Digitális őrszem – IPTraf

Az IPTraf egy nagyon kényelmesen és egyszerűen használható hálózat-elemző program, amely segítséget nyújt a hálózatba kötött gépek adatforgalmának közvetlen, vagy közvetett figyelésére.

Az *IPTraf* telepítése nagyon egyszerű. A hardverkövetelménye szerény, ezért gyakorlatilag az összes ma használatos gépen képes működni, amiben van legalább 16 MBájt memória. Szoftverkövetelményére sem lehet panaszunk, hiszen legalább 2.2-es kernelt követel magának, de természetesen működik a 2.4-es és a 2.6-os sorozattal is. A fordításhoz sincs szükség különleges alkalmazás telepítésére, arra ügyeljünk, hogy az ***ncurses*** a fejlesztői eszközökkel együtt telepítve legyen.

A programot legegyszerűbben az ➲ *ftp://iptraf.seul.org/pub/iptraf* címről tölthetjük le ***tar.gz*** formátumban. A fájlnévben szerepel a verziószám, ami a cikk írásakor a 2.7.0. Az ***FTP*** helyen megtalálhatjuk a már lefordított bináris fájlt is, amely az ***iptraf-2.7.0.bin.i386.tar.gz*** nevet viseli. A letöltés biztosan nem vesz igénybe hosszú időt, hiszen alig több, mint 350 kB a mérete a fájloknak. Sok Linux terjesztésben is megtalálható már, ezért azt is leellenőrizhetjük, hiszen ilyen esetben a telepítés sokkal egyszerűbb lesz.

Miután letöltöttük, ki kell csomagolni egy ideiglenes könyvtárba, amihez használjuk a

```
tar -xzvf iptraf-2.7.0.tar.gz
```

illetve a már lefordított fájl esetében a

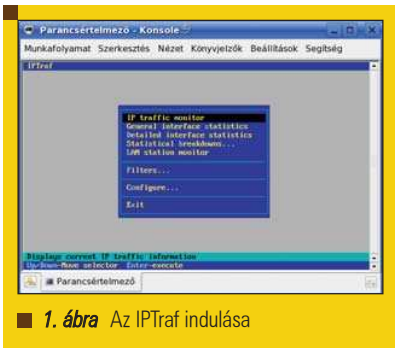
```
tar -xzvf iptraf-
➥2.7.0.bin.i386.tar.gz
```

parancsot.

A kicsomagolás után következhet a telepítés, amely ugyanúgy zajlik, mind a forrás-, mind a lefordított program esetén, csak a háttérben zajló folyamatok lesznek mások. Lépjünk be a könyvtárba, amit a tar létrehozott, majd root jogosultságokkal (ha nem root néven lépnénk, be, akkor használjuk a su parancsot) adjuk ki a `./Setup` parancsot. Ez a parancsfájl felismeri, hogy bináris, vagy forrás állományból dolgozunk és ez utóbbi esetben automatikusan lefordítja a programot. A telepítés tulajdonképpen a létrejött parancsok megfelelő helyre másolását jelenti. Arra figyeljünk, hogy a fordítás rendeben lefusson, hiszen a parancsfájl nem ír ki semmilyen hibaüzenetet. Ezért menjünk vissza a terminál ablakban és ellenőrizzük, hogy nincs hibát tartalmazó sor. A telepítés alapértelmezett könyvtára a */usr/local/bin*. Persze ez eltérhet, ha nem a fent említett módon telepítjük, hanem a ***Linux*** terjesztésünk csomagját használjuk. A ***SuSE Linux*** alatt például a */usr/sbin* könyvtárba kerül a futtatható fájl.

Miután végeztünk a telepítéssel, máris elindíthatjuk a programot, amihez egyszerűen rendszergazdaként adjuk ki az `iptraf` parancsot. Meg kell jelennie a az *IPTraf* köszöntő képernyőjének amiből bármilyen billentyű lenyomásával átléphetünk a főmenübe (*1. ábra*).

Az *IPTraf* programnak szüksége van a ***terminfo*** adatbázisra, amit a */usr/share/terminfo* útvonalon keres. Ha `Error opening terminal` hibaüzenetet kapunk, amikor megpróbáljuk elindítani a programot, akkor valószínűleg az adatbázis más útvonalon található. Ilyen esetben keressük meg, hogy melyik könyvtárban van, majd adjuk ki a



1. ábra Az IPTraf indulása

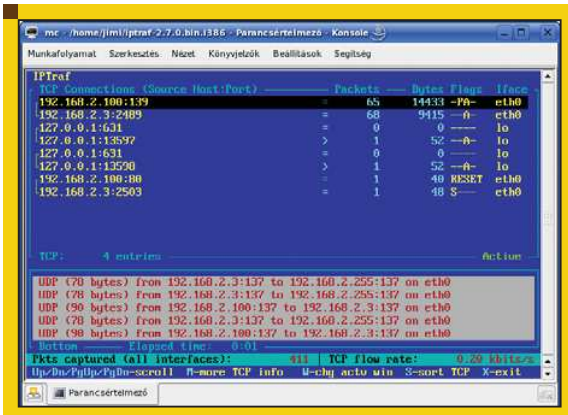
```
TERMINFO=/usr/lib/terminfo
```

majd az

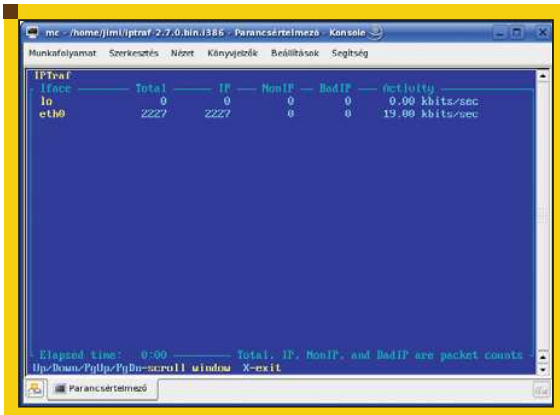
```
export TERMINFO
```

parancsokat. Persze az elérési útvonalat ne felejtsük el átírni. Ahhoz, hogy ne kelljen minden újraindítás után begépelni ezeket a parancsokat, berakhatjuk őket a *~/.profile* fájlba, ami minden bejelentkezésünkkor fog futni. Használhatjuk a rendszer */etc/profile* fájlját is, ugyanis ez minden operációs rendszer betöltődéskor le fog futni. Ha bonyolultnak találjuk ezt a műveletsorozatot, akkor hozzunk létre a könyvtárra egy linket az alábbi paranccsal:

```
ln -s /usr/lib/terminfo
➥/usr/share/terminfo
```



2. ábra Az IP forgalom figyelése



3. ábra Általános csatoló statisztika

Persze ne felejtsük el átírni a megfelelő könyvtárneveket. A program indulása után a menüből tudjuk kiválasztani, hogy az öt üzemmód közül melyiket szeretnénk használni. Az üzemmódok a következők:

IP forgalom figyelése (IP traffic monitor)

Ebben az üzemmódban a kiválasztott csatolón folyó *TCP* adatforgalmat vehetjük szemügyre. Az ablak két részből áll, a felső részben láthatjuk a *TCP* kapcsolatok legfontosabb adatait: a forrás és a cél címét, valamint a szolgáltatás portszámát, a csomagok számát (*Packets*), méretét (*Bytes*), a kapcsolatnál használt állapotjelző biteket (*Flags*), valamint hogy a kapcsolat melyik csatolón keresztül jött létre. Az állapotjelző bitek meghatározzák, hogy az éppen feldolgozott keretek milyen állapotban vannak.

Ezt az üzemmódot vehetjük szemügyre a *2. ábrán*. A címek mindig két részből, egy célból és egy forrásból állnak, amelyek között az összetartozást egy kapocs mutatja. A listában fel-le kurzormozgató billentyűkkel lépkedhetünk, így az ablaknak az a tartalma is elérhető, amely nem fér el a képernyőn. Az *M* billentyű lenyomásával a kapcsolat csomag- és az ablakméretét is ellenőrizhetjük. Fontos, hogy melyik ablakrész az aktív, ezek között a *W* billentyűvel válthatunk.

Az alsó ablakban a kapcsolatban használt csomagok adatai láthatók, a méreten túl a forrás- és célcím, valamint a hálózati csatoló neve szerepel. Az *S* billentyűvel a sorba rendezés szempontját választhatjuk ki, mégpedig két lehetőségből, a csomagok számából, illetve a csomagok méretéből.

Az *IPTraf* jelen verziója már helyesen kezeli és jeleníti meg azoknak a forgalomirányítóknak a forgalmát, amelyek hálózati címfordítást (*Network Address Translation, NAT*) és *IP* cím elrejtést (*IP Masquerading*) végeznek. Ilyen vizsgálatakor minden csomagot kétszer látunk, a bejövő csomagok között éppúgy, mint a kimenők között.

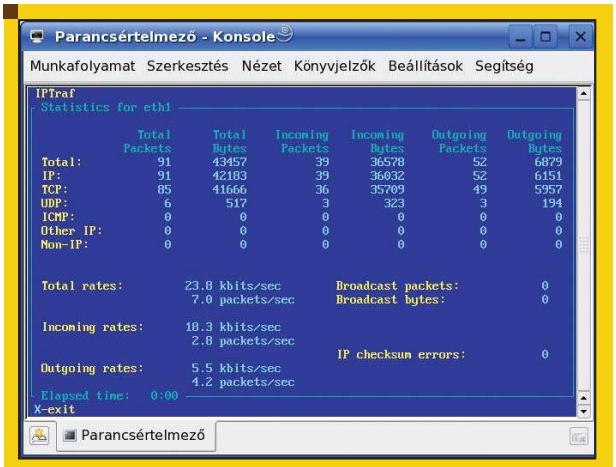
Általános csatolóstatisztika (General interface statistics)

Ebben az üzemmódban a számítógépükbe telepített csatolók összefoglaló adatait látjuk. A táblázatban olvashatjuk a csatoló nevét (*Iface*), a program jelen üzemmódjának indítása óta forgalmazott csomagok számát (*Total*), a használt *IP* címeket (*IP*), a nem *IP* csomagokat (*NonIP*), a hibás *IP* csomagok számát (*BadIP*), valamint az éppen aktuális adatátviteli sebességet. Ezt az üzemmódot mutatja be a *3. ábra*.

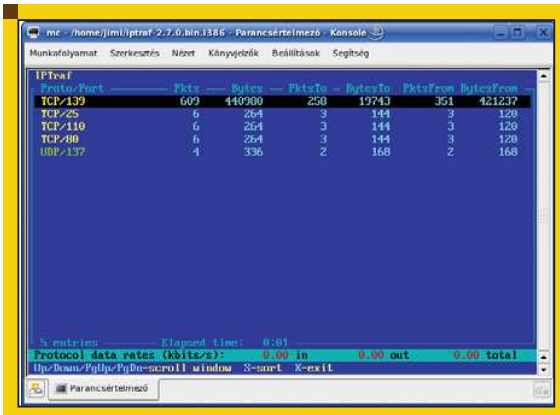
Részletes csatoló statisztika (Detailed interface statistics)

Ez az előző üzemmód bővítése, amit már csak egy csatolóra választhatunk ki. A megjelenő ablakban egy kétdimenziós táblázatban tanulmányozhatjuk, a csomagok számát (*Total Packets*), méretét (*Total Bytes*), a bejövő csomagok számát (*Incoming Packets*) és méretét (*Incoming Bytes*), valamint a kimenő csomagok számát (*Outgoing Packets*) és méretét (*Outgoing Bytes*). Mindezeket az adatokat megmutatja a program az összes csomagra, az *IP* csomagokra, a *TCP*, *UDP* és *ICMP* keretekre, valamint a más *IP* és hibás *IP* kapcsolatokra vonatkoztatva.

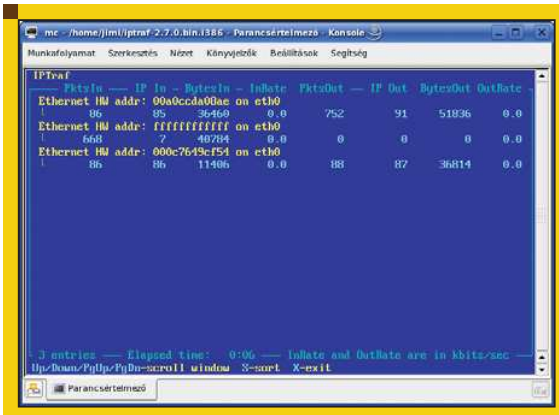
A táblázat alatt sebesség adatokhoz is hozzájuthatunk, hiszen a program megadja a teljes, a bejövő és a kimenő, valamint az adat szórt csomagok számát és méretét, ráadásul még azoknak az *IP* csomagoknak a számát is, amelyek *IP* ellenőrző összege érvénytelen volt. Ezekből az adatokból már egy csatoló működésére következtetni tudunk. Ha sok a hibás ellenőrző összeges csomag, akkor az utalhat hálózati hibára. Az ablak felépítését mutatja az *4. ábra*.



4. ábra Részletes csatoló statisztika



■ *5. ábra* TCP/UDP statisztikai üzemmód



■ *6. ábra* Helyi hálózat forgalmának figyelése

Statisztikai üzemmódban (Statistical breakdowns)

Mint a nevében is benne van, statisztikákat kapunk a képernyőre. A menüpontnak két további almenüje van, amivel kiválaszthatjuk, hogy a statisztika csomagméretre, vagy *TCP/UDP* portra vonatkozzon-e. Az előbbi esetben egy olyan táblázatot kapunk, amelyben csomagméret határok vannak felsorolva és mindegyik után látható, hogy hány darab csomag volt a felügyeleti időszakban abban a tartományban. A csomagméretbe nem tartozik bele az adatkapcsolati fejrész, és a maximális méretet az ***MTU (Maximum Tranfer Unit, maximális adatátviteli egység)*** határozza meg.
A *TCP/UDP* statisztikában egy táblázatban felsorolja a program a portokat (protokoll/portszám), valamint az ezeken keresztülment csomagok számát és méretét, valamint, hogy ezek közül mennyi volt bejövő és mennyi volt kimenő csomag. Ha nem tudjuk, hogy melyik port milyen szolgáltatáshoz tartozik, segítségünkre lehet a */etc/services* fájl, amit a

```
less /etc/services
```

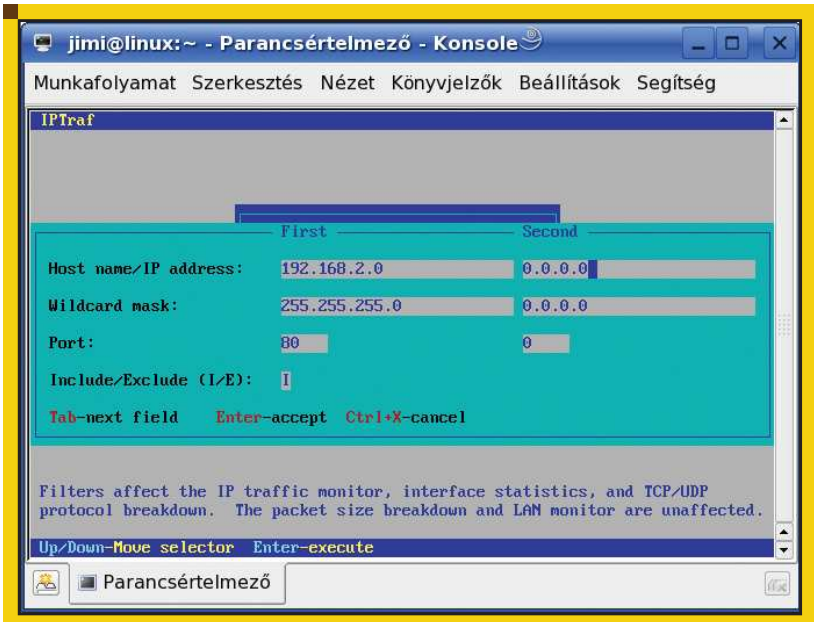
paranccsal írathatunk ki a képernyőre, vagy esetleg a listát szűrhetjük is a `grep` paranccsal, amihez például a 80-as számot tartalmazó sorokhoz az alábbi formában használhatjuk

```
less /etc/services | grep 80
```

A listát sokféleképpen sorba rendezhetjük, amit az *S* billentyű lenyomásával tudunk eldönteni. Itt gyakorlatilag minden oszlopot kiválaszthatunk és a program a csomagokat az szerint fogja sorba rendezni. Az ablak felépítését az *5. ábrán* vehetjük szemügyre.

Helyi hálózati felügyelet (LAN station monitor)

Ebben az üzemmódban a hálózat forgalmát tudjuk felügyelni. Ez akkor hasznos, ha például lelassul a hálózatunk, akkor ebben az üzemmódban kideríthetjük, hogy melyik számítógép bonyolít nagy forgalmat, ami esetleg okozhatja a lassulást.
Az egyéb okokból kialakuló lassulást más, az eddig ismertetett üzemmódokban kereshetjük meg. Két dologra kell felhívnom a figyelmet. Az egyik, hogy a számítógép, amelyen elindítottuk az *IPTraf*-ot, is szerepelni a fog a listában. Ha ez a számítógép egy forgalomirányító, akkor valószínűleg ennek lesz a legnagyobb a forgalma, hiszen a teljes hálózati adatkapcsolat rajta keresztül zajlik.
Ha a listát sorban szeretnénk látni, használjuk az *S* billentyűt, ahol kiválaszthatjuk, hogy milyen szempont szerint szeretnénk ezt megtenni.
A másik, amit megemlítenék, hogy a kártyák fizikai, vagyis *Ethernet* címe látható a listában. Ebből még nem tudjuk, hogy melyik gépben található a hálózati kártya, ezért ehhez használhatjuk a forgalomirányítón az */sbin/arp* parancsot, amely kiírja, hogy melyik *IP* címhez milyen *Ethernet* cím párosul, valamint azt is, hogy ez melyik hálózati csatolón keresztül érhető el. Ennek az üzemmódnak a segítségével már nem tudnak a nagy hálózati forgalmat generáló számítógépek megbújni.
Ezt az üzemmódot mutatja be a *6. ábra*.
Ha nagy a forgalom a hálózatunkban, szükség lehet a hosszú listát valamilyen szempont szerint rövidíteni, vagyis szűrni. Erre szolgál a ***Filters*** menüpont, amely alatt szűrési feltételeket adhatunk meg, törölhetünk szűrőt, illetve alkalmazhatjuk azt valamelyik üzemmódban megkapott listára.
Ha a menüt kiválasztjuk, akkor a választhatunk a ***TCP (TCP...)***, az ***UDP***, a más ***IP (Other IP...)***, az ***ARP***, a ***RARP*** és a nem ***IP (Non-IP...)*** lehetőségek közül. Az almenü jobboldalán látható, hogy milyen szűrési feltételek vannak beállítva a különböző, előbb felsorolt területeken. A ***TCP...*** pont alatt új szűrési feltételt tudunk felvenni (***Define custom TCP filter...***), érvényesíteni tudjuk a szűrőt (***Apply custom TCP filter...***), szerkeszthetjük a szűrőinket (***Edit custom TCP filter...***), valamint törölhetjük is azokat (***Delete custom filter...***).
A szűrő létrehozásnál, tartozzon bármelyik protokollhoz is, kell adnunk egy nevet a szabálynak, majd meg kell adnunk a ***forrás (First)*** és a ***cél IP címét (Second)***, a ***hálózati maszkot (Wildcar mask)***, valamint a portot. Nem árt tudnunk, hogy a forrás- és célcím szerepkörök felcserélődhetnek, a kétirányú kapcsolat következtében, valamint, hogy konkrét gépek címéhez a hálózati maszk `255.255.255.255`. Ha valamelyik címet nem szeretnénk megadni, akkor használjunk ott `0.0.0.0` *IP* címet és a hálózati maszk is `0.0.0.0` legyen.
Az is meghatározhatjuk, hogy azokat a csomagokat lássuk, amelyek megfelelnek a szűrési feltételnek (***Include, I***), vagy azokat, amelyek nem (***Exclude, E***). A mezők között



7. ábra Új TCP szűrő definiálása

a tabulátorral mozoghatunk, míg az *Enter* billentyűvel elfogadhatjuk a beállításokat, a *CTRL+X* kombinációval pedig kiléphetünk. A *7. ábrán* egy minta látható, ahol azt vizsgáljuk, hogy a `192.168.2.0/255.255.255.0` hálózatban milyen web-re irányuló forgalom van.

Az *UDP...* menü alatt hasonló lehetőségeink vannak, azonban itt még két további pontot is kiválaszthatunk, az egyikkel az összes *UDP* csomagot engedélyezhetjük (*Show all UDP packets*), míg a másikkal az összes nem *UDP* csomagot jeleníthetjük meg a képernyőn (*Show no UDP packets*).

Érdekes lehet az *Other IP...* pont, ugyanis itt azokat a csomagokat szűrhetjük, amelyek nem az aktív adatátvitelben vesznek részt, hanem egyéb adatvezérlési szerepük van, mint például az irányító protokollokban használt csomagok.

Éppen ezért a szűrő meghatározásánál azt is megadhatjuk, hogy milyen protokoll látszódjon. Választhatunk az *ICMP (Internet Control Message Protocol, internet üzenettovábbító protkoll)*, az *IGMP (Internet Group Management Protocol, internet csoport menedzselő protokoll)*, az *OSPF (Open Shortest Path First, nyílt legrövidebb út először protokoll)*, az *IGP (Interior Gateway Protocol, belső átjáró protokoll)*, az *IGRP (Interior Gateway Routing Protocol, belső forgalomirányító átjáró protokoll)*, a *GRE (General Routing Encapsulation, általános zárt forgalomirányítás)* és más *IP* protokoll (*Oth IP*) közül. Ha mindegyiket szeretnénk vizsgálni, megtehetjük az *Y* billentyűvel.

Az *ARP (Address Resolution Protocol, címfeloldó protokoll)* és a *RARP (Reverse Address Resolution Protocol, inverz címfeloldó protokoll)* üzeneteit is megjeleníthetjük (*Visible*), vagy éppen elrejthetjük (*Not visible*) a különböző üzemmódokban.

A két lehetőség közül az *Enter* billentyűvel válthatunk.

A *nem IP csomagok (Non-IP)* láthatóságát is tilthatjuk (*Non visible*), vagy engedélyezhetjük (*Visible*). A program beállításait finomhangolhatjuk a *Config* menüpontban. Kissé összetett ablakot kapunk, ha kiválasztjuk ezt a menüpontot.

A *Reverse DNS lookup (inverz DNS névfeloldás)* bekapcsolt állapotában az *IPTraf* megpróbálja a tartományneveket és az *IP* címeket feloldani. Ehhez persze DNS szerverre van szükség, illetve a */etc/hosts* fájlban megfelelő módon be kell jegyezni a számítógépeinket.

A *TCP/UDP service names (TCP/UDP szolgáltatás nevek)* bekapcsolásával a portok helyett a szolgáltatás nevét láthatjuk a képernyőn.

A *Force promiscuous (válogatás nélküli csomagvizsgálat)* bekapcsolásával a kártyát ebbe az üzemmódba kapcsolhatjuk. Ahhoz, hogy megértsük, mit is jelent ez, egy kicsit a hálózati csatolók és a hálózatok működésébe is be kell tekintenünk. Alapesetben a hálózati csatoló csak azokat a kereteket veszi, amelyekben az ő *Ethernet címe (MAC cím)* szerepel, mint célcím. Pontosabban a bemeneti átmeneti tárba minden keret beírásra kerül, de a felsőbb rétegek felé már csak azokat küldi el, amely ténylegesen a mi számítógépünknek szól.

Ha a kártyát átállítjuk *promiscuous* üzemmódba, akkor minden keretet továbbítani fog a felsőbb rétegek felé. Ezzel gyakorlatilag akár a szegmens teljes hálózati forgalmát le lehet hallgatni. Ha egy szerveren futtatjuk a programot, akkor alapvetően minden forgalom rajta keresztül zajlik, viszont ha nem, akkor is rendkívül hasznos lehet ennek a módnak a használata. Azt is meg kell említenem, hogy nem minden hálózati kártya képes ennek az üzemmódnak a kezelésére.

A *Color (szín)* magért beszél, ha engedélyezzük, akkor a program színesben fut, egyéb esetben pedig szürke árnyalatosan.

A *naplózás (Logging)* bekapcsolásával az a forgalom, amit a program a képernyőn mutat, egy fájlban is tárolásra kerül. A naplófájlnak a nevét és az elérési útvonalát a hálózatfigyelés előtt minden üzemmódnál megkérdezi tőlünk a program. A /var/log/iptraf könyvtár szolgál ezeknek az állományoknak a tárolására.

Azt is beállíthatjuk, hogy az átviteli sebességnél *kbit/s* vagy *kBájt* mértékegység közül melyiket szeretnénk használni. Erre szolgál az *aktivitás mód (Activity mode)* menüpont.

Amennyiben szeretnénk a hálózati forgalom figyelésénél a forrásgép fizikai (*MAC*) címét is látni, akkor állítsuk át ezt a *Source MAC addrs in traffic monitor* menüpontban.

A *Timers* menüpont alatt időzítési beállításokat végezhetünk el. A *TCP timeout... (TCP időtúllépés)* pont alatt percekben tudjuk megadni azt az időt, aminek letelte után a a kapcsolatot megszakadtnak tekintjük. Alapértelmezés szerint ez 15 perc.

A *Log Interval... (naplózási időtartomány)* menüben felülbírálhatjuk az a 60 perces értéket, amíg az *IPTraf* a különböző üzemmódok adatait elhelyezi egy fájlba a megadott helyre. Természetes azt is beállíthatjuk, hogy milyen gyakorisággal frissüljön (*Screen update interval...*) a különböző üzemmódokban összeállított lista. Itt másodpercekben adhatjuk meg az időt. A *TCP closed/idle persistence...* menüpontban azt tudjuk meghatározni, hogy az *IPTraf* mennyi idő elteltével távolítsa el a *TCP* ablakból a megszakadt, lezárt vagy forgalommentes kapcsolatokat.
Az *Additional ports...* menüpont alatt meg tudjuk adni annak a porttartománynak az elejét és a végét, amelyet vizsgáltatni szeretnénk az *IPTraf* programmal. Alapértelmezés szerint az *IPTraf* csak a jól ismert szolgáltatások portjait vizsgálja, amelyek portszáma 1024 alatti.
Ha szeretnénk a magasabb portokat forgalmát is megjeleníteni, akkor itt megadhatjuk ezt. Ha már nincs szükségünk a kiegészítő porttartományra, akkor azt törölni a *Delete port/range...* menüponttal lehet.

Az *IPTraf* rendelkezik egy nagyon hasznos lehetőséggel, amely főleg rendszeres használat mellett hálálja meg magát. Amint már láttuk a hálózatban adatokat cserélő gépeket a fizikai cím alapján azonosítja és jeleníti meg. Ahogy már említettem az *ARP* táblát kiírathatjuk, amiből megtudhatjuk az IP címet és ezzel együtt már beazonosíthatjuk a számítógépet. Az *Ethernet/PLIP host descriptions...* menüpontban lehetőségünk van a fizikai címhez leírást párosítani, amivel az *ARP* tábla alapján történő címfeloldást megtakaríthatjuk magunknak. Ha ezt elvégezzük, akkor a forgalom felügyeletnél a MAC cím mellett a gép leírása is olvasható lesz. Ezt a funkciót a gyűrű topológiájú hálózatokban is használhatjuk, ebben az esetben az *FDDI/Token Ring host descriptions...* menüpontban adjuk meg a címek leírását.
Az *IPTraf* nem csak a menürendszerén keresztül kezelhető, hanem a fenti üzemmódokba parancssori kapcsolókkal beléptethető, amivel akár automatizálni is lehet a futását. A kapcsolókról az

```
iptraf --help
```

paranccsal kaphatunk információt. Mit láthattuk, az *IPTraf* programnak nagyon sok lehetősége van és megfelelő tudással nagyon sok mindent el tud árulni a számítógéphálózatunkról és az abban folyó adatforgalomról. A rendszergazdáknak egy nagyon hasznos eszköz, akár automatizálva a teljes forgalom felderíthető. Arra azonban ügyelünk, ha a naplózást bekapcsoltuk, akkor elég tetemes mennyiségű adatot képes eltárolni, ami pedig akár pár nap alatt is betölthet egy /var partíciót. Ennek a kezelésére is megvannak a módszerek, de azt már nem ennek a cikknek a feladata bemutatni.

Markó Imre
(linux@akribisbt.hu)

Hardvermérnök és mérnöktanár végzettsége van. Saját cégében Linux rendszerek tervezésével és üzemeltetésével foglalkozik. Ezen kívül egy főiskolán oktat, elsősorban hardveres tantárgyakat.