Computer PANORÁMA
Computer Panoráma
XIII. évfolyam 19. különszám, 2002/2003. tél
Ára: 695 Ft

HÁLÓZATOK

KÜLÖNSZÁM

CD-melléklettel

33 tipp és trükk

- Hálózati szabványok
- A TCP/IP részletesen
- Windowsos hálózatok építése
- Vezeték nélküli hálózati eszközök
- A leghatékonyabb tűzfalak
- Hálózati diagnózis
- Sok PC – egy modem
- Tűzfal – itthonról

A leghasznosabb ismeretek a hálózatokról

02019
9 770865 524027

...azon rágódtam

megtettem-e mindent, hogy az adataim biztonságban legyenek?

Ma már

nyugodt vagyok, mert tudom, hogy a legsúlyosabb üzemzavar esetén is a nap bármely szakában elérhetem őket és segítenek a problémám megoldásában.

a magyar oktatás és állami szféra hivatalos beszállítója

22 platformon 7 keresőmotort kínálunk egy rendszerben,

közvetlen szakmai támogatást a gyártótól ***egy kézből***

VirusBuster
www.virusbuster.hu

1116 Budapest,
Vegyész utca 17-25.
Tel: 382-7000
Fax: 382-7007
mail@virusbuster.hu

ELMÉLET

GYAKORLAT

HARDVER

SZOFTVER

BIZTONSÁG

IMPRESSZUM

HÁLÓZATOK
A Computer Panoráma különszáma
XIII. évfolyam 19. különszám, 2002. december

Felelős szerkesztő: Horváth Annamária
Tördelőszerkesztő: Dancs Katalin
Titkárságvezető: Szőke Erika
Címlap: Szincsák László

Szerkesztőség:
1091 Budapest, Üllői út 25. I. em.
Telefon: 456-6888, fax: 456-6970
E-mail: c.panorama@cpanorama.hu
Internet: http://www.computerpanorama.hu

Felelős kiadó: Dely Tamás ügyvezető igazgató
1091 Budapest, Üllői út 25. I. em.
Telefon: 456-6888

Kiadó: A HVG Kiadó és a WEKA Computerzeitschriften-Verlag GmbH közös vállalata, a Computer Panoráma Kiadói Kft. Computer Panorama Verlag GmbH

Terjesztés:
Mosolygó Kitti marketing- és terjesztési vezető
1091 Budapest, Üllői út 25. I. em.
Telefon: 456-6964, fax: 456-6970,
e-mail: terjesztes@cpanorama.hu

Ügyfélszolgálat
hétfő–péntek: 9–17 óráig
Terjeszti: a Hírker Rt., az NH Rt. és alternatív terjesztők

Hirdetésfelvétel:
hirdetési vezető: Tasnádi Rózsa
hirdetésszervező: Háder Judit, Kuba Ilona
1091 Budapest, Üllői út 25. I. em.,
Telefon/fax: 456-6974, fax: 456-6970
E-mail: c.panorama@cpanorama.hu

Hirdetésfelvétel Németországban:
Telefon: 0049-8121-95-1182
Telefax: 0049-8121-95-1627
E-mail: Akieger@wekanet.de

A Computer Panoráma különszámai megrendelhetők:
a kiadónál személyesen, levélben, e-mailben, weboldalunkon vagy a postahivatalokban, a hírlapkézbesítőknél és a Hírlap-Előfizetési és Elektronikus Posta Igazgatóságon (HELP)
1900 Bp. XIII., Lehel út 10/A, a Postabank Rt. 219-98636/021-12799 pénzforgalmi jelzőszámon. A különszámok megvásárolhatók a hírlapboltokban, könyvesboltokban, a kiadónál. A régebbi számokat keresse a kiadóban, telefon: 456-6964, 1091 Budapest, Üllői út 25. I. em.

Az Hálózatok különszámot készítette:
Levilágítás: HVG Press Kft.
Nyomtatás: Szegedi Kossuth Nyomda Kft.
6723 Szeged, Makkosházi krt. 1.
Felelős vezető: Gera Imre ügyvezető igazgató

A Computer Panoráma különszámában megjelenő valamennyi cikket és listát szerzői jog védi. Másolásuk bármilyen formája – fotokópia, mikrofilm készítése, adatrendszerekben való tárolása stb. – kizárólag a kiadó előzetes írásbeli engedélyével történhet.

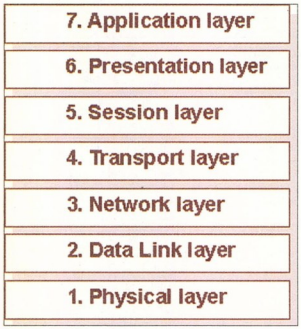
ISSN 0865-5243

Behálózott világ

A történet kezdetén az *OSI rétegmodell* áll, amely roppant hasznosnak bizonyult a számítógépes hálózati technikánál.

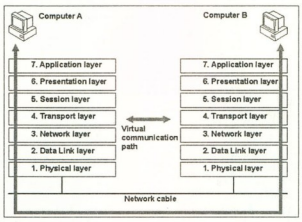
Az OSI modell

A számítógépek közötti hálózati kommunikáció leírásához rendszerint az *OSI (Open Systems Interconnection) modellt* használják. Ez egy *hétszintű réteghalmaz*, ahol a szintek tartalmazzák a kommunikációs protokollokat. A hálózati hardver- és szoftvergyártók ezekhez az előírásokhoz tartják magukat, így lehet a különböző készülékek között *gyártófüggetlen kommunikáció*, azaz egy Macintosh TCP/IP protokoll réteghalmaza egy Unix gép TCP/IP réteghalmazával kommunikálhat.



Az OSI modell hét réteget definiál, ezek tartalmazzák a kommunikációs protokollokat. A TCP/IP az OSI modell egyik implementációja

A kommunikáció a partnerek egymásnak megfelelő rétegei között zajlik. Az egyik számítógép szállítási rétege egy virtuális kapcsolaton keresztül csak a másik számítógép szállítási rétegével képes kapcsolatba kerülni. A valóságban az adatok az adóoldalon fentről lefelé járják végig a réteghalmazt, a kábelen keresztül a vevőhöz kerülnek, és ott is végighaladnak felfelé a réteghalmazon a megfelelő protokollrétegig. A rétegfelépítés előnye, hogy egy rétegnek csak a közvetlenül felette és alatta lévő réteggel kell kommunikálnia, és nem kell törődnie a további összetett lépésekkel. Könnyen lehet protokollokat hozzátenni, mindaddig, amíg a specifikációt betartják. Az OSI modell legalsó rétege a *fizikai réteg*. Ez a bitek kiküldéséért és fogadásáért felel. Ezen kívül meghatározza a feszültséget, a feszültségváltozást, az átviteli sebességet és az átviteli távolságot, valamint a csatlakozó típusát. Az UTP-s Ethernetnek például más a specifikációja, mint a koaxos Ethernetnek.



A két egymással kommunikáló számítógép egymásnak megfelelő rétegei között virtuális kapcsolat létesül. Az adatok azonban egészen más úton haladnak

Írásunkban megismerkedhetnek az olcsó, koaxiális kábeles vagy csavart érpárú Ethernet hálózatok specifikációjával, megtudhatják, hogy miért jobb a Token Ring, és hogy mi a helyzet az üvegszálas hálózatokkal, mint amilyen az FDDI vagy az ATM.

Az *adatkapcsolati réteg* a felette elhelyezkedő szállítási rétegből adatkeretek (frame-ek, bitsorozatok) formájában kapja az adatokat. A fő feladata, hogy bitekre konvertálja az adatkereteket, majd a fizikai réteg felé továbbítsa ezeket. Vagy fordítva: a fizikai rétegből biteket kap, ezekből adatkereteket készít, és a szállítási réteg felé küldi azokat. A kapcsolati réteg olyan funkciókat is ellát, mint a címzés, valamint a hiba- és bitfolyam-ellenőrzés. Ehhez két alrétegre lett felosztva, a *MAC*

rétegre (Media Access Control, közeghozzáférés kontroll) és az *LLC rétegre (Logical Link Control,* logikai hozzáférés kontroll).

A MAC réteg képezi az interfészt a hálózati kártya felé. Specifikálja többek között a hozzáférési módszert és a hálózati topológiát is. Kezeli az úgynevezett fizikai készülékcímeket, röviden a MAC címeket, amellyel egyértelműen lehet azonosítani minden egyes hálózati készüléket. Az Ethernet és Token Ring kártyáknál a címet fixen behuzalozták a kártyákba. Egy Ethernet MAC cím hat bájtból épül fel: az első két bájt a gyártót adja meg, a maradék négyből egy egyértelmű „házszám" képződik a készülék számára. Egy szegmensen belül egy készüléket mindig a MAC címmel lehet megtalálni (pl. a TCP/IP esetében az ARP-vel). A részháló valamennyi készüléke megkapja a keretet, kiértékeli a MAC címet, és ha neki lett szánva, akkor feldolgozza a keretet, különben eldobja. Az LLC alréteg a bitfolyam- és hibaellenőrzésért felelős. A folyamellenőrzés azt az időegységenként átviendő adatmennyiséget határozza meg, amelyet a kapcsolat mindkét résztvevője képes kezelni. A hibaellenőrzés a hibák felismerésért és a sérült keretek ismételt elküldésért felel.

Logikai topológiák

A tényleges gyűrű kivitel ritka. A fizikai topológia rendszerint egy csillag, mint a vezérjeles hálózatoknál, csak épp a jel útja követi a gyűrűt állomásról állomásra, így a logikai topológia a gyűrű.

A kábel zavarai

Mindegyik rézvezető kívülről ható elektromágneses sugárzásnak is ki van téve. Ezt a sugárzást elektromos gépek, neoncsövek, számítógépek, fénymásolók és sok egyéb berendezés kelti. Ez a zaj valamikor olyan erőssé válhat, hogy az eredeti jeltől már nem lehet megkülönböztetni. Ilyenkor már lehetetlen venni az adatokat.

Minél hosszabb egy kábel, annál nagyobb ez a zaj. Ezért az átviteli utak megnöveléséhez úgynevezett *repeater*-eket használnak. Ezek azonban nemcsak a hasznos jelet, hanem a zajt is erősítik. Ezért is lehetetlen végtelen hosszú kábelt használni. Zaj esetén a legjobb védelmi eljárás a kábel leárnyékolása. Az üvegszálas kábeleket nem érinti ez a probléma.

Az úgynevezett jel/zaj-viszony a jel minőségét minősíti:

$$S=10\times\log(\text{jelszint}/\text{zajszint})[\text{dB}]$$

A jel/zaj-viszonyt decibelben (dB) mérik. A nagy érték nagy hasznos jelre és kis zajra utal, vagyis „jó" vezetéket jellemez.

Komplex hálózatok

Egy szegmensen belül tehát a MAC címe alapján lehet megtalálni a készüléket. Az olyan komplex hálózatok esetében, amelyek számos alhálózatból épülnek fel, a készülékenkénti címzés kezelhetetlen lenne. Ezért a teljes alhálózatot logikailag címzik meg, viszont egy alhálón belül külön címzik az egyes készülékeket. Erről a *hálózati réteg* gondoskodik. Ez az egyik alhálóból a másikba vezérli a csomagokat, vagyis utat *(route)* talál a hálón. A *routing (útkeresés)* ennek a rétegnek az egyik feladata.

A hálózati réteg úgynevezett *portokat* használ, amelyek egy számítógép egyik folyamatához vannak rendelve. A portokat szolgáltatásokhoz rendelik hozzá, így például a webböngésző és a webszerver között a 80-as porton keresztül zajlik a kommunikáció, míg az FTP a 21-es porton bonyolódik stb. Ezek a szolgáltatások egyszerre is futhatnak egy olyan számítógépen, amelyhez csak egyetlen egy címet rendeltek. Ez a cím a TCP/IP esetében az *IP-cím.* A különböző szolgáltatások megkülönböztetéséhez az IP-cím és a port-szám kombinált megadására van szükség, amit *socket-nek* is hívnak.

A postahivatal

Egy LAN-szegmens adatcsomagja rendszerint sok különböző router-en megy keresztül, amíg a célszegmensbe jut. Az átvitel eközben különböző módokon bonyolódhat.

A *vonali kapcsolat* esetében a telefonáláshoz hasonlóan a két állomás között fix kapcsolatot létesítenek. Ez a hálózaton keresztül egy fix nyomvonalat és állandó sávszélességet garantál. Az ilyen kapcsolatot azonban más készülékek nem használhatják, ami a sávszélesség pazarlásához vezethet.

A hírátvitel számos különböző úton haladhat a hálón. A router-ek a routing algoritmusok alapján különböző utakat találnak, ami többek között a költségtől is függ (Hopcount). Egy üzenet, például egy e-mail, egy darabban kerül átvitelre, és átmenetileg eltárolódik a kapcsolati készülékeken, mielőtt továbbítódna (store and foreward). Egy bizonyos időkésleltetés, a két számítógép közötti valós idejű kommunikációval ellentétben, itt elfogadható. A hírátvitelnek ez a módja hatékony, mert egy adatcsatornát számos különböző készülék is igénybe vehet, és így a sávszélességet jól kihasználják.

A csomagkapcsolás működése hasonló a hírátviteléhez, de itt több csomagra szabad felbontani az üzenetet. Mindegyik csomag *független üzenetként* viselkedik, és a lehető legjobb úton kerül a célba. A csomagméret korlátozott és hálózatonként eltérő lehet. Ezt a router-ek illesztik – a folyamat neve *fragmentálás.* A csomag méretét általában akkorának választják, hogy a routerek az operatív tárban tudják elintézni a csomagok továbbítását. Az üzenetekkel ellentétben, amelyeket átmenetileg eltárolnak a merevlemezen, a csomagok továbbítása így lényegesen gyorsabb. Az OSI modell a kommunikáció két típusát írja le: az összeköttetés-menteset és az összeköttetés-alapút.

Ha a csomagokat az interneten routolják, akkor az összeköttetésalapú kommunikáció esetében a forrás és a cél között egy nyomvonal vagy egy kapcsolat létesül. A bitfolyam- és hibaellenőrzésben az összes olyan host részt vesz, amelyen a csomag keresztülhalad. Felismeri azt a kapcsolatot amelyhez a csomag tartozik, és ezt be is zárhatja. Hibás átvitelnél a csomag ismételt elküldésére szólíthatja fel a küldő hostot.

Az összeköttetés-mentes kapcsolat esetében a forrás és cél közötti csomópontok nem vesznek részt a kommunikációban, ezek csupán továbbítják a csomagokat. A bitfolyam- és hibaellenőrzést másképpen kell megvalósítani. Erről a *szállítási réteg* gondoskodik.

A csavart érpár kategóriák

Kategória	Ismertetés
1	szokványos telefonkábel
2	beszédszolgáltatások, RS232
3	adatátvitel 16 Mbitig
4	adatátvitel 20 Mbitig
5	adatátvitel 100 Mbitig

A szállítási réteg

A *szállítási réteg* egyfelől az adatok szükség szerinti feldarabolásáról (fragmentálásáról) gondoskodik, másfelől arról, hogy a töredékek a megfelelő sorrendben illeszkedjenek egymáshoz a célban. Ez a réteg végzi a bitfolyam- és hibaellenőrzést is. A hibaellenőrzés két kommunikáló eszköz között *ellenőrző összegekkel* történik. Ha egy sérült szegmens ért célba, akkor az adót a szegmens ismételt elküldésére lehet felszólítani. A hiányos vagy dupla szegmenseket szintén felismeri, és ismét lekéri, illetve eldobja azokat.

A bitfolyam-ellenőrzés a csomagok megérkezésének a nyugtázásával történik. Ha a címzett megkap egy csomagot, akkor ezt nyugtáznia kell, vagyis igazolást küld a feladónak, és csak ezután küldik el a további csomagokat.

A viszony réteg

A *viszony réteg* feladata, hogy két számítógép között *felhasználói viszonyt* létesítsen, s a két készülék közötti párbeszédet is felügyeli. A kommunikáció alapvetően szimplex, fél-duplex vagy duplex eljárással bonyolódhat. A szimplex eljárásnál a kommunikáció egyoldalú, csak adni lehet. A fél-duplex azt jelenti, hogy az adás és a vétel váltakozva követik egymást, míg a duplex eljárásnál az adás és vétel egyidejűleg zajlik (telefon). A modemek rendszerint a duplex eljárást használják.

Egy viszony kialakítása három fázisban történik. A viszony felépítésénél egy kliens egy szolgáltatást kér egy szervertől. A szerver válaszol, és különféle paramétereket küld. Megkezdődik a paraméterek egyeztetése, vagyis a csomagméretnek, a szolgáltatás típusának, a portszámoknak stb. a meghatározása. A kért adatokat kiküldik, miközben a bitfolyam- és hibaellenőrzés is működik.

A viszony megszüntetésekor szabályozottan, kontroll-információk cseréjével zárják le a párbeszédet.

A viszonyok lehetővé teszik, hogy egy megszakadt kommunikációt egy adott időn belül folytatni lehessen. A viszony réteg még *felügyeleti információkat is* beiktat az adatfolyamba, hogy egy esetleges kapcsolat megszakadásnál csak az utolsó felügyeleti jel óta küldött adatokat kelljen megismételni, és ne kelljen a teljes üzenetet újraküldeni.

A *megjelenítési réteg* alkalmazásorientált formátumra alakítja át az alsó rétegek gépfüggetlen adatait. Ide tartozik többek között a bitsorrend megváltoztatása vagy a karakterkészletek közötti konverzió.

Az alkalmazási réteg végül interfészt képez az alkalmazások, például a böngészők vagy más programok felé.

Kapcsolati készülékek

Ha egy hálózatot több kisebb hálózatra bontanak (szegmentálnak), akkor kapcsolati eszközökkel kell összekötni a részhálókat egymással. Ezek a kivitelüktől függően, az OSI modell különböző rétegein működnek.

- Az *ismétlő* a fizikai réteget használja.
- A *híd* a kapcsolati rétegen működik.
- Az *útkiválasztó* (router)a hálózati rétegen működik.

Az *ismétlő* csupán a porton beérkező jel erősítését végzi és egy másik porton ismét kiadja. A feladata a *távolságnövelés*. Tény, hogy a sérült jeleket is erősíti, mivel az adatok vizsgálatára nincs módja. Az ismétlők olcsóbbak és a kezelésük is egyszerűbb. Némelyek különböző kábeltípusok összekapcsolását is megengedik, például a koaxiális és a csavart érpárt.

A *híd* a kapcsolati réteg szintjén szűri az adatforgalmat. Ismeri az általuk összekötött szegmensek hostjának MAC-címét, és egy belső hozzárendelési táblázatot vezet ezekről az adatokról. Így a csomagokat a megfelelő részhálóba továbbítja. Ha egy csomagot nem tud azonosítani, akkor azt, a feladó kivételével, valamennyi résztvevőnek megküldi. A híd, a felépítésétől függően, az ismétlő funkcióit is átvállalhatja, vagyis a jelerősítést és a különböző kábeltípusok összekötését.

Az *útkiválasztó* a hálózati rétegen működik, ahol az összetett routolási algoritmusok számára szükséges információk találhatók. A router-ek belső routing táblázatokat vezetnek, amelyek megmutatják az utat más hálózatokba vagy router-ekhez.

Hozzáférési eljárások

A *topológia* azt a módszert írja le, amely alapján a csomópontokat és a kapcsolati készülékeket kábellel összekötötték egymással, s amely alapján a kommunikáció bonyolódik. A legfontosabb jellemző a *hozzáférési eljárás*. Meghatározza, hogyan férnek a készülékek az átviteli közeghez. Két fontos eljárást különböztetnek meg, a *konkurens-* és a *vezérjeles (token-passing) eljárást*.

CSMA/CD

A konkurens eljárásnál a hálózat valamennyi számítógépe egyenjogú, bármelyik bármikor küldhet adatot. Ha két számítógép egyidejűleg foglalja le a kábelt, akkor *ütközés* lép fel, a jelek átfedik egymást és mindketten kioldódnak. Egy véletlenszerűen megválasztott időtartam elteltével mindkét készülék újra próbálkozik. Ha sok állomás küld egyszerre adatot, akkor a hálózat összeomlik, ami már 30-50%-os terhelés esetén fellép.

Ezért lényeges, hogy lehetőleg ki lehessen küszöbölni az ütközéseket. A *CSMA/CD (Carrier Sense Multiple Access Collision Detection)* módszer ehhez két eljárást használ. Ennek megvalósítására először belehallgatnak a hálózatba *(Carier Sense)*. Ha a kábel éppen foglalt, akkor a számítógép nem kezd el küldeni, hanem vár, amíg szabad nem lesz. Ha ennek ellenére ütközés lép fel *(Collision Detection)*, azt mindkét állomás észreveszi, és leállítja az adást. Egy véletlenszerűen megválasztott időtartam elteltével ismét adásba mennek át. Ehhez az állomások az adás alatt belehallgatnak a kábelbe, hogy megtudják, nem ad-e éppen egy másik állomás is.

A CSMA/CD-t az Ethernet hálózatokban használják. Az átviteli közeg hossza 2500 m-re korlátozott (kapcsolati készülékek nélkül). Hosszabb átviteli utak esetén az ütközés-felismerés már nem működik. Ilyenkor a kábel végén elhelyezkedő állomás nem képes felismerni, hogy egy másik állomás adásban van-e. Az ilyen hálózatokban az adatátvitel sztochasztikus (véletlenszerű), mivel nem lehet előre látni, hogy egy állomás mikor fog adni. A CSMA/CD hardver olcsó (Ethernet) és egyszerűen telepíthető, illetve fektethető. Mivel a legtöbb hálózaton a forgalom csak alkalmi jellegű, ezért az ütközésből eredő zavarok száma viszonylag csekély. Ha az adatforgalom erősen megnő, akkor szegmentálni kell a hálózatot.

Token Passing

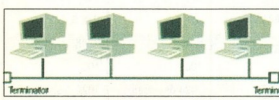
A vezérjel egy olyan *frame*, amelyet egy logikai gyűrűben állomástól állomásig adnak tovább. Ha egy állomás adni

szeretne, akkor elveszi a vezérjelet és nekikezd az adásnak. Ekkor a többi állomás közül egyik sem adhat. Ha befejezte az átvitelt, akkor a vezérjelet ismét kiadja a gyűrűbe. Így egy adott időn belül valamennyi állomás megkapja az adás lehetőségét (determinált hozzáférési eljárás, előre látható). Mivel a Token Ring hálózatokat nem blokkolhatja le ütközés, így a kihasználtságuk nagyobb, mint a konkurens hozzáférési módszer szerinti hálózatoknak. Egyes Token Ring hálózatokon kiegészítésként prioritás-hozzárendelést is alkalmaznak, így egyes állomások kiemelt kezelést kapnak.

A token-passing hozzáférési eljárással működő hálózatok közé tartozik a *Token Ring* (IEEE 802.5) és FDDI *(Fiber Distributed Data Interface)*. A Token Ring hálózatok nagy megbízhatóságra készültek. A hardver ezért különböző diagnózis és ellenőrző mechanizmusokkal van ellátva, ami emeli az árat. Ezek nagy hálózati terhelésnél kedvezőbbek az egyéb eljárásoknál, de kisebb terhelésnél ez az előny már a visszájára fordul, mivel a vezérjel továbbításához is sávszélességre van szükség. Egy 16 Mbites Token Ring és egy 10 Mbites Ethernet hálózat jellemzői közel megegyeznek egymással.

Topológiák: busz, csillag, gyűrű

A topológia meghatározza, hogy hogyan kell egymással összekötni a hálózati készülékeket. Megkülönböztetünk *busz, csillag* és *gyűrű* topológiát.



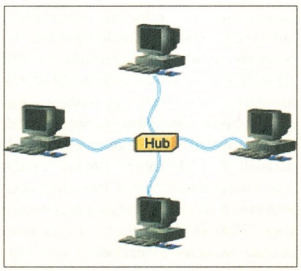
A busz topológiánál valamennyi állomás egy backbone-hoz csatlakozik. Mindkét végét ellenállással kell lezárni. A sebessége és meghibásodással szembeni védelme csekély

A busz esetében valamennyi készülék egy backbone-hoz csatlakozik. A kábelt állomástól állomásig fektetik. A jel reflexiója és a kábelen keletkező interferencia elkerülése érdekében a busz mindkét végét lezáró ellenállással kell ellátni. A busz topológia érzékeny a hibákra. Ha a kábel valahol megszakad, akkor ezzel a teljes hálózat meghibásodik. A 10 Mbit/s átviteli sebesség nagyon kevés, de mivel nincs szükség elosztókra, ezért az ilyen hálózat nagyon olcsó.

Jóval nagyobb biztonságot kínál a *csillag hálózat*. Ennél a topológiánál valamennyi állomás egy központi elosztóhoz (hub vagy switch) kapcsolódik. Egymással több elosztót is össze lehet kapcsolni, ami végül is busz kialakításához vezet (csillag-busz topológia).

Egy állomás meghibásodása a többit nem érinti, csupán egy elosztó meghibásodása érinti a hozzá kapcsolódó állomásokat. A meghibásodás elleni védelme tehát sokkal jobb, mint a busz topológiának, viszont a csillaghálózatnak jóval nagyobb a kábeligénye. A csillaghálózatnál a hibakeresés is egyszerűbb, mivel csak a meghibásodott állomás kábelét kell megvizsgálni, nem pedig a teljes buszt.

A legolcsóbb elosztó a *hub*, amely valamennyi csatlakozó készülékhez továbbítja a jelet. A hub-okat növekvő mértékben váltják fel a *switch*-ek, mivel a chipárak tovább esnek. A switch, a hub-bal ellentétben, amely nem tudja, hogy egy csomag hová tartozik, *intelligens elosztó*. „Tanul" a topológiából és ismeri a csatlakozó állomásokat. Ha egy adatcsomagot kap, azt csupán a célállomáshoz továbbítja. A switch-elt hálózatok szélsőséges esetében valamennyi állomás a saját szegmensében helyezkedik el és így a kábel teljes sávszélességét használhatja.



A csillag topológia egy központi elosztóból áll, amelyhez csillag alakban csatlakoznak az állomások. A meghibásodás elleni védelme és a sebessége is nagyobb, mint a busz topológiának, viszont több kábel kell hozzá

A gyűrűnél valamennyi állomás köralakban van egymással összekapcsolva. Mindegyik csomópont mindkét oldalán van egy szomszéd. A jel egy irányban halad a gyűrűn. Mivel a jelet minden csomópont erősíti (ismétlő funkció), így a jelvesztesség csekély.

Ethernet

Manapság a leggyakrabban az *Ethernet hálózatot* használják. A komponensei olcsók, és könnyű lefektetni a kábelét. Az Ethernet ellátja az OSI modell bitátviteli rétegének a feladatát, s az *Internet réteg* IP-csomagjait úgynevezett Ethernet keretekké (frames) konvertálja, amelyeket a kábel továbbít. Eközben az IP-cím MAC-címmé konvertálása is megtörténik.

Egy Ethernet keret 64 és 1518 bájt közötti méretű, viszont a kerethez legalább 18 bájtra van szükség, így az adatok számára 46-1500 bájtnyi hely marad.

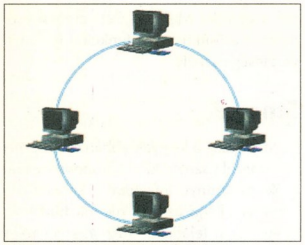
Minden bájt egy, a keret elejére utaló, bevezető jellel kezdődik. Ezt a címzett és a feladó MAC-címei, valamint egy típusmegadás követik, amely a hálózati protokollt (pl. IP vagy IPX) tartalmazza. Ezután az adatok következnek. Az adatokat egy ellenőrzőösszeg zárja.

Az Ethernetet az IEEE 802.3 specifikáció írja le, habár a kettő nem százszázalékosan egyforma. Az Ethernet topológiája a *10Base2* és a *10Base5*, amit *thinnet-nek* és *thicknet-nek* is neveznek, valamint a csavart érpáros változat a *10BaseT* és a *100BaseT*. Az első szám, tehát a 10 vagy a 100 a sebességet adja meg Mbit/s-ban. A Base jelentése alapsáv, szemben a szélessávval. A 2,5 vagy T a *fizikai közeg típusát* jelöli.

Thicknet, 10Base5

Egyes cégeknél még találkozhatunk a ma már elavult thicknet-kábellel, amelyet a sárga színe miatt *Yellow Cabel*-nek is neveznek. A thicknet 10 Mbit/s-os alapsáv, a topológiája busz topológia. A hálózati kártyákon úgynevezett AUI-aljzatokat találunk *(Attachment Unit Interface)*, amelyek AUI- vagy Transceiver-kábelhez kapcsolódnak. Ez utóbbi a kábel és a számítógép között hozza létre a kapcsolatot. Két transceiver között a minimális távolságnak 2,5 méternek kell lennie, a Transceiver kábel hossza legfeljebb 50 méter lehet.

Egy thicknet szegmens maximum 500 méter hosszú lehet, ebbe a transceiver kábel nem számít bele. Itt az *5-4-3 szabály* van érvényben, ahol is maximum 5 backbone szegmenst 4 ismétlőn keresztül le-



A gyűrű topológiát fizikailag csillag topológia alakjában készítik el. Csupán a jel útja kör alakú

het összekötni egymással. A számítógépek azonban csak 3 szegmensben helyezkedhetnek el. Ez összességében 2500 méter hosszat eredményez a thicknet számára, ahol is a három szegmens mindegyikében maximálisan 100 számítógép helyezkedhet el. A thicknet viszonylag nehezen fektethető, de a 2500 m-es méretével nagyobb a thinnet-nél.

Thinnet, 10Base2

A thinnet RG58-as típusú koaxiális kábelt használ a számítógépek összekötéséhez. A kábelt állomástól állomásig kell fektetni. A hálózati kártyákon *BNC aljzatra* van szükség, ide csatlakozik a T-elosztóidom. Mindegyik vége a következő számítógéphez vezet. A busz első és utolsó számítógépén 50 ohmos ellenállással kell lezárni a kábelt. Természetesen ezeket az ellenállásokat is T-elosztókhoz és nem a kártya BNC aljzatához csatlakoztatják.

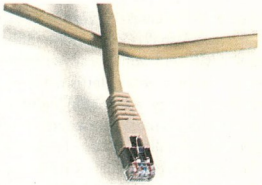
A lezáró ellenállás meggátolja a hullám tükröződését, mivel az megsemmisítené a jelet. A thinnet sebessége 10 Mbit/s alapsávon, egy szegmens maximális hossza 185 méter, a kábel minimális hossza 5 méter. Itt is érvényes az 5-4-3 szabály, ám itt szegmensenként legfeljebb 30 számítógépet lehet csatlakoztatni. Egy thinnet tehát maximálisan 90 számítógépet képes egymással összekötni, és összesen 925 m hosszú lehet (négy ismétlővel).

A thinnet-tel elsősorban otthoni alkalmazásban találkozunk, mivel egy hálózat felépítéséhez ez a legolcsóbb megoldás. A T-elosztók és lezáró ellenállások olcsók, a koaxiális kábel szintúgy, habár az UTP-Cat5 kábelnél drágább, viszont nincs szükség elosztókra. A meghibásodás elleni védelme csekély, mint valamennyi buszos rendszernél. Ha a kábel valahol megszakad, akkor a hálózat lefagy. Nagyobb sebességet és jobb biztonságot eredményez a csavart érpáras kábelezés.

Twisted Pair (csavart érpár)10BaseT

Ma a leggyakrabban a *csavart érpáras kábelt (TP)* fektetik. Ekkor mindegyik állomás egy elosztóhoz (rendszerint hub-hoz) csatlakozik, ami csillag topológiát eredményez. A hub-okat az állomásszám növelésére gyakran Uplink-portokkal vagy keresztezett TP-kábellel kötik össze egymással. A hub-ok egy buszt képeznek, a topológiát összességében *csillagbusznak* nevezik. A régebbi TP-hálózatok UTP-Cat3 kábelt használtak és 10 Mbit/s-mal működtek. A hardver áresésének következtében ma már csak 100 Mbit/s-os UTP-Cat5 kábeles hálózatokat készítenek.

Az árnyékolatlan TP kábelek olcsók és szinte minden esetben megfelelnek. Emellett számos más kábeltípus is létezik, a legismertebbek közé tartozik az *STP (Shielded Twisted Pair)*. Ezt a kábelt, az árnyékolás érdekében méterenként párosával többször megtekerték, sőt egyes típusai árnyékolásként rézfonatot is tartalmaznak. Csatlakozóként *RJ45-ös csatlakozót* használnak, ezeket *Western-csatlakozónak* is nevezik. Ez hasonlít a telefon vagy ISDN csatlakozóhoz, viszont nem szabad összecserélni ezekkel.



A csavart érpár RJ45-ös csatlakozója

A 10BaseT szegmensek legnagyobb hossza 100 méter lehet. Hosszabb szegmenseket ismétlőkkel lehet kialakítani. Két számítógép között a minimális távolság 2,5 méter. Egy 10BaseT hálózat kiegészítő kapcsolati készülékek nélkül összesen 1024 készüléket képes összekötni (a specifikáció alapján).

Egy ideje létezik egy *Gigabájtos Ethernet* is, amit TP Cat5 vagy üvegszálas kábellel üzemeltetnek. A hálózati kártyák és a kapcsolati eszközök azonban még nagyon drágák, így célszerű meggondolni, hogy nem célszerűbb-e egyből FDDI-re vagy ATM-re átállni.

Token Ring

Az IBM féle vezérjeles gyűrűs hálózathoz speciális *Token Ring hálózati kártyákra* van szükség. Ezek ritkák, és jóval drágábbak az Ethernet kártyáknál. A specifikáció az IEEE 802.5, a hozzáférési eljárás

Ethernet szabványok

Tulajdonságok	10Base2	10Base5	10BaseT	100BaseX
Topológia	busz	busz	Busz, csillag-busz	Busz, csillag-busz
Sebesség (Mbit/s)	10	10	10	100
Kábel-típus/ellenállás	Sárga kábel/50 ohm	RG58A/U/50 ohm	UTP 3,5	UTP 5, STP
Csatlakozó	BNC	AUI	RJ45	RJ45
Szegmens hossza (m)	185	500	100	100
Állomások száma szegmensenként	30	100	1024 összesen, kapcsolati készülékek nélkül	1024 összesen, kapcsolati készülékek nélkül
Állomások közötti minimális távolság (m)	0,5	2,5 (MAU-k között)	2,5	2,5
A hálózat teljes hossza	925 m	2500 m	korlátlan	Korlátlan
Hajlítási sugár	5 cm	20 cm	-	

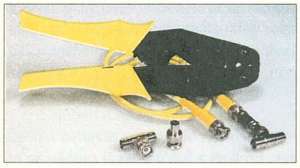
A csavart érpáras kábelek

Megnevezés	Magyarázat
UTP	Unshielded Twisted Pair - árnyékolatlan csavart érpáras Kat3 és Kat5 kábelek, olcsó kábel, a legtöbb alkalmazáshoz elegendő.
STP	Shielded Twisted Pair - árnyékolt csavart érpáros kábel, olyan helyen alkalmazzák, ahol erős elektromágneses zavarokra kell számítani (neonlámpák, gépek).
FTP	Folieshielded Twisted Pair, szintén egy árnyékolt kábel.
SFTP	Screened Folieshielded Twisted Pair. Erősen árnyékolt kábel, gyakran fali aljzatok bekötéséhez használják.

a *token passing*. A fizikai struktúra gyűrűt képez, ami megfelel a vezérjel állomásról állomásra vezető útjának. A gyűrű a hubban helyezkedik el, s a számítógépek gyűrű alakban kapcsolódnak a hub-hoz. Ezért ezt a topológiát *csillag-gyűrű topológiának* is szokás nevezni. A klasszikus Token Ring alapsáv 4 vagy 16 Mbit/s sebességet enged meg. A 100 Mbit/s-os bővítésre a *100VGAnyLAN szolgál (IEEE 802.12)*, ami Ethernet kereteket és Token Ring adatcsomagokat is képes továbbítani. Más elnevezései: *100BaseVG, VG* vagy *AnyLAN*.

Ha egy Token Ring hálózatba bejelentkezik az első számítógép, akkor egy úgynevezett vezérjelet (token) generál. Ez a gyűrűn az egyik irányban állomásról állomásra végigvándorol. A vezérjelet mindegyik állomás veszi, egy újat generál és tovább küldi, vagyis *egyirányú ismétlőként* működik.

Ha valamelyik állomás adni szeretne, fogadja a vezérjelet és egy adatkeretet küld a gyűrűbe. A címzett fogadja az adatkeretet, beállít egy *flag*-et, amellyel a sikeres átvitelt jelzi, és ismét kiadja a gyűrűbe az adatkeretet. Végül is az adatkeretet a feladó távolítja el a gyűrűből és egy



A koaxiális kábeleket t-idomokon keresztül kötik össze a hálózati kártyával. A busz mindkét végét 50 ohmos ellenállással kell lezárni

új vezérjelet küld ki helyette. Csak az adhat, aki a vezérjelet birtokolja. Ezzel elkerülhetők az ütközések és a hálózat terhelhetősége is növekszik. A Token Ring hálózat általánosan 75%-os terhelésnél fagy le, míg az Ethernet már 50%-nál.

A Token Ring hardver jóval drágább, mint az Ethernet hardver. Speciális hubokra (Multi Station Access Unit, MAU) és speciális kábelekre (IBM 1, 2, 3 típus) van hozzá szükség.

FDDI

Az *FDDI (Fiber Distributed Data Interface)* specifikáció egy 100 Mbit/s-os üvegszálas kábelű Token Ring hálózatot ismertet. Az FDDI hálózatok kettős gyűrűből (Dual RIng) épülnek fel (redundancia), gyűrűnként legfeljebb 500 számítógépet tartalmaznak és maximális kiterjedésük gyűrűnként 100 kilométer. Minden második kilométernél egy ismétlőt kell elhelyezni.

Az adatfolyamok ellenkező irányban áramlanak a gyűrűkben. Az egyik gyűrű a *primer*, a másik a *szekunder*. Az adatforgalomhoz alapvetően a primer gyűrűt használják. Ha ez meghibásodna, akkor az FDDI hálózat automatikusan átkonfigurálja magát, és a szekunder gyűrűt kezdi használni.

Az állomások vagy mindkét gyűrűhöz csatlakoznak (A-osztályú állomások), vagy csak az egyikhez (B-osztályú állomások).

A logikai FDDI gyűrű fizikailag csillag alakban készül. Az FDDI állomások és egy hub között pont-pont kapcsolat áll fen.

A hibafelismerés és ezt követő javítás az úgynevezett *Beaconing eljárás* feladata. Ha valamelyik számítógép hibát fedez fel, akkor egy speciális keretet küld ki a gyűrűbe: ez a *Beacon*. Mindaddig küldi ezt a Beacon-t, amíg a közvetlenül felette lévő számítógéptől nem kap egy Beacon-t. Ez a folyamat mindaddig folytatódik, amíg már csak az a számítógép küld Beacon-t, amelyik közvetlenül a zavar alatt helyezkedik el. Ezzel a hibát behatárolták, és újrakonfigurálják a gyűrűt.

Az FDDI-t üvegszálas kábelekkel valósítják meg, így érzéketlen az elektromágneses zavarok iránt, és le sem lehet hallgatni.

ATM

Az *ATM (Asynchronous Transfer Mode)* egy nagy sávszélességű switching technológia. Akárcsak az FDDI, a fizikai réteg szolgáltatására települhet, és maga veszi át a kapcsolati és hálózati réteg funkcióit. Az ATM-mel üvegszálas közeg esetében maximálisan 622 Mbit/s sebesség érhető el, s 155 Mbit a jellemző. Az elmélet határ 1,2 Gbit.

Az ATM számára rendszerint üvegszálas kábelt fektetnek, habár csavart érpár, sőt koaxiális kábel is lehetséges lenne. Az ATM konstans méretű cellákkal éri el az óriási sebességét. Mindegyik cella 53 bájtos, 5 bájtos header-rel valamint 48 hasznos bájttal. Így az adatok routolása és pufferelése nagyon hatékony.

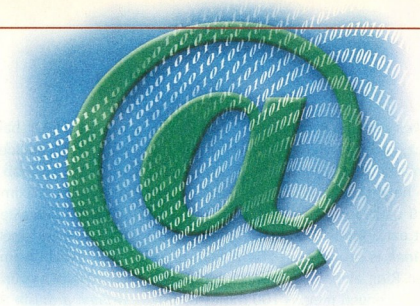
Az ATM *szélessávú technika*, szemben valamennyi eddig ismertetettel, amelyek alapsávúak voltak. A szélessávú technikánál az analóg jeleket több csatornára bontva viszik fel a kábelre, így zene, videó és adat egyszerre kerülhet átvitelre. Ezzel ellentétben az alapsávban a digitális jelek egyetlen egy csatornában futnak (pl. az Ethernet-nél vagy a Token Ring-nél).

Az ATM további jellemzője az *aszinkron átvitel*. Az adatátvitel nem időablakok, hanem prioritások segítségével szabályozódik. Így az időkritikus adatfolyamokat, mint például a zenei adatokat, előnyben lehet részesíteni a kevésbé kritikus adatfolyamokkal szemben. A csatornák a prioritás meghatározásához úgynevezett *cella címkéket (Cell-Labels)* kapnak.

Az ATM számára teljesen új hálózatot kell felépíteni, a meglévő komponenseket rendszerint nem lehet felhasználni. A magas ár (a tapasztalat híján) bizonyos megbízhatatlansággal párosulva, még ma is kalandot csinál az ATM-ből a PC-s világban.

A professzionális területen az adatkommunikáció és a telefontechnika egyre jobban összeforr. Az ehhez szükséges funkcionalitást többnyire az ATM technológiával valósítják meg.

A TCP/IP – részletesen



Aki tudni szeretné, hogy mire jó az IP-cím vagy az alhálózati maszk (subnet maszk), vagy hogy hogyan jutnak az adatok a hálón az adótól a vevőhöz, az szemrevételezi a TCP/IP protokollt. Itt határozzák meg ugyanis, hogyan haladjanak az adatok végig a hálózaton.

A TCP/IP protokoll alapját a *nyilvános RFC-k (Request for Comments)* képezik. Ezek olyan dokumentumok, amelyek részben az internetes szabványokat határozzák meg, részben pedig javaslatokat vagy kiegészítéseket tartalmaznak. Egyesek az idő múlásával fölöslegessé is válnak, vagy újakkal helyettesítődnek.

Minden a TCP/IP-vel kapcsolatos gond esetében először azt kell tudni, hogy *mi is egy IP-cím és hogyan működik.*

Az IP-címek

A hálózatban minden egyes készüléket a címével lehet azonosítani. A TCP/IP-s hálózatokban ez a cím az *IP-cím.* Ennek egyértelműnek kell lennie, és bizonyos szabályok szerint kell felépülnie. Például: 192.168.0.1

Valamennyi IP-cím négy decimális számból épül fel, amit *oktettnek* is neveznek, és az értéke 0 és 255 között változhat. Az egyes számhármasokat ponttal kell elválasztani egymástól.

Az IP-címek két részből épülnek fel: az első a *hálózati azonosító,* amit a *host-azonosító* követ.

A hálózati azonosító meghatározza a hostot tartalmazó alhálót, míg a host-azonosító a számítógépnek ebben az alhálózatban kiadott száma. Ez a struktúra kiválóan megfelel az internet leképezésére. Az internetet tekinthetjük sok, eltérő méretű hálózat egymással összekapcsolt gyűjteményének. Egy adott számítógép címzéséhez tehát meg kell nevezni a hálózatot, valamint az ezen hálózaton belüli helyet. Ezt az *IPv4 (Internet Protokoll Version 4)* végzi, de már fut az utód, az *IPv6* párhuzamos próbaüzeme.

Az IP-címeket voltaképpen binárisan kell értelmezni ahhoz, hogy értelmük legyen, a decimális írásmódot csupán egyszerűbben lehet olvasni és írni (lásd a bináris rendszerrel foglalkozó keretes írásunkat).

Az IP-osztályok

Attól függően, hogy hány bit kerül a hálózati és a host részhez, létezik több hálózat kevesebb hosttal vagy több host kevesebb hálózatban. A hálózatok nagy és kis hálózatokra való felosztására az *osztályok* szolgálnak. Eredetileg öt osztályt definiáltak, amelyek közül azonban csak négyet használnak a Microsoft-világban. Az ötödik osztályt (E) a *Multicasting* részére (IP-rádió és IP-videó) foglalták le, ezek azonban csak lassan terjednek.

A legnagyobbak az *A-osztályú hálózatok.* Ezeknél a hálózatoknál csupán az első bájt (balról nézve) a hálózati azonosító. Ennek az első bitje mindig nulla, így összesen 2^7=128 hálózat címezhető.

A hálózati és host azonosítók esetében két szélső esetet kell figyelembe venni. Mindkét azonosítóra jellemző, hogy nem lehet az összes bit egyszerre 1, illetve 0. A host-ID két szélső esetére a következő vonatkozik: Ha az ID nulla, akkor marad a hálózatszám. Ez az eset a routolás szempontjából nagyon fontos. Ha a host-ID összes bitje egyes, akkor az úgynevezett *multicast cím* keletkezik, amellyel a részháló valamennyi hostját el lehet érni. A hálózati azonosítóra a következők vonatkoznak: Az ID 0-t nem használják. Az ID 127 az úgynevezett *loopback cím,* amelyet csak tesztelési célból használnak. Így például a *ping 127.0.0.1* paranccsal a saját TCP/IP stack korrekt működését ellenőrizhetjük.

Számolás bináris számokkal

A bináris számokkal végzett műveleteknél két művelet a fontos: az ÉS és a VAGY kapcsolat. Az ÉS kapcsolatnál két operandust (bináris számot) bitenként összehasonlítanak. Az eredmény csak akkor 1, ha mindkét bit 1 volt. Ha csak az egyik is nulla vagy ha mindkettő nulla, akkor az eredmény is nulla. Ez a következőképpen néz ki:

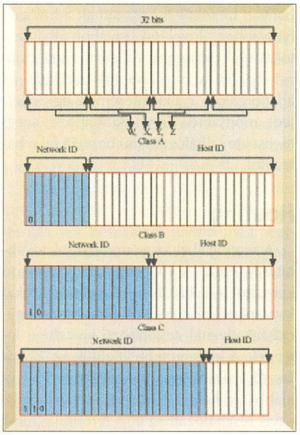
```
1101 1010
1011 1110
1001 1010
```

Az ÉS kapcsolatot arra használják, hogy egy értékből egyes pozíciókat töröljenek. Az a pozíció, amelyet 0-val hozunk ÉS kapcsolatban mindig nullát eredményez.

A második fontos művelet a VAGY kapcsolat. Ez a kapcsolat a következőképpen néz ki:

```
1101 1010
1011 1110
1111 1110
```

Az eredmény csak akkor nulla, ha mindkét operandus nulla, különben mindig 1. A VAGY kapcsolattal egyes pozíciókat 1-re lehet állítani. Ha 1-gyel „VAGY-olunk", akkor az eredmény is mindig 1 lesz, függetlenül attól, hogy a kiindulási operandus 0-t vagy 1-et tartalmazott.



Az IP-címek egy hálózati és egy host hánnyadból épülnek fel. Az IP-osztályok meghatározzák a hálózat méretét és a hostok alhálónkénti számát

Ha a két speciális esettől eltekintünk, akkor világszerte 126 A-osztályú hálózatot kapunk. A host-hányadot a három maradék bájt írja le. Így 2^{24}-2=16777214 hostot lehet megcímezni. Az A-osztályú hálózatok tehát több mint 16 millió számítógépet tartalmazhatnak.

IP-osztályok

Osztály	Hálózatok száma	Hostok száma	Kezdőcím	Befejezőcím
A	126	16777214	1	126
B	16384	65534	128	191
C	2097152	254	192	223
D	-	-	224	-
E	-	-	240	

A B-osztályú hálózatoknál a hálózati hányad két bájtból áll, ahol is az első két bit mindig 1 és 0. Így 16384 hálózatot lehet egyenként 65534 számítógéppel megcímezni. A C-osztályú hálózatoknál a hálózati azonosító 11-el kezdődik. Itt 2097152 hálózatban egyenként 254 host kaphat helyet.

A D-osztályú hálózatokat az úgynevezett multicasting-hoz használják. A hálózati hányadot az első bájt reprezentálja, amelyben az első három bit 1-esre van állítva. A multicast-címek mindig 224-gyel kezdődnek. A multicasting-et az Internet Broadcast alkalmazásaira használják, például az internet-rádióhoz vagy videókhoz, nagyobb számú felhasználóhoz történő továbbítás céljára. Az E-osztályú hálózatok kísérleti célra szolgálnak. Ezeknél az első négy bit lett 1-esre állítva.

Azt tehát, hogy egy IP melyik osztályba tartozik, könnyű felismerni az első számhármasáról. Az IP-osztályok táblázatában az utolsó és az utolsó előtti oszlopok az adott osztály legnagyobb, illetve legkisebb címét tartalmazzák.

A hálózati azonosító első bájtja

Osztály	Kezdet (bináris)	Befejezés (bináris)	Kezdet (decimális)	Befejezés (decimális)
A	0000 0001	1000 0000	1	127
B	1000 0000	1011 1111	128	191
C	1100 0000	1101 1111	192	223
D	1110 0000	1110 1111	224	239
E	1111 0000	1111 1111	240	255

Privát IP-címtartományok

Ha egy LAN nem csatlakozik az internethez, akkor mindegy, hogy melyik IP-osztályt használja. Attól függően, hogy miként valósítják meg az internetes csatlakozást, az alkalmazandó osztályra vonatkozó konzekvenciák adódnak. Ha a hostokat közvetlenül látni kell tudni az internetről, akkor az IP-cím kontingenst egy szolgáltatónál kell megvásárolni. Ezzel az IP-cím problémáját megoldottuk.

Privát IP-címtartományok

Osztály	Kezdőcím	Befejezőcím	Hálózatok száma
A	10.0.0.0	10.255.255.255	1
B	172.16.0.0	172.31.255.255	16
C	192.168.0.0	192.168.255.255	255

Ha *NAT-tal (Network Address Translation)* címzünk, akkor a LAN-ban úgynevezett *privát címtartományokat* kell alkalmazni. Ezek a címek nem továbbítódnak az internet felé. Mindegyik osztály rendelkezik privát címtartománnyal. Hogy végül is melyiket választják, az végső soron az alkalmazásra kerülő szoftvertől függ.

Alhálózati maszkok

Az IP-címkonfigurációhoz egy úgynevezett *alhálózati maszk (subnet maszk)* megadása is hozzátartozik. Ez azt a részhálózatot határozza meg, amelyben a host található. A subnet maszkban azok a bitek 1-esek, amelyek a hálózati hányadot határozzák meg, így például egy B-osztályú hálózatban a hálózati hányad az

Fragmentálás

Az adatcsomagok a különböző hálózatokban eltérő méretűek. A maximális csomagméretet minden hálózatban az úgynevezett *MTU (Maximum Transmission Unit)* határozza meg. Egy kisebb csomagméretű hálózatba való átmenetnél a router feldarabolja a csomagokat, de eközben figyelembe veszi az IP-header információit. A csomagdarabok ezután eltérő úton érkezhetnek célba. Ott az IP ismét a helyes sorrendbe állítja őket.

A DHCP

A TCP/IP kliens kézi konfigurálása nehézkes, és magában rejti a hibázás lehetőségét. Az automatizálás útja egyszerű: az (RFC-konformis) DHCP szolgáltatás (Dynamic Host Configuration Protocol). A DHCP-szerver NT-szerveren fut (létezik a Windows 9x alá is), és automatikusan hozzárendeli az IP-adatokat az új kliensekhez. Ez az eljárás négy lépésben zajlik:

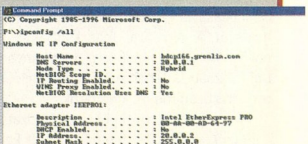
A kliens kiküld egy „Ki itt a DHCP-szever?" tartalmú Broadcast-ot.

Valamennyi rendelkezésre álló DHCP-szerver felkínálja a szolgáltatását.

A kliens kikeres magának egyet (a legközelebbit), és kér egy adatrekordot.

Az érintett DHCP-szerver visszaküld egy vételnyugtázást, és ezzel mindenekelőtt a többi DHCP-szerver felé is jelzi, hogy sikerrel regisztrálta a klienst.

Az IP-cím DHCP-s kiadását *Lease*-nek nevezik, a kliens tehát egy adott időre „kikölcsönöz" magának egy címet. Ezt adott időközök között megújítják. Azt, hogy mely IP-adatokat kaptuk, a Windows 9x alatt a *winipcfg.exe* utility közli, míg az NT alatt az *ipconfig*, amely */all* paraméterrel a kibővített paramétereket is megadja.



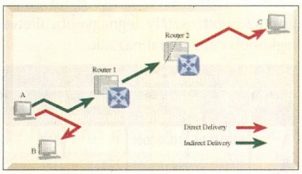
A bővített IP-konfigurációs adatok az NT alatt az „ipconfig/all" paranccsal válnak láthatókká

első két bájtból áll, az alhálózati maszk: 255.255.0.0

Alhálózati maszkok

Cím-osztály	Bináris alhálózati maszk	Decimális alhálózati maszk
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

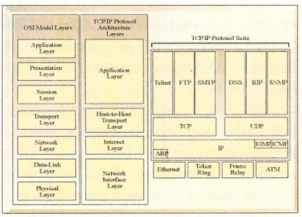
Az alhálózati maszkkal kivonatolják egy IP-címből a hálózati hányadot. Amennyiben az alhálózati maszkot az IP-címmel logikai ÉS kapcsolatba hozzák (lásd a bináris számrendszerrel foglalkozó keretes írásunkat), akkor a végeredmény az, hogy az összes olyan bit törlődik, amelynél az alhálózati maszk nullát tartalmazott. Egy útkiválasztó (router) ezzel az információval határozza meg, hogy melyik alhálózatba kell következőként elküldeni egy adatcsomagot. Az alhálózati maszkok elnevezésű táblázat a különböző IP-osztályok alhálózati maszkjait tartalmazza. Léteznek „csonka" alhálózati maszkok is, amelyeknél az oktettnek nem az összes bitje egyes: pl. 255.255.225.248, ami egy alhálózatos C-osztályú hálózat maszkja. Ennél a host hányad bitjeiből is használnak a hálózati hányadhoz, hogy így további alhálózatokat képezhessenek. Az eljárás neve *subnetting*, és a nagyobb hálózatoknál az adatforgalom csökkentésérnek egy elterjedt módszere. Ennél különböző szegmensekre (alhálózatokra) bontják fel a hálózatot.



A közvetett és a közvetlen továbbítás: ha a feladó és a címzett között egy kapcsolati készülék található, akkor a kézbesítés közvetett

Routing

A *routing* alatt az adatcsomagok továbbítását értik, különböző alhálózatokon keresztül a célhálózatig. Az alhálózatokat kapcsolati készülékek kötik össze egymással. Ilyenek különböző kivitelben léteznek. A legismertebb közülük az *útkiválasztó (router)*. Egy routernek mindig legalább két hálózati interfésze van, mindegyik részhálózathoz egy. A routolás lehet közvetett és közvetlen, ezek magyarázata egyszerű. A *közvetlen routolásnál* közvetlenül is lehet kézbesíteni a csomagokat, mivel a feladó és a címzett ugyanabban a szegmensben (alháló) helyezkedik el. Amint azonban egy kapcsoalti készülék is van kettőjük között, közvetett routolásról van szó. A célhálózat meghatározásához az útkiválasztó megvizsgálja a cél IP-címet és az alhálózati maszkot, amelyeket mindegyik IP-csomag tartalmaz. Meghatározza VAGY eljárással a hálózati azonosítót, és azt összeveti a helyi hálózattal, ahonnan a csomag érkezett. Amennyiben a kettő megegyezik, akkor az adatcsomagot lokálisan lehet kézbesíteni, ellenkező esetben az útkiválasztónak további információk kellenek a célhálózatról, például egy másik útkiválasztó, amelynek az adatcsomagot továbbíthatja. Ezeket az információkat a routing táblázat tartalmazza, amellyel minden IP-készülék rendelkezik. A Windows NT routing táblázatát a *route print* paranccsal lehet megjeleníteni. Minden sor egy útvonal és öt oszlopot



A TCP/IP modell az OSI modellen alapszik. A protokollok bizonyos rétegekhez vannak rendelve

Subnetting

A nagy hálózatoknál, mint amilyenek az A- vagy B-osztályú hálózatok, felmerül a *broadcasting* problémája. A broadcastok a hálózat körözött hírei, olyanok, amelyek valamennyi számítógépet érintenek. A körözött üzenetet mindegyik számítógépnek meg kell vizsgálnia, és reagálnia kell rájuk. Jellemző broadcast, amikor egy gép megpróbál egy másikat megkeresni. Ilyenkor a hálózat mindegyik számítógépéhez kiküld egy adatcsomagot. A csomagot mindegyik számítógépnek meg kell vizsgálnia, hogy megállapíthassa, hogy neki lett-e szánva. Ezzel gépidő pazarlódik el és a hálózatot is terheli. A probléma ténylegesen nagygyá válhat, ha „broadcast-viharok" keletkeznek, mert ezek lefagyaszthatják a hálózatot. A megoldás a *subnetting*. Ehhez egy alhálót (subnet) az alhálózati maszk definiálásával kisebb hálózatokra bontanak szét. Az alhálózati maszk kialakításánál a hálózati hányadhoz a host-hányadból használnak fel biteket – így egy illesztett alhálózati maszk keletkezik.

Ha mondjuk tizenkét részhálózatra van szükség, akkor ehhez négy bit kell. Egy B-osztályú hálózathoz a subnetmaszk tehát így néz ki:

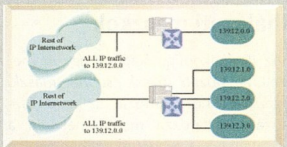
11111111 11111111
11110000 00000000

vagy decimális alakban:

255 255 240 0

Négy bittel 16 állapotot lehet ábrázolni, így 16 részhálózatot lehet leírni. Miként az IP-cím host- és hálózati-hányadánál, úgy itt is le kell vonni két kombinációt (valamennyi bit nulla és valamennyi bit egy). Így a 4 bittel 14 részhálózatot lehet ábrázolni. Ebben a példában a host-hányadnak tizenkét bit marad. Így részhálózatonként 2^{12}-2=4094 hoszt adódik. A két szélső esetet itt is le kell vonni.

Az *Illesztett alhálózati maszk* táblázat valamennyi érvényes, illesztett alhálózati maszkot tartalmaz. A részhálózatok azonosítóit úgy lehet kiszámítani, hogy a járulékos biteket végigvesszük a nullától a maximális értékig. Egy pl. három bites részhálózati azonosítóra egy B-osztályú hálózat esetében az alábbi azonosítók adódnak:



A subnettingnél a host-hányad néhány bitjének a segítségével több kisebb hálóra lehet felosztani egy hálózatot

tartalmaz. Az első oszlopban a cél IP-címe áll, amelyet a subnet maszk követ. Ezt követi az átjáró (Gateway), az interfész és a metrika. A gateway fogadja az adatcsomagot és ezt vagy közvetlenül kézbesíti, vagy egy további útkiválasztóhoz továbbítja. Interfész alatt a hálózati interfészt értik. A hálózati kártyákon kívül ez lehet modem, vagy ISDN, vagy DSL kártya is. Ebben a példában a *route print* utasítás két készüléket jelenít meg: egy hálózati kártyát és egy NdisWAN-adaptert, ami alatt egy modemet értenek. Ez a számítógép egy modemen keresztül kapcsol össze egy LAN-t az internettel, és így *szoftveres útkiválasztóként* működik. A *metrika* megadja az átjárók (gateway-k) számát a célig. A leképezett utak a standard utak, ezek minden rendszeren hasonlóképpen néznek ki.

Az első 0.0.0.0-s út a standard út, amelyet olyankor használnak, amikor különben nem lehet kézbesíteni a csomagokat. A második útvonal a *loopback útvonal*. Ezt akkor használják, amikor a PC saját magának küld csomagokat (tesztelés céljából). A 192.168.0.x LAN-IP-k a 192.168.0.1 átjáróhoz kerülnek, a 217.2.59.x remote-hálózat szintén. Feltűnő a LAN kettes számú metrikája. A LAN PC-k adatcsomagjainak először a gateway-re, majd a remote gateway-re kell kerülniük, ahol talán kézbesíthetők, vagyis legalább két ugrás keletkezik. Valamennyi Windows verzió TCP/IP beállításában meg lehet egy ún. *standard gateway-t* adni. Ez azokat az adatcsomagokat kapja meg, amelyeket másként nem lehet kézbesíteni. Vagy rendelkezik egy útvonallal, vagy megsemmisíti az adatcsomagokat. A Windows 2000 alatt több standard gateway lehetséges, amelyekhez a metrikát is megadják, így meg lehet találni a legelőnyösebb útvonalat.

A nagy hálózatokban a routing táblázatot kézzel (statikus routolás) már nem lehet kezelni, ezért hozták létre a *routingprotokollokat*, amelyek automatikusan átalakítják a routing táblázatokat. Automatikusan felismerik az átjárókat, és konfigurálják a klienseket. A Windows 2000 támogatja a *RIP-routingot* (Routing Information Protocol). Ez egy olyan komponens, amelyet a *Vezérlőpult/Szoftver* menüvel lehet telepíteni. A RIP-routerek RIP-pel küldik az útvonal információkat a hálózathoz. A *Windows 2000 Professional* fogadja ezeket az üzeneteket, és beilleszti a saját routing táblázatába. A hardveres routerek még összetettebb protokollokat használnak az útvonalkeresés hatékonyabbá tételéhez. A routolásért az IP (Internet Protocol) a felelős, ez a TCP/IP protokollhalmaz úgynevezett *Internet* rétegében helyezkedik el.

Az IP-Header felépítése

Mező	Szélesség bitekben	Leírás
Version	4	Az IP protokoll verziószáma: Version 4.
IHL	4	Az Internet Header Length 32 bites szavakat tartalmaz a header-ben. A minimális mérete öt szó.
Type of Service	8	A szolgáltatás típusát pontosabban írja le. A 0-2 bit a prioritást adja meg. Az alábbi kombinációk lehetségesek: 111: Network Control, 110: Internetwork Control, 101: CRITIC/ECP, 100:Flash Override, 011: Flash, 010: Immediate, 001: Priority. 000: Routine. A 3-as bit a késleltetést adja meg: 0=szokványos (alapértelmezés), 1=sürgős. A 4. bit a sebességet adja meg, 0= szokványos, 1= gyors. A 6. és 7. bit foglalt.
Total length	16	A datagram teljes hossza bájtokban (max. 64 kbájt).
Identification	16	Ez és a két következő mező a fragmentálást szabályozza. Az Identification egy olyan szám, amely az adatszeletet egyértelműen egy datagramhoz rendeli, így nem lehet összetéveszteni más datagramok szeleteivel.
Flags	3	A nullás bit foglalt, az értékének 0-nak kell lennie. Az 1-es bit a DF-bit (Don't fragment) Ha 0, akkor szabad fragmentálni, ha 1, akkor nem. A 2-es bit az MF-bit (More Fragments). Az utolsó adatszelet esetében ez a bit 0. Ezt a bitet egy IP-datagram mindegyik szeletében 1-re állítják (kivéve az utolsóban).
Fragment Offset	13	A datagram azon bájtjainak a száma, amelyeket már más szeletekbe helyeztek. Az első szelet offszetje 0. Ezután az ofszet megnövelődik a már átvitt adatokkal (bájtokkal).
TTL	8	A Time To Live 0 és 255 közötti értékeket vesz fel. Minden hop-nál eggyel csökken. A TTL=0 esetében a datagram megsemmisül.
Protocol	8	Azt a protokollt definiálja, amelyet a datagram az IP-nek átadott. Így pl. az ICMP esetében ebben a mezőben egy 1-es áll, vagy a TCP esetében egy 6-os. Az RFC 790 további protokollszámokat definiál.
Header Check sum	16	A header ellenőrző összege. Ezt az ellenőrzőösszeget a header minden változtatásánál újból számolják.
Source Address	32	Forráscím
Destination Address	32	A cél címe

Az UDP

Az UDP *(User Datagram Protocol)* egy egyszerű *transzport protokoll*. Ez egy kapcsolatmentes protokoll, amely nem igényel adatfolyam-ellenőrzést. Ilyen például az IP-rádió és IP-videó is. Az UDP-header tartalmazza a forrás és cél-IP-t, a datagram hosszát bájtokban, valamint egy ellenőrzőösszeget. A TCP-hez hasonlóan, itt is portszámokkal létesül a kapcsolat.

A bináris számok

A 192-es decimális szám jelentése: végy 1x100-at, adj hozzá 9x10-et és 2x1-et. A 100, 10 vagy 1 pozíciókat megszorozzák a pozícióban álló számmal, és az értékeket összeadják. A számolásnak ezt a módját *tízes számrendszer* néven ismerjük. A kettes (bináris) számrendszerben az elv ugyanez, csupán a pozícióértékek mások: 128 64 32 168 4 2 1, és számként csak kettő van megengedve, az 1 és a 0. A 4-es értékű pozícióban például vagy áll szám (1), vagy nem áll. Ezzel szemben a tízes számrendszerben még azt is meg lehet adni, hogy hányszor álljon (0-9-szer). A bináris számokat jobbról balra olvassuk (és írjuk). A 13-as szám (tízes számrendszerben) a kettes számrendszerben 1101 alakot ölti fel, mert 8+4+0+1=13.

Rétegmodellek

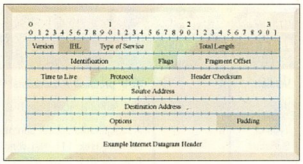
A hálózati architektúrák az OSI *(Open Systems Interconnection)* modellre támaszkodnak. Ez hét réteget definiál, amelyeken az adatcsomagok végighaladnak. A legfelső az *alkalmazási réteg*, amely a programoktól, például a böngészőtől kapja az adatait. Az adatcsomagok innen valamennyi rétegen végighaladnak egészen a legalsóig, a *fizikai rétegig*. Itt elektromos jelekké alakulnak át és kikerülnek a kábelre. A csomagok a célban a fordított úton haladnak végig lentről felfelé, amíg

az adott alkalmazáshoz nem kerülnek. A rétegeken keresztül a kábelig vezető út során a csomagok protokolltól protokollig kerülnek. Minden egyes protokoll fejléc (header) formájában *specifikus információkat* tesz a csomaghoz (ezek adott adatstruktúrák). A csomag a célban ismét protokolltól protokollig vándorol felfelé. Mindegyik protokoll kiértékeli a headereket, majd eltávolítja azokat.

A TCP/IP modell az OSI modellen alapszik, de megelégszik négy réteggel. Az alsó réteg a *hálózati réteg*. Ez protokollfüggetlen, és a különböző hálózattípusok (mint pl. Ethernet, Token Ring, vagy ATM) használatát is garantálja, anélkül, hogy ezzel egy protokollnak vagy egy alkalmazásnak törődnie kellene. Ha megérkezik egy csomag a felette lévő rétegből, akkor kap egy header-t és egy ellenőrző összeget és a cél felé küldik. Ott eltávolítják a header-t, és új ellenőrzőösszeget képeznek. Ha ez megegyezik a csomagban lévővel, akkor kiértékelik a hardvercímet. Ezt a header tartalmazza és hat bájtból áll. Ha a csomag hardvercíme megegyezik a hostéval (amely éppen vizsgálja) a csomagot, akkor a csomag a magasabb rétegek felé továbbítódik, különben eldobják. Ha az ellenőrzőösszeg hibás, akkor szintén eldobják a csomagot. A hálózati réteg az *Internet* rétegből kapja az adatait.

Az Internet réteg

Az *Internet rétegben* zajlik a már említett IP-s útvonalkeresés. Az IP nem garantálja a csomagok hibátlan továbbítását, el is elveszhet csomag, meghibásodhat vagy összekeveredhet a csomagok sorrendje is. Ez egy úgynevezett *állapotmentes protokoll*, mivel nem kell viszonyt kialakítani a célhosttal, mint ahogy ez a TCP-nél szükséges. Ha egy csomag a szállítási rétegből az Internet rétegbe kerül, akkor az IP-protokolltól egy újabb header-t kap, amely tartalmazza többek között a forrás és cél IP-t, a felhasznált transzport protokollt (TCP vagy UDP), egy ellenőrző összeget, valamint a TTL-t (Time To Live). A TTL megadja, hogy mikor lehet megsemmisíteni az adatcsomagot ahhoz, hogy ne bolyongjon a végtelenségig a kábelen. Az egység itt a „hop" (ugrás) és nem a másodperc. Minden olyan router, amelyen átmegy, egy hop-ot jelent (ezt amúgy a tracert-tel lehet megnézni). A standard érték a 128 hop.



Az IP-header a forrás- és a cél-IP-címet, valamint további, az IP-datagrammal kapcsolatos információkat is tartalmaz

Ha a célcím a forráscímmel azonos alhálózatban található, akkor az IP közvetlenül kézbesíti a csomagokat. Ellenkező esetben a routing táblázatból keres egy utat a célhálózatba. Ha nem talál, akkor a csomagot egyszerűen az alapértelmezett gateway-hez továbbítja. Ez útvonalkeresőként működik, és neki kell routolnia a csomagot. Ha az alapértelmezett gateway sem talál útvonalat, akkor megsemmisíti a csomagot. Ez a gateway csökkenti le egygyel például a TTL-t is (a csomagot TTL=0 esetén megsemmisítik) A csomagok így kerülnek routerről routerre egészen a cél hostig.

Fontos RFC-k	
Leírás	RFC
ARP, Address Resolution Protocol	903
Ethernet	894
FTP, File Transfer Protocol	959
ICMP, Internet Control Message Protocol	792
IGMP, Internet Group Management Protocol	1112
IP, Internet Protocol	791
SMTP, Simple Mail Transfer Protocol	821,822
SNMP, Single Netwprk Management Protocol	1098, 1157, 1212
TCP, Transmission Control protocol	793
TELNET	854
TFTP, Trivial File Transfer Protocol	1350
UDP, User Datagram Protocol	768

Részhálózati azonosítók		
Részhálózati azonosító (bináris)	Decimális	Hálózati maszk
000 00000	0	Érvénytelen
001 00000	32	x.y.32.0
010 00000	64	x.y.64.0
011 00000	96	x.y.96.0
100 00000	128	x.y.128.0
101 00000	160	x.y.160.0
110 00000	192	x.y.192.0
111 00000	224	Érvénytelen

A host keresése

Az Internet rétegben helyezkedik el az *ARP (Address Resolution Protocol)*. Erre az IP-nek van van szüksége ahhoz, hogy a célszámítógéphez tudja továbbítani az adatcsomagokat. Ha egy adatcsomag megérkezett a célhálózatba, akkor ezt még a megfelelő számítógéphez kell továbbítani. Ehhez azonban nem az IP címet, hanem a MAC címet használják, amely minden hálózati berendezést világszerte egyértelműen jelöl. A MAC cím hat bájtból áll. Az első két bájt a gyártót definiálja, a többi négy a készüléket. Ezzel 2^{32} vagy kb. 4 milliárd készüléket lehet egymástól megkülönböztetni. A MAC címet az NT/2000 esetében az *ipconfig / all*, vagy a 9x/ME-nél a *winipcfg* paranccsal lehet megjeleníteni.

Az ARP egy *broadcasting* (körhívás) elnevezésű eljárással hozza létre az IP-címekből a MAC címeket. Egy broadcast csak egy alhálózatban hat (broadcast domain), mert ezeket az útvonalkeresők eleve nem továbbítják. Amikor az ARP-nek egy MAC címet kell az IP felé képeznie, először megnézi a saját cache-ében,

ICMP-üzenetek		
Típus	Üzenet	Leírás
0	Echo Reply	Válaszadás egy ping-re
3	Destination Unreachable	A célszámítógép elérhetetlen.
4	Source Quench	A datagram méret túl nagy. Az adó host kisebb csomagokat kér.
5	Redirect	Az útkiválasztó azt jelzi a küldő hostnak, hogy ismer egy jobb útkiválasztót, és a hostnak ezt kellene használnia.
8	Echo Request	Egy ping kiküldése.
11	Time Exceeded	A TTL lejárt.
12	Parameter Problem	Hibás paraméter a header-ben.
13	Timestamp	Időbélyegzők cseréje két host között.
14	Timestamp Reply	Időbélyegzők cseréje két host között.
15	Information Request	A hálózatszám lekérdezése.
16	Information Reply	A hálózatszám lekérdezése.

Illesztett alhálózati maszkok		
Bitek száma	Bináris oktett	Decimális
1	érvénytelen	Érvénytelen
2	11000000	192
3	11100000	2224
4	11110000	240
5	11111000	248
6	11111100	252
7	11111110	254
8	11111111	255

hogy ezt az IP-t az elmúlt időszakban nem bontotta-e már ki. Ha igen, akkor a csomag azonnal kézbesíthető. Ha nem, akkor egy ARP csomagot küld ki az alhálózatba. A hálózat valamennyi hostja köteles megvizsgálni, hogy tartalmazza-e ez az IP-jét. Ezután a cél host jelzi a MAC címét a feladónak, amely eltárolja ezt a cache-ében, és ezután közvetlenül kézbesíti a csomagot. Ha nem találnak hostot, akkor a csomag kézbesíthetetlen és megsemmisül. Az ICMP (Internet Control Message Protocol), valamint az IGMP (Internet Group Management Protocol) szintén az Internet rétegben helyezkedik el. Az ICMP-t a hibaüzenetek cseréjére használják, ez az IP egyetlen lehetősége, hogy egy esetleges hibáról értesíthesse a host-ot.

Az egyik ismert ICMP alkalmazás a *ping* parancs. Ha a pingelés során hiba lépne fel, akkor visszakerül az ICMP-üzenet, például „a host nem elérhető" kommentárral. Valamennyi ICMP üzenetet az *ICMP-üzenetek* című táblázat tartalmazza. Az ICMP egy host-csoport felé továbbítja az adatokat, ilyen a streaming-alkalmazásoknál az IP-rádió vagy -videó. Sok számítógép tehát ugyanazokat az adatokat fogadja (multicasting), ha egy adott címre figyel, ez a *multicast-cím*. Ez egy D-osztályú cím és host-címként érvénytelen.

A TCP

A *TCP* az a *szállítási protokoll*, amellyel két host között kicserélődnek az adatok. Az adatokat a TCP-zsargonban *szegmenseknek* nevezik. A TCP nagy biztonságot garantál, mert a küldött adatokat a vevőnek nyugtáznia kell. Ha ez a nyugtázás hiányzik, akkor egy beállítható időtartam *(Retransmit Timer)* elteltével a szegmens ismét adásra kerül. A *Windows Registry-ben* be lehet állítani, hogy milyen gyakran kell újraküldeni egy szegmenst mindaddig, amíg kézbesíthetetlennek nem minősül és megsemmisíthetővé válik, illetve erről egy hibaüzenet is készül. A TCP egy *viszonyorientált protokoll*. Mielőtt adatokat lehetne cserélni, három lépésben fel kell építeni egy viszonyt, méghozzá a TCP-handshake-kel.

A TCP handshake

Egy kapcsolat iniciálásához a kliens egy 1-re állított SYN-bites TCP szegmenst küld a szervernek. Egy webszerver esetében pl. a 80-as portra küldenek. A saját portszám lényegtelen, mindaddig, amíg 1023-nál nagyobb, és még nem foglalták le másra. A kliens beállítja az *Initial Sequence Number-t* (ISN) és az ablakméretét. Az ISN az a szám, amelytől kezdve az átvitt bájtokat számolni kell. „Kvázi" véletlenszerűen lesz kiválasztva és a szegmens teljes élettartama alatt (ami kb. 4 óra) egyértelmű a teljes interneten. A bájtokban megadott ablakméret lehetővé teszi az adatáramlás ellenőrzését: először megtöltik az ablakot, csak ezután következik az adás vagy a vétel. Az ablak méretét a kliens és a szerver ebben és a következő két lépésben egyezteti egymással. A szerver megkapja a szegmenst, és válaszként 1-re állítja az ACK és a SYN bitet. Az ISN-t átveszi és kiküldi a saját ISN-jét, amelynél elkezdi a számolást. Ezen kívül megadja az ablakméretet is. A harmadik lépésben a kliens az 1-re állított ACK-val elfogadja az ablakméretet és igazodik hozzá. Ezzel felépült a kapcsolat. Egy kapcsolat megszakítása hasonlóan zajlik, csak a SYN bit helyett a FIN bitet használják.

Sliding Window

A magasabb rétegbeli protokollok bájtáramlás alakjában küldik a TCP-hez az adataikat, amelyeket ez szegmensekre bont. A *Sliding Window* (tolóablak) az adatok pufferelésére szolgáló tárterület. Minden hostnak két Sliding Window-ja van: egy az adáshoz és egy a vételhez. A TCP duplex-re alkalmas, vagyis az adás és a vétel egyidejűleg történik.

A TCP handshake alatt a vevőablak méretét az ellenállomás adóablak méretére állítják. Egy adatátvitel során az adóablakot teljesen feltöltik a TCP szegmensekkel, majd valamennyi szegmenst egymás után kiküldik. Ezen kívül elindul a *Retransmit Timer* is, amelyik meghatározza, hogy mikor kell újra küldeni a szegmenseket, ha a címzettől nem érkezett nyugtázás.

Az adó Sliding Window-ja mindaddig megtartja a szegmenseket, amíg ezeket a címzett nem nyugtázza. Amikor valamennyi szegmens vételét nyugtázták, kiürítik az adóablakot, és megtöltik a következő szegmenssel. Ha szegmensek elvesznek, úgy ezekről nem érkezik nyugtázás és a kliens ezeket a Retransmit Timer lejártával ismét elküldi. A címzettnél ismét a helyes sorrendbe rendezik a vett szegmenseket. Ha két szegmens megfelelő sorrendben helyezkedik el, és a megfelelő helyre érkezett, akkor megérkezik a nyugtázás és az adó tovább tolhatja a Sliding Window-ját, és új adatokkal (itt 2 szegmens) töltheti fel.

A TCP-Header felépítése		
Mező	Mérete bitekben	Ismeretetés
Source Port	16	A forrás host portszáma.
Destination Port	16	A cél host portszáma.
Sequence Number	32	A szegmens első adatbájtjának a száma, az adó határozza meg. A következő mezővel közösen ezek a számok azt garantálják, hogy a szegmensek a megfelelő sorrendben kerülnek egymás után a célban.
Acknowledgement Number	32	A nyugtázás száma.
Data Offset	4	A TCP-Header mérete 32 bites szavakként (szokványos 5, ha az opció mező foglalt, akkor 6).
Reserved	6	Jövőbeli alkalmazáshoz fenntartva (0-nak kell lennie).
Flags	6	URG: Urgent Pointer, ACK: Acknowledgement, PSH: azonnali küldés és vétel és nem csak az adó- és vevőpuffer megtöltését követően. , RST: kapcsolat felépítése, SYN: Synchronize, kapcsolat-felépítés iniciálása, FIN: kapcsolat befejezése.
Window	16	A Sliding Window mérete.
Checksum	16	A header és az adatok ellenőrző összege.
Urgent Pointer	15	Az adatok egy részét sürgősként jelöli meg.
Options	24	Információcsere, például a szegmensméret cseréje.
Padding	8	Töltő bitek, annak garantálására, hogy a header egy 32 bites határon fejeződjék be.

Ablakról

Egy windowsos hálózatot létrehozni nem ördöngösség. Az operációs rendszer ugyanis szinte minden szükséges eszközt magával hoz ehhez, ráadásul színes felületek is könnyítik a telepítést.

A név nyomában

Egy TCP/IP-s hálózatban a számítógépek azonosítására kizárólag 32 bites értékeket (= IP-címeket) lehet használni. A kiadott nevek inkább csak „kozmetikai célokat" szolgálnak, mert az ember könnyebben tud szavakat, mint számokat megjegyezni. Viszont a hálózatnak tudnia kell, hogy hogyan képezik le ezek a nevek az IP-címeket.

A nagy hálózatokban, így például az interneten, egy külön szolgáltatás létezik erre, amelynek a feladata, hogy IP-címeket hozzon létre a nevekből. Ez a szolgáltatás a *Domain Name Service*, vagy röviden *DNS*. Kis hálózatokban nincs szükség erre a szervizre, mert ehhez külön DNS szervert kellene létrehozni és kezelni.

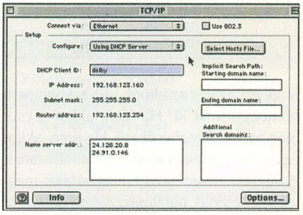
A neveket a NetBIOS esetében is le kell képezni a számítógépen. Ekkor mindegy, hogy a NetBIOS a NetBEUI-val vagy a TCP/IP-vel valósul-e meg. (A TCP/IP-ről lásd még külön cikkünket.)

A NetBIOS-t eredetileg kis hálózatokhoz készítették, így nem kalkuláltak be a névszolgáltatást. A számítógépek egyszerűen körkérdéseket (broadcast) küldenek ki. Más szóval: egy, a hálózatba újonnan bekötött PC egy *Halló, itt vagyok, a nevem XY* jellegű üzenetet küld körbe.

A kis hálózatok esetében (ahol nincs útkiválasztó és más alhálózatok) ez bőven elegendő. A nagy hálózatokban azonban nagyon rossz hatékonyságú lenne ez a megoldás, a többi alhálózatba való routolásnál pedig eleve lehetetlen. (A routerek rendszerint nem engednek át broadcast-okat a másik alhálózatba.)

Ennek a korlátozásnak a kikerülésére a NetBIOS számára kifejlesztettek egy DNS-t. Ennek a szolgáltatásnak az általános neve *Name Server for NetBIOS*. A Microsoft verzió neve viszont, szerencsétlen módon, *Windows Internet Name Service (WINS)*. Szerencsétlen pedig azért, mert a WINS-nek semmi köze az internethez.

A DNS és a WINS csak a nagy hálózatokhoz szükségesek, illetve csak ezeknél hasznosak. A kis hálózatokban a hatékony és megbízható működéshez bőven elég a broadcast-os Name Service.



Célszerű a TCP/IP-t választani

A Windows a jó öreg *Windows for Workgroups-szal* vált hálózatképessé. Hirtelen mindenkinek a módjában állt egy peer-to-peer hálózat kialakítása, feltéve, hogy volt hálózati kártyája. Mindez időközben jóval könnyebbé vált. A Windows 9x, NT és 2000 egyszerű párbeszédes mezőkkel támogatja a hálózati adminisztrátort, így egy hálózat kialakítása szinte gyerekjáték.

Az előkészületek

Habár a Windows alatt egy hálózat kialakítása a grafikus segédprogramoknak köszönhetően igazán kényelmes, néhány lényeges gonddal mégis találkozunk, amelyekkel kapcsolatban célszerű előre elgondolkodni.

Először is magunk konfiguráljuk a hálózati kártyát. A tipikus kérdések mellett, mint például NetBIOS név vagy IP-cím, itt olyan fogalmakkal is kapcsolatba kerülünk, mint DNS vagy WINS. Ezek a fogalmak a hálózati névképzés szempontjából fontosak. Ezekről részletesebben *A név nyomában* című keretes írásunk informál.

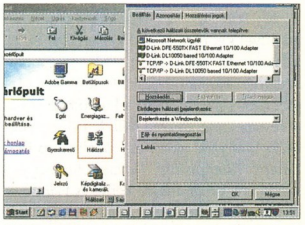
Egy másik lényeges pont a *tartomány* vagy *munkacsoport kérdése*. Ezeket a fogalmakat a hálózati alapokkal foglalkozó cikkünkben már ismertettük. A kérdés mégis nyitva áll, hogy milyen előnyökkel jár az egyik vagy a másik technika használata. Erre a kérdésre a „Hegemónia vagy kooperáció?" című keretes írásunk szolgál válasszal.

Lényeges még a hálózatban használt *protokoll* kérdése is. Amennyiben nem szándékozunk régi, Windows for Workgropus-os PC-t integrálni a hálózatba, amelynek még nincs TCP/IP támogatása, akkor a *TCP/IP*-t célszerű választani. A NetBEUI a TCP/IP-vel szemben némileg hátrányosabb, így ha lehet, használjuk az előbbit. Ha pedig linuxos gépet szeretnénk Samba-val a hálózatba kapcsolni, akkor a TCP/IP eleve kötelező. A Samba ugyanis nem ismeri a NetBEUI-t.

Mindegy, hogy melyik Windows változatot használjuk, a hálózat kialakításának mindig ugyanaz a módja. Először a hálózati kártya illesztőprogramjait kell telepíteni. Ezzel a rétegmodell hálózat elérési rétegét hozzuk létre. Ezt követően egy protokollt telepítünk (TCP/IP vagy NetBEUI), ezzel a szállítási és viszonyréteget keltjük életre. Végezetül konfiguráljuk az alapvető szolgáltatásokat, amelyek a rétegmodell alkalmazási rétegében helyezkednek el.

A Windows 95/98-as hálózat

A Windows 95/98 *Vezérlőpultján* találjuk a *Hálózatok* szimbólumot. Ez pontosan azt tartalmazza, amit a neve alapján



Hálózatunk kapcsolóközpontja itt bújuik meg

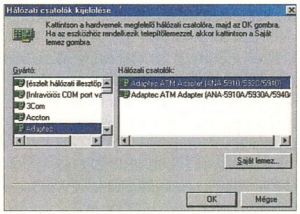
ablakra

ígér. E kis képecske mögött a hálózatunk kapcsolóközpontja búj ik meg. Itt lehet új hálózati kártyákat telepíteni, protokollokat installálni és szolgáltatásokat aktiválni.

Ha beépítünk egy hálózati kártyát a számítógépünkbe, úgy azt a Windows 95/98 rendszerint az indulásnál automatikusan felismeri és konfigurálja. Ha azonban egy régi ISA kártyát használunk, akkor ezt rendszerint nem ismeri fel. Az ilyen kártyát kézzel kell konfigurálni. Ezt az eljárást a *Vezérlőpulton*, a *Hálózat* szimbólum segítségével hajthatjuk végre.

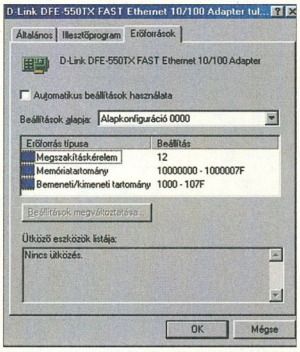
Ahhoz, hogy egy hálózati kártya illesztőprogramjait telepíteni tudjuk, kattintsunk a *Hozzáadás* kapcsolóra. A következő párbeszédes mezőben válasszuk egyszeri kattintással a *Csatoló* bejegyzést. Végezetül kattintsunk a *Hozzáadás-ra*.

Ekkor egy kettéosztott ablak jelenik meg. A bal oldali listában a kártya gyártóját kereshetjük meg, s a jobb oldali mezőben a gyártó valamennyi, a Windows által támogatott modellje megjelenik. Itt azután kiválaszthatjuk az érintett kártyát és az OK-ra kattintva telepíthetjük. Ha a kártyánk nem szerepel a felsorolásban, illetve a kártyához mellékelték az illesztőprogramokat tartalmazó adathordozót (ami új kártya esetén nagyon valószínű), akkor a *Saját lemez* kapcsolóval erről az adathordozóról telepíthetjük fel az illesztőprogramot.



A bal oldali listában a kártya gyártóját, jobbra pedig a kártyamodelleket látjuk

Miután telepítettük a hálózati kártyát, kiválaszthatjuk a főablakban, és a *Tulajdonságok* kapcsolóval konfigurálhatjuk. Az itt megjelenő beállítási lehetőségek a hálókártya típusától függnek. Ezzel kapcsolatban a kártya dokumentációja bővebb felvilágosítással szolgál.

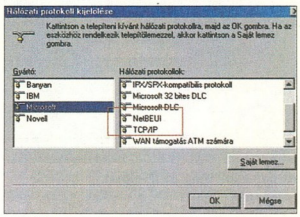


Kézzel kell megadnunk az IRQ-t

Vegyük figyelembe, hogy egy ISA kártya esetében nekünk kell megadnunk az IRQ-t és a portcímet. Ezt a hálózati kártya *Tulajdonságok* menüjében, az *Erőforrások* alatt kell megtennünk. A szükséges információkat a hálózati kártya dokumentációjából tudhatjuk meg.

A protokoll

Miután sikeresen telepítettük a kártyánkat, a *megfelelő protokollt* kell installálnunk. Ehhez is használjuk a *Hozzáadás* kapcsolót. A következő ablakban válaszszuk a *Protokoll-t*. Itt ismét egy kétlistás ablak jelenik meg. A bal oldalon egy gyártót választhatunk ki, míg jobbra a mindenkori, rendelkezésre álló protokollokat láthatjuk. A NetBEUI és TCP/IP protokollokat egyébként a *Microsoft* alatt találjuk.



A Microsoft alatt találjuk a NetBEUI és a TCP/IP protokollt

Miután hozzáadtunk egy protokollt, azt a főablak *Tulajdonságok* kapcsolójával konfigurálhatjuk. Mielőtt azonban erre a kapcsolóra kattinthatnánk, a felső listában ki kell jelölni az érintett protokollt. Ha több hálózati kártyát konfiguráltunk a rendszerünkben, vagy ha csak modemmel vagy ISDN-el lépünk az internetbe, akkor különböző, a protokoll nevével kezdődő felsorolásokat fogunk találni.

Tételezzük fel, hogy a PC-nk egy NE2000 kompatibilis hálózati kártyát tartalmaz, és ISDN-en keresztül lépünk be az internetbe. A helyi hálózathoz a TCP/IP protokoll mellett döntöttünk. Ebben az esetben a listában a *TCP/IP – telefonos hálózati csatoló*, valamint *TCP/IP – NE2000 kompatibilis hálózati kártya* vagy ehhez hasonló bejegyzéseket találjuk. A helyi hálózatunk konfigurálásánál csak a második bejegyzésnek van jelentősége. Ez teszi lehetővé, hogy a hálózati kártyánk TCP/IP protokolljához beállíthassuk a tulajdonságait, így például az IP-címet.

Válasszuk ki tehát a protokoll nevét és a hálózati kártyánkat tartalmazó protokollt, majd kattintsunk a *Tulajdonságokra*. Most a protokoll valamennyi jellemzője megjelenik, több regiszterlapon szétosztva.

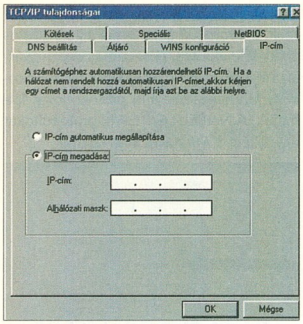
Mivel a NetBEUI beállításai nem túl sokrétűek, és a NetBEUI-t amúgy sem javasoljuk, így a továbbiakban csak a TCP/IP-vel foglalkoznunk.

Az első feladat az *IP-cím megadása*. Ezt a beállítást a *TCP/IP tulajdonságai* elnevezésű regiszterlapon végezhetjük. Itt választhatunk az *IP-cím automatikus megállapítása* és az *IP-cím megadása* között. Az

Átjáróval az internetbe

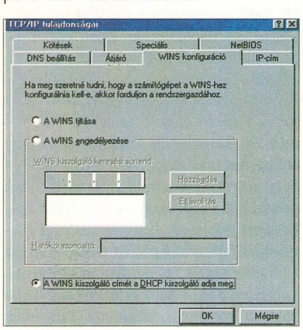
A TCP/IP konfigurálásánál az *Átjáró* regiszterlapon megadhatjuk egy (vagy több) átjáró IP-címét. Egy átjáró egy olyan számítógép, amely lehetővé teszi az átmenetet egy másik alhálózatba (Subnet).

Ha mondjuk egyetlen olyan PC-nk van, amelyik modemmel vagy ISDN kártyával rendelkezik, de valamennyi munkahelyről be akarunk lépni az internetbe, akkor ezt a PC-t *átjáróként* alakíthatjuk ki. Ha egy Linux PC-t alakítottunk ki internetes routernek, akkor ezt az IP-címet kell az átjáró IP-címeként megadni. Ebben az esetben a DNS konfigurálásával is foglalkoznunk kell. Először is aktiváljuk a DNS-t, majd adjuk meg a szolgáltatónk DNS szervereinek az IP-címeit. A *Hozzáadás* kapcsolóval fel lehet venni ezeket a DNS-szerver listájába.



Itt adhatjuk meg az IP-címet

IP-címet automatikusan csak akkor lehet megállapítani, ha a hálózatunk DCHP-szervert tartalmaz, amely automatikusan rendeli az IP-címet a hálózat egyes klienseihez. A kis hálózatokban egy ilyen szerver felesleges volna, ezért itt az IP-cím megadását válasszuk. Ezután a megfelelő mezőkben adjuk meg az IP-címet és a hálózati maszkot. Gondoljunk arra, hogy a megadott IP-cím egyértelmű legyen, tehát a hálózat semelyik másik PC-je se használhassa. A hálózati maszknak is meg kell egyeznie a(z) (al)hálózat többi számítógépénél alkalmazott maszkkal.



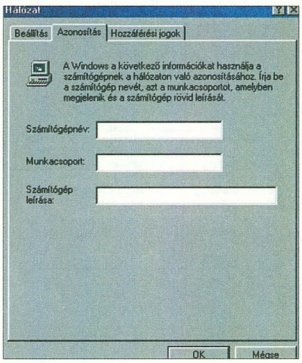
Beállíthatjuk a WINS szervert

A *WINS konfiguráció* és a *DNS beállítás* alatt a WINS és a DNS szervert állíthatjuk be. Ilyen szervereket is csak nagy hálózatokban célszerű megadni. Ezekkel a szolgáltatásokkal kapcsolatban a *A név nyomában* című keretes írásunk szolgál részletesebb információkkal. Kisebb hálózatok esetében mindkettőt kikapcsolhatjuk, kivéve, ha *internetes routert (útkiválasztót)* használunk. Érdekesek az *Átjáró regiszter* beállításai. Ehhez vessünk egy pillantást az *Átjáróval az internetre* című keretes írásunkra. A *Kötések* regiszterben meghatározhatjuk, hogy mely szolgáltatásokat lehessen használni a megfelelő kártyával. Itt rendszerint valamennyi szolgáltatást aktiválhatjuk.

A Windows 95/98 alatt több szolgáltatást és klienst is telepíthetünk. A Windows hálózathoz a *Microsoft Network ügyfélre,* valamint a *Microsoft Network fájl- és nyomtatómegosztás*-ra van szükségünk. Ha egyik vagy másik bejegyzés hiányozna a főablak konfigurációs listájából, akkor kattintsunk a *Hozzáadásra,* és válaszszuk az ügyfelet, illetve a szolgáltatást, hogy utólag telepíthessük a megfelelő bejegyzést.

A név kötelez

A következő lépésben nevet rendelünk a számítógéphez, s ezen a néven lehet elérni a hálózatban a hostot. E célból válasszuk a főablakban az *Azonosítás* regisztert. A *Számítógépnév* alatt adjunk



Rendeljünk nevet a számítógéphez

meg egy szabadon választott nevet. Azonban az IP-címhez hasonlóan, itt is figyeljünk arra, hogy ez a név *egyértelmű* legyen, vagyis a hálózatban, illetve az adott munkacsoportban más host ne használja ezt a nevet.

A *Munkacsoport* alatt egy második nevet adunk meg. Ez a név azt a csoportot jelöli, amelybe a host tartozik. A munkacsoportokkal logikai egységekbe vonhatjuk össze egy hálózat több számítógépét.

A *Számítógép leírásának magadása* opcionális. Itt csupán rövid információt adhatunk meg azzal kapcsolatban, hogy mi a host célja a hálózatban, kinek a számítógépe vagy ehhez hasonlókat. A hálózat működése szempontjából az itt megadottaknak semmi jelentőségük sincs.

Amennyiben a számítógépünknek egy N vagy egy Samba szerver tartományába kell bejelentkeznie, akkor az azonosítási információk megadása után lépjünk át a *Beállítás* regisztерlapra. Itt hívjuk meg a *Microsoft Network ügyfél tulajdonságait.* Itt lehet aktiválni a tartományba történő bejelentkezést. Ezután a megfelelő beviteli mezőben adjuk meg a tartomány nevét. Itt még kiválaszthatjuk, hogy már a bejelent-

Hegemónia vagy kooperáció?

A számítógépeket csoportosítani lehet a windowsos hálózatokban. Erre munkacsoportok és tartományok szolgálnak. A tartomány nem más, mint egy *szerver által kontrollált munkacsoport.* Minden számítógépnek, aki be akar kerülni a tartományba, előbb be kell jelentkeznie a szervernél. Ha a szerveren nincs megfelelő, érvényes felhasználói fiók, akkor a tartomány és ezzel a hálózat elérése visszautasításra kerül.

Egy munkacsoport esetében viszont elegendő, ha a számítógép konfigurációja tartalmazza az adott munkacsoport nevét. Ekkor nem kell magát azonosítania, e nélkül is bejut a hálózatba és a nyilvános, tehát a jelszóval nem védett megosztásokat is elérheti.

A tartományok tehát biztonságosabbak, de a tartományok ellenőrzéséhez legalább egy szerverre *(Primary Domain Controller = PDC)* szükség van. A nagyobb windowsos hálózatokban a meghibásodások okozta gondok elkerülésére egy vagy több pótszerver is létezik *(Secondary Domain Controller = SDC),* amelyek a PDC kiesése esetén ellátják ennek feladatait.

Korábban a tartományalapú hálózatok üzemeltetése jelentős pénzügyi beruházást igényelt, mert egy NT-szerverre is szükség volt. Ma már a Linux alatt egy Samba szervert is lehet úgy konfigurálni, hogy PDC-ként működjön.

A tartományokat a professzionális, nagy hálózatokhoz ajánljuk, amelyeknél jelentős szerepe van a biztonságnak. A kis, otthoni hálózathoz elég egy munkacsoport kiépítése. Viszont valóban érdekes feladat a Sambával behatolni a tartományok területére.

kezésnél ellenőrzésre kerüljön, hogy a hálózati kapcsolat valóban használható-e.

Végül lépjünk be a *Beállításokba*, és az *Elsődleges hálózati bejelentkezés* alatt válasszuk a *Microsoft Network* ügyfelet. Ennek hatására a Windows indulásakor automatikusan megjelenik a hálózati bejelentkezés ablaka.

A hálózat konfigurálást az OK-ra történő kattintással zárjuk le. A hálózat a számítógép újraindítását követően már a rendelkezésünkre áll.

NT, a nagytestvér

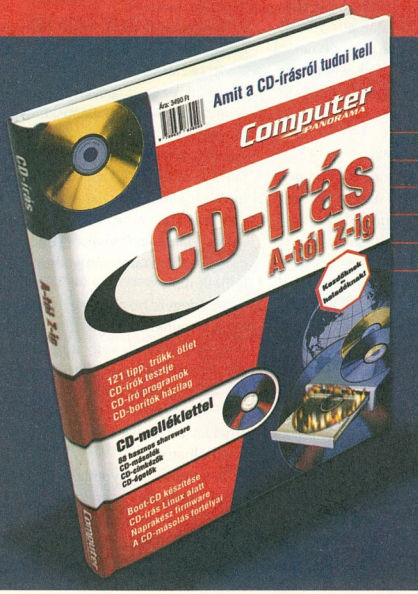
A Windows NT 4.0 konfigurálása szintén a *Vezérlőpulton*, a *Hálózatok* szimbólum mögött húzódik meg. A párbeszédes mezők felépítése azonban alapvetően eltérő kialakítású. A Windows NT 4.0 automatikus hardverfelismerése még némi kívánnivalót hagy maga után, ugyanis nem képes a plug and play módszer szerint felismerni a hálózati kártyánkat. Amikor első alkalommal kattintunk a *Hálózatok* szimbólumra, és előtte még nem telepítettünk hálózati támogatást, akkor megjelenik a *Windows NT hálózati támogatás nincs telepítve* párbeszédes mező. Itt kattintsunk az *Igen*-re, hogy a telepítést ezzel megkezdhessük. Ezután válasszuk a *Közvetlen csatlakozás a hálózathoz* pontot. A *Keresés* kapcsolóra történő kattintással az NT nekifog a hálózati kártyánk keresésének. Ha nem ismerné fel a hálózati kártyánkat, akkor kézzel kell kiválasztani az illesztőprogramot. A *Saját lemez* kapcsolóval a kártyához mellékelt flopiról vagy CD-ről telepíthetjük a drájvereket.

A telepítéshez javasolt szolgáltatásokat is célszerű telepíteni. Ezzel lehetővé válik, hogy a PC-nk egyfelől használja a hálózat megosztott erőforrásait, másfelől viszont saját fájlstruktúrákat és nyomtatókat is meg tudjon osztani a hálózat többi résztvevőjével. Az NT 4.0 alapértelmezés szerint a TCP/IP protokollt választja, s ezen ne is változtassunk.

A hálózati támogatás sikeres telepítését követően a *Vezérlőpult Hálózatok* ablaka egy öt regisztерlapos konfigurációt tartalmaz. A *Hálózati kártyák* alatt további kártyákat konfigurálhatunk, vagy a már telepítettek tulajdonságain változtathatunk. További szolgáltatásokat, mint pl. kliens szoftvert más hálózatokhoz (pl. Novell NetWare) a *Szolgáltatások* regiszterlapon vehetünk fel. Azt, hogy melyik szolgáltatást melyik kártyákkal és protokollokkal lehessen elérni, a *Kapcsolatok* regiszterlapon lehet beállítani. Egy kis, homogén hálózatban azonban rendszerint semmit sem kell megváltoztatni.

Fontos még a *Protokollok* regiszterlap. Itt nemcsak új protokollokat lehet felvenni, hanem a már telepített protokollok tulajdonságain is változtathatunk. A TCP/IP konfigurálásához először is válasszuk ki a *Hálózati protokollok* listájából, majd kattintsunk a *Tulajdonságokra*. Az első regiszter a hálózati kártyánk IP-címe után érdeklődik. Ha a PC több hálókártyát is tartalmaz, akkor ezeket a *Hálózati kártya* mezővel lehet átkapcsolni. A címet mindegyik kártyához vagy manuálisan adhatjuk meg, vagy egy DHCP szerverrel osztatjuk ki. Az utóbbi csak nagy hálózatokra jellemző és csak ott van értelme.

Amit a CD-írásról tudni kell



- A CD másolás fortélyai
- CD-írók tesztje
- 121 tipp, trükk, ötlet
- CD-író programok
- CD-borítók házilag
- Boot-CD készítése

Megrendelhető:
Computer Panoráma Kiadói Kft.
1091 Budapest, Üllői út 25.
Telefon: 456-6964, Fax: 456-6970
E-mail: terjesztes@cpanorama.hu
Ára: 3490 Ft

Második kiadás!

Ezért rendszerint a kis hálózatunkban *kézzel állítjuk be az IP-címet.* A megfelelő kapcsoló aktiválását követően tehát adjuk meg ezt a megfelelő mezőben. Arra persze itt is gondoljunk, hogy a kiadott érték csak egyszer szerepeljen a hálózatban. Az IP-címet a hálózat egy másik számítógépe nem használhatja. Ez az ablak másodikként a hálózati maszkot kéri. Gondoljunk arra, hogy a(z) (al)hálózat valamennyi számítógépének a maszkja azonos kell, hogy legyen. Ezen kívül megadhatunk egy standard átjárót is. Vegyük figyelembe az *Átjáróval az internetbe* című keretes írásunk információit is.

Függetlenül attól, hogy *átjáróval* lépünk-e be az internetbe, a DNS és WINS címeknek csak a nagy hálózatokban van jelentőségük. Ezek a szerverek kis hálózatokban szokványos esetben nem is állnak rendelkezésre. Az ezzel kapcsolatos további információkkal a *A név keresése* című keretes írásunk szolgál. Az *Útvonalkeresés* regiszterlapon található beállításoknak csak olyankor van értelmük, ha a számítógépünk több hálózatos rendszer közös része, és ezek között *útkiválasztóként* (routerként) kell működnie.

A számítógépnek a hálózaton, illetve a munkacsoporton/tartományon belül egyértelmű névre van szüksége. Azt is meg kell adnunk, hogy melyik munkacsoportba vagy tartományba tartozik a PC-nk. Mindezt az *Azonosítás* regiszterlapon, a *Változtatás* kapcsolóval adhatjuk meg.

Ezzel a hálózat NT alatti konfigurálását befejeztük, elindíthatjuk a hálózatot.

A Windows 2000 új generációja

A hálózat konfigurálása a Windows 2000 alatt nagyon megváltozott. Aki hozzászokott a Windows 95/98-hoz vagy az NT-hez, már semmit sem talál a helyén.

A Windows 2000 hardverfelismerése rendszerint automatikusan azonosítja a hálókártyákat. Csupán a régebbi ISA kártyák okozhatnak problémát. Ezeket ugyan felismeri, de nem jól osztja ki az IRQ és portcímeket. Ezt a gondot azonban könnyen megoldhatjuk a *Vezérlőpult Rendszer* szimbóluma alatt. Ehhez kattintsunk a *Hardver* regiszterlapon az *Eszközkezelő* kapcsolójára. Nyissuk meg a hálókártyánk tulajdonságait és az *Erőforrások* alatt adjuk meg az IRQ- és portcímek helyes értékeit.

Amint hálózati kártya van a rendszerünkben, beállíthatjuk annak tulajdonságait a *Hálózati és telefonos kapcsolatok* alatt. Ehhez válasszuk a *LAN-kapcsolatokat.* Erre megjelenik egy párbeszéd, amelynek a *Tulajdonságok* kapcsolója vezet a konfiguráláshoz.

A *Telepítés* kapcsolóval új szolgáltatásokat, protokollokat vagy klienseket tudunk a rendszerbe integrálni más hálózatok számára. Azt, hogy itt mi lett telepítve, a főablak közepén lévő lista árulja el. Hogy ezen protokollok, szolgáltatások vagy kliensek közül melyiket lehet a hálózati kártyával használni, az adott opció kijelölésével adhatjuk meg.

A *Tulajdonságok* kapcsolóval a listában éppen kiválasztott komponenst konfigurálhatjuk. Válasszuk ki az *Internetprotokollt (TCP/IP),* majd a TCP/IP konfigurálásához kattintsunk a *Tulajdonságokra.* Itt adjuk meg a számítógépünk IP-címét és hálózati maszkját. A többi tulajdonságot, mint a DNS, a WINS vagy az átjárók, a Windows 2000-nél a *Speciális* menü tartalmazza. Itt vegyük figyelembe a Windows 95/98-cal és az NT 4.0-val kapcsolatban tett megjegyzéseket.

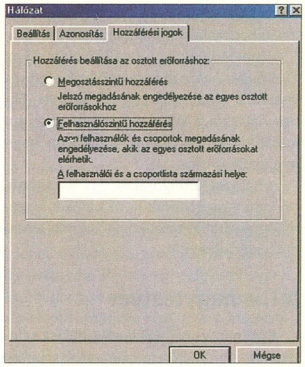
A számítógép hálózati azonosítója a Windows 2000-nél egy rendszerjellemző, és így a *Vezérlőpulton,* a *Rendszer* szimbólumban érhető el. Itt található a Hálózati azonosító regiszterlap, amelynek a *Tulajdonságok* kapcsolójával lehet megváltoztatni a számítógép azonosítóját.

Megosztások

A nyomtatók, könyvtárak vagy lemezegységek hálózati rendelkezésre bocsátásához telepíteni kell a *Fájl- és nyomtatómegosztás* elnevezésű szolgáltatást. Ezt követően a helyi menüben megoszthatjuk az érintett eszközöket. Ehhez kattintsunk az egér jobb oldali gombjával a *Windows Intézőben* az adott mappára vagy nyomtatóra, és válasszuk a *Megosztás* parancsot.

A Windows 2000-ben és az NT-ben az objektumok megosztása mindig felhasználói szinten történik. Világosan definiált, hogy mely felhasználók férhetnek hozzá az objektumokhoz. Ezen rendszerek *Megosztás* ablakában a *Jogosultságok* kapcsolóval határozhatjuk meg, hogy ki, mihez, hogyan (írás/olvasás) férhet hozzá.

A Windows 95/98 standard beállítása alapján a megosztott objektumok *megosztási szinten* érhetők el. Más szóval a



Felhasználói szinten is aktiválhatjuk a megosztást

megosztásnál *jelszóval* szabályozzák, hogy ki kap írási és/vagy olvasási jogokat. Aki ismeri a jelszót, az hozzáférhet az objektumhoz. A Windows 9x-nél a megosztást felhasználói szinten is aktiválhatjuk. Erre szolgál a *Vezérlőpult/Hálózat/Hozzáférési jogok* regiszter. Itt egy olyan számítógépet kell megnevezni, amelyik a szükséges felhasználói listát szolgáltatja. Ideális esetben ez egy NT- vagy Windows 2000-es rendszer.

Függetlenül attól, hogy melyik típusú megosztás-szabályozás mellett döntünk, a megosztásnak nevet kell adnunk. A hálózatban ezen a néven lehet elérni az érintett objektumot. Leírásként még egy megjegyzést is megadhatunk.

Ha a Windows Intézőben vagy az Asztalról a *Hálózati kapcsolatokhoz* fordulunk, ott először a saját munkacsoportunk vagy tartományunk összes PC-jét látjuk. A *Teljes hálózattal* viszont esetleges más csoportokhoz/tartományokhoz is hozzáférhetünk.

Mindegyik hosthoz egy *megosztási listát* is kapunk. A megosztott könyvtárakat vagy közvetlenül, vagy a helyi menü *Hálózati meghajtó csatlakoztatása* parancsával lehet elérni. Az esetünkben például egy kiegészítő G: meghajtót kapunk, amelyet a helyi lemezünkhöz hasonlóan használhatunk.

A megosztott nyomtatókat úgy telepítjük a másik rendszereknél, hogy a helyi menüben kiválasztjuk a *Telepítés* pont alatt az érintett megosztott eszközt. Ezt követően a nyomtató már a rendelkezésünkre áll.

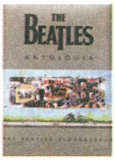
FAX MEGRENDELŐLAP

Computer Panoráma
1091 Budapest, Üllői út 25.● Terjesztési osztály: tel.: 456-69-64, fax: 456-69-70

❒ Igen, megrendelem a **CD-melléklettel** megjelenő **Computer Panorámát** egy évre 11 990 Ft-ért és választok egyet az alábbi négy ajándék közül:

- ○ **World War II (CD)**
- ○ **The Nations (CD)**
- ○ **Beatles antológia (könyv)**
- ○ **Európa-szótár (CD) (német-magyar, magyar-német)**



A lapot 2003. .....havi számtól kérem.
Az előfizetést ❒ csekken
❒ átutalással rendezem.

További információk a választható útikönyvekről a www.computerpanorama.hu/elofizetes címen.

❒ Igen, megrendelem a következő **DVD-melléklettel** megjelenő **Computer Panorámát** 2390 Ft-ért.

❒ Igen, megrendelem az **Monitorok** című kiadványt (495 Ft)
❒ Igen, megrendelem az **Arany Válogatás III** című kiadványt (1690 Ft)
❒ Igen, megrendelem a **Windows XP** című kiadványt (595 Ft)
❒ Igen, megrendelem az **Adatbiztonság** című kiadványt (695 Ft)
❒ Igen, megrendelem az **CAD/CAM** című kiadványt (695 Ft)
❒ Igen, megrendelem az **Arany Válogatás II** című kiadványt (1495 Ft)
❒ Igen, megrendelem az **Notebook** című kiadványt (695 Ft)
❒ Igen, megrendelem a **Digit Fotó** című kiadványt (695 Ft)
❒ Igen, megrendelem a **Mobil Világ** című kiadványt (495 Ft)
❒ Igen, megrendelem a **Monitorok** című kiadványt (495 Ft)
❒ Igen, megrendelem az **Internet** című kiadványt (595 Ft)
❒ Igen, megrendelem a **Nyomtatók** című kiadványt (595 Ft)
❒ Igen, megrendelem az **MP3 Mánia** című kiadványt (990 Ft)

SZÁMLÁZÁSI CÍM:

Cégnév (név): .....
.....
Kapcsolattartó neve/beosztása: .....
.....
Telefon: .....
Fax: .....
E-mail: .....
Cím: ☐☐☐☐ helység: .....
.....
út/utca/tér:.....
h.sz.:..... em./ajtó: .....

POSTACÍM:

Név: .....
Cím: ☐☐☐☐ helység:.....
.....
út/utca/tér:.....
h.sz.:..... em./ajtó: .....
Telefon: .....

.....
dátum

.....
aláírás

Fenti áraink a postaköltséget nem tartalmazzák. A küldeményeket utánvéttel postázzuk.

FAX: 456-69-70

Kötetlenül

Két év is eltelt azóta, hogy megünnepelhettük az Ethernet megszületését, valamint az első kiforrott, vezeték nélküli hálózati eszközökkel találkozhattunk a boltok polcain. Az érdeklődés mellett az adatátviteli sebesség is növekszik, a szolgáltatások sokszínűségéről nem is beszélve. Elérkezettnek láttuk tehát az időt, hogy feltérképezzük e piacot.

A vezeték nélküli jelátvitel módja régóta ismert: elég, ha csak a rádióra gondolunk, ám a hagyományos hangtovábbítás helyett a mobil kommunikációban is ismert *csomagkapcsolt átvitelt* használják. A nagyobb adatsebesség érdekében nemcsak több csatornán (szélesebb frekvenciatartományban), hanem magasabb frekvencián forgalmaznak az adó-vevő egységek. A magasabb frekvencia pedig nagyobb sebességet és kisebb alkatrészeket is lehetővé tesz. A mai 11 Mbites hálózati egységek integrált áramkörei megfelelően kis méretűek, technológiailag semmi újat nem követelnek, hiszen a vezetékes hálózati áramkörök gigabites sebessége tartja a frontot. Ennél a technológiánál az átviteli közeg jelenti a korlátot, amelyre a komolyabb antenna-, jelátviteli- és jelerősítő technológiák jelentik a megoldást. Igen komoly korlátozó tényező, hogy az adók sugárzási teljesítménye, valamint a rendelkezésre álló frekvenciák a különféle szabványoknak megfelelően korlátozottak.

A fejlődés csak most indult be igazán, hiszen a jelenlegi 2,4 GHz-es frekvencia (2400-2483,5 MHz tartomány) által lehetővé tett 22 Mbit sávszélesség – valljuk be – kevés. Azokban az esetekben viszont, amelyekben a körülmények nem teszik lehetővé vezetékes hálózat kiépítését, igencsak hasznosak.

A vezeték nélküli hálózat két fő alkotóelemből áll: a *hozzáférési pont (access point)* és a *kliens adapter*. A működése alapján a kliens adapter megegyezik a hálózati kártyával, azzal a különbséggel, hogy a rádiós kommunikáció következtében ehhez illeszkedő funkciói is állíthatók. Létezik PCI-os, PCMCIA kártya (PC kártya), valamint USB csatlakozós kivitel. A hozzáférési pont alapvetően bridge funkciót lát el, az UTP kábelt használó 10/100-as hálózatokhoz csatolja a vezeték nélküli eszközöket, de újabban ISDN, ADSL interfész (ekkor routerről beszélünk), illetve 10/100-as switch is megtalálható rajta. A kínálat szerencsére meglehetősen sokrétű, ezért inkább az eszközök jellemzőinek bemutatására törekedtünk.

Access Point-ok

A hozzáférési pontok hálózatba illesztésénél a legelső szempont azok elhelyezése. Ideiglenes használatra a minden esetben külső tápegységgel rendelkező eszközt a már meglévő 10/100-as hálózatunkhoz illesztjük, egyszerű sík felületen elhelyezve. Azt figyelembe kell vennünk, hogy a hagyományos vagy beépített antennával rendelkező eszközök gömb, illetve fánk alakú területen sugároznak. Tapasztalataink alapján a dobozra írt adótávolság idealizált, az épületen belüli távolság talán csak egy hangárban való használatkor helytálló. Gyakorlatilag 20-30 méterrel számolhatunk akkor, ha néhány fal útját állja a rádióhullámok terjedésének. A gyártók ennek a tudatában is vannak, ezért az igényeknek megfelelő karakterisztikájú (gúla, félkör stb.) adott terület lefedésére készült antennákat is kínálnak. A hozzáférési pontok antennacsatlakozója szabványos, ez alól csak a különleges antennával ellátott típusok kivételek. Ilyen például a *3Com* kisebbik hozzáférési pontja, amelynek forgatható lapantennája van, vagy a *U.S. Robotics* és az *SMC* kisebbik típusa, amelynek beépített antennája van. Az irányított sugarú antennák azért is fontosak, mert hálózatunkat a titkosítás mellett területi elhatárolással is hatékonyan védhetjük.

A hozzáférési pontokat minden esetben a hálózatunkhoz kell igazítani, hiszen a legritkább esetben működnek a kívánalmaknak megfelelően. A beállítást leggyakrabban a helyi hálózaton keresztül, egy számítógép böngészőjébe írt IP-címmel kezdhetjük. A dokumentációban ez a cím megtalálható, de arra fel kell készülnünk, hogy nem minden esetben illeszkedik az általunk használt címtartományba. Ha a hálózatunkban DHCP szerver is van, akkor a hozzáférési pont keres egy címet, és azt foglalja le. Ekkor pedig a hozzá tartozó konfigurációs programmal állíthatjuk be a jellemzőit. DHCP használata nélkül a készülék egy előre definiált címre „ül be", ekkor csak a konfigurációs program jöhet szóba. Ha olyan intelligens, mint a *LinkSys* keretprogramja, akkor a MAC-cím alapján keresi meg és konfigurálja a hozzáférési pontot, így a beállítás az IP hálózattól függetlenül mindig biztos. Az Intel készülékén konzol

U.S. Robotics

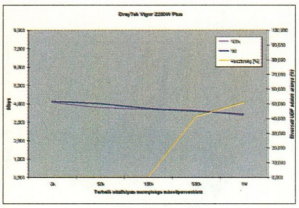
Gyártó, típus: U.S. Robotics 22Mbit vezeték nélküli access point
Forgalmazó: RRC Hungary
Ár: 43 290 Ft
Internet: www.usr.hu, www.rrc.hu

Sebesség	46	50
Telepítés	28	30
Szolgáltatások	12	20

pont **86** Értékelés: felsőkategória

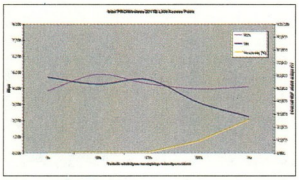
PLUSZ:
- kicsi, könnyen telepíthető, gyors

MINUSZ:
- kevés extra



port is található, tehát egy soros kábel segítségével közvetlenül konfigurálhatjuk. Ez bizonyos biztonságot is jelent, hiszen a beállítások csak így módosíthatók, feltörni tehát nehezen lehet. A harmadik módszer az elsőhöz hasonló, ám nem a helyi hálózatot, hanem a vezeték nélküli hálózatot veszi igénybe: a 3Com kezelőprogramja csak egy kliens használatával tudja elérni a hozzáférési pontot. Itt jegyezzük meg, hogy a 3Com készüléke érdekes módon csak egyetlen csatlakozót tartalmaz: a tápfeszültség és a helyi hálózat egy UTP kábelen keresztül jut el hozzá, a helyi háló tehát a tápegységbe csatlakozik. Ennek előnye, hogy az akár plafonra is rögzíthető készülék nem gazdagítja a kábelrengeteget. Ilyen opcióval az *Intel* eszköze is kiegészíthető. Dicséretes, hogy a készülékek dobozában szinte minden esetben találunk fúrósablont a falra szereléshez.

A konfiguráció meglepően egyszerű volt a *D-Link*, a *LevelOne* és a *LinkSys* esetén, elfogadhatónak éreztük az *Intel*, az *SMC* és a *U.S. Robotics* esetén, és egy picit körülményesnek a *3Com*-nál. Ez a tesztkörnyezetünk által meghatározott előfeltételek miatt volt így, de biztosan



megállapíthatjuk, hogy egy DHCP szerverrel (is) rendelkező hálózat segítségével, valamint egy már meglévő vezeték nélküli hálózattal egyszerűbb és gyorsabb ezt beállítani, mint a többit.

A szolgáltatások is sokrétűek, a hagyományos access point működés mellett, amelyet a U.S. Robotics ismer, klienskénti is használható a 3Com, az Intel, az SMC és a LevelOne hálózati kártyája. A gyakorlatban ez azt jelenti, hogy egy helyi hálózatot vezeték nélküli kapcsolaton keresztül egy másik hálózathoz kapcsolhatunk. Ehhez értelemszerűen legalább két hozzáférési pontot kell használnunk, nagyobb távolságok áthidalásához pedig kis szórású, célzott antennákat. A mezőny tagjai közül az Intel és az U.S. Robotics kivételével mindegyik alkalmas repeater funkciók ellátására, tehát a konfigurálás után a helyi hálózatról leválasztva, egy másik access point hatósugarán belül maradva, a lefedett területet növelhetjük meg, a szabad kapacitás enyhe csökkenésének a feláldozásával.

A 3Com, a D-Link, a LevelOne és a LinkSys *DHCP szerverként is* képes működni, amely különösen a switchet is tartalmazó készülékeknél előnyös. Így nemcsak a vezeték nélküli, hanem a vezetékes készülékek IP-címe is automatikus kiosztásra kerül. Olyan helyen előnyös ez, ahol a rendelkezésre álló címtartomány kevesebb készüléket enged, mint ahányan az adott területen csatlakozhatnak, de ennél kevesebb felhasználó lép fel a hálózatra egy időben. Ezek mellett természetesen a 3Com és az Intel is rendelkezik távoli adminisztrációs (SNMP) lehetőséggel.

Külön kiemelnénk a D-Link és a U.S.

3Com

Gyártó, típus:
3Com Wireless LAN Access Point 8000
Forgalmazó: HRP Hungary
Ár: 151 237 Ft
Internet: www.3com.com, www.hrp.hu

Sebesség	20	50
Telepítés	15	30
Szolgáltatások	18	20

pont 53 Értékelés: alsókategória

PLUSZ:
- az elhelyezését nem korlátozza semmi (UTP kábelen a tápfeszültség)

MINUSZ:
- egyedi csomagoptimalizálás (saját hálózatban előny)

3Com

Gyártó, típus:
3Com 11 Mbps Wireless LAN PC Card
Forgalmazó: HRP Hungary
Ár: 30 050 Ft
Internet: www.3com.com, www.hrp.hu

Sebesség	20	50
Telepítés	30	30
Szolgáltatások	14	20

pont 64 Értékelés: középkategória

PLUSZ:
- kinyitható antenna, funkciókban gazdag kliens program

MINUSZ:
- bonyolított hálózati csatlakozás (SSID mellett más is)

D-Link

Gyártó, típus: D-Link DWL-120
Forgalmazó: CCS Hungary Bt.
Ár: 25 750 Ft
Internet: www.dlink.com, www.ccs.hu

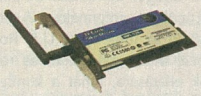
Sebesség	20	50
Telepítés	30	30
Szolgáltatások	10	20

pont 60 Értékelés: középkategória

PLUSZ:
- kiváló használhatóság, egyszerű telepítés

MINUSZ:
- kár, hogy csak USB 1.1

D-Link



Gyártó, típus: D-Link AirPlus DWL-520+
Forgalmazó: CCS Hungary Bt
Ár: 22 915 Ft
Internet: www.dlink.com, www.ccs.hu

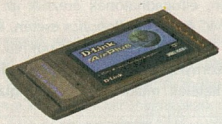
Sebesség	50	50
Telepítés	30	30
Szolgáltatások	12	20

pont **92** Értékelés: csúckategória

PLUSZ:
- kiváló használhatóság, egyszerű telepítés, nagy sebesség

MINUSZ:
- nincs

D-Link



Gyártó, típus: D-Link AirPlus DWL-650+
Forgalmazó: CCS Hungary Bt
Ár: 22 900 Ft
Internet: www.dlink.com, www.ccs.hu

Sebesség	45	50
Telepítés	30	30
Szolgáltatások	14	20

pont **89** Értékelés: felsőkategória

PLUSZ:
- egyszerű telepítés, nagy sebesség

MINUSZ:
- kevés hozzáadott program

D-Link

Gyártó, típus: D-Link AirPlus DWL-900AP+
Forgalmazó: CCS Hungary Bt
Ár: 50 170 Ft
Internet: www.dlink.com, www.ccs.hu

Sebesség	50	50
Telepítés	30	30
Szolgáltatások	18	20

pont **98** Értékelés: csúckategória

PLUSZ:
- nagy sebesség, 256 bites titkosítás

MINUSZ:
- nincs

DrayTek

Gyártó, típus: DrayTek Vigor2200W Plus
Forgalmazó: GamaxNet
Ár: 99 750 Ft
Internet: www.draytek.com.tw, www.gamaxnet.hu

Sebesség	35	50
Telepítés	27	30
Szolgáltatások	20	20

pont **82** Értékelés: felsőkategória

PLUSZ:
- a legtöbb hálózatban sok szolgáltatása miatt jól használható

MINUSZ:
- még csak 128 bites WEP titkosítás

Intel

Gyártó, típus:
Intel PRO/Wireless 2011B LAN PC Card
Forgalmazó: Intel Magyarország
Ár: 32 900 Ft
Internet: www.intel.com

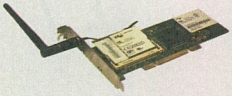
Sebesség	25	50
Telepítés	18	30
Szolgáltatások	18	20

pont **61** Értékelés: középkategória

PLUSZ:
- állítható fogyasztás-adóteljesítmény, gyors hálózatváltás

MINUSZ:
- a meghajtó programot le kellett tölteni, nem volt rajta a mellékelt CD-n

Intel



Gyártó, típus:
Intel PRO/Wireless 2011B LAN PCI Card
Forgalmazó: Intel Magyarország
Ár: 40 110 Ft
Internet: www.intel.com

Sebesség	25	50
Telepítés	24	30
Szolgáltatások	18	20

pont **67** Értékelés: középkategória

PLUSZ:
- kompatibilitási problémák biztosan nem lesznek vele, egyszerű telepítés

MINUSZ:
- az Inteltől többet várnánk

Intel

Gyártó, típus: Intel PRO/Wireless 2011B LAN Access Point
Forgalmazó: Intel Magyarország
Ár: 56 600 Ft
Internet: www.intel.com

Sebesség	30	50
Telepítés	30	30
Szolgáltatások	18	20

pont **78** Értékelés: felsőkategória

PLUSZ:
- konzol portról is konfigurálható

MINUSZ:
- a LED-ek fényei csak felülnézetben láthatók, ingadozó sebesség

Level

Gyártó, típus: LevelOne Wireless LAN PC-Card WPC-0100
Forgalmazó: ASBIS Magyarország
Ár: 25 100 Ft
Internet: www.level-one.hu, www.asbis.hu

Sebesség	35	50
Telepítés	30	30
Szolgáltatások	10	20

pont **75** Értékelés: felsőkategória

PLUSZ:
- könnyű telepítés, megbízható működés

MINUSZ:
- átlagos sebesség

Level

Gyártó, típus: LevelOne Wireless LAN 11Mbps Access Point WAP-0001
Forgalmazó: ASBIS Magyarország
Ár: 54 870 Ft
Internet: www.level-one.hu, www.asbis.hu

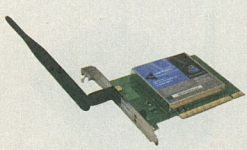
Sebesség	40	50
Telepítés	24	30
Szolgáltatások	14	20

pont **78** Értékelés: felsőkategória

PLUSZ:
- kis méret, gyors üzembe helyezés, megbízható működés

MINUSZ:
- a hatótávolsága egy picivel kisebb az antennás típusokénál

Linksys



Gyártó, típus: Linksys Instant Wireless Network Adapter WPC11
Forgalmazó: Alphasonic Kft.
Ár: 22 625 Ft
Internet: www.linksys.hu, www.alphasonic.hu

Sebesség	35	50
Telepítés	24	30
Szolgáltatások	12	20

pont **71** Értékelés: középkategória

PLUSZ:
- jó monitorprogram

MINUSZ:
- az SSID itt is saját név kézzel kell a hálózathoz igazítani

Linksys

Gyártó, típus: Linksys USB adapter WMP11
Forgalmazó: Alphasonic Kft.
Ár: 22 625 Ft
Internet: www.linksys.hu, www.alphasonic.hu

Sebesség	20	50
Telepítés	30	30
Szolgáltatások	16	20

pont **66** Értékelés: középkategória

PLUSZ:
- tépőzáras rögzítés

MINUSZ:
- AA USB kábelt használ

Linksys

Gyártó, típus: Linksys Wireless Network Access Point WAP11
Forgalmazó: Alphasonic Kft.
Ár: 42 625 Ft
Internet: www.linksys.hu, www.alphasonic.hu

Sebesség	40	50
Telepítés	21	30
Szolgáltatások	14	20

pont **75** Értékelés: felsőkategória

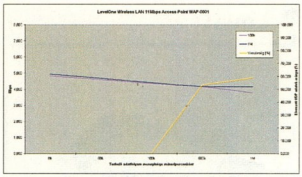
PLUSZ:
- gyors és könnyű telepítés, egyenletes lefedettség

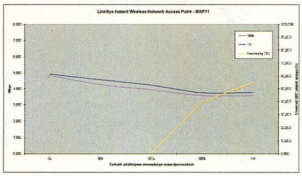
MINUSZ:
- nagy leterheltségnél elvet UDP csomagot

Robotics hozzáférési pontjait, amelyek nemcsak a 22 Mbites sebességet ismerik, hanem a 256 bites titkosító kulcsokat használják a hálózat védelmére.

Végül, de nem utolsósorban essék szó a sebességről: a 22 Mbit adatátviteli sebessége elméletileg 2,75 Mbájt, a méréseink szerint egyetlen kliens esetén éppen eléri az 1 Mbájtot másodpercenként. Ehhez képest a ma még tipikusnak tekintett 11 Mbit az előbbi sebesség kétharmadát is eléri. A sebesség alapján a D-Link és az U.S. Robotics hálózati eszközei kiemelkedők, a többi esetén mindig találkozunk a nagyobb leterheltség okozta adatvesztéssel (stream-ek), amely a biztos TCP alapú átvitel esetén enyhe lassulásban nyilvánul meg. A lassulás és a hibaarány közötti határt típustól függően a hozzáférési pontok különbözőképpen kezelik, amelyre az 500 kbites terhelés ad példát: az SMC inkább a sebességből vesz vissza, hogy az UDP csomagok vétele biztos legyen, míg például a LevelOne az átvitt mennyiséget tartja elsődleges szempontnak. Így a TCP fogja ellátni a hibavezérlést.

A mezőny szolgáltatások tekintetében kiemelkedő tagja a *Draytek Vigor 2200W Plus*, amely a korábbi *Vigor 2200* router





vezeték nélküli változata, s értelemszerűen a routolást is elvégzi. Nemcsak ISDN, hanem WAN csatlakozója is van, tehát *ADSL routerként* is használható. A telepítése egyszerű, ám a webes felületen nagyon sok paraméterrel találkozunk (pl. DNS szerverként, DNS szerverhez való beállítás, NAT funkciók), de a szakemberek számára könnyen konfigurálható. Beépített switch-e miatt szinte minden hálózati funkciót el tud látni, és járulékos eszközök vásárlásától sem kell tartanunk addig, amíg viszonylag kis méretű a hálózatunk. Végül, de nem utolsósorban jó hír, hogy a hozzáférési pontok hálózaton keresztül konfigurálható típusainak szinte minden esetben van frissíthető firmware-jük, tehát a hálózat megbízhatósága és sokoldalúsága vélhetően még nőni fog.

PCI adapterek

A hagyományos hálózati adaptereket tökéletesen kiváltó PCI kártyákat szinte minden cég gyárt. Ezek közül is kiemelkedik a *D-Link AirPlus DWL-520+* PCI adapter, amely az *AirPlus* sorozatba tartozik, ami annyit jelent, hogy a vele kompatibilis egyéb AirPlus (vagy más, 22/11 Mbps-szabvánnyal kompatibilis) termékekkel kombinálva 22 Mbps-os sávszélesség elérésre képes. Méréseink szerint napi körülmények között ez ugyan lehetetlen, ám ennek ellenére az AirPlus eszközökből kiépített WLAN hálózat messze kimagaslott a versenytársak közül a sebesség tekintetében. Kifejezetten jónak mondható a biztonság terén is a kártya, ugyanis akár 256 bites titkosítást is használhatunk.

A DWL-520+ egy 32 bites PCI slotba illeszkedő, közepes méretű eszköz, egy

Linksys

Gyártó, típus: Linksys Wireless Network Access Point Router with 4 port Switch BEFW11S4
Forgalmazó: Alphasonic Kft.
Ár: 42 625 Ft
Internet: www.linksys.hu, www.alphasonic.hu

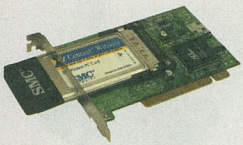
Sebesség	40	50
Telepítés	21	30
Szolgáltatások	18	20

pont 79 Értékelés: felsőkategória

PLUSZ:
- switch is van benne, felár nélkül

MINUSZ:
- nagy leterheltségnél elvet UDP csomagot

SMC



Gyártó, típus:
SMC EZ-Connect PC Card + PCI adapter
Forgalmazó: HRP Hungary Kft.
Ár: 19 900 Ft (csak adapter)
Internet: www.smc.com, www.hrp.hu

Sebesség	20	50
Telepítés	30	30
Szolgáltatások	10	20

pont 60 Értékelés: középkategória

PLUSZ:
- könnyű telepítés, az adapter más kártyát is elfogad

MINUSZ:
- nem Wireless Network-ként jelentkezik be a gépbe

SMC

Gyártó, típus: SMC EZ-Connect 2662W-AR USB adapter
Forgalmazó: HRP Hungary Kft.
Ár: 21 700 Ft
Internet: www.smc.com, www.hrp.hu

Sebesség	20	50
Telepítés	24	30
Szolgáltatások	10	20

pont 54 Értékelés: alsókategória

PLUSZ:
- könnyen telepíthető

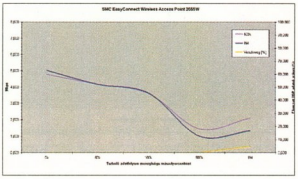
MINUSZ:
- mobil számítógépekkel együtt nehéz mozgatni a rögzítés hiánya miatt

könnyen lecsavarható antennával. A hatótávolság területén közepesnek mondható teljesítményt nyújt, persze ez egy helyhez kötött desktop számítógépnél kevésbé számít. A kártya telepítése tökéletesen plug and play-nek mondható, gyakorlatilag semmilyen problémával nem találkoztunk a teszt során. A mellékelt szoftver segítségével könnyen beállíthatók a működési jellemzők.

Hasonlóan jól használható adapter az *Intel PRO/Wireless 2011B*. Bár a gyártót a legtöbben csak processzorairól ismerik, igen jó névnek számít a hálózati eszközök területén is. Sajnos a 2011B sorszámot viselő 802.11b PCI adaptere nem a legteljesebb mértékben felel meg az elvárásoknak. A készülék működik, használható – csak éppen pont az Inteltől valamivel többet várnánk. Így például hiányzik a 256 bites titkosítási lehetőség.

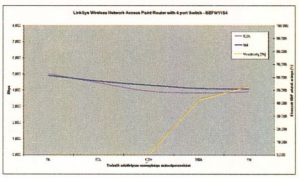
A kártya igen érdekesen néz ki, ugyanis egy „alap"-on, külön csatlakozóval helyezkedik el a vezeték nélküli kommunikációt végző egység (ez egy mini PCI kártya). Ez utóbbin külön csatlakozóval található az antenna is, sőt, még egy plusz csatlakozót is felfedezhet az éles szemű megfigyelő. Ez mintha arra utalna, hogy a cég Access Point-jában is ez a modul dolgozik. Sajnos kicsit „mezei" megoldással, ezen modul rögzítését a kártyán átlátszó ragasztószalag segíti.

Ezen észrevételtől eltekintve, a 2011B telepítése „eseménymentes", és szinte azonnal működik. Sajnos nálunk nem volt képes azonnal megtalálni a tesztlaborban kiépített hálózatot, kicsit játszani



kellett a beállításokkal is.

Külön érdemes megemlíteni az *SMC* által küldött PCI adaptert, amely egy kifejezetten öszvér megoldásnak tekinthető. Bár a cég termékpalettáján található önálló PCI adapter is, szerkesztőségünkben egy PC kártya – PCI adapter, és a hozzá tartozó PCMCIA WLAN adapter tette tiszteletét. Ennek megfelelően a hálózati tulajdonságai megegyeznek a „sima" PCMCIA kártya képességeivel.



Az adapter telepítése a számítógépbe tökéletesen ment, és a kártya behelyezése után a hálózati adapter is „szépen megjelent" az *Eszközkezelőben*. Egyetlen hátránya ennek a megoldásnak, hogy a csatlakozó nem mint vezeték nélküli, hanem mint hagyományos hálózati adapter jelentkezik. Így aztán nem kapunk visszajelzést a rádiókapcsolat minőségéről, csak annyit látunk, hogy 11 Mbps-os hagyományos hálózaton szörfölünk. Sajnos emiatt a Windows XP vezeték nélküli hálózatokhoz szánt konfigurációs felülete nem is használható.

PCMCIA kliens kártyák

Tesztünk valamennyi gyártója küldött vezeték nélküli *kliens adaptert*, amelyek mintaszerűen működtek. A telepítés egy ilyen eszköz esetén csupán a mellékelt

SMC

Gyártó, típus: SMC Easy Connect Wireless Access Point 2655W
Forgalmazó: HRP Hungary Kft.
Ár: 86 075 Ft (PC kártyával együtt)
Internet: www.smc.com, www.hrp.hu

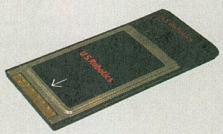
Sebesség	28	50
Telepítés	26	30
Szolgáltatások	12	20

66 pont Értékelés: középkategória

PLUSZ:
- kis méret, könnyű telepítés

MINUSZ:
- kevés extra

U.S. Robotics



Gyártó, típus: U.S. Robotics 22Mbit vezeték nélküli PCMCIA kártya
Forgalmazó: RRC Hungary
Ár: 22 950 Ft
Internet: www.usr.hu, www.rrc.hu

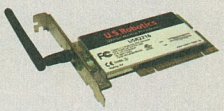
Sebesség	48	50
Telepítés	30	30
Szolgáltatások	12	20

90 pont Értékelés: csúcskategória

PLUSZ:
- kicsi és gyors, 256 bites WAP

MINUSZ:
- kevés hozzá adott program

U.S. Robotics



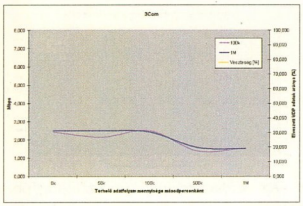
Gyártó, típus: U.S. Robotics 22Mbit vezeték nélküli PCI kártya
Forgalmazó: RRC Hungary
Ár: 28 470 Ft
Internet: www.usr.hu, www.rrc.hu

Sebesség	50	50
Telepítés	30	30
Szolgáltatások	10	20

90 pont Értékelés: csúcskategória

PLUSZ:
- könnyen telepíthető, gyors

MINUSZ:
- kevés hozzá adott program

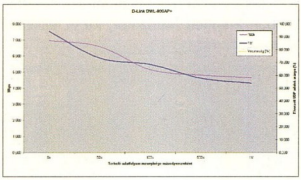


meghajtóprogramon múlik, hiszen az interfész önmagában garantálja a menet közbeni ki- és bekapcsolás lehetőségét. A számítógépet a meghajtó programtól függetlenül egy Windows 9x rendszeren mindenképpen újra kell indítanunk, hiszen a hálózat csak a kliens adapter felismerése után válik láthatóvá. A telepítés mellett egy olyan monitorprogram is a gépre kerül, amely a tálcára ülve láthatóvá teszi a hálózati kapcsolat állapotát. Ilyen programmal az Intel kártyája alapesetben nem rendelkezik, és a monitorprogramban is csak a kapcsolat minőségét tekinthetjük meg, a jel erősségét nem. Különlegessége viszont, hogy a fogyasztás-adáserősség arány több lépésben állítható. Megítélésünk szerint a kisebb adóteljesítmény csupán az elérési ponttól való üzemi távolságot csökkenti, az adatsebességet csak a maximális távolság határán. Ha a munkahelyünkön közel tartózkodunk a hozzáférési ponthoz, akkor ennek a használata mindenképpen előny.

A kártya kialakítása is sokféle lehet, az Intel antennarésze nem magasított, tehát akár a kártya fölött lévő helyre is tehetünk be menet közben kártyát. Még jobb megoldást választott a *3Com*: az antennája becsukható, kinyitásakor a kártya automatikusan keresni kezdi a kapcsolatot.

Apróság ugyan, de az esetek többségében a működést jelző LED más típusoknál akkor világít, ha az valós kapcsolatot talált (a hálózatra be tudunk lépni). Az *U.S. Robotics* kettővel is rendelkezik, de ez egy már működő hálózatnál nem sokat ér. Ennél a típusnál egy kicsivel többnek mértük (kb. 4-5%-kal) az érzékenységet, mint másoknál, az adás biztonsága nagy távolságban pedig a *LevelOne* kártyájánál volt a legjobb.

Csakúgy, mint a hozzáférési pontok esetén, a D-Link és az U.S. Robotics készülékei rendelkeztek 22 Mbites sebességgel, és 256 bites WEP titkosítással. Ha a sebességet nézzük, akkor is ez a kártya volt a legjobb. Mi több, a hozzá tartozó hozzáférési ponttal egyedül ezek a típusok tudtak 2 ms alatti ping időt produkálni. 11 Mbiten már más a helyzet: mindegyik egyenletesen jó sebességet mutatott, ám az Intel kártyájának sebessége erősen ingadozott, ami vélhetően a hozzá tartozó access point jellemzője, hiszen a PCI-os kliens is hasonlóan reagált,



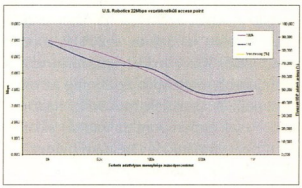
más hozzáférési ponttal viszont jól működött. A sorból kilógott még az SMC kliense, amelynek ugyan nagy sebessége, de igen nagy átlagos ping ideje volt. Ezt a hozzáférési ponttal együtt vizsgálva kiderül, hogy az SMC hálózata a biztonságot részesíti előnyben, és ezért e késleltetés.

Tapasztalatunk szerint nagyobb valószínűséggel fordul elő inkompatibilitás egy nem azonos kliens és a hozzáférési pont között itt, mint egy helyi hálózat kártyái és hub-jai között. Ennek ellenére az egyre jobb firmware-ek miatt lehetséges, hogy a tesztünkben nem működő páros később szóra bírható, de az eltérő márkák párosítását csak indokolt esetben ajánljuk.

USB adapterek

Nagy általánosságban elmondható, hogy a cégek kifejezetten törekednek a minél kisebb adapterek kifejlesztésére, így aztán a verseny leginkább ezen a területen folyik. Sajnos még egyik modell sem volt képes a nagyobb sebességet biztosító USB 2.0 használatára, ezért aztán a 22 Mbps-os átvitel még nem kamatoztatható.

Amint azt tapasztaltuk, az USB adapterek legfontosabb felhasználási területe az



ad-hoc, azaz acces point nélküli hálózatok kiépítésbe lehet. Ennek oka, hogy általában lassabbak, mint PCI vagy PCMICIA társaik, és ez utóbbiaknál kevésbé kényelmesen csatlakoztathatók notebookokhoz.

A *DWL-120* dobozában a telepítő CD-n kívül csak egy USB A-B kábelt találunk. A készülék telepítése teljesen problémamentes, és a tapasztalataink szerint szinte azonnal, mindenféle állítgatás nélkül ké-

Wireless szótár

802.11b – Gyakorlatilag a jelenleg használt WLAN hálózat szabványa. A DSSS kódolás használatával 11 Mbps-os sávszélességet biztosít 2.4 GHz-es frekvencián.

802.11a – A 801.11b „nagytestvére", amely 5.4 GHz-es frekvencián működik, és maximálisan 54 Mbps sávszélességet biztosít – speciális kódolással (OFDM).

802.11g – 22 Mbps sávszélességet biztosító szabvány, a 2,4 GHz-es frekvenciasávon.

Access Point – A WLAN hálózatok központi eleme, amely infrastructure üzemmódban hozzáférést biztosít az egyes hálózati elemeknek. A legtöbb AP a hagyományos vezetékes LAN felé UTP csatlakozóval kapcsolódik, de a drágább modellek különböző extra szolgáltatásokat is nyújtanak, így például DHCP, router, bridge, ISDN és így tovább.

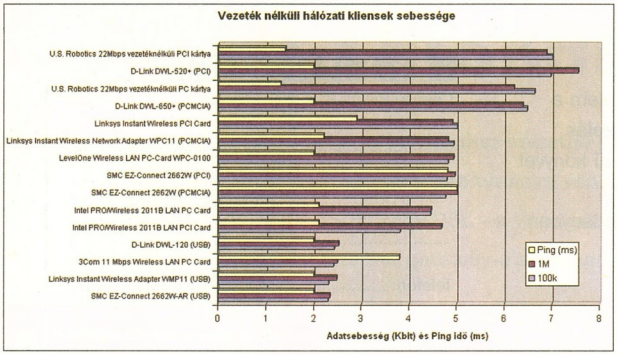
DSSS – A 802.11b által használt kódolási eljárás. Amint a nevéből (Direct-sequence Spread Spectrum) is látható, az átküldendő adatokat a rendelkezésre álló frekvenciatartományban szétosztva továbbítja. Hátránya, hogy körülbelül 22 MHz szélességű csatornát használ.

FHSS – A DSSS-nél lényegesen „hatékonyabb" kódolás a Frequency-hoping Spread Spectrum, amely egy frekvenciát csak egy meghatározott ideig (400 ms) használ. Ennek megfelelően sokkal kisebb az interferencia lehetősége.

MAC – Media Access Control kód. Elméletileg minden egyes, a hálózatban részt vevő elemnek egyedi kódja van, amelyet még a gyártó határoz meg.

SSID – Service Set Identifier. A szóban forgó WLAN „neve"

WEP – Wired Equivalent Privacy. A 802.11b hálózatokon használt biztonsági szabvány. Nem olyan régen többen is bizonyították, hogy a titkosítóeljárás nem nyújt maximális védelmet, így terjedőben vannak az egyéni megoldások is.



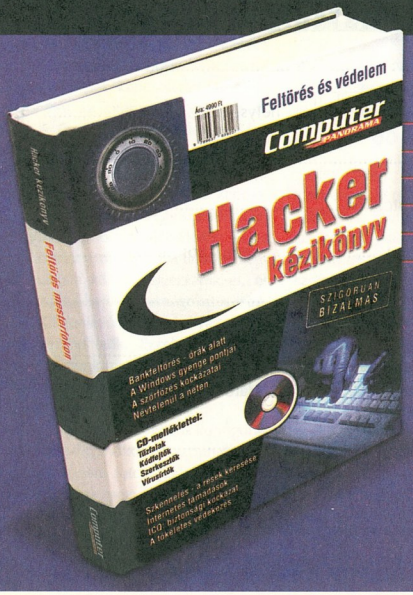
pes csatlakozni a „jelenlévő" hálózatokhoz. Remélhetőleg a gyártó folytatja a fejlesztését, és az USB 2.0 kihasználásával egy 22 Mbps sebességű változatot is piacra dob, mert a mostani USB 1.1-es interfész a cég többi adapteréhez képest bizony nem biztosít megfelelő sebességet.

Bár a többi USB adapterhez képest kicsit nagynak tűnhet, két antennájának köszönhetően jobb vételi lehetőségekkel is rendelkezik a *2662W* névre hallgató, USB 1.1-es interfészhez csatlakozó adapter. Jelen esetben a méret igazán nem számít, hiszen ezen termék legfontosabb felhasználási területe a asztali számítógépek WLAN-ba történő kapcsolása, a „doboz" kinyitása nélkül. Ezen feladatnak az SMC USB adaptere maximálisan képes eleget tenni. Az eszköz telepítése teljesen problémamentes volt, ám csatlakozni nem akart a hálózatunkra. Kis keresgélés után ráleltünk az okra: a hozzánk került egység nem az alapbeállításokon üzemelt, így a hálózati azonosítója (SSID) nem felelt meg a tesztlaborba beállított értéknek. Ezt gyorsan orvosoltuk, és szinte azonnal sikerült is csatlakoznunk a saját hálózatunkhoz.

Külön említést érdemel a *Linksys* USB adaptere, amely talán a legkisebb a hasonló vizsgált eszközök között. A cég szemmel láthatóan a hordozhatóságot tartotta szem előtt, és egy tépőzáras rögzítést is mellékel a *WMP11*-hez. Ennek segítségével vagy a notebook oldalához, vagy pedig az asztali konfiguráció dobozához is „odatapaszthatjuk" az adaptert. Egy apró hibát azért találtunk: érdekes módon nem a hagyományosnak mondható A-B USB kábelen csatlakozik a számítógéphez, hanem A-A típusút használ. Ez akkor lehet hátrány, ha netán drót nélkül szeretnénk valahová magunkkal vinni.

Köhler Zsolt–Rosta Gábor

Feltörés és védelem



- Bankfeltörés - órák alatt
- Internetes támadások
- A tökéletes védekezés
- Támadások a netről
- Jelszófeltörők
- Boncasztalon a trójaiak

Megrendelhető:
Computer Panoráma Kiadói Kft.
1091 Budapest, Üllői út 25.
Telefon: 456-6964, Fax: 456-6970
E-mail: terjesztes@cpanorama.hu
Ára: 4990 Ft

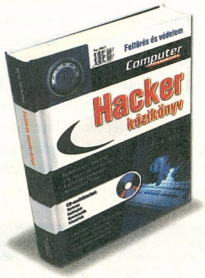
FAX MEGRENDELŐLAP

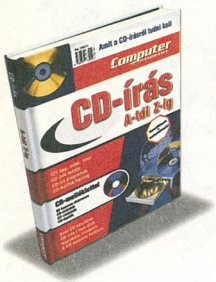
Computer Panoráma
1091 Budapest, Üllői út 25.● Terjesztési osztály: tel.: 456-69-64, fax: 456-69-70

ÚJ

❒ Igen,
megrendelem a
PC-tuningolás
2003 című könyvet
4990-ért
..... példányban

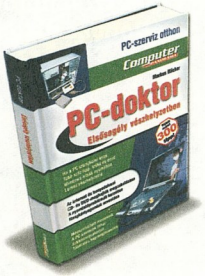
❒ Igen,
megrendelem a
Hacker kézikönyvet
4990 Ft-ért
..... példányban





❒ Igen,
megrendelem a
CD-írás A-tól Z-ig
című könyvet
3490 Ft-ért
..... példányban

❒ Igen,
megrendelem a
PC-doktor
című könyvet
3990 Ft-ért
..... példányban



SZÁMLÁZÁSI CÍM:

Cégnév (név): .....

.....

Kapcsolattartó neve/beosztása: .....

.....

Telefon: .....

Fax: .....

E-mail: .....

Cím: ☐☐☐☐ helység: .....

.....

út/utca/tér:.....

h.sz.:..... em./ajtó: .....

POSTACÍM:

Név: .....

Cím: ☐☐☐☐ helység:.....

.....

út/utca/tér:.....

h.sz.:..... em./ajtó: .....

Telefon: .....

.....

dátum

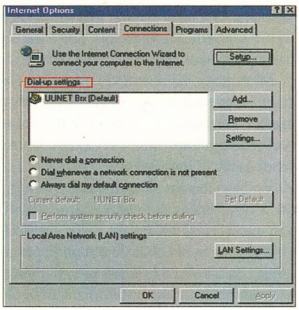
.....

aláírás

Részletes tartalom: **www.computerpanorama.hu/megrendeles** címen.

A fenti áraink a postaköltséget nem tartalmazzák. A küldeményeket utánvéttel postázzuk.

FAX: 456-69-70



Társkeresés

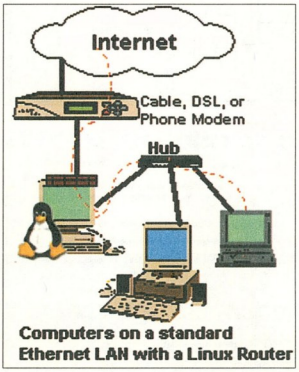
Aki az internethez szeretné csatlakoztatni a hálózatát, annak csak egy telefonvonalra van szüksége. Legyen az analóg, ISDN vagy DSL – a Windows XP-vel bármelyik készülék Internet gateway-é alakítható.

A Windows 98 óta az összes Windows verzió tartalmazza az *Internet Connection Sharing-et* (ICS = Internetes kapcsolat engedélyezés). Az ICS arról gondoskodik, hogy egy otthoni vagy a kisebb irodai hálózat valamennyi PC-jével egy közös modemen keresztül fel lehessen lépni az internetre. Az internetes elérést tartalmazó gépet *hostnak* nevezik, és két kapcsolati eszközzel rendelkezik: egy modemmel (vagy ISDN, illetve DSL kártyával az internetes kapcsolat számára) és a helyi hálózathoz csatlakozó hálókártyával.

A hostot a hálózatban felhasználó többi számítógépet *kliensnek* nevezik. Az ICS segítségével egy kliens nemcsak egy, a hoston futó internetes kapcsolatot képes használni, hanem a hoston keresztül önállóan is képes kapcsolatot létesíteni vagy bontani az interneten. Sajnos nem mindegyik program képes hálózaton keresztül is működni.

Az ICS együttműködik az *Internet Connection Firewall* (ICF = Internet kapcsolati tűzfal) programmal. Ez egy személyi tűzfal program, a hoston aktiválódik és az egész hálózatot védi. Az ICF a host két kapcsolati eszköze között helyezkedik el, és többek között a bejövő csomagokat is megszűri. Az ICF funkciói scriptekkel vagy programmal vezérelhetők. Ezzel a tűzfalban „lyukakat" nyitunk meg, amelyekre egyes a LAN-on futó programoknak van szükségük az internetes kommunikációhoz.

A korábbi ICS verziók kliens konfigurálása nem mindig működött azonnal, számos program nem futott. Ez a helyzet a Windows XP-vel megváltozott. Az ICS-t egy bővítésének köszönhetően könnyű feltelepíteni a kliensekre, lényegesen stabilabban működik, és több alkalmazást támogat. Mindezt a *NAT (Network Address Translation)* NAT *Traversal-lá* történt bővítése teszi lehetővé.



A NAT-bővítés

Egy helyi hálót (LAN) egy proxy-szerveren keresztül – hardveres vagy szoftveres routerekkel – vagy egy NAT szoftverrel, mint amilyen az ICS, csatlakoztatunk az internethez. A szükséges szoftver mindkét változathoz ingyen áll rendelkezésre (proxyként pl. Jana szerver, routerként az XP bridging). A proxyk rugalmasabbak, az alkalmazások számára nagyobb támogatást nyújtanak, a NAT viszont biztonságosabbnak számít. Az ICS a NAT-et használja.

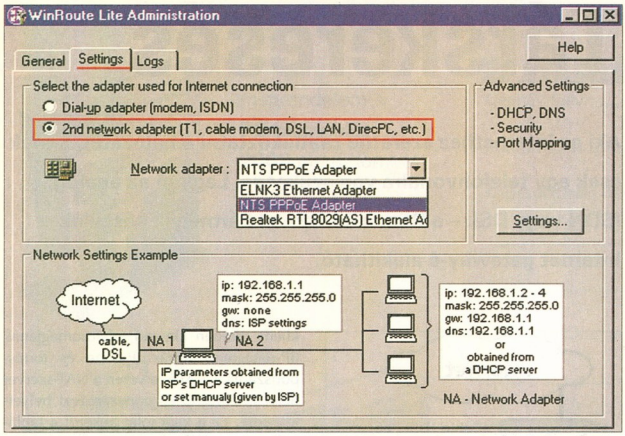
A NAT-nál egy kliens adatcsomagjai a NAT-szerverre kerülnek, amely a kliens nevében az internet felé továbbítja ezeket, a szerver válaszát pedig a LAN megfelelő klienséhez küldi.

Egy NAT-szerver egy hozzárendelési táblázatot vezet, amelyben az összes bejövő és kimenő kapcsolat szerepel. Egy kliens minden kimenő adatcsomagjának (IP-datagram) forrás IP-címe és forrásportszáma a NAT-szerveren a NAT-szerver helyi IP-címével és portszámával helyettesítődik. Ez a kapcsolat bekerül a táblázatba, és a datagram a célszerverhez továbbítódik (IP-Forwarding, routing). Ha a válasz bejövő kapcsolatigényként jön vissza, akkor a NAT-szerver a táblázatban megnézi, hogy létezik-e bejegyzés a kívánt kapcsolathoz (mapping). Ha igen, akkor a datagramot a klienshez továbbítja, ha nem, akkor eldobja.

Az eredeti IP-címnek a host külső IP-címévé történő áttételével a teljes internetes kommunikáció tetszőleges szerverekkel, egyetlen nyilvános IP-címmel, a NAT-szerverén keresztül bonyolódik. A kliens IP-címei nem láthatók az internetről. Ez az egyik ok, ami miatt viszonylag biztonságosnak tartják a NAT-ot. A NAT alapötlete a nyilvános IP-címekkel való takarékoskodás volt, mivel ezek a címek idővel elfogynak. Ennek megfelelően a NAT csak egy átmeneti megoldás addig, amíg az IPv6 elterjed.

NAT-Traversal

A NAT alatt egyes programok nem kapnak engedélyt az internet eléréséhez. Ennek egyik oka az, hogy az érintett alkalmazás nem ismeri fel a NAT-szerver címváltozásait, vagy egy program helytelen vagy fix portszámot tételez fel. Ahhoz, hogy egy LAN-os szolgáltatást el lehessen érni az internetről, a felhasználónak kézzel kell végrehajtania egy *port-mappinget*. Hiányzik az az automatizmus, amely megkönnyítené a felhasználói programok, illetve a NAT-szerver konfigurálását. Egy lehetséges megoldás a *NAT-Traversal*, amelynek a segítségével az alkalmazások

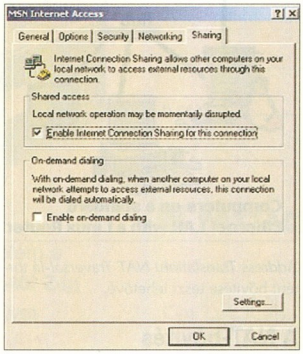


automatikusan megtalálják a NAT-eszközöket, és a hardver-gateway-ket is, és helyesen konfigurálják ezeket. Persze ahhoz, hogy az sikerülhessen, a NAT-eszközöknek UPnP-re (Universal Plug and Play) alkalmasaknak kell lenniük. Az UPnP eszközök, az ICS-hez hasonlóan, két hálózat között közvetítenek, de a helyi hálózati kliens automatikusan programmal vagy script-tel konfigurálhatja őket.

Az alkalmazás a háttérben hozhat létre egy port-mappinget a NAT-szerveren észrevétlenül a felhasználó számára, és az alkalmazás a felhasználó beavatkozása nélkül helyesen fog működni. Ha ICF-et használunk, akkor ott is egy megfelelő port-mappingre van szükségünk, amit egy alkalmazás szintén a háttérben hajt végre az UPnP-vel. E célból az ICF egy programból, akár egy scripttel is vezérelhető. Ez azt jelenti, hogy bizonyos szolgáltatásoknál, mint amilyen például a remote támogatás, hirtelen új port-mappingek bukkanhatnak fel a tűzfalban.

A hardveres gateway-k, mint az ISDN- vagy DSL-router-ek az Internet Gateway Device (IGD) specifikáció betartásával támogatják a NAT Traversalt. Ez elsőként a Windows XP 0.9-es verziójában implementálódott. Az UPnP nemcsak a gateway-k számára ésszerű, hanem mindenféle „hálózatba köthető" készüléknél.

Mindezek a készülékek automatikusan fogják egymást megtalálni a jövő hálózatosított otthonában és helyesen fognak konfigurálódni. Ez az *XP Bridging-re* is vonatkozik, ami egy olyan szoftveres útvonalkeresés (IP-Forwarding), amely nemcsak két hálózat között routol, hanem eltérő médiumok között is, mint az Ethernet és a rádiófrekvenciás hálózatok. Ezzel a funkcióval az XP előtt csak a szerverek rendelkeztek, viszont az XP-nél már a *Home editionben* is megtalálható.



A NAT egy DHCP-szerveren *(Dynamic Host Configuration Protocol)* keresztül automatikusan rendeli a kliensekhez az IP-címeket, amint ezek bejelentkeznek a hálózatba. Eddig a Windows NT és 2000 szerverek gondoskodtak erről. Most már a DHCP szolgáltatásokat a kis Windows 98-as hálózatokban, egy XP-s számítógéppel, drága szerverszoftver nélkül is használhatjuk.

A kliensek az IP-címen kívül automatikusan megkapják az egyéb fontos IP-adatokat is, például a standard gateway, a DNS-*(Domain Name Service)* és a DHCP-szerverek IP-címét. Eddig állandóan egy DHCP-szervernek kellett futnia, ami a kisebb hálózatoktól csak nehezen volt elvárható.

Mi történik, ha a host ki van kapcsolva vagy lefagy, viszont egy új kliens jelentkezik be? Honnan kapja ekkor az IP-címet? A Windows ehhez már a Windows 98 óta rendelkezik megoldással, s ez az *Automatic Private IP Adressing (APIPA)*. Ha a host dinamikus címhozzárendelésre van beállítva (DHCP), és nincs elérhető DHCP szerver, akkor az APIPA ad IP-címet a hostnak a 169.254.0.0/16 tartományban – a helyi hálózat ezen tartományában kiosztott címek figyelembevételével.

A DNS-proxy rejtve működik. Gondoskodik az *FQDN-ek (Fully Qualified Domain Names)* átalakításáról. A kliensek DNS-Resolver kéréseinek továbbítása és a DNS-szerverek válaszának átvétele szintén a DNS-proxy feladata.

Abban a pillanatban, amikor az ICS-t bekapcsoljuk a hoston található kijelölőnégyzettel, automatikusan aktiválódik az *IP-Forwarding* is. Azt, hogy be van-e kapcsolva, úgy ismerhetjük fel, hogy egy parancsot adunk ki a parancssorba. Hívjuk meg a *Start/Minden program/Kellékek* menüt, majd adjuk ki az *ipconfig/all* parancsot. Ha az IP-Forwarding aktív, akkor a hoston az *IP-Routing aktív Igen/Nem* kimenetet látjuk.

Ugyanez a parancs egy DHCP-kliensen többek között az *Automatikus konfigurálás aktív, Igen/Nem* kimenetet eredményezi, amit a hálózatot telepítő varázsló készít el. Így a kliens önállóan találja meg a LAN-on az ICSA-hostot, és ettől IP-konfigurációt kaphat.

Egy kliens bármikor meg tud nyitni egy kapcsolatot automatikus hívással *(AutoDial)* a hoston, amint ezt egy alkalmazás kéri, és a hoston engedélyezve lett az AutoDial. Azonban a mai programok számtalan kapcsolatteremtési kísérletét figyelembe véve, ez a beállítás nem javasolható. Amint a host bebootolt, az XP klienseken automatikusan megjelenik egy új bejegyzés a telefonos hálózatban, amelyyel a kapcsolat létrehozható, illetve bontható. Ha a host nem elérhető, akkor ez a bejegyzés eltűnik.

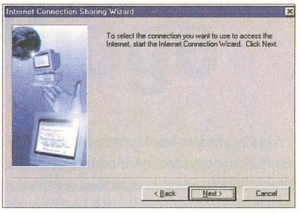
Telepítés

Az ICS telepítését a hoston a hálózattelepítő varázsló végzi, amelyet a *Minden program/Kellékek/Kommunikáció* alatt találunk a *Start* menüben. Az ICS-hez egy

működőképes TCP/IP hálózatra és internet-kapcsolatra van szükség. Mindkettőt ezzel a varázslóval is el lehet intézni. Az internet-hozzáférés interfészének és néhány további egyszerű adatnak a megadását követően a folyamat azzal a figyelmezetéssel záródik, hogy ezt a varázslót a LAN többi PC-jén is le kell futtatni, és ehhez egy flopi elkészítését javasolja. Ezen csupán a *Netsetup.exe* program található (320 Kbájt), és a kliensen kell futtatni.

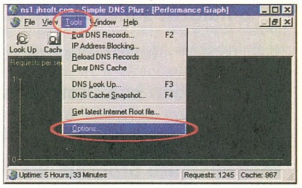
A Microsoft szerint valamennyi Windows 98/Se/ME kliens szóba jöhet, a Windows 2000 viszont nem. Az XP klienseken vagy a hálózattelepítő varázslót használjuk, vagy a Windows XP CD-ről telepítjük a hálózatot. Ehhez válasszuk a CD *Start* menüjében az *Egyéb feladatok végrehajtása/Céges vagy otthoni hálózatok kliensének telepítése* menüpontot.

A *Windows 2000 Professional-lel* végzett kísérletekből kiderült, hogy ez a rendszer is képes egy XP-ICS-hoszttal együttműködni. Az *ipcongif /renew* paranccsal lehet új IP-adatkészletet kérni a hosttól. Ezt követően az ICS csodálatosan működik. Kétes esetben a Microsoft hálózattelepítő csodagyógyszere, a hálózattelepítő varázsló futtatása segíthet.

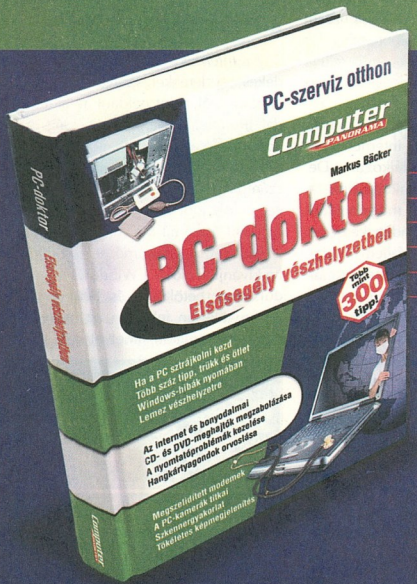


Összegzés

Az ICS-sel olyan alkalmazásokat üzemeltethetünk, mint a web-, az FTP- vagy a News-kliensek. Még az Outlook is működik, így a kisebb hálózatokban feleslegessé válik egy mail-szerver. Nem fog már soká tartani, és még több NAT-Traversalre alkalmas szoftver jelenik meg a piacon, és ezzel egyre több alkalmazás kap internetelérési lehetőséget a LAN-on. Addig azonban kétes esetben mégis csak egy proxy-megoldást kell használni. Az XP saját alkalmazásai, mint az audio- és videokonferenciák, a Remote Desktop, valamint az alkalmazások közös használata, egy *ICS-host mögött futnak*. A tűzfalon történő önhatalmú portmegnyitás sokak számára gyanús lehet, ám nincs más megoldás. Ha nincs port-mapping, akkor internet-hozzáférés sincs. Ez az automatizmus nem várja el a felhasználó beavatkozását, hű marad a Windows filozófiához: legyen a felhasználó dolga minél egyszerűbb, hogy elfogadja a terméket, s ilyenkor a biztonság néha elhanyagolódik. Ezért mindig töltsük le az XP legújabb biztonsági patch-eit, amelyek betömik az UPnP réseit.



Több száz tipp, trükk és ötlet közel 500 oldalon!



- Ha a PC sztrájkolni kezd
- Windows-hibák nyomában
- A nyomtatóproblémák orvoslása
- Szkennergyakorlatok
- Tökéletes képmegjelenítés
- Megszelídített modemek

Megrendelhető:
Computer Panoráma Kiadói Kft.
1091 Budapest, Üllői út 25.
Telefon: 456-6964, Fax: 456-6970
E-mail: terjesztes@cpanorama.hu
Ára: 3990 Ft

A cikkben szereplő, a hálózati diagnózisban segítő programokat CD-mellékletünkön is megtalálhatják.

Pillantás a

Aki hálózatban dolgozik, bizonyára kíváncsi a kapcsolati jellemzőkre, az ellenállomásokra, a hálózat sebességére és leterheltségére. A cikkünkben bemutatott és a CD-mellékletünkön is megtalálható programokkal mindezek az információk egyszerűen megkaphatók.

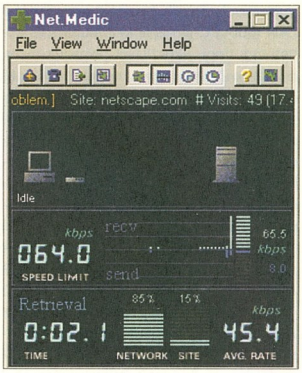
A hálózatok mindig azonos szempontok alapján épülnek fel: van egy vagy több szerver és vannak a számítógépek, amelyek *ügyfélként* vagy *munkaállomásként* csatlakoznak. A belső céges hálózatban a sebesség és elérhetőség szempontjából rendszerint nem merülnek fel problémák. Itt a rendszeradminisztrátor gondoskodik a zökkenőmentes üzemről. Érdekessé akkor válik a helyzet, amikor a világhálón közlekedünk. A nagy hálózatban számos különböző, függetlenül számítógépen jutunk keresztül úgy, hogy észre sem vesszük. Eközben egyre-másra üzemzavarok vagy rendszerlefagyások léphetnek fel. Ha egyes gépek nem érhetők el, akkor az internet átgondolt hálózati topológiájából profitálhatunk. Az A-ból Z-be irányuló kérdésünk sosem a közvetlen úton halad, hanem különböző, pl. a C, G, O és P szervereken keresztül. Ha az útvonalban egy számítógép meghibásodik, akkor egy másik szerver veszi át a feladatát. Ha követni szeretnénk a kérdésünk útját, akkor egy úgynevezett *Trace-útvonalat* választhatunk. Ilyenkor egy IP-csomag egy megadott cél felé indul. Az interneten az IP-csomag különböző szervereken, routereken és kapcsolókon keresztül jut el a célhoz. Minden olyan alkalommal, amikor az adatcsomag egy idegen komponensen (Hop) halad keresztül, akkor ez a komponens a feladó állomásnak elküld egy loopback-csomagot a saját IP-címével. Ezáltal részletesen feljegyződik a számítógépünktől a kívánt címig (FTP, News, Mail vagy www) terjedő út.

Ha egy adott honlapot nem tudunk elérni, akkor egyszerűen kiadunk egy *PING utasítást*. Ezt a legkönnyebben a következőképpen képzelhetjük el: A kívánt ellenállomásnál bekopogunk az ajtón, és amint valaki „szabaddal" felel, választ kapunk. Ha senki sincs otthon, úgy erről is értesítést kapunk. Ha érdekel, hogy ki húzódik meg a **www.cp.hu** cím mögött, akkor kiküldünk egy *WHOIS kérdést*. Ekkor részletes információkat kapunk a cégről, a rendszeradminisztrátorok kapcsolati adatairól és az IP-tartományok adatairól. Ennek akkor van értelme, ha mondjuk egy hacker-támadás áldozatai voltunk, és a támadó IP-címét szeretnénk azonosítani.

Még informatívabbak azok a programok, amelyek az *adatáramlás sebességét* is mérik. Ha egy ISDN-es internetes kapcsolat esetén mindig csak néhány bájtot kapunk, akkor feltehetőleg túlterhelt a szolgáltatónk vagy a felkeresett honlap. Ilyenkor bontsuk a kapcsolatot, és építsük fel újra. Ez az esetek többségében segít. Ha nem, akkor egy későbbi időpontban kísérletezzünk.

Net.Medic 1.22

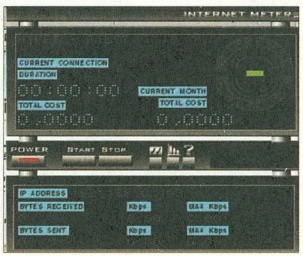
Lassú kapcsolat, lomha adatátvitel, megszakadó kapcsolat – az internen egyre-másra ilyen gondokkal találkozunk. De vajon ki a bűnös? A számítógépünk, a modem, a szolgáltató vagy maga a szerver? Nos, a *Net.Medic* minden kérdésre választ ad, s kíméletlenül felfedi a hiányosságokat. Valamennyi összetevőt analizálja, és áttekinthetően, grafikusan ábrázolja. Ismeri valamennyi internetes kapcsolatfajtát a Windows 95 és az NT alatt, függetlenül attól, hogy LAN-os vagy modemes hálózati kapcsolatról van-e szó. A modemes online kapcsolat esetén még az elért adattömörítési viszonyt is megmutatja. Valamennyi részletet individuálisan jeleníthetünk meg, vagy kizárhatunk a megjelenítésből. Ezen kívül további információkat kérhetünk a szolgáltatóról, vagy egy szerverről, amennyiben ezek elérhetők. A Net.Medic statisztikákat készít az online hálózatokról, az adatátviteli sebességekről, a válaszidőkről és még sok



egyéb jellemzőről. Ha a Net.Medic felismer egy problémát, amelynek oka a PC-nken kívül esik, akkor a pontos hibaleírással elkészít egy e-mailt, amelyet azonnal elküldhetünk a szolgáltatónak.

Internet Meter 2.Ob

Az *Internet Meter* nevű program is érdekes részletekkel szolgál az internetes kapcsolatról, mint például az aktuális oldal IP-címe, a letöltési sebesség, a küldött, illetve a fogadott bájtok száma, a futó kapcsolat költségei és egy megadott elszámolási időszak összköltsége. A tényleges online időt statisztikai alapon méri, és azonnal átszámítja a mindenkori díjtételek szerint. A programot telepíteni kell, s ha kívánjuk, akkor a Windows minden indulásakor betöltődik és beül a tálcára. Automatikusan felismeri az összes internetes kapcsolatot, amelyet egy modem-

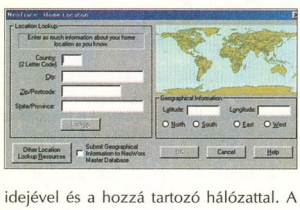


színfalak mögé

mel, egy ISDN kártyával vagy egy ADSL-modemmel építettünk fel. Egy diagramban az összes eddigi kapcsolatot láthatjuk, így gyorsan áttekintést nyerhetünk a saját böngészési jellemzőinkről. Mindennek az az előnye is megvan, hogy a következő számlánál nem fogunk túlzottan meglepődni, és nem lépünk túl egy meghatározott keretet.

Neo Trace 2.12a

A *Neo Trace* egy kedves kialakítású grafikus *tracerouter,* amely részletesen megadja egy lekérdezés útvonalát. Megméri valamennyi csomópont reakcióidejét, megjeleníti a meghatározott sebességet, a lekérdezett oldal tartománynevét, IP-számát és postacímét. Négy különböző nézet között választhatunk: világtérkép a saját helységünkkel mint kiindulási ponttal, a köztes állomásokkal és a célponttal. A *Nodes* üzemmódban valamennyi érintett számítógépet láthatjuk a DNS címekkel és a válaszidőkkel, valamint a helyszínek országászlóival. A *List* nézetben valamennyi számítógép egy táblázatban jelenik meg az IP-címével, nevével, válasz-



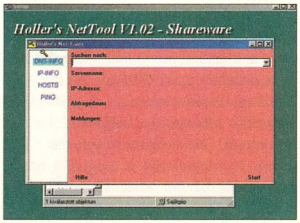
idejével és a hozzá tartozó hálózattal. A *Graph* nézetben ugyan kevesebb részletet láthatunk, viszont megjelennek a válaszidők chart-ként. A részletes jelentéseket archiválás céljából szöveges vagy HTML formátumban tárolhatjuk el. A trace útvonalon kívül ping-elhetünk is.

Genius 3.0

A *Genius* voltaképpen egy több mint 30 különböző segédprogramot tartalmazó *komplex programgyűjtemény,* minden felhasználónál meg kellene lennie. A telepítését követően a Tray-listában jelenik meg. A jól áttekinthető rovatok szerint tagolt modulok egy kattintással azonnal elérhetők. A *Clipboard* alatt az aktuális IP-címet és host-nevünket tehetjük ki a vágólapra. Ez különösen az online játékosokat érdekelheti. Az *Internet-Clients* rovatban saját FTP- és Telnet-klienst, egy egyszerű böngészőt, a FINGER, PING, TRACE segédprogramokat, valamint az idő egy timeszerverrel történő aktualizálását és a WHOIS lekérdezést találjuk. A Genius az *Internet-Tools* menüpont alatt is mindent kínál, amire csak vágyhatunk. A postafiókunkból lekérdezhetjük az új üzeneteket, egy lépésben kiüríthetjük, FTP-keresést indíthatunk, a hacker-betörések ellen figyeltethetjük a portokat, informálódhatunk az aktuális kapcsolatról, valamint az IP-cím felől. Még egy tetszőleges internetes oldal linkjeit is ellenőrizhetjük. Egy kattintás az egérrel, és az aktuális időjárás-térképet látjuk. Mindehhez néhány szervezési segédprogram is társul, mint például a Windows címjegyzék közvetlen elérése, jegyzetlap, jelszó-adatbázis, egy emlékeztető funkció, és egy teendők (to-do) lista. A terjedelmes gyűjteményt *néhány windowsos segédprogram* egészíti ki.

Holler's Net Tool 1.02

Ez a program három modult tartalmaz. A *DNS-Info-lekérdezéssel* egy IP-címből határozhatjuk meg a hozzá tartozó tartománycímet. Az *IP-Info* éppen fordítva működik: egy IP-címhez tartozó tartomány nevét határozza meg, ha az illetékes tartományszerver támogatja ezt a funkciót. A *Hosts* egy windowsos számítógép host fájlának a kényelmes feldolgozásáról gondoskodik. Sebességnövelést



eredményez, mert minden alkalommal, amikor egy URL-t, mint például **www.computerpanorama.hu** begépelünk a böngészőnkbe, a háttérben egy DNS lekérdezés indul a szolgáltatónk szerveréhez, amelyik a tényleges IP-címet ismerteti. Az ellenállomással csak az IP-címmel történhet a kapcsolat felvétele. Ha azonban a DNS neveket helyileg a host fájlban tároljuk, akkor nincs szükség az online lekérdezésre, és a kívánt oldalak már néhány másodperccel korábban is a rendelkezésünkre állnak. A gyűjteményt egy PING modul teszi teljessé, amellyel tetszőleges ellenállomás elérhetőségét és tényleges reakcióidejét lehet ellenőrizni.

BeMuNet 1.0

Ha ezt a hálózatfelügyelő és távkarbantartó modult egy gépen *mint szervert* telepítik, akkor a LAN-on pillanatnyilag elérhető valamennyi BeMuNet kliens-t automatikusan felismeri. Telepítésre, vagy bizonyos portok, esetleg számítógépnevek nehézkes beállítására nincs szükség, így a BeMunet kiválóan megfelel iskolákban, egyetemeken, továbbképző intézetekben, kiseb gyárakban és cégeknél. A rendszeradminisztrátor észrevételenül megtekintheti aktív alkalmazást és screenshots-okat készíthet. A webböngésző valamennyi felkeresett weblapját is ki lehet értékelni. Ha a kollégák túl sokat játszanak, akkor küldhetünk nekik egy e-mail-t. A rendszeradminisztrátorok mindenekelőtt a távvezérlő funkciókat fogják értékelni. A *Blackscreen* funkcióval például egy vagy valamennyi kliens letiltható. A felhasználó ilyenkor csak egy fekete képernyőt lát, hiába ütögeti a billentyűket. Ezen túlmenően a kliensek kikapcsolhatók, újraindíthatók, egyes felhasználók kiés bejelenthetők.

EldoS Pinger 1.41

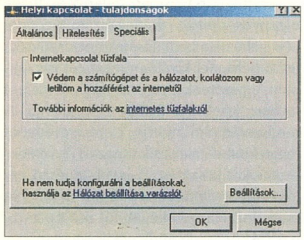
Az *EldoS Pinger* online segédeszköz: az adott ellenállomással fennálló internetes kapcsolat tesztelésére szolgál. Ellenőrzi az internetes kapcsolat státuszát, és beszámol a ping-lekérdezés minimális, maximális és átlagos idejéről. Eközben a szakadásokat (hálózati zavarokat) is számolja. Igen kedvező, hogy az információkat grafikus alakban jeleníti meg, s kérésre valamennyi lekérdezést naplófájlba írja.

Tűzfalprogramok
CD-mellékletünkön megtalálhatnak több, a cikkben is szereplő tűzfalat.

A falakon át

A mai tűzfalprogramok már szinte kivétel nélkül képesek bezárni a portokat. Persze az erősségüket és a gyengéjüket akkor árulják el igazán, amikor egy hackertámadás éri őket. Lássuk, hogy ki, mit kínál a biztonság területén.

A *Windows XP* megjelenése óta egy *operációsrendszer-tűzfal* is létezik. Ezzel nemcsak a céges munkaállomásnak szánt professzionális verziót erősítették meg, hanem az otthoni Windowsnak is a részévé vált.



A Windows XP-nek saját tűzfala van

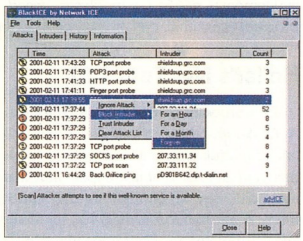
Kattintsunk a *Start/Vezérlőpult* menüben a *Hálózati kapcsolatok* modulra. Itt hívjuk elő az egér jobb oldali gombjával a *Helyi kapcsolatunk* szimbólumot, és válasszuk a *Tulajdonságokat*. A *Speciális* regisztrelapon jelöljük ki az *Internet kapcsolat tűzfalát*, és ettől kezdve már védelem alatt szörfözhetünk. Persze ezzel még nem érezhetjük túl nagy biztonságban magunkat, mert sajnos az XP-tűzfal nem sokat tud. Az egyik nagy gyengéje például, hogy nem foglalkozik az olyan programokkal, amelyek a számítógépünkről kívánnak kapcsolatot létesíteni az internettel. Az ingyenes Microsoft termék tehát nem károsította különösebben a tűzfalkészítőket, még a freeware termékek is többet tudnak nála. Egyes segédprogramok az adatcsomagok szűrésén kívül képesek veszélyes scripteket keresni a weblapok tartalmán, cookie-kat menedzselni, reklámokat kiszűrni és teljes oldalakat letiltani a gyerekek vagy a böngésző kollégák elől.

Számos tűzfal víruskeresőkkel együtt érkezik. Ez nem mindig számít jó üzletnek, mert egy olcsó tűzfallal és egy freeware szkennerrel gyakran jobban járunk. Ha azonban amúgy is akartunk vírusszkennert vásárolni, akkor célszerű csomagban megvenni, a tűzfallal együtt.

BlackICE Defender 2.1

A *BlackICE Defender 2.1* valójában nem tűzfalprogram, hanem *Instruction Detection System (IDS)*. Négy biztonsági fokozatban vizsgálja a bejövő forgalmat, és a NetBIOS Filesharing problémával is foglalkozik.

A BlackICE biztonsági modellje a rendszer- és alkalmazási portok megkülönböztetésében rejlik. A rendszerportok száma 0-tól 1023-ig terjed, valamennyi magasabb portszám alkalmazási porthoz tartozik. A program a beállított biztonsági fokozattól függően vizsgálja a rendszerportokat, az alkalmazási portokat vagy mindkettőt, de mindig csak a bejövő forgalom portjai érintettek. Ez azt jelenti, hogy a „honvágyas" programokat, így például a trójai falovakat nem ismeri fel! Tehát eleve nem szűri az internetre menő forgalmat.



A BlackICE Defender kilistázza a támadásokat

A program igazi erőssége persze a támadások felismerése. A BlackICE Defender felkutatja a betolakodókat, az IP-címmel NS-lookup-lekérdezést hajt végre, és megjeleníti a megtalált nevet. Erről néha már fel lehet ismerni, hogy a betolakodó honnan jött.

Az IDS egy támadásablakban listázza ki a felismert támadásokat. Így egy bejegyzés helyi menüjében is le lehet tiltani egy támadót. Ha egy támadást kijelöltünk, akkor a program az *advICE* kapcsolóval megjelenít egy weblapot, a támadás típusának információival. A BlackICE angol nyelvű dokumentációja is mintaszerű, valamennyi vizsgált termék közül a legrészletesebb.

További infók: www.networkice.com

eSafe Desktop 3.0

Az *eSafe Desktop* voltaképpen egy átfogó biztonsági program és a vírusok, trójai falovak, kéretlen scriptek ellen is véd. Így már érthető, hogy a program egy vírusszkennelőt és egy sandbox-ot, valamint egy rendszermonitort is tartalmaz, bizonyos fájlok változtatásainak a követésére.

Az eSafe sandbox-a határozza meg, hogy egy program hogyan érheti el a mappákat és mely fájlokat futtathatja

A biztonsági elv alapját a *sandbox-technológia* képezi. Mindegyik programhoz egy sandbox-ot lehet definiálni, amely meghatározza, hogy mit szabad a programnak, mely mappákhoz, hogyan férhet hozzá. A program nem léphet ki a sandboxból, így egy veszélyes kód, megfelelő konfigurálás esetén, nem okozhat kárt.

A program *desktop-firewall* modulja a portok felhasználását ellenőrzi. Ehhez különböző előre definiált készleteket használ, amelyek valójában portkorlátozások. A *Trojan Hackers Ports* készlet például olyan portokat tartalmaz, amelyeket előszeretettel használnak a trójai programok, s azok ebben a készletben inaktívak. Per-

Tűzfaltitkok

A tűzfal beépül a számítógép és az internet közé, teljesen elszigetelve őket egymástól. Minden egyes bejövő és kimenő adatcsomagot megvizsgál, majd határoz az átengedésükről, illetve a blokkolásukról. Mindezt persze úgy valósítja meg, hogy nem teszi lehetetlenné a normál szörfözést folytonos akadékoskodással, a jogosulatlan behatolásra ugyanakkor mindig figyelmeztet. Arra is kapható, hogy meghatározott IP-címekről teljesen blokkolja az adatforgalmat, illetve csak egy adott webkiszolgálóval engedélyezze a kapcsolatot létesítését.

Egy tűzfal használatának persze csak akkor van értelme, ha az minden biztonsági lyukat betöm, vagyis mindkét irányban megakadályoz mindenféle jogosulatlan adatforgalmat. A külső behatolásokkal szemben úgy nyújt védelmet, hogy a kapcsolódásra használatos portokat – és így magát az internetre kapcsolt számítógépet is – láthatatlanná teszi a külvilág számára. A belülről kifelé irányuló adatátviteli próbálkozásokat pedig jelzi a felhasználónak, aki eldöntheti, hogy mely programoknak engedélyezi az adatforgalmazást (ezek közé tartozik például a webböngésző és a levelezőprogram).

sze aaját készleteket is definiálhatunk. A készletek szabályokat tartalmaznak, amelyek a port felhasználásáról rendelkeznek. A porton bonyolódó adatforgalmat a szabály minden portjához egyenként lehet beállítani. Ez lehet bejövő, kimenő, vagy kétirányú. Ezt a portot ki vagy be lehet kapcsolni. Mindegyik szabályhoz létezik kivétel is. Ezek olyan hostok, amelyekre a szabály nem vonatkozik. A hostokat a nevükkel vagy az IP-címükkel lehet megadni.

Az *Application-Firewall* modul a telepített programok internetes hozzáférésére felügyel. Hozzáféréssel csak az olyan internetes programok rendelkeznek, amelyek egy előre definiált sandbox-ban helyezkednek el. Ha egy másik program szeretne internetes kapcsolatot létesíteni, akkor lép a színre a modul, és csak az engedélyezés után valósulhat meg a hozzáférés. Az eSafe-nek nincsenek további tűzfalfunkciói, viszont van egy tartalomszűrője. Ez tiltott szavak után keresve végigböngészi az e-mail-címeket, valamint a hírcsoportneveket és fájltartalmakat. A készlet egy tiltott szavakat tartalmazó listából áll. Az előre definiált listák olyan témákat tartalmaznak, mint például hackerek, rasszizmus vagy drogok. A másik jellegzetesség a definiálható karaktersorozatok kódolása. Megadhatunk egy hitelkártyaszámot, s ezt minden alkalommal kódolhatjuk, amikor az interneten továbbítjuk.

További infók: www.esafe.com

Freedom Security & Privacy Suite 3.2

A *Freedom-nál* a PC-nken futó valamennyi alkalmazáshoz külön definiálhatjuk, hogy hozzáférhet-e az internethez vagy sem, hogy működhet-e szerverként, és hogy minden kapcsolatfelvétel előtt előbb kérdeznie kell-e. A felhasználó ezen kívül általánosan vagyis együttesen ki- és bekapcsolhatja a protokollokat. Sokkal több konfigurációs lehetőség nem kínálkozik, de nem is szükséges. A Freedom alapértelmezetten az Ident-port (113) kivételével valamennyi portunkat *stealth* (láthatatlan) állapotba hozza. Az Ident-portot kézzel kell kikapcsolnunk. Az ehhez szükséges opciót a program paraméterezésénél találhatjuk.

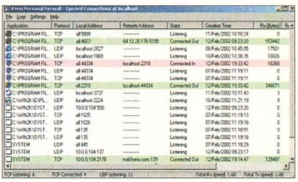
A Freedom kiegészítő funkciókat is kínál: víruskeresőt, reklámtiltót és weblapcenzort. Ezen funkciók kezelése azonban kissé nehézkes, a felhasználónak kézzel kell elkészítenie a tiltott weblapok vagy címszavak jegyzékét.

Kerio Personal Firewall 2

A program a *Tiny Personal Firewall 2.x utódja*. A *Kerio* freeware, és tisztán *csak a tűzfalfunkciókra* korlátozott. Víruskeresőt vagy tartalomellenőrzőt hiába is keresünk.

A konfigurációhoz több biztonsági funkciót is kínál, amelyekhez a felhasználó szabályokat definiálhat. A biztonsági fokozat szintjét attól függően a feljebb vagy lejjebb srófolni, hogy egy megbízható hálózaton vagy az interneten mozgunk-e. A szabályok definiálásánál a Kerio tűzfal rugalmas: lehetőség van a portok, a megbízható hostok, valamint a bejövő vagy kimenő kapcsolatok kiválasztására.

Amikor elindítunk egy internetes programot, például az Internet Explorert, akkor a Kerio rákérdez, hogy engedje-e vagy tiltsa-e a kapcsolatot, és ennek megfelelően maga fogalmaz meg egy szabályt. Ezeken a felhasználó kézzel még változtathat.



A Kerio párbeszédablaka részletes információt mutat valamennyi nyitott kapcsolatról

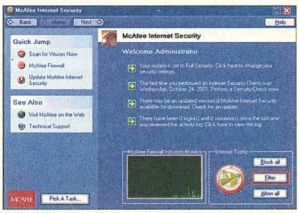
A Kerio a biztonság tekintetében *a középmezőnyben* helyezkedik el. A tűzfal valamennyi portot stealth állapotba hozza, felismeri a módosított levelezőprogramot. A Kerio az egyik legolcsóbb megoldás a számítógép védelmére, s némi hálózati ismeretet feltételezve, könnyen lehet a speciális igényekhez alakítani.

További infók: www.kerio.com

McAfee Internet Security

A *McAfee* egy *teljes biztonsági csomagot* állított össze az *Internet Security-vel*. A tartalomszűrővel is felruházott tűzfalon kívül tartalmazza a McAfee víruskeresőt és egy fájl-shreddert is. A program valamennyi telepítési lépésen végigvezeti a felhasználót, és a PC biztonsági ellenőrzését is elvégzi. Eközben cookie-kat és webbug-okat keres a merevlemezen, meghatározza az internetes programokat és azt, hogy hol tárolódnak a magánadatok.

Valamennyi internetes kapcsolatot kérő programot egy listában kezel. A felhasználó minden bejegyzésről külön eldöntheti, hogy szabad-e adatot cserélnie az adott szoftvernek, és ha igen, mely porton keresztül teheti ezt. Kissé el van-



A McaFee egy komplett csomagot kínál

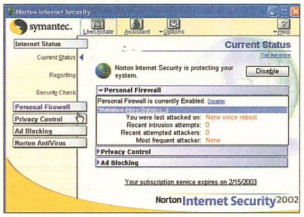
nak rejtve az olyan beállítások, mint a DHCP és ICMP – ezekhez a felhasználónak egy külön menübe kell belépnie, amely a rendszer hálózati adapterein tartalmazza. A beállítási lehetőségek meglehetősen soványkák: az ICMP-t csak ki vagy be lehet kapcsolni.

A McAfee program leginkább kritizálható részei a hiányzó beállítási lehetőségek és a szokatlan kezelői felület. A funkciókat több modulban szétosztották (*Internet Security, Firewall, VirusScan*). Egyeseket olyan almenükben kell megkeresni, amelyek a *Taszk futtatása* kapcsoló mögött húzódnak.

További infók: www.mcafee.com

Norton Internet Security 2002-10-07

A McAfee Internet Security-hez hasonlóan, a *Symantec* terméke is egy *komplett biztonsági csomag*, amely a tűzfaltól a víruskeresőig mindent tartalmaz. Standard és professzionális kivitele is létezik, az utóbbi a PalmOS-hez való víruskeresőt és egy olyan segédprogramot is tartalmaz, amellyel a munkatársakat lehet megakadályozni a böngészésben. A tesztünkhöz a standard verzió állt rendelkezésre.

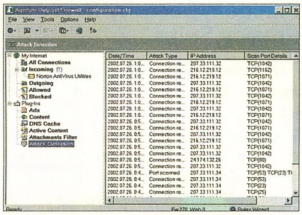


A Symantec terméke is egy komplett biztonsági csomag

A beállításokat a felhasználó kétféleképpen végezheti el. Egyfelől meghatározhatja, hogy *milyen hozzáférési jogokkal rendelkezzenek az internetes programjai*, másfelől *általános szabályokat* definiálhat, és így portokat tilthat és bizonyos számítógépeket megbízható hostnak nevezhet ki. Ehhez a Symantec tűzfala előkészítő munkát végez. A szoftver a számítógépen felkutatja az internetes alkalmazásokat és általános biztonsági szabályokat fogalmaz meg. Ez előnyös, mert a tűzfal kezdettől fogva, a felhasználó beavatkozása nélkül, valamennyi portot stealth állapotba állít. A hátránya viszont, hogy a felhasználónak vigyáznia kell az új szabályok definiálásánál. Előfordulhat, hogy ilyenkor a számos előre definiált szabállyal konfliktusba kerül, és nem várt eredményt kap. Itt bizony hálózati ismeretekre és némi betanulási időre van szükség.

További infók: www.symantec.com

Outpost Firewall 1.0



Az Outpost felülete az Intézőére emlékeztet

A program különlegességét az adja, hogy bedolgozók (plug-inok) készíthetők hozzá, így bárki kiterjesztheti a képességeit. Szolgáltatásai egy részét (így például a levélmelléklet-szűrést és a hirdetésblokkolást) már most is bedolgozók valósítják meg. A Windows Intézőjére emlékeztető barátságos programfelületen könnyen megtalálhatók a szolgáltatások és a beállítási lehetőségek, akár a menüket, akár az eszköztárat használjuk. Szinte nem is kell változtatni a biztonsági konfiguráción: az alapbeállítások a legtöbb felhasználó számára úgy jók, ahogy vannak. Figyelemre méltók a testre szabási lehetőségek is: tág határok között változtatható, hogy a program milyen információkat jelenítsen meg az adatátvitelről, a behatolási kísérletekről, az átengedett és a blokkolt adatcsomagokról, a meglátogatott webhelyekről.

Többnyelvű program lévén telepítéskor az angol mellett más nyelveket is felkínál. A magyar egyelőre nincs a lehetőségek között, ami azért különös, mert a gyártó webhelyéről egy pdf formátumú, magyar nyelvű dokumentáció is letölthető, amelynek képernyő-illusztrációi magyar nyelvűek.

Ötféle biztonsági szint közül választhatunk, az internetezésre használt programok pedig három kategóriába sorolhatók (megbízhatók, blokkoltak és szabály alapján szűrtek). A tesztelés során teljes védelmet nyújtó, 2,7 Mbájtos letöltési méretű Outpost használata ingyenes.

További infók: www.agnitum.com

Secuties Personal Firewall

A *Secuties Personal Firewall* névvel az Agnitum-féle *Outpost Firewall Prót* illetik. A program freeware verzióját a **www.agnitum.com** címen kaphatjuk meg.

A freeware verziónak nincsen jelszavas védelme és a nemkívánatos internetes lapok letiltására alkalmas funkciója sem. A Pro verzió ezen túlmenően több konfigurációt képes készíteni és eltárolni is.

A tűzfal beállításait szintén az internetes alkalmazások jogosultsági kiosztásával végezzük. A Secuties ekkor szabálymintákat kínál a levelező- és böngészőprogramokhoz. Ezeket elfogadhatjuk, és kézzel kiegészíthetjük, de új szabályokat is definiálhatunk. Az egyes portok letiltásához az alkalmazásspecifikus szabályok mellett általános szabályokat is definiálhatunk. Az ICMP-hírekre való reakció részletesen beállítható.

A Secuties tűzfal valamennyi funkcióját egy jól áttekinthető, a *Microsoft Management Console-éhoz* hasonló, fastruktúra tartalmazza. A felhasználó letilthatja a reklámokat és a nemkívánatos honlapokat, korlátozhatja az ActiveX-control-ok, a Java-Applet-ek és scriptek futását, s ellenőrizheti az e-mail-ek mellékleteinek a kezelését. Ezzel a Secuties Firewall az árkategóriájához képest szokatlan lehetőségeket kínál.

További infók: www.secuties.de

Sphinx Personal Firewall

A svájci *Biodata* cég *Sphinx Personal Firewall* programja viszonylag friss termék a piacon. A program kettős tagolású. A főablakban egyszer kezdőknek, egyszer szakértőknek is le lehet hívni a beállításokat. A kezdők beállítását a szakértői beállítás is tartalmazza, csak épp a „szakértő" még további lehetőségeket is kap. A konfigurálást varázslóval végezhetjük. A varázsló nyolc kérdést tesz fel a PC használatával kapcsolatban, például hogy használunk-e webet, e-mail-t, ICQ-t, és hogy vannak-e megosztásaink. A varázsló végül megjeleníti az adatok összesítését.

A Sphinx jellegzetessége *a fehér és a*

A Sphinx fehér és fekete listákra osztja szét a hostokat

fekete lista. A fehér lista a megbízható, ismerős hostokat, a fekete lista ennek megfelelően a letiltottakat tartalmazza. Különbséget tesz web, FTP, news és más szolgáltatások alapján. A *Hozzáadás* kapcsolóval mindegyik listához megadható egy host az URL-jével vagy az IP-címével.

A bővített szűrőszabályok azt definiálják, hogy mely csomagok, milyen irányban léphetik át a tűzfalat. A címzettet, a forrás- és célportot, valamint a használandó protokollt valamennyi szabálynál be kell állítani. A Sphinx a TCP/IP-n kívül elboldogul az LLC, az IPX és a NetBEUI protokollt is. Ezzel ezt a tűzfalat Novell hálózatokban vagy kis hálózatokban (NetBEUI) is lehet a LAN felől érkező támadások kivédésére használni.

A program trial verziója korlátos: nem lehet eltávolni a konfigurációt.

További infók: www.pcfirewall.com

Steganos Internet Security

A *Steganos Internet Security* különböző Steganos termékek gyűjteménye: *Steganos Anonym* (internetes nyomtörlő), egy fájl-shredder, *Kaspersky Anti-Virus, Online Shield* tűzfal. Ez utóbbit a Steganos külön is árulja.

Sajnos az egyes komponenseket nem túl jól integrálták, s valójában nem egy csomagot kapunk, hanem különálló prog-

A Steganos Internet Security különböző Steganos termékek gyűjteménye

ramok készletét. A Kapersky víruskereső a felhasználónak külön kell telepítenie, az Online Shield-től pedig a program kezelése is független.

A tűzfal igen egyszerű felépítésű. Ha egy alkalmazás ki akar jutni az internetre, akkor az Online Shield vészjelzést ad. A felhasználó eldöntheti, hogy megengedi-e a hozzáférést vagy sem. Van még egy vészkapcsoló a teljes internetes forgalom megakasztásához, s ezzel az Online Shield beállítási opcióit messzemenően ki is merítettük. A *Steagnos Online Shield* tehát nem rendelkezik több jellemzővel a freeware termékeknél. Mindezt figyelembe véve pedig kissé drága.

További infók: www.steganos.com

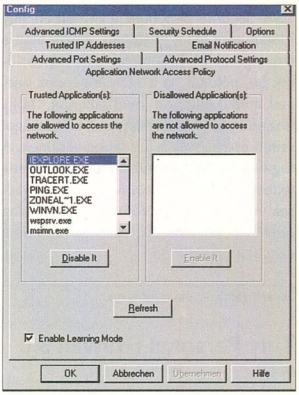
Sygate Personal Firewall 2.1

A *Sygate Firewall* öt fokozatban foglalja össze a biztonsági beállításait. Valamennyi tartalmaz alapértelmezést is, ami persze megváltoztatható. A legegyszerűbb, *Off* fokozatban a tűzfal ki van kapcsolva. A következő a *Low* – ezt akkor

A Sygate Personal Firewall öt biztonsági szintet definiál

használjuk, ha magunk üzemeltetünk szervert, mivel ez elfogadja az internetről érkező kapcsolatokat. A legmagasabb védelmi fokozat az *Ultra High*. Ez a teljes kimenő és bejövő forgalmat gátolja, és akkor javasolható, ha a számítógépek éjjel működnek, de nem akarunk internetes forgalmat. Kevesebb biztonságot kínál az online játékokhoz való *Medium*, valamint a *High*, amelyet a Sygate olyan felhasználóknak ajánl, akik standard programokkal lépnek fel az internetre.

Az *Advanced Port Settings* regiszterlapon célirányosan nyithatunk meg bizonyos well known portokat, vagy zárhatunk be 1000 feletti számúakat. A portok a TCP és UDP számára külön listában kapnak helyet. A *Hálózati kapcsolatok*



A Sygate-nél valamennyi, az internethez forduló alkalmazás pozitív vagy negatív listába kerül

megjelenítését az *Allow to browse Network Neighbourhood-dal*, és ennek elérését az *Allow to share Network Neighbourhood-dal* kapcsolhatjuk ki. Az Allow Bay/Nortel VPN egy speciális beállítás, ehhez a VPN-hez (*Virtual Private Network*). A portbeállítások az online játékok számára is lényegesek, mivel azoknak a portoknak, amelyeket a játék használ, nyitva kell lenniük. Az érintett portszámokat a gyártó honlapja tartalmazza. Így pl. a 139-es port (NetBIOS) akkor nyitható meg, ha bejegyezzük az *Open extra localports that are less than 1000* TCP-listába. Ekkor kijelölődik a megfelelő *Allow to share Network Neighbourhood* opció.

A Sygate kétféle programot ismer, azokat, amelyek hozzáférhetnek az internethez és azokat, amelyek nem. Ehhez be lehet kapcsolni egy tanulási üzemmódot. Ez aktívvá válik, amint egy alkalmazás megpróbál hozzáférni az internethez. Egy ablak jelenik meg, amely az alkalmazás internetes próbálkozását jelzi. Ha igennel nyugtázunk, akkor az alkalmazás bekerül a megbízható alkalmazások listájába (*Trusted Applications*). A jövőben, amint ez a program az internethez fordul, nem jelenik meg többé az előbbi kérdés. A biztonsági szempontból lényeges események egy log-fájlba tárolódnak. Ennek a log-fájlnak a bejegyzéseit e-mailben elküldhetjük magunknak vagy egy tetszőleges címzettnek. A szükséges beállításokat az *Email Notification* regiszterlapon kell elvégezni.

A *Security Schedule* regiszterben egy időtartamot lehet beállítani, amely alatt a legmagasabb védelmi fokozat kapcsolódik be, például ha a számítógépnek éjjel kell működnie, de nem akarjuk, hogy hozzáférjen az internethez. A biztonságot érintő események a log-fájlba kerülnek. A log-fájlok a hibakeresésnél és a betörések felfedésénél hasznosak. Mivel a bejegyzések viszonylag részletesek, így viszonylag pontosan követhetjük, hogy mi mindent csinált a betolakodó.

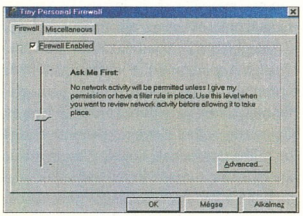
További infók: www.sygate.com

Tiny Personal Firewall 3.0

A *Tiny Software* a 3.0 verzióval megváltoztatta tűzfalának koncepcióját, s a programnak most már *sandbox-a* is van. Ha egyszer bezárunk egy programot a sandbox-ba, akkor a tűzfal nemcsak azt ellenőrzi, hogy mit is tesz az interneten, hanem a számítógépen zajló akcióit is felügyeli. Nagy kár, hogy a program nem ismeri fel a módosult e-mail-klienst. A *Tiny Personal Firewall* számos további funkciót is kínál. Többek között letiltja a reklámot, az ActiveX-controlokat, valamint a scripteket, és még a cookie-k ellenőrzésre is képes.

Negatívumként kell megemlítenünk a program bonyolult kezelését és dokumentációjának minőségét. A betanulásnál a felhasználót csak az online súgó támogatja. A protokollban felbukkanó, a támadásra figyelmeztető üzenetek magyarázó ablakai hiányoznak. Az internetre kívánkozó programokat a felhasználó előre definiált csoportokba sorolhatja. Ezekre adott szabályok érvényesek. Ezek azonban olyan mértékben szerteágazóak és komplikáltak, hogy a megtanulásuk nagyon sok időt igényel.

Igazán bonyolulttá akkor válik a helyzet, ha olyan programmal rendelkezünk, amelyet nem lehet a standard minták közé szorítani: a saját csoport készítése, a rengeteg szabályozási lehetőség következtében, nem egyszerű feladat. Ehhez már haladó hálózati ismeretekre van szükség.



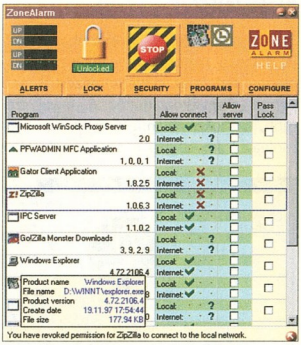
A Tiny Personal Firewall-nál szűrők segítik a konfigurálást

A Tiny Personal Firewall egy erős program, mégis a műkedvelők programja marad, mert a hasonló tűzfalakkal gyorsabban lehet elérni azonos fokú biztonságot.

További infók: www.tinysoftware.com

ZoneAlarm Pro 3.0

A *ZoneAlarm*-ot freeware verziója tette ismertté, amely annyiban különbözik a *Pro* verzitótól, hogy nem képes letiltani a reklámokat, valamint a honlap aktív tartalmát. A cookiek és e-mail-mellékletek kontrollja is hiányzik. A Pro verzióban a szabályokat vagy egyes programokra vonatkoztatva, vagy általában határozhatjuk meg. A



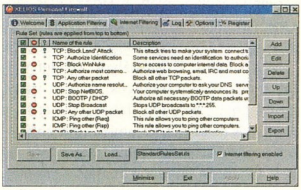
A ZoneAlarm által ismert programok listájában lehet meghatározni a LAN és az Internet elérésének a módját

ZoneAlarm a globális szabályoknál különbséget tesz a *megbízható zónák* és az *internet* között. A felhasználó mindkettőre beállíthatja az engedélyezett portokat és protokollokat. A tűzfal alapkonfigurálásánál egy varázsló segít. Ha a felhasználónak egy vészjelzéssel kapcsolatban kérdései merülnek fel, akkor a ZoneAlarm összeköti a *Zonelabs* honlapjával, ahol további súgószövegeket talál. A ZoneAlarm nagy biztonságot kínál, ennek ellenére a konfigurálása nem állítja nehéz feladat elé a gyakorlatlan felhasználót. A program beállításai annyira rugalmasak, hogy egy LAN-on is lehet használni, anélkül, hogy a hálózat többi részétől elvágnánk magunkat.

További infók: www.zonelabs.com

Xelios Personal Firewall 2.02

A mindössze fél megabájtos program felhasználói felülete egy többlapos párbeszédablak. A főlapon láthatjuk, hogy milyen IP-címen csatlakozunk az internetre, és folyamatosan figyelemmel kísérhetjük a beérkező és kimenő adatcsomagok számát, illetve azt, hogy ezek közül hányat blokkolt a program. Az *Options* lapon állíthatjuk be a működési jellemzőket, többek között a jelszavas védelmet. Az *Internet Filtering* lapon találjuk az alapértelmezésbeli adatszűrő szabályokat, és itt hozhatunk létre újabbakat.



Hiába a sok beépített szűrő, a Xelios védelme mégsem teljes

A biztonsági tesztelés két port esetében *Close* állapotot jelzett, ami azt jelenti, hogy a *Xelios Personal Firewall* megakadályozza az ezeken keresztüli behatolást, a gépünket viszont nem teszi láthatatlanná a külvilág számára. Valószínűleg olyan adatszűrő szabály is létrehozható, amely orvosolja a problémát, ez azonban egy személyi tűzfal használójától nem várható el.

Ennél is nagyobb hiányossága a programnak, hogy az adatot küldő alkalmazások ellenőrzését csak akkor végzi el, ha bejelöljük az *Application Filtering* ablak *Application Filtering Enabled* lehetőségét. Vagyis amíg erre nem jövünk rá, bármelyik program bármit zavartalanul átküldhet a tűzfalon.

Ezután már szigorúan őrködik az adataink felett, és a listára felvett programok futási jellemzőit egyszerű egérkattintásokkal módosíthatjuk.

A Xelios Personal Firewallért a 30 napos kipróbálási időszak letelte után 32 dollár regisztrációs díjat kell fizetni. Emiatt, továbbá figyelembe véve hiányosságait, jobban járunk az ingyenes programok valamelyikével.

További infók: www.xelios.com

A BalaBit IT Kft. kiadta a teljesen magyar fejlesztésű tűzfalszoftver legújabb verzióját, a Zorp Professional 2.0-t. A több tűzfalat is kezelő grafikus menedzsment rendszer mind a hazai, mind a nemzetközi piacon sikerekre számíthat.

Tűzfal – itthonról

Ahogy az informatika és az internet egyre nagyobb mértékben fonja át a vállalatok működésének mindennapjait, úgy lesz egyre fontosabb az IT-rendszerek védelme a kívülről – vagy akár belülről – jövő támadásokkal szemben. Ha a vállalat egészének működése, üzleti sikere a számítógépes rendszertől függ, akkor annak a megbénulása rendkívül súlyos következményekkel járhat. Abban minden szakértő egyetért, hogy az informatikai rendszerek biztonságáról csak *komplex módon* lehet gondoskodni, s ennek egyaránt része az adminisztratív, a fizikai és a logikai védelem is.

Ez utóbbi területen a védelem egyik fontos eszköze a tűzfal (firewall), amely alapvetően a vállalat belső hálózatát különíti el az internettől, illetve a vállalati hálózat egyes szegmenseit egymástól. Ennek révén az internettel kapcsolatos adatforgalom – letöltések, elektronikus levelek, továbbá a webes alkalmazások egymás közötti kommunikációja (például elektronikus vásárlás, on-line banki rendszerek, stb.) – nem juthat el ellenőrizetlenül a belső vállalati hálózatra.

A tűzfalszoftvereknek rendkívül sok képviselője ismert, ám korántsem mindegyikük képes kielégíteni az összetett felhasználói igényeket. Ezt felismerve kezdte el fejleszteni a hazai *BalaBit IT Kft.* 2000-ben saját tűzfalmegoldását, a *Zorp-ot,* amelynek 1.4-es változata 2001 októberében került kereskedelmi forgalomba. A továbbfejlesztések eredményeképpen pedig megszületett a *Zorp Professional 2.0.*

A Zorp Professional 2.0 a tűzfalak közül a ma legmodernebbnek számító altípust, az *alkalmazásszintű, moduláris proxy tűzfal technológiát* képviseli. Ez a módszer jóval nagyobb biztonságot nyújt, mint a hagyományos csomagszűrő tűzfalak – hiszen azoknál négy hálózati OSI-réteggel magasabban működnek, és a csomagoknak nemcsak a fejlécét, hanem a tartalmát is ellenőrzik –, ugyanakkor a végfelhasználó szempontjából észrevétlenül (transzparensen) működnek. Moduláris proxyként nem csupán az egyszerű protokollok kezelését végzi el, hanem képes az egymásba ágyazott protokollok (mint például az SSL-lel titkosított HTTP, azaz a HTTPS) kezelésére is; így a proxykból tetszőleges, a protokollnak megfelelő struktúra építhető ki.

A Zorp Professional 2.0-nak saját operációs rendszere és programozási nyelve (Python) van. Ennek, illetve az erre épülő grafikus kezelői felületnek köszönhetően az adminisztátorok rendkívül rugalmasan, az egyedi igények messzemenő figyelembevételével állíthatják be a rendszert. Ez a távoli felügyeletre is alkalmas grafikus eszköz a *Zorp Management System* (ZMS), amely akár több tűzfal egyidejű, központi menedzselését is lehetővé teszi. A szoftver kiegészítő moduljai révén alkalmas a magas rendelkezésre állású környezetek (HA-k), illetve a virtuális magánhálózatok (VPN-ek) támogatására.

A termékhez 30 napos, ingyenes telepítési támogatás jár, amelyet különféle egyéb támogatási és távfelügyeleti szolgáltatások egészítenek ki.

Alkalmazásszintű átjáró

A Zorp Professional a technológia jelenlegi legfejlettebb szintjét alkotó alkalmazásszintű tűzfalak családjába tartozik, így a rajta keresztül menő forgalmat az átvitt protokollt megvalósító úgynevezett proxyk (megbízottak) ellenőrzik és továbbítják. A Zorp Professional jelenleg az alábbi protokollok teljes formai elemzésére képes: FTP, HTTP, SSL, POP3, FINGER, WHOIS, NNTP, IMAP, TELNET, PRINTER, RADIUS, TFTP, LDAP, PGSQL, ORACLE NET8.

Kiegészítő (plug) proxyval bármely, egy porton keresztül kommunikáló kliens-szerver kapcsolat felügyelhető (SSH, MYSQL, VNC, Microsoft Terminal Service, GOPHER, SMB/CIFS, TALK, SYSLOG, IPP, RSYNC, RIP).

Minimális hardverkövetelmény

Intel x86-os architektúra a becsült forgalom (párhuzamos kapcsolatok száma) alapján méretezve:

- Pentium II kategóriájú processzor (233 MHz)
- 128 Mbájt RAM
- 1 Gbájt háttértár
- A telepítéshez: CD-ROM-olvasó és flopi

Saját rendszer, saját nyelv

A telepítőlemez a Zorp Professional szoftver mellett egy, kifejezetten a tűzfalakhoz konfigurált operációs rendszert is tartalmaz. A *Debian GNU/Linux* alapú, egyedi disztribúció csak a feltétlenül szükséges szolgáltatásokat nyújtja, és speciális beállításai védik a külső behatolástól.

A Zorp-nak beépített programozási nyelve is van, amely lehetővé teszi az adminisztrátor számára, hogy teljes mértékben szabadon állíthassa össze a tűzfal döntéseit. Ez a script nyelv a *Python*, ami könnyen tanulható, egyszerű, mégis hatékony eszköz a hálózati szabályok pontos betartására.

Hatékony hálóhasználat

Írásunkban összegyűjtöttük a leggyakoribb hálózati problémák megoldására alkalmazható leghatékonyabb trükköket és tippeket, hogy olvasóink ne pazaroljanak túl sok időt a hálózat telepítésére és konfigurálására. Az internetezők számára is tartogatunk meglepetéseket: a világháló és a helyi hálózat súrlódásmentes együttműködése érdekében sokszor van szükség kicsi, de hatásos beavatkozásokra ahhoz, hogy ténylegesen működjön a hozzáférés a hálózathoz.

1 Hálózati hibák – és a ping

Ha probléma merül fel a hálózat telepítésénél, akkor nehézkes lehet a hibakeresés. A megfelelő eszközökkel, mint amilyen például a *ping*, gyorsabban megtaláljuk a hibát.

A hibakeresésnél nemcsak az alkalmas hálózati eszközök használata, hanem az *eredmények helyes értelmezése* is fontos. Ha létesíthető hálózati kapcsolat, akkor próbaképpen pingeljük meg a saját IP-címünket. A ping egy olyan parancs, amely adatokat küld a megadott címre, s ezeket a megcímzett számítógép visszaküldi. A ping parancs egy 32 bájtos csomagot küld a hálózatban megadott számítógépnek, és méri a csomag utazási idejét. A „ping"-re az összes hálózatban lévő gépnek válaszolnia kell, mert *abszolút prioritással* rendelkezik a többi hálózati szolgáltatással szemben.

Ha nem sikerül a ping, akkor célszerű megpingelni a számítógép loopback-címét (172.0.0.1). Ha ez sikeres, akkor legalább abban biztosak lehetünk, hogy a TCP/IP

```
C:\users\default>ping 111.111.111.2

Ping wird ausgeführt für 111.111.111.2 mit 32 Bytes Daten:

Antwort von 111.111.111.2: Bytes=32 Zeit<1ms TTL=128
Antwort von 111.111.111.2: Bytes=32 Zeit<1ms TTL=128
Antwort von 111.111.111.2: Bytes=32 Zeit<1ms TTL=128
Antwort von 111.111.111.2: Bytes=32 Zeit<1ms TTL=128

C:\users\default>
```

Ez a helyes ping válasz a DOS, illetve a Windows alatt a konfigurált IP-címre. Ha ehelyett timeout-ot kapunk (kérés időtúllépés) akkor a hibakeresés folytatódhat

üzemel, s a hibát az IP-adatok konfigurációjánál kell keresni. Ha viszont nem tudjuk sikeresen megpingelni a loopback-eszközt, akkor vagy a hálózati kártya hibás, vagy rosszul telepítettük. Ekkor telepítsük újra a meghajtókat (Windows alatt), illetve válasszunk ki egy másik modult (Unix, Linux).

Ha meg tudtunk pingelni egy helyi hálózatbeli IP-címet, akkor megkísérelhetünk egy ping-küldést az internetre: a *216.92.67.128*-as ping segítségével ellenőrizhetjük az internetes hálózati kapcsolatunkat. A 216.92.67.128-as IP-című számítógép azonnal válaszol egy *Reply-jel*.

Ha nem sikerül egy név megpingelése, akkor a legnagyobb valószínűséggel az adatátviteli hálózatkapcsolatban a DNS-szerverben lévő bejegyzés a hibás, mivel nem lehetett átalakítani IP-címmé a nevet.

2 Hibakeresés pingelési hiba esetén

Ha sikertelen az IP-cím megpingelése, akkor további TCP/IP segédprogramok lehetnek a segítségünkre. A *netstart -rn* parancs további felvilágosítást ad hálózati hibavadászatunk során: kilistázza a végrehajtás pillanatában fennálló TCP/IP-kapcsolatokat. Ahhoz, hogy az IP tudja, mikor melyik hálózati interfészt (hálózati kártya, modem, loopback stb.) vegye használatba, szüksége van egy *routing-táblázatra*. A kulcs, amellyel a táblázatban keresünk, a megcélzott számítógép IP-címéből származik, mivel ennek első három bájtja tartalmazza hálózat címét.

A routing-táblázatban minden kapcsolatnak van egy sora. Az egyes oszlopok tartalmazzák az IP-hálózati számokat, a direkt/indirekt flag-et, a router IP-címét, továbbá a használatba veendő interfész számát. Egy IP-csomag elküldése előtt lekérdeződik ez a táblázat. A táblázatot a *route ADD ADDRESS* parancs segítségével megváltoztathatjuk. Az adminisztrátor ezután kézzel beírhat egy kiadandó IP-címet.

3 MAC-cím keresése – az ARP-vel nem gond

A DHCP-nél az automatikus IP-kiosztás hibakeresésénél fontos szerepet játszik a hálózati kártya MAC-címe.

```
C:\users\default>arp 111.111.111.222

C:\users\default>arp -a

Schnittstelle: 111.111.111.2 on Interface 2
  Internet-Adresse      Physische Adresse     Typ
  111.111.111.222       00-50-da-e0-7e-b4     dynamisch
```

Az ARP-pal az összes a hálózatba csatlakozó gépet felderíthetjük

Az *ARP (Address Resolution Protocoll)* hardvercímmé (MAC-címmé) alakítja az IP-címet. Minden hálózati kártyának egyértelmű MAC-címe van, amellyel azonosítható a hálózatban. Ahhoz, hogy a TCP/IP-hálózatban előkerüljön egy számítógép MAC-címe, először a helyi ARP-cache-t ellenőrzik, hogy nem ismert-e a MAC-cím egy korábbi címképzésből. Ha nem ismert, akkor megindul egy körlevél – egy ARP-körlekérdezés a keresett IP-címmel. Ha ez az üzenet eléri a keresett számítógépet, akkor az visszaüzeni a

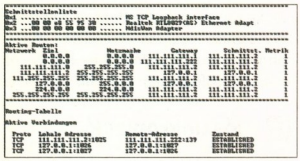
```
C:\users\default>route PRINT 111.111*
===========================================================================
Schnittstellenliste
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 da e0 7e b4 ...... Realtek RTL8029(AS) Ethernet Adapt
0x3 ...00 00 00 00 00 00 ...... Hitachi Adapter
===========================================================================
Aktive Routen:
Netzwerk Ziel            Netzmaske          Gateway       Schnittst. Metrik
      111.111.111.0    255.255.255.0    111.111.111.2   111.111.111.2     1
      111.111.111.2  255.255.255.255        127.0.0.1       127.0.0.1     1
```

A „Route print adresse" segítségével megjeleníthetjük a routing táblázatban már kiadott címeket

hardver-MAC-címet. Ezután a visszajelzés eltárolódik az ARP-cache-ben hogy később még címképzésre használjuk. Az ARP cache-t kézileg kezelhetjük az *ARP.EXE* paranccsal.

4 A célszámítógéphez vezető út

Hogyan jutunk el egy tetszőleges számítógéphez? Milyen számítógépeken keresztül érjük el a célszámítógépeket? Az ilyen „cserkészfeladatok" megoldására a „tracert" nevű IP-eszköz a legalkalmasabb.



Fecsegő: a „netstat" paranccsal áttekintést kapunk a hálózatról

A *tracert* parancs a legkedveltebb TCP/IP-diagnózis eszközök közé tartozik a rendszeradminisztrátor számára, hiszen problémákat észlelhet és oldhat meg vele.

A Tracert nemcsak lépésről lépésre mutatja az utat a célgépig, hanem a szükséges időt is megméri

A nagy hálózati terheltség vagy a célszámítógép nagyon lassú válaszideje esetén fellépő hálózati problémáknál gyakran a *tracert ADDRESS* hoz megoldást. A *tracert* megmutatja azt az utat, amelyet egy adatcsomag megtett a hálózatban, amíg elérhette a megadott számítógépet. A *tracert*-nél a teljes IP-címet vagy a DNS-nevet használhatjuk.

5 DNS problémák

Hogy ki bújik meg egy látszólag névtelen IP-cím mögött, azt az *nslookup* segítségével egy szempillantás alatt megtudhatjuk.

```
C:\users\default>nslookup 216.92.67.128
Server:  dns00.btx.dtag.de
Address:  194.25.2.129

Name:    nickles.de
Address:  216.92.67.128
```

A kis áruló: az „nsloop" megvizsgálja a DNS bejegyzéseket és megmutatja az IP-címhez illeszkedő bejegyzést

A DNS szerverrel kapcsolatos problémák esetében is nélkülözhetetlen az *nslookup*, de persze a kíváncsiak kellemes eszközévé is válik. Tudni szeretnénk, hogy ki rejtőzik a *216.92.67.128* IP-cím mögött? Az *nslookup 216.92.67.128* parancs megadja a választ. Az *nslookup* telefonos hálózati kapcsolat esetében is működik. Az *ipconfig/all* (Windows/DOS), illetve az *ifconfig* (Linux) paranccsal az aktuális IP-címünket tudhatjuk meg.

6 A Windows 95/98 lefagy a kikapcsoláskor

Nagyon bosszantó jelenség: kijelentkezünk a hálózatból, kilépünk a Windows 9x-ből, mire a kliens lefagy.

A Windows 95/98 SE kliensek sok bosszúságot okoznak a hálózati üzemmódban. Éppen a kikapcsoláskor, amikor a hálózati profil eltárolódik a szerveren, vagy amikor fontos adatok lementése zajlik, lefagy a gép. A Windows 95 alatt az *Internet Explorer 4.01* használata esetén ezt rendszerint egy hibás fájl okozza. A bűnös neve *shell.dll*. Célszerű a Microsofttól beszerezni az újabb IE 5.0 vagy 5.5 verziót. A Windows 98 SE alatt a kikapcsolásnál egy általános probléma lép fel. Itt rendszerint az segít, ha a hálózati kliens programban fixre állítjuk a frame típust, és nem hagyjuk meg az alapértelmezett *auto* beállítást.

7 Windows NT/2000 és Linux egy merevlemezen

Csak egy létezhet – ez a Windows filozófiája. Egy kis trükkel azonban utólagosan is beépíthetjük a Linux-szal való bootolást a Windows NT/2000 bootmenüjébe.

Ha már van egy Linux a merevlemezen, a Windows 2000 könyörtelenül felülírja a Linux bootszektort. Ezért a Linux telepítése előtt a root-partícióba kell írni. Jelentkezzünk be root-ként, és telepítsük a LILO-t a Linux root-partícióba. A Lilo beállításait a *liloconfig-gal* érhetjük el. Indítsunk egy új LILO konfigurációt, és a telepítéshez válasszuk a root-partíciót. Ezt követően toldjunk hozzá egy megfelelő Linux partíciót. Most telepíthetjük a Lilo-t, és megírhatjuk a bootszektort. A rendszer újraindítása előtt mentsük le a bootszekort egy fájlba. Ehhez a következő parancsokat használjuk:

dd if=Linux Root-Partition of=fájlnév.lin bs=0512 count=1

A */dev/hdai* Linux root-partíciót (azt, ahol a /boot található), másoljuk be egy fájlba:

dd if=/dev/hda1 of=/bootsect.lin bs=0512 count=1

A Linux partíció neve *dev/hda1*, automatikusan létrejön a *bootsect.lin* fájl, és a Linux gyökérkönyvtárában fog elhelyezkedni.

Mentsük le ezt a fájlt flopira:

cp –a bootsect.lin /floppy

Most újra indíthatjuk a számítógépet, és a Windows NT/2000-rel bootolhatunk. Végezetül ezt a bejegyzést be kell írni a Windows NT/2000 *boot.ini* rendszerfájljába. Az egér jobb oldali gombjával válasszuk a *Tulajdonságokat*, és szabadítsuk fel a fájl írásvédelmét. Most egy tetszőleges editorral szerkeszthetjük a fájlt. A fájl végére írjuk be a

C:\bootsect.lin="Linux indítása"

sort, tároljuk el a fájlt, és ismét állítsuk vissza az attribútumait az eredeti állapotba. A bejegyzést a Windows bootmenüjében a számítógép újraindítását követően láthatjuk.

8 A bootszektor visszaállítása

Ha több operációs rendszert szeretnénk a PC-nkre telepíteni, akkor vigyáznunk kell a Windows NT/2000 telepítésénél. Ha a merevlemezen van már egy „nem Microsoft" operációs rendszer, akkor a Windows NT/2000 könyörtelenül felülírja a partíciótáblázatot. Az esetek többségében az újraindítást követően többé nem tudjuk elindítani a Linuxot vagy az OS/2-t. A tettes a bootszektor, amely elindítja az *NT-loader-t (ntldr)*, és megjeleníti a Windows NT boot-menüt *(boot.ini)*. Egy esetleges korábbi DOS vagy Windows 95/98 bootszektora átmásolódik egy *bootsect.dos* nevű fájlba, amelyet az NT boot-menüjében a DOS bejegyzés alatt lehet elérni.

Ha a Windows 95/98-at vagy a ME-t a Windows NT/2000 után telepítjük, akkor rendszerint a Windows NT/2000 bootszektora tűnik el. Ilyenkor nem lehet többé indítani a Windows NT/2000-t. Az indítóflopis start esetében, az ezt követő *sys a: c:* után is felülíródik a Windows NT/2000 bootszektora. A bootszektor visszaállításához nem kell újra telepíteni a Windowst. A Windows ugyanis a telepítés alatt egy másik szektorba elmenti a

bootszektort – ezt a *bootpart* nevű freeware segédprogrammal visszaállíthatjuk. A parancs a következő:

winnt boot:c:

A *win95 boot:c:* paranccsal a Windows 95-öt írhatjuk be rendszerként a bootszektorba. A bootpart programot a **www.winimage.com/bootpart.htm** címen találjuk az interneten.

9 Praktikus freeware-ek és shareware-ek

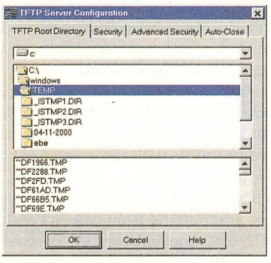
Egyik operációs rendszer sem tökéletes. A hálón a megfelelő segédprogramokkal és eszközökkel válik igazán érdekessé az élet.

Big Brother

A freeware *Big Brother* (az alábbiakhoz: unix/linux v.1.6a, Windows NT client v.1.07b, Novell Netware client, v0.2 Mac OS client:v1.0b6, **http://-maclawran.ca/sean/bb-dnld/index.html)** hostokat és TCP-szolgáltatásokat vizsgál a TCP/IP hálózatokon. A program megnézi, hogy el lehet-e egyáltalán érni a hálózaton egy számítógépet vagy hogy működnek-e a http-, ftp- és POP3 szerverek. Ezen kívül hardverinformációk is megjelennek: mennyire van leterhelve a CPU és a merevlemez, futnak-e bizonyos rendszerkritikus folyamatok, vagy megjelennek-e bizonyos szolgáltatások. Az eredményeket grafikusan meg lehet jeleníteni, és végezetül HTML fájlként rendelkezésre lehet bocsátani.

TFTP Server

A *Solarwinds*.NET TFTP-Server-e **(http://solarwinds.net/Tools/Free_Tools/TFTP_Server/Download.htm)** az egyetlen elérhető freeware Windows TFTP szerver, amely a *Multi-Threading-et* is tudja. Ezáltal több kliens-kérést le-



A TFTP a windowsos hálózatok automatikus telepítésének ideális eszköze

het egyidejűleg feldolgozni minden nagyobb hálózati probléma és hálózatterhelési gond nélkül. Az FTP és TFTP közismerten eltérnek egymástól – a TFTP protokollnak semmi köze a klasszikus FTP protokollhoz; a kliens merevlemez-image-einek létrehozására és visszatöltésére készült.

Servers Alive?

A *Servers Alive?* program kifejezetten a Windows hálózati szerverek felügyeletére készült (az aktuális verzió: v2.1.829, **www.woodstone.nu/salive/).** Beállítható időközönként ellenőrzi, hogy valamennyi megadott PC aktív-e még. Ez történhet egyszerű pingeléssel vagy bizonyos TCP-portok tesztelésével. A Windows NT/2000 alatt a program még bizonyos NT szolgáltatásokat is támogat, vagy ellenőrzi a maradék merevlemez-területet.

Sniffit

A *Sniffit 0.35* a Linux, SunOS, Solaris és FreeBSD alá készült, és egy Linux csomag-sniffer (protokoll analizáló), amely a TCP/IP hálózatokon képes vizsgálni az adatcsomagokat. Az egyetlen előfeltétel, hogy a helyi gépen root-jogokkal rendelkezve dolgozzunk. A freeware programot a **http://reptile.rug.ac. be/-coder/sniffit/files/sniffit.0.3.5.tar** címen találjuk.

VisualRoute

A *VisualRoute 5.0b* a Windows 95/98/NT/2000 alatt egyaránt működő grafikus trace-route program, sebességanalízissel és sebesség-gráffal. Egy IP-cím vagy host név (német nyelven történő) megadása után megtudhatjuk, hogy a hálózat mely részén szűk a keresztmetszet. A válaszidőket táblázatba rendezetten és grafikus alakban is megjeleníti. A Visual Route egy világtérképen megjeleníti a csomag célba jutásának az útvonalát.

10 WINS – a legtöbbször nem szükséges

Éppen a Linux-szerverekkel kapcsolatban okoz gondot a WINS: szükségünk van erre az adatbázisra avagy sem.

A *WINS* a *Windows Internet Network Service* rövidítése, egy *osztott adatbázis* routolt hálózati környezetek számára. Itt tárolódnak a számítógépnév-IP-cím párosok, amelyeket szükség esetén lekérdezhetnek a Windows-kliensek. Ez az adatbázis egy NT/2000-es szerveren fut, amelyet egy Linux/Samba szerverre is át lehet emulálni, hogy a NetBIOS-neveket át lehessen alakítani IP-címekké. Itt jelentik be a WINS-kliensek a NetBIOS-nevüket és az IP-címüket a WINS-szervernél. Ha egy Linux-szervert használunk Windows NT—Samba megoldásként, akkor általában nincs szükség a WINS-re, kivéve, ha a kliensek kifejezetten igénylik a WINS-t.

11 Időszinkronizáló

Gyakran előfordul, hogy ha több számítógéppel dolgozunk, akkor azokon nem mindig egyezik meg az időbeállítás. Egy trükk segítségével szinkronban tarthatjuk a hálózatbeli időket.

Egy egyszerű batch-fájl segítségével beállíthatunk egy szerver-szinkron időt a számítógépen: készítsünk egy tetszőleges editor segítségével egy, a következő sort tartalmazó batch-fájlt:

NET TIME \NT-2000-Servername /SET /YES.

Azon a számítógépen, amelyen elindítjuk ezt a fájlt, a szerver időbeállítása jut érvényre. Ha az összes kliens el van látva ezzel a batch-fájllal, akkor minden egyes alkalommal, ha bejelentkezik egy felhasználó a számítógépnél, szinkronizálódik az idő. Szükség esetén hálózati meghajtók mapping-jeit is előállíthatjuk ebben a batch-fájlban. Ez a trükk egy Linux Samba-szervernél is problémamentesen működik.

12 Windows tartományok közötti hozzáférés-problémák

Ha egy windowsos hálózatban több tartomány szerepel, akkor az adminisztrátoroknak nincsen automatikus hozzáférési joguk az összes tartományhoz, így kisebb kerülőútra van szükség.

Annak ellenére, hogy az X és az Y tartomány között egy egyoldalú megbízhatóság áll fenn, azaz az X tartomány megbízik az Y tartományban, nem működnek az Y tartományra vonatkozó hozzáférési jogok. Így például az X tartományban megosztást készítünk egy hálózati szerveren, amely az Y tartomány adatainak a tárolására szolgál. Itt készülnek a teljes hozzáférésű megosztás- és könyvtárelérési jo-

gosultságok a „tartomány adminisztrátorok" globális csoportja és a „tartományfelhasználó" csoport Y tartománya részére. A tartomány adminisztrátorok az Y tartományból nem tudnak ezen megosztás fájljaihoz hozzáférni, pedig úgy tűnik, hogy a megfelelő jogosultságok kielégítő mértékben szét lettek osztva. Még az X tartománybeli adminisztrátorok sem rendelkeznek a megosztás hozzáférési jogaival. Az ok: ahhoz, hogy az Y tartomány adminisztrátoraként hozzáférjünk X tartománybeli fájlokhoz, *adminisztratív jogokra* van szükségünk, amelyeket sajnos nem kapunk meg automatikusan, amikor egy bizalmi helyzetet hozunk létre. Itt bizony nekünk kell cselekednünk, és az Y tartománybeli „tartomány adminisztrátorok" globális csoportot be kell jegyezni az X tartomány hozzáférés érintett szerverén lévő adminisztrátorok lokális csoportba.

13 Popper a hálózaton

Ha rövid üzenetet szeretnénk küldeni a LAN többi felhasználójához, akkor elegendő a *net* parancs használata. Ennek a segítségével rövid üzeneteket küldhetünk a többi LAN-klienshez egy DOS-ablakban megírt *net send* parancs útján. Az utasítás a következő:

net send tesztelő „Hello, ez egy teszt"

Ezzel a „tesztelő" login nevű felhasználónak küldjük a „Hello, ez egy teszt" üzenetet. Ha a megcímzett felhasználó jelenleg a hálózatban tartózkodik, akkor egy kis párbeszédablakban megjelenik neki az üzenet. Az összes hálózatban tartózkodó felhasználót úgy tudjuk egyszerre megcímezni, hogy egy „*"-gal helyettesítjük a login nevet.

14 Biztonság – fedélzeti eszközökkel

A Windows NT/2000-nél alapvetően nyitott állapotban van az összes TCP- és UDP-port. Ezeket a saját szájízünk szerint át tudjuk állítani, s így védeni tudjuk magunkat a hackerek ellen. Ahhoz, hogy a Windows NT/2000-nél lezárjuk a gyakran nem használt TCP- és UDP-portokat, kattintsunk a jobb egérgombbal a hálózatszimbólumra, és menjünk a *Tulajdonságok-ra*. A *Protokollok* oldalon válasszuk a *TCP/IP*-t, majd a *Tulajdonságok-at*. Most aktiválhatjuk az *Advanced*-nél az *Enable Security-opciót*. A *Konfigurálás* gomb megnyomásával további beállításokra nyílik lehetőség: itt beállíthatjuk a megfelelő portokat, és eldönthetjük, hogy melyek maradjanak nyitva, illetve melyeket kívánjuk bezárni.

15 Várakozás helyett haladás

A *Microsoft Exchange Server* telepítése után sok időt tölthetünk várakozással a szerverből való kilépéskor. Ezen a gondon egy apró Registry-trükkel segíthetünk.

Állítsuk vissza a Registry *HKEY_LOCAL_MASCHINE\SYSTEM\CurrentControlSet\Control\WaitToKillService* könyvtárban a 20000-es bejegyzést. Egy újraindítás után aktivizálódik a változtatás.

16 629-es hiba az internet-hozzáférésnél

Ha egy modem-/ISDN/DSL-kapcsolatot szeretnénk létesíteni a szerverről az internetbe, akkor egy kis bejegyzés tűnik fel: sikertelen a bejelentkezés.

Kényes a helyzet: igaz helyesen adtuk meg a felhasználónevet és a jelszót, mégis sikertelen a bejelentkezés az *Internet Service Provider-hez*. Az ok a következő: a legtöbb esetben a bejelentkezésnél egy tartomány is meg van adva, nos ezt a mezőt ki kell törölni. Érdemes leellenőrizni a modem-beállításokat is – itt aktiváltnak kell lennie a *kódolatlan eredetnyugtázás* opciónak.

17 Az adatmentés automatizálása

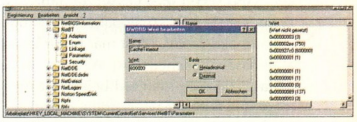
Ha egy Windows NT 4-es szervert használunk, általában egy külső backup programra is szükség van, amely a rendszeres és automatikus adatmentést hajtja végre. Ezt a működést egy trükk segítségével mi is megvalósíthatjuk.

Ahhoz, hogy adatokat, konfigurációs adatokat vagy az operációs rendszer adatait rendszeresen, ráadásul automatikusan el tudjuk menteni a fedélzeti eszközök segítségével, a legjobb, ha a Windows NT *Schedule-szolgáltatását* és az *at* DOS-parancsot használjuk. A Vezérlőpult-beli *Schedule* indítása után a *Szolgáltatások* alatt konfiguráljuk ezeket *automatikus indításra*. Ezután a DOS-promt-on keresztül az *at* parancs segítségével beírhatjuk a szükséges backup-megbízást. Az *MS-DOS-parancssor*-nál az *at* parancsnál megadjuk a batch-fájl indításának az idejét. Ebbe a batch-fájlba írjuk bele mindazokat a parancsokat, amelyeket a megnevezett időpontban végre szeretnénk hajtatni. Az *at 0:00 backup_01.cmd* paranccsal éjfélkor automatikusan indítódik a *backup_01.cmd* nevű batch-fájl. Ebben a fájlban végrehajtathatunk másolási műveleteket, mint az *xcopy* vagy a *copy*, esetleg másfajta fájlműveleteket, mint például a törlés, áthelyezés stb.

Valamivel professzionálisabb megoldás a batch-fájl különböző napokon való végrehajtatása, hiszen nem akar az ember naponta egy rendszermentést. Az *at 0:00 /every:1,4,7 backup_2.cmd* parancs hatására minden első, negyedik és hetedik nap éjfélkor indítódik a *backup_2.cmd* nevű fájl. Ebbe a fájlba is el lehet helyezni különböző fájlműveleteket. Visszatérő feladatokat *bejelentkezési script-ekkel* lehet vezérelni és automatizáltan futtatatni. Egy bejelentkezési script elvileg nem más, mint egy batch-fájl, amely automatikusan indítódik a számítógép bekapcsolásánál. A legjobb, ha ezt a fájlt a *netlogon-ként* megosztott könyvtár alá helyezzük a szerveren. Ezt követően a bejelentkezésnél a Windows-felhasználómenedzser segítségével a megfelelő felhasználóhoz rendelhetjük hozzá az odavágó bejelentkezési script-et.

18 Jelen van, de nem látható

A windowsos hálózati környezetben egyes lemezegységek már nem láthatók, holott még fennáll a hálózati kapcsolat. Persze ennek az ellenkezője is felléphet: láthatók még a hálózati lemezegységek, pedig már lekapcsolták ezeket a számítógépeket. A jelenség oka általában a szerver túl nagy „timeout"-ja. A *Registry-ben*



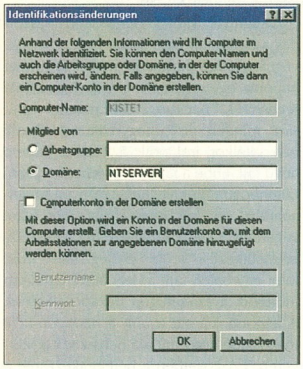
Ha túl gyorsan tűnnek el a hálózati lemezegységek, akkor igazítsunk a „Cache Timeout" paraméteren

a *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters* kulcs segítségével találjuk meg a *Cache*

Timeout-ot. Jó, ha 60000 (ms)-ra van beállítva ez az érték.

19 Felhasználói profilok a Windows NT/2000 alatt (1.)

A szerveren tárolt felhasználói profilok utólagos berendezésénél különböző beavatkozások szükségesek, hogy tisztán működhessenek ezek.



Ahhoz, hogy egy kliens helyesen azonosíthassa magát a szerveren, be kell írni a bejelentkező szerver tartományát

Először ellenőrizzük a *C:\ WINNT\ Profiles* könyvtár megosztását a profil nevével rendelkező bejelentkezési szerveren. Ahhoz hogy a felhasználó hozzá tudjon férni ehhez, ennek megfelelően kell konfigurálni a megosztási jogokat. Ezután indítsuk el a *tartományok felhasználó-menedzserét*, és válasszuk ki a megfelelő felhasználót. Egy dupla kattintással jutunk a *Tulajdonságok-ba*, ahol válasszuk ki a *Profilok-at*. Most megadhatjuk a párbeszédben a felhasználói profil megfelelő elérési útvonalát. Írjuk be például a következőket: **\\NTServer\Profiles\berta**, amivel a Berta nevű felhasználónak készítettünk felhasználói profilt. Most már bezárhatjuk a felhasználómenedzsert. A Berta nevű felhasználó még nem tud bejelentkezni a megfelelő felhasználói profillal – itt még a Windows klienst is testre kell szabni.

Jelentkezzünk be lokálisan a felhasználó munkaállomásán, és a *Vezérlőpultnál* válasszuk ki a *Hálózat* opciót. Itt írhatjuk be a számítógépnevet és a területet, amelynél a Windows-kliensnek be kell jelentkeznie.

Zárjuk be a hálózati párbeszédet, és válasszuk ki a *Vezérlőpultról* a *Rendszer* opciót. Itt a *Felhasználói profilok* fülnél megtaláljuk Berta helyi profilját – ezt kell átmásolni a szerverre. Most bezárhatjuk ezt a párbeszédablakot is, és próbaképpen jelentkezzünk ki. Most a Berta nevű felhasználó újra bejelentkezhet a munkaállomáson.

20 Felhasználói profilok a Windows NT/2000 alatt (2.)

Ha szerveren alapuló profilokkal dolgozunk a Windows NT/2000-nél, akkor gyakran okoznak problémát az olyan hibajelentések, mint *a lokális profil régebbi, mint a szerveren alapuló profil.*

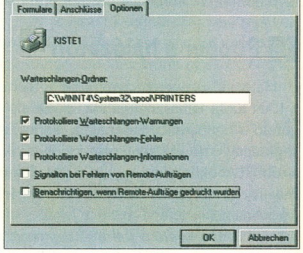
Ez a hibajelentés azoknál a felhasználóknál gyakori, akik gyakran jelentkeznek be különböző klienseknél. Ha sok felhasználói profil van a szerveren, akkor ez nemcsak tárolási kapacitást emészt fel, hanem jelentős mennyiségű adminisztrációs munkát is jelent. Ezért jobban tesszük, ha automatikusan töröljük a munkaállomáson lévő helyi profilokat – a felhasználónak ekkor egyetlen környezet áll a rendelkezésére. Ezt a *Registry-be* tett bejegyzés segítségével érjük el: a *HKEY_LOCAL_MACHINES\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\DeleteRoamingCache* ágban állítsuk át „1"-re a *DeleteRoamingCache* paramétert.

21 Lejárt felhasználói fiókok eltávolítása a Windows NT alatt

Ha sok felhasználói fiókot kell kezelni, könnyen elveszíthetjük az áttekintést. Szerencsére egy script segítségével újra rendet teremthetünk. Az olyan intézményeknél, ahol sok az ideiglenes felhasználó, ajánlatos a felhasználói fiókok automatikus eltávolítása. A Windows NT megengedi a lejárati idővel rendelkező fiókok bevezetését – viszont nem törli automatikusan a postafiókot. Ezek a leállított felhasználói fiókok nemcsak a helyet foglalják, hanem csökkentik az átláthatóságot is. Erre egy olyan script a megoldás, amely automatizálja ezt az eljárást. A Microsoft ad is egy VB-script-et a *Q251334*-es cikkbeli *Microsoft Knowledge Base*-ben, amely Windows Scripting Host-tal, valamint ADSI-vel(Active Directory Services Interface) dolgozik. Ügyeljünk arra, hogy a WSH-t még utólag telepíteni kell – ebben a *Windows NT Option Pack* nevű csomag segít.

22 Problémák a nyomtatással

A Windows kliensekre történő nyomtatómeghajtók telepítése a rendszeradminisztrátor legmacerásabb feladatai közé tartozik. Szerencsére a Windows 9X esetén bevethetünk egy-két trükköt. A Windows 95/98 kliensek számára az NT/2000-szerverek rendszergazdái rendelkezésre bocsáthatnak nyomtatómeghajtókat, ami annyit jelent, hogy ezek egy szabad könyvtárban vannak elhelyezve. Ha felépül egy kapcsolat egy kliens és a



Egy kijelölő pipát ki kell törölni, és máris nyugtunk van, többé nincs nyomtatási üzenet

hálózati nyomtató között, akkor a nyomtatómeghajtót automatikusan betölti a szerver. Ha már meg van osztva a nyomtató, akkor a nyomtatómeghajtók konfigurálása a *Megosztás* regiszteren keresztül történik. A Windows NT-nél gyakran problémát okoznak a nyomtatási munka sikeres befejezését nyugtázó visszajelzések. Ezek sokszor akkor fordulnak elő, amikor egy alkalmazó több kliensen dolgozik, és egy hálózati nyomtatón keresztül nyomtat. Ha sok nyomtatási megbízás van feldolgozás alatt, akkor a visszajelzés inkább zavaró, mint hasznos. A nyomtatási munka befejezéséről szóló visszajelzéseket kikapcsolhatjuk a *Start* menüben a *Beállítások – nyomtató* alatt, a *Fájl – szervertulajdonságok* parancs segítségével. Ha *Remote* nyomtatási megbízásokat nyomtatunk, akkor az *Opciók* regiszterben kikapcsolhatjuk a *Visszajelzés-t*. Ha újraindítjuk a *Vezérlőpult/Szolgáltatások*

alatt megtalálható *Spooler-szolgáltatást*, akkor nem generálódik több visszajelzés.

23 Hálózati kliensek kihasználtsága

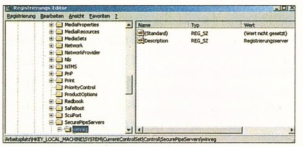
A Windows rendszermonitor segítségével nemcsak a helyi számítógép rendszeradatait kérdezhetjük le, hanem a távoli klienseket is.

A rendszergazdák is lehetnek kíváncsiak: mennyi erőforrást használ fel az A számítógép? Tényleg ilyen lassú a B számítógép? Ezekre a kérdésekre a Windows rendszermonitorával kaphatunk választ. Hogy a hálózatból ne tudjon bárki kémkedni, csak a *rendszeradminisztrátorok* csoport tagjai használhatják ezt a funkciót. Figyelem: a Windows NT 4.0 alatt (ha be van kapcsolva) a vendégek is Remote-hozzáférést gyakorolhatnak a rendszermonitorra. Mivel a legtöbb biztonságkedvelő windowsos rendszergazda zárva tartja a vendég fiókját, ez a probléma elhanyagolható. Ha használatba akarjuk venni a vendégfiókot, akkor a Remote-hozzáférést vezérelni tudjuk egy *Registry* beavatkozás segítségével. A *HKEY_LOCAL_ MACHINE-\SYSTEM\Current ControlSet\ Control\SecurePipeServers\Winreg* ágban a könyvtár a *\Services\Replicators*-ra van beállítva – aki itt olvasási jogosultsággal rendelkezik, az hozzáférhet a rendszerinformációkhoz. Ellenkező esetben *A számítógépnevet nem találtam* hibajelzést kapjuk.

24 Registry – hozzáférések korlátozása és engedélyezése

Nem minden felhasználó férhet hozzá a *Registry-hez* – a rendszergazda akár teljesen is elzárhatja a *Registry-t* a „normál" felhasználó elől. De mi van akkor, ha egyes programok a futási idejük alatt Registry-hozzáférést igényelnek, vagy távolról kell hozzáférni a Registry-hez?

A Windows 4.0 csak a rendszergazdák csoportjának engedi meg kezelni a Registry-t, míg a Windows 2000-nél a rendszergazdákon kívül még a biztonsági operátorok is hozzáférhetnek a regisztrációs adatbázishoz. Hogy ne kelljen külön felhasználócsoportokat létrehozni a Registry-függő programok részére, a Registry-paraméterek beállításával elérhetjük a hozzáférések engedélyezését. A távhozzáférésnél ugyanazok a játékszabályok érvényesek – csak a rendszergazdák férhetnek hozzá a Registry-hez. Ha bővíteni szeretnénk a kört, akkor a Windows NT-nél speciális Registry-bejegyzésekre van szükség. A Microsoft kínál is erre egy megoldást a Knowledge Base-ben *(Q153183)*. Hozzunk létre egy új kulcsot *SecurePipe Servers* néven a *HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control* könyvtárban. Ezt követően hozzunk létre egy újabb kulcsot *winreg* néven a *HKEY_LOCAL_MACHINE-\SYSTEM\CurrentControlSet\Control\SecurePipeServers* ágban. Itt most egy új *Description* jelsorozatot jegyezhetünk be a *Registry Server* stringgel. Most kattintsunk a *winreg* kulcsra, és válasszuk ki a *Biztonság-ot*, és itt menjünk a *Jogosultságokra*. Itt létrehozhatunk hozzávetőleges felhasználókat és csoportokat, amelyek ezután megfelelő Registry-hozzáférési jogokkal fognak rendelkezni. Ezzel az eljárással létrehozhatjuk a Registry speciális bejegyzéseinek hozzáférési jogosultságait is, és meghatározhatunk definiált könyvtárakat a *Registry-ben*, hogy a rájuk való hivatkozásnál megkerülhetők legyenek a definiált korlátok. Ez olyan speciális alkalmazásoknál célszerű, amelyek Registry-hozzáféréseket igényelnek a futási idejük alatt. Egy újraindítás után aktivizálódnak a számítógépen ezek a változtatások.



A Registry-vel a PC, elérését is szabályozhatjuk

25 Gyorsabb Windows Explorer

Az NTFS-beli 8.3 nevek kikapcsolásával egy kisebb teljesítménylöketet érhetünk el. Az NTFS alkalmazása éppen a szerverhasználatnál fontos és ajánlatos – nem utolsósorban biztonsági okok miatt. Viszont az egész kezelési ráfordítás negatívan hat a teljesítményre. Egy kis Registry csíny segítségével azonban egy kicsit visszanyerhetünk: mivel a Windows NTFS a hosszú fájlnevek mellett jó öreg DOS-korabeli 8.3-as szabványú rövid fájlokat is létrehoz, így időt veszítünk. Ha nem akarunk 8.3 konvenciót követelő 16 bites alkalmazásokat futtatni, akkor ajánlatos megspórolni a dupla ráfordítást.

A *Registrty-ben* a *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\FileSystem* könyvtárban található a *NtfsDisable8dot3NameCreation(REG-DWORD)* bejegyzés. Változtassuk meg e bejegyzés értékét *0*-ról *1*-re, amely kikapcsolja a rövid fájlnevek előállítását.

26 Védjük megosztásainkat a felhasználók elől

Windows alatt a megosztott könyvtárak nevei hálózati kapcsolat kialakításakor bárki számára láthatók, annak ellenére, hogy nincs jogosultságuk megnyitni ezeket a könyvtárakat.

Ha meg akarjuk védeni megosztott könyvtáraink nevét a kíváncsi tekintetektől, akkor a megosztási név után tegyünk egy $ jelet. A Windows NT szabványszerűen készít egy pár megosztást, például a Windows NT könyvtárhoz *(Admin$)*, vagy a *C:* meghajtóhoz *(C$)*. Készítsünk egy *TESZTKÖNYVTÁR* nevű könyvtárat, és egy *tesztkönyvtár$* megosztást.

Ha most valaki rá akar kapcsolódni erre a könyvtárra, akkor ismernie kell a könyvtár megosztási nevét, mivel ez már nincs kijelezve a hálózati környezetben. Ha kézzel írjuk be a megosztás nevét, akkor a hálózati kapcsolat kialakításakor ne feledkezzünk meg a „$" jelről.

27 Az Asztal a bejelentkezési scriptre vár

Ahhoz, hogy az Asztal ne várja végig a bejelentkezési script teljes lefutását, a *Registry HKEY_CURRENT_USER\Software\ Microsoft\WindowsNT\CurrentVersion\ Winlogon* könyvtárában állítsuk 1-re a *RunLogonScriptSync* bejegyzés értékét.

28 Lemez-crash – a Windows PDC pótlása

A baj ritkán jár egyedül: ha kiesik egy szerver, akkor a hálózati működés súrlódásmentes fenntartása gondot és sok munkát jelent. Ha baj éri a primer tartományvezérlőt, akkor még örülhetünk, hogy üzemel egy biztonsági tartományvezérlő. Hogy a hálózat gond nélkül működhessen, át kell alakítani ezt a backup tartományvezérlőt primer tartományvezérlővé. Indítsuk el a *Server Manager-t*, és válasz-

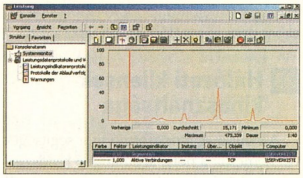
szuk ki a megfelelő biztonsági tartományvezérlőt. Kattintsunk rá a *Primer tartományvezérlővé való előléptetés* opcióra.

Ezután az aktuális tartomány újra visszanyeri a „régi" állapotát. Ha megjavult és bevetésre kész a régi PDC, akkor ezt újra integrálhatjuk a tartományba. Most biztonsági tartományvezérlőként futtathatjuk, és hozzáfűzhetjük a tartományhoz.

Ha vissza akarjuk állítani az eredeti állapotot, és ezt mint PDC szeretnénk futtatni, akkor állítsuk vissza az aktuális PDC-t biztonsági tartományvezérlővé. Állítsuk meg a bejelentkezési szolgáltatást, és válasszuk ki a *Server Manager-ben* a *Degradálás biztonsági tartományvezérlővé* opciót. Ezután szinkronizálni kell a tartományt, hogy aktualizáljuk a régi PDC-t. Most a *Primer tartományvezérlővé való kinevezés* opció segítségével újra PDC-ként használhatjuk a hálózatban a régi PDC-t. A biztonsági PDC-t itt BDC-ként jegyzik be. Ezen átépítési műveletek után javasolt a szolgáltatások és az alkalmazások ellenőrzése: a bejelentkezési szolgáltatás megállításával automatikusan más szolgáltatások is leállnak, amelyek azonban nem indulnak újra maguktól. Ellenőrizzük tehát a *Vezérlőpult* összes szolgáltatását, hogy rendesen működnek-e.

29 Hálózati kihasználtság

Ha szeretnénk tudni, hogy milyen a windowsos hálózatunk kihasználtsága, akkor nincs szükségünk drága LAN-analizáló programokra, windowsos fedélzeti eszközökkel is célba jutunk.



A statisztika nem hazudik: a hálózat terhelését a Windows Rendszermonitorával is láthatjuk

A Windows e célra tartogatja a Rendszermonitort. Ezt Windows NT-nél a *Start/Programok/Adminisztráció(általános)* alatt találjuk meg, a Windows 2000-nél ugyanez a *Start/Programok/Adminisztráció*-nál bújik meg.

A Windows NT-nél az eszköztárnál

30 A legfontosabb Linux parancsok áttekintése

A Linux a KDE-vel kényelmes felhasználói felületet kínál. De bizonyos dolgokat gyorsabban és kényelmesebben lehet a parancssorban, vagyis a shell-ben elvégezni. Összeggyűjtöttük tehát a fontosabb parancsokat.

Parancs	Megjegyzés
arp-a	Megjeleníti az arp-cache tartalmát. Itt látható a kliens MAC-címe.
awk	Az „awk"-val fájlokból, például a log fájlokból lehet kiszűrni és feldolgozni bizonyos információkat.
cd/könyvtár	Váltja az aktuális könyvtárat.
chmod –R	A fájlhozzáférési jogokon változtathatunk a segítségével.
chown –R	A fájl/könyvtár tulajdonosát/csoporthoz tartozását lehet megváltoztatni.
cp –R	Fájlmásolás.
df –k	Jelzi a merevlemez szabad tárkapacitását.
du –s	Megmutatja egy könyvtár által foglalt tárhelyet.
find –name – type – exec – print	Fájlokat, könyvtárakat, készülékeket (devcies) jelenít meg.
Grep	Az adatfolyamból kiszűri azt a sort, amely a megadott mintához illeszkedik.
Ifconfig	Felsorolja a telepített hálókártyák, ISDN kártyák legfontosabb hálózati paramétereit.
Locate	Fájlokat/könyvtárakat kereshetünk adatbázisban.
ls –l –d	Listázza az aktuális könyvtár fájljait.
mkdir KÖNYVTÁR	Létrehozza a KÖNYVTÁR-at.
mount / dev/ fd0 / floppy	Egy frissen behelyezett flopit inicializálhatunk a segítségével.
Mv	Fájlokat vagy könyvtárakat tolhatunk el a merevlemezen.
Netstart – r –n	Különböző hálózati paramétereket tekinthetünk meg, például routing táblázatokat és aktív TCP/UDP csatlakozásokat.
Passwd	Megváltoztathatjuk az aktuális felhasználó jelszavát.
ping –r 111.111.111.111	Megtudhatjuk, hogy aktív-e (még) a megadott IP-cím. Alternatívan DNS nevet is megadhatunk.
Pwd	Megjeleníti az aktuális könyvtárat.
rm –r –f	Fájltörlés.
tail –f/var/log/messages	Élőben követhetjük nyomon a rendszer státuszjelzéseit. Ideális a hibakeresésnél és -javításnál.
tar –vczf	Több fájlt eggyé olvaszt össze.
Tcpdump –i	Informál a hálón szállított összes csomagról.
umount/ floppy	A flopit a kivétele előtt ki kell log-olni a rendszerből.

kattintsunk a plusz jelre, és az *Objektum* mezőben válasszuk ki a hálózati szegmens bejegyzést. Ha ez nincs jelen, akkor utólag telepítsük a hálózati monitor ügynököt. A Windows 2000-nél itt több objektum áll rendelkezésre – mindenekelőtt a *szegmensek/s* teljesítmény-indikátoros TCP objektum lehet érdekes.

31 Eljárások automatizálása Linux alatt

Az ismétlődő eljárásokat, mint például elektronikus levelezés, backupkészítés stb. automatizálni lehet a Linux szervernél. Ebben a *Cron-Job* segít.

A Cron-Jobbal időzítéses irányítással indíthatunk tetszőleges programot a Linux alatt. A Linuxnál ezt a *cron* segítségével oldjuk meg – aki nem szívesen dolgozik a parancssoron, az a KDE alatt alkalmazhatja a *kcron*-t is. Itt némi egérkattintás árán automatizálva hajthatunk végre folyamatokat, viszont jó ha tudjuk, hogy melyik programnak melyik felhasználónál kell futnia a későbbiekben. Ez általában a felhasználó root, amely rendszer- és adminisztrációs munkákat hajtat végre. Természetesen az összes többi felhasználó is definiálhat Cron-Job-okat, amelyek azonban csak akkor hajtódnak végre sikeresen, ha a felhasználó rendelkezik az ehhez való jogosultságokkal.

32 Több IP-cím egy hálózati kártyával

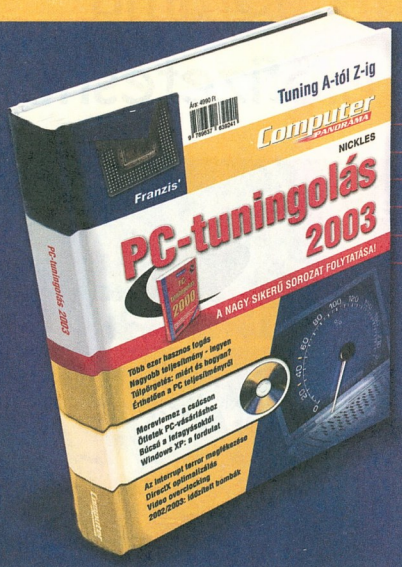
Akinek a linuxos szerverén csak egy hálózati kártyája van, mégis több IP-címre lenne szüksége, az a *yast* nevű program segítségével megoldhatja a hozzárendelést. Nyissuk meg a shellbeli yast-ot a *Rendszeradminisztráció/Hálózati kártya konfigurálása/Hálózati alapkonfiguráció–nál,* és válasszuk ki a megfelelő hálózati kártyát. Írjuk be a kívánt IP-címet, a hálózati maszkot és ha szükséges a Gateway-t, vagy aktiváljuk a hálózati kártya DHCP-jét. Az **F4** funkcióbillentyű segítségével aktiválhatjuk a beállításokat. A második IP-címet a következőképpen kell megadni: válasszunk egy szabad bejegyzést – tehát egy olyat, ahol a hálózati típusnál *<None>* áll, és nyomjuk meg az **F5** funkcióbillentyűt. Ezt követően válasszuk ki a *<másik Device megadása>* bejegyzést, és írjuk be a *Device* megnevezéséhez azt, hogy *eth0,* ha további IP-címre van szükség az eth0 hálózati kártyához. Ezután a megszokott módon konfigurálhatjuk e bejegyzés hálózati paramétereit.

33 A DSL Flat ráta kicselezése

A Flat-ráta egy bizonyos idő elteltével automatikusan bontódik. Hogy a kapcsolat ne szűnjön meg automatikusan, érdemes a mail-programunkat használni. Ezt konfiguráljuk úgy, hogy 10 percenként kérdezze le a mail-szervert beérkezett üzenetek után.

A Microsoft Outlook 2000 esetén menjünk a menüsorban az *Extrák*-nál az *Opciók*-ra, válasszuk ki az *Email átvitelt,* és állítsuk be az *Email-postafiók-opciók-nál* az időintervallum nekünk megfelelő értékét.

Amit a PC-tuningolásról tudni kell



- Több ezer hasznos fogás
- Nagyobb teljesítmény - ingyen
- Túlpörgetés: miért és hogyan?
- Érthetően a PC teljesítményről
- Ötletek PC-vásárláshoz
- Búcsú a lefagyásoktól

Megrendelhető:
Computer Panoráma Kiadói Kft.
1091 Budapest, Üllői út 25.
Telefon: 456-6964, Fax: 456-6970
E-mail: terjesztes@cpanorama.hu
Ára: 4990 Ft

Mi lehet még jobb
egy Computer Panoráma
előfizetésnél?

12 Computer Panoráma,
12 teljes film,
+ 36 CD-nyi számítástechnikai program

23 900 Ft (Két példány ingyen!)

Extra szolgáltatás: minden küldeményt légpárnás, ütés- és törésbiztos borítékban, ajánlott küldeményként postázunk, amelynek költségeit az előfizetési ár TARTALMAZZA.

Ne késlekedjen, fizesse be még most a mellékelt csekken szereplő összeget! Várjuk előfizetőink népes táborában!

ELŐFIZETÉS

Egy DVD-mellékletes Computer Panoráma előfizetés!

Computer Panoráma Kiadói Kft., 1091 Budapest, Üllői út 25.
Telefon: 456-6964, fax: 456-6970
E-mail: terjesztes@cpanorama.hu
Internet: www.computerpanorama.hu/elofizetes

Computer PANORÁMA

LG

OPTIKAI TÁROLÓK

AZ LG OPTIKAI MEGHAJTÓK NEMZETKÖZI DÍJAI

LG Electronics Magyar Kft.
www.lge.co.hu

Computer Hoy | Calidad
Feb. 01 Spain
CED-B0808

Chip | Performance Winner
Nov. 00 Germany
CED-B0808

Computer easy | EMPFEHLUNG
Oct. 00 Germany
CED-B0808

PC Plus | Performance Award
Aug. 00 UK
CED-B0808

PC QUEST | Editor's Choice
Jun. 00 India
CED-B0808

Computer Partner | Component for reference PC
May. 00 Germany
CED-B0808

Computer Bild | Test Winner
May. 00 Germany
CED-B0808

PC WORLD KOMPUTER | Our Best Purchase
Apr. 00 Poland
CED-B0808

Computer Channel | Best Performance
Mar. 00 Germany
CED-B0808

PC Direkt | EMPFEHLUNG
Jan. 00 Germany
CED-B4028

Preis/Leistung
Qualität

PC Praxis | Fast recorder
Jul. 00 Germany
CED-B0808

CHIP TIP
Styczeń 2001
ECONO

Chip | Tip Econo
Jan. 01 Poland
DRD-B1208

PCgo!
1/2001
TESTSIEGER

PC Go | EMPFEHLUNG
Jan. 01 Germany
DRD-B1208

PC PRAXIS
Preistipp

PC Praxis | Price Tip
Jul. 00 Germany
DRD-B0808

PC Magazin
EMPFEHLUNG DER REDAKTION

PC Magazine | Editor's Choice
Jun. 00 UK
DRD-B0808

PC-WELT
TOP 10
PLATZ 1

PC-Welt | Test Winner
May. 00 Germany
DRD-B0808

ENTER

Enter | Editor's Choice
Mar. 00 Poland
DRD-B0808

Gold Award
PC Format

PC Format | Gold Award
Mar. 00 South Africa
DRD-B0808

PC
SHOPPING
EMPFEHLUNG

PC SHOPPING | EMPFEHLUNG
Jan. 00 Germany
DRD-B0108

TESTSIEGER
computer channel

Computer Channel | Test Winner
Feb. 00 Germany
CED-B4028