A QoS hatása az infokommunikációs alkalmazásokra

GÁL ZOLTÁN, BALLA TAMÁS

Debreceni Egyetem TEK, Információtechnológiai Központ
zgal@.unideb.hu, ballat@delfin.unideb.hu

Kulcsszavak: QoS, IPv4, IPv6, TCP, UDP, torlódás, jitter, VoIP, codec, H.323, H.261/H.264, ATM

A hálózati szolgáltatásminőség (Quality of Service) olyan funkció, amely segítségével a forgalom kezelése történik az alkalmazói programok számára. Ehhez alapvető forgalomkezelési mechanizmusokra, valamint ezeket ellenőrző algoritmusokra van szükség. A QoS-funkcionalitás egyrészt a hálózati alkalmazásokat, másrészt pedig a hálózati adminisztrátorokat szolgálja ki. Addig, amíg a hálózati adminisztrátor korlátozza az erőforrásokat, az alkalmazás az erőforrások minél szélesebb körét próbálja igénybe venni.

A QoS az Internet technológiák környezetében a VoIP (Voice over IP) megoldás telefonbeszélgetés költségcsökkentő hatásának következtében jelent meg és terjed el egyre inkább. Az Internet- és intranet-alapú új, sávszélességigényes alkalmazások, valamint az adat-, hang- és videóforgalom IP-infrastruktúra feletti konvergenciája ugyancsak a QoS iránti igényeket hangsúlyozza. A jelenlegi alkalmazások több mint 95%-a Ethernet csomópontokban végződik, így a csomagok ezen átviteltechnikán való homogén továbbítása költségcsökkentést jelent, mivel nem szükséges protokollkonverzió az adatok továbbítása során. A cikkben a QoS mechanizmus L2 és L3 rétegekben kifejtett hatását vizsgáljuk meg egyetlen QoS tartományon belül szabályozott paraméterek segítségével, H.261 és H.264 videó codec alkalmazása mellett. Konkrét mérések alapján az Interneten hagyományosan működő hálózati alkalmazások viselkedését tanulmányozzuk néhány QoS paraméter módosítása esetén. Vizsgáljuk az UDP és a TCP hálózati erőforrás kihasználását és számszerű mérési módszert javaslunk a videóműsor minőségének elemzésére, valamint megvizsgáljuk, hogy IEEE 802.3 környezetben milyen feltételek mellett képesek a valós idejű és a hagyományos adatátviteli szolgáltatások együttműködni.

1. Bevezetés

A hálózatba kapcsolt számítógépes alkalmazások legegyszerűbb megközelítése szerint az alkalmazói program a másik gépen futó alkalmazói programmal úgy kommunikál, hogy az operációs rendszernek adja át az adatokat. Ahogy az adat az operációs rendszerhez jut, hálózati forgalmat generál. A hálózati szolgáltatásminőség (QoS) a hálózat azon tulajdonsága, amely segítségével a forgalom kezelése történik az alkalmazói program számára. Ehhez alapvető forgalomkezelési mechanizmusokra, valamint ezeket ellenőrző algoritmusokra van szükség. A QoS-funkcionalitás egyrészt a hálózati alkalmazásokat, másrészt pedig a hálózati adminisztrátorokat szolgálja ki. Addig amíg a hálózati adminisztrátor korlátozza az erőforrásokat, az alkalmazás az erőforrások minél szélesebb körét próbálja igénybe venni. A QoS az Internet-technológiák környezetében a VoIP (Voice over IP) megoldás telefonbeszélgetés költségcsökkentő hatásának következtében jelent meg és terjed el egyre inkább [1]. Az Internet- és intranet-alapú új, sávszélesség igényes alkalmazás, valamint az adat-, hang-, videoforgalom IP infrastruktúra feletti konvergenciája ugyancsak a QoS iránti igényeket hangsúlyozza [2]. A jelenlegi alkalmazások több mint 95%-a Ethernet csomópontokban végződik, így a csomagok ezen átviteltechnikán való homogén továbbítása költségcsökkentést jelent, mivel nem szükséges protokoll-konverzió az adatok továbbítása során [3].

A különböző alkalmazások egymástól eltérő követelményeket támasztanak az adatforgalmat továbbító hálózat felé. A generált forgalom erőforrásigénye időben változó és általában szükséges, hogy a hálózat megfeleljen ennek az igénynek. Bizonyos alkalmazások többé vagy kevésbé toleránsak a forgalom késleltetésére, valamint a késleltetés változásra. Továbbá néhány alkalmazás képes elviselni korláton belül adatvesztést, míg mások nem. Ezek a követelmények a következő négy QoS-jellegű paraméter segítségével kerülnek kifejezésre. *Sávszélesség:* az alkalmazás forgalmának továbbítási sebessége; *lappangási idő:* az a késleltetés, amit egy alkalmazás a csomag kézbesítésénél képes elviselni; *jitter:* a lappangási idő szórása; *adatvesztés:* az elveszített adatok százalékos aránya [4]. Ha végtelen méretű hálózati erőforrásaink lennének, akkor az alkalmazások forgalma a szükséges sávszélességen, nulla lappangási idővel, nulla jitterrel és nulla adatvesztéssel lenne jellemezhető. Mivel azonban a hálózati erőforrások korlátosak, a rendszer bizonyos részein időtől függően az igények nem teljesíthetők. A QoS mechanizmusok az alkalmazások szolgáltatásigényének függvényében a hálózati erőforrások foglalását szabályozzák.

A hálózati végpontok közötti kapcsolatokhoz különböző hálózati eszközök szükségesek. Mindezek hálózati interfészekkel rendelkeznek, amelyek véges rátával képesek forgalmazni. Ha az adatforgalom olyan irányba halad, ahol az interfész továbbítási rátája kisebb, ott torlódás lép fel. Ezen jelenség kezelésére a köztes eszközök várakozási sorokat alkalmaznak, ezáltal lehetőség nyílik a forgalom eldobására, illetve a torlódás enyhítésére. Emiatt az alkalmazások változó lappangási időt, illetve adatvesztést tapasztalnak. Az interfészek adattovábbítási képessége, valamint a várakozási sor ideiglenes tárolási tulajdonsága az a két alapvető erőforrás, amely az alkalmazások forgalma számára biztosítani tudja QoS-t. A köztes eszközök működési mechanizmusa az egyes forgalmak számára tulajdonképpen meghatározza ezen erőforrásokhoz való hozzáférés sorrendjét, azaz a szolgáltatás minőségét.

Torlódás esetén az erőforrás-kritikus kapcsolatokhoz tartozó csomagok prioritást élveznek az egyéb csomagokhoz képest. Ehhez a köztes hálózati eszközöknek intelligens módon kell az erőforrásokat kezelniük. A különböző prioritások kialakításához az eszköz memóriája meghatározó szerepet játszik. Az erőforrások allokációjához szükséges a különböző típusú forgalmak azonosítása. A forgalom hálózati eszközhöz érkezésekor megtörténik a csomagok osztályozása és különböző adatfolyamokhoz való rendelése. Az eszközön belül minden egyes típusú adatfolyam a kimenő interfész egy-egy várakozási sorába kerül. Ezen várakozási sorok kezelését speciális mechanizmusok végzik, amelyek meghatározzák, hogy az egyes várakozási sorokból külön-külön milyen legyen az interfészen továbbított adatsebesség. A forgalmak típusának meghatározását és a várakozási sorok kezelését együtt az adatforgalom-kezelési mechanizmusok végzik. Fontos megjegyezni, hogy az adatfolyam több módon is definiálható. Egyik lehetséges mód a forrás és a cél logikai címe, a forrás és a cél socket-száma, valamint a session-azonosító kombinációja. Másik lehetséges mód az adott alkalmazástól érkező adatok vagy adott interfészről érkező adatok beazonosítása. A gyakorlatban bármely típusú azonosítást alkalmazhatónak tekintik. A klasszikus hálózati alkalmazások jellemzőit, illetve ezek erőforrás igényének összefoglalóját az *1. táblázat* tartalmazza [5].

A legfontosabb forgalomkezelő mechanizmusok az IEEE 802.1p, a DiffServ (Differentiated Service), az IntServ (Integrated Services), az ATM/ ISSLOW és mások. Ezek mindegyike speciális környezetben képes kifejteni hatását optimálisan.

Az IEEE 802.1p forgalomkezelő mechanizmus

A legtöbb LAN az IEEE 802 (Ethernet, FDDI, Token-Ring stb.) vagy más osztott közeget használó technológiára épül. Az IEEE 802.1p az L2 protokoll adatelem fejrészében egy mezőt alkalmaz, amelyben nyolc prioritás szint fér el. A végfelhasználói csomópontok és a routerek a LAN-ba küldött forgalom kereteiben megadják a prioritás értékét. Az adatkapcsolati eszközök (switch, bridge) a kereteket a prioritásnak megfelelő várakozási sorok segítségével kezelik. A mechanizmus csak alhálózaton belül működik, különböző hálózatok között nem érvényesül.

A DiffServ forgalomkezelő mechanizmus

Ez egy OSI 3 szintű QoS mechanizmus, amelyet annak ellenére, hogy több éve létezik, csak az utóbbi időben kezdtek el alkalmazni. A DiffServ az L3 protokoll adatelem fejrészében DSCP (DiffServ CodePoint) nevű mezőt helyez el. A végfelhasználói csomópontok és a routerek a DiffServ hálózatba küldött forgalom minden egyes csomagját a megfelelő DSCP értékkel látják el. A DiffServ/hálózatban lévő routerek minden csomagra a DSCP érték alapján történő osztályozás szerint specifikus PHB (Per-Hop Behavior) várakozásisor-kezelő algoritmust vagy ütemezőt alkalmaznak. Például az EF (Expedited-Forwarding) PHB limitált adatráta esetén a

1. táblázat

A hálózati forgalmak jellemzői

Forgalom-típus	Jellemző	Hálózati erőforrásigény	Alkalmazásigény
Hang	Párbeszédes, börsztös. Kézbesítési késleltetés <100 msec. Minden csomag sorrendben, jitter nélkül, de csomagvesztés lehetséges.	Csomagok routolása minimális késleltetéssel. Prioritást igényel. L4 szintű kezelhetőség.	Csomagok visszaállítása sorrendben, jittermérő puffer igénye, későn érkező csomagok eldobása.
Adat	Börsztös, nagyon hosszú, folyamatos küldés. Késleltetés elviselhető, de adatvesztés nem.	Csomagok routolása hibaellenőrzéssel L4 szinten. Hangsúlyozottan hibamentes késleltetés.	Csomagok visszaállítása hibaellenőrzéssel, hiba vagy túl sok késés esetén újraküldés.
Videó	Folyamatos. Csomagvesztés kevésbé tolerálható. Kismértékű késleltetés elfogadható, kivéve a videókonferencia, ahol az igények a hangéval azonosak.	Csomagok routolása hibamentesen.	Csomagok visszaállítása jitter mérő pufferrel. Videókonferencia esetén csomagok pufferelése és késleltetés csökkentése kései csomagok törlésével.
Játék	Börsztös adat, hang és folyamatos videó. Valós idejű kézbesítés, csak alacsony mértékű csomagvesztéssel.	Csomagok routolása minimális késleltetéssel. Prioritást igényel. L4 szinten támogatás szükséges.	Csomagok visszaállítása sorrendben, jittermérő puffer, csökkentett késleltetés. Hiba vagy túl sok késés esetén újraküldés.

bemeneti és kimeneti pontok között nagyon alacsony lappangási időt biztosít. Más PHB rögzítheti bizonyos csomagok más csomagokhoz viszonyított relatív prioritását. Ez a prioritás vonatkozhat az átlagos átviteli sebességre, az eldobási sorrendre anélkül, hogy a lappangási időre megkötés létezne. A PHB-k a routerek önálló viselkedési szabályai. Kizárólagosan PHB-k segítségével nem lehetséges végponttól-végpontig típusú QoS garanciát nyújtani.

Előfordulhat olyan eset is, amelynél a végponttól-végpontig QoS szolgáltatást az útvonal menti összes routerben azonos PHB beállításokkal biztosítjuk. Ilyenkor a logikai kapcsolat béreltvonal jellegű összeköttetést ad, amely képes megfelelni akár interaktív hangkapcsolat vagy videó lejátszás számára is.

Az IntServ forgalomkezelő mechanizmus

Ez két modulból álló szolgálathalmaz, részei a Guarranteed Load, vagy Controlled Load (garantált, illetve ellenőrzött terhelés) szolgáltatások. A garantált szolgáltatás a forgalom számára kvantálható mértéket és korlátos lappangási időt biztosít. Az ellenőrzött terhelésű szolgáltatás megadott mértékű forgalom számára terheletlen hálózati környezetet emulál. Ezek a szolgálatok kvantálhatók abban az értelemben, hogy bizonyos forgalommennyiség számára szabályozható a QoS. Az IntServ-szolgáltatások többsége az RSVP jelzésrendszerre épül. Mindegyik IntServ-szolgáltatás beengedés-szabályozási algoritmusokat definiál, amelyek az adott eszköznél befogadott forgalommennyiséget határozzák meg anélkül, hogy romolna a szolgálat minősége. Az IntServ szolgáltatások nem használnak várakozásisor-algoritmusokat.

Az IETF szabványai szerint a QoS alkalmazása leggyakrabban a DiffServ architektúrán alapul [6]. Ez előírja minden csomag osztályba sorolását a hálózaton belül. Az osztályozást az IP csomag fejlécében fenntartott hatbites szolgálat típus (TOS – Type of Service) mező értéke teszi lehetővé. Lehetséges azonban az osztályozás az L2 rétegben szállított minőségi jellemzők alapján is. Ezen speciális biteket az L2 és L3 protokoll adatelemek esetén az *1. ábra* mutatja be.

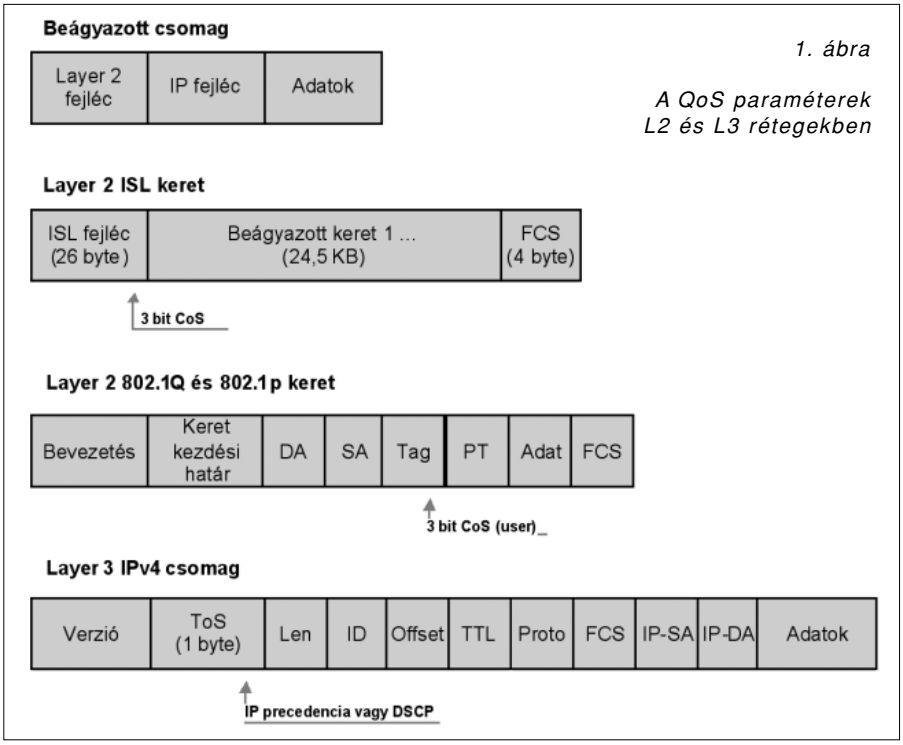
Az L2 Inter-Switch Link (ISL) kereteknek létezik egy 1 bájtos felhasználó (User) mezője, ami az utolsó három biten magában hordozza az IEEE 802.1p CoS (Class of Service) értéket. Az L2 ISL trönk interfészek ISL kereteket továbbítanak. Az IEEE 802.1Q keret egy 2 bájtos TCI (Tag Control Information) mező segítségével szállítja a CoS értéket az utolsó három, User Priority biten. Az ilyen L2-es trönkön minden forgalom 802.1Q kereteket tartalmaz, kivéve a Native VLAN esetében. Más fajta kerettípusok nem tudják szállítani a második rétegbeli CoS értékeket. A CoS értékei 0-7 tartományból vehetnek növekvő prioritású értéket.

Az L3 IP csomagok vagy az IP precedencia, vagy a DSCP (Differentiated Services Code Point) értéket továbbítják. A QoS támogatja mindkét fajta érték használatát, mert a DSCP értékek kompatibilisek az IP precedencia értékekkel. Az IP precedencia értékek 0-7, míg a DSCP értékek 0-63 tartományban léteznek.

Minden switch és router amely az Interneten forgalmaz, a csomagokat osztály információval látja el, amely segítségével az azonos osztályhoz tartozó csomagok azonos kezelésben, a különböző osztályhoz tartozó csomagok pedig különböző kezelésben részesülnek. Az osztály információt a csomagokban végfelhasználói csomópontok, vagy switch, illetve router köztes csomópontok is meghatározhatják, függően, a helyi policy-tól,

2. A QoS értelmezése az infokommunikációs rendszereknél

A hálózatok tipikusan átvételi kötelezettség nélkül (best-effort) kézbesítenek, ami azt jelenti, hogy minden forgalom azonos prioritású, és egyenlő esélye van arra, hogy a kézbesítése egy bizonyos időintervallumon belül megtörténjen. Torlódás esetén viszont minden csomagnak azonos esélye van az eldobásra is. Amikor QoS-t konfigurálunk, ki lehet választani azokat a specifikus hálózati forgalmakat, amelyeket prioritással kezelünk, majd ezekhez használhatunk torlódásvezérlési és torlódást elkerülő technológiákat. A QoS technológia használata a hálózat teljesítményét skálázhatóvá, a sávszélesség kihasználtságát pedig hatékonyabbá teszi.



1. ábra

A QoS paraméterek L2 és L3 rétegekben

a részletes csomagvizsgálattól vagy mindkettőtől. A részletes csomagvizsgálat tipikusan a hálózat hozzáférési pontban történik, annak érdekében, hogy a meghatározó switchek és routerek ne legyenek túlterhelve. A switchek és routerek az útvonalon használhatják az osztály információt, hogy meghatározzák a rendelkezésre álló erőforrás készletet a forgalmi osztályok számára. Egy egyedülálló eszköz DiffServ architektúra szerinti forgalom kezelő viselkedését PHB-nak (Per-Hop Behavior) nevezik. Ha a továbbítási útvonal mentén az összes eszköz konzisztens per-hop módszerrel működik, akkor végponttól-végpontig típusú QoS megoldás érvényesül. A QoS bevezetése a hálózaton függ az aktív eszközök QoS sajátosságától, a forgalom típusától és mintájától a hálózaton, valamint a bejövő és kimenő forgalomra alkalmazott vezérlés részletességétől.

3. A QoS struktúra modellje az L2/L3 rétegeknél

Az osztályozás a forgalmak típus szerinti szétválasztását biztosítja. A bemeneti (ingress) eszköz működése magába foglalja a forgalomosztályozás (classification), a szabályozás (policing), a jelölés (mark), a sorbahelyezés (queing) és az ütemezés (scheduling) feladatokat. A QoS alapmodellt a *2. ábra* mutatja be. Bemeneti interfészeken az osztályozás szétválogatja a különböző típusú forgalmakat [7].

A folyamat készít egy belső DSCP-t csomagonként, ami meghatározza a továbbítás közben végrehajtandó QoS tevékenységeket. A szabályozás meghatározza, hogy a csomag szerepel-e a bekonfigurált profilban összehasonlítva a belső DSCP-t a beállított szabályzókkal (policer), amelyek az adatfolyam által felhasznált sávszélességet korlátozzák. A jelölő (marker) kiértékeli a szabályozót és az interfész szintű konfigurációs információt, majd megvizsgálja azt az előírást, ami szerint kell eljárnia. Ha a csomag a profilon kívül esik, átengedi a csomagot módosított DSCP értékkel vagy eldobja. A sorbahelyezés (queing) megvizsgálja a DSCP vagy a CoS értéket, és ez alapján eldönti, hogy a csomag melyik bemeneti várakozási sorba kerüljön a kettő közül.

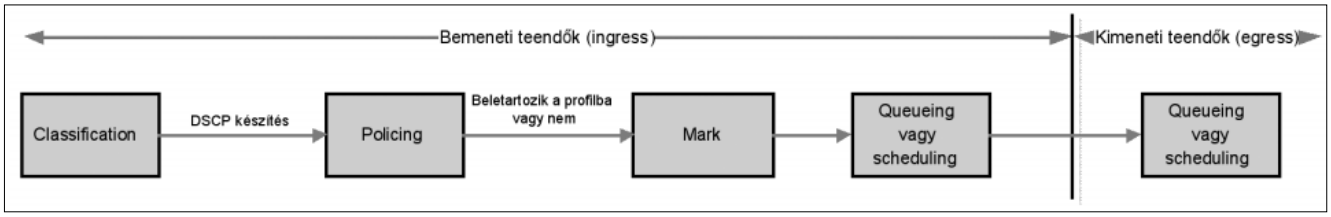
Kimeneti interfészeken a sorbahelyezés (queing) kiértékeli a belső DSCP-t és meghatározza, hogy a 4 kijárati sor közül melyikbe tegye a csomagot. Erre azért van szükség, mert torlódás alakulhat ki eszközön belül, ha a két bemeneti várakozási sor egyszerre küldi az adatot a kimeneti interfész felé. Gyakran torlódás megelőző technológiákat alkalmaznak (WRED – Weighted Random Early Detection, és tail drop) a gigabit képes ethernet portok, illetve egy küszöbértékes „tail drop" mechanizmust a 10/100 Mbps-os ethernet portok. Ütemezéskor (scheduling) a négy kimeneti sor közül egy maximális előnyben (expedite) részesül, így ebbe a sorba kerülő csomagok mindegyike továbbításra kerül mielőtt bármely másik sor tartalma kiszolgálásra kerülne.

IP-től különböző forgalom esetén, ha a beérkező csomag nem rendelkezik CoS értékkel, akkor a bemeneti interfészen érvényes helyi fix beállítás érvényesül. Ha a beérkező keret rendelkezik CoS értékkel, akkor a meneti interfész alkalmazza a CoS-DSCP térképet, ami alapján a kerethez rendeli a belső DSCP értéket. Ha a beállítások MAC szűrő listát (ACL – Access Control List) tartalmaznak, a forrás-, a célcím, illetve a keret típusa alapján történik a DSCP értékének beállítása. Ha nincs ACL, akkor a csomag DSCP=0 értéket kap, azaz „best-effort" alapján továbbítódik.

IP forgalom esetén eszközön belül a beérkező csomagban lévő DSCP használható. Az IETF a ToS mező hat legfontosabb bitjét a DSCP-ként értelmezi. A prioritást a 0-63 intervallumban lévő DSCP érték fejezi ki. Különböző QoS zónák közötti fizikai kapcsolatot biztosító interfészek a DSCP-DSCP mutációs összerendelés alapján megváltoztathatják a két zóna között továbbított csomag DSCP értékét. Lehetőség van a beérkező csomag IP precedencia mezőjének kiértékelésére is, ami alapján a DSCP érték hozzárendelése az IP precedencia-DSCP táblázat alapján történik. Az IPv4 a ToS mező három legnagyobb helyiértékű bitjét használja a precedencia tárolására. Ha a csomagban jelen van a CoS (Class of Service) érték, akkor a DSCP érték a CoS-DSCP táblázatból áll elő. Konfigurált szabványos vagy kiterjesztett IP ACL esetén az IP csomag fejrészében lévő különböző mezők értékei azonosíthatók be. Szűrési találat esetén a szűrőhöz előírt DSCP érték hozzárendelődik az adott csomaghoz. Ha nem létezik ACL, akkor a csomag DSCP=0 értékkel halad tovább.

Az osztályozás-összerendelés (class map) mechanizmus arra használható, hogy egy speciális adatfolyam beazonosítható és megkülönböztethető legyen más adatfolyamoktól. Ez a mechanizmus az adatfolyam további kategóriákba sorolását teszi lehetővé, amihez a döntést az ACL szerinti illeszkedés, DSCP listához vagy IP precedencia listához való tartozás biztosítja. További adatfolyam osztályozásához egy-egy további eltérő nevű osztály-összerendelést lehet készíteni. Ha a csomag egyezik az osztály-összerendelés szabállyal, akkor a policy-összerendelés segítségével megtörténik a kategóriába sorolása. A policy-összerendelés

2. ábra A QoS modell elemei

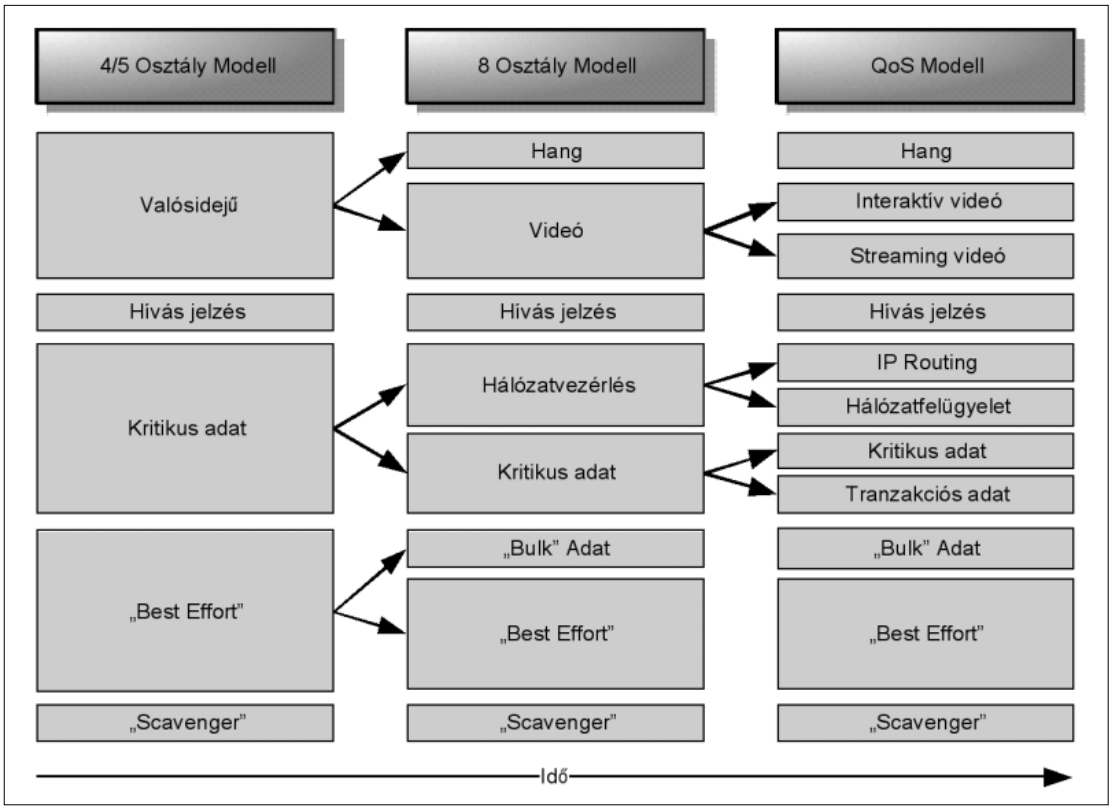


interfészen történő aktivizálása következményeként az alábbi tevékenységek történhetnek: a CoS, DSCP, IP precedencia értékek kiértékelése; a DSCP vagy az IP precedencia érték beállítása; az adatfolyam sávszélességének korlátozása; olyan tevékenység elvégzése, amely a forgalom profile illesztése esetén szükséges. A szolgálat osztályok felsorolását, illetve időben történő kialakulásukat a *3. ábra* mutatja [8]. A „Bulk" adat a háttérben futó nagyméretű adatletöltések jellemzője. A „Scavenger" adattípus az IPv6 esetén kerül előtérbe, amely még a „best-effort" adatnál is könyebben eldobható.

A csomag eszközön belüli DSCP értékének meghatározása után a policing és jelölés események következnek. A policing a forgalom sávszélességének szabályozását lehetővé teszi policerek segítségével. A policerek minden egyes csomagot megvizsgálnak és eldöntik, hogy megfelel-e a profilnak vagy sem. A profilnak megfelelő szabályozásokat a jelölő végzi, amely dönt a csomag kézbesítése vagy eldobása felől. A policer lehet egyedi vagy aggregált. Az egyedi QoS policer a sávszélesség korlátokat a megfelelő forgalom osztályok alapján alkalmazza. Az aggregált QoS policer a beállításokat globálisan kezeli, minden forgalmat megvizsgál. A policer zsetonos vödör (token bucket) algoritmust alkalmaz. Ez hasonlít az ATM átviteltechnikánál alkalmazott megoldásra, de itt csak egy edény és csak egy szivárgó lyuk létezik [9]. Minden beérkező keret esetén a vödörbe egy zsetont helyez el. A beállított sávszélességnek megfelelő ritmusban a vödörből a zsetonok kiszivárognak. Amikor a zseton a vödörbe kerül, a kapcsoló eszköz előzetesen ellenőrzi a vödörben lévő üres helyet. Ha nincs elegendő hely a zseton számára, akkor a csomag nem megfelelő jelölést kap és az annak megfelelő policer intézkedés következik be. Ez lehet a csomag eldobása vagy a DSCP értékének lecsökkentése is. A vödör telítődésének gyorsaságát a vödör mérete (börszt [bájt]) a vödör szivárgásának mértéke (bitráta [bps]) és az átlagos bitráta feletti börszt időtartama befolyásolja. A vödör mérete a börszt hosszát korlátozza és meghatározza az eszközben a bementi pont és a kimeneti pont között továbbítható keretek darabszámát. Alacsony forgalom esetén az adatfolyam nem befolyásolódik. Ha a börszt hosszú és magas bitrátájú, a vödör túlcsordulása miatt a kerettel szemben policer intézkedés lép érvénybe.

A kapcsoló a sorbaállítás és az ütemezés folyamat során torlódás menedzsment célból kimeneti várakozási sorokat, valamint WRR (Weighted Round Robin) mechanizmust használ. Minden Gigabit Ethernet port 4 darab várakozási sorral rendelkezik, amelyek közül egyik kiemelt prioritásúként működhet. A várakozási soroknak két-két küszöbértéke van. A DSCP-küszöbérték táblázat alapján történik a csomag „tail-drop" vagy WRED algoritmus szerinti kezelése. A várakozási sor mérete, a küszöbérték, a „tail-drop" vagy WRED algoritmus és a DSCP-küszübérték táblázat együtt befolyásolja, hogy a küszöbérték meghaladásakor mikor és melyik csomag eldobása következik be. A kimenő interfész fizikai sávszélessége együttesen képezi a négy várakozási sor számára rendelkezésre álló sávszélességet.

A „tail-drop" a Gigabit Ethernet interfészek alapértelmezett torlódást megelőző mechanizmusa. A csomagok addig kerülnek a várakozási sorokba, amíg a küszöbértéket el nem érik. Ilyen esetbe az első küszöbér-



3. ábra

A QoS szerinti hálózat-szolgálati osztályok

tékhez rendelt csomagok eldobása mindaddig ismétlődik, amíg a forgalom a küszöbérték alá nem csökken. Az elsőnél nagyobb második küszöbértékhez rendelt csomagok ilyenkor is továbbítódnak mindaddig, amíg a forgalom második küszöbértéket el nem éri. A küszöbértékek százalékosan a sorok lefoglaltságát mutatják. A „tail-drop” és a WRED két olyan mechanizmus, amely közül csak az egyik működhet egyidőben az interfészen.

A WRED (Weighted Random Early Detection) abban különbözik más torlódás feloldó mechanizmustól, hogy a torlódás kezelése helyett megpróbálja megelőzni annak kialakulását. A WRED felhasználja a TCP azon torlódásvezérlési tulajdonságát, hogy a TCP a várakozási sora méretének szabályozásával képes ideiglenesen leállítani az üzenetek küldését. A WRED véletlenszerűen eldob csomagokat azelőtt, hogy erős torlódás lépne fel, így a forrás TCP protokoll entitás csökkenti a küldési sebességét, és az L3 rétegben megelőzhető a torlódás. A véletlenszerű csomageldobás lehetővé teszi, hogy a „tail-drop” algoritmussal ellentétben ne kelljen sok csomagot eldobni, ugyanakkor a fizikai csatorna jobb kihasználására nyílik lehetőség. A WRED a nagyobb rátájú forgalmakból többet dob el, mint az alacsony rátájúakból. A kimenő interfész mind a négy várakozási sora itt is rendelkezik egy-egy küszöbértékkel. Ennek meghaladása esetén kezdődik véletlenszerűen a forgalom csomagjainak eldobása. Minél jobban meghaladja a küszöbértéket a forgalom, annál több csomagot dob el. A csomagok kezelése a DSCP-küszöbérték táblázat alapján történik.

A csomag QoS miatti módosítása különböző esetekben következik be:

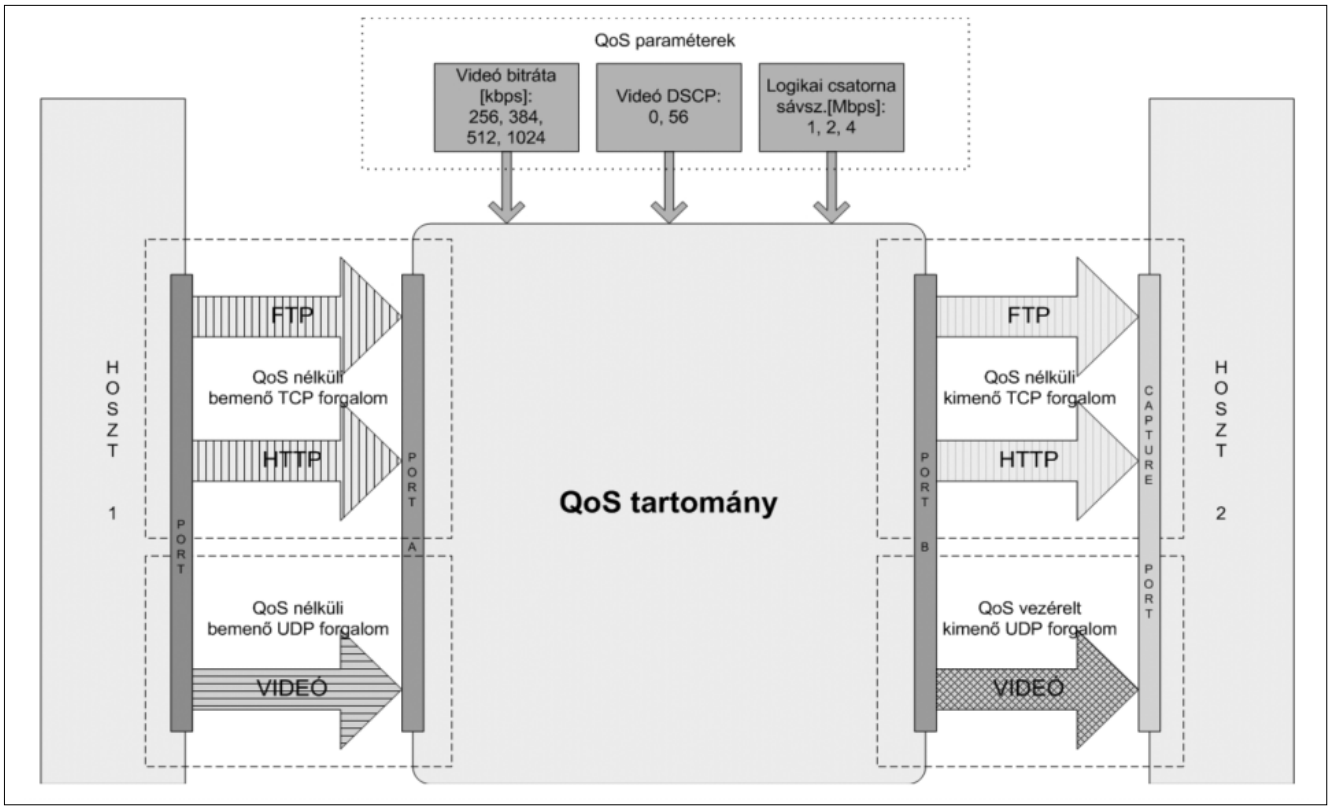
i) IP csomagnál az osztályozás alapján DSCP érték rendelődik a csomaghoz. Előfordulhat, hogy ilyekor a csomag nem módosul, de a DSCP hozzárendelés megtörténik. Ennek az az oka, hogy mivel a QoS osztályozás és az ACL szűrőlista illesztése egyidőben történik, az ACL miatt szükség lehet a csomag különválasztására. Ilyenkor a csomag az eredeti DSCP értékével a kapcsoló CPU-jához kerül, ahol a routing miatt újból ACL illesztés következhet. Az útvonal elemzése az osztályozott DSCP-re épül.

ii) IP-től különböző csomag esetén nem létezik DSCP, így az osztályozás a csomaghoz egy belső DSCP-t rendel. A belső DSCP alapján a csomagot CoS osztályba sorolja és annak megfelelő módon processzálja.

iii) „Policing” fázisban az IP és a nem IP csomagok DSCP értéke módosulhat, ha az előírt profil nem illeszthető. Ilyenkor a módosítást a lejelölés (markdown) funkció végzi el.

Az L4-L7 rétegek esetén is van lehetőség a QoS szabályozására [10]. Ebben az esetben megfelelő mechanizmusok segítségével figyelni lehet statikusan és dinamikusan a TCP és az UDP portok használatának statisztikáját; az UDP, illetve a TCP-től eltérő protokollok alkalmazásának arányát; lehetséges továbbá alport szerinti osztályozás, amely a csomag mélyebb szintű elemzésére épít.

4. ábra A mérési környezet és az adatfolyamok



A HTTP forgalmak osztályozását URL, hoszt, illetve MIME alapján végzik. A valós idejű multimédiás hálózati alkalmazások által használt RTP (Real Time Protocol) kontroll modulja páratlan szám azonosítójú portot, az adat modulja pedig páros szám azonosítójú portot alkalmaz [11].

Az RTP időzítés szabályozást, adatvesztés érzékelést, adatvédelem és tartalomazonosítást biztosít. A hasznos teher osztályozása során a hang, a videó, a sűrített vagy sűrítetlen videó, a codec beazonosítására nyílik lehetőség. A felhasználói egyéb alkalmazások statikus porthozzárendelés alapján azonosíthatók be.

A peer-to-peer fájlmegosztó protokollok (Gnutella, FastTrack stb.) erőteljes erőforrás igénye miatt egyrészt a statikus port értéke, másrészt a generált forgalom dinamikája alapján történhet a szabályozás.

4. A mérési környezet és a mért értékek ismertetése

Egyetlen QoS tartományhoz tartozó forgalmakat vizsgáltunk meg. A Hoszt1 géptől a Hoszt2 gép felé egyidőben TCP, illetve UDP forgalmat generáltunk. A TCP FTP és HTTP letöltéseket, az UDP pedig interaktív videó átvitelt végzett. A mérési környezetet a *4. ábra* mutatja. Mivel az FTP és a HTTP az Ethernet 1500 bájtos MTU-jánál nagyobb méretű IP csomagokkal forgalmaz, ezeknél fragmentáció lépett fel. A QoS paramétereket fragmentum csomagoknál nem lehetséges kezelni, ezért a TCP forgalom „best-effort”, azaz DSCP = 0 érték mellett zajlott.

A videokonferencia UDP forgalom minden csomagja elfér egy-egy Ethernet keretben, így ennek prioritását a TCP forgalom prioritása fölé lehetett emelni az UDP DSCP = 56 értékének beállítása segítségével. A Hoszt1 a lehető legnagyobb rátával küldi a videót a QoS tartományba, ez azonban a forrás fizikai kapacitása miatt legfeljebb 1 Mbps lehet. A Hoszt2 csomópontnál külön a TCP, és külön az UDP hálózati forgalom mérése TCPDump program segítségével történt. A QoS tartományon belül a videó bitrátát és a videó prioritását a Port_A, míg az UDP és a TCP forgalom számára közösen rendelkezésre álló csatorna kimeneti sávszélességét a Port_B pontokban szabályoztuk. A Port_B sávszélességét interfész szintű globális QoS paraméterrel befolyásoltuk. A mérésnél alkalmazott paramétereket a *2. táblázat* tartalmazza.

2. táblázat A mérésnél alkalmazott paraméterek

Paraméter	Értékek
Videó bitráta [kbps]	256, 384, 512, 768, 1024
Videó kódolási algoritmus	H.261, H.264
Videó adatfolyam DSCP értéke	0, 56
Logikai csatorna sávszélesség [Mbps]	1, 2, 4
Adatkapcsolat	IEEE 802.3 (Full Duplex)

Jellemző	Definíció
Átlag *(Mean)* [kbit/sec]	$\mathrm{Mean}(Z_p)=\overline{Z_p}=\frac{\sum_{t=1}^{Tp} z_p(t)}{T_p}$
Szórás *(Standard Deviation)* [kbit/sec]	$\mathrm{STD}(Z_p)=\sqrt{\frac{1}{T_p}\sum_{t=1}^{Tp}\left(z_p(t)-\overline{Z_p}\right)^2}$
Relatív szórás *(Relative STD)* [%]	$\mathrm{RSD}(Z_p)=\frac{\mathrm{STD}(Z_p(t))}{\overline{Z_p}}$
Ferdeség *(Skewness)* [%]	$\mathrm{Skewness}(Z_p)=\frac{\sqrt{T_p}\sum_{t=1}^{Tp}\left(z_p(t)-\overline{Z_p}\right)^3}{\left(\sum_{t=1}^{Tp}\left(z_p(t)-\overline{Z_p}\right)^2\right)^{3/2}}$

3. táblázat Az idősorok jellemzői

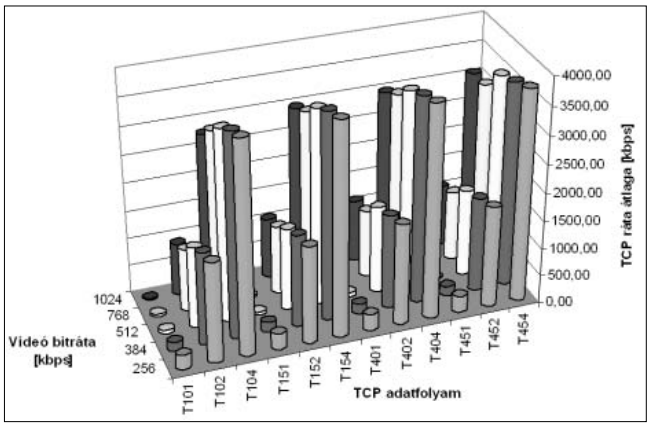
Külön a TCP és külön az UDP forgalmakra az L2 keretek méretét és időpontját rögzítettük. Egy mérés 60 másodpercig tartott, összesen 60 mérés készült. Minden egyes mérésnél ugyanazt a műsort forgalmaztuk a két hoszt között. Az első harminc mérésnél a forrás H.261, a továbbiaknál H.264 kodeket használt. Minden egyes idősorra 100 msec-os mintavételezéssel meghatároztuk a bitrátát. Az így nyert újabb két idősor halmaz $Z_p^T(t)$(p=1,2,...,60 TCP esetén), illetve $Z_p^U(t)$(p=1,2,...,60 UDP esetén) minden eleme T_p= 60.000 értéket tartalmaz. Ezen idősorokat elemeztük matematikai statisztikai szemszögből. A megvizsgált jellemzők a bitráta átlaga, szórása, relatív szórása, valamint a ferdesége. Ezek definícióját a fenti, *3. táblázat* mutatja be.

5. A mérési eredmények elemzése és értelmezése

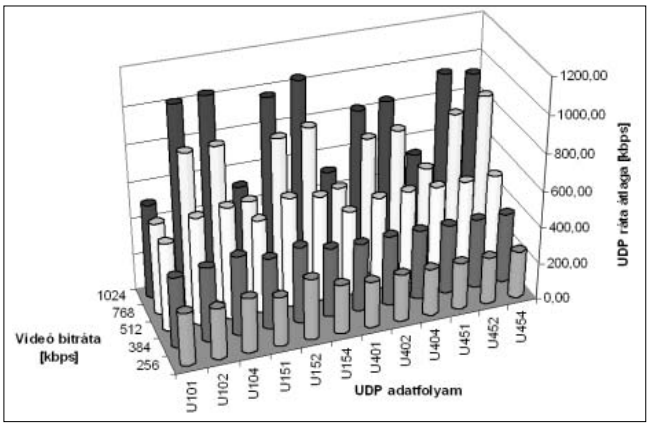
Az *5-12. ábrák* az UDP, illetve a TCP forgalmak bitrátájának átlagát, szórását, realtív szórását, illetve ferdeségét mutatják.

A különböző adatfolyam halmazokat abc=(101...454) index segítségével jelöltük, ahol a=(H.261, H.264), b=(DSCP1=0, DSCP=56), c=(logikai csatorna sebesség= 1 Mbps, 2 Mbps, 4 Mbps). Így például az abc=454 indexű idősor halmaz H.264 codec, DSCP=56 érték és a Port_B logikai csatornájának átviteli sebessége=4 Mbps esetben készült.

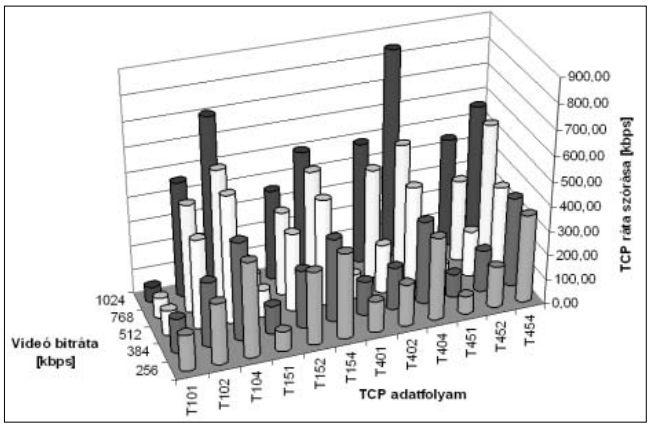
Adott halmaz elemei 256, 384, 512, 768 és 1024 Kbps-os bitráták mellett készültek. A TCP és az UDP „best-effort” jellegű (b=0 halmazok) forgalmazása esetén a különböző adatfolyamok átlagosan kitöltik a rendelkezésre álló sávszélességet, és mindegyik alkalmazás működik. QoS segítségével történő videó bitráta növelése miatt az FTP és a HTTP forgalmak átlagát a TCP automatikusan visszaszabályozza. A H.261 codec a H.264-hez képest átlagosan több UDP adatot képes továbbítani annak ellenére, hogy régebbi algoritmus. Ennek oka, hogy a rendelkezésre álló videó bitráta nem haladja meg az 1 Mbps értéket, ami alatt a H.264 nem működik optimálisan. A forgalmak bitrátájának szórása azt mutatja, hogy nagyobb rátánál növekszik a szórás



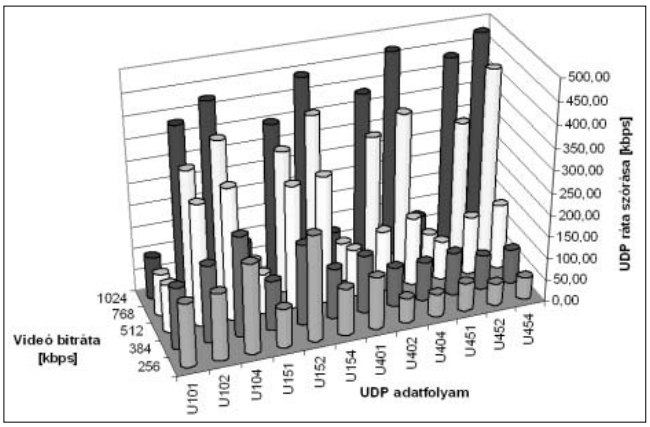
5. ábra A TCP bitráta átlaga



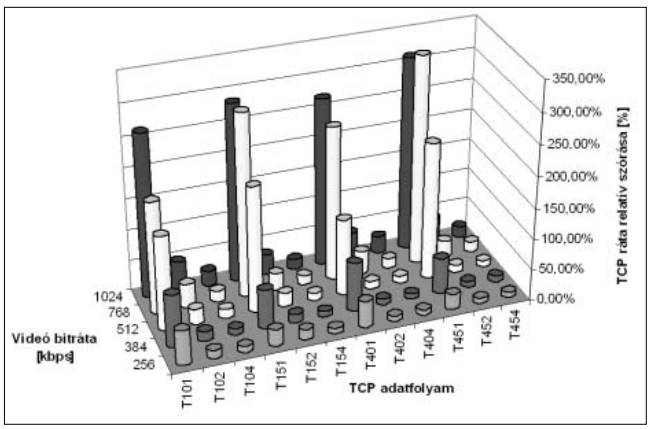
6. ábra Az UDP bitráta átlaga



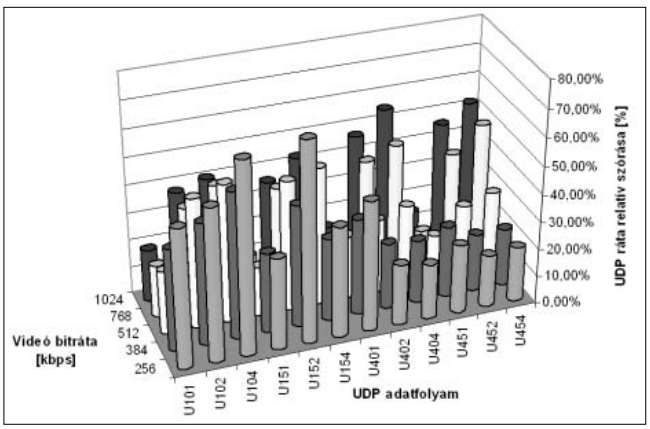
7. ábra A TCP bitráta szórása



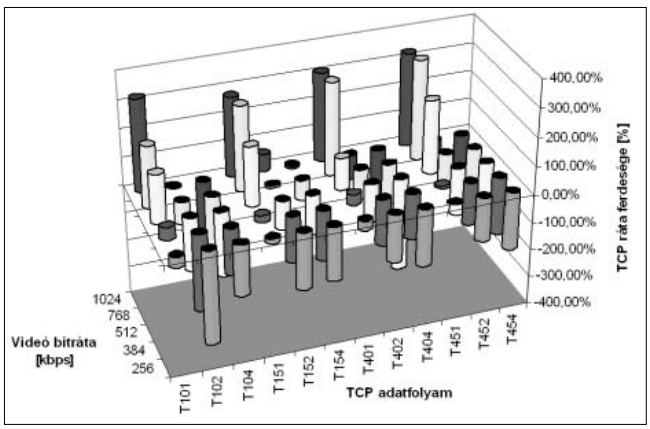
8. ábra Az UDP bitráta szórása



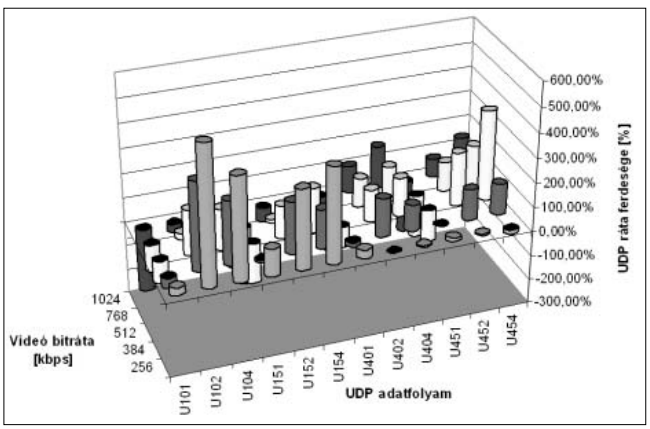
9. ábra A TCP bitráta relatív szórása



10. ábra Az UDP bitráta relatív szórása



11. ábra A TCP bitráta ferdesége



12. ábra Az UDP bitráta ferdesége

Dinamika	Darabosság	Átlapoltság	Színhűség	Értelmezhetőség	OS
Álló	Nagyon	Igen	Nem	Nem	1
Akadozó	Nagyon	Igen	Nem	Nem	2
Akadozó	Közepes	Igen	Nem	Kevésbé	3
Akadozó	Közepes	Igen	Nem	Közepes	4
Akadozó	Közepes	Igen	Nem	Közepes	5
Mozgó	Kevésbé	Nem	Nem	Közepes	6
Mozgó	Nem	Nem	Nem	Közepes	7
Mozgó	Nem	Nem	Nem	Elfogadható	8
Mozgó	Nem	Nem	Nem	Jó	9
Mozgó	Nem	Nem	Igen	Nagyon jó	10

4. táblázat A videó minőségének vélemény-érték (OS) metrikája

is, viszont alacsony videó bitráta esetén a H.264 codec kevesebbet szór, mint a H.261. 4 Mbps csatorna esetén a T104 és T404 erőteljesen szór, ha a videó bitrátája 1 Mbps-on van. Ez azt jelenti, hogy a videó legjobb minősége esetén a TCP a maradék 3 Mbps sávszélességen egyre inkább börsztösíti az adatátvitelét. A TCP bitráta relatív szórása alapján látható, hogy 1 Mbps-os csatorna sávszélesség esetén a TCP erőteljesebben szór, és eléri a 300%-ot is, míg a többi esetben ez jóval 40% alatt marad. Az UDP relatív szórása kis videó bitráta esetén viszonylag magas, de még így is csak 70% alatti.

A H.264 relatívan is kevesebbet szór alacsony videó bitrátánál, függetlenül a csatorna fizikai sávszélességétől. A bitráta ferdesége azt jelenti, hogy a periodogram a súlyvonalához képest balra (negatív) vagy jobbra (pozitív) ferdül el. Negatív ferdeség azt jelenti, hogy az átlagos bitrátánál sokszor kisebb a forgalom, viszont a forgalomban ritkábban börsztös jelenségek léteznek. A pozitív ferdeség azt mutatja, hogy az átlagos bitrátánál gyakran nagyobb a forgalom, de csak kis mértékben, és léteznek hosszabb időszakok, amikor az átvitel szünetel. A TCP bitrátája csak 768 Kbps-nál nagyobb videó bitráta beállítás esetén pozitív ferdeségű, a többi esetben negatív. Az UDP bitrátája ezzel ellentétben csak a H.261 codec és magas videó bitráta esetén negatív ferdeségű, a többi esetben pozitív, sőt gyakran megközelíti az 500%-ot is.

A TCP „best-effort” és az UDP QoS vezérlése (b=5 idősorok) esetén a bitráták átlagának grafikonja nem teszi lehetővé a homogén „best-effort” jellegű forgalmaktól való különbségtételt annak ellenére, hogy a tapasztalt videó minősége lényegesen eltér egymástól a QoS jelenléte, illetve hiánya esetekben.

A TCP mindig a maradék rendelkezésre álló sávszélességet használja ki, mivel az L4 forgalomszabályozás ezt lehetővé teszi. Az UDP a TCP-hez viszonyítva csak 50%-os bitráta szórást okoz, azonban az 1 Mbps-os (c=1 síkok) UDP a 2 Mbps és 4 Mbps csatornákkal ellentétben a videó bitráta növelésével csökkenti a szórást. Erre az a magyarázat, hogy nagyon alacsony csatorna sávszélességnél a TCP radikálisan csökkenti a forgalmát, így a videó továbbítása kevésbé börsztösen lehetséges.

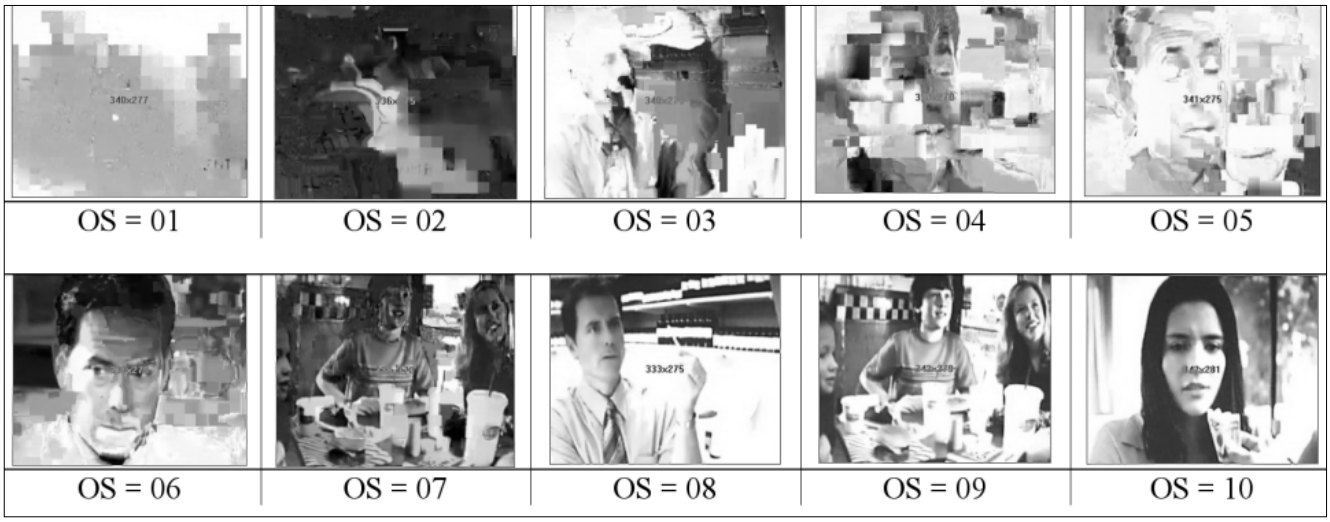
A H.264 relatív szórása független a QoS-től és növekszik a videó bitrátával, ami a H.264 codec dinamikusabb működését igazolja. A TCP bitráta ferdeségére nincs hatással a videó QoS beállítása, mivel a TCP a maradék sávszélességet használja fel. Az UDP bitráta ferdeségét a QoS beállítások kis mértékben csökkentik, de még mindig a pozitív tartományban tartják.

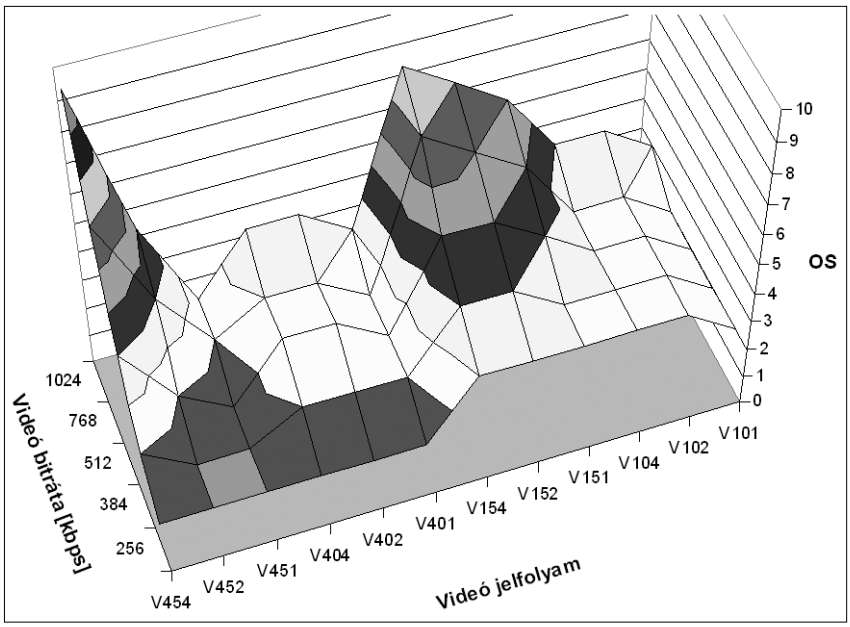
Egy tíz pontos tartományban mérő vélemény-érték (OS – Opinion Score) saját metrikát képeztünk adott videó műsor minőségének globális számszerűsítéséhez. Öt alapvető minőségi szempontot javasolunk, amelyeket a *4. táblázat* mutatja be.

Az OS segítségével a QoS mechanizmus és a codec együttes hatását objektív módon mérhetjük.

Adott videó műsor globális OS, vélemény értékekhez tartozó képeket az *5. táblázat* tartalmazza. Az így összeállított lista lehetővé teszi a videó műsor minőségének számszerű értékelését és kategóriákba sorolását is. Alacsony OS értékek gyenge minőséget, nagy OS értékek jó minőséget képviselnek.

5. táblázat
A vélemény-értékek (OS) szerinti videó képek





13. ábra
A videó forgalmak vélemény-értéke (Opinion Score)

A különböző QoS paraméterekkel szabályozott videó jelfolyamok (V101...V454) egymáshoz viszonyított globális OS, vélemény értékét a *13. ábra* mutatja be. Megfigyelhető, hogy a videó átvitel vegyes terhelésű hálózaton nagymértékben függ a QoS beállításoktól.

A homogén „best-effort" módszer szerinti forgalomtovábbítás megosztja az erőforrásokat a különböző adatfolyamok között, míg a QoS mechanizmus alacsony csatorna sávszélességnél a valós idejű alkalmazásokat megszakítja, nagyobb csatorna sávszélesség esetén pedig erőteljesebb különbséget tesz az eltérő típusú adatfolyamok között. A videó kapcsolat kielégítően jó minőségű átviteléhez végponttól-végpontig minimum 1 Mbps-ra van szükség. Alacsony sávszélességen a H.261 codec jobb minőséget ad, mint a H.264, viszont utóbbi képes akár HDTV minőségű műsor továbbítására is 2 Mbps-nál nagyobb sebességű összeköttetés esetén [11]. QoS mechanizmus működtetése mellett jelentős minőségi ugrást az 500 Kbps-nál nagyobb sebességű adatkapcsolat esetén tapasztalhatunk, amit a felhasználók véleményének az OS tízes skáláján a felső tartományban való elhelyezése tükröz.

6. Összefoglalás

Jelen cikkben a QoS mechanizmus L2 és L3 rétegekben kifejtett hatását vizsgáltuk meg egyetlen QoS tartományon belül szabályozott paraméterek segítségével, H.261 és H.264 videó codec alkalmazása mellett. A mérések alapján kijelenthető, hogy a QoS mechanizmus aktivizálása jelentősen megváltoztatja az Interneten hagyományosan működő hálózati alkalmazások viselkedését. Az UDP egyenletesebb adatfolyamot biztosít, míg a TCP a maradék hálózati erőforrás teljes kihasználására is képes. QoS mechanizmusok segítségével hatékonyan differenciálni lehet a különböző típusú adatforgalmak között, így a valós idejű hálózati alkalmazások (VoIP, video, játék stb.) kielégítő minőségben képesek együttműködni a hagyományos adatátviteli szolgáltatásokkal. Ez jelentős beruházási megtakarításokat jelent a jövőben, hiszen a meglévő infrastruktúra teljes lecserélése nélkül a QoS mechanizmusokkal lehetőség van a hang-, videó-, adatátvitel integrációjának folytatására.

További vizsgálatok szükségesek az egyéb QoS paraméterek, egyetlen, illetve több QoS tartományon átívelő multimédiás kapcsolatok viselkedése, valamint az L4-L7 rétegek működésének minőségi befolyásolhatósága témakörökben.

Irodalom

[1] Luis F. Ortiz:
„Solving QoS in VoIP: A formula for explosive growth?"
Brooktrout Technology
[2] „AutoQoS for Voice Over IP (VoIP)",
White Paper, Cisco Systems Co.,
http://www.cisco.com
[3] „Advanced QoS",
White Paper, Allied Telesis,
http://www.alliedtelesis.com
[4] „Quality of Service",
Technical White Paper, Microsoft Co.,
http://www.microsoft.com/technet/prodtechnol/windows2000serv/plan/qosover.mspx
[5] „QoS" – White Paper, Allied Telesis,
http://www.alliedtelesis.com
[6] „Configuring QoS" – Catalyst 3550 Multilayer Switch Software Configuration Guide, Cisco Systems Co.,
http://www.cisco.com
[7] „Configuring QoS" – Catalyst 3750 Multilayer Switch Software Configuration Guide, Cisco Systems Co.,
http://www.cisco.com
[8] „Enterprise QoS Solution Reference" –
Network Design Guide, Cisco Systems Co.,
http://www.cisco.com
[9] Zoltán Gál, Csaba Szabó:
„Migration to ATM in an Academic MAN Environment – Network Design Considerations and a Case Study",
8th IEEE LAN/MAN Workshop Proceedings,
Berlin, 25-28 August, 1996.
[10] „Network-Based Application Recognition and Distributed Network-Based Application Recognition" – Network Design Guide, Cisco Systems Co.,
http://www.cisco.com
[11] Gál Zoltán, Karsai Andrea, Orosz Péter:
„A WiFi rendszerek multimédiás alkalmazásokra gyakorolt hatása",
Híradástechnika, 2006/6, pp.15–23.