HADMÉRNÖK

V. Évfolyam 2. szám - 2010. június

Bleier Attila
attila.bleier@gmail.com

Rajnai Zoltán
rajnai.zoltan@zmne.hu

A STACIONER HÁLÓZATON HASZNÁLT TECHNOLÓGIÁK JAVASOLT KIALAKÍTÁSA

Absztrakt

Jelen tanulmányban a szerzők bemutatják javaslatukat a Magyar Honvédség fejlett Ethernet és IP hálózati eszközökre épülő stacioner hálózatának kiépítésére. A szerzők részletesen elemzik a jelenlegi hálózati paraméterek beállításait, amelyek ennek jobb felhasználását teszik lehetővé.

In this paper the authors provide a new proposed system design for the fixed network of the Hungarian Army, based on advanced Ethernet and IP networking gear. The authors describe the proposed parameter settings in detail that would make a better use and potential utilization of the current network.

Kulcsszavak: *hálózat, kommunikáció ~ network, communication*

Bevezetés

A Magyar Honvédség gerinchálózat kialakításakor, tervezésekor bizonyos általános irányelveket szükséges figyelembe vennünk, ilyenek például az Összhaderőnemi Doktrínában meghatározott irányelvek, mint azt már korábban (1) kifejtettük. 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 szolgáltatói IP/MPLS hálózatok által nyújtott szolgáltatásokról egy remek áttekintést ad a (2) cikk.

A hálózaton használt protokollok javasolt beállításai

Mind az IS-IS, mind az OSPF szóba jöhető belső útválasztó protokollok (IGP-k) 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
- állapotút algoritmusok (a hálózati ábra elosztott, mindenegyes router függetlenül számolja az utakat a elosztott hálózati ábra alapján)
- Kétszintű hierarchiával rendelkezik
- Designated routert választanak LAN-okon
- széleskörűen használtak
- több együttműködő implementációja van
- támogatják az authentikáció titkosítását

Főbb különbségek:

- Enkapszuláció
    - OSPF IP felett fut
    - ISIS- L2 felett fut
- területi terv
    - OSPF terület határok a routeren belülre esnek, tehát egy router több területhez is tartozhat
    - IS-IS terület határok élekre 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 biztonsítására, ha vezérlési síkbeli hiba van az útválasztókon)

A gerinchálózatban MP-BGP csomagokat célszerű átvinni, az NLRI információ továbbítására a különböző címosztályok között. A Magyar honvédség hálózatában ezt a következő esetben érdemes használni:

- Unicast IP-VPN kialakításakor (L3 IP VPN)
- Unicast IPv4 továbbítására (autonóm-rendszerhatárok között)
- L2VPN szolgáltatásra (BGP jelzésrendszerrel)
- VPLS szolgáltatásra

Az utóbbi két esetben LDP is használható a jelzéskialakításra (signaling). A BGP skálázhatóságának javítására, Route-Reflectorokat (RR) javaslunk. A teljes Magyar Honvédség hálózata egy privát (64512-65535) autónom rendszerbe esik. A belső csomópontok között IBGP, a külsők felé E-BGP 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 hiearchiák : 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

BFD használata ajánlott az Ethernet linkeken. “draft-katz-ward-bfd-00.txt”-ből idézve: a BFD rövid-időtartamú hibadetektálásra képes a szomszédos címtovábbító motorok között, beleértve az interfészeket, adatlinket és a csomagtovábbító motorokat is. 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. PoS interfészek esetén (STM1-4-16-64) a BFD használata sok esetben szükségtelen, az SDH APS algoritmusa 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 használnak:

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

Azért, hogy a másodlagos útnak elegendő védelme legyen 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 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) 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. Mindenegyes 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 transzparansen virtuális "kapcsolóként" viselkedjek. A L3 VPN arra biztosít lehetőséget, hogy a hálózatok L2 forgalmát az egyes telephelyeken leválaszthassuk. Ennek számos előnyei 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. Az alábbi táblázat ezt határozza meg:

	Delay	Buffering	Traffic Symmetry	Bitate
Conversational	▪ Minimum fixed	No	Symmetric	Guaranteed
Streaming	▪ Minimum variable	Allowed	Asymmetric	Guaranteed
Interactive	▪ No guarantees (moderate variable)	Allowed	Asymmetric	No guarantees
Background	▪ No guarantees (big variable)	Allowed	Asymmetric	No guarantees

A conversational és a streaming osztályok főként a valós-idejű forgalmi folyamokat határozzák meg (pl. hang, video, jelzés) míg az interaktive és a background osztályok főként az adat alapú alkalmazásoknak (FTP,Telnet,Email, WWW, etc…). A DiffServ architektúra használt a legtöbbször az erőforrások allokálására. A DiffServ kombinálható a Traffic Engineeringel, így a két technológia kiegészíti egymást (pl. a gerinchálózaton Traffic Engineering + Diffserv, a hozzáférési és aggregációs hálózaton Diffserv alapú QoS.

A gyakorlatban a Magyar Honvédség hálózatán az alábbi szolgáltatás osztályokat használata javasolt:

- VoIP jelzés - signaling - (H.323)
- VoIP hang - voice (RTP)
- Üzemeltetési és IT szolgáltatások – O&M and IT
- Internet

A táblázatban megjelöltük a szolgáltatásosztályokhoz tartozó DSCP osztályokat és az EXP biteket. A különböző MPLS technológiát javaslok az egyes szolgáltatásokhoz. A DSCP (Diffserv Code Point) az IP fejléc QoS célra fenntartott mezője, az EXP pedig az MPLS fejléc QoS célra fenntartott mezői. Így mind tiszta IP, mind IP/MPLS hálózaton meg tudjuk valósítani a QoS-t.

Forgalom típusa	DSCP	EXP	Használt MPLS technológia
VoIP jelzés (H.323)	AF41	4	VPLS
VoIP hang (RTP)	AF43	5	L3VPN
O&M és IT szolgáltatások – O&M	BE	0	L3VPN
Internet traffic	BE	0	L3VPN

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 3-dik rétegbeli (MP-BGP) jelzésrendszert felhasználó virtuális magánhálózati szolgáltatás. Ezekben a cikkek (3), (4) az IP/MPLS gerinhálózatok ideális fejlesztését.
A hálózaton fontos, az egyenletes és stabil szolgáltatásminőség biztosítása, és ezek mérése. A szolgáltatásminőséget a KPI-k (Key Performance Indicatorok) határozzák meg – ezek az ún. szolgáltatátás 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 a valósidejű (Conversational), jelzés (Signalling), streaming (nem valósidejű, de folyamatos szórással sugárzott) az interaktív (Interactive) – amely egy kvázi valósidejű, és a hátter (Background) – tehát best effort jellegű forgalom.
A használt KPI paraméterek a következőek:

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

	Average Delay (msec)	Maximum Delay (msec)	Jitter (msec)	Packet Loss	Failover Time
Conversational	<20	<100	<5	$<10^{-4}$	2 sec
Signaling	<20	<100	/	$<10^{-4}$	/ (Relies on protocol failover)
Streaming	/	/	<100	$<10^{-3}$	5 sec
Interactive	<55	/	/	$<10^{-4}$	5 sec
Background	<108	/	/	$<10^{-3}$	/

Az egyes paraméterek folyamatos monitorozása szükséges, ezt 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.

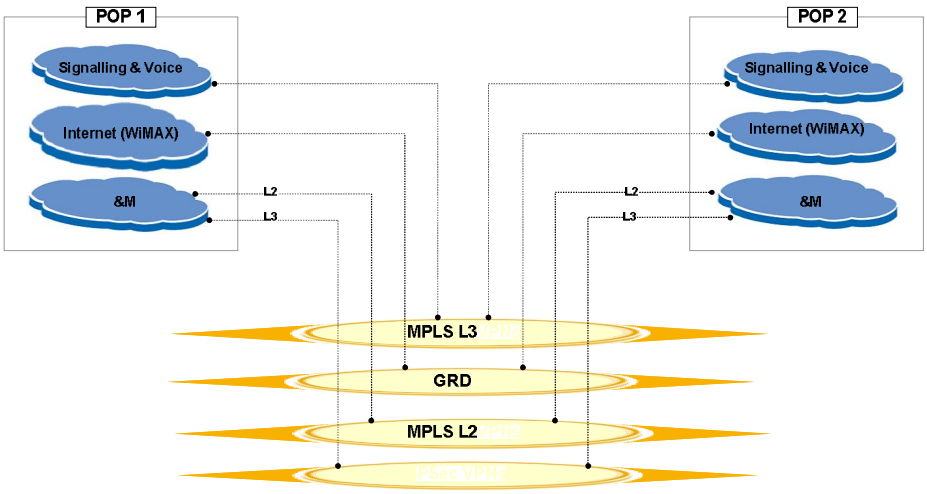
A hálózati biztonság a hálózati biztonsági zónák ("Security Domains") alapvető koncepciójára épülnek. Mindenegyes biztonsági terület összeségében különböző titkosítási szinten lévő forgalmat visz, tehát különböző típusú forgalomnak felel meg, amely különálló privát hálózatnak felel meg.
A privát hálózat a következő kettő típusok egyike lehet:

- fizikai privát hálózat, ahol mindenegyes forgalmi típus egy dedikált fizikai infrastruktúrát használ (tehát külön LAN switcheket 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, de kizárólag meghatározott hálózati elemeken keresztül (eg. 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 technológiák 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.



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

Az alábbi technológiák használata javasolt a IP hálózat biztonságának növelésére:

- az irányított broadcast üzenetek szűrése
- távoli menedzsment hozzáférés meghatározása és naplózása, titkosított protokollokon keresztül
- SNMP Set üzenetek tiltása
- alapértelmezett az útválasztó felé menő ARP üzenetek korlátozása, ez leszűri az ún. ARP viharokat, amelyet a hibás beállítások vagy rosszindulatú cselekedetek indítják, az ARP üzenetek mennyiségét az Ethernet interfészeken tovább korlátozhatjuk
- A fenntartott hoszt és hálózati címek (ún. Marsi, vagy Martian címek), amelyről minden útválasztási információt figyelmen kívül kell hagyni
- DoS támadások a 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 amelynek a forráscímei érvényesek és megfelelnek az útválasztó table 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 table által ellenőrizhető forrás IP című IP csomagokat továbbítja, a többit eldobja
- az ICMP elárasztásos és hasonló támadások elleni védelem érdekében az útválasztó felé irányuló ICMP forgalommennyiség korlátozását javaslom
- A TCP SYN flood támadások elkerülése érdekében, amikor a támadó egy szkriptet vagy programot használva TCP nyitási (SYN) üzeneteket generál, olyan sebességgel amely gyorsabb mint az áldozat bontási ideje
- ezért javasolom, hogy a TCP SYN üzeneteket korlátozzuk
- A PE útválasztókon sávszélesség korlátok használatot javaslom
- Protokoll biztonságterületén az összes használt útválasztási protokollra (BGP, OSPF, IS-IS, RIP és RSVP) a HMAC-MD5-ös authentikáció beállítását javaslom
- Az útválasztóval a kommunikáció csak titkosítottan történhet:
    - 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 authentikációs 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 forgalmak szűrése
        - a router erőforrások (CPU óraciklusok, és kommunikációs sorok) védelme érdekében csak a megbízható forrásból származó protokoll és vezérlési információkat engedélyezhetjük az útválasztó motor felé

Összegzés

A cikkben a Magyar Honvédség stacioner IP/MPLS gerinchálózatán javasolt beállításait mutattuk be. A cikkben szereplő technológiák a polgári életben már bizonyított nagy

rendelkezésre állású szolgáltatói környezet megfelelő adoptálása a Magyar Honvédség stacioner gerinchálózatára. Az adoptáció legnagyobb kihívása Munk Sándor szerint az infokommunikációs rendszerek között az interoperabilitás megteremtése (5), erre az IP/MPLS protokoll teremt lehetőséget.

Irodalomjegyzék

1. The challanges of the 21st century and the requirements of the Hungarian Army. Attila, Bleier. Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-11-1.
2. MPLS alapú IP hálózatok. Dr. Varga Balázs, Géczi Csaba. p. 37-63, MATÁV : MATÁV, 2001., PKI Közlemények 45.. kötet. HU-ISSN 1216-3961.
3. Ethernet alapú szolgáltatói hálózatok és szolgáltatások. Dr. Varga Balázs, Géczi Csaba. p. 137-165, Budapest : Matáv, 2003., PKI közlemények 47. . kötet. HU ISBN: 1216-3961.
4. Szolgáltatói IP gerinchálózat kiépítése Ethernet alapon. Attila, Hámori András - Tanács Ferenc - Balogh. p. 83-99, Budapest : Magyar Telekom Nyrt., 2005., PKI Közlemények 49.. kötet. HU-ISSN 1216-3961.
5. Interoperability infrastructure in military infocommunication systems. Sándor, Munk. Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1 .
6. The Multi-National Missions and the Network Enabled Capability. Károly, Fekete. Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1.
7. Unification of the Hungarian Governmental communications systems. Erik, Pándi. Budapest : ZMNE, Communications 2005. ISBN 963 7060 11 1.
8. Magyar Honvédség elvárásai és a XXI század kihívásai. Attila, Bleier. Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-57-1.
9. Az Észak-Atlanti Szervezetet kiszolgáló kommunikációs rendszerek jellemzői. Pándi Balázs, Pándi Erik. Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-57-1.
10. A jövő várható háborúinak és katonai konfliktusainak a hatása a hazai tábori kommunikációs rendszer megújításának folyamatára. Pándi Balázs, Pándi Erik. Budapest : ZMNE, Communications 2008. ISBN 978-963-7060-11-1.
11. New possibilities of wireless trends in the area of mobile infocommunication and management. Erika, Magyarné Kucsera. p. 166- 174, Budapest : ZMNE, 2007., Communications 2007. kötet. ISBN 978-963-7060-31-1.