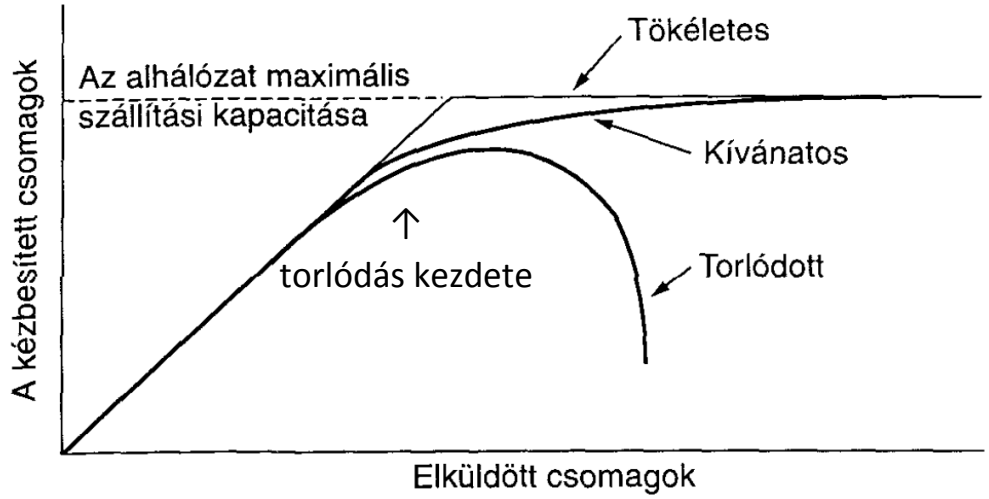
19. fejezet – Torlódáskezelés és A szolgáltatás minősége

Torlódáskezelési algoritmusok

Minden hálózat fizikai rétegében megvannak a teljesítőképesség határai, korlátai. A hálózatok méretezésekor szem előtt kell tartani a várható forgalmat valamint az igénybe vett fizikai réteg(ek) teljesítőképességét. A legkörültekintőbb tervezés mellett is előfordul, hogy egy hálózatban annyira megnő a csomagok száma, hogy a csomagok csak jelentős késedelemmel jutnak el a célállomásokra. Ez a jelenség a torlódás (Congestion).
A torlódásból fakadó problémák közvetlenül a hálózati réteget érintik, hiszen itt jelennek meg a többletcsomagok, melyek csak jelentős késedelemmel kerülhetnek elküldésre. A többletcsomagok átmeneti tárolása a hálózati rétegben csak részmegoldást jelenthet, hiszen egyre több csomag tárolása már időzítési problémákat is okoz, hiszen a csomagoknak egy adott időszegmensen belül meg kell érkezniük. Az igazi megoldást, a torlódások hatékony kezelését csak a hálózati és a (felette elhelyezkedő) szállítási réteg együttműködése biztosíthatja, azaz amikor a szállítási réteg nem „terheli túl" a hálózati réteget (illetve gyakorlatilag lefelé haladva végül is a fizikai réteget).

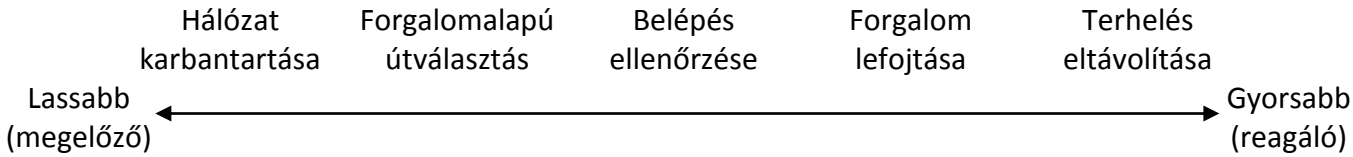


A torlódások nem megfelelően hatékony kezelése a hálózat forgalmának összeomlását is okozhatja.
A torlódások kezelése és a forgalomszabályzás, mint fogalmak közel állnak egymáshoz, és a két fogalom könnyen össze is keverhető. A különbség (mint általában) itt is az ok és az okozat megismerése után lesz egyértelmű.

A forgalomszabályzás feladata az, hogy két kommunikáló hoszt minél folyamatosabban és zökkenő mentesebben legyen képes az adatcserére. Tipikus eset két különböző sebességű hoszt kommunikációja. Ha a vevő a gyorsabb (pl. 1Gb/s-os hálózathoz kapcsolódik) és az adó a lassabb (pl. 100Mb/s-os hálózathoz kapcsolódik) akkor hálózati szempontból nem merül fel megoldandó kérdés, hiszen a gyorsabb vevő kénytelen kivárni a lassabb adó csomagjainak beérkezését. Fordított esetben azonban mindenképpen hatékony forgalomszabályzásra van szükség, hiszen egy gyorsabb adót a lassabb vevő képességeihez kell lassítani, azaz ciklikusan megállásokra kényszeríteni. (Természetesen más folyamatok illetve szálak futhatnak a gyors adóban, csak a csomagjai forgalmát kell szabályozni.)
A torlódáskezelés feladata, hogy a hálózat képes legyen (a hálózati réteg és az alatta lévő rétegek segítségével – végeredményben a fizikai rétegtől elvárható maximális teljesítmény mellett) az átvitelt megoldani, azaz képes legyen minden csomagot a kellő időben elszállítani. A torlódáskezelés, tehát nem hoszt-hoszt közötti kérdés, hanem a hálózat (szegmens illetve tartomány) egészére vonatkozó kérdés. Amennyiben egy hálózaton belül sok hoszt kezd el egymással – akár az érdemi forgalomszabályozás igénye nélkül is – kommunikálni, a hálózat eljuthat a fizikai teljesítőképessége határára. Torlódást okozhatnak továbbá a kis sávszélességű aktív hálózati elemek is.
A két fogalom összekeverésének fő oka valószínűleg az, hogy mindkét esetben valamilyen lassítási eljárás a célravezető megoldás.

A torlódáskezelés alapelvei

A torlódás kialakulása tehát azt jelenti, hogy a hálózat terhelése (még ha csak ideiglenesen is) nagyobb, mint amit a hálózat erőforrásai kezelni képesek. A megoldás tehát ezzel a két dologgal kell, hogy kapcsolatos legyen, azaz vagy a terhelést csökkentése, vagy az erőforrások növelése jöhet szóba. A különböző megoldások feloszthatók megoldás reakcióideje, vagy reagálása alapján is egészen a tervezett megelőzéstől az azonnali gyors beavatkozásig.



- Hálózat karbantartása, megfelelő hálózat építése

  A legalapvetőbb dolog, hogy a hálózatunk a tervezett forgalomnak megfelelően kerüljön kiépítésre, mind az aktív, mind a passzív elemek vonatkozásában. A kis sávszélességet biztosító megoldások a terhelés megnövekedésekor torlódást okozhatnak. Ne felejtsük el, hogy sok egyenként zökkenőmentes kommunikáció is torlódást okozhat, ha szűk a hálózat áteresztő képessége.

  A már üzemelő hálózat aktív eszközei sem mentesek a meghibásodásoktól, zavaroktól. A meghibásodott eszközök komoly fennakadásokat okozhatnak, akár össze is omlaszthatják az egész hálózatot. Menedzselhető aktív hálózati eszközök használata esetén, ha a rendszergazda rendszeresen ellenőrzi a hálózat kondícióit, akkor még egy komoly hiba bekövetkezése előtt képes megtenni a megfelelő lépéseket (például egy bizonytalanul működő Switch cseréjét).

  Az aktív eszközök cseréjét nem csak a meghibásodás indokolhatja, hanem a menet közben megnövekedett igények is. (Ezzel kapcsolatos fogalom a beruházás védelem, ami azt jelenti, hogy célszerű mindig egy kategóriával magasabb műszaki beltartalmú kábelekkel kiépíteni a hálózatot, hiszen amennyiben a későbbiekben igény merül fel a magasabb sebességre illetve nagyobb áteresztőképességre, akkor az aktív eszközöket viszonylag egyszerűen ki lehet cserélni, de egy épületet újrakábelezni már nem olyan egyszerű dolog.)
- Forgalomalapú útválasztás

  A korábbiakban már tárgyalt adaptív algoritmusok, melyek figyelembe veszik a hálózat aktív elemei közötti távolságot és átviteli sávszélességet, valamint a sebességet is mint, komplex topológiát, de ezek mellett az aktuális hálózati forgalommal is számolnak. A preferált útvonalakat így valóban a pillanatnyi terhelésnek megfelelően képesek kiválasztani.
- Belépés ellenőrzése

  A belépés ellenőrzés (Admission Control) a virtuálisáramkör alapú hálózatok (azaz az összeköttetés alapú rendszerek) jellemzően használt megoldása a torlódások elkerülésére. Ez azt jelenti, hogy egy virtuálisáramkört csak akkor építünk fel, ha a hálózat képes ezen virtuálisáramkör kapcsolat csomagjait – azaz a megnövekedett forgalmat – torlódások kialakulása nélkül célba juttatni. A gyakorlat azonban nem ennyire egyszerű, hiszen nem minden esetben jósolható meg sebesség sem, a forgalom pedig, ami ráadásul jellemzően löketes pláne nem.

- Forgalom lefojtása

  A cél a forgalom olyan mértékű korlátozása, hogy az még éppen a torlódási állapot alatt maradjon. Ennek eléréséhez először is az útválasztóknak meg kell tudniuk határozni, hogy torlódás közeli állapotba kerültek, lehetőleg úgy, hogy még maradjon idő és lehetőség a beavatkozásra, azaz a torlódás elkerülésére. Figyelni kell a bemenő és kimenő pufferek telítettségének változásait, az elveszett csomagok számát és a processzor terheltségét.

  A kialakult helyzet egyik kezelési módja, ha a kialakulófélben lévő torlódást okozó útválasztók felé erről az állapotról jelzést küldünk (lefojtó csomagok formájában), és végül a megfelelő helyen beavatkozunk, azaz elérjük, hogy csökkenjen a csomagok száma.

  Egy másik kezelési mód az explicit torlódáskezelés (ECN – Explicit Congestion Notification) amikor az az útválasztó, mely a torlódási helyzet kialakulására kíván figyelmeztetni, nem közvetlenül azt az útvonalválasztót értesíti, ahonnan a csomagok érkeznek, hanem a továbbított csomagokat egy speciális jelzőbittel látja el. Ezt a jelzőbitet a célállomás észleli, és ezután a célállomás értesíti az adóállomást válaszcsomagjában, így érve el a forgalom lassítását.

  Nagyobb távolságok és nagyobb sebesség esetén egy harmadik módszer a jellemző, a lépésről lépésre visszaszorítás (Hop-by-Hop Backpresure). Nagy kiterjedésű hálózatok esetében jelentős idő az, amíg a jelzések a megfelelő helyre eljuthatnak. A lépésről lépésre visszaszorítás esetében a lefojtó csomag minden közbülső útválasztóra hat, ezért a várt hatás hamarabb bekövetkezik.

  A forgalom lefojtása, mint módszer virtuálisáramkör kapcsolt, és datagram alapú hálózatok esetében is használható.

- Terhelés eltávolítása

  Abban az esetben, amikor az eddigi módszerek nem vezetnek eredményre (mert például folyamatosan újabb és újabb forgalom generálódik) nem marad más megoldás, mint a terhelés eltávolítása (Load Shedding). Ez egy drasztikus, de hatékony megoldás, amikor az útválasztók azokat a csomagokat, amelyek a torlódás kialakulásához (illetve fenntartásához) vezettek elvetésre kerülnek. Az eldobott csomagokat természetesen előbb utóbb az érintet hosztok meg fogják ismételni, de ez már talán egy szerencsésebb környezetben fog megtörténni. Így relatíve kis (kvázi kalkulált) veszteség árán elkerülhetjük az egész hálózat összeomlását. Fontos kérdés a priorizálás, azaz, hogy melyik csomagok kerüljenek eldobásra.

Fáljátvitel esetén a régebbi csomagok eldobásánál általában célszerűbb az újabb csomagok eldobása, hiszen csomagokat érkezési sorrendjüknek megfelelően kell majd a felsőbb rétegek felé átadni, és nem mindegy, hogy mennyi csomagot kell pufferelnünk azért, mert korábbi csomagok érkezését várjuk.

Ezzel ellentétes a valós idejű média átvitele, ahol az új csomag fontosabb, mint a régi, mert ha kis ugrással is, de a hang és képátvitel így (kvázi) folyamatos maradhat. Egy régebbi csomag későbbi megérkezése ez esetben abszolút felesleges.

Ez a két koncepció a bor politikájának, illetve a tej politikájának nevezik. Ez arra utal, hogy a régi, azaz az óbor és az új, azaz friss tej, (persze külön-külön) szerencsésebb választás, mint az újbor és a régi tej. A hasonlat persze a közízlést tükrözi, így akár meg is támadható, de legalább szemléletes…

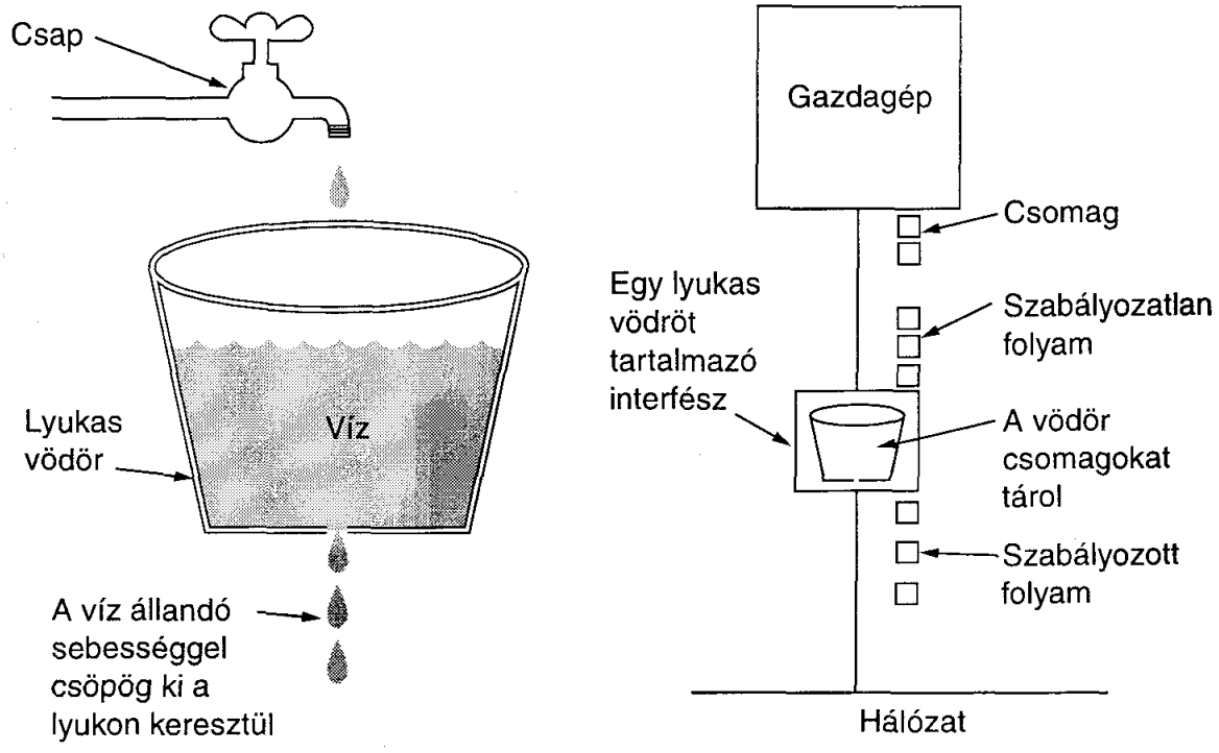
További fontos szempont a torlódás, mint kialakuló helyzet minél korábbi észlelése. Amennyiben a problémát a tényleges felmerülése előtt elkezdjük kezelni, komoly reményünk lehet arra, hogy el is fogjuk tudni kerülni a problémát. A legelső árulkodó jel, amit a rendszernek komolyan kell vennie, az a csomagvesztés. Így akár egy útvonalválasztó akár szándékosan (tehát nem valamely éppen fennálló hiba miatt) is elkezdheti eldobálni a csomagokat, nehogy a helyzet tovább romolva elinduljon a torlódás lejtőjén az összeomlás felé. Az erre szolgáló algoritmus a véletlen korai detektálás (RED – Random Early Detection). Ez esetben az útválasztók figyelik a puffereiket, illetve az egyes portokon a sorok hosszát. Amennyiben a sorhossz elér egy küszöbszintet, ami egyébként még nem jelentene torlódást, de tendenciát igen, az útválasztó elkezdi véletlenszerűen eldobálni az innen érkező csomagokat. Az adó hosztok természetesen érzékelik a csomagvesztést, mivel nem kapnak időben (illetve egyáltalán nem kapnak) nyugtát. Ez a megoldás főleg akkor használatos, ha az útválasztók illetve a hosztok nem képesek az ECN jelzőbitjének érzékelésére.

A lyukas vödör és a vezérjeles vödör algoritmus

A hálózaton az egy adott hoszttól egy másik hosztig továbbított csomagok összességét folyamnak (Flow) nevezzük. Az útválasztók jellemzően a csomagok érkezésének megfelelő sorrendben (FIFO – First In First Out) végzik a kiszolgálást. A beérkező csomagokat pufferelik, és amint lehetőség van rá, továbbítják is azokat. A pufferek mérete nyilván véges, és az sem ritka, hogy egy puffer megtelik, azaz képtelen további csomagok fogadására. Korábban már bizonyítottuk, hogy a végtelen puffer sem jelente megoldást a megnövekedett késleltetés miatt. A megoldás a beérkező csomagok mennyiségének valamilyen korlátozása.

A lyukas vödör (Leaky Bucket) algoritmus (J. S. Turner, 1986) valóban egy lyukas vödörhöz hasonlítható, amennyiben elfogadjuk, hogy a víz bármilyen sebességgel is jusson bele a vödörbe, a lyukon keresztül mindig azonos sebességgel távozik a víz (amennyiben persze nem üres a vödör). Nyilván, ha a vödör megtelik, akkor a továbbiakban érkező víz a vödör szempontjából elveszik.

A modellből azt kell észrevenni, hogy a beáramlás hektikus is lehet, a kiáramlás akkor is egyenletes marad, azaz a kimeneti sebesség a bementi sebességtől függetlenül állandó marad. Az ábra csak egy csapot tartalmaz, de a valóságban egy hoszton belül egyszerre több folyamat is szándékozhat csomagokat küldeni. További analógia azon csomagok eldobása, melyek már nem férnek bele a vödörbe, azaz az átmeneti tárolóba.



A fenti modell előnye tehát az állandó kimeneti sebesség, azonos csomagméret esetén hatékony. Amikor azonban jelentős méretbeli különbség van az egymást követő csomagok között, akkor a sebesség nem biztos, hogy állandó szinten tartható. (Az analógia szerint a cseppek száma és mérete időben állandó.)
Azt se felejtsük el, hogy az alkalmazásaink egy része azt preferálná, hogy amennyiben a hálózat más paraméterei azt nem korlátozzák, a kimenő adatfolyam rugalmasan változtassa a sebességét, de lehetőség szerint ne veszítsen csomagot. Ezt a modellt a vezérjeles vödör (Token Bucket) valósítja meg. Ez esetben a működés mechanizmusa annyiban tér el a lyukas vödör működési mechanizmusától, hogy a vödör ugyan ez esetben is lyukas, de a kiáramlást változó ütemben (általában a telítettség függvényében) generált vezérjelek engedélyezik. Csomag csak vezérjellel együtt, és annak ütemében távozhat a vödörből.
A fő eltérés a két algoritmus között az, hogy a vezérjeles vödör, amikor megtelik, akkor jelzi a küldő hosztnak, hogy nem képes több csomag fogadására, míg a lyukas vödör egyszerűen eldobja a csomagokat.

A szolgáltatás minősége

A torlódások kezelése illetve a forgalom megfelelő szabályozása a legtöbb esetben olyan kompromisszummal jár, ami valamekkora lassuláshoz vezet. Ez a lassulás azonban a felhasználó szintjére az esetek egy jelentős részében nem jut el, hiszen a hivatkozási modell minden egyes rétege a maga lehetőségei szerint optimumra törekszik, de legalább is az adatforgalom fenntartására. A szolgáltatás minősége, mint fogalom nem azonos a hálózat sebességével, sokkal inkább kapcsolatos a hálózat teljesítőképességével.
Arról sem szabad megfeledkezni, hogy milyen jellegű forgalom lesz jellemző a hálózatra – pontosabban fogalmazva, hogy milyen arányban oszlanak meg a különféle hálózati szolgáltatások. Vannak olyan – például multimédiás – alkalmazások, ahol az időzítés a valós időt kell, hogy minél jobban megközelítse, esetleg a csomagok egy kisebb százalékának elvesztése árán is; illetve léteznek olyan alkalmazások – melyek alapja a fájl átvitel – ahol egy adathalmaz tökéletes átvitele az egyedül elfogadható eredmény, függetlenül attól, hogy az egyes csomagokat hányszor kellett megismételni az átvitel folyamán.
Fontos szempont a hálózat kapacitásának méretezésekor a kialakítandó hálózatunk tervezett (helyi és átmenő) forgalma. Ezek szerint egy túlméretezett hálózat szolgáltatásának a minősége jobb, mint egy átlagosan vagy esetleg alulméretezett hálózaté. A túlméretezés azonban jelentős többletköltségekkel jár, ezért természetesen kerülendők az ésszerű tartalékokon túlmutató, pénzt és erőforrást pazarló megoldások.

Ahhoz, hogy a hálózatunk szolgáltatásának minőségét megfelelő módon biztosítani, illetve garantálni tudjuk, összefoglalva a következő négy alapvető szempontot kell megvizsgálni.

- A tervezett helyi forgalom és a várható átmenő forgalom mértéke és aránya.
- A hálózatot igénybevevő szolgáltatások jellege és aránya.
- A hálózatba belépő forgalom szabályozhatósága.
- A hálózat aktív elemeinek teljesítőképessége az erőforrásaik ismeretében.

A definíció szerint a hálózati szolgáltatás minőségét (QoS – Quality of Service) bármilyen típusú és jellegű adatforgalom esetén is ugyanaz a négy paraméter határozza meg:

- Sávszélesség
  A hálózat aktív és a passzív eszközei által biztosított gyakorlati maximum.
- Késleltetés
  A hálózat objektív csomag átviteli, pufferelési késleltetése, mely az aktív és a passzív eszközök, a morfológia, valamint a szoftverek függvénye.
- Dzsitter (Jitter)
  A dzsitter a csomagok érkezési idejének szórását, azaz a minimális (tehát optimális) és még elviselhető maximális késleltetési idő arányát jelenti. A szabálytalan időközönként (nagy dzsitterrel) érkezett csomagok az aktív eszközből pufferelés után már normális időközönként (kis dzsitterrel) távozhatnak.
- Megbízhatóság illetve veszteség
  A hálózat csomagvesztéséi illetve csomag ismétlései alapján meghatározható érték. Nem szabad arról megfeledkezni, hogy csomagvesztések sok esetben ismétléssel, vagy hibajavítással korrigálhatók.

Az egyes hálózati alkalmazások a négy paraméterre nem egyformán érzékenyek, azokat nem azonos súllyal igénylik.

Alkalmazás	Sávszélesség igény	Késleltetési érzékenység	Dzsitter érzékenység	Megbízhatóság illetve veszteség érzékenység
E-mail	kicsi	kicsi	kicsi	közepes
Fájlmegosztás	nagy	kicsi	kicsi	közepes
Web böngészés	közepes	közepes	kicsi	közepes
Távoli bejelentkezés	kicsi	közepes	közepes	közepes
Net rádió/zene	kicsi	közepes	nagy	kicsi
Net TV/Video	nagy	közepes	nagy	kicsi
Net Telefon/VoIP	kicsi	nagy	nagy	kicsi
Net Videókonferencia	nagy	nagy	nagy	kicsi

A gyakorlatban, azokon az aktív eszközökön, ahol arra lehetőségünk van a QoS beállítására jellemzően szolgáltatási kategóriát és/vagy az ahhoz tartozó paramétereket adhatjuk meg.

- A rendelkezésre álló maximális adatsebesség
  fájlátvitel esetében
- Állandó adatsebesség
  VoIP alkalmazások esetében
- Valós idejű, de korlátok között változó adatsebesség
  Realtime video stream esetében
- Nem valós idejű, de korlátok között változó adatsebesség
  Online video esetében (változó adattömörítés)