

Forgalommenedzsment többszörös kapcsolatú tartományoknál

TAKÁCS ATTILA, CSÁSZÁR ANDRÁS, SZABÓ RÓBERT, HENK TAMÁS

Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszék
{takacs, Andras.Csaszar, Robert.Szabo, henk}@tmit.bme.hu

Kulcsszavak: *útválasztás, forgalommenedzsment, terhelésmegosztás*

Az utóbbi időben egyre többen kutatják az IP hálózatok hatékony forgalommenedzsmentjének módjait. A korábbi kutatások jó része csak egyetlen autonóm hálózat belső forgalmának optimalizálására irányult, és csak néhányan vizsgálták a tartományok közötti forgalommenedzsment kérdéseit. Ennek az oka az, hogy míg egy önálló tartományon belül teljes információ és teljes hatáskör áll a forgalommenedzsment rendelkezésére, addig a tartomány határain kívül igen korlátozottak mind az információgyűjtési, mind az útvonalakat befolyásoló lehetőségek. Cikkünkben felvázoljuk a tartományok közötti forgalommenedzsment nehézségeit, és bemutatjuk a BGP által nyújtott lehetőségeket. Ezen felül adunk egy módszert, mellyel a már kifinomult tartományon belüli forgalommenedzsment módszerek kiterjesztésével a szomszédos hálózatok közötti forgalmat szabályozhatjuk.

Bevezető

Az utóbbi időben egyre többen kutatják az IP hálózatok hatékony forgalommenedzsmentjének (*Traffic Engineering, TE*) módjait. A forgalommenedzsment célja tágabb értelemben a felhasználói folyamatok minőségi igényeinek támogatása úgy, hogy közben hatékony, gazdaságos és megbízható módon aknázzuk ki a hálózat lehetőségeit. Szűkebb értelemben a forgalommenedzsment sokszor csak a hatékony és megbízható hálózatkihasználtságra utal.

A korábbi TE kutatások jó része csak egyetlen autonóm hálózat belső forgalmának optimalizálására irányult [1–7]. Ennek eredményeképpen mára számos jól használható javaslat született tartományokon belüli (*intra-domain*) TE megvalósítására, jóllehet gyakorlati alkalmazásuk még nem széleskörű. Ezek a módszerek többnyire megpróbálják csökkenteni a torlódás kialakulásának valószínűségét. Az útválasztókat statikus vagy dinamikus módon képessé teszik a tipikusan használt legrövidebb utak mellett más, alternatív utak használatára is. Ezt úgy érik el, hogy mintegy „elkenik” a forgalmat a hálózatban, így a terhelést megosztják több útvonal között (*load balancing, load sharing*).

Csak néhányan vizsgálták a tartományok közötti (*inter-domain*) forgalommenedzsment kérdéseit. Ennek az oka az, hogy míg egy önálló tartományon belül teljes információ és teljes hatáskör áll a forgalommenedzsment rendelkezésére, addig a tartomány határain kívül igen korlátozottak mind az információgyűjtési, mind az útvonalakat befolyásoló lehetőségek. Ez nem is csoda, hiszen az Internet hierarchikus szervezésű, azaz jól elkülöníthető az autonóm hálózati tartományokon belüli útválasztástól a tartományok közötti útválasztás. A hierarchikus szerveződést egyrészt a jobb skálázhatóság indokolja, hiszen így egy útválasztónak nem kell ismernie a világ minden egyes csomópontjához vezető utat, elég ha csak az adott hálózat felé ve-

zető utat ismeri. Hálózatból márpedig sokkal kevesebb van, mint csomópontból. A kétszintű szerveződés másik fontos indokát üzleti és politikai okok adják, mint például a versenyhelyzetből adódó információ és topológia elrejtés igénye, vagy, hogy az egyes operátorok maguk akarják meghatározni, hogy mely célcímek felé vállalnak csomagtovábbítást, mely szomszédokon keresztül, vagy épp mely szomszédoktól hol fogadnak el csomagokat.

Ezeket az üzleti/politikai igényeket tökéletesen kielégíti a mindmáig egyetlen gyakorlatban alkalmazott tartományok közti útvonalválasztó protokoll – a *Border Gateway Protocol (BGP)* [16]. Ennek a kifejlesztésekor még fel sem merültek a forgalommenedzsment igényei, ehelyett technikailag a stabilitás, robusztusság és a skálázhatóság voltak a főbb szempontok.

Mára azonban nyilvánvalóvá vált, hogy egy önálló hálózat működésének jelentős költségét jelenti a tartományból kimenő forgalom [8]. Ezért a hálózatközi forgalommenedzsment jól szolgálhatja az egyes tartományok üzemeltetőit, hogy optimalizálják kimenő forgalmukat, és így csökkentsék költségeiket.

További fontos kérdés az egyes tartományok összekapcsolása (melyik tartományt melyikkel kössük össze, hányszor, mely csomópontokon keresztül), amelyek helyes megválasztása jelentősen csökkentheti és gyorsíthatja a tartományok közötti forgalmat. Persze nem csupán a gazdaságosság az a kérdés, amelyre a tartományok közötti forgalommenedzsment választ adhat, hanem az egyre fontosabb szolgáltatás minőségi (QoS) elvárások is [9]. Ahogy egy tartományon belül, úgy tartományok között is szükség van a megfelelő késleltetés előírások és adatsebesség igények teljesítésére. Ebben segíthet a megfelelő útvonalak megtalálása és lefoglalása, melynek eredménye a minőségi szolgáltatás.

A cikkben felvázoljuk a tartományok közötti forgalommenedzsment nehézségeit, és bemutatjuk a BGP

által nyújtott lehetőségeket. Ezen felül adunk egy módszert, mellyel a már kifinomult tartományon belüli forgalommenedzsment módszerek kiterjesztésével a szomszédos hálózatok közötti forgalmat szabályozhatjuk.

Mielőtt rátérnénk a BGP és TE kérdéseire, bemutatjuk a tartományok összekapcsolásának szempontjait.

Tartományok csoportosítása

Az Interneten, mint IP hálózatok hálózatán, alapjában véve két tartomány típust különíthetünk el, a vég- és a tranzithálózatokat (*stub/transit domain*).

Beszélhetünk tehát:

- *Egyszerű véghálózatról*, mely csak egy összeköttetéssel kapcsolódik a „külvilághoz”, és átmenő forgalmat nem szállít. Tipikusan ilyen egy kisebb szervezet üzemi- illetve magánhálózata, például egy cég telephelyen létesített hálózat, egy irodai hálózat stb;

- *Többcsatornós kapcsolatú véghálózatról*, mely több összeköttetéssel is rendelkezik az Internet felé, de átmenő forgalmat nem bonyolít. Ez is tipikusan üzemi- illetve magán hálózat, de olyan, melynél az elérhetőség és a rendelkezésre állás kulcsfontosságú, ezért több kapcsolatot tart fent a külvilággal;

- *Tranzit hálózatról*, amely egy olyan szolgáltatói tartomány, ami átmenő forgalmat szállít. Ezek a hálózatok azok, melyek összekötik a kisebb magánhálózatokat és tulajdonképpen az Internet magját képezik.

Egy másik felosztás a tartományok gazdasági kapcsolatrendszerére alapján lehetséges. Kétféle kapcsolat-típust különítünk el. A *szolgáltató-ügyfél* viszonyt, ahol az ügyfél fizet a szolgáltatónak, és cserébe a szolgáltató biztosítja a külvilághoz való kapcsolatot, szerződésben rögzített feltételekkel. Az előző felosztásban ismertetett véghálózat–tranzit hálózathoz kapcsolat egy példa szolgáltató–ügyfél kapcsolatra. A *közvetlen (peer-ing)* kapcsolat esetén két tartomány egyenrangúként kapcsolódik össze, megosztva ennek költségét. Az egymás közötti forgalmat ezen az ún. első választású útvonalon keresztül bonyolítják, megkerülve a magasabb hálózati szinteket, így költséget takarítanak meg.

A tartományokat ezen kívül még hierarchikus elhelyezkedésük alapján is csoportosíthatjuk:

- *Tier-1*: globális méretű hálózatok, melyek az Internet gerincét alkotják,
- *Tier-2*: nemzeti méretű hálózatok és
- *Tier-3*: regionális hálózatok, a helyi hozzáférést biztosítják, tipikusan ezekhez kapcsolódnak a magán hálózatok

A különböző szintekbe sorolt tartományok mind kapacitásban mind számosságban jelentős eltérést mutatnak. Míg *Tier-1*-es hálózat csupán néhány van, addig a *Tier-3* és ez alatti hálózatok rendkívül nagy számúak. Ha még arra is gondolunk, hogy a tartományok mindegyikében ott kell legyen az összes másik tartomány elérhetőségi információja, akkor nem meglepő, hogy a skálázhatóság egy igen fontos szempont a tartományok közötti információ cserében.

Tartományok közti útválasztás BGP-vel

Mint korábban említettük, az Interneten élesen elkülönül a tartományon belüli és a tartományok közötti útválasztás. Az utóbbi célra a gyakorlatban egyetlen egy megoldást alkalmaz minden hálózati szolgáltató, a BGP-t. Egy tartomány a BGP segítségével tudja közölni a szomszédaival, hogy rajta keresztül mely címhalmazok, azaz *prefixek*, érhetőek el. A BGP távolságvektor alapú útvonalválasztást használ, ami annyit tesz, hogy egy címhalmaz elérhetőségét hirdető üzenetben a szükséges útvonal az útba eső tranzit tartományok listájaként kerül feltüntetésre. Idáig nem is tűnik bonyolultnak a dolog, azonban a BGP leglényegesebb része, amely jelentős befolyással van az útvonalválasztásra, egy szövevényes szabályrendszer (*policy*), és ez az, ami a BGP rugalmasságát, de sajnos a komplikált kezelhetőséget is adja. Ezen szabályokat minden AS lokálisan határozza meg saját maga számára, és ezzel szabályozza a saját tartományok közötti útvonalválasztását, így gyakorolva – közvetett – hatást a többi tartományra.

Két szabályrendszert különítünk el. Az úgynevezett import szabályok mondják meg, hogy az egyes kívülről érkező útvonalak közül a tartomány mely útvonalakat használja. Az export szabályok pedig meghatározzák, hogy az autonóm hálózat mely útvonalakat hirdeti tovább szomszédai számára. Ezek a szabályok lehetőséget adnak arra, hogy meghatározzuk, hogy milyen útvonalhirdetéseket fogadunk el illetve adunk tovább. Ilyen módon egy üzemeltető megteheti például, hogy hiába érhető el tőle egy versenytársa, ő ezt az elérhetőséget nem hirdeti más versenytársainak, csak saját ügyfeleinek. Hiszen neki nem érdeke a konkurencia forgalmának szállítása. A szabályok az üzleti érdekek mellett azt a célt is szolgálják, hogy ha egy útválasztó egy célcím-halmaz elérhetőségéről több különböző hirdetést is kapott, akkor az útválasztó képes legyen kiválasztani az egyetlen legjobbat.

A BGP azon tulajdonsága, hogy csak egyetlen utat jelöl ki használatra, illetve továbbhirdetésre a lehető legnagyobb stabilitást szolgálja. Ugyanakkor ezen tulajdonságának is köszönheti, hogy alig alkalmas a forgalommenedzsment támogatására. Ha egy BGP útválasztó több különböző hirdetést kap ugyanazon célcím-halmaz felé, akkor a hirdetésekben megtalálható attribútumok segítségével dönti el a preferencia sorrendet, s a végén csak a legmagasabb preferenciájú útvonallal foglalkozik.

Itt most csak két fő attribútumra térünk ki, melyeket a későbbiekben használni fogunk. A `local_preferance` lehetőséget ad a tartomány adminisztrátora számára, hogy meghatározza, hogy melyik kimenő útvonalválasztót használják a belső forgalomirányítók a tartományok közötti forgalom bonyolítására. Minden határcsomóponthoz rendelhető egy ilyen preferencia, és a beérkező hirdetéseket úgy szűrjük meg, hogy azt az útvonalválasztót használjuk a lehetségesek közül, amelynek a legnagyobb a preferenciája. A `multi_`

`exit_discriminator` (MED) hasonlóan használható, csak itt mi kérhetjük a szomszéd tartományt, hogy az ebben az attribútumban beállított értékek alapján válassza ki melyik bemeneti csomópontunkon át továbbítsa felénk a forgalmat. Ehhez persze szükséges, hogy több kapcsolatunk legyen a szomszédunkkal, hiszen különben nincs értelme a MED használatának. Másrészt meg kell egyezni a szomszéd hálózat operátorával, hogy valóban vegye figyelembe az általunk kért preferenciákat. A BGP TE lehetőségei iránt érdeklődő olvasó figyelmét felhívjuk a következő kitűnő összefoglalást adó cikkekre: [13,14,15,17].

Mint láttuk, a szabályok meghatározásában nagy szerepe van az üzleti szempontoknak. Ez az „üzleti szemlélet” tovább szűkíti a TE lehetőségeket, hiszen jól tükrözi, hogy itt nem lehet az egyes tartományokat vagy linkeket egyenrangúnak tekinteni, mint azt lehetett a tartományon belüli TE esetében. Így az sem csoda, hogy igen szűkösek az információ szerzési lehetőségek is, mivel egyik szolgáltató sem akarja felfedni saját belső hálózatának még a topológiáját sem, nem hogy a kihasználtság információit. Ilyen megszorítások mellett a legésszerűbb TE lépés az lehet, ha kis lépést teszünk, és nem az egész Internet forgalmát akarjuk egyszerre kezelni.

A legjobb kiindulás a tartományunkból kimenő forgalom megfelelő menedzselése. Ezzel lehetőségünk van a kimenő forgalmunk és a tartományon belüli forgalommenedzsment összehangolására. Az üzemeltető saját hatáskörében tudja optimalizálni – akár költségesség szempontjából is – a tartomány kimenő forgalmát figyelembe véve a kimenő linkek telítettségét, és a tartomány belső terhelés kihasználtság eloszlását. A kimenő forgalom menedzseléséhez minden szükséges információ rendelkezésre áll, hiszen a tartományunk kimenő linkeinek telítettségét az üzemeltető maga mérheti hasonlóan a belső linkek kihasználtság méréséhez, így a hálózati adminisztrátor képes a tartományon belül működő terhelés megosztó megoldásának kiterjesztésére egy lépéssel a hálózat határain túl.

A továbblépés előtt, bemutatunk néhány terhelés megosztó módszert.

Forgalomelosztás tartományon belül

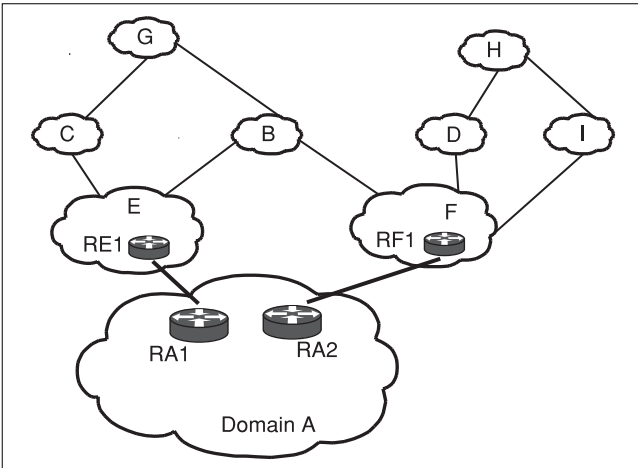
A hálózaton belüli útválasztó protokollok (OSPF vagy IS-IS) a legrövidebb utakat keresik meg a célcsoomópontig, és ezek közül is csak egyet használnak. Az utak hosszát a felhasznált élek költségeinek összege adja. A terhelésmegosztás érdekében az irodalomban javasolt eljárások megpróbálnak több útvonalat is kihasználni a forgalom terelésekor. Statikus megoldásról akkor beszélünk, ha a terhelésmegosztás nem veszi figyelembe a hálózat változó állapotát és a kihasználtsági viszonyokat. A dinamikus megoldások figyelik a hálózat állapotát, és a torlódott utakról elterelik a forgalom egy részét a több szabad erőforrással rendelkező útvonalak felé.

A legtöbb útválasztóban megtalálható *ECMP (Equal Cost Multi-Path)* [11] egy egyszerű, statikus terhelés elosztó megoldás, mely továbbra is csak legrövidebb utakkal dolgozik, azonban ha több egyforma legkisebb költségű út is létezik egy forrás/cél csomópont pár között, akkor ezekre egyenlő arányban tereli a forgalmat. Annak érdekében, hogy az egy folyamhoz tartozó csomagok azonos útvonalon haladjanak, az útválasztók az egy folyamra nézve közös csomagmezőkből (forrás/cél IP cím, forrás/cél port, protokollazonosító) hash eljárással egy adott intervallumba eső véletlenszerű számot képeznek. Az intervallum egyforma méretű részintervallumokból áll, melyek mindegyikét az útválasztó egy-egy alternatív kimeneti kapcsolathoz rendeli. Attól függően dől el egy adott csomaghoz használt kimeneti kapcsolat, hogy a hash érték mely részintervallumba esik.

Egy dinamikus megoldás az *OMP (Optimised Multi-Path)* [10]. Egy forrás/cél csomópont pár között több alternatív útvonalat képes felhasználni, mint az ECMP, mert egy útválasztó minden olyan szomszédot alternatívának tekint, amely közelebb van a célponthoz, mint saját maga. Ezáltal ugyan nem feltétlenül a legrövidebb utakat használja, mégis elkerüli, hogy kör alakuljon ki az útvonalban, hisz egy csomag nem juthat vissza egy korábban már érintett útválasztóhoz. Az alternatív utak közötti terhelésmegosztás hasonlóan megy, mint az ECMP-nél, hash eljárás és részintervallumok segítségével. Az OMP azonban a részintervallumokat nem egyforma hosszúra választja, hanem a hozzárendelt útvonalak kihasználtságához igazítja: minél telítettebb egy út, annál kisebb részintervallum tartozik hozzá. Működéséhez szükséges a hálózatban a kihasználtsági információk periodikus terjesztése. Az OMP egyik problémája, hogy ha változik a hálózat állapota, megváltoznak a részintervallumok hosszai, így lehet, hogy egy hosszabb ideig bent lévő folyam, melynek hash értéke változatlan, egyszer egyik útvonalhoz tartozik, másszor egy másik intervallumba esik. Ez azt jelenti, hogy egy folyam útvonala változhat, azaz a csomagok érkezési sorrendje különbözhet az indulásától, és az átviteli késleltetés is ingadozhat. Ezek csökkentik a TCP teljesítményét is, egyúttal a valós idejű forgalmak minőségét is rontják.

Az általunk javasolt *Core State Limited Load Sharing (CSLLS)* [12] eljárás csökkenti az útvonalak megváltozásának a valószínűségét azáltal, hogy fix ideig garantálja az útvonal választási döntések stabilitását. Ezt úgy éri el, hogy a kihasználtsági viszonyokhoz való alkalmazkodáskor csak az újonnan induló folyamatok útvonalát befolyásolja, a korábban beengedett folyamatokét nem. Legegyszerűbb esetben az új hívásokra vonatkozó részintervallumok súlyai arányosak a hozzájuk tartozó útvonalak szabad kapacitásaival.

Szimulációs vizsgálatainknál a CSLLS tartományon belüli forgalomelosztó megoldást terjesztettük ki hálózati működésre.



1. ábra Tartományok és kapcsolatok

Prefix	Kimenet	Útvonal
B	RA1-RE1	A-E-B
B	RA2-RF1	A-F-B
C	RA1-RE1	A-E-C
D	RA2-RF1	A-F-D
E	RA1-RE1	A-E
F	RA2-RF1	A-F
G	RA1-RE1	A-E-B-G
G	RA2-RF1	A-F-B-G
H	RA2-RF1	A-F-D-H
I	RA2-RF1	A-F-I

1. táblázat Az „A” tartomány ismeretei

A tartományon belüli forgalom-menedzsment kiterjesztése

A hálózatközi útválasztás megértéséhez tekintsük az alábbi példát (1. ábra) az „A” többszörös kapcsolatú véghálózat szemszögéből. A BGP protokoll segítségével az „A” tartomány tudja, hogy elérheti a „B”-től „I”-ig terjedő valamennyi címhalmazt (prefixeket). Ismeri azt is, hogy mely kimeneti éleken (RA1-RE1 vagy RA2-RF1) kell küldenie a csomagokat az egyes címek felé, sőt az útba eső autonóm hálózatok azonosítóit is ismeri. Az „A” tartomány hálózatközi útvonalainak ismereteit az 1. táblázat mutatja. Vegyük figyelembe, hogy a BGP működéséből adódóan egy tranzit hálózat egy prefixről több útvonalon is kaphat hirdetést, azonban ő maga ebből csak az egyiket hirdetheti tovább. Jelen példában az „E” tartomány megkaphatja a „G” címhalmaz útvesztését az „C” hálózaton keresztül és a „B” hálózaton keresztül is, azonban az „A”-nak ebből csak az egyiket adhatja tovább. Amint azt a táblázat mutatja, ebben a példában az „E” tranzit hálózat a „G” prefix felé csak a „B” hálózaton keresztülvezető útvonalat hirdette tovább „A”-nak (a hirdetések hátterét a „Tartományok közti útválasztás BGP-vel” fejezetben tárgyaltuk).

Amint az a táblázatból látható, az „A” tartomány a „B” és a „G” címhalmazok felé is rendelkezik alternatív útvonal ismeretekkel a BGP használatával is, de ezt a mai útválasztók nem képesek tudatosan kihasználni. A BGP protokoll lehetőséget ad arra, hogy az önálló tar-

tomány súlyozza kimeneteit a `local_preference` metrika segítségével. Lényegében ennek segítségével dönti el a tartomány, hogy mely útvonalat használja illetve hirdesse tovább, ha több is van. Egy egyszerű útválasztási megoldás, ha a tartományon belüli útválasztók, ha egy cél címhez több kimenet tartozik, akkor azt választják, amely a `local_preference` metrika szerint a preferáltabb.

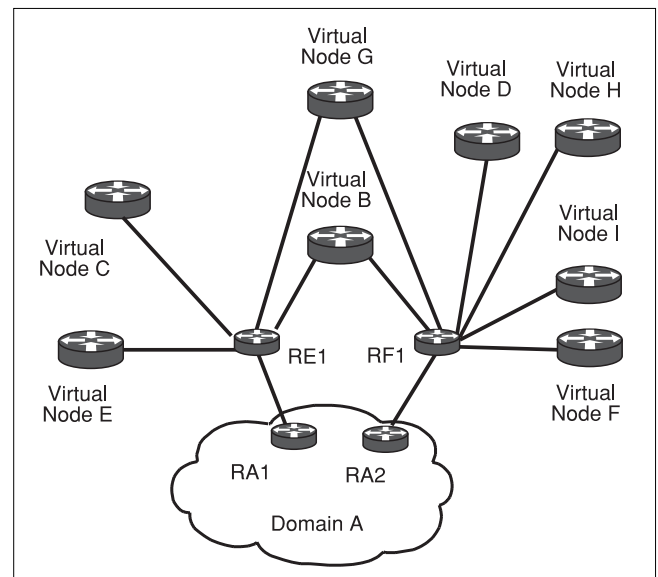
Jelenleg azonban egy tartományon belül az útválasztás nem az előző módon, hanem tipikusan a találón „forró krumpli útválasztásnak” (*hot potato routing*) nevezett módon történik. Ennek célja, hogy a csomagtól a lehető legrövidebb úton szabaduljon meg a hálózat (mint egy forró krumplitól), azaz a hálózat belüli útválasztó a legközelebbi alkalmas kimeneti csomópont felé továbbítja a csomagot. Amint látható, ez a módszer ugyan több kimenetet használ, azaz megosztja köztük a terhelést, de ez nem tudatos, nehezen befolyásolható és nem veszi figyelembe a kimeneti kapcsolatok telítettségét.

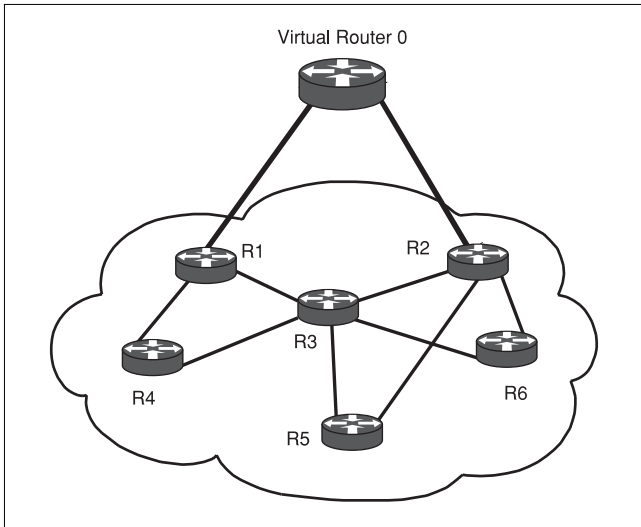
A javaslatunk szerint az „A” tartomány a hálózaton belül működő dinamikus terhelésmegosztó architektúráját egyszerűen, de tudatosan kiterjesztheti hálózatközi térbe is.

Ehhez először vázoljuk grafikusán a táblázat első két oszlopának információit (2. ábra), azaz hogy mely kimeneti kapcsolatokon mely cél cím halmazok érhetőek el. Ha ezeket a cél cím halmazokat mint virtuális útválasztókat tekintjük, akkor az így kapott virtuális hálózaton már használhatjuk a tartományon belül korábban használt terhelésmegosztó megoldásunkat, mellyel például nagyobb átbocsátóképességet nyerhetünk a „B” vagy „G” cél címek felé.

Az elérhető prefixek egyetlen leképezésével és felhasználásával tehát a már meglévő IP hálózatokban is képesek vagyunk terhelésmegosztást megvalósítani. Az elérhető nyereségről a korábbi útválasztó eljárásokhoz képest a következő fejezetben írunk.

2. ábra Tartományok leképezése az „A” tartomány szempontjából





3. ábra A vizsgált tartomány leképzett képe

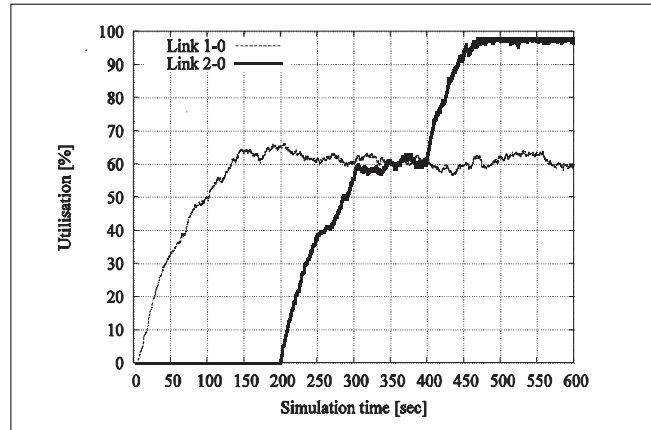
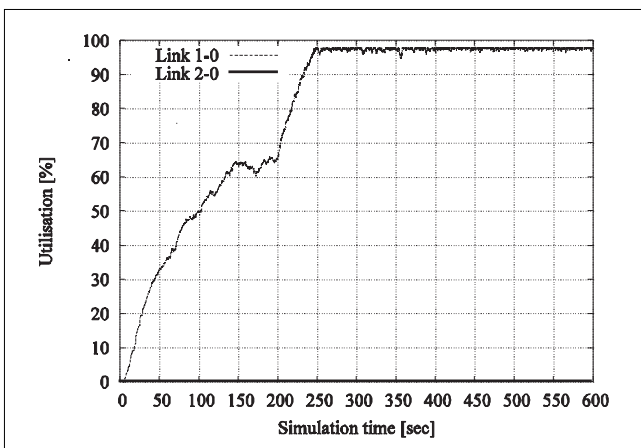
Vegyük persze figyelembe, hogy az autonóm hálózaton kívüli ismereteink szűkösek. A közvetlen a hálózaton kívüli kimenő kapcsolatok telítettségén kívül például biztos, hogy semmilyen információval nem rendelkezünk a virtuális útválasztók felé menő kapcsolatok kihasználtságáról, vagy aktuális szabad kapacitásáról. Ebben a cikkben azonban csak az a célunk, hogy a tartományunkból kimenő forgalmat optimalizáljuk.

Numerikus eredmények

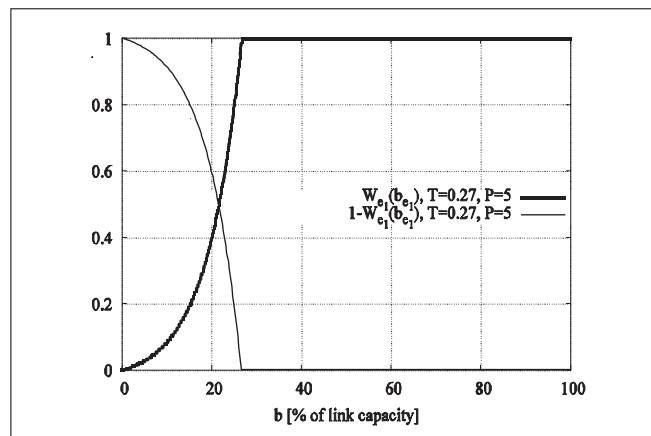
A következőkben néhány szemléletes eredményt mutatunk be. A 3. ábra mutatja az általunk vizsgált többszörös kapcsolatú végtartomány által a külvilágról leképzett virtuális képet. Az egyszerűség kedvéért bármely címtartomány elérhető mindkét határoló csomóponton keresztül, így a hálózatunkon kívüli teljes világ egy virtuális csomópontnak tekinthető.

A vizsgálatokat a *Network Simulator* csomagszintű hálózati szimulációs szoftverrel végeztük. Hogy jól megfigyelhetőek legyenek az algoritmusok sajátosságai, lépésenként növekvő forgalmat generáltunk. Ezt úgy ér-

4. ábra Egyszerű BGP megoldás



5. ábra BGP megoldás IGP metrika alapján



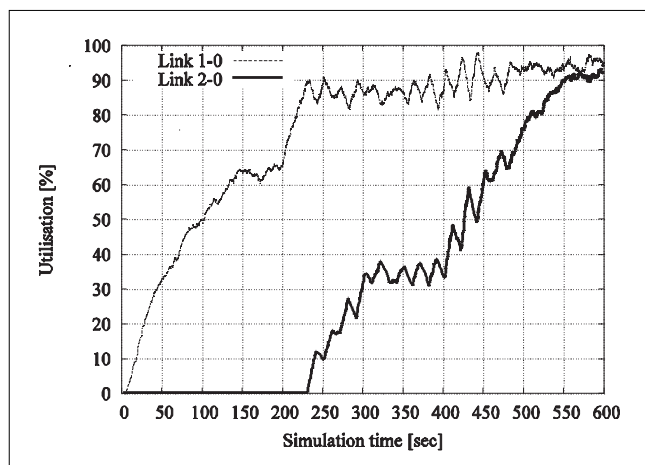
6. ábra Egy lehetséges súlyfüggvény a local_preference figyelembevételéhez

tük el, hogy először csak a 4-es csomópontból érkezett kimenő forgalom, majd az 5-ös csomópont is bekapcsolódott az adatküldésbe, és végül a 4-es, 5-ös és 6-os csomópont mind generált forgalmat.

Nézzünk meg két alap BGP esetet. Először is, ha az egyik link `local_preference` attribútuma nagyobbra van állítva, ezzel például tükrözve, hogy ez az elsődleges útvonal és a másik csak egy tartalék kapcsolat. Ekkor minden kimenő forgalom ezt a linket fogja igénybe venni, és annak ellenére, hogy ezen torlódás alakul ki, a másik link kihasználatlan marad. Ezt mutatja a 4. ábra.

Természetesen, ha nem csak védelmi útvonalként kívánjuk használni a másik linket, akkor lehetőségünk van ezt a BGP-vel is megvalósítani. Erre egy módszer, ha a belső útvonalválasztó protokoll (*Interior Gateway Protocol – IGP*) által látott legrövidebb útvonalat használjuk a kimenő forgalom mielőbbi kijuttatására a hálózatunkból. Ez esetben azonban az elérhető terhelés kiegyenlítés a topológiai sajátosságoktól függ. Ezt jól mutatja a 5. ábra, ahol látszik, hogy amint a forgalom érkezése topológiai szempontból előnytelen, akkor a terhelés kiegyenlítés rögtön felborul.

Kínálkozik azonban egy jó alternatíva, hogy egyesítsük a terhelés kiegyenlítés és a gazdaságossági szempontok előnyeit. Lazíthatjuk a `local_preference`



7. ábra Terhelés kiegyenlítés
a *local_preference* attribútum alapján

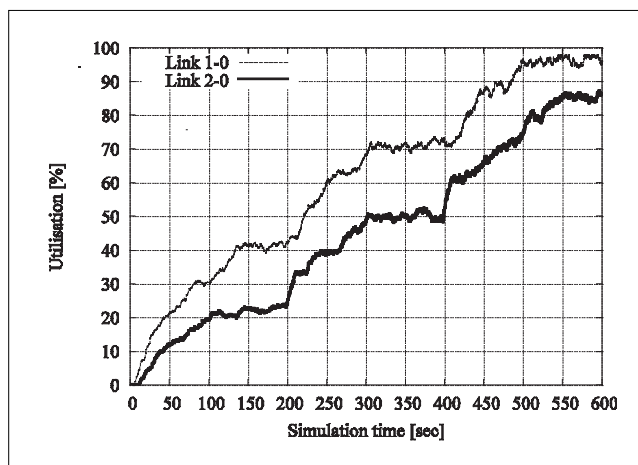
attribútum kötöttségeit, ha egy súlyfüggvényt alkalmazunk, amely egy bizonyos terheltségig határozottan preferálja az elsődleges linket, de annak túlzott telítődése esetén a védelmi utat is elkezd terhelni, hogy elkerülje a linkek telítődését. Egy lehetséges függvényt mutat a 6. ábra. Az ennek segítségével kapott link terhelése a 7. ábra mutatja.

Egy másik lehetőség a *MED* attribútum alkalmazásával tesz lehetővé terhelés kiegyenlítést. Ennek segítségével a szomszédos tartomány belső terhelésének jobb eloszlására nyílik lehetőség, azáltal, hogy az általa kívánt arányban osztjuk meg a bemenő forgalmát, mely a mi kimenő forgalmunk. Egy egyszerű módszer lehet, hogy az egyes tartományok közötti linkekre terjesztett *MED* értékeket súlynak tekintve, a súlyok valamilyen függvényeként terheljük meg az egyes linkeket. Egy egyszerű függvény alkalmazásának eredménye a 8. ábra, ahol az 1–0 linket nagyobb súlyúnak állítottunk be a *MED* segítségével.

Összegzés

A tartományok közötti TE egy igen fontos kérdés lehet a hálózatok közötti forgalmak optimalizálásában. Sajnos az igen erős gazdasági érdekeltségek illetve érdekkellentétek jelentősen megnehezítik, sőt akár lehetlenné is teszik, egy globális méretekben gondolkodó TE megoldás alkalmazását.

Egy frappáns megoldás lehet az egyes tartományok üzemeltetői számára, hogy a korlátozott lehetőségeket számukra a lehető leghatékonyabb módon kihasználják. Mi ehhez adtunk egy javaslatot cikkünkben. Nevezetesen, a tartományon belül alkalmazható – esetleg már alkalmazott – TE megoldást összehangoljuk a tartomány kimenő forgalmának hatékony irányításával. Így a tartomány belső terheltség elosztását – mely teljes hatáskörünkben van – úgy irányíthatjuk, hogy az a tartomány számára legköltségesebb adatáramlást – a tartomány kimenő forgalmát – optimalizálja.



8. ábra
Terhelés kiegyenlítés a *MED* attribútum segítségével

Irodalom

- [1] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, X. Xiao, "Overview and principles of internet traffic engineering" RFC 3272, IETF, 2002. május
- [2] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus, "Requirements for traffic engineering over mpls," RFC 2702, IETF, 1999. szeptember
- [3] Daniel O. Awduche, "Mpls and traffic engineering in IP networks," IEEE Communications Magazine, Vol. 37, no.12, pp.42–47, 1999. december
- [4] A. Feldmann, A. Greenberg, C. Lund, N. Reingold, J. Rexford, "Netscope: Traffic engineering for IP networks," IEEE Network Magazine, Vol. 12, no.2, pp.11–19, 2000. március
- [5] Ashwin Sridharan, Roch Guérin, Christophe Diot, "Achieving near-optimal traffic engineering solutions for current OSPF/IS-IS networks," Tech. Rep., University of Pennsylvania, 2003. (egy rövidebb verzió megjelent az InfoCom'2003 konferencia kiadványban)
- [6] Yufei Wang, Zheng Wang, Leah Zhang, „Internet traffic engineering without full mesh overlaying”, InfoCom'2001, Anchorage, Alaska, 2001. április
- [7] Bernard Fortz, Mikkel Thorup, "Internet traffic engineering by optimizing OSPF weights", IEEE InfoCom'2000, pp.519–528, Tel-Aviv, Israel, 2000. április
- [8] Tracie E. Monk, "Inter-domain Traffic Engineering: Principles and Case Examples," INET2002, 2002. június
- [9] Raymond Zhang, J.P. Vasseur, "Mpls inter-as traffic engineering requirements," Internet Draft, 2004. január
<draft-ietf-tewg-interas-mpls-te-req-04.txt>

- [10] C. Villamizar,
"OSPF optimized multipath (OSPF-OMP),"
A 44-ik IETF kiadványban, 1999. március,
draft-ietf-ospf-omp-02.
Minneapolis, MN, USA: IETF, 1999. március
- [11] C. Hopps,
„Analysis of an equal-cost multi-path algorithm,”
IETF, RFC2992, 2000. november
- [12] A. Takács, A. Császár, R. Szabó, T. Cinkler,
"Thrifty traffic engineering through CSLLS,"
18th International Teletraffic Congress ITC18,
ser. LNCS, Teletraffic Science and Engineering,
Vol. 5., Germany: Elsevier, pp.61–70, 2003. szept.
- [13] Nick Feamster, Jay Borkenhagen, Jennifer Rexford,
„Guidelines for interdomain traffic engineering,”
ACM SigComm Computer Communication Review,
2003. ősz
- [14] Tracie E. Monk,
"Inter-domain Traffic Engineering:
Principles and Case Examples," INET 2002. június
- [15] Bruno Quoitin, Louis Swinnen,
Oliver Bonaventure, Steve Uhlig,
„Interdomain traffic engineering with BGP,"
IEEE Communications Magazine,
pp.122–128, 2003. május
- [16] Y. Rekhter, T. Li, és mások,
„A border gateway protocol 4 (BGP-4),"
IETF, RFC1654, 1994. július
- [17] Marco Gaertler, Maurizio Patrignani,
„Dynamic Analysis of the Autonomous System Graph",
Proceedings of the 2nd International Workshop
on Inter-Domain Performance and Simulation
(IPS2004), Budapest, 2004. március

Hírek

A **Sun Microsystems**, mint a nyílt forráskódot támogató közösség tagja, a Linux World konferencia és Expo-n elhatározta, hogy az AMD Opteron(tm) processzorokra épülő rendszerek továbbfejlesztett családjával biztosítja a 64 bites vállalati rendszerek, a nagytömegű szerverek és munkaállomások alkalmazását. Így a Sun Java Desktop Systems egyértelmű előnyei világszerte tovább növelik a LINUX népszerűségét. A cég a konferencia keretében bepillantást engedett a Solaris 10 OS egyik új, Project Janus kódnevű technológiájába, amely lehetővé teszi a bináris Linux-alkalmazások változatlan formában történő futtatását Solaris OS alatt.

Az **Oracle Application Server 10g** egy olyan integrált, szabványokon alapuló szoftverplatform, amely az adott vállalat méretétől függetlenül lehetővé teszi a változó üzleti követelményekhez történő hatékony alkalmazkodást. Az Oracle Application Server 10g egy csomagba integrálja a J2EE és a számítógépek támogatását, a beépített nagyvállalati portálszoftvert, a gyorsítóárazást, az operatív üzleti adatelemzést, és üzleti folyamatok integrációját, a vezeték nélküli szolgáltatásokat, valamint a web-szolgáltatásokat. Az Oracle Application Server Portal 10g nemrégiben elnyerte a Network Computing rangos szerkesztői díját (Editor's Choice). A „Well-Connected” díjat, amelyet a vállalati környezetben megfigyelt teljesítmény és a különböző teszteredmények alapján ítélnék oda, és az adott év kiemelkedő technológiai termékei és szolgáltatásai kapják. A nyerteseket a Network Computing magazin „Real-World” laboratóriumában tesztelt és értékelt termékek közül szakértő szerkesztők választják ki. A Network Computing az egyes portáltermékeket általános felépítésük, megvalósításuk, biztonsági jellemzőik, áruk és bővíthetőségük alapján értékelt ki, és figyelembe vette, hogy a termékek szabvány alapú alkalmazásokkal és szolgáltatásokkal integrálhatók-e.

A **rEVOLUTION** augusztusban adta el tízezredik Iroda Sorozat szoftverét. Az uniós csatlakozás óta érezhetően megnőtt a kisvállalkozói szoftverek iránti kereslet. Ez egyrészt az Európai Unió csatlakozást követő új törvényi előírásokkal indokolható – amelyek többek között az egyéni vállalkozókat, illetve a devizaszámlát kiállító cégeket érintik leginkább –, másrészt az elvárt, uniókonform cégmegjelenéssel, valamint a piaci verseny erősödése miatt szükséges, naprakész nyilvántartások vezetésével. Az európai uniós csatlakozás ugyanis a számlakiállítás módjában is számos változást ír elő. A csatlakozást követően kötelezővé vált számos új adat feltüntetése (például közösségi adószám feltüntetése közösségi termékértékesítés és szolgáltatásnyújtás esetén), átalakult az előleghámla, más adatok szerepeltetése pedig (például vállalkozói igazolvány számának feltüntetése) a megváltozott adóbefizetési kötelezettségek miatt a vállalkozások egy részénél ajánlott, hiszen elmulasztása plusz adóelőleg-, illetve áfabefizetést von maga után. A kisvállalkozói számlázó szoftverek piacának egyik szereplője, a rEVOLUTION Software a nyári hónapokban is eladást-növekedést jelzett a szoftverek értékesítésében.