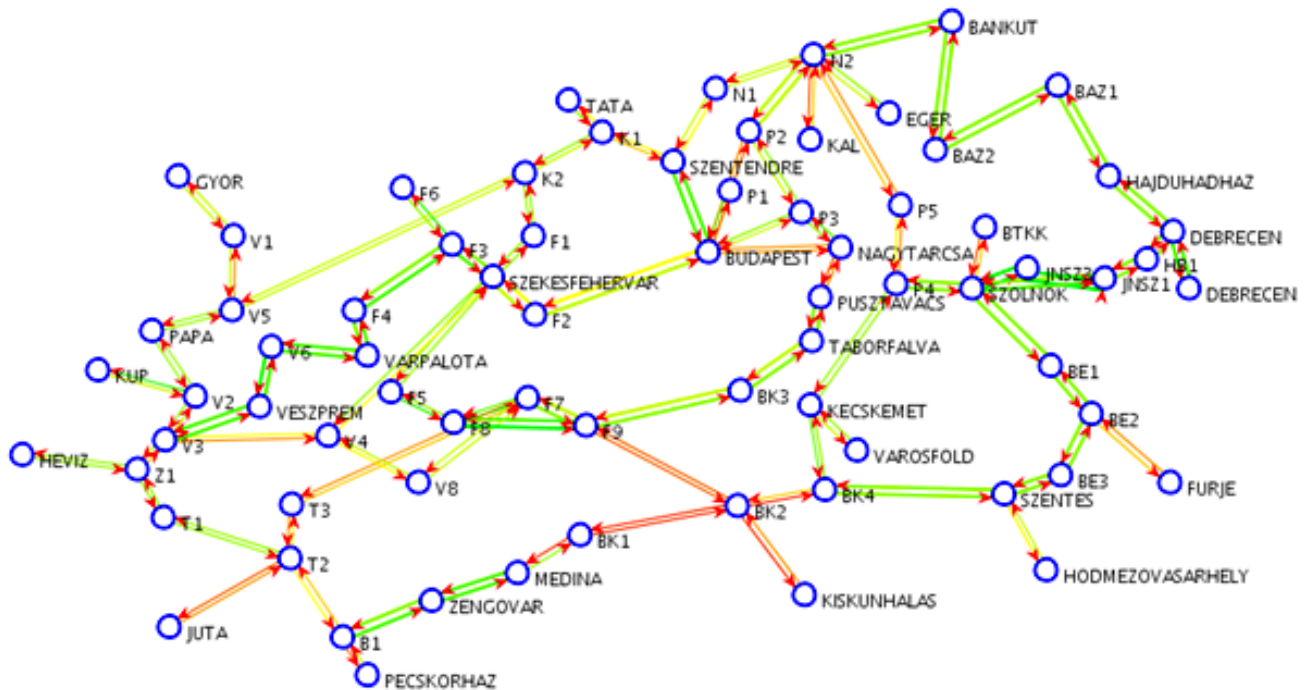
### Alacsony sávszélességű hangforgalom szimulációja

A második esetben, tisztán hangalapú forgalom mennyiséget szimuláltam. Példaforgalomként 128 Kbit/s körüli forgalmakat szimuláltam, ahol az egyes végponti helyszínek forgalmát véletlenszám generátorral generáltam. (A forgalmi mátrix megtalálható a V.II. számú

mellékletben). A véletlenszám generátor normál eloszlású véletlenszámokat generált a végpontokra, 128 Kbit/s-os középértékkel és 20 kbit/s-os szórással. Ezek a forgalmak minden végponti telephelyről, minden végponti telephelyre mennek.

Ez a forgalmi minta megfelel a múlt század '90-es éveinek megfelelő forgalmaknak. Átlagosan két darab PCM kódolású hangcsatornának, vagy 4 db ADPCM (Advanced Pulse Code Multiplex) kódolású hangcsatornának.

A második ábra ezt az esetet mutatja, a korábban már ismertetett színekkel.



II-2. ÁBRA - A HÁLÓZAT FORGALMI VISZONYAI 128 KBIT/S ÁTLAGOS FORGALOM MELLETT

Jól látható, hogy ebben az esetben a hálózat telítettsége jelentősen csökkent, a hálózatban ebben az esetben gyakorlatilag nincsenek 90% feletti telítettségű élek. A 80%-os terheltség feletti éleket az alábbi táblázat (II-10) mutatja:

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség [Mbit/s]	Szabad sávszélesség [Mbit/s]	Telítettség
T2-JUTA	T2	JUTA	8.00	6.90	1.10	86.28%
B1-PECSKORHAZ	B1	PECSKORHAZ	8.00	6.60	1.40	82.54%
BK2-F9	BK2	F9	16.00	14.10	1.90	88.10%
BK1-BK2	BK1	BK2	8.00	7.21	0.79	90.06%
BK1-MEDINA	BK1	MEDINA	8.00	7.21	0.79	90.06%
BUDAPEST-P2	BUDAPEST	P2	16.00	13.38	2.62	83.61%
NAGYTARCSA-PUSZTAVACS	NAGYTARCSA	PUSZTAVACS	16.00	13.21	2.79	82.57%
N2-NAGYHARS	N2	KAL	8.00	6.97	1.03	87.17%
BK2-KISKUNHALAS	BK2	KISKUNHALAS	8.00	7.96	0.04	99.51%
BK2-BK4	BK2	BK4	16.00	13.46	2.54	84.10%
BTKK-SZOLNOK	BTKK	SZOLNOK	8.00	7.02	0.98	87.76%

II-10. TÁBLÁZAT – LEGTELÍTETTEBB ÉLEK 128 KBIT/S

Jól látható, hogy ebben az esetben a BK1-BK2, Bács-Kiskun megyei csomópontok között alakulhat ki ebben az esetben 90% feletti leterheltség. Megállapítható, hogy a hálózat az ilyen jellegű forgalmakat megfelelő mértékben képes kielégíteni. A 10 legnagyobb forgalmú útvonal listája(II-11) ebben a mintaesetben a következő:

Útvonal azonosító	Induló csomópont	Végződő csomópont	Szabad Sáv szélesség [Mbit/s]
LSP-162326215	TABORFALVA	KISKUNHALAS	0.19
LSP-706168055	SZOLNOK	VARPALOTA	0.19
LSP-1051170158	EGER	HAJDUHADHAZ	0.18
LSP-1696730769	HODMEZOVASARHELY	VAROSFOLD	0.18
LSP-2079101251	TABORFALVA	NAGYTARCSA	0.18
LSP-1036924204	VARPALOTA	TABORFALVA	0.18
LSP-415957373	PAPA	BUDAPEST	0.18
LSP-237965403	VESZPREM	DEBRECEN REPTER	0.17
LSP-464109927	BUDAPEST	TABORFALVA	0.17
LSP-1571687308	SZEKESFEHERVAR	KISKUNHALAS	0.17

II-11. TÁBLÁZAT – LEGTELÍTETTEB UTAK 128 KBIT/S

Itt is megállapítható, hogy sok esetben egy hosszabb út, mint például az LSP-1036924204-es lefoglalja a hálózati erőforrások egy jelentős részét. Ezen megfelelő útvonal irányítással (ún. Traffic Engineering útvonalak bevezetésével) megfelelően szabályozható.

### **Katonai informatikai alkalmazás szimulációja**

A harmadik esetben, nagyobb adatforgalom mennyiséget szimuláltam. Példaforgalomként 10 Mbit/s körüli forgalmakat szimuláltam, ahol az egyes végponti helyszínek forgalmát véletlenszám generátorral generáltam. A véletlenszám generátor Poisson eloszlású véletlenszámokat generált a végpontokra, 10 Mbit/s-os középértékkel. Ezek a forgalmak minden végponti telephelyről, minden végponti telephelyre mennek. Ez a forgalmi jelleg megfelel a mai katonai informatikai alkalmazások követelményeinek, lehetővé teszi a valós idejű, nagy sáv szélességű adatforgalmat, a valós idejű képátvitelt és az elosztottan működő hálózati architektúrát, amely a nagy rendelkezésre állással rendelkező hálózati alkalmazásokhoz szükséges.

A következő ábra (II-3) a forgalmi viszonyokat mutatja ebben az esetben:





Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség [Mbit/s]	Fenntartható sávszélesség [Mbit/s]	Telítettség
BK1-MEDINA	BK1	MEDINA	8.00	7.39	0.61	92.42%
SZFVAR-F2	SZEKESFEHERVAR	F2	32.00	31.59	0.41	98.70%
F2-SZFVAR	F2	SZEKESFEHERVAR	32.00	31.61	0.39	98.77%
K1-SZENTENDRE	K1	SZENTENDRE	16.00	14.91	1.09	93.21%
F2-BUDAPEST	F2	BUDAPEST	32.00	31.86	0.14	99.56%
BUDAPEST-F2	BUDAPEST	F2	32.00	31.61	0.39	98.77%
BUDAPEST-SZENTENDRE	BUDAPEST	SZENTENDRE	32.00	30.87	1.13	96.48%
SZENTENDRE-BUDAPEST	SZENTENDRE	BUDAPEST	32.00	30.56	1.44	95.50%
BUDAPEST-NAGYTARCSA	BUDAPEST	NAGYTARCSA	16.00	15.42	0.58	96.37%
NAGYTARCSA-BUDAPEST	NAGYTARCSA	BUDAPEST	16.00	15.14	0.86	94.61%
NAGYTARCSA-PUSZTAVACS	NAGYTARCSA	PUSZTAVACS	16.00	15.42	0.58	96.37%
PUSZTAVACS-NAGYTARCSA	PUSZTAVACS	NAGYTARCSA	16.00	15.14	0.86	94.61%
BUDAPEST-P3	BUDAPEST	P3	16.00	15.75	0.25	98.45%
N2-N3	N2	BANKUT	32.00	29.36	2.64	91.75%
BAZ2-BANKUT	BAZ2	BANKUT	32.00	30.09	1.91	94.04%
BAZ1-BAZ2	BAZ1	BAZ2	32.00	30.00	2.00	93.74%
HAJDUHADHAZ-BAZ1	HAJDUHADHAZ	BAZ1	32.00	31.10	0.90	97.19%
KECSKEMET-BK4	KECSKEMET	BK4	16.00	15.89	0.11	99.30%
KECSKEMET-VAROSFOLD	KECSKEMET	VAROSFOLD	16.00	15.06	0.94	94.11%
VAROSFOLD-KECSKEMET	VAROSFOLD	KECSKEMET	16.00	15.00	1.00	93.75%
P4-P5	P4	P5	16.00	15.07	0.93	94.22%
P5-N2	P5	N2	16.00	15.23	0.77	95.18%
N2-P5	N2	P5	16.00	15.40	0.60	96.24%
JNSZ1-SZOLNOK	JNSZ1	SZOLNOK	34.00	32.20	1.80	94.70%
JNSZ2-JNSZ1	HB1	JNSZ1	34.00	32.20	1.80	94.70%
DEBRECEN-JNSZ2	DEBRECEN	HB1	34.00	32.20	1.80	94.70%
DEBRECEN-HAJDUHADHAZ	DEBRECEN	HAJDUHADHAZ	34.00	30.65	3.35	90.15%
HAJDUHADHAZ-DEBRECEN	HAJDUHADHAZ	DEBRECEN	34.00	31.20	2.80	91.76%
SZOLNOK-BTKK	SZOLNOK	BTKK	8.00	7.69	0.31	96.16%
SZENTES-BE3	SZENTES	BE3	34.00	33.39	0.61	98.21%
BE3-BE2	BE3	BE2	34.00	32.92	1.08	96.82%
BE2-BE1	BE2	BE1	34.00	33.88	0.12	99.64%
BE1-SZOLNOK	BE1	SZOLNOK	34.00	33.88	0.12	99.64%
SZENTES-HODMEZOVASARHELY	SZENTES	HODMEZOVASARHELY	8.00	7.59	0.41	94.81%

II-12. TÁBLÁZAT – LEGTELÍTETTEBB ÉLEK – 10 MBIT/S

A II-3 ábrát, valamint a II-12. táblázatot összevetve, a II-1 ábrával és a II-8 táblázattal azt tapasztaljuk, hogy nincs szignifikáns különbség a két eset között. Ez azt mutatja, hogy a hálózatban nem vezethető el átlagosan az összes végpont felé már 1 Mbit/s-nek megfelelő forgalom sem, a mai katonai alkalmazások 10 Mbit/s-es igényeit pedig a stacioner hálózat nem képes kielégíteni. Az alábbi útvonallista (II-13. táblázat) tartalmazza ebben a mintaesetben a hálózati viszonyokon fellépő 10 legnagyobb forgalmat:

Útvonal azonosító	Induló csomópont	Végződő csomópont	Lefoglalt Sávszélesség [Mbit/s]
LSP-959528328	BANKUT	DEBRECEN	17.00
LSP-1459592305	SZEKESFEHERVAR	BUDAPEST	15.00
LSP-772391265	BUDAPEST	VESZPREM	15.00
LSP-870561522	VAROSFOLD	BANKUT	15.00
LSP-1802450313	TABORFALVA	PUSZTAVACS	14.00
LSP-259278316	VESZPREM	ZENGOVAR	13.00

Útvonal azonosító	Induló csomópont	Végződő csomópont	Lefoglalt Sáv szélesség [Mbit/s]
LSP-879809611	TATA	VESZPREM	12.00
LSP-565292201	PAPA	SZENTENDRE	12.00
LSP-856816017	VARPALOTA	VESZPREM	12.00
LSP-662916574	SZOLNOK	DEBRECEN	12.00

II-13. TÁBLÁZAT – LEGTELÍTETTEBB UTAK, 10 MBIT/S ESETÉN

Hasonlóan a korábbi két forgalmi esetben megállapítható, látható, hogy néhány nagyobb forgalmú, országot átszelő út leterhelheti a teljes hálózatot (a fenti példában az LSP-959528328, ill. LSP-1459592305 útvonal azonosítója viszonylatok). Az útvonallista részletesebb elemzéséből kiderül, hogy a hálózati útvonalak jelentős része nem volt kialakítható a hálózaton, tehát ilyen forgalmi mennyiség átvitelére a Magyar Honvédség stacioner hálózata nem alkalmas.

A technológia helyes megválasztásával, a hálózati eszközök pontos konfigurációjával elérhető, hogy az ilyen jellegű forgalmak a lehető legkevésbé terheljék a gyakrabban használt éleket. Ezt a jelenlegi statikus ill. pusztán a legrövidebb út algoritmusokon alapuló tervezés nem teszi lehetővé.

### Az eredmények kiértékelése – a stacioner hálózat jósága forgalmi szempontból

A teljes hálózat jóságára (forgalmi szempontból) különböző mérőszámokat lehet alkalmazni. Egy lehetséges mérőszám pl. az átlagos forgalmi utak hossza, amely azt mutatja hogy hány csomóponton vagy élen kell áthaladnia átlagosan a forgalmi utaknak.

$$\frac{\sum_{i=0}^n d(i)}{n}$$

#### 1. EGYENLET ÁTLAGOS FORGALMI ÚTHOSSZ

ahol  $n$  a forgalmi utak száma,  $d(i)$  pedig az egyes forgalmi utak hossza (hopszámban mérve).

Ebben az összehasonlításban egy másik mérőszámot alkalmaztam, az élek telítettségének az átlagát, százalékos arányban. Ennek a mérőszámnak a meghatározása az alábbi:

$$\frac{\sum_{i=0}^n u(i)}{n}$$

#### 2. EGYENLET ÉLTELÍTETTSÉG SZÁMTANI ÁTLAGA

Ahol  $n$  az élek számát,  $u(i)$  pedig az  $i$ -edik él telítettségét jelöli (az  $i$ -edik élen a szabad sáv szélesség és a teljes sáv szélesség arányát). Ez a mérőszám minél alacsonyabb annál több szabad kapacitás áll rendelkezésre a forgalmak elvezetésére, így forgalmi szempontból használható a hálózat jóságának a mérésére. Egy másik mérőszámot és megvizsgáltam, az

átlagos szabad átviteli kapacitást az éleken Mbit/s-ban. Ennek a mérőszámnak a meghatározása a következő:

$$\frac{\sum_{i=0}^n f(i)}{n}$$

### 3. EGYENLET – SZABAD KAPACITÁS SZÁMTANI ÁTLAGA

Ahol a n az élek számát, f(i) pedig az i-edik élhez tartozó szabad kapacitást jelöli, Mbpsban. Ez a mérőszám is minél alacsonyabb annál jobb minőségű a hálózat forgalmi szempontból. Ez a két mérőszám közelíti az ideális szubjektív súlyokkal súlyozott szabad kapacitást, vagy élkapacitás kihasználtságot meghatározó mérőszámot. Ennek a meghatározása a következő lenne:

$$\frac{\sum_{i=0}^n w(i) * u(i)}{n}$$

### 4. EGYENLET – SÚLYOZOTT ÉLTELÍTETTSÉGÁTLAG

Ahol n az élek száma, w(i) az i-edik élhez tartozó súlyérték, u(i) pedig az i-edik élen a szabadkapacitás és a teljes kapacitás aránya. Hasonlóan a szabadkapacitáshoz is meghatározhatunk súlyozott átlagot:

$$\frac{\sum_{i=0}^n w(i) * f(i)}{n}$$

### 5. EGYENLET - SÚLYOZOTT SZABAD KAPACITÁSÁTLAG

Ahol n az élek száma, w(i) az i-edik élhez tartozó súlyérték, f(i) pedig az i-edik élhez tartozó szabad kapacitást jelöli. Bár az ideális eset a súlyozott átlag meghatározása lenne (ez is javasolt a jövőben) a súlyfüggvény meghatározása nem egyszerű feladat, és még nem történt meg. Azért, hogy a hálózat jósága mérhető legyen a 2. egyenlet és a 3. egyenlet által meghatározott egyszerű számtani átlagolást használtam.

Az összegző eredményeket az alábbi II-14. táblázatban foglaltam össze.

	128 Kbit/s	1 Mbit/s	10 Mbit/s
Élek telítettségének az átlaga	40,28%	74%	65,20%
Átlagos szabad kapacitás az éleken (Mbps)	13,88	6,37	7,07

II-14. TÁBLÁZAT – FORGALMI ÖSSZEHASONLÍTÓ PARAMÉTEREK

A fenti II-14. táblázatból megállapítható, hogy 128 Kbit/s esetben áll rendelkezésre szabad kapacitás a hálózatban, 1 Mbit/s és 10 Mbit/s esetén nem. 1 Mbit/s-es átlagos forgalom esetén az élek átlagos telítettsége 74%-ra növekszik. Ez az érték nem elfogadható, hálózattervezésben tapasztalati értéként az egyes élek 70%-os telítettsége felett az élek

kapacitásbővítése szükséges, itt pedig az átlagos érték növekedett 74%-ra, így a teljes hálózat kapacitásviszonyai túlságosan telítettek.

A táblázat furcsasága, hogy a 10 Mbit/s esetben látszólag több a szabad kapacitás, mint 1 Mbit/s esetben. Ez nem hiba, abból következik, hogy 1 Mbit/s esetben a teljes hálózaton 188 utat tudunk elvezetni, 10 Mbit/s esetben csak 61 darab utat, mert nem áll rendelkezésre annyi szabad kapacitás, hogy az egyes 1 il. 10 Mbit/s-es utakat elvezessük. Tehát a 10 Mbit/s-es forgalmak még kevésbé vezethetők el a hálózaton, kevesebb utat tudunk végigvinni, ez azt jelenti, hogy a hálózat 65% telítettsége felett már nem áll rendelkezésre annyi szabad kapacitás a hálózaton, hogy 10 Mbit/s utakat vezessünk el, csak 1 Mbit/s lenne elvezethető.

A fenti táblázatból megállapítható, hogy 128 Kbit/s-es hangforgalomra a hálózat kapacitásai megfelelőek. 1 Mbit/s –es forgalmak a hálózaton már nem teljes mértékben elvezethetők, és a hálózatot telítésbe viszik, 10 Mbit/s átlagos végpontok közti forgalmak pedig nem vezethetők el.

## II.4 Összegzés

Ebben a fejezetben azt vizsgáltam, hogy a Magyar Honvédség stacioner hálózata mennyire felel meg azoknak a sávszélesség követelményeknek, amiket a modern katonai informatikai alkalmazások támasztanak. Az első fejezetben bemutattam, hogy a stacioner hálózatban az I.4 fejezetben részletezett technológiai jellegű hibák vannak.

A követelmények vizsgálatához a fejezet első felében egy mintaalkalmazás, egy katonai háromdimenziós radar sávszélesség igényszámítását végeztem el. A sávszélességigényt összehasonlítva a rendelkezésre álló kapacitásokkal látható, hogy a **stacioner hálózat kapacitásai nem elégségesek a 3 dimenziós radarok sávszélességigényét kielégíteni**. A fejezet második felében azt elemzem, hogy három forgalmi esetben a stacioner hálózaton hogyan alakulnak a forgalmi viszonyok. A fejezetben tudományos módszert alkalmazok arra, hogy:

- az adatkapcsolt hálózaton különböző végponti forgalmi eseteket figyelembe véve, a kapacitásviszonyok hogyan alakulnak
- az adatkapcsolt hálózaton, hogyan modellezhető egy forgalmi helyzet
- egy hálózati modellen milyen torlódási és túlterhelési problémák jelentkeznek
- ezek a túlterhelési problémák mit eredményeznek a valós hálózatban
- a stacioner hálózat hogyan reagál az alkalmazás réteg által megnövelt hálózati forgalomra

A fentiekben ismertetett módszer a Magyar Honvédség stacioner hálózatának tudatosabb forgalmi tervezését is elősegíti, a stacioner hálózat kapacitásproblémáit következőképpen segíti:

1. **A módszer használatával a hálózati erőforrások megfelelőbb kihasználtsága érhető el**
2. Adatforgalomnövekedés esetén a kiszolgáló hálózat szükséges kapacitásviszonyai meghatározhatóak a módszer segítségével, így a **hálózat szükséges sávszélességviszonyai pontosabban modellezhetőek**
3. **Stacioner és tábori hálózatok közti adatforgalom kapacitástervezésére** használható a módszer
4. **A stacioner hálózat folyamatos és időszakos forgalmi modellezésére** alkalmas a módszer, segítségével megállapíthatóak a hálózat szűk keresztmetszetei és kritikus forgalmi helyei

Ez a módszer gyakorlatban mind az oktatásban, mind az iparban hasznosítható. Oktatás területén jól modellezi az erőforrás problémák által okozott járulékos forgalmi problémákat, ezért javaslom az alkalmazását mind a műszaki mind a katonai műszaki képzésben. Az iparban az erőforrásmodellezés, a kapacitástervezés tudatosabb döntésekhez, pontosabb döntéshozói képhez vezet, így költséghatékonyabbá és kiszámíthatóbbá teszi az átviteltechnikai és IP hálózatok üzemeltetését és modellezését.

### III. A Magyar Honvédség stacioner hálózatának javasolt kialakítása

*“Valójában a tudomány sohasem fedez fel semmi újat. Az újat mindig az emberi intuíció fedezi fel, a maga egyéni és más emberek számára nemigen követhető útján. A tudomány csak arra alkalmas, hogy az intuitíve meglátott igazságokat szigorú módszerességgel bebizonyítsa.”*

*Mérő László*

A Magyar Honvédség hálózata független stacioner és informatikai hálózatból épül fel. A stacioner hálózatban is és az informatikai hálózatban is javasolt a módosítások meghatározása, ill. a két hálózati réteg összevonása, amely akkor történhet meg, ha a hálózat egységes IP alapra történő átállása megtörtént. Ez a folyamat a civil szférában is folyamatosan történik, az átviteltechnikai (a stacioner hálózatnak megfelelő civil hálózati réteg) egyre inkább Ethernet első és második rétegbeli technikákat használó technológiai réteg lesz. Ezen térnyerés legfőbb oka az Ethernet hálózatok költséghatékony kialakíthatósága.

Az I/4-es fejezetben bemutattam a stacioner hálózat technológiai jellegű hibáit.

Ebben a fejezetben a fenti problémák megoldására teszek javaslatot. Meghatározom, hogy

- a stacioner hálózatot milyen technológia alapokra szükséges helyezni
- a stacioner hálózat rendszerbeállításai hogyan kell, hogy kinézzenek ezen technológia alapokon
- erre az ideális hálózatra milyen módon lehetséges a migráció

A fejezetben a Magyar Honvédség stacioner hálózatának javasolt modernizációs útját fogom szerepeltetni, olyan mélységben, amely egy rendszerterv kialakításához szükséges. Az itt szereplő fejezetben a jelenlegi problémákra keresem a választ, és az új technológiák által nyitott lehetőségeket nem szerepeltetem. A kialakítást az elvi hálózati síkokkal fogom kezdeni, majd egy-egy tipikus gerinchálózat telephelyen használt hálózati eszközöket fogom meghatározni. Az én értelmezésemben a klasszikus átviteltechnikai hálózatot és az IP alapú átviteltechnikai hálózatot egységes egészként fogom kezelni, ahol az átviteltechnikai hálózat pont-pont összeköttetéseket biztosítja optikai szálon, hullámhosszokon vagy mikrohullámú összeköttetésen keresztül. A stacioner hálózat kapcsolóelemei pedig IP alapú útválasztó eszközök. A hálózat szolgáltatásrétegét (webszerverek, katonai informatikai alkalmazások, beszédcélú átvitel) nem tekintem a kutatásom tárgyának.

### III.1 Hálózati rétegek

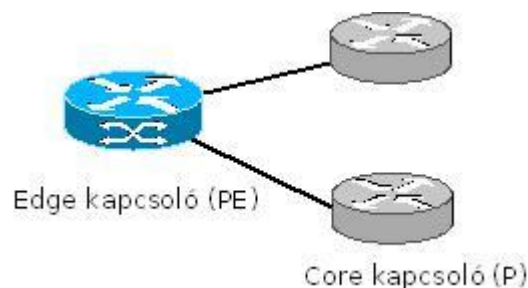
A rendszer kialakítását általános IP hálózati tervezési irányelveknek [21] megfelelően végeztem el A Magyar Honvédség stacioner hálózatában az ajánlott hálózati topológia három rétegből áll, teljesen redundáns kiépítésben. A rétegek a következők:

- Gerinchálózati réteg (P/PE (Provider/Provider Edge) csomópontok MPLS terminológiában), ezeket a csomópontokat a stacioner hálózati csomópontokba kell elhelyezni
- Aggregációs réteg (Layer 3-as Carrier Ethernet képes MPLS csomópontokból)
- Hozzáférési (access) réteg (Layer 3 MPLS képes csomóponti routerekből)

A rétegek ezen tiszta szeparációja lehetővé teszi a hierarchia alapú tervezést és optimális szabadságot biztosít a hálózat bármely irányú fejlesztésére (akár kapacitásban akár csomópontszámban, akár az ajánlott szolgáltatásokat tekintve), ugyanakkor a hálózat továbbra is megőrzi az egyszerűségét ami az üzemeltető személyzet számára könnyebbséget jelent. A hálózati hozzáférési (úgynevezett access) réteg kialakítása nem a stacioner hálózat kialakításának a része, ezért ennek a részletesebb taglalásától eltekintek.

Ez a hálózati rétegekialakítás hálózatstruktúrális szempontból, egy más megközelítés szerint -> átviteltechnikai réteg -> hálózati réteg -> szolgáltatásréteg, amelyből én az átviteltechnikai és hálózati rétegekkel foglalkozom itt.

A fenti háromrétegű hierarchiában minden egyes csomópont meghatározott funkcióval rendelkezik, minden egyes réteg szerepe más. A gerinchálózati széleken lévő (EDGE) csomópontokban tartozkodó routerek (útválasztók) szerepe a hálózati szolgáltatások nyújtása. A gerinchálózat stabil, kiszámítható, megbízható és nagy-teljesítményű csomagtovábbítást biztosít. Egy üzemelő hálózatban a gerinchálózati réteg topológiája stabil és ritkán változik. Az egyes Edge hálózati csomópontok a maghálózatra (core) redundánsan kapcsolódnak.



III-1. ÁBRA AZ EDGE ÚTVÁLASZTÓK ÉS CORE ÚTVÁLASZTÓK KÖZTI REDUNDANCIA

Az ajánlott hálózatban a gerinchálózati linkek 1 Gbps-es linkek, LAN interfészekkel, amely SFP+ csatlakozót használnak. A gerinchálózatban a repeater telephelyeken nem szükséges IP kapcsolóként funkcionáló csomópont. Az MPLS P és PE routereket célszerű 1 típusú csomópontban egységesíteni. A repeater telephelyeket CORE telephelyekként állapítottam meg, ezen telephelyeken nem kell kapcsolási funkciót végezni. A telephelyek besorolását a II-7 táblázat tartalmazza



### III.1.1 Tervezési elvek

A tervezés során a Juniper Networks [22] és a SAF [23] gyártók portfólióját vettem alapul, de más hasonló képességű hálózati gyártók (pl. Cisco Systems (24), Motorola (25)) termékportfóliójából is kialakítható hasonló. A hálózatot három rétegre bontottuk, Gerinc, Aggregációs, és Hozzáférési rétegekre. Aggregációs régióból 3 nagyobb régiót célszerű kialakítanunk, egyet a budapesti telephelyek forgalmának begyűjtésére, egyet a nyugati és egyet a keleti országrész forgalmának a begyűjtésére.

Az eszközök kiválasztásánál az alábbi alapelveket vettük figyelembe:

- Minden eszköz támogassa az IP v4 és OSI (Open Systems International) CLNS (Connectionless Network Service), és IPv6 harmadik rétegbeli protokollokat
- Minden eszköz 230V –AC (Alternating Current – váltóáram) táppal rendelkezzen
- Minden eszköz SFP (Small Form Pluggable) modulokkal bővíthető Gigabit Ethernet uplink modulokkal rendelkezzen
- az eszközök MPLS képesek legyenek, így a forgalomtervezési (traffic engineering), valamint a védelmi mechanizmusok használhatóak legyenek a hálózatban

Az IP címtartományok dinamikus routolását routerekre korlátozzuk. Az OSI/ISIS (Intermediate System-Intermediate System) útválasztási területekre bontását nem változtatjuk, mely felesleges átkonfigurálással járna mind a routereken, mind pedig az SDH (Synchronous Digital Hierarchy) perendezéseken. Az IP/OSPF útválasztás **egyszerűsítésének** főbb okai a következők:

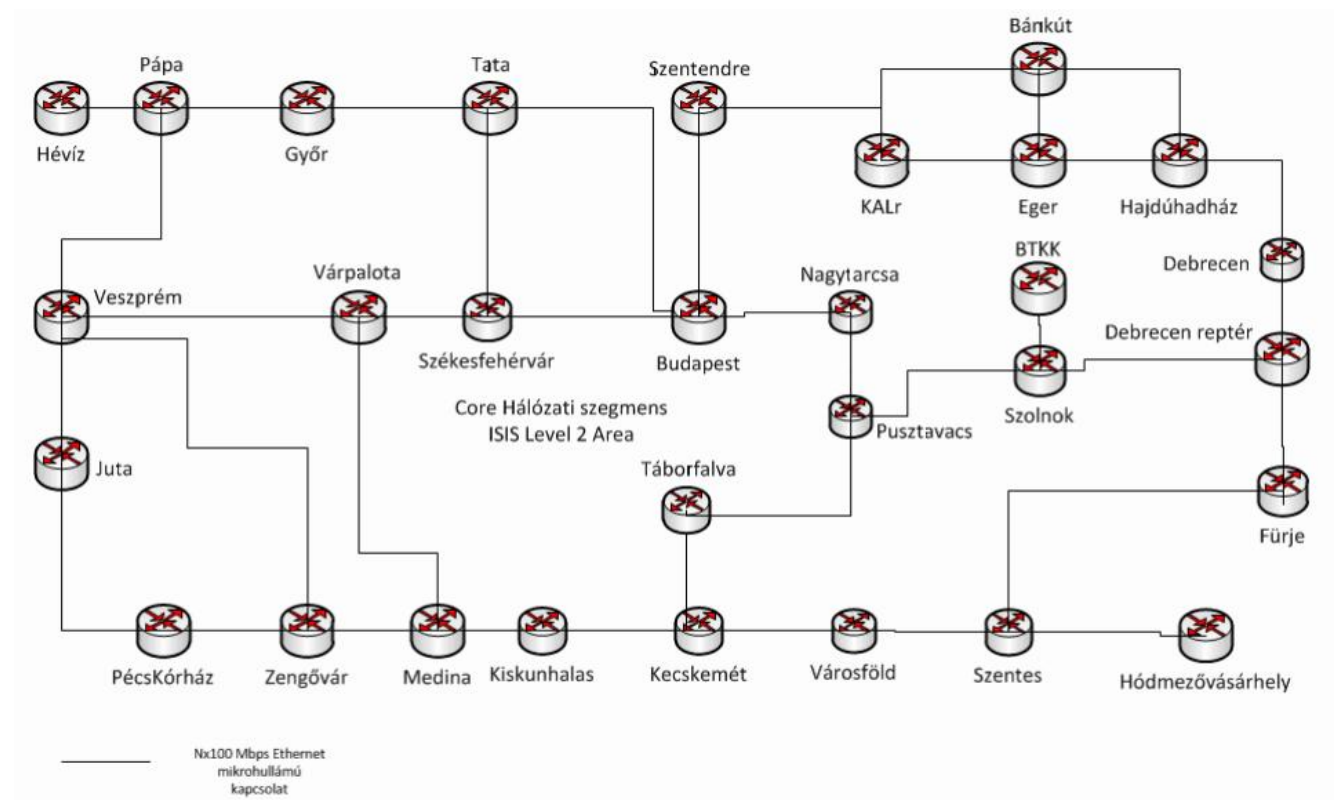
- A dinamikus útválasztási protokollok képességeinek korlátainak figyelembe vétele
- Átláthatóbb hálózati infrastruktúra, a hierarchikus felépítés mellőzése (flat topológia használata)
- Menedzselte végberendezések terhelésének csökkentése (alapértelmezett átjáró és statikus útvonal esetén nincs terhelés)
- Univerzálisan használható topológia az esetleg jövőben csatlakoztatott további végberendezésekhez.
- A hibakeresés elősegítése, gyorsítása
- A hibák könnyebb lokalizálhatósága
- Végberendezési hibák és gerinchálózati hibák elkülönítésének lehetősége
- A végberendezések konfigurációjának minimálisra csökkentése.
- Az útválasztók konfigurációjának egyszerűsítése

A fenti felsorolásból kitűnik, fontos célkitűzés, hogy a rendszer felügyeléséhez, valamint karbantartásához nem kell szakértői tudás a dinamikus IP forgalomirányítás terén. Az OSPF (Open Shortest Path First) útválasztási határának beszűkítése arra is lehetőséget ad, hogy az összes routert egyetlen OSPF területbe vonjuk, tehát az összes Juniper útválasztó képes lesz az egyetlen 0-ás, vagyis gerinc területen belül kommunikálni anélkül, hogy ez

útválasztási problémákat okozna. Ez mind a konfigurációt, mind a útválasztási adatbázisokat, valamint az IP útválasztási táblát is egyszerűsíti. Az egyszerűsítéssel és alapértelmezett átjárók használatával a kiterjedt hálózaton javíthatjuk egy esetleges útválasztó kiesése esetén a konvergencia időt is.

## A stacioner hálózat topológiája

Az alábbi III-2-es ábrán jelöltem az elképzelt rendszerhálózati topológiát. Az egyes telephelyekre MPLS képes nagy mennyiségű Gigabit Ethernet, és E1 (ISDN PRI 2MBit/s Interface) portokkal bővíthető routereket terveztem, az átviteltechnikai hálózat kialakítását pedig egyrészt privát bérelt vonalakon keresztül, másrészt saját célú Ethernet mikrohullámú hálózaton keresztül javaslom kialakítani. Az E1 interfészek használata a végső megoldás esetén nem szükséges, azonban a köztes átmeneti lépésekben számolni kell a meglévő hangszolgáltatások folyamatos migrációjával, ezért ezek szükségesek lehetnek a jövőben is. A fontosabb csomópontokat célszerű szolgáltatótól bérelt privát vonali Ethernet szolgáltatásokkal megvalósítani. Az alábbi ábra (III-2) az EDGE-el jelölt telephelyek közti kapcsolatokat mutatja. A nagymennyiségű iBGP kapcsolatok miatt úttükröző útválasztók (ún. route-reflectorok ) használata javasolt.



III-2. ÁBRA - A STACIONER HÁLÓZAT EDGE ROUTEREINEK JAVASOLT TOPOLÓGIÁJA

Ezek a telephelyeken tartalék útvonalként Ethernet privát vonali szolgáltatást célszerű, külső közcélú adatszolgáltatást biztosító szolgáltató segítségével igénybe venni. Az Ethernet privát vonali szolgáltatások viszonyait az alábbi táblázat tartalmazza.

A privát vonali Ethernet szolgáltatások javasolt listáját az alábbi (III-2. táblázat) táblázat tartalmazza:

Viszonylat azonosító	Kezdő csomópont	Végcsomópont	Mbps
V1	Győr	Tata	100
V2	Győr	Székesfehérvár	100
V3	Győr	Pápa	100
V4	Pápa	Veszprém	100
V5	Pápa	Hévíz	100
V6	Hévíz	Veszprém	100
V7	Hévíz	Juta	100
V8	Juta	Veszprém	100
V9	Juta	PécsKórház	100
V10	Veszprém	Zengővár	100
V11	Veszprém	Várpalota	100
V12	PécsKórház	Zengővár	100
V13	Zengővár	Medina	100
V14	Veszprém	Várpalota	100
V15	Várpalota	Medina	100
V16	Medina	Kiskunhalas	100
V17	Várpalota	Székesfehérvár	100
V18	Székesfehérvár	Budapest	100
V19	Tata	Budapest	100
V20	Budapest	Szentendre	100
V21	Budapest	Nagytarcsa	100
V22	Nagytarcsa	Pusztavacs	100
V23	Pusztavacs	Táborfalva	100
V24	Pusztavacs	Szolnok	100
V25	Táborfalva	Kecskemét	100
V26	Kecskemét	Kiskunhalas	100
V27	Kecskemét	Városföld	100
V28	Városföld	Szentes	100
V29	Szentes	Hódmezővásárhely	100
V30	Szentes	Fürje	100
V31	Fürje	Debrecen reptér	100
V32	Debrecen reptér	Debrecen	100
V33	Debrecen	Hajdúhadház	100
V34	Hajdúhadház	Eger	100
V35	Hajdúhadház	Bánkút	100
V36	Bánkút	KALr	100
V37	KALr	Szentendre	100

III-2. TÁBLÁZAT ÉLVISSZONYLATOK TÁBLÁZATA

A privát vonali utak megvalósíthatóak saját hálózaton is, azonban megfelelő országos szintű optikai szálhálózattal a Magyar Honvédség nem rendelkezik, ezért célszerű megfelelő szolgáltató bevonása ebből a célból.

## III.2 A stacioner hálózat kialakítása

### Átviteltechnikai rendszer

A hálózaton a budapesti csomópontok kivételével egységesen Ethernet mikrohullámú eszközök használata biztosítja a Pont-pont viszonylatokban a legnagyobb sávszélességet. Ezek a mikrohullámú eszközök Gigabit Ethernet csatlakozóval csatlakozhatók az útválasztókhoz. Az EDGE-el jelölt telephelyeken olyan eszközök használata javasolt amelyek rendelkeznek E1-es interfészekkel, az esetleges migráció megkönnyítése érdekében. Ezek a mikrohullámú eszközök 1U-nyi (1U – 1 rack unit, azaz 44mm) helyet igényelnek a hálózati szekrényekben, de sok esetben beltéri egység használata sem szükséges. Az alábbi ábra (III-3) egy Ethernet mikrohullámú eszköz kültéri és beltéri egységét mutatja, ez egy ún. split (különálló kültéri és beltéri egységgel rendelkező) egység.



III-3. ÁBRA – SAF SPLIT ETHERNET MIKRO, [26]

Az eszköz főbb paramétereit az alábbi táblázatban (III-3 Táblázat) határoztam meg, a táblázattól való eltérés indokolt esetben lehetséges.

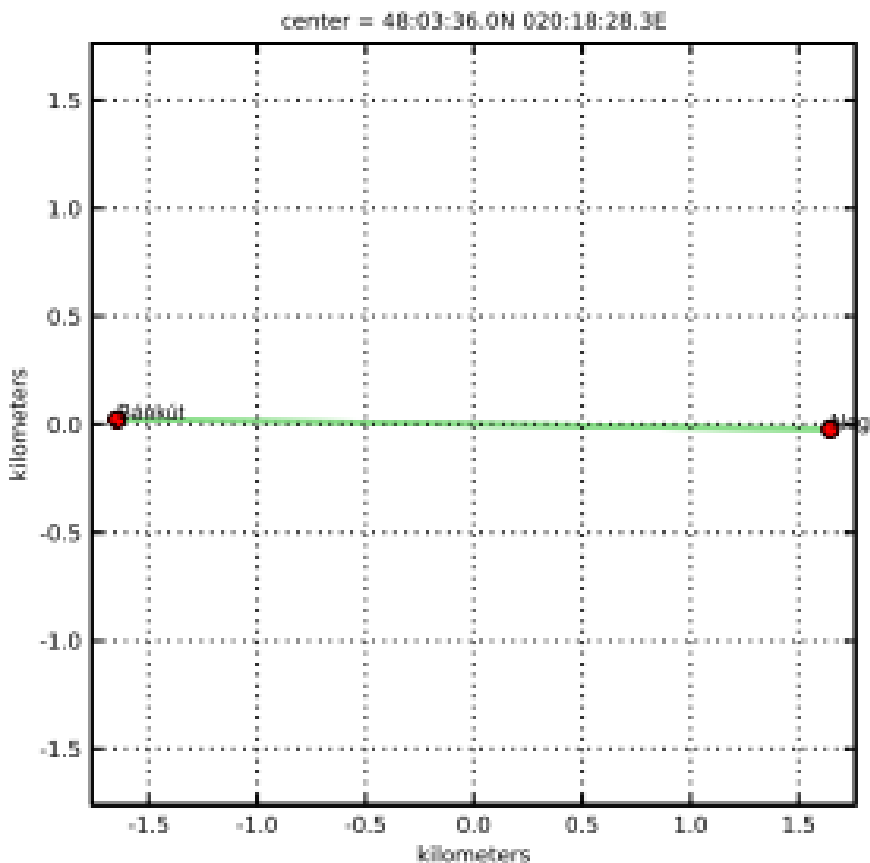
Fizikai méretek	IDU 1U (45x430x240mm)
Súly	3kg
Adátviteli csatorna kapacitás	max. 366Mbps
Csatorna sávszélesség	7 - 28; (7 - 56) MHz
Moduláció	QPSK - 256QAM
Interfészek	4 x 1000Base-T RJ-45, 20 E1/T1 RJ-45
Forgalom típusa	Ethernet + E1
Frekvencia sávok (ETSI):	7/8; 10/11; 13/15; 18/23; 24; 26; 38 GHz

III-3. TÁBLÁZAT – ETHERNET MIKROHULLAMÚ ESZKÖZ TULAJDONSÁGAI

A frekvenciasávok kijelölésénél figyelembe kell venni a NATO által használt frekvenciasávokat (346/2004. (XII. 22.) Korm. rendelet a frekvenciasávok nemzeti felosztásának megállapításáról), így ezen kormányrendelet, nem polgári célú frekvenciasávjából a NATO célra fenntartott frekvenciasávokat kell használni. A mikrohullámú eszköznek rendelkeznie kell Magyarországon, valamint a NATO-ban használt tartományokra frekvenciaengedéllyel.

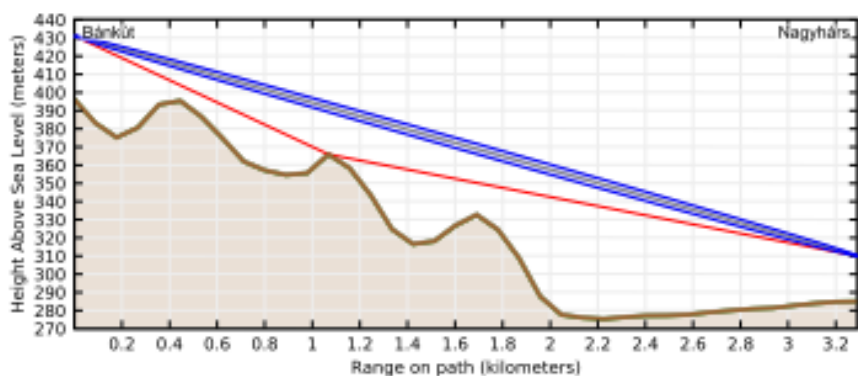
## Az átviteltechnikai hálózat javasolt kialakítása

Példahálózatként a Magyar Honvédség két telephelyét vittem be egy mikrohullámú kapcsolatszerkesztő eszközbe. A kapcsolatszerkesztő eszköz a Motorola cég PTP (Point-to-Point) Link-planner eszköze, amely a [27]–webhelyen szabadon hozzáférhető.



III-4. ÁBRA BÁNKÚT – NAGYHÁRS VISZONYLAT

Mintakapcsolatként Bánkút és Nagyhárs viszonylatot vizsgáltam, egy 18 Ghz és egy 5.9 Ghzes mikrohullámú kapcsolattal (szabadon hozzáférhető ETSI – European Telecommunication Standard Institute, nem NATO frekvenciasávokkal). A Bánkút – Nagyhárs egymáshoz közel eső két telephely, kb. 3 km-es távolságban egymástól (Isd. III-4. ábra). A viszonylat terepmetszetét a (III-5. ábra ) mutatja:



III-5. ÁBRA BÁNKÚT-NAGYHÁRS VISZONYLAT TEREPMETSZETE

A Fresnel zóna helye kék színnel van jelölve az ábrán. Az ábra Y koordinátája a tengerszint feletti magasságot mutatja méterben, az X koordinátája pedig a két telephely közötti légvonalbeli távolságot mutatja kilométerben. Látható, hogy 25-35 m közötti antennákkal az átláthatóság biztosítható a két telephely között. Fenti körülményeket feltételezve az alábbi eredményre jutunk:

	Performance to Bánkút	Performance to Nagyhárs
Mean IP	364,9 Mbps	364,9 Mbps
IP availability	99,99996% for 1 Mbps	99,99996% for 1 Mbps

III-6. ÁBRA SÁVSZÉLESSÉG ÉS RENDELKEZÉSREÁLLÁSI VISZONYOK

Látható, hogy az átlagos sávszélesség 364.9 Mbps és az út rendelkezésreállása jobb mint 99,99996 % a számított eredmények alapján (az esetek több, mint 99,99%-ban az útvonal legalább 1 Mbps IP forgalmat fog tudni szállítani).

Link Summary			
Link length	3,293 km	System Gain	167,2 dB
Band	18 GHz	System Gain Margin	38,8 dB
Regulation	ETSI	Mean Aggregate Datarate	729,6 Mbps
Modulation	adaptive	Annual Link Availability	99,99996%
Bandwidth	55 MHz	Annual Link Unavailability	13 sec / year
Total Path Loss	128,40 dB		

III-7. ÁBRA A KAPCSOLAT PARAMÉTEREI

A fenti (III-7.) ábrán látszik, hogy a telephelyek pontos, légvonalban mért távolsága 3.293 km, a vizsgált sávszélessége 18 Ghz. Adaptív modulációt használunk (tehát több modulációs séma közül a környezeti feltételeknek legmegfelelőbbet választja a rendszer). Az útvonal alatt a teljes úton a veszteség 128.4 dB, a rendszer nyereség pedig 167.2 dB. A nettó nyereség a kettő különbsége 38.80 dB. Az átlagos aggregált sávszélesség (tehát mindkét irányba) 729.8

Mbps. A link éves rendelkezésreállása jobb mint 99.99% és a számított éves link kesés 13 másodperc.

Climatic Factors, Losses and Standards			
dN/dH not exceeded for 1% of time	-266.40 N units/km	Link Type	Line-of-Sight
Area roughness 110x110km	143.87 metre	Excess Path Loss	0.00 dB
Geoclimatic factor	9.84e-005	Atmospheric Gasses	ITU-R P.676-7, ITU-R P.835-4
Fade Occurrence Factor (Po)	2.84e-006	Diffraction Loss	ITU-R P.526-10
Path inclination	36.81 mr	Propagation	ITU-R P.530-12
0.01% Rain rate	37.50 mm/hr	Rain Rate	ITU-R P.837-5
Free Space Path Loss	128.24 dB	Refractivity Index	ITU-R P.453-9
Atmospheric Absorption Loss	0.17 dB		

### III-8. ÁBRA KLÍMAVISZONYOK ÁLTAL OKOZOTT VESZTESÉGEK

A klímaviszonyokat a fenti III-8. ábra mutatja, ennek részletesebben ismertetésére nem térnék ki (technológiafüggetlenül a klímaviszonyok azonosak minden használt mikrohullámú eszközre viszonyítva, kizárólag a frekvenciafüggőségre szeretnék kitérni).

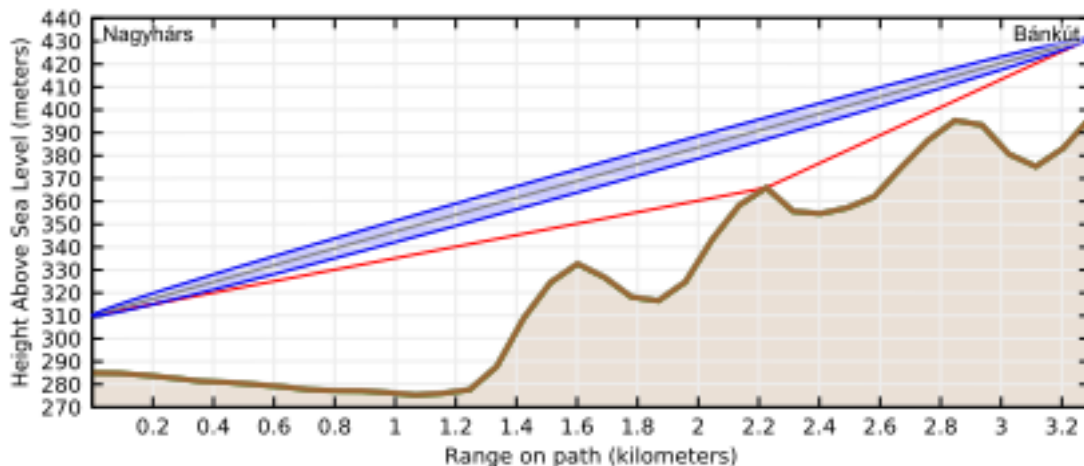
A javasolt alkatrészlistát az alábbi III-9. ábra mutatja:

Part Number	Qty	Description
(no part number)	2	Unspecified 18 GHz ODU (invalid TX frequency selection)
30010194001	2	50 Ohm Braided Coaxial Cable - 75 meter
85010089006	2	1' HP Antenna, 17.70 ~ 19.70 GHz, Single Pol, Mot Interface
WB3480	2	PTP800 Modem 1000/100BaseT with Capacity CAP 10 Mbps
WB3546	2	PTP800 Modem Capacity CAP - Full Capacity (per Unit)
WB3616	2	Coaxial Cable Installation Assembly Kit (W/O LPU End Kit)
WB3657	2	LPU END KIT PTP800 (1 kit required per Coaxial cable)

### III-9. ÁBRA ALKATRÉSZLISTA

A második esetben az 5.9 Ghz-es verziót vizsgáltam, az alábbi III-10. ábra a Fresnel zónát mutatja, a koordináta rendszereket a III-5-ös ábra ismertetésénél meghatároztam.





III-10. ÁBRA FRESNEL ZÓNA 5.9 GHZ ESETÉN

Az eszköz által nyújtott rendelkezésreállást a ( III-11. ábra) mutatja:

	Performance to Nagyhárs	Performance to Bánkút
Mean IP	135.4 Mbps	135.4 Mbps
IP Availability	100.00000 % for 1.0 Mbps	100.00000 % for 1.0 Mbps
E1/T1 Availability	100.00000 %	100.00000 %

III-11. ÁBRA 5.9 GHZ RENDELKEZÉSREÁLLÁSA ÉS SÁVSZÉLESSÉGVISZONYAI

A III-12. ábra azt mutatja, hogy az átlagos IP sávszélesség 135.4 Mbps ebben az esetben a rendelkezésreállítás pedig 100%-os 1 Mbps-re.

Link Summary			
Link Length	3.293 km	Mean Aggregate Data Rate	270.9 Mbps
Band	5.9 GHz	Annual Link Availability	100.00000 %
Regulation	Full Power	Annual Link Unavailability	0 secs/year
Modulation	adaptive	TDM Mode	1 x E1
Bandwidth	30 MHz	TDM Availability	99.999999 %
Total Path Loss	118.21 dB	TDM Annual Unavailability	0 secs/year
System Gain	158.53 dB	TDM One Way Latency	2.00 ms
System Gain Margin	40.32 dB		

III-12. ÁBRA AZ 5.9 GHZ-ES KAPCSOLAT ÖSSZEGZŐ TÁBLÁZATA

A fenti ábrán látszik a légvonalban mért távolság megegyezik a III-7-es táblázatban lévő távolsággal, a vizsgált sávszélessége 5.9 Ghz. Adaptív modulációt használunk (tehát több modulációs séma közül a környezeti feltételeknek legmegfelelőbbet választja a rendszer). Az útvonal alatt a teljes úton a veszteség 118.21 dB, a rendszer nyereség pedig 158.53 dB. A nettó nyereség a kettő különbsége 40.32 dB. Az átlagos aggregált sávszélesség (tehát mindkét irányba) 270.9 Mbps. A link éves rendelkezésreállása közel 100% és a számított éves link kimaradás 0 másodperc.

Part Number	Qty	Description
WB2789	1	PTP 25/59600 Software Key X -> 30 MHz Link
WB2907	4	LPU End Kit PTP400/600 (2 kits required per Link)
WB3097	1	PTP 59600 (5 MHz) Integrated - Link Complete
WB3176	1	328 ft (100 m) Reel Outdoor Cooper Glad CAT5E (Recommended for PTP)

### III-13. ÁBRA AZ 5.9 GHZ-ES KAPCSOLAT ALKATRÉSZLISTÁJA

Az 5.9-es kapcsolat alkatrészlistáját a ( III-13. ábra az 5.9 Ghz-es Kapcsolat alkatrészlistája) mutatja.

### III.3 A stacioner adatátviteli hálózat rendszerterve

Ebben az alfejezetben egy egységes IP/MPLS hálózatot javaslok adatátviteli gerinchálózatnak. Polgári szolgáltatói hálózatok jelentős részében az IP kapcsolók és útválasztók átvették a korábbi időmultiplex kapcsolók szerepét. Javaslom az átviteltechnikai hálózat és az adatátviteli hálózat szorosabb együttműködését, ezért a két hálózati szegmenst egységessé határozom meg. Polgári szolgáltatói hálózatokban a két réteg együttműködése a jellemző.

#### Csomagkapcsolt hálózati eszközök

Az összes útválasztónak támogatnia kell az IP v4, IP v6, valamint ISO CLNS protokollokat, statikus és dinamikus útválasztással. A dinamikus útválasztó protokollok közül a RIPv2 (Routing Information Protocol), OSPF, BGP (Border Gateway Protocol) és ISIS protokollokat kell támogatnia. Az eszköz legyen használható BGP route reflektorként (úttükrözőként) is. Az eszköz támogassa az IP Multicastot (többszörös IP) a PIM (Protocol Independent Multicast), SDP (Session Description Protocol) és DVMRP (Distance Vector Multicast Routing Protocol) 7-es protokollokkal, valamint legyen MPLS képes, és támogassa a DHCP (Dynamic Host Configuration Protocol) kliens, szerver és relay üzemmódját. Az adatkapcsolati rétegbeli protokollok közül Ethernetet, szinkron PPP (Point-to-Point Protocol) és Multilink PPP protokollt, Frame Relay, HDLC (High Level Datalink Control) és PPPoE (Point to Point Protocol over Ethernet) enkapsulációkkal. Soros (RS-232, RS-449, X21, V35 és Eia-530-as fizikai rétegbeli interfészekon keresztül.

Az eszközök legyenek képesek forgalommenedzsmentre, képesek a csomagok megjelölésére, megfelelő policing és shaping algoritmusok használatára, tűzfalfunkciókra, VPN-re (Virtual Private Network) IPsec (IPSecurity) protokollon keresztül, DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard), AES (Advanced Encryption Standard) algoritmus támogatásával. MD5 (Message Digest 5) és SHA-1(Secure Hash Algorithm) autentikációs algoritmusokkal. Az útválasztók támogassák a nagy rendelkezésre állású működést, VRRP (Virtual Router Redundancy Protocol) vagy más protokollokon keresztül. Az eszközök legyenek képesek valós idejű teljesítmény menedzsmentre , a folyamamonitoring és accounting

funkciókon keresztül pedig a hálózati folyamatokról gyűjthessünk folyamatos statisztikákat. Az eszközök kiválasztásakor azok támogassák a :

- commit és rollback funkciókat támogatása, a commit funkció segítségével a parancsok csak akkor kerülnek az élő konfigurációba, amikor a commit parancsot kiadjuk, a rollback paranccsal egy parancs segítségével visszaléphetünk az előző működő konfigurációra. Amennyiben ez nem adott, egy ezzel egyenértékű megoldást kell biztosítani
- a commit confirm funkciót, commit confirm parancs használatával amennyiben téves konfiguráció került be az eszközbe és emiatt az üzemeltető személyzet nem tudná elérni a hálózati eszközt, az eszköz visszaáll a legutóbbi működő konfigurációra. Amennyiben ez nem biztosított, egy ezzel egyenértékű funkciót kell biztosítani.

A naplózás és monitorozás syslog protokollon és traceroute parancson keresztül megvalósított. Az eszközök legyenek beilleszthetők a meglévő hálózatmenedzsmentbe, valamint rendelkezzenek valamilyen szintű elemenedzsment funkcióval. Az eszközök legyenek webes interfészen keresztül is menedzselhetők a hálózatmenedzsment és a parancssori interfészek mellett.

A stacioner hálózati telephelyeket három csoportra osztottam. Az EDGE-el jelölt telephelyekre a szekrényekbe egy 2 U magas hálózati útválasztó eszközt terveztem. A hálózati útválasztó eszköz az ilyen telephelyeken beépített Gigabit Ethernet porttal rendelkezik, amit telephelytípustól függően SFP (amennyiben optikai szálal összekötéssel rendelkezik a telephely), ill. RJ45-ös csatlakozójú Gigabit Ethernet portokkal rendelkező modulokkal bővíthetjük. Az eszköz bővíthető kell legyen E1, és soros interfészekkel, valamint analóg és digitális hangkapcsolatra képes modulokkal.

Eszköznek bővíthetőnek kell lennie minimum 16 db Ethernet portra ill. 4 db E1 portra. A telephelyek közötti Pont-Pont összeköttetést Ethernet mikrohullámú eszközökkel javasolt megvalósítani. Ezek az eszközök a mai modulációs technológiák, és antennarendszerek mellett, több 100 Mbit/s-es sávzélességre képesek. Az alábbi III-14. ábrán egy tipikus gerinchálózati csomópont eszközt mutatunk be. A tipikus telephelyen rendelkezésre áll már egy 19"-os maghálózati szekrény (a szekrény magassága nem feltétlenül 220 cm, lehet kisebb is.). Minden eszköznek MPLS, és L2, L3 VPN szolgáltatások megvalósítására alkalmasnak kell lennie. Egy ilyen eszközt az alábbi (III-14. ábra) ábrán látható.



III-14. ÁBRA – 2 U MAGAS VÉGPONTI ÚTVÁLASZTÓ [28]

Egy tipikus repeater (Core-al jelölt) csomópont esetén 1 U magas eszköz használata javasolt, amely 24 Gigabit Ethernet portra bővíthető, és SFP modulokkal ellátható. Minden eszköznek MPLS, és L2, L3 VPN szolgáltatások megvalósítására alkalmasnak kell lennie. Egy ilyen eszköz az alábbi ábrán (III-15. ábra) látható:



III-15. ÁBRA - 1 U MAGAS VÉGPONTI ÚTVÁLASZTÓ [29]

A legnagyobb forgalmakat létrehozó budapesti gerinchálózati kialakítása más elveket igényel. Itt a Magyar Honvédség sok esetben rendelkezik szabad optikai szállal vagy szabad hullámhosszal, így ezeket az erőforrásokat a fentiekől eltérően, jobban kihasználhatjuk, nagyon kapcsolási sebességű eszközök alkalmazásával. Ezen telephelyek kialakítása olyan eszközökből kell, hogy történjen, amely 50 Gbps kapcsolási sebességekre képesek és ezen kapcsolási sebesség mellett képesek IP, és MPLS csomagokat továbbítani teljes sebességgel (ezt ún. wire-speed eszközöknek hívják), tehát nincs olyan problémája, hogy a csomagkapcsolási sebesség a csomagméret függvényében csökken.

Egy ilyen hálózati eszköz pl. az alábbi (III-16. ábra - Nagykapcsolási sebességű 2U magas útválasztó) ábrán szereplő Juniper MX80-as, de több más hálózati gyártó (Cisco, Alcatel-Lucent pl.) is rendelkezik hasonló eszközzel. Ezekben a telephelyeken az eszközök optikai szálon való összekötés esetén 10 Gigabit Ethernet interfészek használata javasolt, XFP vagy SFP+ modulokkal.



III-16. ÁBRA - NAGYKAPCSOLÁSI SEBESSÉGŰ 2U MAGAS ÚTVÁLASZTÓ[30]

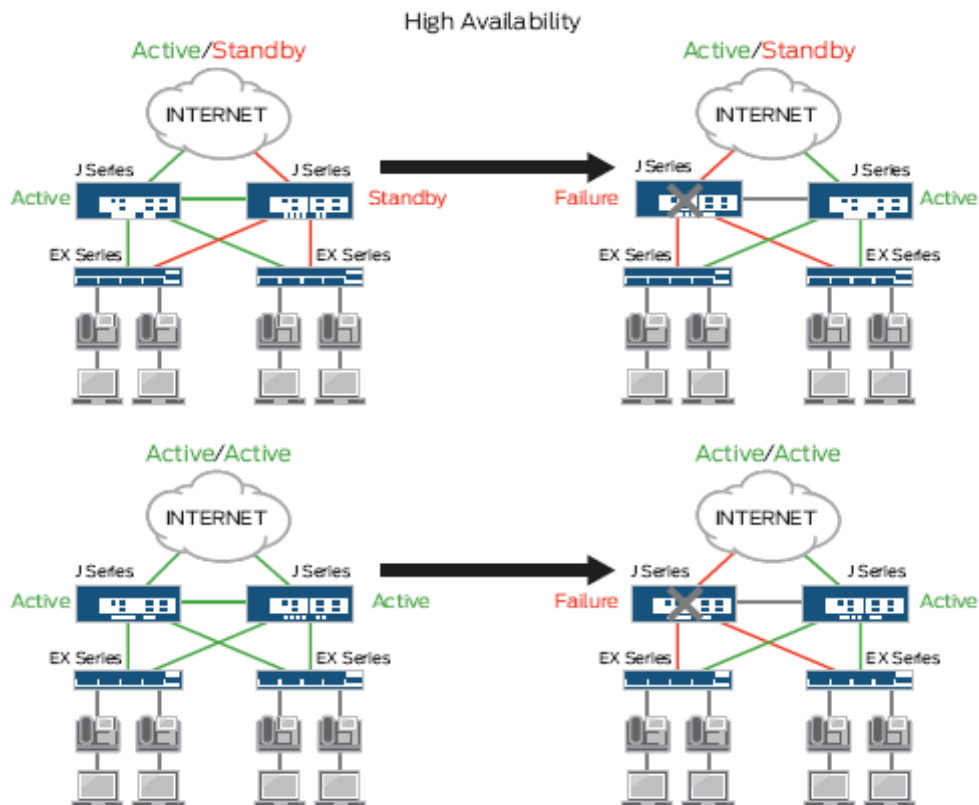
A fent meghatározott hálózati eszközök beltéri alkalmazásra kell, hogy alkalmasak legyenek, így a hőmérséklettartományuk, ill. a környezeti paramétereik elegendő, hogy ha az alábbi táblázatnak megfelelnek:

Környezeti paraméterek	Budapesti, optikai szállal rendelkező telephelyek	Edge típusú, végponti telephelyek	Core típusú végponti telephelyek
Fizikai méretek (W x H x D)	445 x 876 x 596 mm	445 x 44 x 383 mm	445 x 44 x 383 mm
Súly (kg)	13.7 kg		
Tápellátás (DC/AC)	-40 to -72 VDC 100 to 240 VAC	100–240 VAC	100–240 VAC -48 to -60 VDC
AC tápfogyasztás (elméleti aggregált)	500 W	80W	80W
DC tápfogyasztás consumption (elméleti aggregált)	500 W	N/A	80W
Működési hőmérséklet tartomány	0° - 40° C	0° to 50° C	0° to 50° C
Páratartalom	5% - 90%	5% - 90%	5% - 90%
Magasság	Nincs teljesítmény degradáció 4,000 m-ig	Nincs teljesítmény degradáció 4,000 m-ig	Nincs teljesítmény degradáció 4,000 m-ig
MTBF (Telcordia model)	min. 5 év	min. 5 év	min. 5 év

III-4. TÁBLÁZAT – ÚTVÁLASZTÓK KÖRNYEZETI PARAMÉTEREI

A fenti (III-4. táblázat – útválasztók környezeti paramétereit) táblázatból is látható, hogy a használt eszközök jellemzően 230 V AC tápellátással rendelkeznek. Minden telephelyen a szünetmentes tápellátás kialakítása javasolt, minimum 1 óra áthidalási idővel.

A kiemelt hálózati telephelyek (pl. a 3D-radarokkal ellátott, vagy kiemeltebb parancsnokságok telephelyei) nagy rendelkezésre állás kialakításban kell, hogy telepítésre kerüljenek. Ez történhet aktív-standby, vagy aktív-aktív módszerrel. Ilyen esetekben a telephelyeket kiegészítő telephelyi kapcsolókat is kell használnunk. Az alábbi ábra a két kialakítási típust ábrázolja. Aktív-standby esetben a tartalék csomópontra átálláskor az aktív csomópont nem üzemel, tehát nincs terheléelosztás a két csomópont között.



III-17. ÁBRA - NAGY RENDELKEZÉSRE ÁLLÁSÚ MŰKÖDÉS [31]

Aktív-aktív esetben, normál üzemben a két eszköz egyszerre működik és a hálózati forgalom által biztosított terhelést egyenletesen osztja el. Hiba esetén kizárólag az egyik működik, a másik passzív módban marad.

A gerinchálózat kialakításakor, tervezésekor bizonyos általános irányelveket szükséges figyelembe vennünk. Az irányelvek meghatározásakor szükséges a használt különböző belső és külső útválasztási protokollok beállításainak, a hibadetektálás és hibavédelem módjának, a hálózat által nyújtott szolgáltatásoknak és a szolgáltatásminőségnek, ill. a hálózat biztonsági beállításainak a meghatározása.

### A hálózaton használt útválasztó protokollok

Mind az IS-IS, mind az OSPF szóba jöhető belső útválasztó protokollok (IGP-k- Interior Gateway Protocol) a stacioner hálózatban. Mindkét protokoll állapot-út protokoll családba tartozik és hasonló jellegzetességekkel rendelkezik a stabilitás, skálázhatóság és Traffic Engineering és konvergencia terén.

A két protokoll hasonló annyiban, hogy:

- funkcióban és mechanizmusban nagyon hasonlóak

- állapotútalgoritmusok (a hálózati ábra elosztott, mindenegyres router függetlenül számolja az utakat a elosztott hálózati ábra alapján)
- Kétszintű hierarchiával rendelkeznek
- Designated routert (kiválasztott útválasztót) választanak LAN-okon
- széles körben használtak
- több együttműködő implementációja van
- támogatják az autentikáció titkosítását

Főbb különbségek:

- Enkapszuláció
  - OSPF IP felett fut
  - ISIS- L2 felett fut
- területi terv
  - az OSPF terület határok a routeren belülre esnek, tehát egy router több területhez is tartozhat
  - az IS-IS terület határok élre esnek, tehát egy router csak egy L1 területbe tartozhat (plusz még a L2 gerincre)

A döntés, hogy az egyik protokollt a másik elé helyezzük, pusztán preferencia alapon történhet – amennyiben a Magyar Honvédség üzemeltető személyzete jobban ismeri valamelyik protokollt, akkor azt érdemesebb előnyben részesíteni. Traffic engineering esetén a ISIS némi előnyt biztosít (részletesebben lehet információkat kinyerni, és jobban támogatja a hosztnevek alkalmazását)

Tervezési javaslatok:

1. Függetlenül melyik protokollt választjuk kiindulópontnak, a gerinchálózatot célszerű egy egységes területnek tervezni
  - a. OSPF egy gerinchálózat (area 0.0.0.0)
  - b. IS-IS egy level-2 terület
2. Mindkét esetben a résztvevő interfészek a következők:
  - a. Gerinchálózati belső linkek (PE-P, P-P)
  - b. loopback interfészek
3. Traffic engineeringet engedélyezzük OSPF-re, ill. ISIS-re (bizonyos router típusoknál ez az alapértelmezett)
4. Graceful Restart funkció engedélyezése (a router újraindulásakor az újraindulásról a szomszédokat értesíti)
5. Non-stop Forwarding (a folyamatos csomagtovábbítás biztosítására, ha vezérlési síkbeli hiba van az útválasztókon)

A gerinchálózatban MP-BGP (Multiprotocol Border Gateway Protocol) csomagokat célszerű átvenni, az NLRI (Network Layer Reachability Information) információ továbbítására a különböző címosztályok között. A Magyar honvédség hálózatában ezt a következő esetben érdemes használni:

- Unicast IP-VPN (Internet Protocol Virtual Private Network) kialakításakor (L3 (Layer 3) IP VPN)
- Unicast IPv4 továbbítására ( autonóm-rendszerhatárok között)
- L2VPN (Layer 2 Virtual Private Network) szolgáltatásra (BGP jelzésrendszerrel)
- VPLS (Virtual Private Lan Service) szolgáltatásra

### **A hálózaton használt jelzésprotokollok és szolgáltatások**

Az utóbbi két esetben LDP (Label Distribution Protocol) is használható a jelzéskialakításra (signaling). A BGP skálázhatóságának javítására, route-reflectorokat (RR) javasolunk. A teljes Magyar Honvédség hálózata egy privát (64512-65535) autonóm rendszerbe esik. A belső csomópontok között IBGP (Internal Border Gateway Protocol), a külsők felé E-BGP (External Border Gateway Protocol) használata javasolt, így az útvonalak kialakítása finomabb, és pontosabb szolgáltatási határ tesz lehetővé a harmadik rétegben. Konföderációk használata nem szükséges.

A hálózaton javasolt az MPLS kialakítása, amely a szolgáltatói hálózatban két főbb célt szolgál:

- VPN hálózati szolgáltatások kialakítását
- Traffic Engineering (TE) szolgáltatások kialakítását

Az MPLS technológia alapja az LSP (Label Switched Path – címkekapcsolt útvonal), amely két protokoll segítségével alakítható ki:

- Label Distribution Protocol (LDP)
- Resource Reservation Protocol with Traffic Engineering Extensions (RSVP-TE)

Az LDP működése automatikus, és minimális üzemeltetési beállítást igényel, azonban nem rendelkezik Traffic Engineering és Fast Reroute képességekkel, emiatt az RSVP-TE használata javasol. Helyes beállításokkal az RSVP-TE 10 miliszekundumos beállításra képes, a gyors konvergencia nagyon fontos nagy rendelkezésre állású hálózatok tervezésekor. A LSP jelzésrendszer tervezésekor kialakíthatunk hierarchiákat is,

1. LDP over RSVP (mind LDP+RSVP) egyaránt használt.
2. LSP hierarchiák : RSVP – TE, RSVP –TE-ben



Az LSP jelzésrendszer kialakításától függetlenül, különleges figyelmet szükséges folytatni a speciális esetekre – így a hangjelzésrendszerre és a hangforgalomra.

## **Hibadetektálás, hibavédelem a stacioner hálózatban**

BFD (Bidirectional Forwarding Detection) használata ajánlott az Ethernet linkeken. A Bidirectional Forwarding Detection-t definiáló Internet-Draft dokumentumból (draft-katzward-bfd-00.txt) idézve: a BFD rövid-időtartamú hibadetektálásra képes a szomszédos címtovábbító motorok között. A fizikai interfészeket, adatlinket és a csomagtovábbító motorokat is képes detektálni. A hardver platformtól függően, a hiba detektálása 10 ms-os nagyságrendben lehet. Néhány közeg (pl. Ethernet) nem biztosítja a gyors hibadetektálás lehetőségét, a BFD segítségével ez biztosítható, így a gyors hibadetektálás lehetséges a link-típusától függetlenül. Esetleges PoS (PPP over SDH) interfészek esetén (STM1-4-16-64) a BFD használata sok esetben szükségtelen, az SDH APS (Automatic Protection Switching) algoritmusai miatt.

A hibadetektálási idő mellett, a hibavédelem rendkívül fontos egy nagy rendelkezésre állású hálózat tervezésekor. A hibavédelemre alapvetően két megoldás létezik:

- végponttól – végpontig – útvonalvédelem
- pont-pont – helyi védelem

A legtöbb nagy rendelkezésre állású hálózatban mindkettő használt, és ezek használata a Magyar Honvédség hálózatában is javasolt. A hálózati telepítésekkor általános gyakorlat az elsődleges-tartalék megközelítés az útvonalvédelemre. Ebben a felépítésben két LSP-t (Label Switched Path) használnak:

- elsődleges: normál üzemben használt
- másodlagos: csak hibaesetben használt, amikor az elsődleges LSP út már nem áll rendelkezésre

A megfelelő védelem kialakításához az szükséges, hogy egy hiba ne befolyásolja az elsődleges és a másodlagos utat is. Ahhoz, hogy ezt elérjük az elsődlegesnek és a másodlagos LSP-nek két független úton kell keresztülmennie a hálózaton. A két különböző útvonal egyszerűen elérhető, ha az LSP-k egy IGP területen belül vannak, ebben az esetben használhatóak az IGP (Interior Gateway Protocol) Traffic Engineering (TE) képességei.

A helyi védelem esetén csak a hiba lokális környezetében kerül a forgalom átirányításra. A végpont-végpont (útvonal) védelemhez képest (amely a teljes jelzés végigfuttatását igényli a végpontig), a helyi védelem gyorsabb hibajavítást tesz lehetővé.

A helyi védelmi mechanizmusok kétféle osztályba sorolhatóak

- Osztályozhatóak a védett erőforrások típusa szerint, amely lehet egy él vagy egy csomópont. Így a helyi védelem lehet élvédelem vagy csomópontvédelem. A védett

erőforrástól függetlenül, a helyi védelmi mechanizmusokra együtt, mint helyi védelemre, vagy gyors útvonalváltás (FRR – Fast Reroute) hivatkozhatunk

- A védelmi út által védett LSP-k száma alapján is osztályozhatunk, így lehet 1:1, vagy N:1 védelem. Természetesen itt figyelembe kell venni a tartalékút skálázhatóságát, és hogy a forgalom hogyan továbbítható a védelmi úton

## **Hálózati szolgáltatások, szolgáltatásminőség biztosítása**

Az EDGE telephelyekként jelölt telephelyeken az alábbi szolgáltatásokat kell, hogy egy MPLS PE útválasztó nyújtson:

- biztonságos hozzáférés Internet hálózati szolgáltató hálózatához - így a forgalom a lehető legrövidebb úton, megbízható és biztonságos szolgáltató hálózatán keresztül jusson el az Internetre
- MPLS L2, L3 IP VPN hálózati szolgáltatás, a belső hálózati forgalmak számára
- Hangszolgáltatás biztosítása, a hangforgalmak migrálása a hálózatra
- Dedikált útvonalak biztosítása a hálózaton, a különböző jellegű és célú adatoknak, ezen típusú adatok közti világos szeparáció létrehozása
- Meglévő egyéb szolgáltatások migrálásának a támogatása
- IPv6 képesség
- Mobil adatszolgáltatások támogatása

Az MPLS VPN nem pusztán forgalmi izolációt jelent, hanem arra is biztosít lehetőséget, hogy nem IP alapú második rétegbeli forgalmat is keresztül lehessen vinni a hálózaton. Minden egyes VPN független, logikai hálózati szegmenst képvisel mind a vezérlési mind a továbbítási síkon. Ez forgalomvédelmet biztosít transzparens módon a hálózati rétegben, a gerinchálózatot használó ügyfeleknek.

Layer 2, Layer 3 VPN szolgáltatásokkal a hálózat egyes szolgáltatásait forgalmilag elválaszthatjuk egymástól. A Layer 2 alapú VPN arra biztosít lehetőséget, hogy a hálózat L2 szint felett transzparensen virtuális “kapcsolóként” viselkedjen. A L3 VPN arra biztosít lehetőséget, hogy a hálózatok L2 forgalmát az egyes telephelyeken leválaszthassuk. Ennek számos előnye lehetnek, néhányat itt soroltam fel:

- szolgáltatásminőség biztosítása, az egyes hálózati szolgáltatások számára (így pl. egy nagyobb fontosságú szolgáltatás számára prioritást tudunk biztosítani)
- dedikált erőforrások biztosítása az egyes szolgáltatásokra
- forgalmi szeparáció így az egyes szolgáltatások biztonságosan, és szeparáltan futhatnak egy virtualizált hálózaton

A szolgáltatásminőség biztosítására legkevesebb 4 szolgáltatásosztályt javaslok (ezek megfelelnek a 3GPP Release 4 dokumentum által meghatározottaknak). A gyakorlatban négy vagy nyolc szolgáltatásosztály használt a hálózatokon a legtöbb esetben. Ennek az oka az,

hogy a QoS (szolgáltatásminőség) osztályok bevezetése egységes kell, hogy legyen a hálózatokon.

Az alábbi (III-5) táblázatban felsoroltam a szolgáltatásokra kialakított szolgáltatásminőség jellemzőket. Az ábrán szereplő táblázat oszlopai a szolgáltatás jellegét mutatják a késleltetés, puffereles, forgalmi szimmetria, és garantált sávszélesség sorrendben, a sorai pedig a sávszélesség osztályokat tartalmazzák (beszélgetési, folyamjelleű, interaktív és háttér).

	Késleltetés	Puffereles	Forgalmi szimmetria	Garantált sávszélesség
beszélgetési (voice)	lehetséges minimum fix (15 ms)	hálózat szinten nincs	szimmetrikus	garantált
folyamjelleű (video / streaming)	minimum változó (30 ms)	engedélyezett	asszimmetrikus	garantált
interaktív forgalom (premium)	csekély mértékben változó (40 ms)	engedélyezett	asszimmetrikus	nem garantált
háttér forgalom (best effort)	nagy mértékben változó (50 ms)	engedélyezett	asszimmetrikus	nem garantált

III-5. TÁBLÁZAT SZOLGÁLTATÁSMINŐSÉGI PARAMÉTEREK

A beszélgetési és folyam osztályok főként a valós-idejű forgalmi folyamatokat határozzák meg (pl. hang, video, jelzés) míg az interaktív és a háttér osztályok főként az adat alapú alkalmazásoknak (FTP (File Transfer Protocol), Telnet, Email, WWW (World Wide Web), SMS stb). A DiffServ (Differentiated Services) architektúra a leggyakrabban használt az erőforrásallokációra. A DiffServ kombinálható állandó forgalmi utakat biztosító forgalomtervezéssel (Traffic Engineering-gel), így a két technológia kiegészíti egymást (pl. a gerinchálózaton Traffic Engineering + Diffserv, a hozzáférési és aggregációs hálózaton Diffserv alapú QoS). A fentieknek megfelelően öt szolgáltatásosztály használatát javaslom a gyakorlatban:

- Hálózati jelzésprotokollok – NC – network connect szolgáltatásosztály
- VoIP (Voice Over Internet Protocol) jelzés - signaling - (H.323), ez a beszélgetési szolgáltatásosztály
- VoIP hang - voice (RTP – Real Time Protocol) – beszélgetési szolgáltatásosztály
- Kiemelt adatforgalom – katonai informatikai alkalmazások, minősített adatok számára
- Üzemeltetési és IT szolgáltatások – O&M (Operation and Maintenance) and IT (Information Technology), Internet - háttér szolgáltatások

Az alábbi táblázatban (III-6. táblázat - Forgalmi osztályba sorolás) megjelöltem a szolgáltatásosztályokhoz tartozó DSCP osztályokat és az EXP biteket. A különböző MPLS technológiát javaslom az egyes szolgáltatásokhoz. A DSCP (DiffServ Code Point) az IP fejléc QoS célra fenntartott mezője, az EXP (Experimental) pedig az MPLS fejléc QoS célra fenntartott mezője. Így mind tiszta IP, mind IP/MPLS hálózaton meg tudjuk valósítani a szolgáltatásminőséget biztosító szolgáltatásosztályokat.

Forgalom típusa	DSCP osztályok	EXP	Használt MPLS technológia
Hálózati jelzésprotokollok	NC (Network Control)	7	N/A
VoIP jelzés (H.323)	AF41 (Assured forwarding)	4	VPLS
VoIP hang (RTP)	AF43 (Assured Forwarding)	5	L3VPN
Kiemelt adatforgalom	EF (Expedited Forwarding)	3	L2VPN/VPLS
O&M és IT szolgáltatások – O&M	BE (Best Effort)	0	L3VPN
Internet traffic	BE (Best Effort)	0	L3VPN

III-6. TÁBLÁZAT - FORGALMI OSZTÁLYBA SOROLÁS

A VPLS az MPLS szolgáltatás feletti virtuális privát LAN szolgáltatás. A szolgáltatás felhasználója szempontjából a hálózat egy LAN hálózatnak látszik. L3VPN az RFC 2547bis szabványban meghatározott harmadik rétegbeli (MP-BGP) jelzésrendszert felhasználó virtuális magánhálózati szolgáltatás.

A hálózaton fontos az egyenletes és stabil szolgáltatásminőség biztosítása, és mérése. A szolgáltatásminőséget a KPI-k (Key Performance Indicatorok) határozzák meg – ezek az ún. szolgáltatás minőségi jellemzők. Az alábbi táblázat a legfontosabb KPI-ket határozza meg a különböző szolgáltatás osztályokra, az itt használt táblázathoz a 3GPP forgalmi osztályait vettem alapul. Ezek alapján a hálózati elemeken létrehozhatóak a szolgáltatásminőség (Qos) profiljai, és tervezési dimenziói. Az egyes szolgáltatások (III-7. táblázat Forgalmi osztályok Minőségparaméterei) a valósidejű (Conversational), jelzés (Signalling), streaming (nem valósidejű, de folyamatos szórással sugárzott) az interaktív (Interactive) – amely egy kvázi valósidejű és a háttér (Background) – tehát best effort jellegű forgalom.

A használt KPI paraméterek a következők:

- átlagos késleltetés (average delay) – miliszekundumban
- maximális késleltetés (maximum delay) – miliszekundumban
- a késleltetés változása (jitter)
- csomagvesztés (packet loss)
- átkapcsolási idő (failover time)

	Átlagos késleltetés(msec)	Maximum késleltetés(msec)	Jitter(msec)	Csomagvesztés	Átkapcsolási idő
Beszélgetési	<20	<100	<5	<10 <sup>-4</sup>	2 sec
Folyamjellegű (jelzés)	<20	<100	-	<10 <sup>-4</sup>	(protokollátkapcsoláson múlik)
Folyamjellegű (hang)	-	-	<100	<10 <sup>-4</sup>	5 sec
Interaktív	<55	-	-	<10 <sup>-4</sup>	5 sec
Háttér	<100	-	-	<10 <sup>-3</sup>	-

III-7. TÁBLÁZAT FORGALMI OSZTÁLYOK MINŐSÉGPARAMÉTEREI

Az egyes paraméterek folyamatos monitorozása szükséges. Ez az ún. SLA monitoring rendszereken keresztül biztosítható. Ezek a rendszerek a KPI paramétereket a hálózat folyamatos mérésével állapítják meg. A hálózati paraméterek értéke meg kell, hogy feleljen

az SLA szerződésben meghatározott rendelkezésre állási és KPI paraméter értékeknek. Az SLA szerződés a hálózat üzemeltetője és a hálózat felhasználói között kell, hogy létrejöjjön.

## **A hálózat biztonságának biztosítása**

A stacioner hálózat kialakításakor egy másik kiemelt kérdés a hálózat biztonságának biztosítása. Itt a elsősorban az informatikai biztonság kérdésével foglalkozom, a fizikai és egyéb biztonsági kérdésekre itt nem térek ki. A hálózati biztonság a hálózati biztonsági zónák (“Security Domains”) alapvető koncepciójára épülnek. Minden egyes biztonsági terület összeségében különböző titkosítási szinten lévő forgalmat visz, tehát különböző típusú forgalom, amely különálló privát hálózatnak felel meg.

A privát hálózat a következő két típus egyike lehet:

- fizikai privát hálózat, ahol minden egyes forgalmi típus egy dedikált fizikai infrastruktúrát használ (tehát külön LAN switch-eket routereket, átviteli utakat stb.)
- virtuális privát hálózat, ahol több forgalmi típus egy közös fizikai infrastruktúrán osztozik (ebben az esetben a szeparáció még mindig megvalósul az ún. erőforrás “virtualizáció” által)

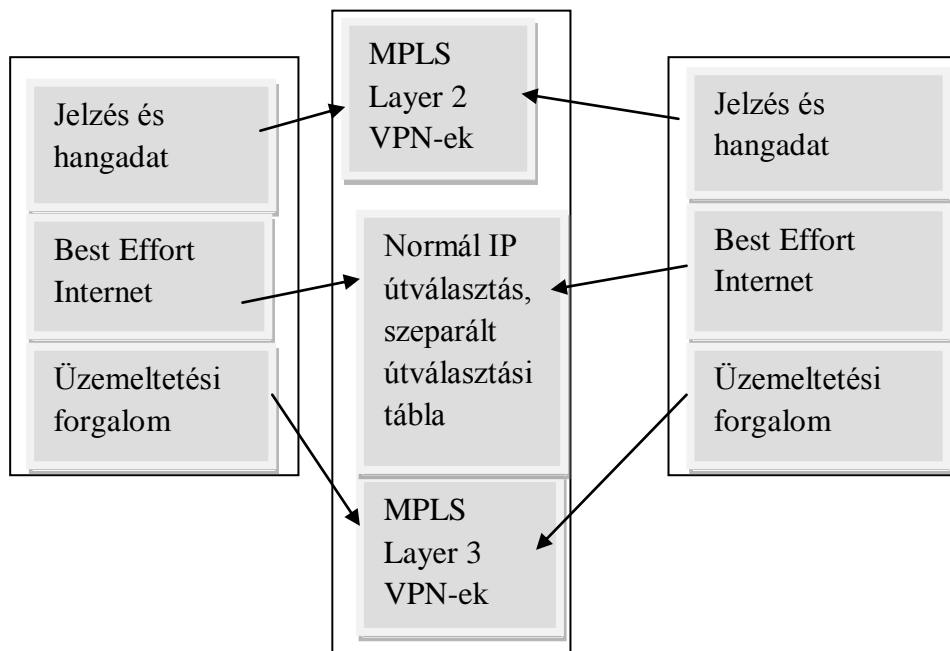
Általában véve a különböző típusú privát hálózati forgalmak nem keverednek, de bizonyos meghatározott pontokon átmehetnek egy biztonsági zónából egy másikba, kizárólag meghatározott hálózati elemeken keresztül (pl. tűzfalakon keresztül) és csak meghatározott és szigorú szabályoknak megfelelően – amit a biztonsági szabályzat ír elő.

A hálózati virtualizáció egyre jobban meghatározó technológiává válik a hálózati iparágban.

Különböző technológiákat használnak erre:

- virtuális LAN-okat (VLAN-ok)
- IP/MPLS VPN-ek – IP MPLS virtuális privát hálózatok , akár a második (L2VPN, L2circuit) akár a harmadik rétegben (L3VPN)
- IPSecurity (IPSec) – titkosítás használata az IP hálózati szinten

Általában véve a VLAN-okat egy hálózati POP (Point of Presence)-on belül használnak, az MPLS-t pedig a gerinchálózaton. Az IPSec egy további titkosított biztonsági réteget képezhet, szuperszenzitív forgalmak számára, úgy mint O&M, számlázás, törvényes lehallgatás (LI). Ezek a technológiák nem zárják ki egymást , de általában nem ugyanazon a forgalmi típuson, vagy hálózati rétegben fordulnak elő. Az alábbi ábra a szolgáltatásosztályok VPN technológiával való szeparációját mutatja be. Ezek a VPN osztályok skálázhatóak, hogy olyan további forgalmi osztályokat tartalmazzanak, amelyeket a jövőben kívánnánk használni.



III-18. ÁBRA – FORGALMAK ÉS SZOLGÁLTATÁSOK ÖSSZERENDELÉSE

Az üzemeltetési célú (O&M) forgalom IPSec titkosítással ellátott lehet. Az általános célú Internet forgalmat nem célszerű titkosítani, míg a hang és belső célú minősített forgalmak titkosítással ellátottak lehetnek.

Az IP hálózat biztonságának növelésére javaslom, hogy az

- az irányított broadcast üzenetek szűrésre kerüljenek
- távoli menedzsment hozzáférés meghatározása naplózott, titkosított protokollokon keresztül
- SNMP (Simple Network Message Protocol) Set üzenetek tiltva, vagy csak meghatározott IP címekről elérhető módon legyenek frkonfigurálva
- alapértelmezett az útválasztó felé menő ARP (Address Resolution Protocol) üzenetek korlátozása, ami leszűri az ún. ARP viharokat, amelyeket a hibás beállítások vagy rosszindulatú cselekedetek indítanak. Az ARP üzenetek mennyiségét az Ethernet interfészekon tovább korlátozhatjuk
- csak meghatározott hoszt és hálózati címeket használjunk (ún. Marsi, vagy Martian címek), amelyről minden útválasztási információt figyelmen kívül kell hagyni

DoS (Denial of Service) támadások gyorsan változó forráscímeket használhatnak, amelyeket a támadók a lokalizálás és szűrés kivédésére használnak. Az ún. unikaszt RPF (reverse path forwarding), úgy semlegesíti ezeket a támadásokat, hogy csak olyan csomagokat továbbít az ezt alkalmazó útválasztó, amelynek a forráscímei érvényesek és megfelelnek az útválasztó tábla által meghatározottaknak. Az unikaszt RPF szolgáltatás, olyan problémák elhárításában segít, amely a hamisított forrás IP címeket nem engedi be a

hálózatban azáltal, hogy csak az útválasztó tábla által ellenőrizhető forrás IP című IP csomagokat továbbítja, a többit eldobja.

Az elárasztásos támadások elleni védelemre az alábbi beállításokat javaslom:

- az ICMP elárasztásos támadások elleni védelem érdekében az útválasztó felé irányuló ICMP forgalom mennyiség korlátozását javaslom
- A TCP (Transmission Control Protocol) SYN flood támadások elkerülése érdekében, a TCP SYN üzenetek korlátozását javaslom. Ebben az esetben a támadó egy szkriptet vagy programot használva TCP nyitási (SYN) üzeneteket generál, olyan sebességgel amely gyorsabb mint az áldozat bontási ideje
- A PE útválasztókon sávszélesség korlátok használatát javaslom

Az útválasztók biztonságát a titkosított útválasztási protokollok használata tovább növeli. Ezért az összes használt útválasztási protokollra (BGP, OSPF, IS-IS, RIP és RSVP (Resource Reservation Protocol) a HMAC-MD5-ös (Hash-based Message Authentication Code) autentikáció beállítását javaslom. Az útválasztóval a kommunikáció csak titkosítottan történhet ezért az alábbi protokollok használatát javaslom:

- ssh (secure shell), a router inband menedzsmentjére az SSH titkosított kommunikációt biztosít, egy nem megbízható hálózaton
- SCP (secure copy), az SSH titkosítási mechanizmusán keresztül, titkosítottan másol fájlokat a hosztok között
- Központi autentikációs szolgáltatást használva az útválasztókon, a hálózati belépés egyszerűsödik
  - ezt RADIUS, vagy TACACS+ protokollokon keresztül lehet megoldani
  - OTP (one time password) egyszeri használatú jelszavak használata

Az útválasztó motorhoz bejövő forgalmakat szükséges szűrni azért, hogy az útválasztó erőforrásai (CPU óraciklusok, és kommunikációs sorok) védve legyenek. Ezért csak a megbízható forrásból származó protokoll és vezérlési információkat engedélyezhetjük az útválasztó motor felé.

## **Példakonfiguráció kialakítása a beállításoknak megfelelően**

Az alábbi konfigurációs beállítások mellett lehetővé válik a hálózaton az automatikus útválasztás, az előre lefoglalt utak használata, l2vpn szolgáltatások használata, a forgalmi rétegek elkülönítése, az erőforrásfoglalás RSVP jelzésrendszerrel, hibadetektálás és gyors hibavédelem, gyors útválasztási protokoll konvergencia amennyiben a hálózati topológia gyorsan változna valamint tervezhető kapacitású útvonalak kialakítása a gerinchálózaton. Az alábbiakban részletesem ismertetem, hogy milyen konfigurációs beállítások szükségesek az útválasztókon:

```
rsvp {  
  
  interface ge-0/0/1.0 {  
  
    link-protection {  
  
      bandwidth 100m;  
  
    }  
  
  }  
  
}
```

#### 1. KONFIGURÁCIÓ - RSVP SÁVSZÉLESSÉG LIMITTEL

A fenti konfigurációs sorok segítségével RSVP protokollt használva, 100 Mbps-es sávszélességet foglalhatunk le az útvonalvédelem céljára minden egyes interfészen.

```
mpls {  
  
  traffic-engineering bgp-igp-both-ribs;  
  
  label-switched-path toHold {  
  
    to 192.168.1.14;  
  
    bandwidth 10m;  
  
    node-link-protection;  
  
    fast-reroute;  
  
  }  
  
}
```

#### 2. KONFIGURÁCIÓ MPLS LSP ÚTVONAL KONFIGURÁCIÓ

A fenti konfigurációs sorok segítségével engedélyezzük a traffic engineering funkciót, valamint kialakítjuk az útvonalat 10 Mbps-el, és csomópont-link-védelemmel, valamint gyors új-útválasztás funkciókkal ( ez utóbbi funkció biztosítja, hogy az eszközök képesek legyenek az 50 ms-on belüli útválasztásra), valamint engedélyezzük a többprotokollós címkekapcsolást (MPLS) valamennyi interfészen.



```

ospf {
    traffic-engineering;
    area 0.0.0.0 {
        interface all {
            ldp-synchronization;
            bfd-liveness-detection {
                minimum-interval 50;
            }
        }
        interface ge-0/0/0.0 {
            disable;
        }
    }
    interface ge-0/0/1.0;
}

```

A fenti konfigurációs sorok segítségével biztosítjuk az ldp protokoll és ospf protokoll a szinkronizációt, biztosítva a hibás hálózati konfiguráció esetén az átjelzést egyik protokollból a másikba. Valamint a BFD protokollt, amelynek segítségével az egyes csomagtovábbító motorok közti utak kiesése esetén tudunk ms-os nagyságrendben átjelezni, és újra csomagot továbbítani.

```

ospf3 {
    area 0.0.0.0 {
        interface ge-0/0/2.0;
    }
}

```

#### 4. KONFIGURÁCIÓ OSPFV3 KONFIGURÁCIÓ

A fenti konfigurációs sorok engedélyezik az OSPFv3 protokollt (az IPv6 dinamikus útválasztó protokollját).

```

ldp {
    interface ge-0/0/1.0;
    interface lo0.0;
}

```

#### 5. KONFIGURÁCIÓ LDP KONFIGURÁCIÓ

A fenti sorok az LDP protokollt engedélyezik az interfészeken.

```
l2circuit {  
  
    neighbor 192.168.1.12 {  
  
        interface ge-0/0/1.1111 {  
  
            virtual-circuit-id 1111;  
  
        }  
  
    }  
  
}
```

#### 6. KONFIGURÁCIÓ L2VPN ÁRAMKÖR

A fenti sorok egy mintakonfigurációt mutatnak, pont-pont L2VPN (Ethernet privát vonali ) szolgáltatáson keresztül egy szolgáltatás biztosítására.

### **A hálózat kiépítésének költségvonzata**

Egy modern műszaki értekezésben nem tekinthetünk el a kiépítés költségvonzataitól. A fentiekben leírt hálózat kialakítása 30 csomópontot, a hozzátartozó Ethernet mikrohullámú hálózatot és az IP/MPLS útválasztókat figyelembe véve, néhány százmilliós költséggel jár, ez az optikai útvonalak kiépítésének és/vagy bérlésének a költségét nem tartalmazza, azonban az eszközpark kialakítását, és az egyes telephelyeken elvégzendő munkákat beleértve a hálózatmenedzsment, a kábelezés, a szünetmentes tápellátás, a pont-pont valamint a hálózatszintű kialakítás költségeit. A költségeket telephelyenként lebontva, egy hosszabb távú fejlesztési koncepcióban kell részletesebben meghatározni.

A költségekben ott adódhat jelentős különbség, hogy az útválasztókat milyen teljes adatkapacitásra méretezzük. Ezt érdemes a fizikai hálózat sajátosságaihoz méretezni – Ethernet mikrohullámú hálózatrészekre 1 Gbps képes eszközöket, az optikai gerinchálózatra pedig portonként 10 Gbps képes eszközöket - a korábban már meghatározott módon.

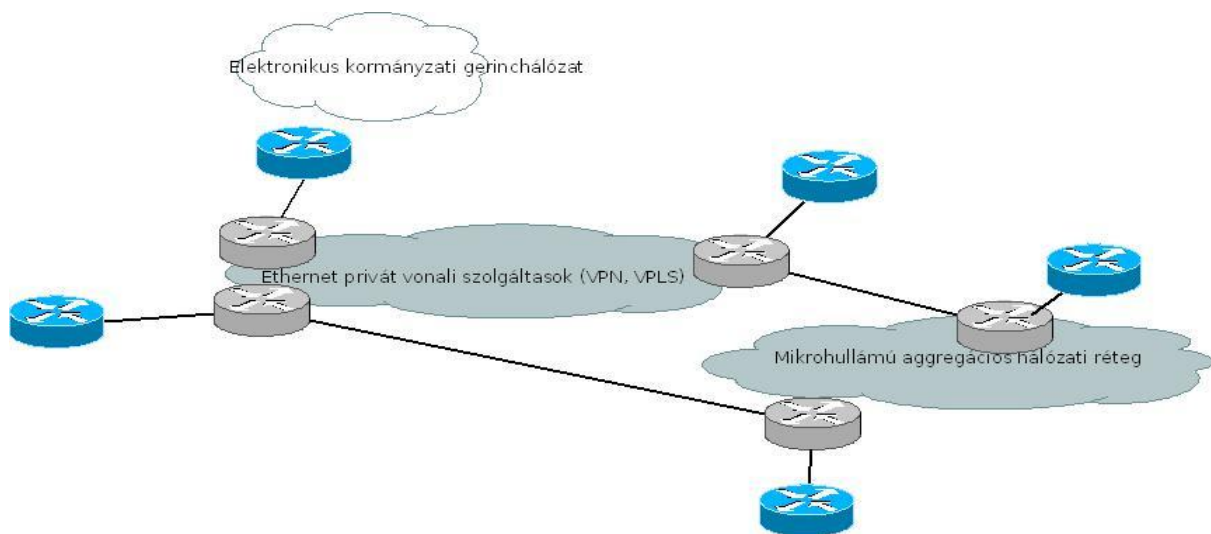
### **A Magyar Honvédség stacioner hálózatának javasolt migrációs útja**

Az egyik legfontosabb kihívás, az IP alapú adatforgalom dinamikus növekedése, és az ezzel járó strukturális és kapacitásproblémák áthidalása. Az IP alapú adatforgalom a távközlési hálózatokban [32] exponenciálisan növekszik, és 2002-2003-as évek tájékán a legtöbb hálózatban forgalmi volumen tekintetében meghaladta a hangforgalmat, és mára dominánssá

vált. Ezért olyan hálózatot célszerű építeni, amely ezen forgalom volumenére és jellegére tervezett, mindazonáltal meg kell őrizni, a korábban megszokott, és jogosan elvárt hangszolgáltatások minőségét.

A fejlesztés és integráció irányaként egy többlépcsős fejlesztést javaslok. Az integráció első lépésében az IP hálózat kiépítése szükséges, hogy az eddig elszigetelt LAN-okat egy egységes hálózatban láthassuk – ez a menedzselhetőséget nagyban megkönnyíti. Ezek a fejlesztések folyamatban vannak, vagy a rövid távú fejlesztési tervekben szerepelnek.

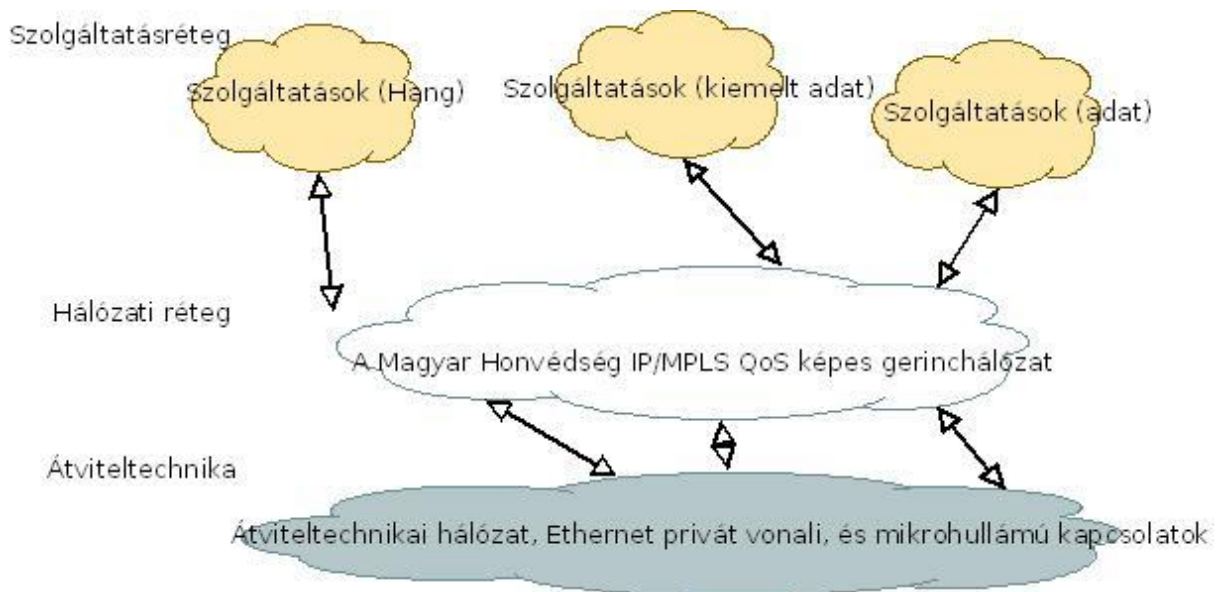
A második lépcsőben meglévő mikrohullámú hálózatot az aggregációs szintre kell helyezni, és a gerinchálózatot pedig nagy sebességű mikrohullámú, optikai szálas, vagy az EKG keresztüli VPN/VPLS szolgáltatáson keresztüli összekötése szükséges. Ez a lépcső megoldja a gerinchálózat és az aggregációs hálózat kapacitásproblémáit. Az alábbi ábra (III-19. ábra) mutatja a hálózat sematikus képét ezután a lépés után.



III-19. ÁBRA A MAGYAR HONVÉDSÉG ÁLLANDÓ HÍRRENDSZERÉNEK VÁZLATA

A harmadik lépcsőben a teljes hálózatot QoS képessé kell tenni, egységes QoS mechanizmust kell kialakítani a hálózatban, ill. a hang és video hívások hívásvezérlését szoftveres, IP feletti központi kapcsolóval kell megoldani. A helyi központok trunk oldali IP képessé tétele is fontos.

A negyedik ütemben az IP képes gerinchálózatot, az MPLS – által nyújtott lehetőségekkel kell kiegészíteni (MPLS Traffic Engineering, QoS, tartalékútvonalak, FRR, Pseudowire, VPN/VPLS szolgáltatások), ezzel egyidejűleg az MPLS képes routereket, szoftveresen moduláris, nagy rendelkezésre állású redundáns vezérlővel ellátott, szeparált csomagtovábbító, és vezérlőrendszerrel rendelkező routerekre kell cserélni. Ezzel párhuzamosan be kell vezetni a hálózati szintű folyamméréseket, ill. a különböző Ethernet, és MPLS útvonalparaméterek mérését a QoS paramétereknek megfelelően. Így kialakítható a szolgáltatás, a hálózati és az átviteltechnikai hálózati szegmensek között megfelelő hálózatminőséget biztosító SLA kapcsolatok. Az alábbi ábra (III-20. ábra)



III-20. ÁBRA MAGYAR HONVÉDSÉG STACIONER HÁLÓZATI RÉTEGEI

A fenti ábra stilizáltan mutatja az elért hálózati képet, a migrációs ütemeket követően. Ezen ütemek bevezetése után lehet a hálózat valóban szolgáltatás-orientált, és mondhatjuk azt róla, hogy megfelel az Összhaderőnemi doktrínában kitűzött céloknak. A fenti ütemek megvalósulása, megoldja az előző alfejezetben leírt problémákat, és a Magyar Honvédség állandó hírendszereit felkészíti a közeljövőben várható katonai informatikai fejlesztések által támasztott adatátviteli igényekre..

A korábbi fejezetek során megállapítottam, hogy a stacioner hálózat legnagyobb problémája jelenleg a gerinchálózati kapacitások szűkös jellege. Ennek a megoldására az Ethernet mikrohullámú eszközök kínálkoznak, a jelenlegi stacioner hálózati eszközök esetleges kiváltására. Ezen eszközök specifikációját az előző fejezetben meghatároztam, így ebben a fejezetben az áttérés módját írom le.

A migráció első lépcsőjében az Ethernet mikrohullámú hálózat kialakítása történhet meg. Ennek a hálózatnak műszaki szempontból a legbiztonságosabb migrációs útja a meglévő PDH mikrohullámú eszközök mellett, párhuzamos Ethernet mikrohullámú hálózat kialakítása. Minden más megoldás szolgáltatásmegszakadással járhat amelynek a költségvonzatai nehezen felmérhetőek, mert az összes meglévő hálózati szolgáltatást érintené, beleértve a hangalapú szolgáltatásokat is.

A stacioner hálózat módosítása mellett a fenti hálózati módosítás érinti az informatikai hálózatot is. Az informatikai hálózatban a fenti szolgáltatás működtetéséhez szabad Gigabit Ethernet portokra van szükség.

A migráció második lépcsőjében egy egységes kormányzati szolgáltató által nyújtott vonali szolgáltatások használata javasolt. Ennek a műszaki oka az, hogy stratégiai távlatokra kitekintve a fizikai közeg korlátai miatt optikai szálakon alapuló hálózat kialakítása szükséges. Nem célszerű egy ilyen infrastruktúra saját célra kiépítése, ezért az alternatíva egy

kormányzati szolgáltató bevonása lehet. Erre a Nyugat-Európában vannak kezdeményezések (pl. [17]). Infrastruktúra tekintetében a szóba jöhető országos optikai hálózati szolgáltatók a következők:

- Magyar Villamos Művek (áramszolgáltatói hálózatokon kialakított hálózat)
- Invitel/HTCC (Magyar Állam Vasútak hálózata mentén kialakított hálózat)
- Magyar Telekom Nyrt. (Saját infrastruktúra hálózat a volt Matáv, ill. Magyar Posta infrastruktúráján)

A fenti szolgáltatók közül az alábbi érvek mentén szükséges mérlegelni a kiválasztandó szolgáltatót:

- a beruházás megvalósításának költségei a Magyar Honvédség ill. a beruházó számára
- a Magyar Állam kezében lévő cégről van szó, vagy privát / külföldi befektetők kezében lévő cég (ezt a beruházás nemzetbiztonsági fontossága indokolja)
- mely szolgáltató hálózata minősül kritikus infrastruktúrának, így a szolgáltatónál vélhetően kialakult gyakorlat van nagy-rendelkezésre állású hálózatok üzemeltetésére

Ezen kritériumok mindegyikének csak a Magyar Villamos Művek felel meg, de a fenti három szolgáltató hálózatán (bizonyos megkötésekkel) kialakítható egy hasonló célú hálózat. A kérdésben mindenféleképpen kormányzati tenderkiírás javasolt.

Bármelyik szolgáltatót választják, minden esetben javasolt a szolgáltatótól Ethernet privát vonali vagy virtuális privát LAN szolgáltatás bérlése. Természetesen ebben az esetben is szükséges a korábban ismertetett biztonsági eljárások betartása, ill. biztonsági szolgáltatások használata. Szintén szükséges egy, a szolgáltató hálózatától független útválasztó hálózat kialakítása.

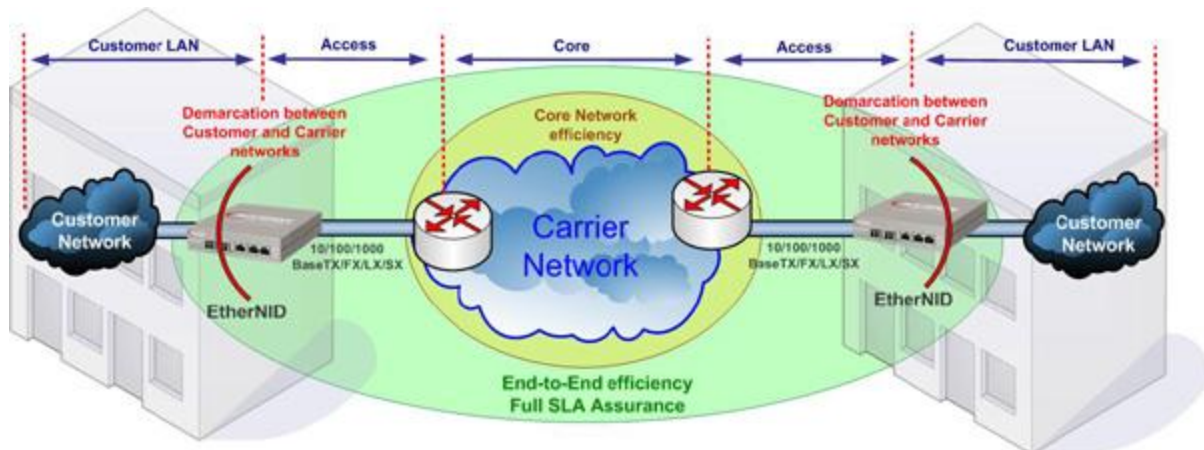
A minősített és általános célú adatforgalmi utak szétválasztásához szükséges szolgáltatói privát vonali szolgáltatás biztosítására szükséges valamilyen útválasztó eszköz használata az egyes telephelyeken.

A javasolt stacioner adatátviteli hálózat beállításait egy mintahálózaton munkatársaimmal megvalósítottam és a nyújtandó szolgáltatásokat teszteltem. A mellékletben csatoltam a teszt kialakítását és eredményeit.

### **III.4 A hálózat rendszerszintű mérése**

A hálózat rendszerszintű mérése azért szükséges, hogy a szolgáltatás minőségét folyamatosan fenntarthatassuk. A mérési, ellenőrzési funkció a belépési/kilépési pontokon, a hálózat határvonalán lehetséges. A hálózat mérése az egyes a hálózat által biztosított szolgáltatások szolgáltatásminőségi paramétereinek (KPI – Key Performance Indicator) mérésével lehetséges.

A hálózat rendszerszintű mérése többféleképpen lehetséges. Legáltalánosabban elterjedt módszer szerint, Ethernet mérőpontok ún. probe-ok, vagy tap-ek közbeiktatásával, a forgalom zavarása nélkül mérhetőek a forgalmi paraméterek. További lehetőséget biztosít egyes gyártók által biztosított valós idejű teljesítmény (performancia) monitorozás. Az Ethernet tapok másolatot készítenek az átvitt forgalomról és ezt egy fenntartott porton továbbítják feldolgozásra. A feldolgozás lehet mérőcélú feldolgozás, de az adatokat felhasználhatjuk forgalmi analízisre, ill. a forgalmi minták elemzésére is – ezek alapján a hálózati szolgáltatásokat a forgalmi és felhasználói igények változásainak megfelelően alakíthatjuk ki.



III-21. ÁBRA VÉGPONT-VÉGPONT KÖZTI SZOLGÁLTATÁSSZINT MÉRÉSE [38]

A fenti ábra (III-21. ábra) a szolgáltatásszint (SLA) mérések elvét mutatja két demarkációs eszközként szolgáló Ethernet tap között. Az Ethernet tapok, az szolgáltatási határszinten képesek a forgalom figyelésével, és megfelelő feldolgozó szoftverek alkalmazásán keresztül az egyes szolgáltatások (így VoIP, Video konferencia, VPN, Best Effort jellegű forgalmak) szolgáltatásminőségének mérésére.

Egyes útválasztókon támogatott a valós idejű teljesítménymérés az ún. real-time-performance monitoring. Amennyiben külső eszköz nem adott a teljesítmény mérésére, ez a módszer is megfelelő eredményeket biztosít, és az alkalmazása költséghatékonyabb, mint a külső Ethernet tapoké. Útválasztókon történő teljesítményérzéses tesztek a kutatásaim során végeztem, ennek eredményei szerepelnek a mellékletben. Ebben az esetben az eszköz RPM (real-time-performance-monitoring) modulját használtam a méréshez. Mérésméleti szempontból ez nem tökéletes, mert a mérendő útválasztó teljesítménye befolyásolhatja a mérés eredményét, azonban a gyakorlati életben nagyon jól használható funkció.

### III.5 Összegzés

Az első fejezetben bemutattam, hogy a stacioner hálózatban az alábbi technológiai jellegű hibák vannak:

**Inhomogén hálózati elemekből és technológiákból épül fel**, hiszen vegyes TDM és csomagkapcsolt alapú rendszerek alkotják, amik több humán erőforrást igényelnek az üzemeltetői oldalról (nem egységes technológia miatt). Erre a problémára a fejezet során **egységes Ethernet/IP/MPLS hálózatot** javaslok, nagysebességű IP/MPLS útválasztókkal és Ethernet mikrohullámú eszközökkel.

Sok esetben a **hálózati erőforrások nincsenek megfelelően kihasználva** (a hangforgalom nem tölti meg a mikrohullámú hálózatban rendelkezésre álló kapacitásokat, így a kapcsolatok kihasználtsága alacsony, az adatforgalom telíti a hálózatot. A problémát új nagykapacitású útválasztók használatával, nagykapacitású Ethernet mikrohullámú eszközök használatával és tudatos kapacitástervezéssel javaslom megoldani.

A stacioner hálózat jelenleg, **nem teszi lehetővé** a katonai informatikai rendszerek által megkövetelt **nagyobb mennyiségű adatok gyors átvitelét**. Ezt a problémát is az előző két fejezetben ismertetett módon, új nagykapacitású útválasztók használatával, nagykapacitású Ethernet mikrohullámú eszközök használatával és tudatos kapacitástervezéssel javaslom megoldani.

**Nincs megfelelő adatátviteli sebességű kapcsolat a stacioner és tábori kommunikációs rendszerek között**. A helyzetet belföldi tábori esetben Ethernet mikrohullámú eszközök alkalmazásával javaslom megoldani.

Egyes helyeken elszigetelt LAN-okból áll a Magyar Honvédség stacioner hálózata. Ez egy strukturális probléma, célszerű egységes, és minél inkább összekötött hálózatot kialakítani. A minnél inkább összekötött hálózatot hálózati szinten rugalmas IP/MPLS útválasztók alkalmazásával javaslom megoldani.

**Nincs egységes QoS (szolgáltatásminőség) bevezetve a hálózatban**, ami azt eredményezi, hogy jelenleg a hálózat Best Effort jellegű szolgáltatásokat nyújt (elindult ennek a bevezetése, az IP feletti hangátvitel kialakításával együtt). Ez egy paraméterbeállítási és tervezési kérdés. A paraméterek konfigurációját ebben a fejezetben részletesen ismertettem.

**Nem használtak az IP/MPLS nagyobb megbízhatóságot nyújtó védelmi mechanizmusai**, a jelenleg használt útvonalvédelmi mechanizmusok nem elégségesek ill. megfelelőek katonai gerinchálózat védelmére. A védelmi mechanizmusok kialakításához üzembiztos útválasztókra van szükség, a védelmi mechanizmusok kialakítását a fejezet során **kialakítottam és meghatároztam**.

**Nincs Traffic Engineering a hálózatban**. A hálózatban nem használtak azok a protokollok ill. hálózati technológiák amelyek lehetővé tennék a megfelelő hálózatkihasználtságot, a tartalékútvonalak üzembiztos használatát. A hálózat kapacitásterhelésének megfelelőbb elosztását a második fejezetben ismertetett forgalmi tervezés, ill. a harmadik fejezetben ismertetett gerinchálózati technológiák teszik lehetővé.

**Nincs** releváns **hálózati szintű mérés** a hálózatban. A hálózat paramétereinek mérésére a fejezetben ismertetett SLA ellenőrző rendszerek alkalmazását javaslom.

A fejezet során meghatároztam a Magyar Honvédség stacioner hálózatában javasolt hálózati technológiákat. Ethernet mikrohullámú eszközöket javaslok használni a hálózat meglévő PDH mikrohullámú eszközei helyére, mert ezek az eszközök:

- csomagkapcsolt forgalomra méretezettek
- nagy sávszélességet biztosítanak (nx100 Mbps-et a jelenlegi nx2Mbit/s-k) helyett
- nem visznek az adatforgalom számára plusz keretelési terhelést.

A javasolt Ethernet mikrohullámú eszközökkel szemben támasztott követelményeket a fejezet során meghatároztam. Az Ethernet mikrohullámú eszközök mellett IP/MPLS útválasztó eszközök használatát javaslom a hálózaton. Ezek a hálózati eszközök egységes, megbízható platformot biztosítanak a szolgáltatások nyújtására. A második generációs IP/MPLS hálózati eszközök 99,99% rendelkezésre állással bírnak. Az eszközök lehetővé teszik MPLS alapú VPN szolgáltatások biztosítását, így a második és harmadik rétegbeli többprotokollós címkekapcsolás feletti virtuális magánhálózatok létrehozását. Ezekkel a virtuális magánhálózatokkal a szervezeti egységeket különíthetjük el, ill. a különböző típusú katonai informatikai alkalmazások számára a különböző szolgáltatásszintet biztosíthatunk. A szolgáltatásszinteket a hálózaton útvonalak, (LSP-k) kijelölésével biztosíthatjuk. Az LSP-ket jelölhetjük ki automatikusan, vagy kiemelt utak esetén kézzel. Az egyes végpontokon olyan hálózati végpontokat alkalmazhatunk amelyek képesek a különböző típusú forgalom biztosítására. A javasolt IP/MPLS hálózati útválasztó eszközökkel szembeni követelményeket meghatároztam a fejezet során.

A fenti topológia kialakítás az alábbi előnyökkel jár:

- Egységes hálózati technológián alapuló gerinchálózatot alakíthatunk ki
- A távközlési hálózatokban általánosan megszokott, második generációs IP/MPLS technológia lehetővé teszi:
  - a hálózat kapacitásainak jobb kihasználtságát
  - a hálózat rendelkezésre állásának nagyságrendekkel való javítását
- A technológia egységes volta miatt:
  - egységes tartalékanyagbázis
  - egységes tudásbázis
  - egységes megoldás
  - NATO szabványban [34] meghatározott megoldás

alakítható ki. Ez a Magyar Honvédség számára költséghatékony üzemelésben és kialakítható szakmai képzésben és egységes tartalékanyag rendszerben nyilvánul meg.

A hálózati szintű IP/MPLS paramétereket részletesen meghatároztam olyan mélységi szinten amely megfelel a hálózat rendszertervének. A jövőben kialakítandó hálózaton ezeket a paraméter beállításokat javaslom figyelembe venni. Felhívtam a figyelmet, hogy a hálózati



szolgáltatások célszerűen biztosíthatóak külső IP/MPLS szolgáltató szolgáltatásainak igénybevételével.

A fejezet során megvizsgáltam azt is , hogy milyen migrációs úton juthatunk el a jelenlegi hálózatról egy modern, második generációs stacioner hálózatig, valamint javasoltam egy migrációs utat a jelenlegi hálózatról egy jövőállóbb hálózat felé. Ennek a migrációs útnak a során fokozatosan, lépcsőzetesen haladva az egyes hálózati rétegeket egy magasabb minőségi szinten újraalkotjuk.

## **IV. A vizsgálatok összegzése és az értekezés végkövetkeztetései**

### **A vizsgálatok összegzése**

Az új évezred, új kihívásokat hozott mind a nemzetközi mind a hazai katonai infokommunikációs rendszerek számára. Ezen legfontosabb kihívások között az áttérést harmadik generációs, információ-központú hadviselésre történő áttérést az egyre szélesebb körben használt katonai információs és kommunikációs rendszerek megfelelő kiszolgálását, ill. az új katonai infokommunikációs koncepciók támogatását emeltem ki.

A polgári célú IP/MPLS hálózat kialakításánál azt tapasztaltam, hogy a nagyrendelkezésű szolgáltatói hálózatokban használt tervezési alapelveket célszerű alkalmazni a stacioner hálózat kialakításakor. A nagy-rendelkezésre állású, szolgáltatói IP/MPLS hálózatok fejlett, minőségi szolgáltatásokra képesek, megvalósítva a kutatási hipotézisemben felvázolt egységes hálózati felület feletti szolgáltatásréteget.

Kutatásaim során kevés alkalommal találkoztam a magyar katonai szakirodalomban a IP/MPLS technológiával foglalkozó cikkel, publikációval, így ezt a területet külföldi szakirodalom tanulmányozása után vizsgáltam. Elemeztem az IP/MPLS hálózat felépítését, szolgáltatásait, az új technológia és az általa nyújtott szolgáltatások jobb kihasználásának lehetőségeit. Bemutattam a nagyrendelkezésre állású IP/MPLS gerinchálózati fejlesztések irányvonalait, valamint ezen eszközök jövőbeni alkalmazásának lehetőségeit.

Az értekezésben a témával összefüggő alapvető fogalmak tisztázását követően, a kutatási rész cél megvalósítása érdekében az IP/MPLS hálózat kialakulását és szolgáltatásait mutattam be. Ráműtöttem arra, hogy egy egységes Ethernet/IP/MPLS alapú technológián egységesített hálózat a következő technológiai előnyökkel jár. Az új évezred, új kihívásokat hozott mind a nemzetközi mind a hazai katonai infokommunikációs rendszerek számára. Ezen legfontosabb kihívások között az áttérést harmadik generációs, információ-központú hadviselésre történő áttérést az egyre szélesebb körben használt katonai információs és kommunikációs rendszerek megfelelő kiszolgálását, ill. az új katonai infokommunikációs koncepciók támogatását emeltem ki a bevezetést követő első fejezetében.

Az első fejezetben arra kerestem a választ, hogy az Összhaderőnemi Doktrína milyen követelményeket, milyen elvárásokat támaszt a szűkebb kutatási területem - Magyar Honvédség híradó és informatikai rendszerével kapcsolatban. Azt is vizsgáltam, hogy a Magyar Honvédség stacioner hálózata mennyire felel meg ezeknek a követelményeknek, és mennyiben tartalmazza a választ azon kihívásokra, amelyet az első fejezetben megfogalmaztam.

A fejezetben kiemelttem, hogy az Összhaderőnemi doktrína a Magyar Honvédség híradó és informatikai rendszerét, mint egy harci támogató rendszert fogalmazza meg, és új megközelítés lehetőségét vettem fel a támogató-támogatott viszonyt illetően – mellyel

részletesebben a következő fejezetben foglalkoztam. Meghatároztam a főbb irányvonalakat (rendszerintegrációs, katonai műszaki, és biztonsági, információvédelmi) amelynek mentén a híradó és informatikai rendszerrel szemben elvárt követelményeket meghatározták. Az Összhaderőnemi Doktrína alapján meghatároztam azon irányelveket, amelyek mentén a híradó és informatikai rendszert ki kell, kellett alakítani. Felhívtam a figyelmet, hogy a doktrína az információs műveleteket is a híradó és informatikai rendszer feladataként jellemzi.

Az Összhaderőnemi Doktrína meghatározta azon irányelveket, amelyek mentén a Magyar Honvédség híradó és informatikai rendszerét tervezni, kivitelezni és üzemeltetni szükséges. Ezen irányelvek lehetővé teszik polgári életben használt nagy rendelkezésre állású hálózatok tervezéséhez, kivitelezéséhez és üzemeltetéséhez használt módszerek és eszközök használatát, amennyiben a katonai alkalmazásból adódó speciális követelményeket figyelembe vesszük.

A fejezetben kiemeltem, hogy az Összhaderőnemi Doktrína a Magyar Honvédség híradó és informatikai rendszerét, mint egy harci támogató rendszert fogalmazza meg, és új megközelítés lehetőségét vetettem fel a támogató-támogatott viszonyt illetően – mellyel részletesebben a következő fejezetben foglalkoztam. Meghatároztam a főbb irányvonalakat (rendszerintegrációs, katonai műszaki, és biztonsági, információvédelmi) irányvonalakat amelynek mentén a híradó és informatikai rendszerrel szemben elvárt követelményeket meghatározták. Az Összhaderőnemi Doktrína alapján meghatároztam azon irányelveket, amelyek mentén a híradó és informatikai rendszert ki kell, kellett alakítani. Felhívtam a figyelmet, hogy a doktrína az információs műveleteket is a híradó és informatikai rendszer feladataként jellemzi.

A fejezeti további része az aktuális fejlesztési tervvel foglalkozik, amely pusztán irányvonalak meghatározását tartalmazza, semmilyen rendszerfejlesztést nem tartalmaz, amit komoly problémának gondolok, ill. definiálja a hírendszer, a híradó és informatikai rendszert, valamint az ezzel szemben elvárt követelményeket határozom meg a szakirodalom alapján. A fejezet második alfejezete, a Magyar Honvédség híradó és informatikai rendszerének sajátosságaival foglalkozik, elemzi a kihívások, elvárások tükrében, feltárja a problémákat. Problémaként jelöltem meg, a Magyar Honvédség híradó és informatikai rendszere nem egységes egész, hogy hiányzik a szolgáltatásalapú megközelítés (ill. több ezzel összefüggő problémát) ill. hiányoznak a módszerek kiemeltem, hogy ezen módszerek hiánya hátráltatja a tervezési munkát – amely költségvonzattal is jár. A fejezet utolsó alfejezetében megoldási javaslatot, migrációs utat vetíték elő problémák orvoslására.

Az első fejezetben meghatároztam a jelenlegi stacioner hálózat felépítését, sajátosságait valamint megfogalmazom az állandó hírendszer strukturális és szolgáltatási hibáit, azt hogy inhomogén hálózati elemekből és technológiákból épül fel, a hálózati erőforrások nincsenek megfelelően kihasználva, az adatátviteli sebességek alacsony voltát, ill. egyes LAN-ok elszigeteltségét, szolgáltatásminőségi és védelmi problémákat, ill. a hálózati szintű mérés hiányát. A harmadik fejezetben részletes javaslatot teszek arra, hogy az egyes hibákat hogyan lehet, hogy IP/MPLS hálózattal kiküszöbölni.

A fejezet további részében fejlesztési irányvonalat javaslok, amelyet több lépcsőre bontok. Az egyes lépcsők célja:

1. az elszigeteltség megszüntetése, egységes hálózat kialakítása
2. kapacitásproblémák megoldása
3. Hálózat egységes QoS képessé tétele, hívásirányítás IP alapúvá tétele, fokozatosan a VoIP elterjesztése
4. Az MPLS széleskörű bevezetésével a rendelkezésreállítás, kihasználtság valamint szolgáltatás paramétereinek javítása

A második fejezetben arra kerestem a választ, hogy az a katonai informatikai alkalmazások milyen elvárásokat támasztanak a Magyar Honvédség híradó és informatikai rendszerével kapcsolatban, ill. mennyire felel meg, tartalmazza a választ azon kihívásokra, amelyet az első fejezetben megfogalmaztam. Itt kiemeltem három forgalmi esetet tekintve vizsgáltam, hogy a hálózat jövőállóságát, ill. a jelenlegi katonai informatikai alkalmazások által generált forgalomnak való megfelelését.

A három forgalmi eset szimulálja a infokommunikációs, ill. katonai informatikai rendszerek három fejlődési szakaszát. Az első szakasz megfelel a második forgalmi esetben leírtaknak, gyakorlatilag a 90-es évek első felének infokommunikációs technológiai színvonalát képviseli a civil szférában, a hangforgalmak átvitelére alkalmas a csomópontok között. Megállapítható, hogy a stacioner hálózat az ilyen jellegű forgalom kielégítésére teljes mértékben alkalmas.

A második fejlődési szakasz, az adathálózatok kialakulásának a szakasza, ez a civil szférában a 1998-2004-es időszak, amikor az első adathálózatok megjelentek, és az IP szélesebb teret nyert. Ezt az időszakot vegyes hang és adatforgalmú alkalmazások jelzik, és központosított jelleg. A fejezetben megállapítom, hogy a hálózat az ilyen jellegű forgalmak kielégítésére korlátozásokkal alkalmas.

A harmadik fejlődési szakasz, a nagy sávszélességű adathálózatok kialakulásának szakasza. Ez a szakasz az erősen elosztott, és hálózati alkalmazások széleskörű elterjedése jellemzi, a civil szférában ez kb. 2003-2004-től folyamatosan történik meg. Megjelennek a valósídejű képátviteli forgalmak, az üzenetküldő rendszerek, a forgalom pedig ma már kizárólag adat, amelynek a jellege lehet valósídejű hang vagy egyéb adat. A fenti fejezetben megállapítom, hogy a stacioner hálózat az ilyen jellegű forgalmak kielégítésére alkalmatlan, nem rendelkezik a megfelelő technológiai és kapacitási viszonyokkal.

Az is egyértelműen megállapítható, hogy miután a katonai informatikai alkalmazások használata a Magyar Honvédség alapvető érdeke, ezért a stacioner hálózat fejlesztése szükséges.

A harmadik fejezetben az állandó/stacioner jellegű híradó és informatikai rendszerrel javasolt kiépítésével foglalkozik, a fent említett fejlesztéssel foglalkozik. A fejezet során meghatároztam a Magyar Honvédség stacioner hálózatában javasolt hálózati technológiákat. Ethernet mikrohullámú eszközöket javaslok használni a hálózat meglévő PDH mikrohullámú eszközei helyére, mert ezek az eszközök:

- csomagkapcsolt forgalomra méretezettek
- nagy sávszélességet biztosítanak (nx100 Mbps-et a jelenlegi nx2Mbit/s-k) helyett
- nem visznek az adatforgalom számára plusz keretelési terhelést.

A javasolt Ethernet mikrohullámú eszközökkel szemben támasztott követelményeket a fejezet során meghatároztam. Az Ethernet mikrohullámú eszközök mellett IP/MPLS útválasztó eszközök használatát javaslom a hálózaton. Ezek a hálózati eszközök egységes, megbízható platformot biztosítanak a szolgáltatások nyújtására. A második generációs IP/MPLS hálózati eszközök 99,99% rendelkezésre állással bírnak. Az eszközök lehetővé teszik MPLS alapú VPN szolgáltatások biztosítását, így a második és harmadik rétegbeli többprotokollos címkekapcsolás feletti virtuális magánhálózatok létrehozását. Ezekkel a virtuális magánhálózatokkal a szervezeti egységeket különíthetjük el, ill. a különböző típusú katonai informatikai alkalmazások számára a különböző szolgáltatásszintet biztosíthatunk. A szolgáltatásszinteket a hálózaton útvonalak, (LSP-k) kijelölésével biztosíthatjuk. Az LSP-eket jelölhetjük ki automatikusan, vagy kiemelt utak esetén kézzel. Az egyes végpontokon olyan hálózati végpontokat alkalmazhatunk amelyek képesek a különböző típusú forgalom biztosítására. A javasolt IP/MPLS hálózati útválasztó eszközökkel szembeni követelményeket meghatároztam a fejezet során.

A hálózati szintű IP/MPLS paramétereket részletesen meghatároztam olyan mélységi szinten amely megfelel a hálózat rendszertervének. A jövőben kialakítandó hálózaton ezeket a paraméter beállításokat javaslom figyelembe venni. Felhívtam a figyelmet, hogy a hálózati szolgáltatások célszerűen biztosíthatóak külső IP/MPLS szolgáltató szolgáltatásainak igénybevételeivel.

A fejezet során megvizsgáltam azt is , hogy milyen migrációs úton juthatunk el a jelenlegi hálózatról egy modern, második generációs stacioner hálózathoz, valamint javaslom egy migrációs utat a jelenlegi hálózatról egy jövőállóbb hálózat felé. Ennek a migrációs útnak a során fokozatosan, lépcsőzetesen haladva az egyes hálózati rétegeket egy magasabb minőségi szinten újraalkotjuk.

## **Összegzett következtetések**

A kutatási céljaim eléréséhez az értekezést három fejezetre tagoltam. Az első fejezetben az Összhaderőnemi Doktrína alapján meghatároztam a követelményeket, valamint a stacioner hálózat jelenlegi kialakítása alapján meghatároztam a stacioner hálózat alkalmazásával szembeni követelményeket. A második fejezetben modelleztem a stacioner hálózat viselkedését három forgalmi modell alkalmazásával, szoftveres úton kialakítottam a hálózat modelljét. Ebben a fejezetben azt vizsgáltam, hogy a Magyar Honvédség stacioner hálózata mennyire felel meg azoknak a sávszélesség követelményeknek, amiket a modern katonai informatikai alkalmazások támasztanak. A követelmények vizsgálatához a fejezet első felében egy mintaalkalmazás, egy katonai háromdimenziós radar sávszélesség igényszámítását végeztem el. Ilyen háromdimenziós katonai radart több telephelyen használnak Magyarországon. A fejezet második felében azt elemzem, hogy három forgalmi esetben a stacioner hálózaton hogyan alakulnak a forgalmi viszonyok.

A fejezetben tudományos módszert alkalmazok arra, hogy:

- az adatkapcsolt hálózaton a kapacitásviszonyok hogyan alakulnak különböző végponti forgalmi eseteket figyelembe véve,
- az adatkapcsolt hálózaton, hogyan modellezhető egy forgalmi helyzet,
- egy hálózati modellen milyen torlódási és túlterhelési problémák jelentkeznek,
- ezek a túlterhelési problémák mit eredményeznek a valós hálózatban,
- a stacioner hálózat hogyan reagál az alkalmazás réteg által megnövelt hálózati forgalomra.

A harmadik fejezetben konkrét javaslatokat dolgoztam ki az új stacioner és informatikai hálózat kialakítására, a technológia meghatározásától a stacioner hálózaton alkalmazandó eszköztípusok, valamint hálózati szintű paraméterek és szolgáltatások meghatározásáig, és elvi ajánlásokat adtam a technológia alkalmazására a Magyar Honvédség stacioner hálózatában. Ebben a fejezetben a fenti problémák megoldására teszek javaslatot. Meghatározom, hogy a stacioner hálózatot milyen technológia alapokra szükséges helyezni, a stacioner hálózat rendszerbeállításai hogyan kell, hogy kinézzenek ezen technológia alapokon ill. hogy erre az ideális hálózatra milyen módon lehetséges a migráció. A fejezetben a Magyar Honvédség stacioner hálózatának javasolt modernizációs útját fogom szerepeltetni, olyan mélységben, amely egy rendszerterv kialakításához szükséges. Az itt szereplő fejezetben a jelenlegi problémákra keresem a választ, és az új technológiák által nyitott lehetőségeket nem szerepeltetem. A kialakítást az elvi hálózati síkokkal fogom kezdeni, majd egy-egy tipikus gerinchálózat telephelyen használt hálózati eszközöket fogom meghatározni. Az én értelmezésemben a klasszikus átviteltechnikai hálózatot és az IP alapú átviteltechnikai hálózatot egységes egészként fogom kezelni, ahol az átviteltechnikai hálózat pont-pont összeköttetéseket biztosítja optikai szálon, hullámhosszokon vagy mikrohullámú összeköttetésen keresztül. A stacioner hálózat kapcsolóelemei pedig IP alapú útválasztó eszközök. A hálózat szolgáltatásrétegét (webszerverek, katonai informatikai alkalmazások, beszédcélú átvitel) nem tekintem a kutatásom tárgyának.

## **Új tudományos eredmények**

Javaslatot adtam a stacioner hálózat kialakításának módjára, matematikai módszerrel elemezve a kapacitásproblémákat a hálózatban. Forgalmi elemzést végeztem a hálózaton, a teljes stacioner hálózat forgalmi viszonyai meghatároztam a múlt, a jelen és a jövő forgalmi eseteinek figyelembe vételével. Meghatároztam a kapacitásproblémák helyeit, és a kapacitásproblémák technológiai okait, eszközszinten határoztam meg egy kialakítandó hálózat képét, a javasolt hálózati eszközökkel szembeni követelményeket, hálózatszinten határoztam meg a gerinchálózati eszközök beállítási paramétereit, hálózatszinten határoztam meg, a javasolt szolgáltatásokat, szimuláltam teszhálózaton a hálózat javasolt megvalósítását.

## Új tudományos eredmények tartom:

1. **A Magyar Honvédség stacioner hálózatában lévő hiányosságok meghatározását és a hibák rendszerezését**, mind technológiai, mind szervezeti, mind hálózati kapacitásviszonyokat figyelembe véve. Annak az egyértelmű megállapítását, hogy **a jelenlegi technológia színvonalon**, az első fejezetben említett okok miatt, **a hálózat nem jövőálló**, és nincs felkészülve a katonai informatikai alkalmazások – így pl. a 3 dimenziós radarképek – adatátvitelére. **A hálózat** egy elavult hálózatfejlesztési koncepciót képvisel, amelynek a **felülvizsgálata szükséges**, A primer kutatási eredmények tartom **a hálózat szolgáltatásalapú megközelítésre történő kialakítását, ennek a technológia oldali kidolgozását**, ahol az egyes réteget (szolgáltatás, hálózat, átviteltechnikai) közötti kapcsolat SLA szerződésekben meghatározott.
2. Primer alkalmazott kutatási eredmények tartom **a stacioner hálózat forgalmi modelljének meghatározását** három forgalmi esetet figyelembe véve. **Primer alkalmazott kutatási eredmények tartom, a hálózat forgalmi modelljének kialakítását, a forgalmi modell reprodukálhatóvá tételét**, ezzel meghatározva az utat ez és más hasonló célú hálózatok részletesebb forgalmi vizsgálatának. **Mind a forgalmi elemzés leírt és alkalmazott módszerét, mind a forgalmi elemzés eredményét primer alkalmazott kutatási eredmények tartom.**
3. **Primer és szekunder kutatási eredmények tartom a Magyar Honvédség jövőbeni stacioner hálózatának a tervét, ill. az elkészített modelljét, a paraméterek, beállítások részletes meghatározását.**
4. **Szekunder kutatási eredmények tartom a polgári célú, országos gerinchálózati szolgáltatói infrastruktúra vizsgálatát, annak lehetséges használhatóságát a Magyar Honvédség stacioner hálózatának kialakítására, ill. a figyelem felhívását a kritikus információs infrastruktúra védelmének fontosságára.**

## Javaslat az értekezés hasznosítására

- A Magyar Honvédség stacioner hálózatának technikai kialakítása során a fejlesztési stratégia kialakításakor ajánlott alapul venni;
- A Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi és Katonai Műszaki Doktori Iskolákban, valamint az egyetemi alap és kiegészítő képzésekben a szakirányú tárgyak oktatása során ajánlott irodalomként felhasználni;
- A MH stacioner hálózatának további vizsgálatait során tanulmányok, pályázatok és egyetemi jegyzetek elkészítéséhez felhasználni.
- A MH stacioner hálózatának forgalmi tervezésekor, kapacitásviszonyok újragondolásakor a használt módszereket javasolt felhasználni

- A MH stacioner hálózatának fejlesztésekor a javasolt kialakítás szerint a fejlesztéskor figyelembe venni.

Budapest, 2010. május 30.

(Bleier Attila Károly)



## V. Jegyzékek

### V.1 Ábrajegyzék

I-1. ÁBRA FIKTÍV HÁLÓZATI ÁBRA A 3D RADARKÉPEK TOVÁBBÍTÁSÁRA .....	20
II-1. ÁBRA FORGALMI HÁLÓZATI VISZONYOK 1 MBIT/S MELLETT .....	35
II-2. ÁBRA - A HÁLÓZAT FORGALMI VISZONYAI 128 KBIT/S ÁTLAGOS FORGALOM MELLETT .....	39
II-3. ÁBRA - A HÁLÓZAT FORGALMI VISZONYAI ÁTLAGOS 10 MBIT/S FORGALOM MELLETT .....	41
III-1. ÁBRA AZ EDGE ÚTVÁLASZTÓK ÉS CORE ÚTVÁLASZTÓK KÖZTI REDUNDANCIA.....	48
III-2. ÁBRA - A STACIONER HÁLÓZAT JAVASOLT TOPOLOGIÁJA.....	50
III-3. ÁBRA - SPLIT ETHERNET MIKRO, [ 26].....	53
III-4. ÁBRA BÁNKÚT – NAGYHÁRS VISZONYLAT .....	54
III-5. ÁBRA BÁNKÚT-NAGYHÁRS VISZONYLAT TEREPMETSZETE .....	55
III-6. ÁBRA SÁVSZÉLESSÉG ÉS RENDELKEZÉSREÁLLÁSI VISZONYOK .....	55
III-7. ÁBRA A KAPCSOLAT PARAMÉTEREI .....	55
III-8. ÁBRA KLÍMAVISZONYOK ÁLTAL OKOZOTT VESZTESÉGEK .....	56
III-9. ÁBRA ALKATRÉSZLISTA .....	56
III-10. ÁBRA FRESNEL ZÓNA 5.9 GHZ ESETÉN .....	57
III-11. ÁBRA 5.9 GHZ RENDELKEZÉSREÁLLÁSA ÉS SÁVSZÉLESSÉGVISZONYAI.....	57
III-12. ÁBRA AZ 5.9 GHZ-ES KAPCSOLAT ÖSSZEGZŐ TÁBLÁZATA .....	57
III-13. ÁBRA AZ 5.9 GHZ-ES KAPCSOLAT ALKATRÉSZLISTÁJA.....	58
III-14. ÁBRA – 2 U MAGAS VÉGPONTI ÚTVÁLASZTÓ[28].....	60
III-15. ÁBRA - 1 U MAGAS VÉGPONTI ÚTVÁLASZTÓ[29].....	60
III-16. ÁBRA - NAGYKAPCSOLÁSI SEBESSÉGŰ 2U MAGAS ÚTVÁLASZTÓ[30] .....	61
III-17. ÁBRA - NAGY RENDELKEZÉSRE ÁLLÁSÚ MŰKÖDÉS [31] .....	62
III-18. ÁBRA – FORGALMAK ÉS SZOLGÁLTATÁSOK ÖSSZERENDELÉSE.....	70
III-19. ÁBRA A MAGYAR HONVÉDSÉG ÁLLANDÓ HÍRRENDSZERÉNEK VÁZLATA.....	75
III-20. ÁBRA MAGYAR HONVÉDSÉG STACIONER HÁLÓZATI RÉTEGEI.....	76
III-21. ÁBRA VÉGPONT-VÉGPONT KÖZTI SZOLGÁLTATÁSSZINT MÉRÉSE .....	78

## V.2 Táblázatjegyzék

II-1. TÁBLÁZAT 3D RADAR PARAMÉTEREK .....	30
II-2. TÁBLÁZAT KÉPPONTOK SZÁMA 1 DIMENZIÓ .....	30
II-3. TÁBLÁZAT KÉPPONTOK SZÁMA 3D-BEN.....	30
II-4. TÁBLÁZAT TÖMÖRÍTETT ADATMENNYISÉG.....	30
II-5. TÁBLÁZAT SÁVSZÉLESSÉGIGÉNY .....	31
II-6. TÁBLÁZAT – 3D RADARÁLLOMÁSOK RENDELKEZÉSRE ÁLLÓ SÁVSZÉLESSÉGEI.....	31
II-7. TÁBLÁZAT – FIKTÍV HÁLÓZATI TOPOLOGIA, CSOMÓPONTOK TÁBLÁZATA.....	33
II-8. TÁBLÁZAT – ÉLTELÍTTETTSÉG 1 MBIT/S FORGALOM MELLETT 1 MBIT/S.....	38
II-9. TÁBLÁZAT - LEGTÖBB SÁVSZÉLESSÉGET FOGLALÓ UTAK – 1MBIT/S.....	38
II-10. TÁBLÁZAT – LEGTELÍTTETTEBB ÉLEK 128 KBIT/S.....	40
II-11. TÁBLÁZAT – LEGTELÍTTETEBB UTAK 128 KBIT/S.....	40
II-12. TÁBLÁZAT – LEGTELÍTTETTEBB ÉLEK – 10 MBIT/S .....	42
II-13. TÁBLÁZAT – LEGTELÍTTETTEBB UTAK, 10 MBIT/S ESETÉN .....	43
II-14. TÁBLÁZAT – FORGALMI ÖSSZEHASONLÍTÓ PARAMÉTEREK .....	44
III-1. TÁBLÁZAT – CSOMÓPONTOK BESOROLÁSA .....	49
III-2. TÁBLÁZAT ÉLVISZONYLATOK TÁBLÁZATA .....	51
III-3. TÁBLÁZAT – ETHERNET MIKROHULLÁMÚ ESZKÖZ TULAJDONSÁGAI .....	53
III-4. TÁBLÁZAT – ÚTVÁLASZTÓK KÖRNYEZETI PARAMÉTEREI.....	61
III-5. TÁBLÁZAT SZOLGÁLTATÁSMINŐSÉGI PARAMÉTEREK .....	67
III-6. TÁBLÁZAT - FORGALMI OSZTÁLYBA SOROLÁS.....	68
III-7. TÁBLÁZAT FORGALMI OSZTÁLYOK MINŐSÉGPARAMÉTEREI.....	68
V-1. TÁBLÁZAT - RÖVIDÍTÉSJEJYZÉK.....	93

### V.3 Rövidítések jegyzéke

<b>Rövidítés/Acronym</b>	<b>Angol/English</b>	<b>Magyar/Hungarian</b>
IU, 2U stb.	Unit	U - hálózati technológiában használt hosszúságmérték, 44mm-nek felel meg.
3D	3 dimension	3 dimenziós
AARMS	Academic and Applied Research in Military Science	Academic and Applied Research in Military Science
ADLER	Artillerie-, Daten-, Lage- und Einsatz-Rechner	Tüzérségi, adat, helyzet és bevetési számítógép hálózat
ADPCM	Adaptive Pulse Code Modulation	modulációs mód
APS	Automatic Protection Switching -	Automata védelmi kapcsolás
ARP	Address Resolution Protocol	Címfeloldási protokoll
ATM	Asynchronous Transfer Mode	Aszinkron átviteli mód
BER	Bit Error Rate	Bíthibaarány
BFD	Bidirectional Forwarding Detection	A csomagtovábbító motorok közti hibákat detektáló protokoll
BGP	Border Gateway Protocol	Útválasztó protokoll
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance	vezetés-irányítás, híradás, számítógép, hírszerzés, megfigyelés, felderítés
CPU	Central Processing Unit	Központi proceszor
CSPF	Constrained Shortest Path First	Korlátos legrövidebb út algoritmus
DAMOTE	Decentralized Agent for Mpls Online Traffic Engineering	Módosított gráfelméleti algoritmus, kapacitások jobb kihasználtságára
DiffServ	Differentiated Services	IETF QoS architektúra
DoS	Denial Of Service	Szolgáltatás-megtagadás
DSCP	Differentiated Services Code Point	Megkülönböztetett szolgáltatási kódpont
E1	ISDN Primary Rate Physical Interface Standard	2 Mbit/s-es jel időmultiplex rendszerekben
E-BGP	Exterior Border Gateway Protocol	Autonóm rendszerek közötti útválasztó protokoll
ETSI	European Telecommunication Standard Institute	Szabványügyi szervezet
EU	European Union	Európai Unió
EXP	MPLS Experimental QoS bitek	experimental, jelenleg QoS prioritás jelzésére
FR, FRR	Fast reroute	Gyors útválasztás
GCCS	Global Command and Control System	Globális vezetési és irányítási rendszer
HEROS	Heeres Führungsinformation System (für die rechnerunterstützte) Operationsführung in Staeben	Csapatvezetési információs rendszer, hadműveleti vezetés a törzsekben
HMAC-MD5	Hash-based Message Authentication Code - Message-Digest algorithm 5	Titkosítási algoritmus
IARCCIS	Interim ACE Rapid Reaction Corps Information System	ACE Gyorsreagálású hadtest átmeneti informatikai rendszere
IBGP	Interior Border Gateway Protocol	Útválasztó protokoll
ICMP	Internet Control Message Protocol	az UDP-hez hasonlóan) datagram-orientált kommunikációs protokoll
IEEE	Institute of Electrical and Electronics Engineers, Inc	nemzetközi villamosmérnöki szabványügyi szervezet

<b>Rövidítés/Acronym</b>	<b>Angol/English</b>	<b>Magyar/Hungarian</b>
IETF	Internet Engineering Task Force	Internet működésében részt vevő szabványok meghatározó szabványügyi szervezete
IGP	Interior Gateway Protokoll	autonóm rendszeren belüli útválasztó protokoll
IP	Internet Protocol (usually version 4)	Internet Protokoll (általában 4-es verzió)
IPSec	IP Security	
IPv4	Internet Protocol version 4	Internet Protocol 4-es verzió
IPv6	Internet Protocol version 6	Internet Protokoll 6.-s verzió
IS-IS	Intermediate System to Intermediate System	Útválasztó protokoll
IT	Information technológia	Információtechnológia
ITU	International Telecommunication Union	Nemzetközi távközlési szabványügyi szervezet
JOPEs	Joint Operation Planning and Execution System	Összhaderőnemi hadművelet-tervező és végrehajtó rendszer
KPI	Key Performance Indicator	Kulcsfontosságú teljesítményjelzők
L2	Layer 2	Második réteg
L2VPN	Layer 2 Virtual Private Network	Layer 2 virtuál magán hálózati szolgáltatás
L3	Layer 3	harmadik réteg
LAN	Local Area Network	Helyi hálózat
LDP	Label Distribution Protocol	Címke elosztási protokoll
LI	Lawful Interception	Törvényes lehallgatás
LSP	Label Switched Path	Címkekapcsolt útvonalak
MP-BGP	Multiprotocol Border Gateway Protocol	Útválasztó protokoll
MPLS	Multiprotocol Label Switching	Többprotokollos címkekapcsolás
MTBF	Mean Time Between Failure	Hibaesetek közötti eltelt átlagos idő, az alkatrészek rendelkezésreállítását leíró paraméter
NATO	North Atlantic Treaty Organization	Nemzetközi politika-katonai szövetség
NMCS	National Military Command System	Nemzeti katonai vezetési rendszer
O&M	Operation and Maintenance	Üzemeltetés és karbantartás
OSPF	Open Shortest Path First	útválasztó protokoll
OTP	One Time Password	Jelszó egy alkalomra
P	Provider	Szolgáltató
PCM	Pulse Code Modulation	modulációs mód
PDH	Plesiochronouse Digital Hierarchy	Pleziokron digitális hierarchia
PE	Provider Edge	Szolgáltatói hálózat pereme
POS, PoS	PPPOverSDH, Packet over Sonet	Csomagkapcsolt adatok továbbítására szolgáló interfész TDM hálózatok felett
QoS	Quality of Service	Szolgáltatásminőség
Radius	Remote Authentication Dial In User Service	Hálózati autentikációs protokoll
RIP	Routing Information Protocol	Útválasztási információs protokoll
RJ45	registered jack 45	Rézalapú Ethernet csatlakozó szabvány
RPF	Reverse Path Forwarding	Fordított Forwarding

<b>Rövidítés/Acronym</b>	<b>Angol/English</b>	<b>Magyar/Hungarian</b>
RR	Route-reflector	Útvonal tükröző
RSVP	Resource Reservation Protocol	Erőforrás foglalási protokoll
RSVP-TE	Resource Reservation Protocol with Traffic Engineering extensions	Erőforrás foglalási protokoll forgalom irányítással
RTP	Real-time-Protocol	Valós idejű protokoll
RTT	Round trip time	Körülfordulási idő
SCP	Secure Copy	Titkos másolat
SDH	Synchronous Digital Hierarchy	Szinkron digitális hierarchia
SFP	Small Form Pluggable	optikai interfésszabvány Gigabit Ethernet csatlókhhoz
SFP	10 Gigabit Small Form Factor Pluggable	Optikai interfésszabvány 10 Gigabit Ethernet csatlókhhoz
SGEA	Système de Guerre Électronique de l'Avant	Elektronikai hadviselési rendszer
SLA	Service Level Agreement	Szolgáltatási szint szerződés
SNMP	Simple Network Management Protocol	Egyszerű hálózat menedzsment protokoll
SPF	Shortest path first	Legrövidebb út algoritmus
SPF	Shortest Path First	Legrövidebb út algoritmus
SSH	Secure Shell	Egy szabványcsalád, és egyben egy protokoll is, amit egy helyi és egy távoli számítógép közötti biztonságos csatorna kiépítésére fejlesztettek ki.
STANAG	Standardization Agreement	NATO szabványok
STRIDA	Système de Traitement et de Représentation des Informations de Défense Aérienne	Légvédelmi információk kezelésének és megjelenítésének rendszere
Tacacs+	Terminal Access Controller Access-Control System Plus	Hálózati autentikációs protokoll
TCP	Transmission Controll Protocol	Átvitel-vezérlési Protokoll
TCP SYN	TCP message	TCP üzenet
TDM	Time Division Multiplexing	Időmultiplex
VLAN	Virtual LAN	Virtuális hálózat
VoIP	Voice over IP	Hang IP forgalom felett
VPLS	Virtual Private LAN Service	Virtuális privát LAN szolgáltatás
VPN	Virtual private network	Virtuális magánhálózat
WWMCCS	World Wide Military Command and Control System	Világméretű katonai vezetési rendszer
ZMNE	Zrínyi Miklós Defense University	Zrínyi Miklós Nemzetvédelmi Egyetem

V-1. TÁBLÁZAT - RÖVIDÍTÉSJEJYZÉK

## VI. Irodalomjegyzékek

### VI.1 Hivatkozott Irodalom

1. **Károly, dr. Fekete.** A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei. *Phd. értekezés.* Budapest: ZMNE, 2003.
2. **Magyar Honvédség.** *A Magyar Honvédség Összhaderőnemi Doktrínája.*
3. **Honvédelmi Minisztérium.** Honvédségi Szemle. [Online] [Cited: 04. 14., 2010.] [http://www.hm.gov.hu/hirek/kiadvanyok/uj\\_honvedsesegi\\_szemle/nato-csucstalalkozok](http://www.hm.gov.hu/hirek/kiadvanyok/uj_honvedsesegi_szemle/nato-csucstalalkozok).
4. **National Intelligence Council.** *Global Trends 2015: A Dialogue About the Future With Non-Governmental Experts.* Washington D.C. : National Intelligence Council, 2000.
5. **The United States Commission on National Security/21st Century.** *NEW WORLD COMING: American Security in the 21 st century.* U.S. : U.S., 1999.
6. Belföldi hírek. *fn.hu.* [Online] 05 2010.05.16, 2010. [Cited: 05 18, 2010.] [http://www.fn.hu/belfold/20100516/katasztrofalis\\_helyzet\\_miskolcon/](http://www.fn.hu/belfold/20100516/katasztrofalis_helyzet_miskolcon/).
7. Hurricane Katrina. *Wikipedia.* [Online] 05 2010. [Cited: 05 29, 2010.] [http://en.wikipedia.org/wiki/Hurricane\\_Katrina](http://en.wikipedia.org/wiki/Hurricane_Katrina).
8. Hatalmas olajfolt a Mexikói-öbölben. *HVG.HU.* [Online] 05 2010. [Cited: 05 29, 2010.] [http://hvg.hu/vilag/20100427\\_olajfolt\\_levegobol](http://hvg.hu/vilag/20100427_olajfolt_levegobol).
9. **Sándor, Dr. Munk.** *Katonai informatika a XXI. század elején.* Budapest : Zrínyi kiadó, 2007. ISBN: 978 963 327 4194.
10. **Sándor, Munk.** *Interoperability infrastructure in military infocommunication systems.* Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1 .
11. **Pándi Balázs, Pándi Erik.** *A jövő várható háborúinak és katonai konfliktusainak a hatása a hazai tábori kommunikációs rendszer megújításának folyamatára.* Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-11-1.
12. **Maros, Dóra - Mészáros, Árpád.** *A magyar távközlési rendszer anomáliái a londoni terrortámadás tükrében, Kommunikáció 2005.* Budapest: ZMNE, 2005. ISBN 963 7060 11 1.
13. **Maros, Dóra.** *Távközlési hálózatok működésének nemzetközi és hazai szabályozási kérdései veszélyes katasztrófhelyzetekben,* Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, doktori értekezés
14. **Csákány Éva, Konkoly Lászlóné, Jakab Tivadar, Zsóka Zoltán, Lakatos Zsolt.** *A T-Com IP maghálózat megbízhatósági analízisének módszere.* p. 57-79, Budapest : Magyar Telekom Nyrt. , 2006, Vol. PKI Közlemények 50. HU - ISSN 1216-3961.

15. **Magyarné Kucsera, Erika - Dr. Sándor , Miklós.** *A zártcélú hálózat forgalmi optimalizálásának problémái.* 2005/3 p.104-110, Budapest : ZMNE, 2005, Vol. Kard és Toll. ISSN 1587-558X.
16. **Nemzetvédelmi Egyetem,** *A Magyar Honvédség stacioner hálózata.* 2010.
17. **BWI.** [Online] BWI. [Cited: 03 23, 2010.] <http://www.bwi-it.de/>.
18. **Université de Liège.** TOTEM project - A TOolbox of Traffic Engineering Methods. *Research unit in Networking - Université de Liège.* [Online] 2005. [Cited: 02 28, 2009.] <http://www.run.montefiore.ulg.ac.be/Projects/Presentation/index.php?project=TOTEM>.
19. **Balon, S., et al.** *Traffic Engineering an Operational Network with the TOTEM Toolbox.* 51 - 61, Geneve : IEEE, 2007, Vol. 4/1 . ISSN: 1932-4537.
20. **European Parliament and Council.** Directive on universal service and access rights. *EURACTIV.* [Online] 03 2002.03.07, 2002. [Cited: 09. 12, 2009.] [http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l\\_108/l\\_10820020424en00510077.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/oj/2002/l_108/l_10820020424en00510077.pdf).
21. **Cisco Systems Inc.** Designing Large Scale IP Networks. *Cisco Systems Inc.* [Online] Cisco. [Cited: 05 28, 2010.]
22. **Juniper Networks.** Juniper Networks. *Juniper Networks.* [Online] 2010. [Cited: 05 28, 2010.] <http://www.juniper.net/us/en/>.
23. **SAF Tehnika.** SAF. *SAF.* [Online] [Cited: 05 28, 2010.] <https://www.saftehnika.com/>.
24. **Cisco Systems Inc.** Cisco Systems Inc. *Cisco Systems Inc.* [Online] [Cited: 05 28, 2010.] <http://www.cisco.com/>.
25. **Motorola Inc.** *Motorola.* [Online] [Cited: 05 28, 2010.] <http://www.motorola.com/consumers/v/index.jsp?vgnextoid=3540f5de485af110VgnVCM100008806b00aRCRD>.
26. **SAF Tehnika JSC.** CFIP sorozatú Ethernet mikrohullámú eszközök. *SAF Tehnika.* [Online] [Cited: 05 29, 2010.] <https://www.saftehnika.com/products/cfip-product-line/cfip-phoenix-tdm-ip->.
27. **Motorola.** Motorola Network planning tools. *Motorola Network planner.* [Online] [Cited: 04 22, 2010.] <http://www.motorola.com/Business/US-EN/Business+Product+and+Services/Wireless+Broadband+Networks/Point-to-Point+Bridges/Network+Planning+Tools>.
28. **Juniper Networks.** J 2350-es útválasztó. *Juniper Networks.* [Online] [Cited: 05 29, 2010.] <http://www.juniper.net/us/en/products-services/routing/j-series/j2350/>.
29. **Juniper Networks.** J2320-as útválasztó. *Juniper Networks.* [Online] [Cited: 05 29, 2010.] <http://www.juniper.net/us/en/products-services/routing/j-series/j2320/>.

30. **Juniper Networks Inc.** MX 80-as útválasztó adatlapja. *Juniper Networks Inc.* [Online] [Cited: 05 29, 2010.] <http://www.juniper.net/us/en/products-services/routing/mx-series/mx80/#specifications>.
31. **Juniper Networks.** J sorozatú útválasztók adatlapja. *Juniper Networks Incorporated.* [Online] [Cited: 05 29, 2010.] <http://www.juniper.net/us/en/local/pdf/datasheets/1000206-en.pdf>.
32. **Czinkóczy András, Konkoly Lászlóné, Liptákné Csákány Éva, Jakab Tivadar, Lakatos Zsolt, Szegedi Péter.** *A MATÁV IP maghálózatának költséghatékonyságfejlesztése a jövő szolgáltatásainak tükrében.* p. 19-55, Budapest : MATÁV, 2004, Vol. PKI Közlemények 48. HU ISSN: 1216-3961.
33. **NXTCOMMNEWS.** Assuring IP Service Quality is Job One. *NXTCOMMNEWS.* [Online] [Cited: 05 30, 2010.] <http://nxtcommnews.com/ipassurance/news08/assuring-ip-service-0529/>.
34. **North Atlantic Treaty Organization.** NATO C3 Technical Architecture. *Allied Data Procedure 34.*
35. **I. T. Pereszepkin.** *HÍRADÁS A NAGY HONVÉDŐ HÁBURÚBAN,* Zrínyi katonai kiadó, Bp. 1979
36. *Objective voice quality measurement.* [Online]. [Cited: 13 10., 2010.] <http://www.ims.uni-stuttgart.de/phonetik/EGG/page13.htm>.
37. *QoS Measurement Methods and Tools,* [Online]. [Cited: 13 10., 2010.], <http://ew.thales.no/common/VTT/T.4.1.%20QoS%20Measurement%20Methods%20and%20Tools.pdf>
38. **Damien Rame,** *Ethernet SLA Monitoring: Map out the health of your network.* [Online]. [Cited: 13 10., 2010.] [http://nxtcommnews.com/contributed/articles/ethernet\\_sla\\_monitoring\\_051407/](http://nxtcommnews.com/contributed/articles/ethernet_sla_monitoring_051407/)



## VI.2 Felhasznált irodalom

1. **Károly, dr. Fekete.** A Magyar Honvédség állandó telepítésű kommunikációs rendszere továbbfejlesztésének technikai lehetőségei. *Phd. értekezés.* Budapest: ZMNE, 2003.
2. **Magyar Honvédség.** *A Magyar Honvédség Összhaderőnemi Doktrínája.*
3. **Sándor, Dr. Munk.** *Katonai informatika a XXI. század elején.* Budapest: Zrínyi kiadó, 2007. ISBN: 978 963 327 4194.
4. **Sándor, Munk.** *Interoperability infrastructure in military infocommunication systems.* Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1.
5. **Pándi Balázs, Pándi Erik.** *A jövő várható háborúinak és katonai konfliktusainak a hatása a hazai tábori kommunikációs rendszer megújításának folyamatára.* Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-11-1.
6. **Maros, Dóra - Mészáros, Árpád.** *A magyar távközlési rendszer anomáliái a londoni terrortámadás tükrében, Kommunikáció 2005.* Budapest: ZMNE, 2005. ISBN 963 7060 11 1.
7. **Maros, Dóra.** *Távközlési hálózatok működésének nemzetközi és hazai szabályozási kérdései veszélyes katasztrófavhelyzetekben,* Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, doktori értekezés
8. **Csákány Éva, Konkoly Lászlóné, Jakab Tivadar, Zsóka Zoltán, Lakatos Zsolt.** *A T-Com IP maghálózat megbízhatósági analízisének módszere.* p. 57-79, Budapest : Magyar Telekom Nyrt. , 2006, Vol. PKI Közlemények 50. HU - ISSN 1216-3961.
9. **Magyarné Kucsera, Erika - Dr. Sándor, Miklós.** *A zártcélú hálózat forgalmi optimalizálásának problémái.* 2005/3 p.104-110, Budapest : ZMNE, 2005, Vol. Kard és Toll. ISSN 1587-558X.
10. BWI. [Online] BWI. [Cited: 03 23, 2010.] <http://www.bwi-it.de/>.
11. **Université de Liège.** TOTEM project - A TOolbox of Traffic Engineering Methods. *Research unit in Networking - Université de Liège.* [Online] 2005. [Cited: 02 28, 2009.] <http://www.run.montefiore.ulg.ac.be/Projects/Presentation/index.php?project=TOTEM>.
12. . **Balon, S., et al.** *Traffic Engineering an Operational Network with the TOTEM Toolbox* 51 - 61, Geneve : IEEE, 2007, Vol. 4/1 . ISSN: 1932-4537.
13. **Czinkóczy András, Konkoly Lászlóné, Liptákné Csákány Éva, Jakab Tivadar, Lakatos Zsolt, Szegedi Péter.** *A MATÁV IP maghálózatának költséghatékony fejlesztése a jövő szolgáltatásainak tükrében.* p. 19-55, Budapest : MATÁV, 2004, Vol. PKI Közlemények 48. HU ISSN: 1216-3961.
14. **Tibor, Farkas.** *Informatik Network Management in the Hungarian Defence Forces.* p. 152-160, Budapest : ZMNE, 2007, Vol. Communications 2007. ISBN: 978-963-7060-31-1.

15. **Tanács Ferenc, Hámori András, Balogh Attila.** *Ethernet alapú szélessávú szolgáltatások a Matáv IP hálózatában.* p. 55-81, Budapest : MATÁV, 2004, Vol. PKI Közlemények 48. HU ISSN: 1216-3961.
16. **Suter, Manuel.** A Generic National Framework For Critical Information Infrastructure Protection (CIIP). *ITU.* [Online] 2007. [Cited: 06 25, 2009.] <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf>.
17. **Selin Cerav Erbas, Rudolf Mathar.** *An Offline Traffic Engineering Model for MPLS Networks.* 166-174, New York : IEEE, 2002, Vol. Communications. ISSN 0163-6804.
18. **Précsényi Zoltán, Solymosi József.** *Towards EU-NATO cooperation in the protection of European critical infrastructure.* Hadmérnök : ZMNE, 2007., Vol. II./2. ISSN 1788-1919.
19. **Pándi Balázs, Pándi Erik.** *Az Észak-Atlanti Szervezetet kiszolgáló kommunikációs rendszerek jellemzői.* Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-57-1.
20. **Ossama Younis, Latha Kant, Kirk Chang and Kenneth Young, Telcordia Technologies, Inc., Charles Graff, U.S. Army CERDEC.** *Cognitive MANET Design for Mission-Critical Networks.* 64-72., New York : IEEE, 2009, Vols. IEEE Communications, Vol. 47. No. 10. ISSN 0163-6804.
21. **Lucek, Ina Minei - Julian.** *MPLS-Enabled Applications - Emerging Developments and New Technologies.* The Atrium, Southern Gate, Chichester : John Wiley & Sons, Ltd., 2005. ISBN 0-470-01453-9.
22. **Liège, Université de.** Overview. *E-next - Totem Project - Toolbox for Traffic Engineering Methods.* [Online] [Cited: 02 28, 2009.] <http://totem.run.montefiore.ulg.ac.be/>.
23. **Konkoly Lászlóné, Rózsa István Gergő, Csákány Éva.** *IP forgalom mérés eszközei és felhasználása a hálózat méretezésében.* p. 57-83, Budapest : Matáv, 2003, Vol. PKI Közlemények 47. HU- ISSN 1216-3961.
24. **Károly, Fekete.** *Towards a new generation of wlan in military communications.* Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1.
25. **Károly, Fekete.** *The secure based wireless IP protocols with regard to closed networks.* Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1.
26. **Károly, Fekete.** *The Multi-National Missions and the Network Enabled Capability.* Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1.
27. **Jordán Tibor, Recski András, Szeszlér Dávid.** *Rendszeroptimalizálás.* Budapest : Typotex Kiadó, 2004. ISBN 963-9548-39-1.
28. **Hiroyuki Takahashi, Akihiko Hirata, Naoya Kukutsu, Yuichi Kado, Toshihiko Kosugi, and Koichi Murata.** Compact, Low-power, 120-GHz-band Wireless Link for 10-Gbit/s Data Transmission. *NTT Technical Review.* [Online] 2009. [Cited: 06 23, 2009.] <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200903sf2.html>.

29. **Erika, Magyarné Kucsera.** *New possibilities of wireless trends in the area of mobile infocommunication and management.* p. 166- 174, Budapest : ZMNE, 2007, Vol. Communications 2007. ISBN 978-963-7060-31-1.
30. **Erik, Pándi.** *Unification of the Hungarian Governmental communications systems.* Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1.
31. **Dr. Varga Balázs, Géczi Csaba.** *MPLS alapú IP hálózatok.* p. 37-63, MATÁV : MATÁV, 2001, Vol. PKI Közlemények 45. HU-ISSN 1216-3961.
32. **Dr. Varga Balázs, Géczi Csaba.** *Ethernet alapú szolgáltatói hálózatok és szolgáltatások.* p. 137-165, Budapest : Matáv, 2003, Vol. PKI közlemények 47. . HU ISBN: 1216-3961.
33. **Bleier Attila, dr. Rajnai Zoltán.** *Vezeték nélküli képátviteli rendszer.* p. 118-129, Budapest : ZMNE, 2007, Vol. Communications 2007. ISSN: 1587-558X .
34. **Bleier Attila, dr. Rajnai Zoltán.** *Optimization of a transmission networ.* p. 264-285, Budapest : ZMNE, 2007, Vol. Communications 2007. ISBN: 978-963-7060-31-1.
35. **Bleier Attila, dr. Rajnai Zoltán.** *Bolyai Hadmérnöki Phd konferencia: Új generációs hálózati megoldások alkalmazása a Magyar Honvédség stacioner hálózatának modernizációjában.* Bleier Attila, Budapest : s.n., 2009.
36. **Attila Bleier, dr. Rajnai Zoltán.** *Traffic Optimization in a backbone.* 309-328, Budapest : Zrínyi Miklós Nemzetvédelmi Egyetem Publishing Office, 2008, Vol. 7/2. ISSN 1588-8789.
37. **Hámori András - Tanács Ferenc - Balogh Attila.** *Szolgáltatói IP gerinchálózat kiépítése Ethernet alapon.* p. 83-99, Budapest: Magyar Telekom Nyrt., 2005, Vol. PKI Közlemények 49. HU-ISSN 1216-3961.
38. **Attila, Bleier.** *Új generációs hálózati megoldások alkalmazása a Magyar Honvédség hálózatának modernizációjában.* Budapest : ZMNE, 2009., Hadmérnök, IV./2. kötet, old.: 19-28. ISSN 1788-1919.
39. **Attila, Bleier.** *The challanges of the 21st century and the requirements of the Hungarian Army.* Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-11-1.
40. **Attila, Bleier.** *Magyar Honvédség elvárásai és a XXI század kihívásai.* Budapest: ZMNE, Communications 2008. ISBN 978-963-7060-57-1.
41. **ZDNet.** STANAG 5066: The Standard for Data Applications Over HF Radio. *ZDNet.com.* [Online] 2008. [Cited: 06 23, 2009.]  
<http://whitepapers.zdnet.com/abstract.aspx?docid=396371>.
42. *STANAG 5048 Minimum Scale of Convectivity for Communications and Information Systems for NATO Land Forces-ED 5 AMD 0. NORTH ATLANTIC TREATY ORGANIZATION NC3B Sub-Committee AC/322 SC/1).* NATO : s.n.

43. SERVICE PROVIDERS ROUTER: Next Gen Routing. *Voice&Data*. [Online] 2005. [Cited: 02 28, 2009.] <http://voicendata.ciol.com/content/goldbook/goldbook05/105030506.asp>.
44. **IEEE Higher Speed Study Group**. IEEE 802.3ba. *IEEE Higher Speed Study Group*. [Online] 2009. [Cited: 06 24, 2009.] <http://www.ieee802.org/3/hssg/index.html>.
45. **Műszaki Magazin Online**. Elérkezik a zettabajt korszaka. *Műszaki Magazin Online*. [Online] 06 24, 2009. [Cited: 06 24, 2009.] [http://www.mm-online.hu/cikk/Elerkezik\\_a\\_zettabajt\\_korszaka](http://www.mm-online.hu/cikk/Elerkezik_a_zettabajt_korszaka). ISSN 1417-0132.
46. Critical Information Infrastructure Protection - a new initiative in 2009. *Europe's Information Society Thematic Portal*., 2009, 06 23, 2009. [http://ec.europa.eu/information\\_society/policy/nis/strategy/activities/ciip/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm).
47. Communication from the Commission on a European Programme for Critical Infrastructure Protection. *Access to European Union law*. 2006. [http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006\\_0786en01.pdf](http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf).
48. *Németország - konferencia az IT-katasztrófahelyzetekről* [Online] [Cited: 2010-06-02T18:33:51Z],[http://www.sg.hu/cikkek/74621/nemetorszag\\_konferencia\\_az\\_it\\_katasztrofahelyzetekrol](http://www.sg.hu/cikkek/74621/nemetorszag_konferencia_az_it_katasztrofahelyzetekrol)
49. *Uniós ütemterv az állampolgárok megfigyeléséről* [Online] [Cited: 2010-05-29T15:16:30Z], [http://www.sg.hu/cikkek/74651/unios\\_utemterv\\_az\\_allampolgarok\\_megfigyeleserol](http://www.sg.hu/cikkek/74651/unios_utemterv_az_allampolgarok_megfigyeleserol)
50. *6DEPLOY - IPv6 Deployment and Support*, <http://www.6deploy.org/index.php?page=tutorials>, 2010-01-14T09:07:35Z
51. *Az USA katonai erővel válaszolhat egy kibertámadásra*, [http://www.sg.hu/cikkek/74369/az\\_usa\\_katonai\\_erovel\\_valaszolhat\\_egy\\_kibertamadasra](http://www.sg.hu/cikkek/74369/az_usa_katonai_erovel_valaszolhat_egy_kibertamadasra), 2010-05-14T19:32:24Z
52. *Internet kinézete ma*, [http://www.sg.hu/cikkek/74082/hogy\\_nez\\_ki\\_ma\\_az\\_internet](http://www.sg.hu/cikkek/74082/hogy_nez_ki_ma_az_internet), 2010-05-03T17:47:35Z
53. *Traffic Engineering Network planning*,<http://www.sanog.org/resources/sanog7/saraph-te-network-planning-mpls.pdf>,2010-04-30T19:30:42Z
54. *NAViGaTOR - Network Analysis, Visualization, & Graphing TORonto*, <http://ophid.utoronto.ca/navigator/download.html>, 2010-04-22T18:29:02Z
55. *USA: jön az átfogó kibervédelmi program - HVG.hu*, [http://hvg.hu/Tudomany/20100304\\_USA\\_kibervedelmi\\_program#rss](http://hvg.hu/Tudomany/20100304_USA_kibervedelmi_program#rss), 2010-03-15T16:57:32Z
56. *A NATO kiemelt feladata lesz a jövőben a hálózatok védelme*, [http://www.sg.hu/cikkek/72931/a\\_nato\\_kiemelt\\_feladata\\_lesz\\_a\\_jovoben\\_a\\_halozatok\\_vedelme](http://www.sg.hu/cikkek/72931/a_nato_kiemelt_feladata_lesz_a_jovoben_a_halozatok_vedelme), 2010-03-15T16:36:01Z

57. *Wolfram/Alpha Examples - Engineering*,  
<http://www.wolframalpha.com/examples/Engineering.html>, 2010-02-05T19:39:38Z
58. *HP POD demonstration | HP Enterprise TV: Online Videos and Podcasts*,  
[http://h30423.www3.hp.com/index.jsp?fr\\_story=7cbadbae073b914862d7c29e59a08356c690ebf8&rf=bm](http://h30423.www3.hp.com/index.jsp?fr_story=7cbadbae073b914862d7c29e59a08356c690ebf8&rf=bm), 2010-01-30T19:09:39Z
59. *SG.hu - Másodpercenként éri kibertámadás a közműveket*,  
[http://www.sg.hu/cikkek/72222/masodpercenkent\\_eri\\_kibertamadas\\_a\\_kozmuveket](http://www.sg.hu/cikkek/72222/masodpercenkent_eri_kibertamadas_a_kozmuveket), 2010-01-30T16:50:19Z
60. *Juniper Networks with Aerohive Wireless LAN*,  
<http://www.juniper.net/us/en/local/pdf/solutionbriefs/3510329-en.pdf>, 2010-01-30T12:10:32Z
61. *Aerohive Networks, Inc. | Partners*, <http://www.aerohive.com/partners/technology.html>,  
 2010-01-30T12:09:49Z
62. *Networks and Communication Systems Branch*, <http://cs.itd.nrl.navy.mil/focus/>, 2010-01-06T13:36:05Z
63. *Háborúba megy az iPhone* [http://www.sg.hu/cikkek/71596/haboruba\\_megy\\_az\\_iphone](http://www.sg.hu/cikkek/71596/haboruba_megy_az_iphone),  
 2009-12-22T07:23:48Z
64. *Totem project home page*,<http://www.run.montefiore.ulg.ac.be/Projects/Presentation/index.php?project=TOTEM>,  
 2009-12-20T10:35:46Z
65. *Éghajlatváltozás jelei*,  
[http://hvg.hu/Tudomany/20091206\\_eghajlatvaltozas\\_tiz\\_veszjel.aspx](http://hvg.hu/Tudomany/20091206_eghajlatvaltozas_tiz_veszjel.aspx), 2009-12-06T13:58:02Z
66. *Overview of IPv6*, <http://ipv6.niif.hu/tipster6/papers/overview/>, 2009-12-06T13:28:21Z
67. *Joe Biden kér valamit*,  
[http://index.hu/kulfold/2009/12/01/joe\\_biden\\_kerni\\_akar\\_valamit\\_magyarorszagtol/](http://index.hu/kulfold/2009/12/01/joe_biden_kerni_akar_valamit_magyarorszagtol/), 2009-12-01T12:26:49Z
68. *Northern Ireland Research Queens University*,<http://www.csit.qub.ac.uk/Partners/CurrentPartners/>,2009-11-06T20:33:20Z
69. *Social network analysis software - Wikipedia, the free encyclopedia*,[http://en.wikipedia.org/wiki/Social\\_network\\_analysis\\_software](http://en.wikipedia.org/wiki/Social_network_analysis_software),2009-11-06T08:14:17Z
70. *Deliverables : Bandwidth On Demand (AutoBAHN) : Research : GEANT2*,<http://www.geant2.net/server/show/nav.1914>,2009-10-15T14:14:17Z
71. *Távközlési részleget hoz létre a német állam*,  
[http://www.sg.hu/cikkek/70015/tavkozlesi\\_reszleget\\_hoz\\_letre\\_a\\_nemet\\_allam](http://www.sg.hu/cikkek/70015/tavkozlesi_reszleget_hoz_letre_a_nemet_allam), 2009-09-29T17:15:00Z

72. *A hálózatok csapdájában - FN.hu*,  
[http://www.fn.hu/tudomany/20091009/halozatok\\_csapdajaban/](http://www.fn.hu/tudomany/20091009/halozatok_csapdajaban/), 2009-10-12T07:25:57Z
73. *Budapesten a V4-ek honvédelmi miniszterei - FN.hu*,  
[http://www.fn.hu/belfold/20091008/budapesten\\_v4\\_ek\\_honvedelmi/](http://www.fn.hu/belfold/20091008/budapesten_v4_ek_honvedelmi/), 2009-10-08T12:02:38Z
74. *Farkas Károly honlapja*, <https://inf.nyme.hu/~farkas/>, 2009-10-05T08:31:50Z
75. *Ausztrália - vírus fenyegeti az áramellátást*,  
[http://www.sg.hu/cikkek/70107/ausztralia\\_virus\\_fenyegeti\\_az\\_aramellatast](http://www.sg.hu/cikkek/70107/ausztralia_virus_fenyegeti_az_aramellatast), 2009-10-04T05:57:51Z
76. *A hálózat a világ kulcsa - FN.hu*,  
[http://www.fn.hu/tudomany/20091003/halozat\\_vilag\\_kulcsa/](http://www.fn.hu/tudomany/20091003/halozat_vilag_kulcsa/), 2009-10-04T05:46:56Z
77. *Arcane Technologies » Demos*, [http://www.arcane-technologies.com/?page\\_id=19](http://www.arcane-technologies.com/?page_id=19), 2009-09-23T17:22:12Z
78. *Defense University - A Pentagon számára már biztonsági kockázat az éghajlatváltozás*,  
[http://hvg.hu/Tudomany/20090814\\_pentagon\\_klimavaltozas\\_globalis\\_kockazat.aspx](http://hvg.hu/Tudomany/20090814_pentagon_klimavaltozas_globalis_kockazat.aspx), 2009-08-14T12:30:55Z
- 79 *NIS | Europa - Information Society*,  
[http://ec.europa.eu/information\\_society/policy/nis/strategy/activities/ciip/index\\_en.htm](http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm), 2009-06-19T05:31:25Z
80. *Schutz Kritischer Infrastrukturen in Deutschland*,  
<http://www.bsi.bund.de/fachthem/kritis/index.htm>, 2009-06-19T05:29:56Z
81. *NCOIC - Net Enabled Emergency Response (NEER) Integrated Project Team (IPT)*,  
<https://www.ncoic.org/technology/activities/neer>, 2009-06-12T09:50:02Z
82. *MUNK : Katonai informatika: Egyetemi jegyzet*, <http://www.bibl.u-szeged.hu/bibl/mil/konyvek/elmelet/m/bibJAT00725132.html>, 2008-06-07T19:19:05Z
83. *Honvédelmi Minisztérium*, <http://www.hm.gov.hu/miniszterium>, 2008-06-07T19:18:07Z
84. *Communications Systems and Equipment - Army Technology*, <http://www.army-technology.com/contractors/navigation/>, 2008-06-07T19:13:55Z
85. *BWI Leistungsverbund | Unternehmen*, [http://www.bwi-it.de/stellenmarkt\\_informationstechnik.html](http://www.bwi-it.de/stellenmarkt_informationstechnik.html), 2008-01-10T14:14:33Z
86. *FGAN-FKIE - Profile*, [http://www.fgan.de/fkie/fkie\\_en.html](http://www.fgan.de/fkie/fkie_en.html), 2008-01-05T15:16:01Z
87. *PhiniseD - Hall of Phame*, <http://www.phinished.org/phame.php>, 2008-01-03T20:50:39Z
88. *NDG - Network Design Group*,  
<http://www.telecom.lth.se/ndg/research/publications/publications.html>, 2007-10-19T08:47:07Z

89. *Python Patterns - Implementing Graphs*, <http://www.python.org/doc/essays/graphs.html>, 2007-01-19T13:49:10Z

90. *Samsung develops machine gun sentry robot costs \$200k - Newlaunches.com*, [http://www.newlaunches.com/archives/samsung\\_develops\\_machine\\_gun\\_sentry\\_robot\\_costs\\_200k.php](http://www.newlaunches.com/archives/samsung_develops_machine_gun_sentry_robot_costs_200k.php), 2006-11-19T13:14:58Z

91. *DARPA Office Programs*, [http://www.darpa.mil/body/off\\_programs.html](http://www.darpa.mil/body/off_programs.html), 2006-10-05T11:05:23Z

92. *Nesi - Wikipedia, the free encyclopedia*, <http://en.wikipedia.org/wiki/Nesi>, 2006-09-29T09:16:45Z



### VI.3 Publikációs jegyzék

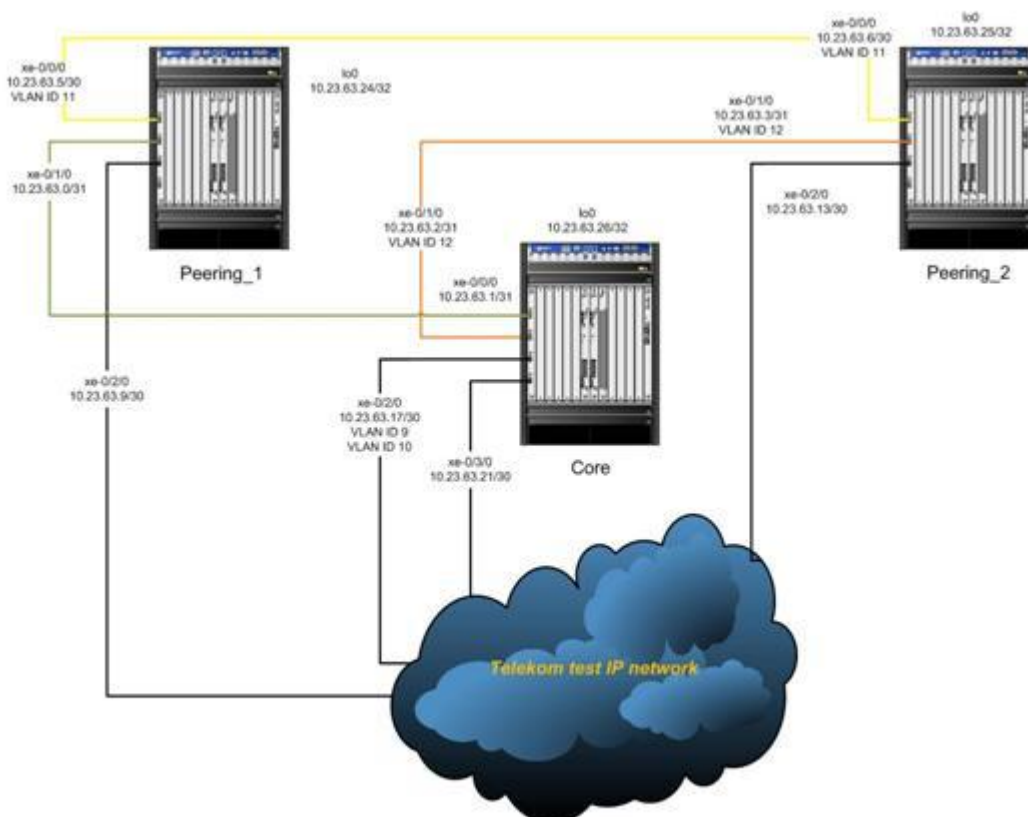
1. **Bleier Attila, dr. Rajnai Zoltán.** *Vezeték nélküli képátviteli rendszer.* p. 118-129, Budapest : ZMNE, 2007, Vol. Communications 2007. ISSN: 1587-558X .
2. **Bleier Attila, dr. Rajnai Zoltán.** *Optimization of a transmission network.* p. 264-285, Budapest : ZMNE, 2007, Vol. Communications 2007. ISBN: 978-963-7060-31-1.
3. **Bleier Attila, dr. Rajnai Zoltán.** *Bolyai Hadmérnöki Phd konferencia: Új generációs hálózati megoldások alkalmazása a Magyar Honvédség stacioner hálózatának modernizációjában.* Bleier Attila, Budapest : s.n., 2009.
4. **Attila Bleier, dr. Rajnai Zoltán.** *Traffic Optimization in a backbone.* 309-328, AARMS, Budapest : Zrínyi Miklós Nemzetvédelmi Egyetem Publishing Office, 2008, Vol. 7/2. ISSN 1588-8789.
5. **Attila, Bleier.** *Új generációs hálózati megoldások alkalmazása a Magyar Honvédség hálózatának modernizációjában.* Budapest : ZMNE, 2009., Hadmérnök, IV./2. kötet, old.: 19-28. ISSN 1788-1919.
6. **Attila, Bleier.** *The challenges of the 21st century and the requirements of the Hungarian Army.* Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-11-1.
7. **Attila, Bleier.** *Magyar Honvédség elvárásai és a XXI század kihívásai.* Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-57-1.
8. **Zoltán Rajnai dr., Attila Bleier.** *Technical problems in the IP communication system of the Hungarian Army.* p15-23, AARMS, Budapest : Zrínyi Miklós Nemzetvédelmi Egyetem Publishing Office, Vol. 9. 2010/1. ISSN 1588-8789.
9. **Attila Bleier, Zoltán Rajnai dr.,** *A magyar honvédség stacioner hálózati forgalmi viszonyainak vizsgálata.* p185-200, Bolyai Szemle, Budapest, ZMNE, 2010. XIX. évf. 2. szám, ISSN: 1416-1443



## VII. Mellékletek

### VII.1 Gerinchálózati tesztelrendezés

A tesztek folyamán az alábbi tesztelrendezésben teszteltünk egy nagy rendelkezésre állású IP gerinchálózatot. A gerinchálózati eszközöket a Juniper Networks szállította, a gerinchálózatot a egy nagy magyar gerinchálózati szolgáltató számára alakítottuk ki, hogy az új, nagy rendelkezésre állású gerinchálózati útválasztóit tesztelhessük. A teszt során teszteltük a korábban felsorolt Non-Stop-routing, Graceful-Restart, OSPF és ISIS gyors konvergencia és MPLS által nyújtott szolgáltatásokat. A kialakítandó hálózatot folyamatosan SLA naplózó rendszerrel vizsgáltuk, amely az egyes tesztviszonylatokat 10 másodperces gyakorisággal mérte, és 1 perces gyakorisággal átlagot képzett belőlük. A teszt során a hálózat kiválóra vizsgázott, az eszközök irányító motorját jelentő kapcsoló modulok durva fizikai eltávolításakor az eszközök 1,2 ms-os forgalomkiesést követően automatikusan a tartalék kapcsolóeszközre váltottak. Ugyanezt a tesztkonfigurációt és elrendezést bármely nagy rendelkezésre állású IP/MPLS hálózatában sikeresen alkalmazható, így a Magyar Honvédség hálózatában is ajánlott a használata.



### VII.1.1 A teszt eredménye

A teszt során azt tapasztaltuk, hogy 800 bájtos UDP csomagokkal mérve a hálózat két csomópont között 100 mikroszekundumos nagyságrendű round-trip-time (RTT) értékeket tapasztaltunk. A round-trip-time a csomag oda és visszaérkezését méri a hálózat két pontja között. Tehát a teljes útvonal késleltetése jobb, mint 50 mikroszekundum.

Owner, Test	Probe received	Round trip time
P1, CORE-to-P1_800byte	Fri Feb 26 10:45:39 2010	105 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:45:45 2010	105 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:45:51 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:45:57 2010	112 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:46:03 2010	105 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:46:09 2010	103 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:46:15 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:46:21 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:46:27 2010	105 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:46:33 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:47:39 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:47:45 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:47:51 2010	105 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:47:57 2010	116 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:48:03 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:48:09 2010	103 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:48:15 2010	103 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:48:21 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:48:27 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:48:33 2010	105 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:49:39 2010	117 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:49:45 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:49:51 2010	105 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:49:57 2010	103 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:50:03 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:50:09 2010	103 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:50:15 2010	117 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:50:21 2010	121 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:50:27 2010	106 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:50:33 2010	102 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:51:39 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:51:45 2010	111 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:51:51 2010	106 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:51:57 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:52:03 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:52:09 2010	104 usec

P1, CORE-to-P1_800byte	Fri Feb 26 10:52:15 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:52:21 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:52:27 2010	103 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:52:33 2010	102 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:53:39 2010	104 usec
P1, CORE-to-P1_800byte	Fri Feb 26 10:53:45 2010	104 usec
P2, CORE-to-P2_800byte	Fri Feb 26 10:45:40 2010	102 usec

## VII.1.2 A teszt mérésre használt tesztkonfigurációja

A tesztre a mérőmodult az alábbi konfigurációnak megfelelően konfiguráltuk fel:

```

services {
  rpm {
    probe <*> {
      test <*> {
        probe-type udp-ping;
        probe-count 10;
        probe-interval 6;
        test-interval 60;
        destination-port 7;
        inactive: source-address 10.23.63.26;
        history-size 255;
        moving-average-size 50;
        data-size 800;
        thresholds {
          successive-loss 3;
          total-loss 5;
          rtt 2000000;
          jitter-rtt 20000;
        }
        traps [ probe-failure test-failure jitter-exceeded rtt-exceeded ];
        destination-interface sp-11/0/0.20;
        inactive: hardware-timestamp;
      }
    }
  }
}

{master}[edit]
admin@C1-re0# show services rpm
apply-groups RPM_TEMPLATE;
probe P1 {

```

```

test CORE-to-P1_800byte {
    target address 10.23.63.61;
}
}
probe P2 {
    test CORE-to-P2_800byte {
        target address 10.23.63.62;
    }
}
probe-server {
    udp {
        port 7;
    }
}

```

A teszt során bizonyítottuk, hogy az új generációs IP/MPLS hálózatok a **gyakorlatban használhatóak** egy új nagy rendelkezésre állású infrastruktúra alapköveként.

### **VII.1.3 Az eszközök az alábbi konfigurációban szerepeltek a tesztekben:**

#### ***VII.1.3.1 Core csomópont konfigurációja***

```

show conf|no-more
## Last commit: 2010-01-22 13:48:34 CET by admin
version 10.0R2.10;
groups {
    re0 {
        system {
            host-name core-re0;
        }
        interfaces {
            fxp0 {
                unit 0 {
                    family inet {
                        address 10.23.64.2/24 {
                            master-only;
                        }
                    }
                }
            }
        }
    }
}

```

```

        address 10.23.64.5/24;
    }
}
}
}
}
rel {
    system {
        host-name core-rel;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 10.23.64.2/24 {
                        master-only;
                    }
                    address 10.23.64.6/24;
                }
            }
        }
    }
}
CORE-INTF {
    interfaces {
        <xe-*> {
            traps;
            mtu 9192;
            hold-time up 5000 down 0;

```

```

link-mode full-duplex;
gigether-options {
    no-auto-negotiation;
}
unit <*> {
    family iso;
    family mpls;
}
}
}
}
RPM_TEMPLATE {
    services {
        rpm {
            probe <*> {
                test CONNECTIVITY {
                    probe-type icmp-ping-timestamp;
                    probe-count 10;
                    probe-interval 1;
                    test-interval 300;
                    thresholds {
                        successive-loss 3;
                        total-loss 5;
                        rtt 2000000;
                        jitter-rtt 20000;
                    }
                    traps [ probe-failure test-failure jitter-exceeded rtt-exceeded ];
                    destination-interface sp-11/0/0.0;
                }
            }
        }
    }
}

```



```

server {
    10.23.12.120 source-address 10.23.63.26;
}
}
}
}
login {
class operator-local {
    idle-timeout 30;
    permissions [ clear interface-control network reset trace view view-configuration ];
}
class readonly-local {
    idle-timeout 30;
    permissions view;
}
class superuser-local {
    idle-timeout 30;
    permissions all;
}
user admin {
    uid 2000;
    class superuser-local;
    authentication {
        encrypted-password "$1$buSwv/6D$2MAsAWLAKhp3whRZaCJ1A1"; ##
SECRET-DATA
    }
}
/* RADIUS/TACACS template for read-only users. Must be called 'remote' */
user remote {
    full-name "All remote users";
}

```



```
    uid 9997;
    class readonly-local;
}
/* RADIUS/TACACS template for super-users. */
user remote_admin {
    full-name "Remote superusers";
    uid 9999;
    class superuser-local;
}
/* RADIUS/TACACS template for operators. */
user remote_operator {
    full-name "Remote operators";
    uid 9998;
    class operator-local;
}
}
services {
    ftp {
        connection-limit 10;
        rate-limit 10;
    }
    ssh {
        root-login deny;
        protocol-version v2;
        connection-limit 10;
        rate-limit 10;
    }
    telnet {
        connection-limit 5;
```

```

        rate-limit 5;
    }
}
syslog {
    archive size 5m files 10 world-readable;
    user * {
        any critical;
    }
    host other-routing-engine {
        any error;
        log-prefix other-RE;
    }
    host 10.5.78.254 {
        any notice;
        authorization info;
        daemon any;
        kernel any;
        firewall info;
        pfe info;
        interactive-commands any;
        facility-override local6;
        log-prefix MX-CORE;
        explicit-priority;
    }
    host 10.23.12.44 {
        any notice;
        authorization info;
        daemon any;
        kernel any;

```

```
firewall info;
pfe info;
interactive-commands any;
facility-override local6;
log-prefix MX-CORE;
explicit-priority;
}
host 10.23.12.19 {
any notice;
authorization info;
daemon any;
kernel any;
firewall info;
pfe info;
interactive-commands any;
facility-override local6;
log-prefix MX-CORE;
explicit-priority;
}
host 10.230.191.5 {
any notice;
authorization info;
daemon any;
kernel any;
firewall info;
pfe info;
interactive-commands any;
facility-override local6;
log-prefix MX-CORE;
```

```

    explicit-priority;
}
file messages {
    any notice;
    authorization none;
    explicit-priority;
}
file security {
    authorization any;
    explicit-priority;
}
file commands {
    authorization info;
    interactive-commands any;
    explicit-priority;
}
file firewall {
    firewall any;
}
console {
    any alert;
}
time-format year millisecond;
source-address 10.23.63.26;
}
inactive: archival {
    configuration {
        transfer-on-commit;
        archive-sites {

```

```
"scp://username@10.10.10.20:22//directory1/directory2/directory3/" password  
"$9$PQ3/CAp1RSFnreMWdVsYgJjHf5F"; ## SECRET-DATA
```

```
}
```

```
}
```

```
}
```

```
commit synchronize;
```

```
inactive: ntp {
```

```
    boot-server 10.10.10.10;
```

```
    server 10.10.10.10;
```

```
    source-address 10.23.63.26;
```

```
}
```

```
}
```

```
chassis {
```

```
    redundancy {
```

```
        routing-engine 0 master;
```

```
        routing-engine 1 backup;
```

```
        failover {
```

```
            on-loss-of-keepalives;
```

```
            on-disk-failure;
```

```
        }
```

```
        graceful-switchover;
```

```
    }
```

```
fpc 11 {
```

```
    pic 0 {
```

```
        tunnel-services {
```

```
            bandwidth 1g;
```

```
        }
```

```
    }
```

```
}
```

```
alarm {
```

```

management-ethernet {
    link-down yellow;
}
ethernet {
    link-down red;
}
}
}
interfaces {
    xe-0/0/0 {
        description Core-to-P1;
        unit 0 {
            family inet {
                filter {
                    input BLOCK-P1-L0-SEC;
                }
                address 10.23.63.1/31 {
                    primary;
                }
            }
            family inet6 {
                address fec0::1/127;
            }
        }
    }
    xe-0/1/0 {
        description Core-to-P2;
        flexible-vlan-tagging;
        inactive: gigether-options {

```

```

source-filtering;
source-address-filter {
    00:19:e2:b1:80:29;
}
}
unit 12 {
    vlan-id 12;
    family inet {
        address 10.23.63.2/31 {
            primary;
        }
    }
    family inet6 {
        address fec0::2/127;
    }
}
}
xe-0/2/0 {
    description Core-to-RTK1;
    flexible-vlan-tagging;
    unit 9 {
        vlan-id 9;
        family inet {
            address 10.23.63.17/30 {
                primary;
            }
        }
        family inet6 {
            address fec0::17/126;

```

```

    }
}
unit 10 {
    vlan-id 10;
    family inet {
        address 10.23.63.32/31;
    }
}
}
xe-0/3/0 {
    description Core-to-RTK2;
    unit 0 {
        family inet {
            address 10.23.63.21/30 {
                primary;
            }
        }
        family inet6 {
            address fec0::21/126;
        }
    }
}
lt-11/0/0 {
    unit 100 {
        encapsulation ethernet;
        peer-unit 200;
        family inet;
    }
    unit 200 {

```



```

    encapsulation ethernet;
    peer-unit 100;
    family inet;
}
}
sp-11/0/0 {
    unit 0 {
        rpm client;
        family inet {
            address 10.23.63.50/32;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.23.63.26/32 {
                primary;
            }
            address 10.23.63.66/32;
        }
        family iso {
            address 49.0000.0100.2306.3026.00;
        }
        family inet6 {
            address fec0::26/128;
        }
    }
}
unit 100 {

```

```

        family inet {
            address 10.10.10.10/32;
        }
    }
}

routing-options {
    graceful-restart {
        restart-duration 240;
    }
    static {
        route 1.1.1.1/32 discard;
    }
    autonomous-system 65001;
    confederation 200 members [ 65001 65002 ];
    forwarding-table {
        indirect-next-hop;
    }
}

protocols {
    mpls {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
    bgp {
        traceoptions {
            file bgp.log size 5m files 10;
        }
    }
}

```

```

    flag general;
    flag open;
    flag state;
}
log-updown;
inactive: damping;
authentication-key "$9$vVRL7Vws4oZjwYoGUif5"; ## SECRET-DATA
graceful-restart;
tcp-mss 4096;
group intra-conf-BGP {
    type internal;
    local-address 10.23.63.26;
    family inet {
        unicast;
    }
    family inet-vpn {
        unicast;
    }
    export self-next-hop;
    multipath;
    neighbor 10.23.63.24 {
        description Peering-1;
        bfd-liveness-detection {
            minimum-interval 300;
            multiplier 3;
        }
    }
}
group inter-conf-BGP {

```

```

type external;
multihop {
    inactive: ttl 254;
}
local-address 10.23.63.26;
family inet {
    unicast;
}
family inet-vpn {
    unicast;
}
export self-next-hop;
multipath;
neighbor 10.23.63.25 {
    description Peering-2;
    import DL-10;
    peer-as 65002;
    outbound-route-filter {
        prefix-based {
            accept {
                inet;
            }
        }
    }
}
}
group eBGP {
    type external;
    multihop;
}

```

```

family inet {
    unicast;
}
family inet-vpn {
    unicast;
}
multipath;
neighbor 10.23.63.18 {
    description OSR1;
    inactive: import DL-10;
    export [ set bela_bgp_exp ];
    peer-as 300;
    inactive: outbound-route-filter {
        prefix-based {
            accept {
                inet;
            }
        }
    }
}
neighbor 10.23.63.22 {
    description OSR2;
    export POLICY-LIST-NAME-2;
    peer-as 100;
}
}
}
isis {
    traceoptions {

```

```

file isis.log size 5m files 10;

flag error detail;

flag general;
}
reference-bandwidth 1000g;
lsp-lifetime 65535;
spf-options {
    delay 50;
    holddown 2000;
    rapid-runs 5;
}
overload timeout 300;
level 1 disable;
level 2 {
    authentication-key "$9$zuyL6CuOBEhyKO1hrlv7N"; ## SECRET-DATA
    authentication-type md5;
    wide-metrics-only;
}
interface xe-0/0/0.0 {
    point-to-point;
    node-link-protection;
}
interface xe-0/1/0.12 {
    point-to-point;
    node-link-protection;
}
interface xe-0/2/0.0 {
    point-to-point;
    node-link-protection;
}

```

```

}
interface xe-0/3/0.0 {
    point-to-point;
    node-link-protection;
}
interface fxp0.0 {
    disable;
}
interface lo0.0 {
    point-to-point;
    passive;
}
}
ospf {
    traceoptions {
        file ospf.log size 5m files 10;
        flag error detail;
        flag general;
        flag event;
    }
    spf-options {
        delay 50;
        holddown 2000;
        rapid-runs 5;
    }
    reference-bandwidth 1000g;
    area 0.0.0.0 {
        interface xe-0/0/0.0 {
            interface-type p2p;

```

```

node-link-protection;
authentication {
    simple-password "$9$Oz5QRclKvLXNbKMX-dwaJ"; ## SECRET-DATA
}
bfd-liveness-detection {
    minimum-interval 100;
    multiplier 3;
}
}
interface xe-0/1/0.12 {
    interface-type p2p;
    node-link-protection;
    authentication {
        md5 2 key "$9$LJwNVYg4ZGjqgoGiH.zF"; ## SECRET-DATA
    }
}
interface lo0.0 {
    interface-type p2p;
    passive;
}
interface fxp0.0 {
    disable;
}
interface sp-11/0/0.0 {
    interface-type p2p;
    passive;
}
}
}

```



```

ldp {
  interface all;
  interface fxp0.0 {
    disable;
  }
  session 10.23.63.24 {
    authentication-key "$9$I5.crvW87NVYWLNbw2GU"; ## SECRET-DATA
  }
  session 10.23.63.25 {
    authentication-key "$9$kPT36/tpOR69pB1EeK"; ## SECRET-DATA
  }
}
lldp {
  interface xe-0/0/0;
  interface xe-0/1/0;
  interface xe-0/2/0;
  interface xe-0/3/0;
}
}
policy-options {
  prefix-list PR-10 {
    192.168.1.0/24;
  }
  policy-statement DL-10 {
    term 1 {
      from {
        prefix-list PR-10;
      }
      then accept;
    }
  }
}

```

```

}
term 2 {
    then reject;
}
}
policy-statement POLICY-LIST-NAME-2 {
    term 1 {
        from {
            community 20;
            metric 10;
        }
        then accept;
    }
    term 2 {
        then reject;
    }
}
policy-statement bela_bgp_exp {
    term 1 {
        from {
            route-filter 10.23.63.24/32 exact;
            route-filter 10.23.63.25/32 exact;
            route-filter 10.23.63.26/32 exact;
        }
        then accept;
    }
}
policy-statement self-next-hop {
    term change-next-hop {

```





```

        target address 10.23.63.24;
    }
}
probe P2 {
    test CONNECTIVITY {
        target address 10.23.63.25;
    }
}
}
}

```

```
{ master }
```

```
admin@core-re0>
```

### **VII.1.3.2 P1 csomópont konfigurációja:**

```
===== PuTTY log 2010.01.22 14:02:37
```

```
=====
```

```
show configuration |no-more
```

```
## Last commit: 2010-01-20 17:30:10 CET by admin
```

```
version 10.0R2.10;
```

```

groups {
  re0 {
    system {
      host-name p1-re0;
    }
    interfaces {
      fxp0 {
        unit 0 {
          family inet {
            address 10.23.64.3/24 {
              master-only;
            }
            address 10.23.64.7/24;
          }
        }
      }
    }
  }
}
re1 {
  system {
    host-name p1-re1;
  }
}

```

```

interfaces {
  fxp0 {
    unit 0 {
      family inet {
        address 10.23.64.3/24 {
          master-only;
        }
        address 10.23.64.8/24;
      }
    }
  }
}
CORE-INTF {
  interfaces {
    <xe-*> {
      traps;
      mtu 9192;
      hold-time up 5000 down 0;
      link-mode full-duplex;
      gigheter-options {
        no-auto-negotiation;
      }
      unit <*> {
        family iso;
        family mpls;
      }
    }
  }
}
RPM_TEMPLATE {
  services {
    rpm {
      probe <*> {
        test CONNECTIVITY {
          probe-type icmp-ping-timestamp;
          probe-count 10;
          probe-interval 1;
          test-interval 300;
          thresholds {
            successive-loss 3;
            total-loss 5;
            rtt 2000000;
            jitter-rtt 20000;
          }
          traps [ probe-failure test-failure jitter-exceeded rtt-exceeded ];
          destination-interface sp-11/0/0.0;
        }
      }
    }
  }
}

```

```

    }
  }
}
apply-groups [ re0 re1 CORE-INTF ];
system {
  backup-router 10.23.64.200;
  time-zone Europe/Budapest;
  default-address-selection;
  no-redirects;
  authentication-order [ tacplus password ];
  ports {
    console {
      log-out-on-disconnect;
      insecure;
      type vt100;
    }
  }
  root-authentication {
    encrypted-password "$1$XSvD8FHv$Eh7E2xztu2TGPWW0KEr3v/"; ## SECRET-
DATA
  }
  inactive: tacplus-server {
    10.23.12.120;
  }
  accounting {
    events [ login change-log interactive-commands ];
    destination {
      tacplus {
        server {
          10.23.12.120 source-address 10.23.63.24;
        }
      }
    }
  }
}
login {
  class operator-local {
    idle-timeout 30;
    permissions [ clear interface-control network reset trace view view-configuration ];
  }
  class readonly-local {
    idle-timeout 30;
    permissions view;
  }
  class superuser-local {
    idle-timeout 30;
    permissions all;
  }
  user admin {
    uid 2000;
    class superuser-local;
  }
}

```

```

    authentication {
        encrypted-password "$1$buSwv/6D$2MAsAWLAKhp3whRZaCJ1A1"; ##
SECRET-DATA
    }
}
/* RADIUS/TACACS template for read-only users. Must be called 'remote' */
user remote {
    full-name "All remote users";
    uid 9997;
    class readonly-local;
}
/* RADIUS/TACACS template for super-users. */
user remote_admin {
    full-name "Remote superusers";
    uid 9999;
    class superuser-local;
}
/* RADIUS/TACACS template for operators. */
user remote_operator {
    full-name "Remote operators";
    uid 9998;
    class operator-local;
}
}
services {
    ftp;
    ssh {
        root-login deny;
        protocol-version v2;
    }
}
syslog {
    archive size 5m files 10 world-readable;
    user * {
        any critical;
    }
    host other-routing-engine {
        any error;
        log-prefix other-RE;
    }
    host 10.5.78.254 {
        any notice;
        authorization info;
        daemon any;
        kernel any;
        firewall info;
        pfe info;
        interactive-commands any;
        facility-override local6;
        log-prefix MX-PEERING-1;
    }
}

```



```

    explicit-priority;
}
host 10.23.12.44 {
    any notice;
    authorization info;
    daemon any;
    kernel any;
    firewall info;
    pfe info;
    interactive-commands any;
    facility-override local6;
    log-prefix MX-PEERING-1;
    explicit-priority;
}
host 10.23.12.19 {
    any notice;
    authorization info;
    daemon any;
    kernel any;
    firewall info;
    pfe info;
    interactive-commands any;
    facility-override local6;
    log-prefix MX-PEERING-1;
    explicit-priority;
}
host 10.230.191.5 {
    any notice;
    authorization info;
    daemon any;
    kernel any;
    firewall info;
    pfe info;
    interactive-commands any;
    facility-override local6;
    log-prefix MX-PEERING-1;
    explicit-priority;
}
file messages {
    any notice;
    authorization none;
    explicit-priority;
}
file security {
    authorization any;
    explicit-priority;
}
file commands {
    authorization info;
    interactive-commands any;
}

```

```

        explicit-priority;
    }
    file firewall {
        firewall any;
    }
    console {
        any alert;
    }
    time-format year millisecond;
    source-address 10.23.63.24;
}
inactive: archival {
    configuration {
        transfer-on-commit;
        archive-sites {
            "scp://username@10.10.10.20:22//directory1/directory2/directory3/" password
"$9$PQ3/CAp1RSFnRMWdVsYgJjHf5F"; ## SECRET-DATA
        }
    }
}
commit synchronize;
inactive: ntp {
    boot-server 10.10.10.10;
    server 10.10.10.10;
    source-address 10.23.63.24;
}
}
chassis {
    redundancy {
        routing-engine 0 master;
        routing-engine 1 backup;
        failover {
            on-loss-of-keepalives;
            on-disk-failure;
        }
        graceful-switchover;
    }
    fpc 11 {
        pic 0 {
            tunnel-services {
                bandwidth 1g;
            }
        }
    }
}
alarm {
    management-ethernet {
        link-down yellow;
    }
    ethernet {
        link-down red;
    }
}

```

```

    }
  }
}
interfaces {
  xe-0/0/0 {
    flexible-vlan-tagging;
    unit 11 {
      description P1-to-P2;
      vlan-id 11;
      family inet {
        address 10.23.63.5/30 {
          primary;
        }
      }
      family inet6 {
        address fec0::5/126;
      }
    }
  }
  xe-0/1/0 {
    unit 0 {
      description P1-to-Core;
      family inet {
        address 10.23.63.0/31 {
          primary;
        }
      }
      family inet6 {
        address fec0::0/127;
      }
    }
  }
  xe-0/2/0 {
    unit 0 {
      description P1-to-RTK;
      family inet {
        address 10.23.63.9/30 {
          primary;
        }
      }
      family inet6 {
        address fec0::9/126;
      }
    }
  }
  sp-11/0/0 {
    unit 0 {
      rpm client;
      family inet {
        address 10.23.63.51/32;
      }
    }
  }
}

```

```

    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.23.63.24/32 {
        primary;
      }
      address 10.23.63.64/32;
    }
    family iso {
      address 49.0000.0100.2306.3024.00;
    }
    family inet6 {
      address fec0::24/128;
    }
  }
  unit 100 {
    family inet {
      address 10.10.10.1/32;
    }
  }
}
}
routing-options {
  graceful-restart {
    restart-duration 240;
  }
  autonomous-system 65001;
  confederation 200 members [ 65001 65002 ];
  forwarding-table {
    indirect-next-hop;
  }
}
protocols {
  mpls {
    interface all;
    interface fxp0.0 {
      disable;
    }
  }
  bgp {
    traceoptions {
      file bgp.log size 5m files 10;
      flag general;
      flag open;
      flag state;
    }
    log-updown;
  }
}

```

```

authentication-key "$9$taFeOIcyrvMLNyIMXx-2g"; ## SECRET-DATA
graceful-restart;
tcp-mss 4096;
group intra-conf-BGP {
    type internal;
    local-address 10.23.63.24;
    family inet {
        unicast;
    }
    family inet-vpn {
        unicast;
    }
    multipath;
    neighbor 10.23.63.26 {
        description Core;
        bfd-liveness-detection {
            minimum-interval 300;
            multiplier 3;
        }
    }
}
group inter-conf-BGP {
    type external;
    multihop;
    local-address 10.23.63.24;
    family inet {
        unicast;
    }
    family inet-vpn {
        unicast;
    }
    multipath;
    neighbor 10.23.63.25 {
        description Peering-2;
        peer-as 65002;
    }
}
group eBGP {
    type external;
    multihop;
    family inet {
        unicast;
    }
    family inet-vpn {
        unicast;
    }
    multipath;
    neighbor 10.23.63.10 {
        description OSR1;
        peer-as 300;
    }
}

```

```

    }
  }
}
isis {
  traceoptions {
    file isis.log size 5m files 10;
    flag error detail;
    flag general;
  }
  reference-bandwidth 1000g;
  lsp-lifetime 65535;
  spf-options {
    delay 50;
    holddown 2000;
    rapid-runs 5;
  }
  overload timeout 300;
  level 1 disable;
  level 2 {
    authentication-key "$9$zuyL6CuOBEhyKO1hrlv7N"; ## SECRET-DATA
    authentication-type md5;
    wide-metrics-only;
  }
  interface xe-0/0/0.11 {
    point-to-point;
    node-link-protection;
  }
  interface xe-0/1/0.0 {
    point-to-point;
    node-link-protection;
  }
  interface xe-0/2/0.0 {
    point-to-point;
    node-link-protection;
  }
  interface fxp0.0 {
    disable;
  }
  interface lo0.0 {
    point-to-point;
    passive;
  }
}
ospf {
  traceoptions {
    file ospf.log size 5m files 10;
    flag error detail;
    flag general;
    flag event;
  }
}

```

```

spf-options {
  delay 50;
  holddown 2000;
  rapid-runs 5;
}
reference-bandwidth 1000g;
area 0.0.0.0 {
  interface xe-0/0/0.11 {
    interface-type p2p;
    node-link-protection;
  }
  interface xe-0/1/0.0 {
    interface-type p2p;
    node-link-protection;
    authentication {
      simple-password "$9$Oz5QRclKvLXNbKMX-dwaJ"; ## SECRET-DATA
    }
    bfd-liveness-detection {
      minimum-interval 100;
      multiplier 3;
    }
  }
  interface fxp0.0 {
    disable;
  }
  interface lo0.0 {
    interface-type p2p;
    passive;
  }
  interface sp-11/0/0.0 {
    interface-type p2p;
    passive;
  }
}
}
ldp {
  interface all;
  interface fxp0.0 {
    disable;
  }
  session 10.23.63.25 {
    authentication-key "$9$hz4rK8XxdVs4X7VY2oji"; ## SECRET-DATA
  }
  session 10.23.63.26 {
    authentication-key "$9$wigaUji.m5FjHmTQ3tp"; ## SECRET-DATA
  }
}
lldp {
  interface xe-0/0/0;
  interface xe-0/1/0;
}

```

```

        interface xe-0/2/0;
    }
}
routing-instances {
    VPN {
        instance-type vrf;
        interface lo0.100;
        route-distinguisher 10.23.63.24:100;
        vrf-target target:200:100;
    }
}
services {
    rpm {
        apply-groups RPM_TEMPLATE;
        probe CORE {
            test CONNECTIVITY {
                target address 10.23.63.26;
            }
        }
        probe P2 {
            test CONNECTIVITY {
                target address 10.23.63.25;
            }
        }
    }
}

{master}
admin@p1-re0>

```

### VII.1.3.3 Core2 csomópont konfigurációja

```

===== PuTTY log 2010.01.22 14:04:04
=====

```

```
{master}
```

```

admin@p2-re0> show con  figuration |no-more
## Last commit: 2010-01-20 17:27:43 CET by admin
version 10.0R2.10;
groups {
    re0 {
        system {
            host-name p2-re0;
        }
        interfaces {
            fxp0 {
                unit 0 {
                    family inet {

```



```

        address 10.23.64.4/24 {
            master-only;
        }
        address 10.23.64.9/24;
    }
}
}
}
}
}
re1 {
    system {
        host-name p1-re1;
    }
    interfaces {
        fxp0 {
            unit 0 {
                family inet {
                    address 10.23.64.4/24 {
                        master-only;
                    }
                    address 10.23.64.10/24;
                }
            }
        }
    }
}
CORE-INTF {
    interfaces {
        <xe-*> {
            traps;
            mtu 9192;
            hold-time up 5000 down 0;
            link-mode full-duplex;
            gigheter-options {
                no-auto-negotiation;
            }
            unit <*> {
                family iso;
                family mpls;
            }
        }
    }
}
RPM_TEMPLATE {
    services {
        rpm {
            probe <*> {
                test CONNECTIVITY {
                    probe-type icmp-ping-timestamp;
                    probe-count 10;
                }
            }
        }
    }
}

```



```

    permissions [ clear interface-control network reset trace view view-configuration ];
}
class readonly-local {
    idle-timeout 30;
    permissions view;
}
class superuser-local {
    idle-timeout 30;
    permissions all;
}
user admin {
    uid 2000;
    class superuser-local;
    authentication {
        encrypted-password "$1$buSwv/6D$2MAsAWLAKhp3whRZaCJ1A1"; ##
SECRET-DATA
    }
}
/* RADIUS/TACACS template for read-only users. Must be called 'remote' */
user remote {
    full-name "All remote users";
    uid 9997;
    class readonly-local;
}
/* RADIUS/TACACS template for super-users. */
user remote_admin {
    full-name "Remote superusers";
    uid 9999;
    class superuser-local;
}
/* RADIUS/TACACS template for operators. */
user remote_operator {
    full-name "Remote operators";
    uid 9998;
    class operator-local;
}
}
services {
    ftp;
    ssh {
        root-login deny;
        protocol-version v2;
    }
}
syslog {
    archive size 5m files 10 world-readable;
    user * {
        any critical;
    }
    host other-routing-engine {

```

```

    any error;
    log-prefix other-RE;
}
host 10.5.78.254 {
    any notice;
    authorization info;
    daemon any;
    kernel any;
    firewall info;
    pfe info;
    interactive-commands any;
    facility-override local6;
    log-prefix MX-PEERING-2;
    explicit-priority;
}
host 10.23.12.44 {
    any notice;
    authorization info;
    daemon any;
    kernel any;
    firewall info;
    pfe info;
    interactive-commands any;
    facility-override local6;
    log-prefix MX-PEERING-2;
    explicit-priority;
}
host 10.23.12.19 {
    any notice;
    authorization info;
    daemon any;
    kernel any;
    firewall info;
    pfe info;
    interactive-commands any;
    facility-override local6;
    log-prefix MX-PEERING-2;
    explicit-priority;
}
host 10.230.191.5 {
    any notice;
    authorization info;
    daemon any;
    kernel any;
    firewall info;
    pfe info;
    interactive-commands any;
    facility-override local6;
    log-prefix MX-PEERING-2;
    explicit-priority;
}

```

```

}
file messages {
  any notice;
  authorization none;
  explicit-priority;
}
file security {
  authorization any;
  explicit-priority;
}
file commands {
  authorization info;
  interactive-commands any;
  explicit-priority;
}
file firewall {
  firewall any;
}
console {
  any alert;
}
time-format year millisecond;
source-address 10.23.63.25;
}
archival {
  configuration {
    transfer-on-commit;
    archive-sites {
      "scp://username@10.10.10.20:22//directory1/directory2/directory3/" password
"$9$PQ3/CAp1RSFnreMWdVsYgJjHf5F"; ## SECRET-DATA
    }
  }
}
commit synchronize;
ntp {
  boot-server 10.10.10.10;
  server 10.10.10.10;
  source-address 10.23.63.25;
}
}
chassis {
  redundancy {
    routing-engine 0 master;
    routing-engine 1 backup;
    failover {
      on-loss-of-keepalives;
      on-disk-failure;
    }
    graceful-switchover;
  }
}

```

```

fpc 11 {
  pic 0 {
    tunnel-services {
      bandwidth 1g;
    }
  }
}
alarm {
  management-ethernet {
    link-down yellow;
  }
  ethernet {
    link-down red;
  }
}
}
interfaces {
  xe-0/0/0 {
    flexible-vlan-tagging;
    unit 11 {
      description P2-to-P1;
      vlan-id 11;
      family inet {
        address 10.23.63.6/30 {
          primary;
        }
      }
      family inet6 {
        address fec0::6/126;
      }
    }
  }
  xe-0/1/0 {
    flexible-vlan-tagging;
    unit 12 {
      description P2-to-Core;
      vlan-id 12;
      family inet {
        address 10.23.63.3/31 {
          primary;
        }
      }
      family inet6 {
        address fec0::3/127;
      }
    }
  }
  xe-0/2/0 {
    unit 0 {
      description P2-to-RTK;
    }
  }
}

```

```

    family inet {
        address 10.23.63.13/30 {
            primary;
        }
    }
    family inet6 {
        address fec0::13/126;
    }
}
sp-11/0/0 {
    unit 0 {
        rpm client;
        family inet {
            address 10.23.63.52/32;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            filter {
                input RE-FILTER;
            }
            address 10.23.63.25/32 {
                primary;
            }
            address 192.168.1.1/32;
            address 10.23.63.65/32;
        }
        family iso {
            address 49.0000.0100.2306.3025.00;
        }
        family inet6 {
            address fec0::25/128;
        }
    }
    unit 100 {
        family inet {
            address 10.10.10.2/32;
        }
    }
}
}
routing-options {
    graceful-restart {
        restart-duration 240;
    }
    aggregate {
        route 192.168.1.0/24 discard;
    }
}

```

```

    route 192.168.1.0/26 discard;
}
autonomous-system 65002;
confederation 200 members [ 65001 65002 ];
forwarding-table {
    indirect-next-hop;
}
}
protocols {
    mpls {
        interface all;
        interface fxp0.0 {
            disable;
        }
    }
}
bgp {
    traceoptions {
        file bgp.log size 5m files 10;
        flag general;
        flag open;
        flag state;
    }
    log-updown;
    authentication-key "$9$T3/tu0IRcluORSyeXx"; ## SECRET-DATA
    graceful-restart;
    tcp-mss 4096;
    group inter-conf-BGP {
        type external;
        multihop;
        local-address 10.23.63.25;
        family inet {
            unicast;
        }
        family inet-vpn {
            unicast;
        }
    }
    multipath;
    neighbor 10.23.63.26 {
        description Core;
        export TO-CORE;
        peer-as 65001;
        outbound-route-filter {
            prefix-based {
                accept {
                    inet;
                }
            }
        }
    }
    neighbor 10.23.63.24 {

```



```

        description Peering-1;
        peer-as 65001;
    }
}
group eBGP {
    type external;
    multihop;
    family inet {
        unicast;
    }
    family inet-vpn {
        unicast;
    }
    multipath;
    neighbor 10.23.63.14 {
        description OSR2;
        peer-as 100;
    }
}
}
isis {
    traceoptions {
        file isis.log size 5m files 10;
        flag error detail;
        flag general;
    }
    reference-bandwidth 1000g;
    lsp-lifetime 65535;
    spf-options {
        delay 50;
        holddown 2000;
        rapid-runs 5;
    }
    overload timeout 300;
    level 1 disable;
    level 2 {
        authentication-key "$9$zuyL6CuOBEhyKO1hrlv7N"; ## SECRET-DATA
        authentication-type md5;
        wide-metrics-only;
    }
    interface xe-0/0/0.11 {
        point-to-point;
        node-link-protection;
    }
    interface xe-0/1/0.12 {
        point-to-point;
        node-link-protection;
    }
    interface xe-0/2/0.0 {
        point-to-point;
    }
}

```

```

        node-link-protection;
    }
    interface fxp0.0 {
        disable;
    }
    interface lo0.0 {
        point-to-point;
        passive;
    }
}
ospf {
    traceoptions {
        file ospf.log size 5m files 10;
        flag error detail;
        flag general;
        flag event;
    }
    spf-options {
        delay 50;
        holddown 2000;
        rapid-runs 5;
    }
    reference-bandwidth 1000g;
    area 0.0.0.0 {
        interface xe-0/0/0.11 {
            interface-type p2p;
            node-link-protection;
        }
        interface xe-0/1/0.12 {
            interface-type p2p;
            node-link-protection;
            authentication {
                md5 2 key "$9$kPT36/tpOR69pB1EeK"; ## SECRET-DATA
            }
        }
        interface fxp0.0 {
            disable;
        }
        interface lo0.0 {
            interface-type p2p;
            passive;
        }
        interface sp-11/0/0.0 {
            interface-type p2p;
            passive;
        }
    }
}
ldp {
    interface all;
}

```

```

interface fxp0.0 {
    disable;
}
session 10.23.63.24 {
    authentication-key "$9$IDmMLNdVY2oGdb2aJU.m"; ## SECRET-DATA
}
session 10.23.63.26 {
    authentication-key "$9$5F6Apu1Ihrp0IcSILX"; ## SECRET-DATA
}
}
lldp {
    interface xe-0/0/0;
    interface xe-0/1/0;
    interface xe-0/2/0;
}
}
policy-options {
    policy-statement TO-CORE {
        term 1 {
            from {
                protocol aggregate;
                route-filter 192.168.1.0/24 exact;
                route-filter 192.168.1.0/26 exact;
            }
            then accept;
        }
    }
}
}
firewall {
    family inet {
        filter RE-FILTER {
            term CORE-BGP-ALLOWED {
                from {
                    source-address {
                        10.23.63.26/32;
                    }
                    protocol tcp;
                    ttl 254-255;
                    port bgp;
                }
                then {
                    count CORE-BGP-ALLOWED;
                    accept;
                }
            }
            term CORE-BGP-DENIED {
                from {
                    source-address {
                        10.23.63.26/32;
                    }
                }
            }
        }
    }
}
}

```



## VII.2 A stacioner hálózat forgalmi tervezésének eredményei

### VII.2.1 Összegző táblázatok

	128 Kbit/s	1 Mbit/s	10 Mbit/s
Élek telítettségének az átlaga	40,28%	74%	65,20%
Átlagos szabad kapacitás az éleken (Mbps)	13,88	6,37	7,07

### VII.2.2 Csomópontok táblázata

Csomópont azonosítója	Típusa	Státusz	Belső azonosító
K1	CORE	UP	0
K2	CORE	UP	1
TATA	EDGE	UP	2
V1	CORE	UP	3
GYOR	EDGE	UP	4
PAPA	EDGE	UP	5
V2	CORE	UP	6
V3	CORE	UP	7
V4	CORE	UP	8
SZEKESFEHERVAR	EDGE	UP	9
F1	CORE	UP	10
F2	CORE	UP	11
V5	CORE	UP	12
F3	CORE	UP	13
F4	CORE	UP	14
VARPALOTA	EDGE	UP	15
F6	CORE	UP	16
V6	CORE	UP	17
VESZPREM	EDGE	UP	18
V8	CORE	UP	19
F5	CORE	UP	20
KUP	CORE	UP	21
HEVIZ	EDGE	UP	22
Z1	CORE	UP	23
T1	CORE	UP	24
T2	CORE	UP	25
JUTA	EDGE	UP	26
T3	CORE	UP	27
F7	CORE	UP	28
F8	CORE	UP	29
B1	CORE	UP	30

Csomópont azonosítója	Típusa	Státusz	Belső azonosító
ZENGOVAR	EDGE	UP	31
PECSKORHAZ	EDGE	UP	32
MEDINA	EDGE	UP	33
F9	CORE	UP	34
BK1	CORE	UP	35
BK2	CORE	UP	36
BK3	CORE	UP	37
TABORFALVA	EDGE	UP	38
PUSZTAVACS	EDGE	UP	39
SZENTENDRE	EDGE	UP	40
BUDAPEST	EDGE	UP	41
P1	CORE	UP	42
NAGYTARCSA	EDGE	UP	43
P2	CORE	UP	44
N2	CORE	UP	45
N1	CORE	UP	46
P3	CORE	UP	47
KAL	EDGE	UP	48
EGER	EDGE	UP	49
BANKUT	EDGE	UP	50
BAZ1	CORE	UP	51
BAZ2	CORE	UP	52
HAJDUHADHAZ	EDGE	UP	53
DEBRECEN	EDGE	UP	54
DEBRECEN REPTER	EDGE	UP	55
JNSZ3	CORE	UP	56
JNSZ1	CORE	UP	57
HB1	CORE	UP	58
SZOLNOK	EDGE	UP	59
BTKK	EDGE	UP	60
KISKUNHALAS	EDGE	UP	61
BK4	CORE	UP	62
KECSKEMET	CORE	UP	63
VAROSFOLD	EDGE	UP	64
P4	CORE	UP	65
P5	CORE	UP	66
BE1	CORE	UP	67
BE2	CORE	UP	68
BE3	CORE	UP	69
SZENTES	EDGE	UP	70
HODMEZOVASARHELY	EDGE	UP	71
FURJE	EDGE	UP	72

## VII.2.3 Élek telítettsége 1 Mbit/s-s átlagos forgalom esetén

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
GYOR-V1	GYOR	V1	8,00	7,98	0,02	99,71%
V1-GYOR	V1	GYOR	8,00	5,51	2,49	68,91%
V1-V5	V1	V5	8,00	7,98	0,02	99,71%
V5-V1	V5	V1	8,00	7,92	0,08	98,96%
V5-Papa	V5	PAPA	16,00	10,34	5,66	64,63%
Papa-V5	PAPA	V5	16,00	14,64	1,36	91,52%
Papa-V2	PAPA	V2	16,00	14,33	1,67	89,57%
V2-Papa	V2	PAPA	16,00	14,07	1,93	87,92%
V2-V3	V2	V3	16,00	16,00	0,00	99,99%
V3-V2	V3	V2	16,00	15,42	0,58	96,35%
V3-V4	V3	V4	16,00	15,87	0,13	99,19%
V4-V3	V4	V3	16,00	15,98	0,02	99,85%
V4-SZFVAR	V4	SZEKESFEHER VAR	16,00	12,05	3,95	75,33%
SZFVAR-V4	SZEKESFEHER VAR	V4	16,00	12,61	3,39	78,82%
SZFVAR-F1	SZEKESFEHER VAR	F1	16,00	8,83	7,17	55,19%
F1-SZFVAR	F1	SZEKESFEHER VAR	16,00	14,80	1,20	92,47%
F1-K2	F1	K2	16,00	8,78	7,22	54,87%
K2-F1	K2	F1	16,00	14,80	1,20	92,47%
K2-V5	K2	V5	16,00	11,44	4,56	71,53%
V5-K2	V5	K2	16,00	15,95	0,05	99,66%
K2-K1	K2	K1	16,00	15,70	0,30	98,15%
K1-K2	K1	K2	16,00	15,84	0,16	99,03%
K1-TATA	K1	TATA	16,00	15,87	0,13	99,16%
TATA-K1	TATA	K1	16,00	10,55	5,45	65,93%
V4-V8	V4	V8	16,00	16,00	0,00	99,98%
V8-V4	V8	V4	16,00	13,12	2,88	82,00%
KUP-V2	KUP	V2	8,00	3,23	4,77	40,32%
V2-KUP	V2	KUP	8,00	0,72	7,28	9,01%
V3-VESZPREM	V3	VESZPREM	32,00	21,93	10,07	68,52%
VESZPREM-V6	VESZPREM	V6	32,00	19,03	12,97	59,46%
V6-VARPALOTA	V6	VARPALOTA	32,00	19,03	12,97	59,46%
VARPALOTA-F4	VARPALOTA	F4	32,00	20,92	11,08	65,39%
F4-F3	F4	F3	32,00	19,48	12,52	60,88%
F3-SZFVAR	F3	SZEKESFEHER VAR	32,00	21,66	10,34	67,68%
SZFVAR-F3	SZEKESFEHER VAR	F3	32,00	25,03	6,97	78,22%
F3-F4	F3	F4	32,00	24,92	7,08	77,87%
F4-VARPALOTA	F4	VARPALOTA	32,00	24,92	7,08	77,87%
VARPALOTA-V6	VARPALOTA	V6	32,00	16,70	15,30	52,18%
V6-VESZPREM	V6	VESZPREM	32,00	13,33	18,67	41,65%
VESZPREM-V3	VESZPREM	V3	32,00	16,90	15,10	52,81%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
F3-F6	F3	F6	8,00	0,79	7,21	9,94%
V3-Z1	V3	Z1	16,00	15,93	0,07	99,54%
Z1-V3	Z1	V3	16,00	15,96	0,04	99,76%
Z1-HEVIZ	Z1	HEVIZ	16,00	12,01	3,99	75,06%
HEVIZ-Z1	HEVIZ	Z1	16,00	11,03	4,97	68,91%
Z1-T1	Z1	T1	16,00	12,50	3,50	78,10%
T1-Z1	T1	Z1	16,00	11,94	4,06	74,61%
T1-T2	T1	T2	16,00	13,03	2,97	81,41%
T2-T1	T2	T1	16,00	11,94	4,06	74,61%
T2-T3	T2	T3	16,00	14,68	1,32	91,73%
T3-T2	T3	T2	16,00	15,33	0,67	95,79%
F5-SZFVAR	F5	SZEKESFEHER VAR	16,00	15,99	0,01	99,93%
SZFVAR-F5	SZEKESFEHER VAR	F5	16,00	15,91	0,09	99,45%
F5-F8	F5	F8	16,00	11,32	4,68	70,77%
F8-F5	F8	F5	16,00	15,99	0,01	99,93%
F8-F7	F8	F7	16,00	0,00	16,00	0,00%
F7-F8	F7	F8	16,00	1,90	14,10	11,88%
T2-JUTA	T2	JUTA	8,00	6,77	1,23	84,58%
JUTA-T2	JUTA	T2	8,00	7,78	0,22	97,28%
T3-F7	T3	F7	16,00	15,90	0,10	99,36%
F7-T3	F7	T3	16,00	15,33	0,67	95,79%
F7-V8	F7	V8	16,00	13,12	2,88	82,00%
V8-F7	V8	F7	16,00	13,61	2,39	85,06%
T2-B1	T2	B1	16,00	15,89	0,11	99,33%
B1-T2	B1	T2	16,00	15,44	0,56	96,48%
B1-ZENGOVAR	B1	ZENGOVAR	32,00	9,62	22,38	30,07%
ZENGOVAR-B1	ZENGOVAR	B1	32,00	5,65	26,35	17,65%
PECSKORHAZ-B1	PECSKORHAZ	B1	8,00	7,59	0,41	94,83%
B1-PECSKORHAZ	B1	PECSKORHAZ	8,00	7,46	0,54	93,29%
ZENGOVAR-MEDINA	ZENGOVAR	MEDINA	32,00	6,96	25,04	21,76%
MEDINA-ZENGOVAR	MEDINA	ZENGOVAR	32,00	8,73	23,27	27,27%
F8-F9	F8	F9	32,00	11,32	20,68	35,38%
F9-F8	F9	F8	32,00	15,99	16,01	49,96%
F9-F7	F9	F7	32,00	20,61	11,39	64,39%
F7-F9	F7	F9	32,00	20,24	11,76	63,25%
F9-BK2	F9	BK2	16,00	12,97	3,03	81,06%
BK2-F9	BK2	F9	16,00	16,00	0,00	99,98%
BK2-BK1	BK2	BK1	8,00	8,00	0,00	99,99%
BK1-BK2	BK1	BK2	8,00	4,25	3,75	53,07%
BK1-MEDINA	BK1	MEDINA	8,00	8,00	0,00	99,99%
MEDINA-BK1	MEDINA	BK1	8,00	1,55	9,55	19,37%
F9-BK3	F9	BK3	32,00	23,05	8,95	72,03%
BK3-F9	BK3	F9	32,00	25,05	6,95	78,28%



Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
BK3-TABORFALVA	BK3	TABORFALVA	32,00	23,05	8,95	72,03%
TABORFALVA-BK3	TABORFALVA	BK3	32,00	23,14	8,86	72,32%
TABORFALVA-PUSZTAVACS	TABORFALVA	PUSZTAVACS	32,00	13,55	18,45	42,35%
PUSZTAVACS-TABORFALVA	PUSZTAVACS	TABORFALVA	32,00	23,03	8,97	71,97%
SZFVAR-F2	SZEKESFEHERVAR	F2	32,00	31,37	0,63	98,04%
F2-SZFVAR	F2	SZEKESFEHERVAR	32,00	31,92	0,08	99,75%
K1-SZENTENDRE	K1	SZENTENDRE	16,00	15,69	0,31	98,05%
SZENTENDRE-K1	SZENTENDRE	K1	16,00	15,56	0,44	97,24%
F2-BUDAPEST	F2	BUDAPEST	32,00	31,65	0,35	98,90%
BUDAPEST-F2	BUDAPEST	F2	32,00	31,92	0,08	99,75%
BUDAPEST-SZENTENDRE	BUDAPEST	SZENTENDRE	32,00	22,93	9,07	71,65%
SZENTENDRE-BUDAPEST	SZENTENDRE	BUDAPEST	32,00	20,52	11,48	64,13%
BUDAPEST-P1	BUDAPEST	P1	8,00	3,25	4,75	40,57%
P1-BUDAPEST	P1	BUDAPEST	8,00	1,22	6,78	15,20%
BUDAPEST-NAGYTARCSA	BUDAPEST	NAGYTARCSA	16,00	15,72	0,28	98,23%
NAGYTARCSA-BUDAPEST	NAGYTARCSA	BUDAPEST	16,00	15,90	0,10	99,35%
BUDAPEST-P2	BUDAPEST	P2	16,00	16,00	0,00	99,97%
P2-BUDAPEST	P2	BUDAPEST	16,00	15,80	0,20	98,74%
SZENTENDRE-N1	SZENTENDRE	N1	16,00	15,99	0,01	99,94%
N1-SZENTENDRE	N1	SZENTENDRE	16,00	15,98	0,02	99,87%
N1-N2	N1	N2	16,00	15,09	0,91	94,32%
N2-N1	N2	N1	16,00	15,98	0,02	99,87%
P2-N2	P2	N2	32,00	27,76	4,24	86,76%
N2-P2	N2	P2	32,00	26,25	5,75	82,03%
NAGYTARCSA-PUSZTAVACS	NAGYTARCSA	PUSZTAVACS	16,00	15,98	0,02	99,85%
PUSZTAVACS-NAGYTARCSA	PUSZTAVACS	NAGYTARCSA	16,00	15,80	0,20	98,73%
NAGYTARCSA-P3	NAGYTARCSA	P3	16,00	15,82	0,18	98,88%
P3-NAGYTARCSA	P3	NAGYTARCSA	16,00	12,66	3,34	79,14%
P3-BUDAPEST	P3	BUDAPEST	16,00	13,29	2,71	83,06%
BUDAPEST-P3	BUDAPEST	P3	16,00	13,00	3,00	81,27%
P3-P2	P3	P2	16,00	16,00	0,00	99,99%
P2-P3	P2	P3	16,00	15,77	0,23	98,54%
N2-NAGYHARS	N2	KAL	8,00	6,36	1,64	79,45%
NAGYHARS-N2	KAL	N2	8,00	7,83	0,17	97,83%
N2-EGER	N2	EGER	16,00	15,86	0,14	99,12%
EGER-N2	EGER	N2	16,00	9,65	6,35	60,29%
N2-N3	N2	BANKUT	32,00	30,74	1,26	96,07%
N3-N2	BANKUT	N2	32,00	32,00	0,00	99,98%
BANKUT-BAZ2	BANKUT	BAZ2	32,00	31,87	0,13	99,60%
BAZ2-BANKUT	BAZ2	BANKUT	32,00	27,60	4,40	86,24%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
BAZ2-BAZ1	BAZ2	BAZ1	32,00	31,87	0,13	99,60%
BAZ1-BAZ2	BAZ1	BAZ2	32,00	27,50	4,50	85,94%
BAZ1-HAJDUHADHAZ	BAZ1	HAJDUHADHAZ	32,00	31,87	0,13	99,60%
HAJDUHADHAZ-BAZ1	HAJDUHADHAZ	BAZ1	32,00	28,61	3,39	89,39%
BK2-KISKUNHALAS	BK2	KISKUNHALAS	8,00	7,98	0,02	99,72%
KISKUNHALAS-BK2	KISKUNHALAS	BK2	8,00	5,41	2,59	67,63%
BK2-BK4	BK2	BK4	16,00	10,23	5,77	63,92%
BK4-BK2	BK4	BK2	16,00	13,94	2,06	87,13%
BK4-KECSKEMET	BK4	KECSKEMET	16,00	6,21	9,79	38,83%
KECSKEMET-BK4	KECSKEMET	BK4	16,00	5,39	10,61	33,70%
KECSKEMET-VAROSFOLD	KECSKEMET	VAROSFOLD	16,00	11,67	4,33	72,94%
VAROSFOLD-KECSKEMET	VAROSFOLD	KECSKEMET	16,00	13,21	2,79	82,58%
KECSKEMET-P4	KECSKEMET	P4	16,00	11,96	4,04	74,77%
P4-KECSKEMET	P4	KECSKEMET	16,00	7,62	8,38	47,59%
P4-P5	P4	P5	16,00	15,85	0,15	99,04%
P5-P4	P5	P4	16,00	13,57	2,43	84,80%
P5-N2	P5	N2	16,00	16,00	0,00	99,99%
N2-P5	N2	P5	16,00	15,88	0,12	99,22%
P4-SZOLNOK	P4	SZOLNOK	34,00	20,54	13,46	60,40%
SZOLNOK-P4	SZOLNOK	P4	34,00	14,98	19,02	44,06%
SZOLNOK-JNSZ1	SZOLNOK	JNSZ1	34,00	17,94	16,06	52,75%
JNSZ1-SZOLNOK	JNSZ1	SZOLNOK	34,00	23,56	10,44	69,29%
JNSZ1-JNSZ2	JNSZ1	HB1	34,00	18,58	15,42	54,65%
JNSZ2-JNSZ1	HB1	JNSZ1	34,00	23,56	10,44	69,29%
JNSZ2-DEBRECEN	HB1	DEBRECEN	34,00	18,40	15,60	54,12%
DEBRECEN-JNSZ2	DEBRECEN	HB1	34,00	23,56	10,44	69,29%
DEBRECEN-HAJDUHADHAZ	DEBRECEN	HAJDUHADHAZ	34,00	33,95	0,05	99,85%
HAJDUHADHAZ-DEBRECEN	HAJDUHADHAZ	DEBRECEN	34,00	33,37	0,63	98,16%
DEBRECEN-DEBRECEN REPTER	DEBRECEN	DEBRECEN REPTER	34,00	13,21	20,79	38,87%
DEBRECEN REPTER-DEBRECEN	DEBRECEN REPTER	DEBRECEN	34,00	14,67	19,33	43,14%
SZOLNOK-BTKK	SZOLNOK	BTKK	8,00	7,73	0,27	96,66%
BTKK-SZOLNOK	BTKK	SZOLNOK	8,00	7,99	0,01	99,86%
BK4-SZENTES	BK4	SZENTES	34,00	10,95	23,05	32,19%
SZENTES-BK4	SZENTES	BK4	34,00	14,63	19,37	43,04%
SZENTES-BE3	SZENTES	BE3	34,00	21,89	12,11	64,38%
BE3-SZENTES	BE3	SZENTES	34,00	20,15	13,85	59,26%
BE3-BE2	BE3	BE2	34,00	21,42	12,58	62,99%
BE2-BE3	BE2	BE3	34,00	20,15	13,85	59,26%
BE2-BE1	BE2	BE1	34,00	16,10	17,90	47,36%
BE1-BE2	BE1	BE2	34,00	16,52	17,48	48,58%
BE1-SZOLNOK	BE1	SZOLNOK	34,00	16,10	17,90	47,36%
SZOLNOK-BE1	SZOLNOK	BE1	34,00	16,52	17,48	48,58%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
SZENTES-HODMEZOVASARHELY	SZENTES	HODMEZOVASARHELY	8,00	4,08	3,92	51,04%
HODMEZOVASARHELY-SZENTES	HODMEZOVARHELY	SZENTES	8,00	7,71	0,29	96,35%
SZOLNOK-HB1	SZOLNOK	JNSZ3	34,00	0,00	34,00	0,00%
HB1-SZOLNOK	JNSZ3	SZOLNOK	34,00	0,00	34,00	0,00%
HB1-JNSZ1	JNSZ3	JNSZ1	34,00	0,00	34,00	0,00%
HB1-JNSZ1-1	JNSZ3	JNSZ1	34,00	0,00	34,00	0,00%
F6-F3	F6	F3	8,00	2,97	5,03	37,13%
BE2-FURJE	BE2	FURJE	8,00	7,39	0,61	92,32%
FURJE-BE2	FURJE	BE2	8,00	7,84	0,16	98,04%
				14,91	6,37	74%

## VII.2.4 Élek telítettsége 128 kbit/s-s átlagos forgalom esetén

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
GYOR-V1	GYOR	V1	8,00	3,69	4,31	46,14%
V1-GYOR	V1	GYOR	8,00	3,59	4,41	44,91%
V1-V5	V1	V5	8,00	3,69	4,31	46,14%
V5-V1	V5	V1	8,00	6,00	2,00	74,96%
V5-Papa	V5	PAPA	16,00	3,68	12,32	22,97%
Papa-V5	PAPA	V5	16,00	6,19	9,81	38,66%
Papa-V2	PAPA	V2	16,00	3,37	12,63	21,03%
V2-Papa	V2	PAPA	16,00	6,09	9,91	38,09%
V2-V3	V2	V3	16,00	5,03	10,97	31,46%
V3-V2	V3	V2	16,00	7,44	8,56	46,52%
V3-V4	V3	V4	16,00	12,74	3,26	79,60%
V4-V3	V4	V3	16,00	9,39	6,61	58,68%
V4-SZFVAR	V4	SZEKESFEHERVAR	16,00	8,28	7,72	51,77%
SZFVAR-V4	SZEKESFEHERVAR	V4	16,00	5,07	10,93	31,70%
SZFVAR-F1	SZEKESFEHERVAR	F1	16,00	3,31	12,69	20,67%
F1-SZFVAR	F1	SZEKESFEHERVAR	16,00	4,30	11,70	26,84%
F1-K2	F1	K2	16,00	3,26	12,74	20,34%
K2-F1	K2	F1	16,00	4,30	11,70	26,84%
K2-V5	K2	V5	16,00	7,29	8,71	45,53%
V5-K2	V5	K2	16,00	7,63	8,37	47,68%
K2-K1	K2	K1	16,00	6,95	9,05	43,43%
K1-K2	K1	K2	16,00	6,27	9,73	39,19%
K1-TATA	K1	TATA	16,00	9,14	6,86	57,10%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
TATA-K1	TATA	K1	16,00	3,32	12,68	20,72%
V4-V8	V4	V8	16,00	9,37	6,63	58,57%
V8-V4	V8	V4	16,00	6,81	9,19	42,57%
KUP-V2	KUP	V2	8,00	3,23	4,77	40,32%
V2-KUP	V2	KUP	8,00	0,72	7,28	9,01%
V3-VESZPREM	V3	VESZPREM	32,00	5,88	26,12	18,37%
VESZPREM-V6	VESZPREM	V6	32,00	3,26	28,74	10,19%
V6-VARPALOTA	V6	VARPALOTA	32,00	3,26	28,74	10,19%
VARPALOTA-F4	VARPALOTA	F4	32,00	4,66	27,34	14,55%
F4-F3	F4	F3	32,00	3,22	28,78	10,05%
F3-SZFVAR	F3	SZEKESFEHER VAR	32,00	5,39	26,61	16,85%
SZFVAR-F3	SZEKESFEHER VAR	F3	32,00	12,59	19,41	39,34%
F3-F4	F3	F4	32,00	12,48	19,52	38,99%
F4-VARPALOTA	F4	VARPALOTA	32,00	12,48	19,52	38,99%
VARPALOTA-V6	VARPALOTA	V6	32,00	6,21	25,79	19,40%
V6-VESZPREM	V6	VESZPREM	32,00	2,84	29,16	8,87%
VESZPREM-V3	VESZPREM	V3	32,00	4,57	27,43	14,30%
F3-F6	F3	F6	8,00	0,79	7,21	9,94%
V3-Z1	V3	Z1	16,00	7,17	8,83	44,83%
Z1-V3	Z1	V3	16,00	9,93	6,07	62,05%
Z1-HEVIZ	Z1	HEVIZ	16,00	5,67	10,33	35,47%
HEVIZ-Z1	HEVIZ	Z1	16,00	5,48	10,52	34,27%
Z1-T1	Z1	T1	16,00	4,64	11,36	28,97%
T1-Z1	T1	Z1	16,00	6,01	9,99	37,53%
T1-T2	T1	T2	16,00	5,16	10,84	32,28%
T2-T1	T2	T1	16,00	6,01	9,99	37,53%
T2-T3	T2	T3	16,00	7,87	8,13	49,21%
T3-T2	T3	T2	16,00	11,55	4,45	72,19%
F5-SZFVAR	F5	SZEKESFEHER VAR	16,00	3,97	12,03	24,79%
SZFVAR-F5	SZEKESFEHER VAR	F5	16,00	6,07	9,93	37,93%
F5-F8	F5	F8	16,00	1,48	14,52	9,25%
F8-F5	F8	F5	16,00	3,97	12,03	24,79%
F8-F7	F8	F7	16,00	0,00	16,00	0,00%
F7-F8	F7	F8	16,00	2,01	13,99	12,55%
T2-JUTA	T2	JUTA	8,00	6,90	1,10	86,28%
JUTA-T2	JUTA	T2	8,00	6,05	1,95	75,63%
T3-F7	T3	F7	16,00	9,09	6,91	56,84%
F7-T3	F7	T3	16,00	11,55	4,45	72,19%
F7-V8	F7	V8	16,00	6,81	9,19	42,57%
V8-F7	V8	F7	16,00	6,98	9,02	43,64%
T2-B1	T2	B1	16,00	9,30	6,70	58,11%
B1-T2	B1	T2	16,00	9,61	6,39	60,06%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
B1-ZENGOVAR	B1	ZENGOVAR	32,00	5,55	26,45	17,35%
ZENGOVAR-B1	ZENGOVAR	B1	32,00	5,79	26,21	18,11%
PECSKORHAZ-B1	PECSKORHAZ	B1	8,00	3,28	4,72	40,98%
B1-PECSKORHAZ	B1	PECSKORHAZ	8,00	6,60	1,40	82,54%
ZENGOVAR-MEDINA	ZENGOVAR	MEDINA	32,00	4,68	27,32	14,62%
MEDINA-ZENGOVAR	MEDINA	ZENGOVAR	32,00	4,95	27,05	15,46%
F8-F9	F8	F9	32,00	1,48	30,52	4,62%
F9-F8	F9	F8	32,00	3,86	28,14	12,06%
F9-F7	F9	F7	32,00	14,96	17,04	46,76%
F7-F9	F7	F9	32,00	11,15	20,85	34,83%
F9-BK2	F9	BK2	16,00	12,28	3,72	76,75%
BK2-F9	BK2	F9	16,00	14,10	1,90	88,10%
BK2-BK1	BK2	BK1	8,00	7,21	0,79	90,06%
BK1-BK2	BK1	BK2	8,00	7,98	0,02	99,80%
BK1-MEDINA	BK1	MEDINA	8,00	7,21	0,79	90,06%
MEDINA-BK1	MEDINA	BK1	8,00	2,19	5,81	27,36%
F9-BK3	F9	BK3	32,00	11,10	20,90	34,70%
BK3-F9	BK3	F9	32,00	15,48	16,52	48,39%
BK3-TABORFALVA	BK3	TABORFALVA	32,00	11,10	20,90	34,70%
TABORFALVA-BK3	TABORFALVA	BK3	32,00	13,58	18,42	42,43%
TABORFALVA-PUSZTAVACS	TABORFALVA	PUSZTAVACS	32,00	10,57	21,43	33,05%
PUSZTAVACS-TABORFALVA	PUSZTAVACS	TABORFALVA	32,00	12,77	19,23	39,89%
SZFVAR-F2	SZEKESFEHESZFVAR	F2	32,00	13,50	18,50	42,19%
F2-SZFVAR	F2	SZEKESFEHERSZFVAR	32,00	16,89	15,11	52,78%
K1-SZENTENDRE	K1	SZENTENDRE	16,00	9,64	6,36	60,23%
SZENTENDRE-K1	SZENTENDRE	K1	16,00	9,19	6,81	57,45%
F2-BUDAPEST	F2	BUDAPEST	32,00	13,78	18,22	43,05%
BUDAPEST-F2	BUDAPEST	F2	32,00	16,89	15,11	52,78%
BUDAPEST-SZENTENDRE	BUDAPEST	SZENTENDRE	32,00	6,19	25,81	19,35%
SZENTENDRE-BUDAPEST	SZENTENDRE	BUDAPEST	32,00	6,16	25,84	19,26%
BUDAPEST-P1	BUDAPEST	P1	8,00	3,25	4,75	40,57%
P1-BUDAPEST	P1	BUDAPEST	8,00	1,22	6,78	15,20%
BUDAPEST-NAGYTARCSA	BUDAPEST	NAGYTARCSA	16,00	11,30	4,70	70,65%
NAGYTARCSA-BUDAPEST	NAGYTARCSA	BUDAPEST	16,00	12,12	3,88	75,73%
BUDAPEST-P2	BUDAPEST	P2	16,00	13,38	2,62	83,61%
P2-BUDAPEST	P2	BUDAPEST	16,00	11,78	4,22	73,63%
SZENTENDRE-N1	SZENTENDRE	N1	16,00	8,61	7,39	53,82%
N1-SZENTENDRE	N1	SZENTENDRE	16,00	7,45	8,55	46,59%
N1-N2	N1	N2	16,00	7,71	8,29	48,21%
N2-N1	N2	N1	16,00	7,45	8,55	46,59%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
P2-N2	P2	N2	32,00	13,87	18,13	43,34%
N2-P2	N2	P2	32,00	13,80	18,20	43,11%
NAGYTARCSA-PUSZTAVACS	NAGYTARCSA	PUSZTAVACS	16,00	13,21	2,79	82,57%
PUSZTAVACS-NAGYTARCSA	PUSZTAVACS	NAGYTARCSA	16,00	11,91	4,09	74,45%
NAGYTARCSA-P3	NAGYTARCSA	P3	16,00	3,22	12,78	20,14%
P3-NAGYTARCSA	P3	NAGYTARCSA	16,00	6,35	9,65	39,72%
P3-BUDAPEST	P3	BUDAPEST	16,00	4,59	11,41	28,68%
BUDAPEST-P3	BUDAPEST	P3	16,00	7,75	8,25	48,45%
P3-P2	P3	P2	16,00	4,72	11,28	29,52%
P2-P3	P2	P3	16,00	7,33	8,67	45,81%
N2-NAGYHARS	N2	KAL	8,00	6,97	1,03	87,17%
NAGYHARS-N2	KAL	N2	8,00	5,26	2,74	65,79%
N2-EGER	N2	EGER	16,00	7,79	8,21	48,68%
EGER-N2	EGER	N2	16,00	4,75	11,25	29,66%
N2-N3	N2	BANKUT	32,00	11,62	20,38	36,31%
N3-N2	BANKUT	N2	32,00	12,35	19,65	38,60%
BANKUT-BAZ2	BANKUT	BAZ2	32,00	9,62	22,38	30,07%
BAZ2-BANKUT	BAZ2	BANKUT	32,00	9,71	22,29	30,33%
BAZ2-BAZ1	BAZ2	BAZ1	32,00	9,62	22,38	30,07%
BAZ1-BAZ2	BAZ1	BAZ2	32,00	9,61	22,39	30,03%
BAZ1-HAJDUHADHAZ	BAZ1	HAJDUHADHAZ	32,00	9,62	22,38	30,07%
HAJDUHADHAZ-BAZ1	HAJDUHADHAZ	BAZ1	32,00	10,72	21,28	33,48%
BK2-KISKUNHALAS	BK2	KISKUNHALAS	8,00	7,96	0,04	99,51%
KISKUNHALAS-BK2	KISKUNHALAS	BK2	8,00	6,20	1,80	77,55%
BK2-BK4	BK2	BK4	16,00	13,46	2,54	84,10%
BK4-BK2	BK4	BK2	16,00	10,61	5,39	66,34%
BK4-KECSKEMET	BK4	KECSKEMET	16,00	5,24	10,76	32,75%
KECSKEMET-BK4	KECSKEMET	BK4	16,00	2,88	13,12	18,03%
KECSKEMET-VAROSFOLD	KECSKEMET	VAROSFOLD	16,00	6,56	9,44	41,03%
VAROSFOLD-KECSKEMET	VAROSFOLD	KECSKEMET	16,00	3,40	12,60	21,24%
KECSKEMET-P4	KECSKEMET	P4	16,00	5,16	10,84	32,24%
P4-KECSKEMET	P4	KECSKEMET	16,00	3,98	12,02	24,90%
P4-P5	P4	P5	16,00	11,35	4,65	70,97%
P5-P4	P5	P4	16,00	8,25	7,75	51,59%
P5-N2	P5	N2	16,00	11,51	4,49	71,92%
N2-P5	N2	P5	16,00	10,56	5,44	66,01%
P4-SZOLNOK	P4	SZOLNOK	34,00	8,96	25,04	26,34%
SZOLNOK-P4	SZOLNOK	P4	34,00	7,40	26,60	21,76%
SZOLNOK-JNSZ1	SZOLNOK	JNSZ1	34,00	6,05	27,95	17,79%
JNSZ1-SZOLNOK	JNSZ1	SZOLNOK	34,00	8,39	25,61	24,67%
JNSZ1-JNSZ2	JNSZ1	HB1	34,00	6,69	27,31	19,68%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
JNSZ2-JNSZ1	HB1	JNSZ1	34,00	8,39	25,61	24,67%
JNSZ2-DEBRECEN	HB1	DEBRECEN	34,00	6,51	27,49	19,16%
DEBRECEN-JNSZ2	DEBRECEN	HB1	34,00	8,39	25,61	24,67%
DEBRECEN-HAJDUHADHAZ	DEBRECEN	HAJDUHADHAZ	34,00	10,84	23,16	31,89%
HAJDUHADHAZ-DEBRECEN	HAJDUHADHAZ	DEBRECEN	34,00	9,44	24,56	27,78%
DEBRECEN-DEBRECEN REPTER	DEBRECEN	DEBRECEN REPTER	34,00	3,76	30,24	11,05%
DEBRECEN REPTER - DEBRECEN	DEBRECEN REPTER	DEBRECEN	34,00	5,78	28,22	16,99%
SZOLNOK-BTKK	SZOLNOK	BTKK	8,00	5,28	2,72	65,96%
BTKK-SZOLNOK	BTKK	SZOLNOK	8,00	7,02	0,98	87,76%
BK4-SZENTES	BK4	SZENTES	34,00	11,95	22,05	35,15%
SZENTES-BK4	SZENTES	BK4	34,00	10,62	23,38	31,23%
SZENTES-BE3	SZENTES	BE3	34,00	9,32	24,68	27,40%
BE3-SZENTES	BE3	SZENTES	34,00	11,47	22,53	33,72%
BE3-BE2	BE3	BE2	34,00	8,84	25,16	26,01%
BE2-BE3	BE2	BE3	34,00	11,47	22,53	33,72%
BE2-BE1	BE2	BE1	34,00	8,64	25,36	25,42%
BE1-BE2	BE1	BE2	34,00	11,32	22,68	33,30%
BE1-SZOLNOK	BE1	SZOLNOK	34,00	8,64	25,36	25,42%
SZOLNOK-BE1	SZOLNOK	BE1	34,00	11,32	22,68	33,30%
SZENTES-HODMEZOVARHELY	SZENTES	HODMEZOVARHELY	8,00	3,81	4,19	47,64%
HODMEZOVARHELY-SZENTES	HODMEZOVARHELY	SZENTES	8,00	3,65	4,35	45,65%
SZOLNOK-HB1	SZOLNOK	JNSZ3	34,00	0,00	34,00	0,00%
HB1-SZOLNOK	JNSZ3	SZOLNOK	34,00	0,00	34,00	0,00%
HB1-JNSZ1	JNSZ3	JNSZ1	34,00	0,00	34,00	0,00%
HB1-JNSZ1-1	JNSZ3	JNSZ1	34,00	0,00	34,00	0,00%
F6-F3	F6	F3	8,00	2,97	5,03	37,13%
BE2-FURJE	BE2	FURJE	8,00	5,07	2,93	63,32%
FURJE-BE2	FURJE	BE2	8,00	5,64	2,36	70,55%
				7,38	13,88	40,28%

## VII.2.5 Élek telítettsége 10 Mbit/s-s átlagos forgalom esetén

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
GYOR-V1	GYOR	V1	8,00	0,00	8,00	0,00%
V1-GYOR	V1	GYOR	8,00	0,17	7,83	2,11%
V1-V5	V1	V5	8,00	0,00	8,00	0,00%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
V5-V1	V5	V1	8,00	2,57	5,43	32,16%
V5-Papa	V5	PAPA	16,00	12,87	3,13	80,41%
Papa-V5	PAPA	V5	16,00	15,26	0,74	95,38%
Papa-V2	PAPA	V2	16,00	12,72	3,28	79,50%
V2-Papa	V2	PAPA	16,00	13,55	2,45	84,68%
V2-V3	V2	V3	16,00	14,39	1,61	89,93%
V3-V2	V3	V2	16,00	14,90	1,10	93,11%
V3-V4	V3	V4	16,00	14,68	1,32	91,73%
V4-V3	V4	V3	16,00	14,41	1,59	90,04%
V4-SZFVAR	V4	SZEKESFEHERVA R	16,00	13,38	2,62	83,64%
SZFVAR-V4	SZEKESFEHE RVAR	V4	16,00	11,98	4,02	74,89%
SZFVAR-F1	SZEKESFEHE RVAR	F1	16,00	2,75	13,25	17,18%
F1-SZFVAR	F1	SZEKESFEHERVA R	16,00	3,62	12,38	22,59%
F1-K2	F1	K2	16,00	2,70	13,30	16,86%
K2-F1	K2	F1	16,00	3,62	12,38	22,59%
K2-V5	K2	V5	16,00	15,13	0,87	94,57%
V5-K2	V5	K2	16,00	15,09	0,91	94,32%
K2-K1	K2	K1	16,00	15,09	0,91	94,32%
K1-K2	K1	K2	16,00	14,67	1,33	91,71%
K1-TATA	K1	TATA	16,00	5,58	10,42	34,86%
TATA-K1	TATA	K1	16,00	12,00	4,00	75,00%
V4-V8	V4	V8	16,00	14,68	1,32	91,73%
V8-V4	V8	V4	16,00	13,38	2,62	83,64%
KUP-V2	KUP	V2	8,00	3,23	4,77	40,32%
V2-KUP	V2	KUP	8,00	0,72	7,28	9,01%
V3-VESZPREM	V3	VESZPREM	32,00	25,24	6,76	78,86%
VESZPREM-V6	VESZPREM	V6	32,00	25,24	6,76	78,86%
V6-VARPALOTA	V6	VARPALOTA	32,00	25,24	6,76	78,86%
VARPALOTA-F4	VARPALOTA	F4	32,00	28,24	3,76	88,24%
F4-F3	F4	F3	32,00	26,79	5,21	83,73%
F3-SZFVAR	F3	SZEKESFEHERVA R	32,00	28,97	3,03	90,53%
SZFVAR-F3	SZEKESFEHE RVAR	F3	32,00	24,30	7,70	75,92%
F3-F4	F3	F4	32,00	24,18	7,82	75,57%
F4-VARPALOTA	F4	VARPALOTA	32,00	24,18	7,82	75,57%
VARPALOTA-V6	VARPALOTA	V6	32,00	31,38	0,62	98,07%
V6-VESZPREM	V6	VESZPREM	32,00	28,01	3,99	87,54%
VESZPREM-V3	VESZPREM	V3	32,00	21,46	10,54	67,05%
F3-F6	F3	F6	8,00	0,79	7,21	9,94%
V3-Z1	V3	Z1	16,00	15,19	0,81	94,91%
Z1-V3	Z1	V3	16,00	15,44	0,56	96,50%
Z1-HEVIZ	Z1	HEVIZ	16,00	2,19	13,81	13,66%



Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
HEVIZ-Z1	HEVIZ	Z1	16,00	2,03	13,97	12,69%
Z1-T1	Z1	T1	16,00	15,03	0,97	93,94%
T1-Z1	T1	Z1	16,00	13,86	2,14	86,65%
T1-T2	T1	T2	16,00	15,56	0,44	97,25%
T2-T1	T2	T1	16,00	13,86	2,14	86,65%
T2-T3	T2	T3	16,00	1,97	14,03	12,29%
T3-T2	T3	T2	16,00	5,06	10,94	31,60%
F5-SZFVAR	F5	SZEKESFEHERVA R	16,00	13,02	2,98	81,37%
SZFVAR-F5	SZEKESFEHE RVAR	F5	16,00	15,59	0,41	97,43%
F5-F8	F5	F8	16,00	11,00	5,00	68,75%
F8-F5	F8	F5	16,00	13,02	2,98	81,37%
F8-F7	F8	F7	16,00	0,00	16,00	0,00%
F7-F8	F7	F8	16,00	1,90	14,10	11,88%
T2-JUTA	T2	JUTA	8,00	3,49	4,51	43,66%
JUTA-T2	JUTA	T2	8,00	2,54	5,46	31,78%
T3-F7	T3	F7	16,00	3,19	12,81	19,92%
F7-T3	F7	T3	16,00	5,06	10,94	31,60%
F7-V8	F7	V8	16,00	13,38	2,62	83,64%
V8-F7	V8	F7	16,00	12,29	3,71	76,80%
T2-B1	T2	B1	16,00	15,93	0,07	99,58%
B1-T2	B1	T2	16,00	14,39	1,61	89,96%
B1-ZENGOVAR	B1	ZENGOVAR	32,00	13,00	19,00	40,63%
ZENGOVAR-B1	ZENGOVAR	B1	32,00	11,00	21,00	34,38%
PECSKORHAZ-B1	PECSKORHA Z	B1	8,00	0,00	8,00	0,00%
B1-PECSKORHAZ	B1	PECSKORHAZ	8,00	2,93	5,07	36,66%
ZENGOVAR-MEDINA	ZENGOVAR	MEDINA	32,00	5,00	27,00	15,63%
MEDINA-ZENGOVAR	MEDINA	ZENGOVAR	32,00	10,00	22,00	31,25%
F8-F9	F8	F9	32,00	11,00	21,00	34,38%
F9-F8	F9	F8	32,00	13,02	18,98	40,68%
F9-F7	F9	F7	32,00	15,58	16,42	48,67%
F7-F9	F7	F9	32,00	11,19	20,81	34,96%
F9-BK2	F9	BK2	16,00	15,27	0,73	95,42%
BK2-F9	BK2	F9	16,00	15,69	0,31	98,05%
BK2-BK1	BK2	BK1	8,00	7,39	0,61	92,42%
BK1-BK2	BK1	BK2	8,00	5,80	2,20	72,46%
BK1-MEDINA	BK1	MEDINA	8,00	7,39	0,61	92,42%
MEDINA-BK1	MEDINA	BK1	8,00	0,00	8,00	0,02%
F9-BK3	F9	BK3	32,00	11,19	20,81	34,96%
BK3-F9	BK3	F9	32,00	17,17	14,83	53,66%
BK3-TABORFALVA	BK3	TABORFALVA	32,00	11,19	20,81	34,96%
TABORFALVA-BK3	TABORFALVA	BK3	32,00	15,27	16,73	47,71%
TABORFALVA- PUSZTAVACS	TABORFALVA	PUSZTAVACS	32,00	25,19	6,81	78,71%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
PUSZTAVACS-TABORFALVA	PUSZTAVACS	TABORFALVA	32,00	22,27	9,73	69,58%
SZFVAR-F2	SZEKESFEHERVAR	F2	32,00	31,59	0,41	98,70%
F2-SZFVAR	F2	SZEKESFEHERVAR	32,00	31,61	0,39	98,77%
K1-SZENTENDRE	K1	SZENTENDRE	16,00	14,91	1,09	93,21%
SZENTENDRE-K1	SZENTENDRE	K1	16,00	2,49	13,51	15,54%
F2-BUDAPEST	F2	BUDAPEST	32,00	31,86	0,14	99,56%
BUDAPEST-F2	BUDAPEST	F2	32,00	31,61	0,39	98,77%
BUDAPEST-SZENTENDRE	BUDAPEST	SZENTENDRE	32,00	30,87	1,13	96,48%
SZENTENDRE-BUDAPEST	SZENTENDRE	BUDAPEST	32,00	30,56	1,44	95,50%
BUDAPEST-P1	BUDAPEST	P1	8,00	3,25	4,75	40,57%
P1-BUDAPEST	P1	BUDAPEST	8,00	1,22	6,78	15,20%
BUDAPEST-NAGYTARCSA	BUDAPEST	NAGYTARCSA	16,00	15,42	0,58	96,37%
NAGYTARCSA-BUDAPEST	NAGYTARCSA	BUDAPEST	16,00	15,14	0,86	94,61%
BUDAPEST-P2	BUDAPEST	P2	16,00	12,62	3,38	78,87%
P2-BUDAPEST	P2	BUDAPEST	16,00	9,80	6,20	61,25%
SZENTENDRE-N1	SZENTENDRE	N1	16,00	13,64	2,36	85,26%
N1-SZENTENDRE	N1	SZENTENDRE	16,00	13,06	2,94	81,60%
N1-N2	N1	N2	16,00	12,74	3,26	79,64%
N2-N1	N2	N1	16,00	13,06	2,94	81,60%
P2-N2	P2	N2	32,00	12,53	19,47	39,14%
N2-P2	N2	P2	32,00	9,07	22,93	28,36%
NAGYTARCSA-PUSZTAVACS	NAGYTARCSA	PUSZTAVACS	16,00	15,42	0,58	96,37%
PUSZTAVACS-NAGYTARCSA	PUSZTAVACS	NAGYTARCSA	16,00	15,14	0,86	94,61%
NAGYTARCSA-P3	NAGYTARCSA	P3	16,00	11,64	4,36	72,73%
P3-NAGYTARCSA	P3	NAGYTARCSA	16,00	11,62	4,38	72,59%
P3-BUDAPEST	P3	BUDAPEST	16,00	13,59	2,41	84,93%
BUDAPEST-P3	BUDAPEST	P3	16,00	15,75	0,25	98,45%
P3-P2	P3	P2	16,00	4,14	11,86	25,86%
P2-P3	P2	P3	16,00	4,59	11,41	28,68%
N2-NAGYHARS	N2	KAL	8,00	3,45	4,55	43,12%
NAGYHARS-N2	KAL	N2	8,00	6,90	1,10	86,29%
N2-EGER	N2	EGER	16,00	12,09	3,91	75,57%
EGER-N2	EGER	N2	16,00	12,20	3,80	76,24%
N2-N3	N2	BANKUT	32,00	29,36	2,64	91,75%
N3-N2	BANKUT	N2	32,00	20,09	11,91	62,79%
BANKUT-BAZ2	BANKUT	BAZ2	32,00	21,20	10,80	66,24%
BAZ2-BANKUT	BAZ2	BANKUT	32,00	30,09	1,91	94,04%
BAZ2-BAZ1	BAZ2	BAZ1	32,00	21,20	10,80	66,24%
BAZ1-BAZ2	BAZ1	BAZ2	32,00	30,00	2,00	93,74%
BAZ1-	BAZ1	HAJDUHADHAZ	32,00	21,20	10,80	66,24%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
HAJDUHADHAZ						
HAJDUHADHAZ-BAZ1	HAJDUHADH AZ	BAZ1	32,00	31,10	0,90	97,19%
BK2-KISKUNHALAS	BK2	KISKUNHALAS	8,00	5,93	2,07	74,09%
KISKUNHALAS-BK2	KISKUNHALA S	BK2	8,00	2,49	5,51	31,14%
BK2-BK4	BK2	BK4	16,00	14,07	1,93	87,94%
BK4-BK2	BK4	BK2	16,00	13,89	2,11	86,80%
BK4-KECSKEMET	BK4	KECSKEMET	16,00	10,01	5,99	62,57%
KECSKEMET-BK4	KECSKEMET	BK4	16,00	15,89	0,11	99,30%
KECSKEMET-VAROSFOLD	KECSKEMET	VAROSFOLD	16,00	15,06	0,94	94,11%
VAROSFOLD-KECSKEMET	VAROSFOLD	KECSKEMET	16,00	15,00	1,00	93,75%
KECSKEMET-P4	KECSKEMET	P4	16,00	3,25	12,75	20,34%
P4-KECSKEMET	P4	KECSKEMET	16,00	7,20	8,80	45,02%
P4-P5	P4	P5	16,00	15,07	0,93	94,22%
P5-P4	P5	P4	16,00	13,09	2,91	81,82%
P5-N2	P5	N2	16,00	15,23	0,77	95,18%
N2-P5	N2	P5	16,00	15,40	0,60	96,24%
P4-SZOLNOK	P4	SZOLNOK	34,00	14,25	19,75	41,92%
SZOLNOK-P4	SZOLNOK	P4	34,00	16,70	17,30	49,13%
SZOLNOK-JNSZ1	SZOLNOK	JNSZ1	34,00	29,27	4,73	86,09%
JNSZ1-SZOLNOK	JNSZ1	SZOLNOK	34,00	32,20	1,80	94,70%
JNSZ1-JNSZ2	JNSZ1	HB1	34,00	29,91	4,09	87,98%
JNSZ2-JNSZ1	HB1	JNSZ1	34,00	32,20	1,80	94,70%
JNSZ2-DEBRECEN	HB1	DEBRECEN	34,00	29,73	4,27	87,45%
DEBRECEN-JNSZ2	DEBRECEN	HB1	34,00	32,20	1,80	94,70%
DEBRECEN-HAJDUHADHAZ	DEBRECEN	HAJDUHADHAZ	34,00	30,65	3,35	90,15%
HAJDUHADHAZ-DEBRECEN	HAJDUHADH AZ	DEBRECEN	34,00	31,20	2,80	91,76%
DEBRECEN-DEBRECEN REPTER	DEBRECEN	DEBRECEN REPTER	34,00	8,32	25,68	24,46%
DEBRECEN REPTER - DEBRECEN	DEBRECEN REPTER	DEBRECEN	34,00	22,28	11,72	65,53%
SZOLNOK-BTKK	SZOLNOK	BTKK	8,00	7,69	0,31	96,16%
BTKK-SZOLNOK	BTKK	SZOLNOK	8,00	3,58	4,42	44,72%
BK4-SZENTES	BK4	SZENTES	34,00	28,95	5,05	85,14%
SZENTES-BK4	SZENTES	BK4	34,00	22,05	11,95	64,84%
SZENTES-BE3	SZENTES	BE3	34,00	33,39	0,61	98,21%
BE3-SZENTES	BE3	SZENTES	34,00	17,20	16,80	50,58%
BE3-BE2	BE3	BE2	34,00	32,92	1,08	96,82%
BE2-BE3	BE2	BE3	34,00	17,20	16,80	50,58%
BE2-BE1	BE2	BE1	34,00	33,88	0,12	99,64%
BE1-BE2	BE1	BE2	34,00	13,20	20,80	38,82%
BE1-SZOLNOK	BE1	SZOLNOK	34,00	33,88	0,12	99,64%
SZOLNOK-BE1	SZOLNOK	BE1	34,00	13,20	20,80	38,82%
SZENTES-	SZENTES	HODMEZOVASARH	8,00	7,59	0,41	94,81%

Élazonosító	Indulócsomópont azonosítója	Végcsomópont azonosítója	Sávszélesség [Mbit/s]	Fenntartott sávszélesség	Fenntartható sávszélesség	Telítettség
HODMEZOVASARHELY		ELY				
HODMEZOVASARHELY-SZENTES	HODMEZOVA SARHELY	SZENTES	8,00	7,18	0,82	89,74%
SZOLNOK-HB1	SZOLNOK	JNSZ3	34,00	0,00	34,00	0,00%
HB1-SZOLNOK	JNSZ3	SZOLNOK	34,00	0,00	34,00	0,00%
HB1-JNSZ1	JNSZ3	JNSZ1	34,00	0,00	34,00	0,00%
HB1-JNSZ1-1	JNSZ3	JNSZ1	34,00	0,00	34,00	0,00%
F6-F3	F6	F3	8,00	2,97	5,03	37,13%
BE2-FURJE	BE2	FURJE	8,00	1,54	6,46	19,25%
FURJE-BE2	FURJE	BE2	8,00	7,14	0,86	89,24%
				14,20	7,07	65,20%

## VII.2.6 Forgalmi utak táblázatai







Útvonal azonosító	Induló csomópont	Végződő csomópont	Sávzárlat [Mb]	Útvonal	BK1	BK2	BK3	BK4	SZENTES	BE3	BE2	BE1	SZOLI	BTKK	HB1	DEBRECEN	HAJDUHADHAZ	HODMEZOVASARHELY	SZENTENDRE	K1	TATA
LSP-1523206633	MEDINA	KISKUNHALAS	0,13 >	MEDINA	BK1	BK2	KISKUNHALAS														
LSP-1617154250	ZENGOVAR	BTKK	0,13 >	ZENGOVAR	MEDINA	BK1		BK4	SZENTES	BE3	BE2	BE1	SZOLI	BTKK							
LSP-713715542	JUTA	PECSKORHAZ	0,13 >	JUTA	T2	B1	PECSKORHAZ														
LSP-210700923	ZENGOVAR	HAJDUHADHAZ	0,13 >	ZENGOVAR	MEDINA	BK1	BK2	BK4	SZENTES	BE3	BE2	BE1	SZOLI	JNSZ1	HB1	DEBRECEN	HAJDUHADHAZ				
LSP-583162509	GYOR	HODMEZOVASARHELY	0,13 >	GYOR	V1	V5	K2	F1	SZEKESFEHERVAI	F5	F8	F9	BK2	BK4	SZENTES						
LSP-1347256308	TABORFALVA	SZENTES	0,13 >	TABORFALVA	BK3	F9	BK2	BK4	SZENTES												
LSP-782258379	FURJE	NAGYTARCSA	0,13 >	FURJE	BE2	BE1	SZOLNOK	P4	P5	N2	P2	BUDAPEST	NAGYTARCSA								
LSP-149319526	VAROSFOLD	VARPALOTA	0,13 >	VAROSFOLD	KECSKEMET	BK4	BK2	F9	F8	F5	SZEKESFEHERVAR	F3	F4	VARPALOTA							
LSP-984312444	MEDINA	TATA	0,13 >	MEDINA	ZENGOVAR	B1	T2	T3	F7	F9	BK3	TABORFALVA	PUSZTAVACS	NAGYTARCSA	BUDAPEST	SZENTENDRE	K1				> TATA
LSP-1424677318	KISKUNHALAS	TABORFALVA	0,13 >	KISKUNHALAS	BK2	F9	BK3	TABORFALVA													
LSP-1612342569	HEVIZ	SZEKESFEHERVAR	0,13 >	HEVIZ	Z1	V3	V4	SZEKESFEHERVAR													
LSP-109279141	DEBRECEN	FURJE	0,13 >	DEBRECEN	HB1	JNSZ1	SZOLNOK	BE1	BE2	FURJE											
LSP-1908158272	SZENTES	ZENGOVAR	0,13 >	SZENTES	BK4	BK2	BK1	MEDINA	ZENGOVAR												
LSP-1049439716	HODMEZOVASARHELY	VESZPREM	0,13 >	HODMEZOVASARHELY	SZENTES	BK4	BK2	BK2	F9	V8	V4	V3	VESZPREM								
LSP-812440709	MEDINA	PECSKORHAZ	0,13 >	MEDINA	ZENGOVAR	B1	PECSKORHAZ														
LSP-1249759086	TABORFALVA	DEBRECEN	0,13 >	TABORFALVA	BK3	F9	BK2	BK4	SZENTES	BE3	BE2	BE1	SZOLI	JNSZ1	HB1	DEBRECEN					
LSP-660303087	PAPA	BANKUT	0,13 >	PAPA	V5	K2	K1	SZENTENDRE	N1	N2	BANKUT										
LSP-25448390	HAJDUHADHAZ	VAROSFOLD	0,13 >	HAJDUHADHAZ	DEBRECEN	HB1	JNSZ1	SZOLNOK	P4	KEC	VAROSFOLD										
LSP-2057921414	BUDAPEST	PECSKORHAZ	0,13 >	BUDAPEST	NAGYTARCSA	PUSZTAVACS	TABORFALVA	BK3	F9	F7	T3	T2	B1	PECSKORHAZ							
LSP-541824825	SZENTES	TATA	0,13 >	SZENTES	BE3	BE2	BE1	SZOLNOK	P4	P5	N2	N1	SZEN	K1	TATA						
LSP-1191936504	DEBRECEN	HAJDUHADHAZ	0,13 >	DEBRECEN	HAIJDUHADHAZ																
LSP-1640288056	PAPA	JUTA	0,13 >	PAPA	V2	V3	Z1	T1	T2	JUTA											
LSP-240232586	DEBRECEN	ZENGOVAR	0,13 >	DEBRECEN	HB1	JNSZ1	SZOLNOK	BE1	BE2	BE3	SZENTES	BK4	BK2	BK1	MEDINA	ZENGOVAR					
LSP-2010352423	ZENGOVAR	SZOLNOK	0,13 >	ZENGOVAR	MEDINA	BK1	BK2	BK4	SZENTES	BE3	BE2	BE1	SZOLNOK								
LSP-1104429392	HEVIZ	GYOR	0,13 >	HEVIZ	Z1	V3	V2	PAPA	V5	V1	GYOR										
LSP-1955877140	BTKK	JUTA	0,13 >	BTKK	SZOLNOK	BE1	BE2	BE3	SZENTES	F9	F7	T3	T2	JUTA							
LSP-1010208787	JUTA	NAGYTARCSA	0,13 >	JUTA	T2	T3	F7	F9	BK3	TAB	PUSZTAVACS	NAGYTARCSA									
LSP-34095675	SZENTES	SZOLNOK	0,13 >	SZENTES	BE3	BE2	BE1	SZOLNOK													
LSP-1159868907	DEBRECEN	NAGYTARCSA	0,13 >	DEBRECEN	HAIJDUHADHAZ	BAZ1	BAZ2	BANKUT	N2	P2	BUDAPEST	NAGYTARCSA									
LSP-76566384	ZENGOVAR	HEVIZ	0,13 >	ZENGOVAR	B1	T2	T1	Z1	HEVIZ												
LSP-566723684	ZENGOVAR	KISKUNHALAS	0,13 >	ZENGOVAR	MEDINA	BK1	BK2	KISKUNHALAS													
LSP-987763591	VESZPREM	FURJE	0,13 >	VESZPREM	V3	V4	V8	F7	F9	BK2	BK4	SZENTES	BE3	BE2	FURJE						
LSP-892795139	VARPALOTA	BUDAPEST	0,13 >	VARPALOTA	F4	F3	SZEKESFEHERVAR	F2	BUDAPEST												
LSP-1573931684	HODMEZOVASARHELY	BUDAPEST	0,13 >	HODMEZOVASARHELY	SZENTES	BE3	BE2	BE1	SZOLNOK	P4	P5	N2	P2	BUDAPEST							
LSP-1289968319	VESZPREM	NAGYTARCSA	0,13 >	VESZPREM	V3	V4	SZEKESFEHERVAR	F2	BUDAPEST	NAGYTARCSA											
LSP-1766738477	BANKUT	PAPA	0,13 >	BANKUT	N2	N1	SZENTENDRE	K1	K2	V5	PAPA										
LSP-885042265	FURJE	EGER	0,13 >	FURJE	BE2	BE1	SZOLNOK	P4	P5	N2	EGER										
LSP-167538260	JUTA	MEDINA	0,13 >	JUTA	T2	B1	ZENGOVAR	MEDINA													
LSP-1569513809	TATA	GYOR	0,13 >	TATA	K1	K2	V5	V1	GYOR												
LSP-29853459	ZENGOVAR	PECSKORHAZ	0,13 >	ZENGOVAR	B1	PECSKORHAZ															
LSP-494448126	SZENTES	KAL	0,13 >	SZENTES	BE3	BE2	BE1	SZOLNOK	P4	P5	N2	KAL									
LSP-2109931161	HEVIZ	HAIJDUHADHAZ	0,13 >	HEVIZ	Z1	V3	V4	SZEKESFEHERV	F2	BUC	P2	N2	BANKI	BAZ2	BAZ1	HAIJDUHADHAZ					
LSP-1912241577	KAL	PECSKORHAZ	0,13 >	KAL	N2	P2	P3	NAGYTARCSA	PUSZTAVACS	F9	F7	T3	T2	PECSKORHAZ							
LSP-1846775634	TATA	PECSKORHAZ	0,13 >	TATA	K1	SZENTENDRE	BUDAPEST	NAGYTARCSA	PUSZTAVACS	F9	F7	T3	T2	PECSKORHAZ							
LSP-1668234032	HODMEZOVASARHELY	PUSZTAVACS	0,13 >	HODMEZOVASARHELY	SZENTES	BK2	BK2	BK3	BK3	TAB	PUSZTAVACS										
LSP-1193220836	PECSKORHAZ	TABORFALVA	0,13 >	PECSKORHAZ	B1	T2	T3	F7	F9	BK3	TABORFALVA										
LSP-609422234	PECSKORHAZ	PAPA	0,13 >	PECSKORHAZ	B1	T2	T1	Z1	V3	V2	PAPA										
LSP-580297446	PAPA	DEBRECEN	0,13 >	PAPA	V5	K2	K1	SZENTENDRE	N1	N2	BANKUT	BAZ2	BAZ1	HAIJDUHADHA	DEBRECEN						
LSP-585496090	SZENTES	PUSZTAVACS	0,13 >	SZENTES	BK4	BK2	F9	BK3	TABORFALVA	PUSZTAVACS											
LSP-1648830224	BTKK	VAROSFOLD	0,13 >	BTKK	SZOLNOK	P4	KECSKEMET	VAROSFOLD													
LSP-1398527546	SZENTENDRE	DEBRECEN REPTER	0,13 >	SZENTENDRE	N1	N2	BANKUT	BAZ2	BAZ1	HAIJ	DEBRECEN	DEBRECEN REPTER									
LSP-228669259	PAPA	EGER	0,13 >	PAPA	V5	K2	K1	SZENTENDRE													
LSP-1123164185	HAIJDUHADHAZ	PAPA	0,13 >	HAIJDUHADHAZ	BAZ1	BAZ2	BANKUT	N2	N1	SZE	K1	K2	V5	PAPA							
LSP-76968413	DEBRECEN REPTER	ZENGOVAR	0,13 >	DEBRECEN REPTER	DEBRECEN	HB1	JNSZ1	SZOLNOK	BE1	BE2	BE3	BK4	BK2	BK1	MEDINA	ZENGOVAR					
LSP-154424125	SZEKESFEHERVAR	HAIJDUHADHAZ	0,13 >	SZEKESFEHERVAR	F2	BUDAPEST	P2	N2	BANKUT	HAJDUHADHAZ											
LSP-1109235720	PECSKORHAZ	SZEKESFEHERVAR	0,13 >	PECSKORHAZ	B1	T2	T1	Z1	V3	V4	SZEKESFEHERVAR										
LSP-542784934	DEBRECEN	SZENTENDRE	0,13 >	DEBRECEN	HAIJDUHADHAZ	BAZ1	BAZ2	BANKUT	N2	N1	SZENTENDRE										
LSP-504156926	DEBRECEN REPTER	HAIJDUHADHAZ	0,13 >	DEBRECEN REPTER	DEBRECEN	HAIJDUHADHAZ															
LSP-1748176250	BTKK	GYOR	0,13 >	GYOR	V1	V5	K2	K1	SZENTENDRE	N1	N2	P5	P4	SZOLNOK	BTKK						
LSP-1092863840	FURJE	KAL	0,13 >	FURJE	BE2	BE1	SZOLNOK	P4	P5	N2	KAL										
LSP-192572467	DEBRECEN	VESZPREM	0,13 >	DEBRECEN	HAIJDUHADHAZ	BAZ1	BAZ2	BANKUT	N2	P2	BUDAPEST	F2	SZEKE	V4	V3	VESZPREM					
LSP-495897730	HEVIZ	VAROSFOLD	0,13 >	HEVIZ	Z1	V3	V4	V8	F7	F9	BK2	BK4	KECSI	VAROSFOLD							
LSP-514283225	FURJE	TABORFALVA	0,13 >	FURJE	BE2	BE3	SZENTES	BK4	BK2	F9	BK3	TABORFALVA									
LSP-1498297852	EGER	MEDINA	0,13 >	EGER	N2	P2	P3	NAGYTARCSA	PUSZTAVACS	F9	F7	T3	T2	B1	ZENGOVAR						> MEDINA
LSP-1757554371	KISKUNHALAS	NAGYTARCSA	0,13 >	KISKUNHALAS	BK2	F9	BK3	TABORFALVA	PUSZTAVACS	NAGYTARCSA											
LSP-1935396207	ZENGOVAR	HODMEZOVASARHELY	0,13 >	ZENGOVAR	MEDINA	BK1	BK2	BK4	SZENTES	HODMEZOVASARHELY											
LSP-1577262458	NAGYTARCSA	DEBRECEN REPTER	0,13 >	NAGYTARCSA	BUDAPEST	N2	BANKUT	BAZ2	BAZ1	DEBRECEN	DEBRECEN REPTER										
LSP-986556853	KISKUNHALAS	FURJE	0,13 >	KISKUNHALAS	BK2	BK4	SZENTES	BE3	BE2	FURJE											
LSP-524447818	TABORFALVA	MEDINA	0,13 >	TABORFALVA	BK3	F9	F7	T3	T2	B1	ZENGOVAR	MEDINA									
LSP-451072151	BTKK	DEBRECEN REPTER	0,13 >	BTKK	SZOLNOK	JNSZ1	HB1	DEBRECEN	DEB												





Útvonal azonosító	Induló csomópont	Végződő csomópont	Sávsebesség [Mb]	Útvonal	N2	P2	BUDAPEST	F2	SZEKESFEHERVAR	N2	P2	BUDAPEST	F2	SZEKESFEHEI	F3	F4	VARPALOTA	
LSP-1132468017	EGER	SZEKESFEHERVAR	0,12 >	EGER	N2	P2	BUDAPEST	F2	SZEKESFEHERVAR	N2	P2	BUDAPEST	F2	SZEKESFEHEI	F3	F4	VARPALOTA	
LSP-1549470409	DEBRECEN REPTER	VARPALOTA	0,12 >	DEBRECEN REPTER	N1	N2	BANKUT	BAZ2	BANKUT	N2	P2	BUDAPEST	F2	SZEKESFEHEI	F3	F4	VARPALOTA	
LSP-198237496	SZENTENDRE	HAJDUHADHAZ	0,12 >	SZENTENDRE	N1	N2	BANKUT	BAZ2	BAZ1	HAJDUHADHAZ	N2	P2	BUDAPEST	F2	SZEKESFEHEI	F3	F4	VARPALOTA
LSP-1313820198	HEVIZ	SZOLNOK	0,12 >	HEVIZ	Z1	V3	V4	SZEKESFEHERV	F2	BUC P2	SZOLNOK	N2	P5	P4				
LSP-2044071422	SZOLNOK	NAGYTARCSA	0,12 >	SZOLNOK	P4	P5	N2	P2	P3	NAGYTARCSA	SZENTES	N2	P5	P4				
LSP-1445486615	EGER	SZENTES	0,12 >	EGER	N2	P5	P4	SZOLNOK	BE1	BE2 BE3	SZENTES	N2	P5	P4				
LSP-1858321023	SZENTENDRE	TATA	0,12 >	SZENTENDRE	K1	TATA												
LSP-1322061890	MEDINA	VAROSFOLD	0,12 >	MEDINA	BK1	BK2	BK4	KECSKEMET	VAROSFOLD	BUC NAGYTARCSA	PUSZTAVACS	TABORFALVA						
LSP-1205318614	GYOR	TABORFALVA	0,12 >	GYOR	V1	V5			SZENTENDRE									
LSP-1501440741	GYOR	TATA	0,12 >	GYOR	V1	V5	K2	K1	TATA									
LSP-1123405879	DEBRECEN	HEVIZ	0,12 >	DEBRECEN	HAJDUHADHAZ	BAZ1	BAZ2	BANKUT	N2	P2 BUDAPEST	F2	SZEKESFEHEI	V4	V3	Z1	HEVIZ		
LSP-710367926	JUTA	SZOLNOK	0,12 >	JUTA	T2	T3	F7	F9	BK2	BK4 SZENTES	BE3	BE2	BE1	SZOLNOK				
LSP-2104140451	NAGYTARCSA	PECSKORHAZ	0,12 >	NAGYTARCSA	PUSZTAVACS	TABORFALVA	BK3	F9	F7	T3 T2	B1	PECSKORHAZ						
LSP-1769277495	TATA	BUDAPEST	0,12 >	TATA	K1	SZENTENDRE	BUDAPEST											
LSP-149184298	TABORFALVA	HODMEZOVASARHELY	0,12 >	TABORFALVA	BK3	F9	BK2	BK4	SZENTES	HODMEZOVASARHELY								
LSP-706450226	VAROSFOLD	SZENTENDRE	0,12 >	VAROSFOLD	KECSKEMET	P4	P5	N2	N1	SZENTENDRE								
LSP-661784565	GYOR	ZENGOVAR	0,12 >	GYOR	V1	V5	PAPA	V2	V3	Z1 T1	T2	B1	ZENGOVAR					
LSP-643048563	SZOLNOK	SZENTES	0,12 >	SZOLNOK	BE1	BE2	BE3	SZENTES										
LSP-395624117	FURJE	DEBRECEN	0,12 >	FURJE	BE2	BE1	SZOLNOK	JNSZ1	HB1	DEBRECEN								
LSP-1869667484	KISKUNHALAS	SZEKESFEHERVAR	0,12 >	KISKUNHALAS	BK2	F9	F8	F5	SZEKESFEHERVAR									
LSP-1058515761	TATA	BTKK	0,12 >	TATA	K1	SZENTENDRE	N1	N2	P5	P4 SZOLNOK	BTKK	HODMEZOVASARHELY						
LSP-669436878	PECSKORHAZ	HODMEZOVASARHELY	0,12 >	PECSKORHAZ	B1	ZENGOVAR	MEDINA	BK1	BK2	BK4 SZENTES	HODMEZOVASARHELY							
LSP-1274485350	NAGYTARCSA	DEBRECEN	0,12 >	NAGYTARCSA	BUDAPEST	P2	N2	BANKUT	BAZ2	BAZ HAJDUHADHAZ	DEBRECEN							
LSP-1218324646	EGER	PECSKORHAZ	0,12 >	EGER	N2	P2	P3	NAGYTARCSA	PUSZTAVACS	TAB BK3	F9	F7	T3	T2	B1	PECSKORHAZ		
LSP-924075651	EGER	DEBRECEN REPTER	0,12 >	EGER	N2	BANKUT	BAZ2	BAZ1	HAJDUHADHAZ	DEE DEBRECEN REPTER								
LSP-20122326	EGER	JUTA	0,12 >	EGER	N2	P2	P3	NAGYTARCSA	PUSZTAVACS	TAB BK3	F9	F7	T3	T2	JUTA			
LSP-1461175650	DEBRECEN REPTER	SZEKESFEHERVAR	0,12 >	DEBRECEN REPTER	DEBRECEN	HAJDUHADHAZ	BAZ1	BAZ2	BANKUT	N2 P2	BUDAPEST	F2	SZEKESFEHERVAR					
LSP-1807505810	SZOLNOK	EGER	0,12 >	SZOLNOK	P4	P5	N2	EGER										
LSP-1583582088	PAPA	SZENTES	0,12 >	PAPA	V2	V3	V4	V8	F7	F9 BK2	BK4	SZENTES						
LSP-497396234	NAGYTARCSA	BUDAPEST	0,12 >	NAGYTARCSA	BUDAPEST													
LSP-149673055	SZOLNOK	GYOR	0,12 >	SZOLNOK	P4	P5	N2	N1	SZENTENDRE	K1 K2	V5	V1	GYOR					
LSP-364701839	HAJDUHADHAZ	KAL	0,12 >	HAJDUHADHAZ	BAZ1	BAZ2	BANKUT	N2	KAL									
LSP-27111395	BUDAPEST	JUTA	0,12 >	BUDAPEST	NAGYTARCSA	PUSZTAVACS	TABORFALVA	BK3	F9	F7 T3	T2	JUTA						
LSP-23193577	MEDINA	EGER	0,12 >	MEDINA	ZENGOVAR	B1	T2	T3	F7	F9 BK3	TABORFALVA	PUSZTAVACS	BUDAPEST	P2	N2	EGER		
LSP-2127679953	PECSKORHAZ	PUSZTAVACS	0,12 >	PECSKORHAZ	B1	T2	T3	F7	F9	BK3 TABORFALVA	PUSZTAVACS							
LSP-1077080763	SZOLNOK	HAJDUHADHAZ	0,12 >	SZOLNOK	JNSZ1	HB1	DEBRECEN	HAJDUHADHAZ										
LSP-1802067050	HODMEZOVASARHELY	DEBRECEN REPTER	0,12 >	HODMEZOVASARHELY	SZENTES	BE3	BE2	BE1	SZOLNOK	JNS HB1	DEBRECEN	DEBRECEN REPTER						
LSP-308630711	VAROSFOLD	KAL	0,12 >	VAROSFOLD	KECSKEMET	P4	P5	N2	KAL									
LSP-419148590	FURJE	BUDAPEST	0,12 >	FURJE	BE2	BE1	SZOLNOK	P4	P5	N2 P2	BUDAPEST							
LSP-926499978	VAROSFOLD	FURJE	0,12 >	VAROSFOLD	KECSKEMET	BK4	SZENTES	BE3	BE2	FURJE								
LSP-103012144	BUDAPEST	HODMEZOVASARHELY	0,12 >	BUDAPEST	NAGYTARCSA	PUSZTAVACS	TABORFALVA	BK3	F9	BK2 BK4	SZENTES	HODMEZOVASARHELY						
LSP-1323315139	EGER	DEBRECEN	0,12 >	EGER	N2	BANKUT	BAZ2	BAZ1	HAJDUHADHAZ	DEBRECEN								
LSP-2134858121	VESZPREM	GYOR	0,12 >	VESZPREM	V3	V2	PAPA	V5	V1	GYOR								
LSP-1300031161	MEDINA	NAGYTARCSA	0,12 >	MEDINA	ZENGOVAR	B1	T2	T3	F7	F9 BK3	TABORFALVA	PUSZTAVACS						
LSP-1882764390	TATA	SZEKESFEHERVAR	0,12 >	TATA	K1	SZENTENDRE	BUDAPEST	F2	SZEKESFEHERVAR									
LSP-773589807	GYOR	VAROSFOLD	0,12 >	GYOR	V1	V5	K2	K1	SZENTENDRE	N1 N2	P5	P4	KECSKEMET	VAROSFOLD				
LSP-2011634613	BTKK	NAGYTARCSA	0,12 >	BTKK	SZOLNOK	P4	P5	N2	P2	P3 NAGYTARCSA								
LSP-1073570462	MEDINA	VESZPREM	0,12 >	MEDINA	ZENGOVAR	B1	T2	T1	Z1	V3 VESZPREM								
LSP-3271116670	SZENTENDRE	ZENGOVAR	0,12 >	SZENTENDRE	BUDAPEST	NAGYTARCSA	PUSZTAVACS	TABORFALVA	BK3	F9 F7	T3	T2	B1	ZENGOVAR				
LSP-215057103	KAL	EGER	0,12 >	KAL	N2	EGER												
LSP-175280492	HODMEZOVASARHELY	SZENTENDRE	0,12 >	HODMEZOVASARHELY	SZENTES	BE3	BE2	BE1	SZOLNOK	P4 P5	N2	N1	SZENTENDRE					
LSP-42372142	JUTA	HODMEZOVASARHELY	0,12 >	JUTA	T2	T3	F7	F9	BK2	BK4 SZENTES	HODMEZOVASARHELY							
LSP-243985552	FURJE	PAPA	0,12 >	FURJE	BE2	BE3	SZENTES	BK4	BK2	F9 F7	V8	V4	V3	V2	PAPA			
LSP-1963467665	HEVIZ	KAL	0,12 >	HEVIZ	Z1	V3	V4	SZEKESFEHERV	F2	BUC P2	N2	KAL						
LSP-1819859964	VESZPREM	ZENGOVAR	0,12 >	VESZPREM	V3	Z1	T1	T2	B1	ZENGOVAR								
LSP-1090980426	VAROSFOLD	HAJDUHADHAZ	0,12 >	VAROSFOLD	KECSKEMET	P4	SZOLNOK	JNSZ1	HB1	DEE HAJDUHADHAZ	VARPALOTA							
LSP-285551322	BANKUT	VARPALOTA	0,12 >	BANKUT	N2	BANKUT	BUDAPEST	F2	SZEKESFEHERV	F3 F4								
LSP-1583754226	KISKUNHALAS	VESZPREM	0,12 >	KISKUNHALAS	BK2	F9	F7	V8	V4	V3 VESZPREM								
LSP-684024368	SZENTENDRE	PUSZTAVACS	0,12 >	SZENTENDRE	BUDAPEST	NAGYTARCSA	PUSZTAVACS											
LSP-328238701	PAPA	NAGYTARCSA	0,12 >	PAPA	V5	K2	K1	SZENTENDRE	BUDAPEST	NAGYTARCSA								
LSP-1798272941	MEDINA	HODMEZOVASARHELY	0,12 >	MEDINA	BK1	BK2	BK4	SZENTES	HODMEZOVASARHELY									
LSP-12407949	NAGYTARCSA	HEVIZ	0,12 >	NAGYTARCSA	BUDAPEST	F2	SZEKESFEHERVAR	V4	V3	Z1 HEVIZ								
LSP-379672923	BANKUT	PUSZTAVACS	0,12 >	BANKUT	N2	P2	P3	NAGYTARCSA	PUSZTAVACS									
LSP-775531258	DEBRECEN REPTER	PECSKORHAZ	0,12 >	DEBRECEN REPTER	DEBRECEN	HB1	JNSZ1	SZOLNOK	BE1	BE2 BE3	SZENTES	BK4	BK2	BK1	MEDINA	ZENGOVAR	> B1	
LSP-1739959386	VARPALOTA	PAPA	0,12 >	VARPALOTA	V6	VESZPREM	V3	V2	PAPA									
LSP-1911667250	BUDAPEST	PAPA	0,12 >	BUDAPEST	SZENTENDRE	K1	K2	V5	PAPA									
LSP-1453391611	BUDAPEST	HEVIZ	0,12 >	BUDAPEST	F2	SZEKESFEHERV	V4	V3	Z1	HEVIZ								
LSP-636797986	EGER	VARPALOTA	0,12 >	EGER	N2	P2	BUDAPEST	F2	SZEKESFEHERV	F3 F4	VARPALOTA							
LSP-586315531	TATA	HEVIZ	0,12 >	TATA	K1	SZENTENDRE	BUDAPEST	F2	SZEKESFEHERV	V4 V3	Z1	HEVIZ						
LSP-532397682	BANKUT	ZENGOVAR	0,12 >	BANKUT	N2	P2	P3	NAGYTARCSA	PUSZTAVACS	TAB BK3	F9	F7	T3	T2	B1	ZENGOVAR		
LSP-1086591020	TABORFALVA	EGER	0,12 >	TABORFALVA	PUSZTAVACS	NAGYTARCSA	P3	P2	N2	EGER								
LSP-913218304	SZOLNOK	PAPA	0,12 >	SZOLNOK	P4	P5	N2	N1	SZENTENDRE	K1 K2	V5	PAPA						
LSP-847049170	FURJE	SZEKESFEHERVAR	0,12 >	FURJE	BE2	BE3	SZENTES	BK4	BK2	F9 F8	F5	SZEKESFEHERVAR						
LSP-80508927	DEBRECEN	DEBRECEN REPTER	0,12 >	DEBRECEN	DEBRECEN REPTER													
LSP-2101814741	VARPALOTA	MEDINA	0,12 >	VARPALOTA	V6	VESZPREM	V3	Z1	T1	T2 B1	ZENGOVAR	MEDINA						
LSP-796227876	PECSKORHAZ	MEDINA	0,12 >	PECSKORHAZ	B1	ZENGOVAR	MEDINA											
LSP-1605953114	KISKUNHALAS	PUSZTAVACS	0,12 >	KISKUNHALAS	BK2	F9	BK3	TABORFALVA	PUSZTAVACS									
LSP-1832229229	SZEKESFEHERVAR	JUTA	0,12 >	SZEKESFEHERVAR	V4	V8	F7	T3	T2	JUTA								
LSP-136276619	BANKUT	DEBRECEN REPTER	0,12 >	BANKUT	BAZ2	BAZ1	HAJDUHADHAZ	DEBREC										





Útvonal azonosító	Induló csomópont	Végződő csomópont	Sávszélesség [Mb]	Útvonal
LSP-2051093836	KISKUNHALAS	VAROSFOLD	0,09 >	KISKUNHALAS
LSP-1812352191	BUDAPEST	HAJDUHADHAZ	0,09 >	BUDAPEST
LSP-325694817	SZENTENDRE	JUTA	0,09 >	SZENTENDRE
LSP-908038146	PUSZTAVACS	TABORFALVA	0,09 >	PUSZTAVACS
LSP-954037127	HEVIZ	FURJE	0,09 >	HEVIZ
LSP-1238230859	ZENGOVAR	MEDINA	0,09 >	ZENGOVAR
LSP-349942870	BTKK	VARPALOTA	0,09 >	BTKK
LSP-2033963703	SZENTES	GYOR	0,09 >	SZENTES
LSP-845327306	PECSKORHAZ	FURJE	0,09 >	PECSKORHAZ
LSP-239005312	VARPALOTA	FURJE	0,09 >	VARPALOTA
LSP-1014276713	SZEKESFEHERVAR	PUSZTAVACS	0,09 >	SZEKESFEHERVAR
LSP-91390147	PAPA	TATA	0,09 >	PAPA
LSP-1013240352	VESZPREM	HEVIZ	0,08 >	VESZPREM
LSP-356594522	BUDAPEST	VESZPREM	0,08 >	BUDAPEST
LSP-261526964	VESZPREM	VARPALOTA	0,08 >	VESZPREM
LSP-1457899907	SZEKESFEHERVAR	GYOR	0,08 >	SZEKESFEHERVAR
LSP-77120016	JUTA	SZENTES	0,08 >	JUTA
LSP-1333713741	JUTA	TABORFALVA	0,08 >	JUTA
LSP-1658498138	EGER	BANKUT	0,08 >	EGER
LSP-284181670	KAL	BTKK	0,08 >	KAL
LSP-404763265	VESZPREM	HAJDUHADHAZ	0,08 >	VESZPREM
LSP-1616522596	FURJE	GYOR	0,08 >	FURJE
LSP-171980158	HEVIZ	JUTA	0,07 >	HEVIZ
				BK2
				P2
				BUDAPEST
				TABORFALVA
				Z1
				V3
				V4
				V8
				F7
				F9
				BK2
				BK4
				SZEN' BE3
				BE2
				FURJE
				MEDINA
				SZOLNOK
				P4
				BK2
				ZENGOVAR
				F9
				F8
				BK1
				BK2
				BUDAPEST
				P2
				N2
				P5
				K2
				K1
				TATA
				Z1
				HEVIZ
				F4
				VARPALOTA
				V6
				VESZPREM
				F3
				VARPALOTA
				K2
				V5
				V1
				GYOR
				BK2
				BK3
				BK4
				SZENTES
				TABORFALVA
				N2
				BANKUT
				N2
				P5
				P4
				SZOLNOK
				SZEKESFEHERVAR
				F2
				SZOLNOK
				P4
				JUTA
				BTKK
				BUDAPEST
				P2
				N2
				N2
				N1
				BANKUT
				SZENTENDRE
				BAZ2
				BAZ1
				HAJDUHADHAZ
				K1
				K2
				V5
				V1
				GYOR

Ünneplétszám	Induló csoport	Végzős csoport	Százezer (Mbit)	Ünneplétszám	Induló csoport	Végzős csoport	Százezer (Mbit)
LSP-13275693	BANKUT	SZOLNOK	4,12	BANKUT	N2	P8	P4
LSP-210831028	VARPALOTA	VARPALOTA	3,91	SZENTES	BK4	F9	F8
LSP-105284489	PAPA	FURJE	3,77	PAPA	V2	V3	V4
LSP-38803809	VAROSFOLD	SZEKESFEHERVAR	3,75	VAROSFOLD	BK4	BK4	BK4
LSP-94237098	SZENTES	ZENGOVAR	3,73	SZENTES	BK4	BK4	BK4
LSP-38884339	NAGYTARCSA	BUDAPEST	3,73	NAGYTARCSA	BUDAPEST	BE2	BE1
LSP-12487144	VEZPREM	BE3	3,72	SZENTES	F4	F3	F2
LSP-40288235	BUDAPEST	BANKUT	3,49	BUDAPEST	P2	BE2	BE1
LSP-132042078	PECSKORHAZ	PECSKORHAZ	3,41	HOMOEZOVARSELY	SZENTES	BE3	BE2
LSP-1911551397	HOMOEZOVARSELY	HEVIZ	3,40	SZEKESFEHERVAR	V4	V3	V2
LSP-104889781	DEBRECEN	SZEKESFEHERVAR	3,28	DEBRECEN	HAJDUHADHAZ	BAZ1	BAZ2
LSP-860242612	NAGYTARCSA	HAJDUHADHAZ	3,28	NAGYTARCSA	HAJDUHADHAZ	BAZ1	BAZ2
LSP-147149490	VEZPREM	JUTA	3,28	VEZPREM	V3	Z1	T1
LSP-188471371	BUDAPEST	PUSZTAVACS	3,28	BUDAPEST	NAGYTARCSA	BE3	BE2
LSP-1074001250	FURJE	VAROSFOLD	3,11	FURJE	BE3	BE3	BE3
LSP-203968310	EGER	DEBRECEN	3,07	EGER	N2	BANKUT	BAZ2
LSP-87279481	HOMOEZOVARSELY	TABORFALVA	2,92	HOMOEZOVARSELY	DEBRECEN	BA21	BA21
LSP-923818122	VAROSFOLD	VARPALOTA	2,82	VAROSFOLD	SZOLNOK	F4	F3
LSP-178891445	BUDAPEST	VARPALOTA	2,82	VARPALOTA	SZOLNOK	JNSZ1	JNSZ1
LSP-122853793	NAGYTARCSA	KAL	2,91	NAGYTARCSA	BUDAPEST	P2	N2
LSP-174281031	NAGYTARCSA	VAROSFOLD	2,90	NAGYTARCSA	P3	P2	N2
LSP-33492398	VEZPREM	GYOR	2,90	VEZPREM	V3	V2	V1
LSP-128998988	BTOK	HEVIZ	2,88	BTOK	SZOLNOK	JNSZ1	H1
LSP-25060278	PECSKORHAZ	TABORFALVA	2,88	PECSKORHAZ	B1	BUDAPEST	T2
LSP-87234301	SZEKESFEHERVAR	EGER	2,84	SZEKESFEHERVAR	F2	BUDAPEST	N1
LSP-134692348	BUDAPEST	TATA	2,83	BUDAPEST	SZENTENDRE	K1	TATA
LSP-148868972	VEZPREM	EGER	2,82	VEZPREM	V3	V4	SZEKESFEHERVAR
LSP-181889871	DEBRECEN	EGER	2,82	DEBRECEN	HAJDUHADHAZ	BAZ1	BAZ2
LSP-49923443	DEBRECEN REPTER	SZEKESFEHERVAR	2,79	DEBRECEN REPTER	HAJDUHADHAZ	BAZ1	BAZ2
LSP-1061519078	SZEKESFEHERVAR	BTOK	2,68	SZEKESFEHERVAR	BUDAPEST	N1	N2
LSP-88592770	SZENTENDRE	PAPA	2,64	SZENTENDRE	K1	PAPA	PAPA
LSP-132599416	PUSZTAVACS	HAJDUHADHAZ	2,64	PUSZTAVACS	NAGYTARCSA	P3	N2
LSP-60434184	BTOK	DEBRECEN	2,63	BTOK	DEBRECEN	BE2	BE2
LSP-199924280	HAJDUHADHAZ	DEBRECEN	2,60	HAJDUHADHAZ	NAGYTARCSA	H1	JNSZ1
LSP-75308454	PUSZTAVACS	DEBRECEN REPTER	2,59	PUSZTAVACS	NAGYTARCSA	P3	N2
LSP-207503853	DEBRECEN REPTER	DEBRECEN REPTER	2,57	HEVIZ	VEZPREM	V6	V3
LSP-134844812	DEBRECEN	SZENTENDRE	2,56	DEBRECEN	HAJDUHADHAZ	BAZ1	BAZ2
LSP-181404878	GYOR	SZENTENDRE	2,56	GYOR	N2	GYOR	N2
LSP-178843843	BUDAPEST	TABORFALVA	2,56	BUDAPEST	SZEKESFEHERVAR	F8	F8
LSP-182172730	NAGYTARCSA	PAPA	2,55	NAGYTARCSA	BUDAPEST	K2	V5
LSP-180781026	VAROSFOLD	EGER	2,53	VAROSFOLD	KECSKEMET	SZOLNOK	JNSZ1
LSP-196399038	DEBRECEN REPTER	REPTER	2,53	DEBRECEN REPTER	DEBRECEN	HAJDUHADHAZ	BAZ1
LSP-46619182	NAGYTARCSA	DEBRECEN	2,51	NAGYTARCSA	P3	BAZ1	BAZ2
LSP-124788313	HAJDUHADHAZ	DEBRECEN	2,51	HAJDUHADHAZ	DEBRECEN	N2	BAZ1
LSP-164841897	DEBRECEN REPTER	HAJDUHADHAZ	2,48	DEBRECEN REPTER	HAJDUHADHAZ	T2	T3
LSP-170676545	PECSKORHAZ	TATA	2,48	PECSKORHAZ	V1	F7	V8
LSP-105278018	PAPA	TATA	2,41	PAPA	V5	K2	TATA
LSP-15442435	KAL	BANKUT	2,39	KAL	BANKUT	N2	BANKUT
LSP-167466222	DEBRECEN REPTER	DEBRECEN REPTER	2,33	DEBRECEN REPTER	DEBRECEN REPTER	B1	T2
LSP-132026988	MEDNA	TABORFALVA	2,30	MEDNA	ZENGOVAR	F7	F9
LSP-187799251	DEBRECEN REPTER	DEBRECEN	2,29	DEBRECEN REPTER	DEBRECEN	F9	BK3
LSP-172301448	VARPALOTA	MEDNA	2,25	VARPALOTA	VEZPREM	V3	Z1
LSP-145230385	PAPA	SZENTENDRE	2,24	PAPA	V2	K1	K1
LSP-208621478	VEZPREM	BUDAPEST	2,24	VEZPREM	VARPALOTA	F4	F3
LSP-115022599	PUSZTAVACS	SZENTENDRE	2,23	SZENTENDRE	SZEKESFEHERVAR	F2	BUDAPEST
LSP-210339285	NAGYTARCSA	PAPA	2,20	PAPA	V5	K2	SZOLNOK
LSP-220191862	TATA	NAGYTARCSA	2,19	TATA	SZENTENDRE	F8	BUDAPEST
LSP-706234803	PECSKORHAZ	VEZPREM	2,18	PECSKORHAZ	B1	T2	BUDAPEST
LSP-23487473	PECSKORHAZ	SZOLNOK	2,18	PECSKORHAZ	H1	JNSZ1	SZOLNOK
LSP-184103245	TABORFALVA	PUSZTAVACS	2,15	TABORFALVA	T2	T3	F7
LSP-166896139	ZENGOVAR	KISKUNHALAS	2,10	ZENGOVAR	B1	T2	F3
LSP-121875349	SZOLNOK	FURJE	2,07	SZOLNOK	F2	BK2	BE2
LSP-164284039	HAJDUHADHAZ	HAJDUHADHAZ	2,06	KISKUNHALAS	BE4	BE4	BE4
LSP-139084439	PUSZTAVACS	NAGYTARCSA	2,02	PUSZTAVACS	NAGYTARCSA	BK3	F9
LSP-172277889	ZENGOVAR	TABORFALVA	1,98	PUSZTAVACS	TABORFALVA	V6	V2
LSP-151238217	VARPALOTA	PAPA	1,98	VARPALOTA	VEZPREM	V3	V2
LSP-71145388	FURJE	FURJE	1,94	FURJE	SZENTES	BE2	BE2
LSP-639180192	VARPALOTA	ZENGOVAR	1,94	VARPALOTA	VEZPREM	V3	Z1
LSP-186229949	HEVIZ	MEDNA	1,94	HEVIZ	T2	B1	T2
LSP-192200384	BANKUT	HAJDUHADHAZ	1,90	BANKUT	BAZ1	HAJDUHADHAZ	HAJDUHADHAZ
LSP-23273573	JUTA	NAGYTARCSA	1,89	JUTA	T3	F7	F9
LSP-183860480	TABORFALVA	EGER	1,83	EGER	N2	P3	NAGYTARCSA
LSP-1396967978	TABORFALVA	HEVIZ	1,82	TABORFALVA	BK2	T3	F7
LSP-160128886	TATA	TATA	1,82	TATA	F1	K1	F1
LSP-843760015	PUSZTAVACS	SZENTENDRE	1,82	PUSZTAVACS	BUDAPEST	SZENTENDRE	F1
LSP-129670247	GYOR	HOMOEZOVARSELY	1,80	GYOR	V1	K2	F9
LSP-138697301	DEBRECEN	HAJDUHADHAZ	1,79	BANKUT	BAZ1	JNSZ1	SZOLNOK
LSP-142995281	PAPA	VEZPREM	1,78	PAPA	V2	V3	VEZPREM
LSP-377306987	TATA	PUSZTAVACS	1,72	TATA	V2	K2	V5
LSP-156838382	SZEKESFEHERVAR	PAPA	1,68	SZEKESFEHERVAR	V1	K2	V5
LSP-198184989	JUTA	JUTA	1,68	JUTA	T2	Z1	V3
LSP-93366230	SZEKESFEHERVAR	BUDAPEST	1,68	SZEKESFEHERVAR	BUDAPEST	Z1	V3
LSP-8493472	JUTA	NAGYTARCSA	1,64	JUTA	T2	T1	SZENTENDRE
LSP-1915062879	KAL	NAGYTARCSA	1,64	KAL	NAGYTARCSA	N1	SZENTENDRE
LSP-196042130	HEVIZ	GYOR	1,63	HEVIZ	V3	V2	PAPA
LSP-173444813	PUSZTAVACS	HEVIZ	1,63	PUSZTAVACS	TABORFALVA	V7	F7
LSP-177896951	HAJDUHADHAZ	SZEKESFEHERVAR	1,62	HAJDUHADHAZ	DEBRECEN	H1	JNSZ1
LSP-70457927	HEVIZ	SZEKESFEHERVAR	1,61	HEVIZ	Z1	V3	VEZPREM
LSP-61138884	TABORFALVA	BUDAPEST	1,58	TABORFALVA	BK3	F9	F8
LSP-171819827	BANKUT	BUDAPEST	1,58	BANKUT	BAZ1	BE2	BE2
LSP-1185181	PAPA	VARPALOTA	1,57	PAPA	V6	V3	VEZPREM
LSP-87523272	KAL	BUDAPEST	1,55	KAL	N2	N1	SZENTENDRE
LSP-143862871	PUSZTAVACS	DEBRECEN	1,52	PAPA	V2	BE3	BE3
LSP-160221578	BANKUT	BANKUT	1,52	BANKUT	BAZ2	HAJDUHADHAZ	DEBRECEN
LSP-87881904	DEBRECEN REPTER	SZOLNOK	1,51	DEBRECEN REPTER	DEBRECEN	H1	JNSZ1
LSP-180738072	PUSZTAVACS	PAPA	1,50	PUSZTAVACS	TABORFALVA	F7	F7
LSP-217595318	VAROSFOLD	HAJDUHADHAZ	1,49	VAROSFOLD	KECSKEMET	P4	SZOLNOK
LSP-354821888	PAPA	GYOR	1,48	GYOR	V1	BE5	PAPA
LSP-212734697	SZENTENDRE	SZOLNOK	1,45	SZENTENDRE	N1	N2	BANKUT
LSP-146214871	PUSZTAVACS	SZEKESFEHERVAR	1,44	PUSZTAVACS	TABORFALVA	BK3	BAZ2
LSP-48237529	VARPALOTA	VARPALOTA	1,44	VEZPREM	VARPALOTA	V5	VARPALOTA
LSP-166489288	TATA	MEDNA	1,43	TATA	K1	K2	F1
LSP-603139125	PUSZTAVACS	VARPALOTA	1,42	PUSZTAVACS	TABORFALVA	F1	F9
LSP-65026190	BANKUT	DEBRECEN REPTER	1,41	BANKUT	BAZ2	BAZ1	HAJDUHADHAZ
LSP-196104848	VAROSFOLD	DEBRECEN	1,38	VAROSFOLD	KECSKEMET	K2	SZOLNOK
LSP-211980811	VEZPREM	VARPALOTA	1,36	VEZPREM	V3	V2	PAPA
LSP-89969518	EGER	PAPA	1,27	EGER	MEDNA	N2	BANKUT
LSP-172788620	ZENGOVAR	MEDNA	1,27	ZENGOVAR	MEDNA	N2	BANKUT
LSP-12303688	EGER	VAROSFOLD	1,27	EGER	N2	BANKUT	BAZ2
LSP-51709078	BTOK	SZENTES	1,27	BTOK	SZOLNOK	H1	JNSZ1
LSP-1241202104	SZOLNOK	SZENTES	1,24	SZOLNOK	BE1	BE2	BE3
LSP-150295384	TABORFALVA	PAPA	1,23	TABORFALVA	BK3	F9	F7
LSP-196078793	TATA	VEZPREM	1,22	TATA	K1	F4	F4
LSP-408372862	GYOR	SZEKESFEHERVAR	1,18	GYOR	V1	V5	K2
LSP-181866701	VARPALOTA	SZEKESFEHERVAR	1,17	VARPALOTA	F3	F3	SZEKESFEHERVAR
LSP-112118874	TABORFALVA	VEZPREM	1,16	TABORFALVA	BK3	F9	V8
LSP-171220214	PUSZTAVACS	BANKUT	1,13	PUSZTAVACS	TABORFALVA	BK3	V3
LSP-121118886	MEDNA	MEDNA	1,11	MEDNA	ZENGOVAR	F7	F7
LSP-49324892	SZOLNOK	VAROSFOLD	1,10	SZOLNOK	P4	VAROSFOLD	F3
LSP-203786010	SZEKESFEHERVAR	VEZPREM	1,07	SZEKESFEHERVAR	F4	VEZPREM	F4
LSP-444429130	HEVIZ	BUDAPEST	1,07	HEVIZ	T1	T2	T3
LSP-404737849	HOMOEZOVARSELY	HEVIZ	1,06	HOMOEZOVARSELY	SZENTES	BE1	BE1
LSP-157932513	SZEKESFEHERVAR	VEZPREM	1,05	SZEKESFEHERVAR	V4	V3	VEZPREM
LSP-86794462	PUSZTAVACS	TABORFALVA	1,04	PUSZTAVACS	TABORFALVA	VEZPREM	VEZPREM
LSP-40886190	VARPALOTA	VEZPREM	1,03	VARPALOTA	V5	VARPALOTA	V5
LSP-122220436	BANKUT	SZENTENDRE	1,01	BANKUT	N2	N1	SZENTENDRE
LSP-203179344	VEZPREM	NAGYTARCSA	1,00	VEZPREM	V6	VARPALOTA	F4
LSP-653677917	PAPA	NAGYTARCSA	0,98	PAPA	V2	F3	SZEKESFEHERVAR
LSP-200847021	PAPA	BANKUT	0,98	EGER	N2	BANKUT	VEZPREM
LSP-7759173	PAPA	BUDAPEST	0,93	PAPA	V3	VEZPREM	V8
LSP-17287779	HAJDUHADHAZ	HOMOEZOVARSELY	0,89	HAJDUHADHAZ	DEBRECEN	H1	JNSZ1
LSP-40647739	KISKUNHALAS	ZENGOVAR	0,89	KISKUNHALAS	DEBRECEN	BK2	ZENGOVAR
LSP-1821856195	HAJDUHADHAZ	SZENTES	0,85	HAJDUHADHAZ	DEBRECEN	H1	JNSZ1
LSP-178489878	DEBRECEN	SZENTES	0,83	DEBRECEN	DEBRECEN	BE1	BE2
LSP-2131217782	HAJDUHADHAZ	SZOLNOK	0,82	HAJDUHADHAZ	DEBRECEN	H1	JNSZ1
LSP-147241731	VARPALOTA	GYOR	0,81	VARPALOTA	F4	F3	SZEKESFEHERVAR
LSP-102242711	DEBRECEN REPTER	SZENTES	0,77	DEBRECEN REPTER	DEBRECEN	H1	JNSZ1
LSP-7246832	SZEKESFEHERVAR	VARPALOTA	0,77	SZEKESFEHERVAR	F3	F4	VARPALOTA
LSP-468811527	SZENTES	SZOLNOK	0,74	SZENTES	BE3	BE2	BE3
LSP-184177356	SZENTES	DEBRECEN REPTER	0,74	SZENTES	BE3	BE2	BE3

