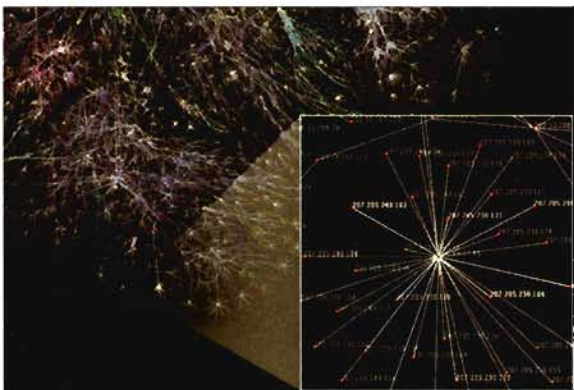


Alapbeállítások és hálózati alap



Router iskola – 1. rész

Új sorozattal jelentkezőnk, amelynek elolvasása után nagy biztonsággal fogjuk kezelni a broadband routereket. Bemelegítésként ismerkedjünk meg a hálózatbeállítás alapfogalmaival.

Szerző: Köhler Zsolt



A routerek fénykora az internet elterjedésével együtt kezdődött, hatalmas sikerüket az egyszerű webes konfigurációnak és kedvező áruknak köszönhetjük. Noha beállításuk csakugyan egyszerű, a sok opció között könnyen elveszhetünk. A funkciók megértéséhez egy kis elméleti kitérőt szükséges tennünk, amelyből kiderül, hogyan és milyen szabályok szerint működik a hálózat, az internet.

A hálózat hét bőre

Minden vezeték vagy vezeték nélküli hálózatnak megfelelő protokoll szerint kell működnie. A szabályok arra vonatkoznak, ki, milyen módon adhat és vehet adatot. A hálózatok működésének szemléltetéséhez leggyakrabban az OSI (Open

Systems Interconnection Basic Reference Model) modellt használják. Ezt a modellt az ISO 1977-ben dolgozta ki, és minden létező hálózatra adaptálható.

A modell hét rétegből áll, ezek az „alkalmazástól a rézdrótig” képezik a modellt egy-egy részét, egymással kapcsolatban állva. A részletekbe most felesleges lenne belemenni, de azt mindenképpen tudnunk kell, hogy a rétegek (és a mögötük lévő konkrét hardverek és szoftverek) teszik lehetővé azt, hogy az adatok a fizikai rétegre eljutva minden olyan információval el legyenek látva, amelyek a nagy hálózatokban való hatékony mozgathatóságukhoz szükségesek. A hálózaton átjutott adat ugyanezeket a rétegeket fordítva járja be, hogy a végén a számítógé-

pen használt alkalmazáshoz eljusson. Jelentős különbségek vannak a programokból küldött és a „dróton” mozgó adatok között – utóbbiak a különféle azonosító, hibajavító és titkosító módszerek miatt nagyobbak. Az ilyen többletadatokat hívják overheadnek. Ezek nem csak az Ethernet és WLAN hálózatokban, hanem szinte minden tényleges hálózatban (pl. GSM) és kommunikációs rendszerben (például az alaplapok buszrendszerénél) is léteznek.

Címéhség

Az internet alapvető protokollja a TCP/IP (Transmission Control Protocol/Internet Protocol), amely valójában protokollok gyűjteménye. Ezek az átküldendő adatokat csomagokra bontják, azokat ellátják a szükséges fejléccel (ún. headerrel), majd továbbítják őket. Ahhoz, hogy a küldőt és a fogadót is azonosítani lehessen, minden számítógépnek szüksége van egy azonosítóra.

OSI Modell

Szint	Neve	Adat típusa	Funkció röviden	Adott szinthez (is) tartozó példa
7	Alkalmazási réteg	Adat	Alkalmazásszintű kommunikáció	HTTP, FTP, SMTP, SNMP, Telnet
6	Megjelenítési réteg	Adat	Adatformátumot hoz létre az alkalmazások számára (adatkonverzió)	ASCII, EBCDIC, JPG, SSL
5	Viszonylati (session) réteg	Adat	Alkalmazások közötti adatkapcsolat kezelése duplex vagy félduplex módon	NetBIOS, NWLink
4	Szállítási réteg	Szegmens	Transzparens adatátvitel biztosítása, kapcsolat ellenőrzése	TCP, UDP, SPX, NetBEUI
3	Hálózati réteg	Csomag (packet)	Útvonalválasztás, magasabb szintű hibajavítás, logikai címzés	IP, ICMP, IPX, RIP, BGP
2	Adatkapcsolati réteg	Keret (frame)	Adatok kezelése, hibajavítás, fizikai címzés kezelése	Ethernet, PPP, ATM, Fibre, Channel, MAC
1	Fizikai réteg	Bit	Adatok továbbítása, kapcsolat kezelése (elektromos vezetékek)	RS-232, 100BaseTX, ISDN, DSL, X.25

A router iskola részei

1. Alapbeállítások és hálózati alapismeretek
2. WAN és LAN
3. Vezeték nélküli
4. Tűzfalak, szűrők, VPN
5. VoIP és streaming
6. Haladó beállítások
7. Hardvertuning, firmware-frissítés
8. Hardveres-szoftveres különlegességek

ismeretek

A hálózati kártyák és minden hálózati eszköz rendelkezik hardveres MAC (*Media Access Control*) címmel, ám ez hossza miatt nem hatékony, csak a közvetlenül egymáshoz kapcsolódó készülékek alacsony szintű kommunikációjában vesz részt. Mivel a hálózatokhoz kapcsolódik, ezzel is foglalkoznunk kell. Magasabb szinten a készülékek IP-címet kapnak, amely jellemzően négy, legfeljebb 255 (hexadecimálisan FF) számjegyből áll.

Ezzel a módszerrel 256⁴, tehát körülbelül 4,29 milliárd IP-cím képezhető. Eből le kell vonnunk a privát helyi hálózati

saját privát IP-címet kap, kötelezően eltérőt, amelyet a külső hálózat használ. Ennek megfelelően a routernek egy belső (LAN) és egy külső (WAN) oldala van, és mind a kettőnek saját címe van.

Nézzünk egy példát! Ha a bővíteni kívánt hálózat helyi címe a 192.168.0.1-192.168.0.254 tartományban van, akkor az alatta lévő hálózat ezt nem használhatja, helyette egy másik privát tartományt, például a 192.168.1.1-192.168.1.254 címeket veheti fel. A router dolga az, hogy a kívülről érkező adatokat a belső hálózat megfelelő számítógépére továbbítsa és viszont: a kapott csomagokat úgy módosítja, hogy azok a másik hálózatban is értelmezhetők legyenek, pontosan ahhoz hasonlóan el, akiknek szánták őket. Az úgynevezett *routing table* megmutatja, hogy

meglátogatnak ahhoz, hogy a célállomáson a fogadó számítógép azokat összerakva értelmezni tudja az üzenetet.

Forgalomirányítás

De honnan tudja a router, hogy a belső hálózaton mozgó adatok közül melyiket kell kiküldenie? A fent említett címfordítás igen erőforrás-igényes feladat lenne, ha a helyi hálózaton mozdó összes csomagot ellenőrizni kellene. A művelet meggyorsítása érdekében találták ki az alhálózati maszkot (*Subnet mask*).

Mint a neve is mutatja, a maszkot a router az IP-cím „maszkolására” használja, így villámgyorsan meg tudja állapítani, hogy a csomag a helyi hálózatba vagy az internetre irányul-e. A maszknak egy helyi hálózaton belül minden gépen azonosnak kell lennie, hiszen így azonosítja azokat a gépeket, amelyek a hálózathoz tartoznak. Ez a maszk az alhálózat nagyságától függően változhat (lásd a táblázatot).

Az interneten (publikus hálózaton) kiküldött adatok nem véletlenül, hanem a routerek szabályainak megfelelően vá-

tok számára fenntartott címeket (kb. 18 millió), az úgynevezett multicast címeket (kb. 270 millió).

Máris láthatjuk, hogy hamarosan elfogy a rendelkezésre álló címek mennyisége. Az IPv4 helyett éppen ezért használják már sok helyen az IPv6-ot is, amely nem négy, hanem hat számból áll. Kiszámolhatjuk, hogy ezzel 65 536-szor több cím hozható létre, amely körülbelül annyi, hogy a föld minden négyzetmilliméterére ötezer IP-cím jutna. Ez már egészen biztosan elég, legalábbis addig, amíg az emberiség néhány bolygót nem gyarmatosít.

Azért, mert az internet soha nem statikus, mindig igény van arra, hogy egy hálózatot egy másik hálózathoz csatlakoztassunk (fizikailag). A káosz elkerülésére született meg a router.

Mire való a router?

A router a hálózatba kötve úgy viselkedik, mintha számítógép lenne: adatokat küld és fogad. Saját IP (és MAC) címmel rendelkezik, tehát gond nélkül illeszkedik a hálózatba. Attól különleges, hogy számítógépeket köthetünk rá, amelyek egy belső hálózatot fognak alkotni, a külvilággal pedig a routeren keresztül tartják a kapcsolatot. A belső hálózat minden gépe

Néhány fontos címtartomány

Tartomány	CIDR jelölés	Funkció	Kliensek száma
10.0.0.0-10.255.255.255	10.0.0.0/8	Privát címek	16 777 216
127.0.0.0-127.255.255.255	127.0.0.0/8	Helyi loopback címek	16 777 216
172.16.0.0-172.31.255.255	172.16.0.0/12	Privát címek	1 048 576
192.168.0.0-192.168.255.255	192.168.0.0/16	Privát címek	65 536
224.0.0.0-239.255.255.255	224.0.0.0/4	Multicast	268 435 456

melyek egy kommunikációs kapcsolat külső és belső hálózaton lévő partnerei. Ez a tábla a kapcsolatok létrejöttékor folyamatosan frissül, és a router ez alapján végzi el a kitöltésének megfeleltetést. Ez a folyamat a NAT (*Native Address Translation*), amelyet minden router ismer.

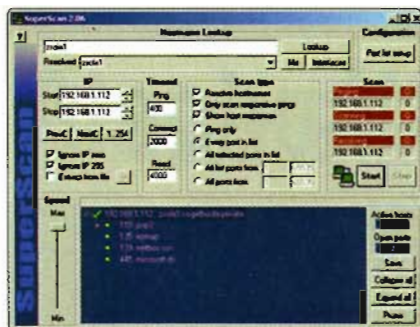
A fenti kétszintű hálózat egyszerűnek tűnik, de ha nekünk a világ másik oldalára, több hálózaton keresztül kell adatot küldelnünk, akkor a routereknek együtt kell működniük egymással. Mivel a hálózatok egyszerre több hálózattal is kapcsolatban áll(hat)nak, a küldő és a fogadó között több lehetséges út létezik. A routerek feladata minél hamarabb, minél biztosabban eljuttatni a csomagot a címzettnek. Ha egy hálózat – mint gyenge láncszem – kiesik vagy gyengén teljesít, a routerek közösen új utat keresnek. Az is lehet, hogy a világ túloldalára küldött állományunk csomagjai egymástól távol eső helyeket is

lasztják meg az útvonalukat. Innen ered a router magyar neve, az *útválasztó*. A routerek egymással a különféle speciális protokollokat használva tartják a kapcsolatot. Közülük a legrégebbi a RIP (*Routing Information Protocol*), ám léteznek biztonságosabb, dinamikusabb vagy éppen egy-egy hálózaton hatékonyabb protokollok is, például az IGRP, az OSPF vagy az internet gerinchálózatán használt BGP. A legkisebb hálózatokban a RIP a leggyakoribb, variánsairól természetesen később szót ejtünk.

Portok

A portok szó szerint kikötők, a csomagok mindegyike tartalmazza a hozzá tartozó portcímet is. Egy számítógépnek 65 535 portcíme lehet.

A portok leegyszerűsítik a hálózati adatok kezelését, egy böngészőszoftver segítségével pontosan tudja, hogy szá-



Tűzfal nélkül a nyitott portok várják az adott kategóriába tartozó csomagokat

mára a 80-as porton adat érkezett, és azt a http szabvány szerint kell értelmeznie.

Ugyanígy a levelezőprogramok a 110-es (POP3) porton kérdezik le a leveleket a szerverről, a programok levélküldésre pedig a 25-öst használják. Egy magas számú portot is említhetünk: a Call of Duty 2 című játék például a 28960-as portot használja. Ha már itt tartunk: a 49152 és a 65535 közötti tartomány a dinamikus (a programok által létrehozott és ideiglenesen használt) portok számára van fenntartva. A portok a router szempontjából azért fontosak, mert a NAT során nem csak az IP-cím, de a portcím is számít, azzal különféle „trükköket” is véghez lehet vinni, portot nyitni egy program számára vagy szabályozni a forgalmat. A programon múlik, hogy melyik portot használja: az ajánlás nem kötelező érvényű, de szükséges a kompatibilitáshoz.

A hardver

Térjünk rá most a hardverre: tipikusan egy WAN (Wide Area Network) – internet felé irányuló – és négy LAN (Local Area Network) – helyi port – található egy routeren. Számítógépeinket a LAN portra kötjük, akár többet is: switchekkel a hálózat tovább bővíthető, elvileg ezért egy LAN port is elegendő.

A vezetékek nélküli változatok leggyakrabban egy hálózatként kezelik a LAN és a WLAN (Wireless LAN) területet, ám sok kivétel is akad. A készülékeken LED-eket látunk, amelyek a hálózati kártyák hátoldalán lévő visszajelzőkkel azonos módon működnek: kapcsolat esetén folyamatosan világítanak, forgalom esetén pedig villognak. Típusa válogatja, hogy a készüléken WAN1 és WAN2, illetve DMZ (DeMilitarized Zone, erről később), STATUS vagy FIREWALL LED-ek is vannak-e.

A routerben egy célprocesszor (ASIC, Application-specific Integrated Circuit) működik a hozzá tartozó memóriával,

integrált vagy különálló hálózatvezérlő áramkörrel. WLAN routernél ez kiegészül az alaplapra szerelt WLAN IC-vel vagy a csatlakozóba szerelt PCMCIA vagy miniPCI moduldal.

Valóban különleges és ritka esetekben érdekelhet, hogy mekkora a router memóriája, és hány MHz-en ketyeg a CPU órajele, de fontosabb kérdés, hogy mit tud az eszköz, és például hány felhasználót, hány csatlakozást képes egyszerre kiszolgálni.

A router tudásának nagy részét a processzoron futó program, a *firmware* hordozza, azt pedig legjobban a működésén keresztül lehet megérteni.

Előkészületek

Vettünk egy új routert, de be kell állítanunk: vagy a hozzá tartozó szoftverrel kényelmesen, lépésről lépésre haladunk (D-Link), vagy belépünk a router adminisztr-



Az IPCONFIG /ALL parancs hatására hálózati kártyánk MAC-címét is megkérdezzük

ációs menüjébe, és ott végezzük el a beállításokat. Mivel ez utóbbi módon szinte minden router konfigurálható (még a D-Link is), ezt mutatjuk be.

Első lépésként csatlakoztassuk számítógépünk egyik szabad hálózati kártyájához a router egyik LAN portját, majd kapcsoljuk be a készüléket. Kis idő elteltével a router LAN lámpái villogni, majd világítani kezdenek, jelezve, a kapcsolat rendben van. Ugyanezt a jelzést a hálózati kártya (NIC, Network Interface Controller) hátulján lévő LED-ek is adják. Ha a képernyő jobb alsó sarkában nem jelenik meg a hálózati kapcsolat ikonja, akkor nyissuk meg a *Vezérlőpult/Hálózati helyek/Tulajdonságok* ablakát, majd a helyi hálózati kapcsolat tulajdonságok ablakában kapcsoljuk be az alsó két opciót. A tálcákon jó csatlakozás esetén két monitorral jelzi, hogy a kapcsolat rendben van,

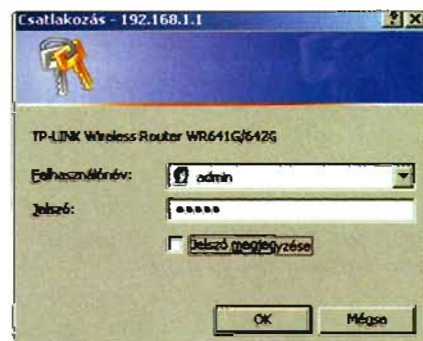
ha viszont sárga felkiáltójelet kapunk, akkor a kapcsolat jó, de számítógépünk nem kapott IP-címet.

A routerek gyári konfigurációja szerint minden esetben bekapcsolt a DHCP szerver (*Dynamic Host Configuration Protocol*), a legegyszerűbb a router újraindítása a hátoldalán lévő reset gomb 4-8 másodpercig tartó megnyomásával. Az újraindulás után gépünk már kap IP-címet a szerverről. Ha mégsem, akkor ne nyomogassuk/kapcsolgassuk a routert, bizonyos esetekben ugyanis a firmware is törölhető ily módon. Segíthet, ha megnezzük a router alját: azon sok esetben ott van a gyári IP-cím (192.168.0.1, 192.168.1.1, 192.168.2.1, esetleg 192.168.2.254).

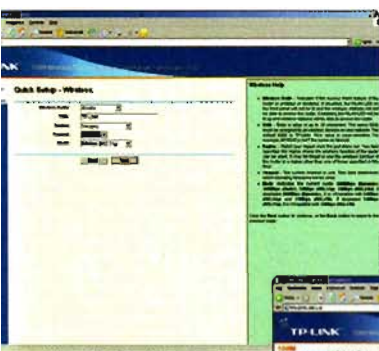
Ha a DHCP szerver nincs bekapcsolva, kézzel kell címet adnunk gépünknek, a routerrel azonos tartományban, tehát csak az utolsó számjegyek kell különböznie (100-150 között egészen biztosan szabad). A Subnet mask szokás szerint 255.255.255.0 legyen, az átjáró ekkor még nem szükséges, internetezéshez viszont majd a router IP-címével kell egyeznie. Ha a kapcsolat felépült, nyissunk meg egy böngészőt, és a címsorába írjuk be a router IP-címét! Ha mással nem, Internet Explorerrel működni kell. Jó esetben, ha a DHCP kezdetektől fogva működött, a hálózati kapcsolat állapot ablakának *Tárogatás* füle alól „lelehetjük” a router címét az *Alapértelmezett átjáró* sorban.

Belépés, beállítás

A megjelenő ablakban adjuk meg felhasználói nevünket és jelszavunkat! Ezt szintén a router alján vagy a mellékelt dokumentációban találjuk: a „Username” leggyakrabban admin vagy administrator, de lehet smcadmin, root is. Gyakori megoldás, hogy vagy ezt vagy a jelszót nem kell megadnunk, de ha jelszó kell, akkor az admin, a default, 1234 vagy a pass sza-



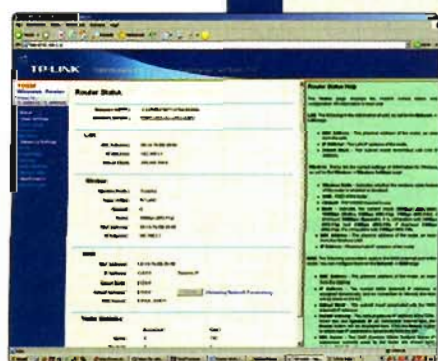
A bejelentkezés néha csak Internet Explorer alatt működik – routere válogatja



Gyors beállításoknál a WLAN konfigurációja egyszerű, alapértelmezett módban is működik

Ennél többre nincs szükségünk: PPPoE, dinamikus vagy statikus IP kapcsolat

A Status alatt ellenőrizhetjük a beállítások helyességét



vakból válogasunk.

Első választásunk (ha van) a gyors beállítás legyen (Quick Setup). Akár ezt, akár a normál beállítást

választjuk, néhány opciót mindenképpen be kell állítanunk. A WAN Connection Type alatt csatlakozásunk típusát kell megadnunk. ADSL esetén PPPoE, kábelmodem esetén Dynamic IP-t kell választanunk. Előbbinél a szolgáltató által adott felhasználói nevet és jelszót kell megadnunk, utóbbinál viszont a router az IP-címet úgy szerzi a szolgáltatótól, ahogyan a gépünk a routertől: DHCP-t használva. A szolgáltató ez esetben a hálózati kártyánk MAC-címét is bejegyzí.

Routerünknek tehát számítógépünkre kell hasonlítani minden szempontból, ezért kell használnunk a Clone MAC Address opciót a MAC-cím lemásolására. Ebből adódik, hogy azzal a számítógéppel végezzük a router beállítását, amellyel egyébként az internetre csatlakozunk.

A helyi hálózatunk a sikeres csatlakozás esetén biztosan működik, igény szerint módosíthatjuk mind a router IP-címét, mind a hálózati tartományt. Ha nem működne, engedélyezhetjük az esetleg tiltott DHCP szervert, amely kisebb biztonságot ad, de leegyszerűsíti a további számítógépek csatlakoztatását. A vezeték nélküli hálózat beállítására később térünk ki, az alapértelmezett opciók általában olyanok, hogy a vele azonos kategóriájú (54 Mbites) klienssel biztosan csatlakozni tudunk a routerhez. Az ország beállítása segít, hogy ne szegjünk törvényt: hazánkban az 1-13 csatornák frekvenciái használhatók szabadon.

A konfiguráció mentése után menjünk a Status menübe, és ellenőrizzük, hogy a router csatlakozik-e az internethez. Ekkor a WAN csatlakozó többek között IP-címet is kap, a WAN LED pedig aktivitást jelez.

Az internetkapcsolatnak ezek után mindenhol működnie kell, amelyet a későbbi beállításokra térve még finomhangolunk. A hibakeresésre igény szerint, az Olvasói rovatunkba érkező levelek alapján térünk majd ki.



TP-LINK

Behálózuk a világot.



Super G & Kiterjesztett Hatótáv™ 54/108Mbps vezeték nélküli Router

- 108M vezeték nélküli LAN Router, 2.4GHz
- 802.11g/b, beépített 4-portos Switch-csel
- 108M Super G™ technológia
- 2x-3x Kiterjesztett Hatótáv™ technológia
- forgatható SMA Antenna



Super G & Kiterjesztett Hatótáv™ 54/108M vezeték nélküli USB Adapter

- IEEE 802.11g WLAN USB Adapter
- Super G™, akár 54/108Mbps átvitel
- teljes 802.11b kompatibilitás
- Kiterjesztett Hatótáv™, akár 9x nagyobb, mint a normál vezeték nélküli adaptereknél



Super G & Kiterjesztett Hatótáv™ 54/108M vezeték nélküli PCMCIA Adapter

- IEEE 802.11g WLAN PCMCIA Adapter
- Super G™, akár 54/108Mbps átvitel
- teljes 802.11b kompatibilitás
- Kiterjesztett Hatótáv™, akár 9x nagyobb, mint a normál vezeték nélküli adaptereknél



6dBi 2.4GHz beltéri asztali Yagi Antenna

- Frekvencia távolság: 2.4GHz - 2.5GHz
- Sugárzási irány: kétféle
- Jél erősség (csúcsérték): 6dBi
- Kábel hossz: 100cm
- Csatlakozó: SMA közvetlen dugó/fordított



Kábel/DSL Router beépített 4/8 portos Switch DDNS felügyelet, 802.1X

- 4/8 db 10/100Mbps LAN port
- 1 db 100Mbps Auto-Negotiation WAN RJ45 port
- Beépített tűzfal IP cím szűréssel
- Domain Name és MAC cím szűrés
- Felhasználói adminisztráció, webcím szűrés

Adatátvitel



Kiemelt importőr:
Mercury Magyarország Kft.

1131 Budapest, Dolmány u. 14.
tel.: 221-3020 fax: 221-4254
www.mercurycomputer.hu
mercury.hungary@ahol.com

WAN és LAN hálózatok



Router iskola – 2. rész

Sorozatunk második részében a mélyére ásunk annak, mi mindent módosíthatunk ahhoz, hogy a LAN oldalon ne csupán csatlakozni tudjunk, de hatékonyan és gyorsan internetezhessünk is.

Szerző: Köhler Zsolt

Internet



Különleges esetekben VPN szerverhez is csatlakozhatunk; ha sikerül, megjelennek a távoli hálózat címei

Internet, esetleg WAN névvel jelölik azokat az opciókat, amelyek a router kívül felé irányuló portját konfigurálják. Mivel a tényleges munkavégzés a routeren belül, illetve a belső hálózaton történik, itt viszonylag keveset találunk. A kapcsolat típusa (*Connection type*) az előző számunkban már említett

PPPoE vagy *Dynamic IP (DHCP Client)* üzemmódokon kívül sok esetben lehet még *statikus*, *PPTP* vagy *L2TP* beállítású. Ha a *BigPond* névvel találkozunk, azt egészen biztosan nem kell majd használnunk, hiszen ez egy ausztrál internetszolgáltató kapcsolataira vonatkozik.

A *statikus IP*-ről már ejtettünk szót, ennél a módnál meghatározhatjuk routerünk WAN oldali, azaz publikus IP-címét. Otthoni használatban ez nyilván nem működik, ám ha cégünk hálózatában kell létrehoznunk egy alhálózatot, akkor a jelenlegi LAN hálózatba illeszkedő címet kell adnunk a routernek akkor, ha a nagyobb hálózaton nem működik DHCP szerver. Ha igen, a *DHCP Client*-et kell beállítanunk.

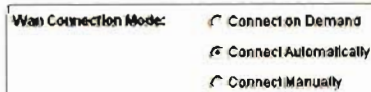
A helyi hálózatot ritkán kell így bővítenünk, a statikus IP indokolt lehet akkor, ha egy WLAN routerből szeretnénk internet-hozzáférést adó hozzáférési pontot létrehozni.

A *PPTP (Point-to-Point Tunneling Protocol)* kapcsolódásnál két, a világon bárhol lévő router belső hálózatát köthetjük össze úgy, hogy az adatok az interneten titkosítva halad-

nak. Ez a VPN, amelyről később lesz szó részletesen. Nagyon kevés olyan „otthoni” router létezik, amelyik VPN szerverként is működik, a céges hálózathoz való csatlakozást viszont megoldhatjuk vele. Kliensként fix IP-címmel kell rendelkez-nünk, és tudnunk kell cégünk VPN szerverének szintén fix IP címét is. Ez utóbbi a *Gateway IP address*, amelyet meg kell adnunk a felhasználói név és jelszó társaságában.

Az *L2TP* hasonló szintű kapcsolatként funkcionál, mint a *PPTP*, szintén VPN hálózat létrehozására való. Itt csak a szerver címét, felhasználói nevünket és jelszavunkat kell megadnunk, mivel a kapcsolat kiépítését mindig a kliens kezdi.

Meddig netezhetünk?



Automatikus csatlakozáskor a router figyel, mikor lesz (ismét) elérhető az internet, ha valami miatt megszakad

Azoknál a kapcsolatoknál, ahol a hálózatba be kell jelentkeznie a routernek (PPPoE, VPN), a kapcsolat felett a szerver rendelkezik. Az internetszolgáltatók azért hasz-

nálják a DHCP-t, mert nem kell nyilvántartani az alkalmi vagy a hosszú távon csatlakozó klienseket.

A szolgáltató oldalán lévő hálózati eszközöknek boldogulniuk kell a változó számú aktív felhasználóval, ezért adott időközönként megszakítják a kapcsolatot. Szoftveres csatlakozás esetén csak egy ablak jelenne meg „a kapcsolat időtúllépés miatt megszakadt” üzenettel. A routeren nem tudnánk, hogy éppen él-e a kapcsolatunk, ezért a router két minta között dönt, milyen csatlakozási stratégiát válasszon: az elsőnél a router akkor fog a hálózatra csatlakozni, ha a belső hálózatról valaki ki szeretne menni a netre. Le- vagy feltölt egy adatot, majd sokáig hallgat.

Mielőtt a szolgáltató szakítaná meg a kapcsolatot, a router le tud lépni a hálózatról, majd igény szerint újra csatlakozik. Ez a *Connect On Demand* módszer, amelynél a lekapcsolódásig eltelt tétlen időt is megadhatjuk (mivel a routerekben van belső óra is). Különleges eset, ha nullát adunk meg az *Idle Time* értékének: a router nem fogja megszakítani a kapcsolatot. A szolgáltató viszont egy rövid időre igen, amikor a DHCP szervere új IP-címet ad nekünk. Ez még akkor is előfordulhat, ha fix IP-címünk van, ekkor ugyanazt a címet kapjuk vissza, ami volt.

A másik módszer a *Keep Alive*, aktiválásakor a router adott időnként küld és fogad adatot (pingel), így a szolgáltató számára úgy tűnik, hogy aktív, a kapcsolatot ezért nem szakítja meg.

Az előbbi opciót akkor válasszuk, ha napjában csak pár-szor csatlakozunk az internetre (ha állandóan fent vagyunk, akkor nullázzunk), az utóbbit pedig akkor, ha a szolgáltató előszeretettel szakítja meg netkapcsolatunkat. Ez utóbbi ma már nem divat, ezért szerencsére nincs rá sok szükség.

A belső óráról

Az órával kapcsolatos beállításokat nem szokták előre kitölteni, mert a routert a világ minden táján használhatjuk

lítása azért is fontos, mert időzítve indíthatunk különféle szolgáltatásokat az igazán nagy tudású típusokon, de hogy csak egy egyszerű dolgot mondjunk: a naplófájlhoz pontos idő is tartozik.

Érdekességként említsük meg az *NTP (Network Time Protocol)* rendszert, amely közvetlen hozzáférést biztosít a világ különféle atomóráihoz; segítségükkel több számítógép óráját – így a routerét is – szinkronizálni lehet.

Elsőként a *D-Link* kezdte használni a pontatlanságot kiküszöbölő NTP-támogatást, amely adott időközönként aktiválódott. Sajnos publikus atomóra szerverek voltak megadva, és mivel az NTP protokoll valós idejű, tehát extra prioritást élvez, az igen népszerű routerek milliónyi időkéretet zúdítottak az addig csak szórványosan használt szerverekre. Még is bémúlt a forgalom, a *D-Link* ezért beállított egy saját szervert (hát nem rendese?), átállította routereit, a hiba meg is szűnt. Sőt: az opció kiválóan működik, igen kár, hogy kevés hálózati eszköz ismeri.

Sebességmámor

A fejléccadatok számítása alapján ez az érték is maximális: ha egy tűzfalon nem jutunk át, akár az MTU megváltoztatása is segíthet

dó PC-ken a Windows „logikus” beállításai következtében kicsi volt, csigalassúságot eredményezve. Ma már minden szolgáltató a maximumot, 1492-t használ.

Néhány routeren ez hibásan 1500, hozzá számolva a 8 bit azonosítót is. Ha kapcsolatunk a kábelek hibája miatt kissé zajos, az MTU csökkentése növeli a sebességet, hiszen kisebb adatokat kell a hibák miatt újraküldeni. Az ideális nagyságot sajnos csak tapasztalati úton próbálhatjuk ki, kifogástalan

Szinte minden esetben szerepel az *MTU (Maximum Transmission Unit)*, amely a közvetlenül kapcsolódó

Super G & Kiterjesztett Hatótáv™ 54/108Mbps vezeték nélküli Router

- 108M vezeték nélküli LAN Router, 2.4GHz
- 802.11g/b, beépített 4-portos Switch-csel
- 108M Super G™ technológia
- 2x-3x Kiterjesztett Hatótáv™ technológia
- forgatható SMA Antenna

Super G & Kiterjesztett Hatótáv™ 54/108M vezeték nélküli USB Adapter

- IEEE 802.11g WLAN USB Adapter
- Super G™, akár 54/108Mbps átvitel teljes 802.11b kompatibilitás
- Kiterjesztett Hatótáv™, akár 9x nagyobb, mint a normál vezeték nélküli adaptereknél

Super G & Kiterjesztett Hatótáv™ 54/108M vezeték nélküli PCMCIA Adapter

- IEEE 802.11g WLAN PCMCIA Adapter
- Super G™, akár 54/108Mbps átvitel teljes 802.11b kompatibilitás
- Kiterjesztett Hatótáv™, akár 9x nagyobb, mint a normál vezeték nélküli adaptereknél

6dBi 2.4GHz beltéri asztali Yagi Antenna

- Frekvencia távolság: 2.4GHz - 2.5GHz
- Sugárzást irány: kétirányú
- Jel erősség (csúcsérték): 6dBi
- Kábel hossz: 100cm
- Csatlakozó: SMA közvetlen dugó/fordított

Kábel/DSL Router beépített 4/8 portos Switch DDNS felügyelet, 802.1X

- 4/8 db 10/100Mbps LAN port
- 1 db 100Mbps Auto-Negotiation WAN RJ45 port
- Beépített tűzfal IP cím szűréssel
- Domain Name és MAC cím szűrés
- Felhasználói adminisztráció, webcím szűrés

Adatátvitel



Kiemelt importőr:

Mercury Magyarország Kft.

1131 Bp., Dolmány u. 14. tel.: 221-3020 fax: 221-4254
www.mercurycomputer.hu mercury.hungary@ahol.com

hálózatban csökkentése a sebességet csökkenti, hiszen kevesebb adathoz relatív több fejlécadat (overhead) társul.

DDNS



Regisztráció után írjuk be adatainkat, majd léptessük fel a routert a DDNS szerverre – routerünk így egyszerűen elérhetővé válik

A dinamikus IP-cím egyszerű fenntarthatósága csak egy hátrányt hordoz, ez pedig a domainnév hiánya. Jellemző, hogy a céges internet-hozzáférések klasszikus esetben fix címmel rendelkeznek éppen azért,

hogy lehetőség legyen a belső hálózatra web- vagy FTP szerver telepíteni, amely egy böngészővel bárholnan elérhető.

De mi történik akkor, ha otthoni számítógépünket bárholnan és bármikor el szeretnénk érni? Ismernünk kellene az éppen aktuális IP-címét. Noha léteznek szerverek nélküli szoftverek e célra, a megbízhatóbb és egyszerűbb megoldást a DNS-szolgáltató szerverek jelentik.

Ezek a szerverek (és szolgáltatóik) előzetes regisztráció után létrehoznak egy aldomaint, majd nyilvántartják routerünk aktuális címét. Ha az internetről megnyitják a szolgáltatónál lévő weboldalunkat, az a felhasználót routerünkre irányítja. Ehhez az kell, hogy a szolgáltató ismerje routerünk mindig aktuális IP címét, amely éppen ezzel a támogatással küldi el a DDNS (Dynamic DNS) szolgáltatónak a címét.

A módszer praktikus, de hátránya is van: a routernek ismernie kell az adott szolgáltatót. A legnépszerűbb a névadó DynDNS, ám ezen kívül tíznél is több cég kínál ilyen szolgáltatást. Szerencsés esetben routerünkön van Custom (egyedi) opció, ahol bármilyen szolgáltató adatait (szervercím, felhasználói név, jelszó, egyedi opciók) megadhatjuk.

Internet nélkül

Az otthoni routereket csak bekapcsolt NAT-tal használjuk, noha a router alapvetően a hálózatok bővítésére szolgál. Ha egy nagyobb méretű hálózatban több routert kapcsolunk egymás alá, amelyben minden számítógépnek látnia kell a másikat, akkor a routeren ki kell kapcsolni a címfordítást (NAT-ot).

A Gateway opció átjárót jelent, ilyenkor a készülék használ NAT-ot. Ekkor gyakorlatilag teljesen mindegy, hogy az internetszolgáltatóhoz vagy egy másik hálózathoz csatlakozunk, a készülék kapcsolatot teremt a két (al)hálózat között.

A router iskola részei

1. Alapok
2. WAN és LAN
3. Vezeték nélkül
4. Tűzfalak, szűrők, VPN
5. VoIP és streaming
6. Haladó beállítások
7. Hardvertuning, firmware-frissítés
8. Hardveres-szofteres különlegességek

Ha kikapcsoljuk a címfordítást, a routerekkel kialakított hálózat logikailag egy egységet képez, fizikailag viszont nem csak csillag, illetve fa topológiájú lehet: a nagy hálózatban két pont között előnyös, ha egyszerre több útvonal létezik.

Az előző részben említettük, hogy a routerek különleges protokollokkal tartják a kapcsolatot, ezek egyikét kell bekapcsolni. Hogy melyiket, az a hálózat bonyolultságától és kihasználtságától függ.

A legáltalánosabb a RIP (Routing Information Protocol), amely viszonylag kis hálózatokban működik csak jól, a hálózat változásaihoz viszont nagyon lassan igazodik. Az OSPF (Open Shortest Path First) rendszert egyre több router ismeri, ám ennek hatékony működtetéséhez az összes routert finomhangolni kell, azon kívül, hogy pontosan meg kell adni, milyen hálózati topológián csúcsul.

Ha több, különféle routelési technikával működő nagy hálózatot kell összekapcsolnunk, akkor jön a képbe a BGP (Border Gateway Protocol), amely teljesen szabványos TCP kapcsolatot használva cseréli ki a routerek között az útvonalakat, és egyszerű PING csomagokkal ellenőrzi az útvonalak működőképességét.

Statikus útvonalak

Az automatikus rendszerek mellett minden routeren lehetőségünk van statikus útvonalakat létrehozni, ekkor meg kell adnunk, hogy a belső hálózat melyik számítógépéről hova továbbítódjanak az adatok. A forrás IP-címhez és portcímhez tehát cél IP-cím és portcím tartozik.

Ezzel a módszerrel a hálózat adott gépeinek forgalmát az általunk megadott útvonalra terelhetjük. A statikus útvonalaknak otthoni felhasználás esetén nincs sok jelentősége, ennek beállításával csak akadályozhatjuk a kapcsolatunkat, javításra ez nem használható.

DHCP-t mindenkinek!



A DHCP server listájában nyolc felhasználó rögzítése otthonra biztosan elég

Miután sikeresen beállítottuk a helyi hálózatunkat, rádobbenünk, hogy közvetlenül egészen kevés opció vonatkozik a LAN portokra. Néhány típusnál talán állíthatjuk a kapcsolat sebességét (10/100

Megabit, fél- vagy

fullduplex – ahonnan a 100 Mbit full az üdvözlő), és talán a portok egymáshoz képesti prioritását. A hálózati cím, a subnet maszk természetesen kötelező.

A legfontosabb itt a DHCP server, amely a helyi hálózaton (LAN és WLAN) adja meg gépeinknek az IP címüket, az aktuális átjárót (több routeres hálózatban nem feltétlenül ennek a routernek a címe), és a DNS szerverek címeit, amelyet az internetszolgáltatóhoz való kapcsolódáskor kérdezett le. Ilyenkor megadhatjuk, mely tartományban (pl. 192.168.0.100-192.168.0.150) adjon a csatlakozott gépeknek címet. Sok routeren csak a kezdőcímet, illetve az utána kiosztható címek számát kell megadnunk, mivel a kettő hatása teljességgel ugyanaz.

LAN

MAC Address: 00-14-78-EB-88-C6

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Save

Ennyi és nem több: IP-cím és subnet mask

DHCP Settings

DHCP Server: ☐ Disable ☒ Enable

Start IP Address: 192.168.1.100

End IP Address: 192.168.1.199

Address Lease Time: 120 minutes (1-2880 minutes, the default value is 120)

Default Gateway: (optional)

Default DNS: (optional)

Primary DNS: (optional)

Secondary DNS: (optional)

Save

A TP-Link routerével akár fix DNS szerverekkel is dolgozhatunk

kiosztható cím. Néhány router megengedi, hogy MAC-cím alapján rögzítsük az adott kártyának szánt IP-címet. Így a belső gépek minden esetben ugyanazt a címet kapják, mások csak kézi beállítás használatkor foglalhatják el azt (a címütközés nem szerencsés), és megmaradt a DHCP adta kényelem.

Praktikus ez a módszer akkor is, ha például egy notebookról van szó, amelyet a céges hálózatban hasonló módon, DHCP használatával helyezünk üzembe – így a notebookot sem kell állandóan más címre helyezni. Nagyon ritkán a DHCP Forwarder vagy DHCP Bypass opciót is elérjük, ami azt jelenti, hogy a router a DHCP adatokat átengedi (a NAT ekkor nem használható), a belső gépek pedig transzparens módon kapnak IP címeket.

Virtuális!

Intel(R) PRO/100 S adapter tulajdonságai

Általános Speciális Illesztőprogram Ellátások Energiagazdálkodás

A következő tulajdonságok tartoznak ehhez a hálózati kártyához. Kattintson bal oldalon a módosítandó tulajdonságra, majd jobb oldalon válassza ki az értéket.

Tulajdonság: Érték:

802.1p QoS csomagkezelés ☒

Biztonsági társítások ☒

Coalescence pufferek ☒

Fogadó pufferek ☒

Kapcsolati sebesség és késleltetés ☒

Küldő vezérlők ☒

Teljesítmény ☒

Válassz az érvényesítésre

OK Mégse

A hálózati kártyánál meglévő VLAN Tagging és VLAN ID itt Helyi felügyeletű címeke néven fut

laszthatjuk például a könyvelést. A routeren általában az adott LAN portokhoz rendelhetjük a VLAN csoportokat (biztos, ami biztos), de igazából ennek akkor van jelentősége, ha a VLAN csoportokhoz önálló routing- és biztonsági szabályokat rendelhetünk.

Következő számunkban részletesen foglalkozunk a vezeték nélküli hálózattal (WLAN). Ezt a műfajt azok is szeretik, akik orvul megcsapólják mások kapcsolatát, így valóban fontos megismerni a WLAN finomságait és buktatóit. ■

Nagyon fontos a Lease Time, amely megakadályozza, hogy a szabad címek elfogyjanak: a router ennyi idő után felülvizsgálja a címeket. A csatlakozott felhasználók pedig ismét megkapják az imént használt címüket, a már nem csatlakozók címei törölődnek a DHCP listából. Ezt az időt nyugodtan megnövelhetjük, csökkenteni csak sok felhasználó esetén érdemes, így mindig felszabadul



ROUTER JÁTÉK

Játsszon velünk és nyerje meg a két Netgear RangeMax NEXT WLAN router egyikét!



Netgear RangeMax NEXT Wireless-N 300 router

- WNR854T:
- akár 300 Mbit/s vezeték nélküli adatátviteli sebesség
 - ideális a multimédia adatfolyamokhoz
 - kitűnő teljesítményű előrehangolt belső antennák
 - integrált Gigabit switch
 - Intel "Connect with Centrino" minősítés, garantált kompatibilitás a WiFi N adapterekkel
 - Draft 802.11n és 802.11b/g kompatibilitás

1. Keresse fel honlapunkat!
www.cp.hu



2. Típelje meg a helyes válaszokat kérdéseinkre!
3. Nyerjen!

Jelentkezési határidő: július 29.
Sorsolás: július 30.

Együttműködő partnerünk: **NETGEAR**
Connect with Innovation™

Router iskola – 3. rész

Sokak számára nem okoz különösebb gondot a vezeték nélküli hálózat beállítása, ám még ők sem tudhatnak mindent. Cikkünk átfogó ismereteket kínál a vezeték nélküli hálózatokról.

Szerző: Köhler Zsolt

Vezeték nélkül



Vezeték nélküli hálózatunk kiépítéséhez a router (vagy WLAN AP, azaz hozzáférési pont) opcióinak egy részét kötelező jelleggel kell beállítanunk, máshol a finomhangolásra is lehetőségünk van. Vágjunk is bele mindjárt!

WLAN alapok

A vezeték nélküli hálózatot előbb engedélyeznünk kell, ezt az újabb routereken az *Enable Wireless (Router) Radio* opció beállításával tehetjük meg. Régebbi típusokon azért nem találjuk meg ezt az opciót, mert akkor még egyáltalán nem volt kritikus a WiFi hálózatok biztonsága. Ha csak ritkán csatlakozunk vezeték nélküli hálózatunkhoz, tartsuk kikapcsolva, és csak alkalmanként kapcsoljuk be. Egyes routereken (pl. Seneao) még hardveres kapcsolót is találunk erre a célra.

Hálózatunknak adjunk nevet a *Name/SSID* opcióval, a név szórását pedig az *(Accept) Broadcast SSID* v. *Enable SSID Broadcast* bekapcsolásával engedélyezhetjük. A név egyértelműen azonosíthat minket, de ha sűrűn lakott és nagy forgalmú területen nagyobb biztonságra törekszünk, érdemes letiltani a név sugárzását. Ha egy ismeretlen kliens rádiónk hatósugarába kerül, akkor az SSID ismerete nélkül nem fog tudni csatlakozni a hálózathoz.



Furfangos SSID azonosítót csak rejtve van értelme adni (Netgear RangeMax Next)

hoz. A nevet mindenképpen változtassuk meg, hiszen például a „default”, „dlink” vagy a „linksys” még az elrejtés ellenére is nagyon könnyen kitalálható.

Szól a rádió...

Mint ahogyan minden rádiót más frekvencián foghatunk, a WLAN is egy adott frekvenciasávot használ. A kis-közepes hatótávolságú sugárzás a 2,4–2,5 GHz tartományban (802.11b/g/n), illetve 802.11a esetén kis kihagyásokkal az 5,15–5,825 GHz tartományban történik. A rendelkezésre álló frekvenciasávot úgynevezett csatornákra osztják, a kommunikáció ezeken a csatornákon zajlik.

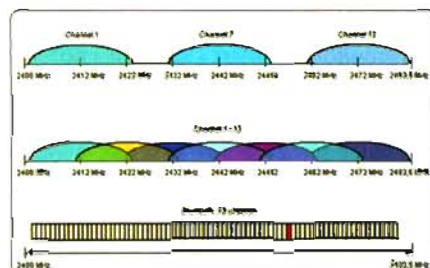
Az elterjedtebb B/G hálózatokban tizennégy egymást átfedő csatornát különböztetnek meg. Miért fedik át ezek egymást? Mert így a rendelkezésre álló frekvenciasáv a lehető legteljesebb mértékben kihasználható. Két egymás mellett lévő készüléknek lehetőleg egymást nem zavaró csatornát kell beállítanunk, de ha már elfogytak a szabad csatornák, akkor a távolságot is figyelembe kell vennünk a csatorna kijelölésénél. Végszükség esetén használhatunk egy távol lévő adóval azonos csatornát is, mert az kevésbé zavarja adásunkat. Az egymást nem zavaró 1-es, 7-es és 13-as csatornák közt tehát csak akkor kell újabbat (4-es, illetve 10-es) csatornát igénybe vennünk, ha a közelben kettőnél több WLAN router vagy hozzáférési pont (AP – Access Point) is működik. Utóbbi csatornákat már zavarani fogja a szomszédos csatorna forgalma, ekkor sebességsökkenést fogunk tapasztalni.

A csatornát „meglepő” módon a

A szabványokról

Nem mindenki számára világos, mit is jelent a 802.11g vagy 802.11n. A számozást az IEEE (Institute of Electrical and Electronics Engineers) non-profit szervezet osztja ki, amelynek körülbelül 175 országban több, mint 360 ezer tagja van.

Bennünket ez csak annyiban érint, hogy a fejlesztőket tömörítő társaság hoz döntést egy-egy új szabvány működésének módjáról, azért, hogy a megszülető eszközök egymással kompatibilisek legyenek. Az IEEE 802 csoport (amely „véletlenül” 1980 februárjában ülése-



Szűkös frekvenciatartomány: egymást nem átfedő csatornák (felül), az egymást átfedő páratlan számú csatornák (középen), a kommunikációt nem zavaró Bluetooth csatornák (alul)

Channel opcióval választhatjuk ki. Néhány készüléken az *Auto* opció is megtalálható, ezt beállítva a router figyelni a csatornákat egy ideig, majd a forgalomtól függően egy üres (nek vélt) csatornára áll be. WLAN kliensünkkel végezzünk egy felderítést (*Site Survey*), így láthatjuk, a közelben ki, milyen csatornát használ. Egyes modernebb routerek is érzékelni tudják a többi eszközt, ez segíthet, de a legjobb mégis a klienssel körbekémlelni, hiszen lehet, hogy a használat helyén zavarja a kommunikációt más, a routernél ez viszont nem érzékelhető.

Nagyon gyakran a használat helyét is

A router iskola részei

1. Alapok
2. WAN és LAN
3. Vezeték nélkül
4. Tűzfal, szűrők, VPN
5. VoIP és streaming
6. Haladó beállítások
7. Hardvertuning, firmware-frissítés
8. Hardveres-szoftveres különlegességek

zett először) az OSI modell (lásd az első rész anyagát) alsó két rétegével foglalkozik. A 802.11 a Wireless LAN munkacsoportot jelöli, ezen belül a különféle szabványok betűmegjelölést kaptak. A 802.11 önmagában egy 2,4 GHz-en 1 Mbps, illetve 2 Mbps sebességű WLAN szabványt jelölt, ám megjelent a 802.11b (2,4 GHz, 11 Mbit/s), majd a 802.11a (5 GHz, 54 Mbit/s).

A jelenlegi legnagyobb működő WLAN-sebességet kínáló szabvány a 802.11n, véglegesítése 2008 szeptemberére várható.

Mivel immár nem csak a számítástechnikai, de a szórakoztatóelektronikai cégek is képviselve vannak a szervezetben, a köztük való megegyezés sem mindig könnyű. Ezért kaphatunk a boltban „draft N”, illetve „pre-N” jelzésű routereket, amelyek 2,4 GHz és/vagy 5 GHz frekvenciákon MIMO (Multiple In-Multiple Out) technológiával akár 250-300 Mbit/s sebességet is el tudnak érni. A tipikus sebesség ennél kisebb, de mégis gyorsabb, mint az A/G 54 Mbit/s maximális sebessége.



Netgear KWGR614 WLAN router: nem csak MIMO-s, de a divatnak megfelelően nyílt forráskódú

meg kell adnunk a *Region* opcióval. Itt bármit beállíthatunk azzal a feltétellel, hogy a 14-es csatornát nem használjuk. Ez az opció kizárólag arra szolgál, hogy megelőzze a törvénysértést: bizonyos országokban még a 13-as csatorna sem használható (pl. Franciaországban, Spanyolországban), máshol pedig a 14-es is (Japánban). A csatorna kiválasztása a rádió adóteljesítményétől is függ: ha nagyobb antennát vásárolunk a routerre, akkor csak az 1-8 csatornákat használhatjuk. Hogy miért, arról majd a 7. részben.

Egyszerű védelem

A biztonságot az újabb technológiák is segítik: minél gyorsabb (egyedibb) kom-

munikációra állítjuk be a routert, annál kisebb az esélye annak, hogy valaki egy régebbi (általános) klienssel tud csatlakozni hozzá. A *Wireless Mode* alapjában véve nem erre szolgál, hanem arra, hogy a régebbi kliensek is tudjanak csatlakozni. A *802.11b Only* vagy *802.11g Only* opció csak az adott sebességű klienseket fogadja el, a *Mixed* bármelyiket.

A gyorsabb készülékek a saját sebességük mellett a lassabbakat is kezelhetik, de ez szintén csak a klientsől függ: a 108 Mb/s sebességű routerhez ilyen sebességgel csak azonos chipsetű (azaz márkájú) kliens tud csatlakozni. Ha az üzemmód *Static*, akkor a router nem enged a sebességből, ha *Dinamic*, akkor egy lassabb (pl.



Ha a sebesség 300 megabithez közelít, egyes értékek nem állíthatók – csak rontánánk vele (Netgear RangeMax Next)

54 megabites) kliens is tud csatlakozni. Előbbi nagyobb biztonságot, utóbbi egyszerűbb üzembe helyezést eredményez.

Ugyanez a helyzet a hibrid eszközökkel, amelyek a 802.11b-n kívül a 802.11a-t



ROUTER JÁTÉK

Játsszon velünk és nyerje meg a két Netgear WLAN router vagy a két switch egyikét!

Együttműködő partnerünk:

NETGEAR
Connect with Innovation™

2x



NETGEAR – PoE portokkal ellátott Switch-en keresztül működő professzionális AccessPoint

FS108P

PROSAFE 8portos 10/100 SWITCH
4 PoE csatlakozóval
4 portos – Power over Ethernet (PoE) látja el árammal az Access Pointokat, kamerákat, stb.

WG102

PROSAFE™ 802.11G WIRELESS ACCESS POINT
Vállalati szintű funkcionálitás akár 108 Mbps sebesség
WPA – 802.11i-képes biztonság támogatása
IEEE 802.11n szabvány
Point-to-point/multipoint vezeték nélküli hálózati mód
Ismerős mód
Rugalmas Transzmit Power Control (TPC)
100 mW-tól akár 0 mW-ig

Élettartam garancia a NETGEAR minden Prosafe termékére (switch-ekre, vezeték nélküli eszközökre, tűzfalakra és egyéb Prosafe eszközökre)

2x



NETGEAR
LIFETIME
WARRANTY

1. Keresse fel honlapunkat!
www.cp.hu

CP Computer PANORAMA ONLINE

2. Típelje meg a helyes válaszokat kérdéseinkre!
3. Nyerjen!

Jelentkezési határidő: augusztus 27.

Sorsolás: augusztus 28.

Elkerülni az ütközést

Az egy médiát egyszerre használó több kliens kommunikációs módok közül a legnagyobb hálózati kihasználtságot eredményező CSMA (Carrier Sense Multiple Access) séma a legelterjedtebb. Ebben a kliensek egymás között úgy osztoznak a sávszélességen, hogy valamilyen módon eldöntik, kié a szó.

A vezetékes hálózatokon – ilyen az Ethernet is – a CSMA/CD a legelterjedtebb változat, itt a CD Collision Detection, azaz az ütközések érzékelését jelenti. Egy valaki forgalmazni kezd, és ha abba más is beleszól, elrontva a kommunikációt, mind a kettő felfüggeszti az adását, és elindít egy véletlenszerű ideig számoló órát. Majd újra próbál-

kozik. Annak az esélye, hogy a másik is éppen a kommunikáció kezdetén (amikor is mindenki számára szabad a pálya) kezdene forgalmazni, minimális. A mindig változó várakozási idő miatt a kliensek prioritása is szabályozható, hiszen átlagosan mindegyik adott ideig várakozik.

Vezeték nélküli hálózatokban gyakori a CSMA/CA (Collision Avoidance – ütközés elkerülés), amelynél, ha már valaki elkezdett adatot forgalmazni, nem zavarják meg. A véletlenszerű ideig történő késleltetés itt is létezik, ám ha az óra lejár, a kliens ellenőrzi a szabad médiát, és forgalmazni kezd. A prioritás itt is változtatható, és azt is beláthatjuk, hogy ütközés (de főleg rádiós zavar) itt is előfordul.

részünk, az utóbbival pedig limitálhatjuk a router sebességét. Az alapértelmezés az előbbinél ezért a legkisebb, utóbbinál a legnagyobb sebesség.

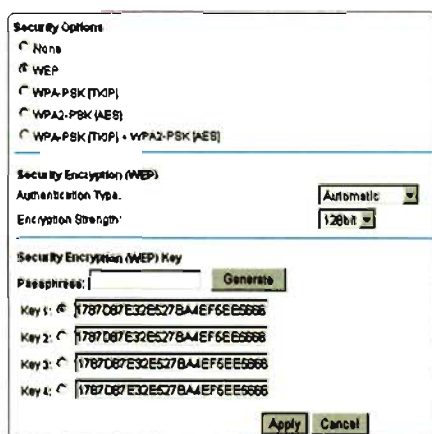
De a sebesség nem minden, kapcsolódni is kell valahogyan: minden esetben szükség van egy szinkronizáló jelre, amelynek hosszát a Preamble Mode opcióval állíthatjuk be. A 11 megabites klienseknek a Long (hosszú) módra van szükségük, a 22 megabit/s sebességnél gyorsabbra képesek jellemzően a Short (rövid) módot kívánják. Akkor, ha van még esély régi kliensek csatlakozására, illetve nagyobb távolságban bizonytalan a csatlakozás, a Long módot válasszuk ki.

A szinkronizáláson kívül a hálózati kommunikáció beállítását, ütemezését végzi az ún. Beacon packet, (szabad fordításban bolya-csomag), amelyet a router

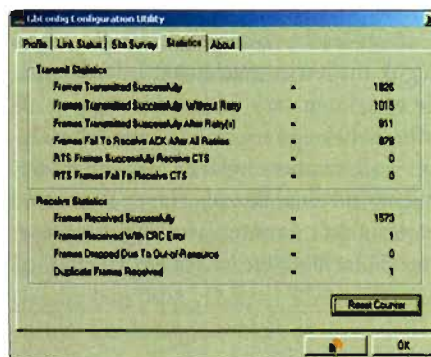
is ismerik. Fontos az új, 802.11n-es eszközök 20 MHz és 20/40 MHz opciója: a 802.11a/b/g eszközökkel kompatibilis rendszerben engedélyezhetjük a 40 MHz-es csatornáméret használatát (a korábbiak dupláját), ezáltal nagyobb sebességet érhetünk el. Az „N”-es router ezen módja a felülről való kompatibilitás miatt már nem biztonsági, csupán sebességbeli különbséget jelent.

Rádiós időzítések

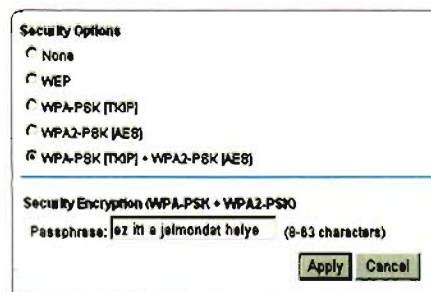
A rádiós kommunikáció nem csak abból áll, hogy a készülékek „vaktában” adatokat küldenek; az adott méretű csomagok mellett azok időzítése is kritikus – akik emlékeznek még a BIOS iskola memóriával foglalkozó részére, találhatnak itt egy kis párhuzamot. Az alábbi értékeket sok esetben nem kell módosítanunk, alapértelmezett módban a legtöbb készülék működik.



A WEP kulcsok készítésekor a lehető legerősebb kulcsot használjuk (képpünkön ez 128 bit)

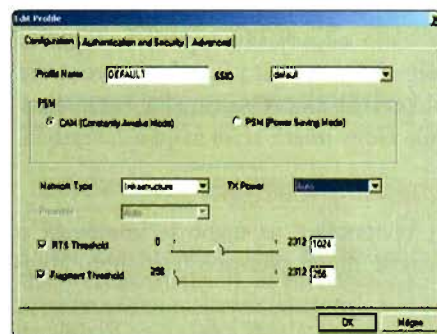


Ha magas a Fail sorban a csomagok száma, csökkenteni kell a Fragment Threshold értéket (Gigabyte Mini-PCI 54g kliens)



Egyszerűbb és biztonságosabb, de kicsit lassabb a hálózat a WPA használatakor

Az adatok átviteli sebességét a Basic Rate, valamint a Transmit Rate értékekkel állíthatjuk be, 1, 2, 5, 11 (és így tovább) Mbit sebességre. Az alapvető kapcsolódás a Basic Rate sebességen megy végbe, majd ideális vételi viszonyok között átlép a Transmit Rate által meghatározott sebességre, próbálva elérni a lehető legnagyobb. Érthető, hogy az előbbi minél magasabbra állítva gyorsabb, de kevésbé megbízható kapcsolódásban lehet



Kliens kártyáknál a PSM (Power Saving Mode) bekapcsolásával takaríthatunk meg energiát – hátránya, hogy megszakadhat a kapcsolat

rendszeres időközönként küld a kliensek felé. A kliensek ezt figyelve eldönthetik, hogy melyik hozzáférési ponthoz csatlakozzanak, természetesen csak akkor, ha több nyílt hálózat is elérhető.

A Beacon Period/Interval (1-65535) ezeknek a csomagoknak a küldési gyakoriságát adják meg. Ha a lehető legkisebbre (1-re) vesszük, akkor olyan környezetben, ahol több nyílt hozzáférési pont található, a kliensek a lehető leggyorsabban tudnak roamingolni – azaz mozgásuk közben gyorsan hozzáférési pontot váltani. Ha viszont csak egyetlen routerünk van, a kliensek csak és kizárólag ehhez csatlakoznak, esetleg akár úgy, hogy soha nem mozgathatjuk őket. Ilyenkor ezt az értéket nyugodtan növelhetjük.

Mivel ezt a csomagot a kliensek energiatakarékos üzemmódjukhoz is felhasználják, egy Beacon csomag beérkezése után a forgalmazni nem kívánó kliensek energiatakarékos állapotba kerülnek. Fontos, hogy ez az alvó mód csupán

néhány milliszekundumig tart, de ez is elég ahhoz, hogy egy notebook WLAN-kártyája által fogyasztott energia harmadát-felét megtakarítsuk.

A klienseket a *DTIM Period/Interval* (1-255) által meghatározott sűrűségben küldött csomagok tájékoztatják arról, hogy számukra adat érkezett. Nagyobb érték esetén a DTIM csomagok ritkábban kerülnek elküldésre, ezáltal több idő jut a tényleges adatcsomagok küldésére. Ha tehát az alvó klienst a DTIM magas értékével tovább hagyjuk aludni, akkor az egyes programok által küldött Unicast/multicast (mindenkinek szóló) csomagoknak várakozniuk kell, ami szélsőséges esetben hibát is okozhat a kommunikációban.

Adósok vagyunk a fenti számok értékével. Noha szinte egyetlen gyártó sem írja oda, mi mit jelent, legfeljebb csak a TU, azaz Timing Unit jelzés olvasható, a számok valójában kilo-milliszekundumot jelölnek, egy egység tehát 1024 mikroszekundum, körülbelül egy ezredmásodperc. Ha a Beacon Interval értékének a maximumot adjuk, akkor körülbelül 67 másodperc is eltelik, amíg a kliens megkezdheti a csatlakozást – itt is legyünk körültekintőek!

Emelkedett kommunikáció

Az *RTS (Request To Send)* csomag arra szolgál, hogy egy IP adatcsomag átvitele előtt megadja annak méretét. Az RTS csomag – ahogyan az előbb ismertetettük – a hálózat vezérlésében játszik szerepet. Az *RTS Threshold* értékét növelve az RTS csomagok ritkábban kerülnek elküldésre, tehát több idő jut a tényleges adatok továbbítására. Akkor viszont, ha a hálózati kommunikációban ütközés keletkezik, a teljes kommunikáció csak a következő RTS csomag elküldésekor áll helyre. Nagy kiterjedésű, zsúfolt hálózatokban ezért az RTS Threshold értékét csökkentve ugyan csökken kicsit a teljes átviteli sebesség, de kevesebb fennakadással szembesülünk – összességében nyerünk vele.

Sok esetben a *CTS (Clear to Send)* küldésének időzítését is megadhatjuk. A router fogadja az RTS csomagot („küldhetek?”) a klientsől, majd válaszol neki a CTS („jöhetsz!”) csomaggal. Az *RTS Retry* mennyisége megadja, hány alkalommal megkíséreljük a WLAN eszköz RTS-t akkor, ha nem kapott rá CTS választ. Ezután következik az egyeztetett adatmennyiséget magába foglaló adatátvitel. A *CTS Threshold* működését ezért nem kell részleteznünk, hiszen – ha van a router menüjében – ugyanúgy működik, mint az RTS Threshold.

Érdekesebb a *Fragment(ation) Threshold*, amely megadja, hány bájt lehet egy rádiós csomag. Adáskor ugyebár bármikor megzavarhatják az adatátvitelt, amely egy bizonyos szintig javítani, még magasabb szinten pedig érzékelni tudja a hibákat. Ha a hiba nem javítható, az adott csomagot újra kell küldeni. Minél nagyobb az átvinni kívánt csomagunk, annál nagyobb az esélye a hibának, és annál több adatot kell feleslegesen újraküldelnünk – hiszen kisebb csomagot hamarabb át tudunk küldeni.

Mint minden csomagokkal kapcsolatos variációnak, itt is az overhead hasznos adatokhoz mért aránya a problematikus: több csomag, nagyobb overhead. Ökölszabály, hogy ha a hibák/ütközések aránya a teljes forgalom 5%-át nem haladja meg, a *Fragmentation Threshold* értékkel nem kell foglalkoznunk. Nagy forgalmú hálózatokban érdemes 1000-ról indulni, majd a sebesség/ütközések arányában felfelé, illetve lefelé módosítanunk.



TP-LINK®

Behálózuk a világot.






Super G & Kiterjesztett Hatótáv™ 54/108Mbps vezeték nélküli Router

- 108M vezeték nélküli LAN Router, 2.4GHz
- 802.11g/b, beépített 4-portos Switch-csel
- 108M Super G™ technológia
- 2x-3x Kiterjesztett Hatótáv™ technológia
- forgatható SMA Antenna



Super G & Kiterjesztett Hatótáv™ 54/108Mbps vezeték nélküli USB Adapter

- IEEE 802.11g WLAN USB Adapter
- Super G™, akár 54/108Mbps átvitel teljes 802.11b kompatibilitás
- Kiterjesztett Hatótáv™, akár 9x nagyobb, mint a normál vezeték nélküli adaptereknél



Super G & Kiterjesztett Hatótáv™ 54/108Mbps vezeték nélküli PCMCIA Adapter

- IEEE 802.11g WLAN PCMCIA Adapter
- Super G™, akár 54/108Mbps átvitel teljes 802.11b kompatibilitás
- Kiterjesztett Hatótáv™, akár 9x nagyobb, mint a normál vezeték nélküli adaptereknél



6dBi 2.4GHz beltéri asztali Yagi Antenna

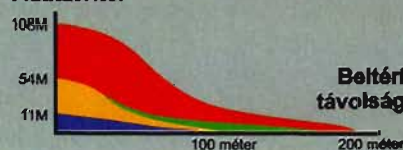
- Frekvencia távolság: 2.4GHz - 2.5GHz
- Sugárzási irány: kétirányú
- Jél erősség (csúcsérték): 6dBi
- Kábel hossz: 100cm
- Csatlakozó: SMA közvetlen dugó/fordított



Kábel/DSL Router beépített 4/8 portos Switch DDNS felügyelet, 802.1X

- 4/8 db 10/100Mbps LAN port
- 1 db 100Mbps Auto-Negotiation WAN RJ45 port
- Beépített tűzfal IP cím szűréssel
- Domain Name és MAC cím szűrés
- Felhasználói adminisztráció, webcím szűrés

Adatátvitel



- Hagyományos 802.11b eszköz
 - Hagyományos 802.11g eszköz
 - TP-LINK vezeték nélküli eszköz 2x-3x kiterjesztett hatótávval
 - TP-LINK vezeték nélküli eszköz 2x-3x kiterjesztett hatótávval és 6dBi Yagi Antenna
- A beltéri távolság függ a működési környezettől is.

Kiemelt importőr:

Mercury Magyarország Kft.

1131 Bp., Dolmány u. 14. tel.: 221-3020 fax: 221-4254
www.mercurycomputer.hu mercury.hungary@ahol.com

Tűzfalak, szűrők,

▶▶ Mi mással is kezdenénk a hálózatok biztonságáról szóló összeállításunkat, mint a vezetékek nélküli biztonsági opciókkal? Az alapbeállítások után át is térünk a legtöbb routerben megtalálható, többé-kevésbé hatékony tűzfalra, és az ehhez kapcsolódó beállításokra.

WLAN biztonság

Általában a WLAN Security vagy egyszerűen WLAN options menüpont alatt találjuk a WLAN biztonságát szabályozó opciókat. Azt, hogy a router használjon-e valamilyen titkosítást, az Open System/Shared Key menüben állíthatjuk be: előbbinél semmilyen védelmünk nincs, utóbbinál az, amelyet beállítunk.



Az egyszerű tűzfalak be- és kikapcsolhatók, többnyire csak a Proxy forrást, sütiket, Javát és ActiveX-et tudják külön letiltani

Mivel már a legelső szabványnál gondot jelentett, hogy a rádió könnyen lehallgatható, megjelent a WEP (Wireless Equivalent Privacy) titkosítás, amely egyáltalán nem olyan biztonságos, mint az Ethernet. Alapvető védelmet azért ad, hiszen csak speciális programmal törhető fel. Ha beállítjuk, sebességsökkenéssel nem kell számolnunk, ezért ha lehet, válasszunk minél nagyobb bitszámú titkosító kulcsot. 128-at minden eszköz támogat, néha még a 152 vagy a 256 is elérhető. Mint minden biztonsági beállításra, erre is vonatkozik, hogy a klienseket is azonos módon kell beállítani. Az itt található Key Format lehet ASCII, de Hexa típusú is, előbbinél egyszerűbb a dolgunk, hiszen a kulcs nem csak 0-9,

Router iskola – 4. rész

Sorozatunk mostani részében a hálózatunk biztonságáról lesz szó. A szerteágazó témából az otthon leginkább használt opciókat emeljük ki, és kitérünk a sokak számára jó szolgálatot tevő Port Forward opcióra is.

Szerző: Köhler Zsolt

illetve A-F kombinációkból állhat. Sok router magától tud kulcsokat generálni egy általunk beírt mondatból (így a konfigurálás egyszerűbb – egy verssort például könnyen megjegyezzünk). Négy kulcs pedig azért van, hogy azokat heti-havi rendszerességgel cserélni tudjuk, mindig az aktuálisat kijelölve. Újabb készülékeken van (Auto) Key Rotation opció is, ez önmagától „forgatja” a kulcsokat, tehát nem kell vele annyit törődnünk.

Sokkal fejlettebb a WPA, illetve a még biztonságosabb WPA2, amelyek a kliens csatlakozásakor véletlenszerűen generált ideiglenes kulccsal kódolt kulcsot (bonyolult, de így jó) küld át, majd azt az egész kommunikáció alatt használja. A kulcs ekkor kódolva ugyan, de átküldésre kerül, ezért használhatjuk a WPA-PSK, illetve WPA2-PSK (Pre-shared Key) opciókat, amelyeket szintén be kell állítanunk, de az alap kódoló kulcs a biztonság egyeztetésénél nem kerül átküldésre. Azt, hogy a titkosítás során milyen algoritmust használjon a rendszert, almenüből választhatjuk ki. Az AES egészen biztonságos, közepesen lassú kommunikációt ad, a TKIP magas biztonságú, lassúbb rendszer. A WPA speciális beállításaira várhatóan sorozatunk hatodik részében térünk vissza.



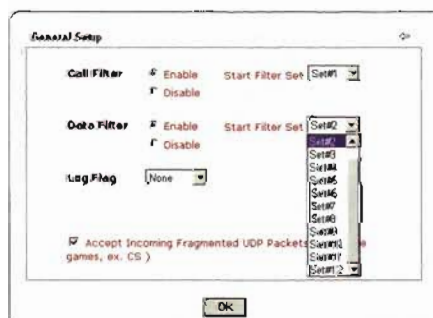
A sok opciót az esetek többségében úgyis mindig bejelöljük, a flood típusú támadások finomhangolása a szerverek hatékony védelmét segíti

ságos, közepesen lassú kommunikációt ad, a TKIP magas biztonságú, lassúbb rendszer. A WPA speciális beállításaira várhatóan sorozatunk hatodik részében térünk vissza.

Amit a tűzfalról tudni kell

A tűzfalak a legtöbb otthoni routerben egyszerűek, az általunk definiált szűrőket kivéve azt blokkolják vagy engedik, amit megadtunk nekik. Sok készüléken feltüntetik az SPI (Stateful Packet Inspection) jelzőket, ami annyit tesz, hogy a router a bejövő adatok forrását minden esetben összehasonlítja a kimenő adatok céljával.

Ez a vizsgálat minden egyes csomag esetében megtörténik, tehát ez a tűzfal az OSI modell 3-dik szintjén (hálózati réteg) működik. A Layer-3 tűzfalak a csomagok vizsgálatát gyorsan elvégzik, hiszen csak a kapcsolatok teljes életét jegyző naplóval és az általunk megadott szabályokkal kell dolgoznia. Röviden úgy is jellemezhetjük ezeket a tűzfalakat, hogy csak azt a forgalmat engedik be, amelyet mi belülről



Komolyabb tűzfalak a csomagok fejlécében és az adatokat elemezve is szűrni tudnak, és különböző konfigurációkat is előre létrehozhatunk

VPN



A legfőbb kérdés, hogy az általunk megadott lista tiltó vagy engedő jellegű-e: az engedő (Allow) listában nem szereplők tiltva lesznek

kértünk vagy elvártunk. A kapcsolatok létrehozása a TCP protokollnak megfelelő SYN, „kérő” csomagok, visszafelé pedig az ACK „nyugtató” csomagok küldésével történik, ebből a tűzfal tudja, hogy új kapcsolatról van szó. Ez a rendszer ésszerű, a működéséhez nem is kell különlegesen gyors vagy bonyolult hardver, alapszinten véd. Ha a konfigurációs menüben bekapcsoljuk az Enable SPI Firewall opciót, a védelem működik. Ezt az opciót egészen meglepő módon a Firewall vagy az Advanced főmenü alatt találjuk.

Az SPI-nél alaposabb Deep Inspection módszer lassabb, de a csomagokat össze-illesztve azok tartalmát is elemzi, így a kártékony kódok kiszűrésére is van lehetőség. Ilyet csak a dedikált hardveres routerek tudnak, de – mint néhány példával illusztráljuk is – akár egyes WLAN routerek is többet tudnak az egyszerű SPI-nél. Ha routerünk történetesen Draytek Vigor, akkor ennél többet is kaphatunk, már-már elérve a hardveres típusok színvonalát.

Nem DOS, DoS!

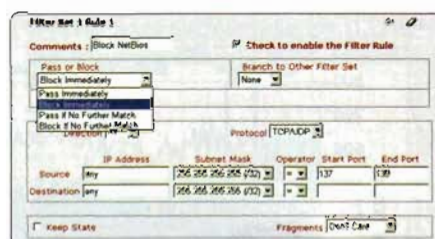
A SYN-ACK pároknak van egy hátrányuk is, az SPI tűzfalak ugyanis sérülékenyek a DoS (Denial of Service – szolgáltatás akadályozás) támadásokra. Ezek egészen egyszerűen úgy tesznek, mintha egy új kapcsolatot próbálnának létesíteni, sok-sok SYN csomag küldésével. A router kapcsolatokat követő táblázata a sok SYN kérés miatt betelül, a router pedig képtelen új kapcsolatot létrehozni. Az otthoni

felhasználók ebből csak azt tapasztalják, hogy lelassul a hálózatuk, ám ha a router mögött egy sokak által látogatott szerver van, akkor ahhoz más felhasználók nem tudnak kapcsolódni. Ez a támadás viszonylag egyszerűen védhető: ha a menüben a DoS Prevention/Protection opciót látjuk, kapcsoljuk be!

Támadások, védelmek

A különböző rendszerbeli sebezhetőségek (vulnerability-k) kihasználására sok módszer (exploit) jelent meg, illetve alkalmazható a tűzfalak ellen. Ha a routerben találunk külön SYN/UDP/ICMP flood defense opciót, az éppen a flood (elárasztás) típusú támadások ellen véd. Ha állíthatjuk az érzékenység (threshold) értékét, akkor az megadja, hogy egymás után, adott időkorlát (Timeout) alatt hány csomag érkezik, amit még nem minősít támadásnak a tűzfal. „Paranoiások” az érzékenységet lejjebb véve esetleg az olyan kívülről csatlakozni próbáló felhasználókat is akadályozhatják, akiknek lassú vagy bizonytalan a kapcsolata. A kliensük sokszor küld SYN csomagot, ezért egy időre tiltólistára kerül.

Nem kimondottan támadás, csak egy azt megelőző tevékenység lehet a Port



Az okosabb tűzfalak beállításától függően akár egy kihágást engednek (Pass If No Further Match)

Scan, amelynek kívülről egy program a router összes portját leteszteli, hogy nyitva van-e. Ezzel a művelettel alapvető módon tesztelhetjük, hogy routerünk vagy számítógépünk (akár a belső hálózat összes számítógépe) milyen portokon vár csatlakozókat. A nyitott portok veszélyesek lehetnek, a gyermek hackerek előszeretettel futtatnak PortScan a hálózatokon, hátha találunk egy számítógépet, amelynek a portját egy trójai megnyitotta. Ha a routeren a Disable Port Scan vagy Enable Port Scan Detection opciót találjuk, nyugodtan kapcsoljuk be. Csak akkor tiltsuk le, amikor mi végzünk tesztet.

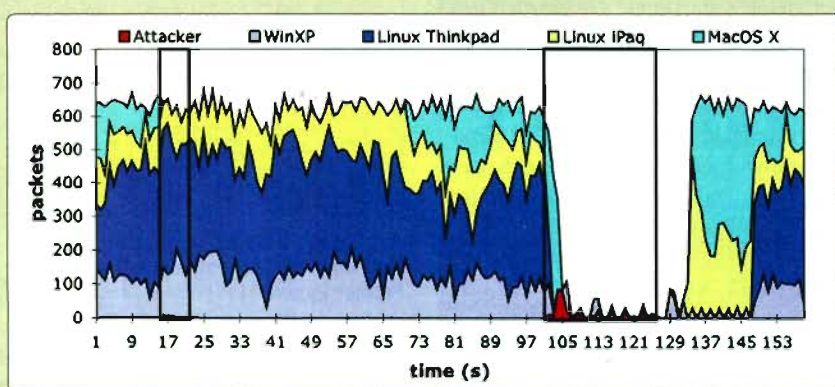
A különféle Block opciókkal egyes támadások védhetők ki, ezek ellen a legtöbb router sajnos nem véd. Ha esetleg

VIGOR2910 SERIES
DUAL-WAN SECURITY ROUTER

- Dual WAN funkció terheléelosztással
- 32 VPN csatorna
- Policy based tűzfal
- Content Security Management
- Sáv szélesség management
- QoS a jó minőségű VoIP-ért
- 6 SIP regisztráció
- SDN loop through
- SDN On/Off-Net

DrayTek

GAMAXNET
1114 Budapest, Baross Béla út 137c
Tel: 372-7480 Fax: 372-7481
info@gamaxnet.hu www.gamaxnet.hu



A keretezett részekben a támadó jutott szóhoz: előbb csak szimatolt (bal oldalon), majd támadott (jobbra). A támadás eredményeképpen sokan elvesztették kapcsolatukat

Érdekes támadások

Akárcsak a SYN flood, a tűzfal pufferében túlsordulást okozó támadásokból van még egy pár. A legegyszerűbb a Ping of Death, amely villámgyorsan „pingeli” a célt. Mivel ezek az ICMP (Internet Control Message Protocol) csomagok más csomagok felett elsőbbséget élveznek, a router is ezekre reagál először. Ha sokat kell válaszolni a Pingre, nem jut idő a valós forgalomra.

Igen alattomosak a Smurf/Fraggle támadások, amelyek ICMP/UDP csomagokkal végeznek pingelést. De nem akárhogyan, és „kamu” forráscímmel egy teljesen normális szervert (gépet) bombáznak, amely a valós forráscímre küldi vissza a nyugtázó csomagok ezreit.

A bénító támadás másképp is elérhető: ICMP vagy SYN, nem szabványos töredék-csomagokat is lehet kül-

deni a megtámadott gépre, így az nem tud mit kezdeni a hiányos információval. Ehhez hasonló, de teljes csomagot kap a router Land támadáskor, ám a csomagok felépítése nem szabványos. Így a router nem tudja értelmezni a csomagot: ha hibás (egyszerű), akkor megbénul.

A routerek a nem szabványos kommunikációval sem tudnak mit kezdeni, a Teardrop támadásnál több, egymást átfedő, azonos paraméterű IP csomag érkezik, ám ezek összeillesztése a védelem nélküli gépnek nem mindig sikerül. Az eredmény ismert.

Végül, de nem utolsósorban a TCP flag scan a hagyományos PortScanhez hasonlóan felderíti a nyitott portokat, de úgy, hogy az ellenőrzés helyett valós csomagokat küld – erre a tűzfal nélküli gép biztosan válaszol.

része a DoS Protection csomagjának, arról sehol nem szerezhettünk tudomást.

Érdekes opció az Allow Fragmented (UDP) Packets. Bizonyos támadások csak csomagtöredékeket küldenek, tehát szándékosan hibás tranzakciót generálnak. Az ilyen töredékek a router puffereit töltik csordultig, az ugyanis egészen addig nem továbbítja a csomagot, amíg annak minden adata meg nem érkezett. Akkor viszont, ha UDP kommunikációval tartjuk a kapcsolatot az internet egy másik gépével (ez jellemző a hálózatos játékok többségére), a hálózati kapcsolat viszont instabil, akkor a tűzfal meg fogja szakítani a kapcsolatot. Az opciót engedélyezve lassan, de legalább biztosan működni fog a kapcsolat.

Szabályok definiálása

A tűzfalakhoz szinte minden esetben saját szabályokat hozhatunk létre, amelyeket



Könc a kutyák elé: a DMZ-be tett PC bármilyen sérülékenysége kihasználható

vagy enged (Allow), vagy tilt (Deny) a tűzfal. Az egyszerűbb típusoknál csak egy listát hozhatunk létre adott IP-címekkel és portokkal, és globálisan határozhatjuk meg, hogy ezek mind a „csak ezek engedélyezettek” vagy „csak ezek tiltottak” kategóriába tartozzanak.

Fejlettebb routereken egyenesen forrás és cél IP, port és protokoll (pl. TCP, UDP) alapján adhatjuk meg a szabályt. Szabályt konkrét célcím nélkül is létre-

hozhatunk, de ekkor a forgalom irányát (IN/OUT) is meg kell adnunk. A bejövő forgalomra figyeljünk különösen, hiszen ez a veszélyesebb, de egy nyitva hagyott kimenő port egy, az adott gépen működő trójaival karöltve vidáman rést üt a legjobb tűzfalon is.

Életünket nagyban megkönnyíti, ha az otthoni routereket tiltó üzemmódban, a cégeseket pedig engedélyező módban használjuk, de biztonságot az ad igazán, ha az általunk megadott címeket egyedi elbírálás alapján engedélyezzük. Ez a rendszergazda feladata.

A folyamatosan változó kliensek adminisztrálása egyenként bonyolult lehet, de ha a Range opcióval találkozunk, akkor IP-, illetve portcím tartományt is megadhatunk, biztosítva például a felhasználók hálózathasználatát. Konkrét példát csak azért nem adunk, mert ezek az adatok függenek az adott PC-től, programtól és helyzettől.

Fegyvermentes övezet

Tegyük fel, hogy a belső hálózat egyik gépén olyan programot kell futtatnunk, amelynek nem ismerjük az internetre nyíló portjait. Otthoni példával élve, pár órára kipróbálnánk egy játékot, amely az internetre csatlakozik. Ahelyett, hogy fáradságos munkával monitorozni kezdenénk gépünk portjait, a játék leírását nem találva gyorsan kell megoldanunk a csatlakozást. A tűzfal letiltása nem szerencsés, hiszen a többi gépnek (is) kell a védelem. Használjuk ekkor a DMZ (Demilitarized Zone) opciót, amely a tűzfalon kívülre helyezi az általunk megadott IP-című gépet. Ekkor már nem kell törődnünk azzal, mely portokat kell megnyitni, a szűrés hiánya miatt az összes elérhetővé válik. Ebben rejlik a módszer hátránya is: könnyen állítható szoftveres tűzfal hiányában az adott gép internetes támadások célpontja lehet.

Időzítés

Extra felszereltségű routereknél a szabályokat időzíthetjük, megadva azok

A router iskola részei

1. Alapok
2. WAN és LAN
3. Vezeték nélküli
4. Tűzfalak, szűrők, VPN
5. VoIP és streaming
6. Hálódó beállítások
7. Hardvertuning, firmware-frissítés
8. Hardveres-szoftveres különlegességek

működési idejét. A Schedule/Scheduler menü alatt a től-ig időt vagy a hét napjait (hétfőtől vasárnapig) bejelölve adott időtartamra korlátozhatjuk a szűrő(k) működését. A portokat tiltó szabályoknál vigyázzunk az időzítéssel, különösen a bejövő (IN) típusúaknál!

Ha van kulcsszó alapján szűrő üzemmód, azt a gyermekek védelmére beállíthatjuk. A szűrők teljes jogot kaphatnak az adott IP címeken (alul)

Tartalomszűrés

Az időzítés még fontosabb a tartalomszűrés esetén, ezt a legtöbb router Access Control, Content Filter, Child Protection menüjében találjuk. A menü az opciók konkrét nevét is megadhatja. Az URL (Access) Control/Filter a beírt szavakat figyel a csomagokban, és ha egyezést talál, a kommunikációt megszakítja, az adott címről nem tölt le adatot. Így egyszerűen szűrhetünk ki bizonyos szavakat tartalmazó weboldalakat (pl. www.sex.com). A módszer hátránya, hogy rengeteg olyan

weboldalt átenged, amelyben nincs meg az általunk megadott kulcsszó. Ennél jobb az URL/Web Content Filter, amely a weboldalon lévő szó alapján szűr.

Kevésbé a konkrét tartalmat, sokkal inkább az alkalmazott kódolást tiltja a Restrict Web Feature. Itt külön-külön bejelölhetjük, hogy a router ne engedje át a Java és ActiveX tartalmakat, a sütiket (Cookie) vagy a Proxy szerveren keresztüli kommunikációt. Ez utóbbi igen fontos, a legtöbb esetben a hacker proxy szerverként működő gépet használ tevékenysége álcázására. Akkor, ha nem jön be néhány weboldal, vagy fontos nekünk az adott opció (pl. a netbankoláshoz Java szükséges), akkor kivételesen ne tiltsuk őket.

Még jobb a szűrő, ha tömörített (compressed files), végrehajtható (executable) filmeket és zenéket (multimedia files) is fel tud ismerni, le tud tiltani. A hardveres tűzfalak egy feltöltött vírus- és site-adatbázis alapján még alaposabb szűrésre is képesek. Kivételesen persze itt is tehetünk: az adott IP címtartományban szereplő/nem szereplő

Ez ám a szigor: se Battlefield, se Doom3, se iTunes, se MSN Messenger. Csak ha jönnek a jó jegyek!

A listát a hálózati kártya MAC címe, a PC IP címe vagy címtartománya alapján készíthetjük el. Hogy ezeket mind tiltjuk vagy engedjük, máshol kell eldöntenünk

gépeknél letilthatjuk a szűrőfunkciókat. A magukra vigyázni tudó felhasználók ide sorolhatják magukat.

Adott gépek blokkolása

A belső hálózatot is biztosítani kell, ki tudja, mikor fog valaki WLAN-on keresztül bekapcsolódni a hálózatunkba, vagy az irodába beosonva felcsatlakozni az általában igen sérülékeny LAN-ra. Az Access Control menüben találhatjuk az IP/MAC filtering opciókat, ezek leggyakrabban engedélyező módban működnek: amit ide felvesszünk, annak joga lesz kapcsolódni a többiekhez és a világhálózathoz (néha még a hatókörzetet is megadhatjuk LAN, WAN és WLAN

2 TB hálózati adattároló eszköz ReadyNAS NV+

- ➔ akár 2 TB tárolókapacitás
- ➔ egyedülálló X-Raid technológia
- ➔ EMC Retrospect® - backup szoftver
- ➔ 3x multifunkciós USB port
- ➔ csendes működés

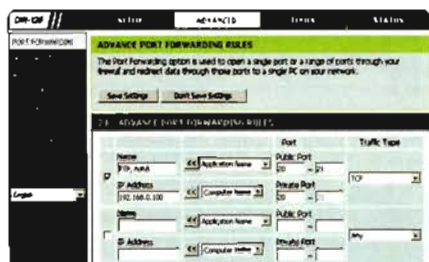
- ➔ Nagyvállalati adatmentő eszköz munkacsoportok számára. 2 TB tárolási kapacitás (4x HOT SWAP SATA HDD 500 GB).
 - ➔ RAID 0, 1, 5 egyedülálló X-RAID technológia a könnyű bővíthetőségért. RAID HW gyorsítás - a hagyományos NAS eszközökhöz akár 30%-kal gyorsabb.
 - ➔ A különböző operációs rendszerek (MS, MAC, LINUX) natív támogatása és közöttük fájlcsere lehetősége.
 - ➔ Médiaszerver, integrált iTunes támogatás, távoli elérés web-en, HTTP-n vagy FTP-n keresztül.
- (Rack változatban 3 TB tárolókapacitással is kapható.)

(Visszonteladók számára a HRP, mint disztribútor forgalmazza - www.hrp.hu, info@hrp.hu)



NETGEAR
Connect with Innovation™

www.netgear.com



A Port Forward funkció a NAT kezelésére való. Ez csak a portok kezelésében hasonlít a tűzfalhoz, valójában nem az

képében). A kényelmes weboldalakon a DHCP szerver által kiosztott címeket a gépek nevei alapján könnyedén bemásolhatjuk, de ha mindezt kézzel kell megtennünk, akkor használjuk a jól ismert *Hálózati kapcsolatok/Állapot/Támogatás* ablakának tartalmát, vagy a CMD hatására nyíló ablakban az `IPCONFIG /ALL` parancsot. A lista kialakítása időigényes, de mindenképpen megéri!

Portbűvészet

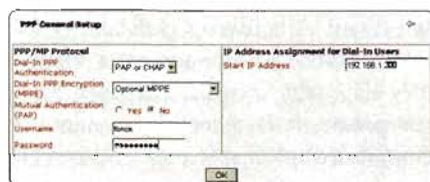
Otthoni routerek üzembe helyezése után nem sokkal abba a problémába ütközhetünk, hogy egy-két program nem tud csatlakozni az internetre. Ez azért van, mert a router címfordítást végez, és nem

tudja (ugyan, miért is tudná?), hogy például az MSN milyen portot használ. Az *Application Rules/Advanced* menü alatt találjuk a Port Forwarding opciót, ezzel egy adott belső PC adott portját megnyithatjuk a külvilág számára. Így már az összetett szerverekről érkező adatokat is fogadni tudja a gépünk, felcsatlakozva például csevegni, állományokat áttölteni is tudunk. A Port Forwarding beállításainál a belső gép IP-címét, portját, valamint a külvilág felé nyitandó portcímét kell megadni, akár tartomány (től-ig) formában. Így nem csak az adott alkalmazásnak adunk utat (pl. FTP esetén a 20-as és 21-es nyitásával), de akár több gép azonos portját is a külvilág felé irányíthatjuk.

Tegyük fel, hogy két belső gépen fut FTP szerver, és mind a kettőt elérhetővé szeretnénk tenni. A külvilág számára csak

egy 21-es (és 20-as) port létezik, ezért azt kell irányítanunk. Létrehozunk hát egy szabályt, amely az egyik gépnek a 20-as és 21-es belső portjait a router 20-as és 21-es külső portjára, a másiknak pedig egy olyat, amelyben a 20-as és 21-es belső portjait a router (összünk a hasunkra, és keressünk egy szabad portot) 2020-as és 2121-es portjaira irányítja. Így a második szerver a 2020-as FTP Control és a 2121-es FTP Data portokon válik elérhetővé. Ehhez persze az is kell, hogy az interneten csücsülő kliens programja ezekre a portokra legyen beállítva.

Érdekesebb funkciót lát el a Port Trigger. Ebben ugyanúgy definiálunk portokat, mint az előbb, de minden egyes szabályhoz tartozik egy ún. Trigger Port is. Alapjában véve ugyanúgy működik, mint a Port Forward, de a router megfelelő portjait csak akkor nyitja meg, ha a belső oldalon a PC-ről a trigger portjára folyamatosan érkezik adat. Ez a rendszer nagyobb biztonságot ad, hiszen csak akkor fogják megtalálni routerünk publikus oldalon nyitott portját, ha éppen forgalom zajlik. A módszer szépséghibája, hogy ennek kihasználásához megfelelő programra van szükség, amely



Ritkán használt funkció, de akkor nagyon fontos lehet, hogy a router VPN szerverként is üzemel (Draytek Vigor)



ROUTER JÁTÉK

Játsszon velünk és nyerje meg a TP LINK termékek egyikét vagy egy Gainward videokártyát!

1. Keresse fel honlapunkat!
www.cp.hu



2. Típelje meg a helyes válaszokat kérdéseinkre!
3. Nyerjen!

Jelentkezési határidő: szeptember 23.

Sorsolás: szeptember 24.



5/6 portos switch



6dBi beltéri antenna



108M PCMCIA kártya



108M WiFi router



108M WiFi USB adapter



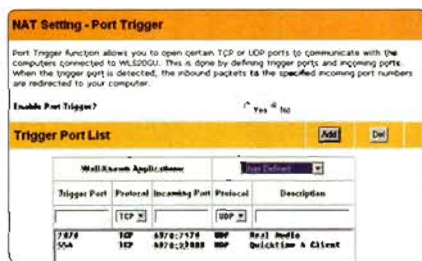
Gainward 8600 GT VGA

Együttműködő partnerünk:

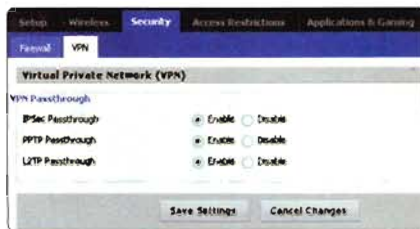


az adatátvitel mellett stimulálja a trigger portot is. Ritka megoldás, általában nem kell hozzányúlnunk.

Szerencsénk van, hogy a Microsoft befoltozta a Windows alatt sérülékeny Universal Plug and Play rendszert, ennek egyik szolgáltatása, hogy a vele szót értő routereken igény szerint portokat nyisson és csukjon. Az UPnP bekapcsolásával mentesülhetünk a portnyitási bonyodalmak egy részétől. Jobb routereken előre elkészített alkalmazás-listát találunk, így elég csak a gépünk IP-címét és a használni kívánt programot megadni (pl. ICQ, Battlenet), az automatikusan megnyitja a hozzá tartozó portokat.



Egy ASUS routeren megtaláljuk azt a két alkalmazást, amely kamatoztatni tudja a Port Trigger funkciót: a RealAudio és a QuickTime



A VPN támogatás engedélyezése nem jár biztonsági hiányossággal, a kapcsolatot ugyanis csak a belső hálózathoz jövő kezdeményezésre épül fel

VPN

A VPN (Virtual Private Network) segítségével két hálózatot kapcsolhatunk össze nem biztonságos hálózatot, tehát az internetet használva. A két hálózat, amely végletes esetben csupán két számítógépből áll, titkosított csatornát használva kommunikál egymással. A kommunikáció számukra transzparens: a VPN ún. Tunneling protokoll, ami azt jelenti, hogy bármilyen másik protokoll csomagjait egy titkosított csomagon belül mozgatni tudja. Ennek megfelelően a VPN lassabb, mint a közvetlen TCP/IP kommunikáció, a szoftvereknek és hardvereknek a biztonsági kódolásokat is kezelniük kell. A VPN önmagában is megérne egy egész

tanfolyamot, telepítése és bonyolultsága okán. Egy otthoni router annyira támogatja a VPN-t, hogy felismeri és átengedi a kommunikációját. A protokoll teljesen zárt, ezért a benne lévő forgalmat nem lehet szűrni a tűzfallal. A routeren általában három VPN-nel kapcsolatos opciót engedélyezhetünk: az Enable/Passthrough IPsec, PPTP és L2TP.

Kezdjük a PPTP-vel (Point-to-Point Tunneling Protocol), amely egy PPP kapcsolat alatt hozza létre a virtuális hálózatot. Leggyakrabban az MSCHAP-v2, illetve a tanúsítványt használó, biztonságosabb EAP-TLS hitelesítést használja. Mivel az előbbi a Windows szervert használó cégek előnyben részesítik, a PPTP-t esetükben engedélyezni kell.

Az L2TP (Layer 2 Tunneling Protocol) a Cisco L2F és a Microsoft PPTP protokolljának együttes előnyeit használja, és több OSI réteget átfog. Magas biztonságot csak az IPsec-kel (IP Security) együtt ad. Hogy cégünk melyiket használja, azt a rendszergazdától tudhatjuk meg. Ha egyáltalán nem használunk VPN-t, akkor ezeket az opciókat tiltsuk le.

Megjegyezzük, hogy egyes routerek VPN szerverként is működhetnek. ■

5 évesek lettünk!

IPM

A GONDOLKODÓ EMBER LAPJA

- > érthető tudomány
- > élvezhető művészet
- > olvasható irodalom



Rendeljen **20%-os** kedvezménnyel
éves IPM előfizetést
7740 helyett **MOST 6192 Ft-ért!**

3 szerencsés előfizetőnket
wellness-hétvégével ajándékozzuk meg!



A kedvezmény 2007. szeptember 1. és december 15. között beérkezett megrendelésekre érvényes.

Előfizethető telefonon: **(1) 225-2390**, faxon: **(1) 225-2399**,
e-mailen: elofizetes@interpressmagazin.hu,
interneten: www.interpressmagazin.hu.



Router iskola – 5. rész

Ezen az órán a routerekhez erősen kötődő VoIP beállításával, a filmek, játékok hatékony használatát is segítő forgalomszabályozással, no meg a WLAN médialejátszók finomhangolásával ismerkedünk meg. Csak elszántaknak!

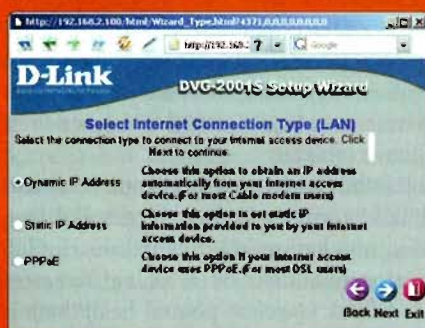
Szerző: Köhler Zsolt

VoIP és streaming

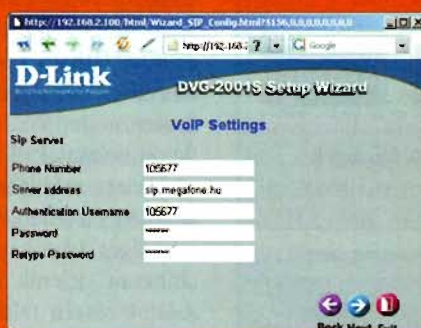
A VoIP (Voice over IP) kezelését a cégeknél jellemzően dedikált vezérlők végzik, ám a technológia annyira elérhető, hogy egyre több önálló TA (Telephony Adapter) és VoIP-képes router képében megkaphatjuk. A TA és a VoIP router között annyi a hasonlóság, hogy míg előbbi szinte bármelyik hálózatba integrálhatjuk, utóbbinak a TA-val azonos szolgáltatásait kell csak használnunk. Noha akár a szoftveres csevegőprogramok hangkommunikációját is nevezhetjük VoIP-nak. Több zárt rendszer mellett két nyílt és elterjedt protokoll van: a P2P alapú Skype és a központosított SIP.

program, ezért ugyanúgy konfigurálható a routeren, mint más programok. Az előző részben a portnyitás fortélyait is bemutattuk, a hatékony működéshez viszont nem árt, ha szabályozzuk a forgalmat. A forgalomhoz a Skype az összes portot igénybe veheti, de a 443-as és 80-as portok elegendők számára.

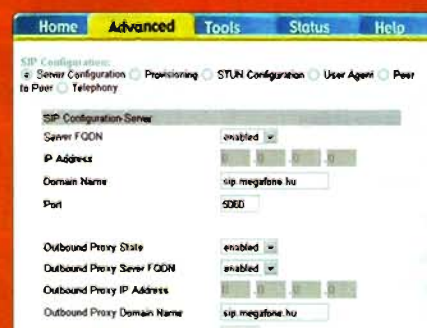
A SIP (Session Initiation Protocol) ezzel szemben annyira centralizált, mint egy telefonközpont. Az IP hálózat előnye, hogy nem szükséges minden egyes végponthoz külön vezetékét húzni, de ez azt is jelenti, hogy a készülékünk a világon bárhol lehet. Híváskor csatlakozunk a központhoz, adataink azon



A telefonadaptert akár a router nélkül is használhatjuk, ekkor úgy konfiguráljuk, mint egy router WAN csatlakozását



Az alapadatok, amelyeket a szolgáltató a szerződésében megad



A telefonadaptereket a szolgáltatók előre konfigurálják – ez csak a jéghegy csúcsa

Hasonlóságok

A Skype P2P (peer to peer) protokoll, tehát a szerver csak azt követi, hogy mikor, honnan és ki jelentkezett be a hálózatba. Azt már nem, ha kezdeményezünk egy kapcsolatot, az adatok ugyanis közvetlenül a két végpont között fognak áramlani, így nem csak a hálózatot, a szervert is kímélik. Az adatokban nincsen semmilyen különleges, TCP és UDP csomagokat használ

keresztül fognak haladni. A SIP Layer5 protokoll, az adatok a Skype-hoz hasonlóan TCP vagy UDP csomagok formájában közlekednek, részben a hívó felek között.

A SIP előnye, hogy minden hívónak saját hívószáma lehet, a publikus telefonhálózat (PSTN) és a VoIP hálózat közötti átjárás automatikus. A SIP hardverei és szoftverei az 5060-as portot használják.

A telefonos szolgáltatások használatához a Provisioning funkciót is beállítják

Ha az adapter a router mögött van, a STUN segítségével átjuthat a NAT-on

A hálózat egyszerűbb kihasználásához kapcsoljuk be a VAD funkciót!

A használt kodekek vizsgálati sorrendje egyértelmű, a mögötte lévő idő a vizsgálat periódusát adja meg

Codec	Priority	Packet Interval
G.711a-law	2nd	20 ms
G.711u-law	1st	20 ms
G.729a	3rd	20 ms
G.726	4th	20 ms
ILBC	no-use	20 ms

VoIP alapok

A TA-k és VoIP routerek túlnyomó többsége a SIP protokollt, a PC-hez kapcsolható telefonok pedig többnyire a Skype protokollját támogatják. Alapfeltétel, hogy a számítógépeken futó programoknak portot nyissunk, a többi általános regisztráció alapján működik. A SIP protokoll funkcióit csak és kizárólag a szolgáltató kérésére szabad módosítani, de mit tegyünk, ha nekünk éppen egy másik szolgáltató tetszik meg?

A SIP Server FQDN bonyolult paraméternek hangzik, ez csupán a szerver domain neve. Az FQDN jelentése *Fully-Qualified Domain Name*, azaz tökéletesen hiteles domainnév. Az opció ki- és bekapcsolható, tehát ha a szolgáltatónk teljesen hivatalos, engedélyezhetjük, a kapcsolat felvétele gyorsabb lesz. A *Domain name/service domain* mellé a szolgáltatónk nevét, a *port* sorba pedig 5060-at kell írunk. Ugyanezeket az opciókat egyébként proxyhoz is megadhatjuk, ami azért érdekes, mert ez egy VoIP proxy a szolgáltatónál. Magyarország nem olyan nagy, hogy szükség lenne régióként proxyszerverekre, de ha a szolgáltató ezt kéri, akkor be kell állítanunk.

Lehet, hogy szolgáltatónk DNS szerveret is üzemeltet, akkor azt szolgáltatónk kérésére be kell állítanunk a *DNS-SRV Query Domain* alatt, a *Use DNS-SRV* opciót pedig engedélyeznünk kell.

Szolgáltatások

A kliensek a szolgáltató bővített szolgáltatásait (pl. az üzenet-rögzítőt) is használhatják, ehhez az XML használatával tudnak különféle parancsokat elérni a kliensek, így a TA is. Ha engedélyezzük az *XML Provisioning function*-t, akkor a szolgáltató hatékonyabban tudja kezelni a klienseket. Mint sok más, ez sem divat mindenhol. A kapcsolódás titkosításához az *SSL*-t kell engedélyezni, az XML-hez tartozó szervernevet (*Server URL*), címet és portszámot, no meg hitelesítő kulcsot a szolgáltató adatai alapján kell megadnunk.

A belső hálózatot, egészen pontosan a routerek címfordítását (NAT) érinti a VoIP telefonokba is épített STUN (angolul kábítást, átmítást jelent). A *Simple Traversal of UDP over NAT* annyit tesz, hogy a NAT mögötti telefon a csomagok fejlécét úgy módosítja, hogy a publikus hálózaton vele kapcsolatot tartó STUN szerver a telefont gond nélkül elérje. Ennek kapcsán a routerünk publikus IP-címét is megszerzi. Ez a módszer akkor hasznos, ha a routeren a telefon számára nem nyitottunk dedikált portot. A STUN csak aszimmetrikus NAT-okon használható, mint amilyen az otthoni routereken van, használata azonban bonyodalmakat okoz a közvetlenül, kézzel beállított címzésekkel operáló routereken.

Ha mégis használjuk, a konfiguráció alatt a szerver *IP-címét*, *portját*, valamint a szinkronizálás sűrűségét (*ReqInterval*) a szolgáltató adatai szerint kell beállítanunk. Ha a készülék felismeri, akkor a *NAT Type* alatt jelzi routerünk címfordítási rendszerét. A regisztráció, tehát a szerverrel való kapcsolat létét a router (vagy TA) az általunk beállított időszakonként ellenőrzi. Erre a *Register Expiration* opció szolgál, értéke másodperc.

Akárcsak az internet-hozzáférés, a VoIP is állítható szakaszos üzemre, az inaktivitás utáni lecsatlakozás türelmi idejét az *Initial Unregister* opcióval állíthatjuk be. A tárcsázott hívás utáni válasz megérkezésének idejét a *Session Expires* idővel lehet változtatni (ajánlott: 1800s), a *Min-SE* idővel pedig ennek minimálisan



D-Link Vezeték nélküli ADSL akció!

Keresd meg ADSL modemed, és vásárolj most D-Link vezeték nélküli routert akár 5000 Ft kedvezménnyel!

Regisztrálj D-Link modemed vásárlásához a www.dlink.hu honlapon, és a D-Link vezeték nélküli routert akár 5000 Ft kedvezménnyel!



- Vezeték nélküli ADSL router
- Vezeték nélküli LAN
- Vezeték nélküli Wi-Fi
- Vezeték nélküli USB
- Vezeték nélküli FireWire
- Vezeték nélküli Bluetooth



www.dlink.hu

TIPPEK, TRÜKKÖK

kötelező értékét; az alapérték itt is 1800s. Ez utóbbiak növelésével terheltebb lesz a szolgáltató szervere, túlzott csökkentése hibaüzenetet eredményez. A szervereknek azért kell követniük a tranzakciókat, hogy hálózati hiba esetén hatékonyan tudják másfele irányítani az adatokat, biztosítva a folyamatos telefonálás lehetőségét. A másodperceknek semmi közük ahhoz, hogy mi éppen hány másodpercet telefonálunk, ezt ne növeljük feleslegesen.

Érdekes, inkább nagyobb forgalmú helyeken alkalmazott a *P2P lista*, amelynek bejegyzései az általunk gyakran hívott címek azonosítóit (ha tetszik: telefonszámaikat) és fix IP-címüket tartalmazzák. A gyorsabb hívás feltétele, hogy mindkét félnek állandó IP-címe legyen, de ekkor a célállomás speciális porton keresztül is fogadhatja hívásunkat.

Telefonközelsben

A VoIP használatához egy felhasználói nevet (telefonszámot) és jelszót is kapunk, amely értelemszerűen elengedhetetlen a szolgáltatás használatához. Mikor társalgunk, akkor a hívó fél számát megkapja a telefonunk, ha engedélyezzük a *Display CID* opciót, mások pedig a miénket kapják meg, ha bekapcsoljuk a *Caller ID Delivery* opciót.

Bármily furcsának hat, a tárcsázás IP alapokon is működik (mi több, még faxolhatunk is); ezt a *DTMF Method* funkcióval állíthatjuk, hiszen a SIP protokoll a *DTMF (Dual-Tone Multi Frequency)* kódokat is natív módon kezeli, továbbítja. Ezeket minden nyomógombos telefon ismeri, és alkalmazza az *RFC2833*-as szabvány alapján. A router/TA ezt ismeri és értelmezi különböző módokon. A régebbi SIP rendszereknél

A router iskola részei

1. Alapok
2. WAN és LAN
3. Vezeték nélkül
4. Tűzfalak, szűrők, VPN
5. VoIP és streaming
6. Haladó beállítások
7. Hardver tuning, firmware-frissítés
8. Hardveres-szoftveres különlegességek

az *inbound* jól működött, de az *RFC*-n és *Info*-n kívül lehetőség szerint ne válasszunk mást.

Beszélgetés közben nem vesszük észre, de sokat hallgatunk, érdemleges információt nem kell továbbítani. Ahhoz, hogy a csönd átvitelére ne pazaroljunk adatokat, kapcsoljuk be a *VAD (Voice Activity Detection)* opciót. Az adaptereken sok esetben még a telefon felől vett és a feléje adott jeleket erősíteni lehet a *Receive*, illetve a *Transmit gain* opcióval. A decibel értéket finoman hangoljuk be, ha a telefonunkon nem lehet hangerőt állítani, a decibel skála ugyanis logaritmikus.

Ha már a hangminőségnél tartunk, emeljük ki a hangátvitel során használt kodekek prioritási sorrendjét (*Codec priority-packet interval*). Míg a régi programokban csak egyetlen hangtömörítő kodeket használhattunk, a VoIP programok/hardverek a rendelkezésre álló pillanatnyi sávszélesség függvényében dinamikusan tudják változtatni az éppen használt kodeket.

A lehetséges kodekek egy részét ismerik a hardverek, a kifejezetten audió alkalmazásokra kifejlesztett, ősrégi *G.711* (a *u-law* Amerikában, az *a-law* szinte mindenhol máshol használt a telefonközpontokban). Minősége jó, sávszélességigénye 64 kbit.



ROUTER
JÁTÉK

Játsszon velünk és nyerjen
egy Netgear zsinornélküli
„Dual” Skype telefont!

1. Keresse fel honlapunkat!
www.cp.hu



2. Típelje meg a helyes
válaszokat kérdéseinkre!
3. Nyerjen!

Jelentkezési határidő: október 25.

Sorsolás: október 26.

NETGEAR zsinornélküli „Dual” Skype telefon – SPH200D

- Egy készlet az internet alapú ingyenes hívásokhoz és a hangminőséges vezeték nélküli telefonáláshoz
- Ingyenes beállítások és lehetőség Skype-felhasználókkal (nem igényel számítógépet)
- Nagy hatótávolság a DECT zsinornélküli technológiának köszönhetően
- A jövő további fejlesztéséhez (SPH150D) kapcsolható hozzá
- Kristálytiszta hangminőség



Együttműködő partnerek:

NETGEAR
Connect with innovation™

A G.729a kis processzorigényű, minősége elviselhető, támogatja a VAD-ot, és jellemzően csak 8 kbit/s az igénye. A G.726 a kettő között helyezkedik el, 16–40 kbit/s a sávszélességigénye, hangminősége körülbelül a G.711-hez hasonló, ezt használják a nemzetközi beszélgetéseknél a hang kódolására.

Jó alternatíva lehet a GSM (ismert minőség, 12,2 kbit/s) vagy az iLBC (Internet Low-Bandwidth Codec) a maga 15,2 kbit/s sebességével. A prioritás meghatározásánál alapvetően mindegyik eszköz a jó hangminőséget részesíti előnyben, majd adja alább a csekély sávszélesség-foglaltság felé, ezt megfordítva gyengébb hangminőséget, de több szabad sávszélességet kapunk eredményül.

Félúton a QoS felé

A QoS (Quality of Service) magyarul forgalomszabályzást jelent, amelyet az adatcsomagok különféle megjelölésével, felismerésével és e szerint történő csoportosításával – előnyben részesítésével

„gaming” üzemmód például a játékok és streaming videók által előszeretettel használt UDP csomagokat engedi át kisebb fennakadással (*Optimize for gaming*), de a QoS ennél több beállítással is rendelkezhet, például a kényelmesen konfigurálható D-Link DGL-4300 esetében.

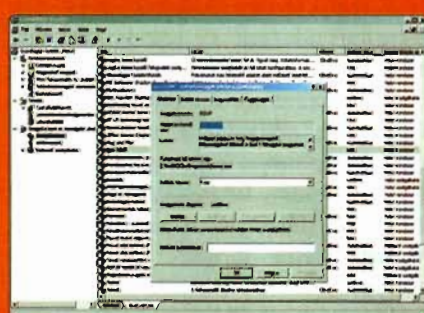
A legfontosabb, hogy a forgalomszabályzó algoritmusnak ismernie kell a rendelkezésünkre álló maximális le- és feltöltési sebességet (*Up/Downlink speed*), ezt kbit/s-ban kell megadnunk, hiszen az adott forgalmat ehhez méri. A router vagy a publikus oldalon (*WAN port*) vagy a belső oldalon (*LAN & WLAN portok*) tudja szabályozni a forgalmat. Ez már nem minden router szolgáltatása, az otthoniak többsége csak a belső oldalt kezeli, ami nekünk tökéletesen elég.

Bizonyos esetekben, pl. a DD-WRT firmware-ben (ennek használatáról később) a QoS rendszerét is megadhatjuk. A HFSC (*Hierarchical Fair Service Curve*) egy valós idejű, adaptív sebességű szolgáltatás, amely kiváló rendszer, a Linux-rendsze-



Ha a Signaling TOS és RTP TOS után 7-et állítunk be, és a router is kezeli a QoS-t, az akadózás oka nem a mi hálózatunkban lesz

Egy jól működő QoS konfiguráció DD-WRT alatt: a SIP protokoll kiemelt szerepet kap



A Windows QoS-támogató szolgáltatásának is futnia kell, különben a programok nem élhetnek kiemelt hálózati jogaikkal

vel vagy korlátozásával – érünk el. A QoS és a VoIP szinte kéz a kézben jár, de ma már a hálózati játékok és letöltések elterjedésével a QoS önmagában otthoni felhasználásra is csábító.

A TA-ban találunk néhány QoS kapcsolót: a QoS type lehet TOS vagy DiffServ rendszerű, ezzel igazából a VoIP adapter által küldött forgalmat jelölhetjük a routerünk számára. A TOS (*Type of Service*) és a DiffServ (*Differential Services*) egyaránt a prioritás beállítására szolgál (0-kikapcsolva, 1-háttér, 7-valós időben), de a fejlett adott bájttát másképpen értelmezik a routerek. A TOS régebbi, ám mind a kettő hatékony használatához szükséges az adatokat megfelelően értelmező router.

Az igazi QoS

A QoS lényegét már elmondtuk, ám a fejlett routerekben ez még tovább hangolható. Visszakanyarodva a routerek funkcióira, a QoS-t igyekeznek egyszerű módon tálni az otthoni felhasználóknak. Ekkor nem kell portokkal és IP-címekkel variálnunk, elég megadnunk, hogy a netről töltődő videók gyorsabban jöjjenek le, mint az általános adatok, de akár a VoIP javára is billenthetjük három-négy ágú mérlegünk nyelvét.

Ehhez persze fontos, hogy a PC-n ne legyen letiltva az operációs rendszer QoS támogatása, így a programok önmaguk meg tudják jelölni csomagjaikat, akárcsak a VoIP adapter. A

reknek is része. A HTP (*Hierarchical Token Bucket*) algoritmus egyszerűbb, bizonyos esetekben gyorsabb, ám az adatok továbbításának biztonságaért kevésbé felel. Viszonylag kevés, egy időben egymás mellett használt program esetén, ha azok adatforgalma nem túl ingadozó, az utóbbit nyugodtan választhatjuk, más esetekben az előbbi.

A rendszertől függetlenül nekünk kell meghatározunk, hogy mely szolgáltatások, mely portokon, mennyi előnyt kaphatnak a többiekhez képest. Érthető, hogy ha mindegyiket előnyben részesítjük, akkor valójában egyiket sem emeltük ki a többi közül. Alapvető módszer szolgáltatás (portcím) alapján szabályozni, ez esetben adott IP-címeket, portcímeket hozhatunk létre – olyan routereknél, mint a D-Link DGL vagy DIR családja –, a portokhoz szolgáltatások és programok vannak rendelve, csak választanunk kell.

A Bulk (terjedelmes, lassú), a Standard, Express és Premium fokozatok mellett ritkán még kivételt is tehetünk valami számára a QoS alól az Exempt opcióval. Ez éppen elég egy QoS-hez, de esetenként hálózati tartományokhoz, egyedi IP vagy MAC címekhez, vagy akár konkrét Ethernet portokhoz kapcsolhatjuk a szabályokat. Egy jól beállított QoS gördülékenyebbé teszi az internet elérését, de ne számítsunk arra, hogy csak e miatt szárnyakat kapnak a letöltések.

Haladó beállítások

▶▶ Az otthoni routerek egyikén sincs két WAN port, amelyiken ugyanis van, az már üzletinek minősül. Célja az, hogy a megkettőzött internetkapcsolatnak köszönhetően a belső hálózat akkor is elérje a világhálót, amikor az egyik kapcsolat megszakad.

A két WAN-os routerek csábítóak lehetnek, ám az olcsóbbaknál csupán a *Failover* funkció létezik. Ekkor a WAN1 ugyanúgy csatlakozik a szolgáltatóhoz, mint hagyományos esetben, az általunk kijelölt szerverek elérhetetlensége esetén (a hiba a szolgáltató oldalán van, de nem közvetlenül a router előtt) automatikusan átvált a WAN2 portra, amely értelemszerűen egy másik szolgáltatóhoz csatlakozik. A módszer nagy biztonságot ad, hiszen ritkán fordul elő, hogy egyszerre mindkét szolgáltatás leáll – ennél nagyobb biztonságra csak a valóban nagy hálózatok esetében van szükség.

A Failover működéséhez nem kell WAN2 port, azt a routerbe épített ISDN modemmel vagy soros portra csatlakoztatott modemmel – ha mérsékelt sebességgel is –, de használni lehet.

Router iskola – 6. rész

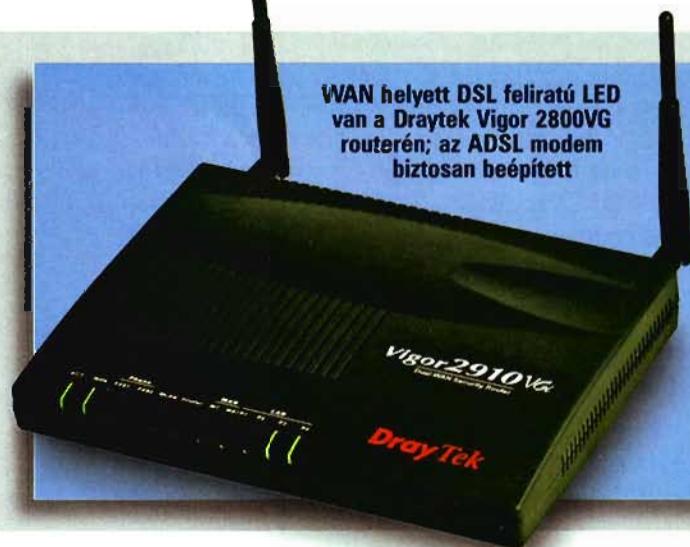
Az előző részekben a routerek főbb működési paramétereit tekintettük át. Most további hasznos és különleges opciókat részletezünk – „Mindent bele!” mottóval.

Szerző: Köhler Zsolt

Az igazi Load Balancing – mint a neve is mutatja – a terhelés függvényében intelligensen szabályozza a rendelkezésre álló WAN kapcsolatok bejövő és kimenő forgalmát. Sok esetben ez szorosan összekapcsolódik a QoS rendszerrel, amellyel igény szerint oda irányítjuk a forgalmat, ahova csak szeretnénk. Az egyik kapcsolat kiesésekor értelemszerűen a másik veszi át a terhelést, ebből a felhasználók csak annyit vesznek észre, hogy az internet elérése kis mértékben lassul.

WAN helyett DSL feliratú LED van a Draytek Vigor 2800VG routerén; az ADSL modem biztosan beépített

Nemcsak a biztonságot növeli WAN2 portjával a Draytek Vigor 2910VG, de analóg telefont is csatlakoztathatunk rá a VoIP használatához



Még ma is kaphatunk olyan Draytek routert (Vigor 2910G), amely a WLAN mellett ezt a funkciót is biztosítja.

De még ez a kis és közepes felhasználók számára méretezett router is csak a *Bandwidth on Demand* típusú Load Balancing technikát ismeri, amely mindkét vonal működőképessége esetén is használni tudja a második csatlakozást. Ha a felhasználók igénye túllépi a WAN(1) port sávszélességét, akkor a router automatikusan kapcsolódik a második hozzáférésre is, amelyre a többletterhelést irányítja. Ha a második vonalat idő vagy adatmennyiség alapján használjuk, akkor ezzel a módszerrel pénzt takaríthatunk meg.

Relay

Ez a különleges funkció lehetővé teszi, hogy a PPPoE kapcsolat VPN csatornán (L2TP) keresztül épüljön fel. Ezzel a szolgáltató oldalán lévő szerverek meg tudják hirdetni szolgáltatásait a kliens(ek) számára, amelyek bármiféle különleges program nélkül használni tudják ezeket a szolgáltatásokat. Ha tehát a szolgáltatónk ezt a kapcsolatot igényli, akkor biztosak lehetünk abban, hogy speciális szolgáltatásokat is kínál. A PPPoE Relay csak kevés routeren érhető el (pl. D-Link, Repotec), ha tehát egy ilyen kapcsolatot szeretnénk megosztani, a lehetőségeink igencsak korlátozottak lesznek.

Egy kis LAN

Bemutattuk, hogyan működik a NAT, egyes routereken (pl. Zyxel Prestige) pedig a SUA funkcióval is találkozhatunk. A Single User Account az egyre szaporodó felhasználók internetre csatlakozására készült, és egy kicsit másképpen működik, mint a NAT. A cím fordítása itt is megtörténik, ám a küldő címét a router küldés előtt átírja egy előre meghatározott címre. A válaszcsomagok erre a címre érkeznek, a router kézbesítés előtt pedig visszairja a célcímre.

Ennek a módszernek az előnye akkor mutatkozik meg, ha a nagy cégek nem gondoskodtak globális, egyedi IP címről, illetve hálózatuk nagysága többet kívánna. A kis hálózatoknál viszont az előny abban nyilvánul meg, hogy a belső hálózaton több szervert működhet, egymás zavarása nélkül.

Ha már itt tartunk, meg kell említenünk a Multi-NAT funkciót is (Draytek, Netgear, Zyxel), amely az üzleti felhasználásban mutatja meg erejét. Ha az ISP (internetszolgáltató) nem csak egy, hanem több fix IP címet adott a cégünknek, a routert rábírhatjuk arra, hogy a publikus IP címeket belső IP címekhez párosítsa. A One to One – nevéből adódóan – egy az egyhez megfeleltetést jelent, a Many One to One esetben több lokális és globális IP cím van összepárosítva. A Many to One módban az imént említett SUA lép életbe, a Many to One Overload esetén több helyi címet foghatunk össze egy publikus cím használatához.

Integrált modemmel

A következő opciókkal már az önálló ADSL modemek is beállíthatók, ám azt tudnunk kell, hogy a szolgáltatás mellé adott modem szinte minden esetben a szolgáltató tulajdonát képezi. A beállítások megváltoztatásának így többnyire nincs értelme, még akkor sem, ha modemmel egybeépített routert kapunk – a

Bár nem látszik rajta, a Zyxel Prestige P-335WT többet tud a hagyományos NAT-nál

A router iskola részei

1. Alapok
2. WAN és LAN
3. Vezeték nélküli
4. Tűzfal, szűrők, VPN
5. VoIP és streaming
6. Haladó beállítások
7. Hardvertuning, firmware-frissítés
8. Hardveres-szoftveres különlegességek



Behálózuk a világot.







Super G & Kiterjesztett Hatótáv™
54/108Mbps vezeték nélküli Router

- 108M vezeték nélküli LAN Router, 2.4GHz
- 802.11g/b, beépített 4-portos Switch-csatló
- 108M Super G™ technológia
- 2x-3x Kiterjesztett Hatótáv™ technológia
- forgatható SMA Antenna



Super G & Kiterjesztett Hatótáv™
54/108Mbps vezeték nélküli USB Adapter

- IEEE 802.11g WLAN USB Adapter
- Super G™, akár 54/108Mbps átviteli teljes 802.11b kompatibilitás
- Kiterjesztett Hatótáv™, akár 9x nagyobb, mint a normál vezeték nélküli adaptereknél



Super G & Kiterjesztett Hatótáv™
54/108Mbps vezeték nélküli PCMCIA Adapter

- IEEE 802.11g WLAN PCMCIA Adapter
- Super G™, akár 54/108Mbps átviteli teljes 802.11b kompatibilitás
- Kiterjesztett Hatótáv™, akár 9x nagyobb, mint a normál vezeték nélküli adaptereknél



6dBi 2.4GHz beltéri asztali Yagi Antenna

- Frekvencia távolság: 2.4GHz - 2.5GHz
- Sugárzási irány: kétirányú
- Jel erősség (csúcsérték): 6dBi
- Kábel hossz: 100cm
- Csatlakozó: SMA közvetlen dugó/fordított



Kábel/DSL Router beépített 4/8 portos Switch DDNS felügyelet, 802.1X

- 4/8 db 10/100Mbps LAN port
- 1 db 100Mbps Auto-Negotiation WAN RJ45 port
- Beépített tűzfal IP cím szűréssel
- Domain Name és MAC cím szűrés
- Felhasználói adminisztráció, webcím szűrés

Adatátvitel



Beltéri távolság

108M, 54M, 11M

100 méter, 200 méter

- Hagyományos 802.11b szabvány
- Hagyományos 802.11g szabvány
- TP-LINK vezeték nélküli szabvány 2x-3x kiterjesztett hatótávval
- TP-LINK vezeték nélküli szabvány 2x-3x kiterjesztett hatótávval és 108M Super G-val

A beltéri távolság függ a működési környezettől is.

Kiemelt importőr:

Mercury Magyarország Kft.

1131 Bp., Dolmány u. 14. tel.: 221-3020 fax: 221-4254

www.mercurycomputer.hu mercury.hungary@ahol.com

TIPPEK, TRÜKKÖK

szolgáltatók ezt általában előre konfigurálják. Ha teljes egészében lecserélnénk modem-router párosunkat, és nem tudunk fellépni az internetre, hogy ellenőrizzük a modem paramétereit, akkor (is) jól jön, ha ismerjük a főbb beállításokat – legalább azért, hogy tudjuk, mit nem szabad elállítani.

A legfontosabb beállítás általában az *ADSL Settings* menüpont alatt található, a neve *Modulation Type*. A modem nem a szabványos Ethernet jelszintekkel dolgozik, hanem a telefonvonalon néhány kilométer távolságig eljutó magas frekvenciás jelekkel (25 kHz felett).

Hogy milyen legyen a fizikai moduláció, azt a szolgáltató *DSLAM (Digital Subscriber Line Access Multiplexer)* készüléke határozza meg, a modemet ehhez kell igazítani. Az ADSL modulációi az ANSI T1.413 (8/1,5 Mbit), az ITU G.992.1 (G.DMT, 8/1 Mbit) és az ITU G.992.2 (G.Lite, 1,5/0,5 Mbit). ADSL2/2+ jelzésű modemeken az ADSL2 (12/3,5 Mbit), Annex L (24/1 Mbit), esetleg Annex M (24/3,4 Mbit) lehet. E két utóbbi egyébként az ADSL2+ sebessége, ám a sort még folytathatnánk, a későbbiekben ugyanis jöhetnek majd a VDSL előfizetések.

Az *ATM (Asynchronous Transfer Mode)* az ADSL alap adatátviteli módja, és az Ethernethez hasonlóan csomagkapcsolt, 53 bit nagyságú, fix méretű csomagokat használ, amelyek csak a két végpont kapcsolatának felépítése után továbbíthatók. A kapcsolatot jelző *VPI (Virtual Path Identifier)*

nálói nevünket, jelszavunkat is itt állíthatjuk be. Előfordulhat, hogy a kapcsolat minőségét javíthatjuk a hibajavító *Trellis* algoritmus bekapcsolásával, a *Bit Swapping* engedélyezésével az adatáramlás egyenletesebb lesz, illetve kevesebb energia szükséges az adatok továbbításához. Végül, de nem utolsósorban az *SRA Enable* opció bekapcsolásával a modem a kapcsolat fenntartása mellett meg tudja változtatni annak sebességét (*Seamless Rate Adaptation*), így a kapcsolat rossz körülmények esetén sem szakad meg.

Láthatjuk, hogy csak az utóbbi három opciót érdemes a sebesség és stabilitás növelésére használnunk, a többi megtartása kötelező.

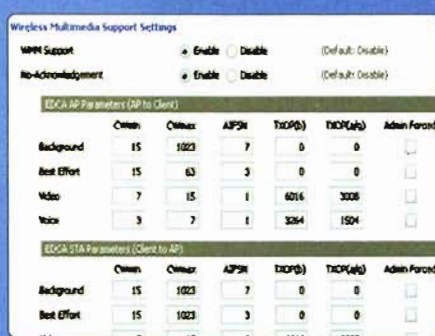
WLAN streaming

Leginkább a QoS-hez illik a WLAN routerek *WMM Support* opciója, amely a vezeték nélküli hálózatban szabályozza a streamelt anyagok szállítását. Kezdjük az elején: a *WMM*, azaz *Wi-Fi Multimedia*, más néven *Wireless Multimedia Extension (WME)* olyan szabvány, amely garantálja a vezeték nélküli hálózatokban a különféle multimédiás eszközök együttműködését. A filmek, zenék, hangok (VoIP) átvitele egy bizonytalan vezeték nélküli hálózatban gondokat okoz, a forgalom jelentősen lelassulhat vagy megakadhat már egy kisebb zavar esetén is.

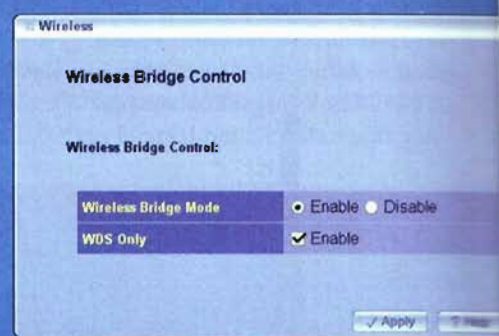
A *WMM* energiatakarékossági és QoS funkciókat is tartal-



A WAN kapcsolat konfigurálásánál furcsa opciók fogadnak, azokat a szolgáltató paramétereit szerint kell beállítanunk



A WMM-támogatáshoz tartozó táblázat értékeit csak fix, nem mozgó hálózatban van értelme módosítgatnunk



Ha kell WDS, akkor csak a partner routerek MAC-címeit kell megadnunk, az azonosítás innentől kezdve nem IP alapú

és *VCI (Virtual Channel Identifier)* a csomagok fejlécében található. Az *ATM VC Settings* alatti értékek állandóak, a változtatásuk nincs hatással a sebességre. A *VPI* 8 vagy 16 bit, a *VCI* 16 bit hosszú.

A fizikai kapcsolaton kívül a WAN kapcsolat típusát is beállíthatjuk, választva a *Statikus* és *Dinamikus IP*, a *Bridge* és a *PPPoE/PPPoA* között. Bridge esetén a közvetlen kapcsolat az *IP LLC* vagy a nagyobb hatékonyságot biztosító *VC-Mux* szabályai szerint működhet. Még érdekesebb, hogy az aszinkron kapcsolaton is működik a QoS, ám ennek otthon az *UBR (Unspecified BitRate)* változatát kell használnunk, hiszen csak egy kapcsolaton él, alkalmazásszintű szabályokat pedig IP alatt hozhatunk csak létre.

A *PPPoE* már ismert, ám az aszinkron adatátvitel miatt a *PPPoA (PPP over ATM)* is használt, ez viszont nem szenved a korábban vázolt MTU méret okozta sebességszökkenésben. Ha PPP-t használunk, amire otthon nagy az esély, akkor a felhasználó

maz. A nagyobb hálózati hatékonyság érdekében elég a WLAN routeren a *WMM Support* opciót bekapcsolnunk, és már nyugodtan hátra is dőlhetünk. Ötletes újítás, hogy a QoS keretében a rádió sugárzott csomagok *Ack* és *NoAck* jelölést kapnak, ami annyit jelent a vevőnek, hogy azokat nyugtáznia (*acknowledge*) kell, vagy nem kell. A streamelt adatokat nem szükséges nyugtázni, hiszen ha például elvesz egy-két csomag a beszélgetésből, az átadott információ lényege megmarad. Ezt a módszert néha külön is engedélyeznünk kell a *No-Ack* opcióval.

Az utolsó beállítás csak a legészakutabbakat érdekelheti: az *EDCA AP (AP->kliens)* és *STA (kliens->AP)* paraméterek táblázata. A sorokban *Background* (háttér), *Best Effort* (leggyorsabban átadott), *Video* és *Voice* nevek szerepelnek, ezek a különféle adattípusokat adják meg az itt külön, tehát csak a WLAN részen tevékenykedő QoS motor számára. A sorokban négy paramétert adhatunk meg, szabályozva az adatok kezelését. A táblázatokban mindenütt időket adunk meg.



A komoly WDS-hez irányított antennák dukálnak



Ha megtelik a napló, az okos router e-mailben figyelmeztet arra, hogy olvassuk el annak tartalmát



Komolyabb routerek az úgynevezett Syslog szerverre is el tudják küldeni a lehető leg-részletesebb naplót

A CWmin és CWmax értékek egy nem túl egyszerű, de hatékony számítási algoritmus alapján azt adják meg, hogy mennyi ideig várakozzon a router vagy a multimédia kliens, mielőtt újra adást kísérel meg. A pontos beírandó értékek helyszínektől függően változhatnak, és elsősorban a vételi minőségtől függenek. Az értékek módosításával az esetlegesen akadozó WMP (Wireless Multimedia Player) képe kisimítható.

Mindezzel csak akkor érdemes foglalkozni, ha az adó és a vevő helyzete nem változik. Az AIFSN (Arbitration Inter-Frame Spacing Number) értéke megadja, hogy két adás között mennyit várakozzon a hálózati eszköz. A legegyszerűbb hálózatban ennek értéke lényegtelen, de több kliens mellett előfordulhat, hogy mindkét készülék ugyanabban a pillanatban kíván adni, ütközést előidézve a hálózaton. Ekkor természetesen mind a kettőnek várakoznia kell, tehát csökken a hálózat kihasználtsága. Nagyon fontos, hogy az AIFSN értékével az eszközök prioritását lehet módosítani a „mezei” WLAN kliensekhez képest.

A TXOP(b) és a TXOP(a/g) az adatok küldésének várakozási idejét adja meg a 11 mbps és 54 mbps sebességű kliensek felé. A Transmission Opportunity nagyon hasonlít az AIDSN-hez, de ez nem a csomagok közötti várakozási időt, hanem a router adás-kezdeményezéseinek idejét állítja be. Ha tetszik, ezzel szabályozhatjuk a kevert (802.11b és a/g) hálózatokban a lassú-gyors kliensek hálózathasználati arányát.

Végül az Admin forced opció letiltja a készülékek adaptív rendszerét, és csak azokat az értékeket használja, amelyeket mi megadtunk neki.

WDS és társai

A WLAN routerek körében egyre gyakoribb szolgáltatás a WDS (Wireless Distribution System), amelynek bekapcsolásával a routerek meg tudják osztani egymással a klienseket, de a fő router internetcsatlakozását is, így nem kell minden egyes hozzáférési pontot bekábelezni. A kliensek csupán a WLAN



ROUTER JÁTÉK

1. Keresse fel honlapunkat!
www.cp.hu



2. Típelje meg a helyes válaszokat kérdéseinkre!
3. Nyerjen!

Jelentkezési határidő: november 26.
Sorsolás: november 27.

Játsszon velünk és nyerjen egy NETGEAR ProSafe™ ADSL Vezetéknélküli Tűzfal terméket és egy zsinórnélküli „Dual” Skype telefont.



NETGEAR DGV338 ProSafe™ ADSL Vezetéknélküli Tűzfal

- Integrált, kompakt kialakítás a kis- és közepes vállalatok részére
- hat-az-egyben funkcionáltság: Wireless Access Point, Switch, VPN, Firewall, Router & ADSL 2+ Modem
- VPN csatlakozás támogatása 60 IPSec-t
- SNMP menedzselhetőség
- WPA2 nagyvállalati vezeték nélküli adatvédelmi kódolás
- 8 port 10/100 LAN switch, 1 ADSL WAN Port és 1 WAN port failover-hez

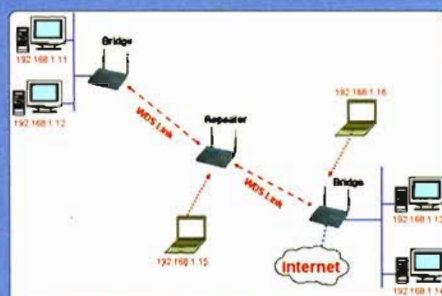


NETGEAR zsinórnélküli „Dual” Skype telefon - SPH2000

- Egy készülék az Internet alapú ingyenes hívásokhoz és a hagyományos vezetékes telefonhálózathoz
- Ingyenes beszélgetési lehetőség Skype-telefonokkal (nem igényel szimulációt)
- Nagy hatótávolság a DECT zsinórnélküli technológiának köszönhetően
- Akár további 3 kiegészítő (SPH1000) kiegészítő hozzá
- Kiszélesített hangminőség

Együttműködő partnerünk:

NETGEAR
Connect with Innovation™



Ez a kép jól szemlélteti a WDS lehetőségeit. Kár, hogy a távol (bal felső sarok) lévő felhasználók mindenkivel osztoznak a sávszélességen



Az egyszerű router az alapvető működéséről ad információkat, például azt, mikor kértek tőle automatikus IP címet

Az egyszerű LinksysLogon kívül általános monitorprogramok is léteznek a forgalom figyelésére



térert érzékelik, két azonos beállítású hozzáférési pont (AP vagy WLAN router) közül azt választják, amelyiknek nagyobb a téreje, így a sebessége.

A WDS működése során a routereknek látniuk kell egymást; a beállítások alatt a routerek MAC címét rögzítenünk kell, minden beállítás azonos, csak az SSID nem. Tipikus esetben tíz másik AP fogható munkára, ezeket WDS Relay/Repeater üzemmódba kell állítanunk.

Ha egy WAN csatlakozással ellátott routertől távol álló kliens adatot küld, a hozzá legközelebb álló AP a csomagot megismétli a következő WDS AP-nak, az pedig tovább addig, amíg a WAN-ba kapcsolt routerre ér. A távolságtól, illetve az AP-k számától függően egyre lassabb a kapcsolat, hiszen az azonos WLAN csatornán működő AP-k közül egyszerre csak egy beszélhet.

Noha egyes routereken kiválaszthatjuk a WDS Hibrid (ASUS) opciót, nagyobb távolságokon ez kifejezetten lassú. Ezzel a beállítással a router úgy működik a WDS hálózatban, hogy a LAN portján lehetőséget ad a vezetékes kliensek csatlakozására is, amelyek nem a WAN, hanem a WLAN hálózaton (akár több AP-n) keresztül csatlakoznak az internetre.

Ha nem használjuk a WDS-t, de az előbbi módszer szerint csatlakozunk, akkor ahhoz a routernek az egyre népszerűbb WISP (Wireless Internet Service Provider) rendszert is ismernie kell. Ilyen például a nálunk is járt D-Link DAP-1160. Ekkor a router a WLAN interfészen keresztül csatlakozik a szolgáltatóhoz, a kapcsolatot pedig a LAN portok osztja szét. Ez speciális

módszer, hiszen a kapcsolat a WLAN-on épül fel, ehhez pedig ajánlott az erősen irányított antenna, és szükséges a szolgáltató antennájára való közvetlen rálátás. A WISP itthon még nem igazán terjedt el, ám a jövőben nagyszerű módszer lesz a kisebb települések internet-hozzáféréseinek biztosítására.

Napló

Az Event/System LOG opció alatt a router működését követhetjük nyomon. Itt az újraindulások idejéről, az adminisztrátor bejelentkezési idejéről, esetleg hibás jelszaváról kapunk információt. Erre a szolgáltatásra minden router képes, de arra már kevesebben, hogy a bejelentkezési próbálkozásokról e-mailt küldjenek.

A DHCP szerver kapcsán említettük a csatlakozott felhasználók listáját – ez sok esetben a WLAN kliensekkel is működik. ám a napló fő feladata mégsem a felhasználók kijelzése. Sokkal inkább az, hogy a rendszerünk hibáira fényt derítsen, és értesítsen a biztonságot érintő változásokról.

A tűzfal naplóját (Firewall LOG) azért érdemes nézegetni, mert a napló részletessége a tűzfal szűrési módszeréről árulkodik: minél alaposabb, annál több támadási módokról ad információt. Ha változtatni lehet a naplózási mélységet, elégedjünk meg az alacsony-közepes részletességgel, illetve azzal, hogy a tűzfal csak a kritikus támadásokat naplózza. Ha a napló részletes, akkor a router memóriája hamar megtelik, ezért a naplóban lévő időtartam lecsökken, a legrégebbi bejegyzés lehet, hogy csak néhány óráé lesz.

Diagnosztika

A hálózati kapcsolatokat a PING paranccsal ellenőrizhetjük a csatlakozó PC-ről, de alkalmanként szükség lehet arra, hogy a router és egy másik PC (LAN oldalon), vagy az internet egyik szerverének (WAN oldalon) az elérhetőségét ellenőrizzük. Előfordulhat ugyanis, hogy az adminisztrátori PC-ről nem érjük el az internetet, a router viszont csatlakozott már – a hiba tehát a PC-ben van.

Ennek kiderítésére a Diagnostic/Test Connection alatti menüpont Ping opcióját kell használnunk, ez ugyanúgy működik, mint a PC-n. Jó esetben a válaszidőket is megjeleníti, máskor csak azt, hogy sikeres-e a csatlakozás.

Elvéve még a Trace opciót is megtaláljuk, ezzel az interneten követhetjük végig egy kijelölt szerverig az útvonalat, minden állomás válaszüzejével együtt.

A Netgear legújabb, FDVG338 típusú VPN routere komoly tűzfallal védi a belső hálózatot, de ez tudásának csak kis része



Hardvertuning, firmware-frissítés



Router iskola – 7. rész

Az előző részekben sorra vettük a routerek valamennyi beállítását, ezek után már senkinek nem szabad, hogy gondot jelentsen a konfigurálás. Van még néhány fogás, amelyekről szót kell ejtenünk.

Szerző: Köhler Zsolt

A routerek nem bővelkednek a tuninglehetőségekben – az egyedüli kivétel a Linksys WRT-54G család. De ne szaladjunk ennyire előre, előbb térjünk ki néhány alapvető funkcióra, amelyek a tuninggal kapcsolatos firmware-frissítés során is szerepet játszhatnak.

Beállítások elmentése

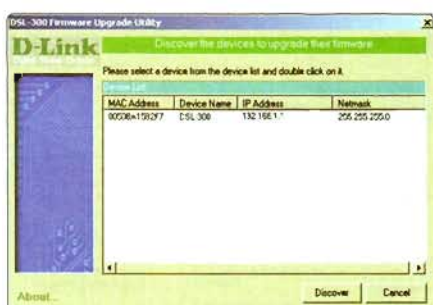
A fárasztóan beállított konfigurációt, különösen ha a tűzfalnál beállított portok száma már legalább kettőre rúg, érdemes elmenteni. Erre minden router lehetőséget ad úgy, hogy a *Backup Configuration* menüvel a routerről a PC-re másoljuk a konfigurációs állományt. A frissítés után ezt a *Restore Configuration* ponttal másolhatjuk vissza, majd indítsuk újra a routert.

Néhány routernél az is előfordul, hogy a konfigurációt nem a PC-re tudjuk elmenteni, hanem magára a routerre. Ha létezik *Save/Write to NVRam* és *Load/Read from NVRam* opció, akkor a router flashmemóriájának azon részére kerülnek az adatok, amelyet a firmware frissítése nem érint.

A firmware frissítése

A router iskola részeire ránézve talán többen elgondolkodtak azon, hogy ugyan mit is lehet írni a firmware frissítéséről, hiszen elég feltölteni az új verziót. Nos, igazuk van: nem lehet vele oldalakat megtölteni, de ez a mi szerencsénk.

A router gyártójának weboldalát kell csak megkeresnünk, majd onnan a *Support* menüpont alatt az adott készülékhez tartozó állományokat elérve a legújabb firmware-t kell letöltenünk. A gyártó megállapítása sokszor egyértelmű,



Egyszerű a frissítés webes felület használata nélkül a D-Link DSL-300 modemeknél, hála a dedikált programnak

kétes esetben pedig használjuk az internetes keresőt, amelybe írjuk be a router alján lévő címke típusadatait vagy az FCC-ID-t.

A letöltött állományt, amely általában BIN kiterjesztésű, adjuk meg a *Firmware* sorban, majd kattintsunk az *Update* gombra.

Fontos, hogy a művelet folyamán használjunk a PC-t és a routert ellátó szünetmentes áramforrást, a BIOS-okhoz hasonló biztonsági funkciók itt ugyanis nem érhetők el. Ha egy villamos zaj miatt egy helyen módosul a firmware, az hibás működéshez, esetenként végzetes hibához vezet. Ellenőrzésre sincs lehetőségünk, ezért a legkisebb hibát sem szabad megengednünk.

A frissítés után indítsuk újra a routert, lehetőleg a webes felület *Restart/Reset* gombjával, de ha erre nincs lehetőségünk, akkor nyomjuk meg a *Reset* gombot röviden. Ha nem indul újra, akkor húzzuk ki, várjunk egy fél percet, majd dugjuk be ismét. Ha a gyári beállításokkal és a legutóbbi konfigurációnkkal sem tudunk bejelentkezni rá, akkor addig nyomjuk a

Reset gombot, amíg az előlapi LED-ek nem állnak alaphelyzetbe (felvillannak, majd kialszanak egy időre).

Egyes routerek csak akkor állnak gyári alaphelyzetbe, ha a *reset* gombot a bekapcsolás közben nyomjuk, majd nyomva tartjuk legalább tíz-tizenöt másodpercig.

Ha valamilyen okból ez sem lenne elég, akkor a következő lépések már a sikertelen frissítés miatti javítás kategóriájába tartoznak.

Javítás

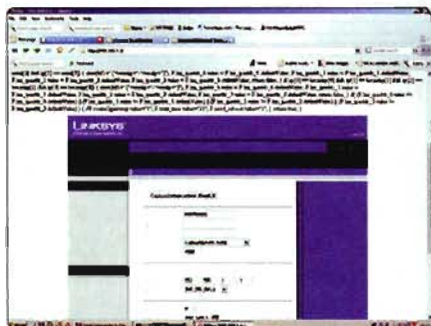
Akárcsak az alaplap BIOS esetében, a javítás a Flash-ROM újrairásával történik. Míg egy alaplapban ki lehet cserélni a memória IC-t, addig egy routerben erre nincs lehetőség, hiszen az minden esetben rá van forrasztva a panelra.

Mivel egy hibás firmware-es router annyit ér, mint egy jó állapotban lévő tégla, a javítást „debricking”, azaz „téglatlanítás” névvel illetik.

A Linksys WRT-54G-s családban (is) a javítás a router frissítés által nem érintett firmware-en (ha tetszik, BIOS-án) alapzik: a router az indulás első pár másodpercében a 192.168.1.2 címről elfogadja a TFTP (*Trivial FTP*) protokollal feltöltött firmware-t. Ha a hiba a firmware

A router iskola részei

1. Alapok
2. WAN és LAN
3. Vezeték nélkül
4. Tűzfalak, szűrők, VPN
5. VoIP és streaming
6. Haladó beállítások
7. Hardvertuning, firmware-frissítés
8. Hardveres-szoftveres különlegességek



A rosszul sikerült firmware-frissítés szerencsés változata, amikor a hiba az adminisztrációs felületen látszik, a router pedig elérhető a hálózaton keresztül

felírásakor keletkezett, akkor az a rész, amely elvégzi ezt az alapvető feltöltést, szerencsés esetben sértetlen maradt. A javítás után már elindul a router, legfeljebb resetelnünk kell az alapértelmezések visszaállításához.

Ha az Ethernet porton keresztül nem hallgat ránk a router, akkor az alapvető szoftver feltöltését a router szétszerelése után hozzáférhető JTAG porton keresztül lehet elvégezni egy megfelelő „flasher” programmal. Ennek a programnak támogatnia kell a router kommunikációs áramkörét, és a programot tároló flashmemória

típusát. A műszaki hókuszpókusz nélkül gyakorlatilag ugyanazt kell elvégeznünk, mint az alaplap BIOS-ok felírásakor az Uniflash programmal, csak itt a program CICLaMaB, illetve a HairyDairyMaid WRT54G Debrick Utility névre hallgat.

A programokkal akár a teljes firmware, akár csak a TFTP-s feltöltést végző bootloader is felírható, tehát a JTAG portos javítás után a routernek már úgy kell működnie, mint új korában. Ezek után ellenőrizzük a működőképességet (LED-villogás, Ping, bejelentkezés), ám ha semmilyen pozitív jelezt nem produkál a router, akkor egészen biztosan tönkrement. Ha szerencsénk van, az áramköri lap tápegységoldali részét talán meg tudja javítani egy „szaki”, ennél bonyolultabb javításokra az áramkör integritása miatt nem igazán van lehetőség.

Alap tuning

Ha minden jól működik, akkor kétféle módon tuningolhatjuk a routert: az antennája cseréjével



Figyelem!

A firmware frissítését csak a műszakilag képzett felhasználóknak ajánljuk, a módosításokat pedig mindenki csak a saját felelősségére végezze!

és/vagy a firmware módosításával. Az alapvető cél általában az, hogy megnöveljük a router által besugárzott terület nagyságát, így téve alkalmassá arra, hogy több falon keresztül, problémás vételi viszonyok között javítsunk a WLAN kliensek kapcsolatán.

A router iskola harmadik részében (CP 2007/08) több tippet is adtunk arra, hogyan lehet stabilabbá tenni a vezeték nélküli kapcsolatot, a valós megoldás mégis az antennák cseréje, fejlesztése. A kérdéses számban egy WLAN antenna-tesztet is közlünk, ám a tanulságokat most itt is összefoglaljuk.

Az irányított antennák egy távoli WLAN kliens kapcsolatát teszik stabilabbá (TP-Link)

COMPUTERBOOKS

Teljes kínálatunk a
www.computerbooks.hu
weboldalon!

1126 Bp., Tartsay Vilmos u. 12.
Levélcim: 1253 Budapest, Pf. 71.
Telefon: 375-1564
Telefon/Fax: 375-3591
Email: info@computerbooks.hu

TE KIKÖTNÉD?

D-Link Vezeték nélküli ADSL akció!

Keresd meg ADSL modemed, és vásárolj most D-Link vezeték nélküli routert akár 5000 Ft kedvezménnyel!

Regisztráld D-Link modemed gyári számát a <http://adsl.dlink.hu> oldalon, jelöld meg, melyik terméket választod, és már másnap vezeték nélkül netezhetsz otthon vagy irodádban!

DIR-524 Wireless G router
~~8 590 Ft~~ **8 590 Ft**

DIR-524 + DWR-G122 Wireless G kezdőcsomag
~~13 580 Ft~~ **13 580 Ft**

- Ideális megoldás kisebb lakások ADSL kapcsolatának vezeték nélküli megteremtésére több számítógép között
- 54Mbps vezeték nélküli sebesség
- WEP, WPA, WPA2
- NAT tűzfal VPN támogatással
- Lecsatlakozható antenna
- D-Link Click'n Connect telepítőprogram

DIR-615 Wireless N router
~~19 990 Ft~~ **19 990 Ft**

DKT-410 Wireless N kezdőcsomag
~~29 990 Ft~~ **29 990 Ft**

- Nagyobb otthonok teljes vezeték nélküli lefedésére egyetlen eszközzel
- Draft-11n technológia - 300 Mbps vezeték nélküli sebesség
- Kompatibilis a 11g és 11b vezeték nélküli hálózattal
- Quality of Service StreamEngine-mel
- D-Link Click'n Connect telepítőprogram

Magyar nyelven | 06 1 461-3001
A csatlakozás hálózati kábelrel és 11b/11g vezeték nélküli adapterrel történik.

D-Link
Building Networks for People

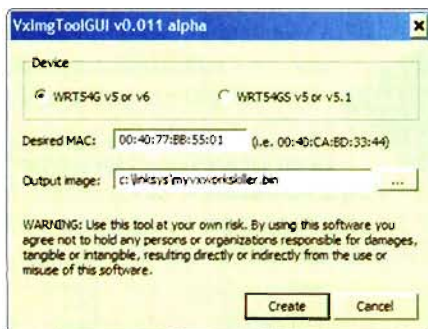
THINK D-Link
Building Networks for People

www.dlink.hu

Antennacsere nélkül a kimenő teljesítmény növelésével a hatótávolságot, esetleg a sebességet is növelhetjük, de csak egy bizonyos szintig. Akkor, ha a kliens hatótávolsága nem elég ahhoz, hogy a router vegye a jeleit, hiába növeljük az adóteljesítményt az egekig, fordított irányban nem nő a teljesítmény. A router jel-zaj viszonya szélsőséges esetben romlik, a közeli csatornákra jobban átszór – zavarva a közelben lévő többi AP forgalmát. A router adó- és vételi teljesítményét nagyobb méretű antennával növelhetjük, de ugyanezt a kliens (ha PCI-os, vagy külső AP) antennájával is megtehetjük.

Haladó tuning

Szóba került az adóteljesítmény növelése, ami bizonyos esetekben jól kiegészíti a nagyobb, esetleg az irányított antenára teljesítményét. Sajnos nem minden routeren tehetjük ezt meg, egy bizonyos



A Linksys WRT-54G jól tuningolható router. A V5 és V6 verziókon nem Linux, hanem VxWare rendszer fut, amelynek letöltéséhez speciális programot kell használnunk

Elterjedt platform: az AR7-es

A routerek egy része a Texas Instruments AR7-es, RISC processzoros, hálózati interfészekkel, USB 1.1 csatolóval és esetenként WiFi kártya-interfészsel ellátott alaplapjaira épül. Mivel a hardver elég olcsó, csak egy megfelelő kinézetű dobozba kell beszerezni, módosítani a hozzá tartozó „gyáribb” firmware-t, és már készen is van egy versenyképes termék. A TI AR7-es alaplapját használja – a teljesség igénye nélkül – az AVM Fritz/Box család, a D-Link DSL-xxxT modemek, a Linksys néhány WAG-családba tartozó ADSL modeme, a Netgear DG834G AP-je és a ZyXEL Prestige 660M.

csoporton belül is csak akkor, ha speciális, módosított firmware-t töltünk fel rá. Bizonyára sokan ismerik a Linksys WRT-54G családot, amelynek első verziójának megjelenésekor többen felfedezték, hogy a firmware valójában egy Linux. A lelkes fejlesztőket látva a Linksys úgy döntött, hogy szabaddá teszi a firmware-t – a szokásos árversenyen kívül ez oda vezetett, hogy a router széles körben elterjedt. Később, a V5 és V6 verziók már nem



A piacon alig van olyan router, amellyel pontosabban tudnánk a QoS-t konfigurálni (DD-WRT)

Linux, hanem VxWare alapokon működtek, ezek módosítása még összetettebb, a náluk is újabbak módosítására pedig az elmúlt hetekben született megoldás. A router beszerzésekor nem kell azon gondolkodnunk, hogy jó verzió-e a miénk, hiszen a piacon a V5-ös változat mellett megjelent a WRT-54GL, amelyet kifejezetten a módosításra ajánlottak.

Akkor sem kell keseregnünk, ha nem Linksys a routerünk típusa, a közel azonos beltartalom miatt egyes ASUS (WL-500g), Buffalo (WBR-G54), Motorola és Siemens routerek is szóba jöhetnek.

Az új firmware-ek között ingyenes és fizetős változatok is akadnak, a legtöbb szolgáltatással az ingyenes DD-WRT büszkélkedhet. A fejlesztők egyébként nem a firmware-ekkel, hanem a vele ellátott speciális hardverekkel csinálnak pénzt. Nagy szerencse, hogy a még mindig ingyenes firmware fejlesztése szakadatlan.

A DD-WRT telepítéséhez le kell töltenünk a www.dd-wrt.com címről a legfrissebb firmware-t (Downloads/Stable/dd-wrt.v23 SP2 alól a dd-wrt.v23_sp2_mini.zip és a dd-wrt.v23_sp2_voip.zip vagy a dd-wrt.v23_sp2_vpn.zip állományt). A frissítéshez először a Mini firmware-t kell feltöltenünk, hiszen a gyári nem minden esetben engedi a nagyobb méretű firmware feltöltését. Ezután a VoIP-

JTAG

A JTAG (Joint Test Access Group) csatlakozó általános diagnosztikai csatlakozó, amelyet az áramköri lapon elhelyezett összes, jellemzően programozható digitális áramkörrel való kommunikációra fejlesztettek ki. A JTAG használható a programozható áramkörök valós idejű tesztelésére (ICE – In-circuit emulator) is, a routerek kapcsán számunkra csak a javító funkciók érdekesek.

JTAG csatlakozó kiosztás

nTRST	1	2	GND
TDI	3	4	GND
TDO	5	6	GND
TMS	7	8	GND
TCK	9	10	GND
nSRST	11	12	GND / n/a
n/a	13	14	Vcc

Megjegyzés: a 12 érintkezős változat (Linksys) a 12-es érintkező nincs bekötve

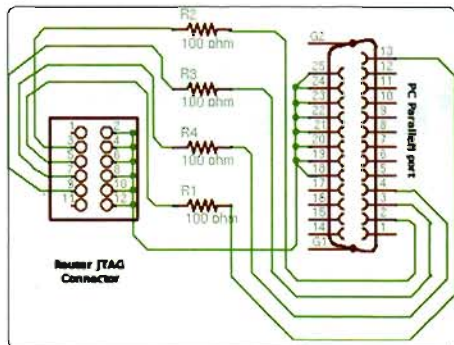
vagy a VPN-támogatással bíró változatot kell feltöltenünk. Azt, hogy használhatjuk-e a nagyobb firmware-eket, illetve routerünkre telepíthető-e a DD-WRT, a www.dd-wrt.com/wiki/index.php/Supported_Devices oldalon tekinthetjük meg.

Javítás szerelés nélkül

A javító számítógépen állítsunk be fix 192.168.1.2-es IP címet, majd nyissunk egy parancssoros ablakot (CMD). Itt adjuk ki a `TFTP -i 192.168.1.1 PUT C:\firmware.bin` utasítást. A PUT után a router gyári, vagy a DD-WRT mini firmware-ének elérési útja található. Az utasítás kiadása előtt húzzuk ki a hálózathoz, vagy kapcsoljuk ki a routert, majd a visszakapcsolása után a második-harmadik



Nem router, de hálózati eszköz és firmware is frissíthető rajta – élő netkapcsolat esetén az egész folyamat automatikus (Netgear SC101 NAS)



A Linksys routerek JTAG csatlakozókábeléhez négy 100 ohmos ellenállás az alkatrészigény

másodpercben nyomjuk le az Entert. Néhány másodperc várakozás után visszkapjuk a parancssort. Ha

ez nem hibaüzenet, akkor fél perc várakozás után kapcsoljuk ki, majd ismét be a routert. A rajta lévő fényeknek úgy kell villogniuk, mint a jól működő készülékeken. Próbáljuk megpingelni a 192.168.1.1-es (illetve a gyárilag megadott) IP címet, de ha ez nem válaszol, reseteljük a routert, majd próbálkozzunk ismét. Sikeres feltöltés után az adminisztrációs felületen frissíthetjük a nekünk tetsző változatra a firmware-t.

Javítás szereléssel

Első feladatunk szétszedni a routert, és megkeresni rajta a JTAG feliratú portot. El kell készítenünk egy egyszerű, vagy elektronikai szempontból biztonságosabb JTAG kábelt. Ez némi elektronikai gyakorlattal nem gond, az alkatrészek pár ezer forint körüli összegből megvásárolhatók és percek alatt összeszerelhetők. Komplet kábel is vásárolható (Xilinx JTAG letöltőkábel, ChipCAD) 5900 forintért.

A következő lépés a feltölteni kívánt firmware és az azt JTAG-on keresztül feltöltő (égető) program letöltése. Több közül is választhatunk, nekünk a legjobban a downloads.openwrt.org/utis oldalról tölthető parancssoros *HairyDairyMaid WRT54G Debrick Utility* tejszett. A program a `-backup:cfe`, `-backup:nvram`, illetve `-backup:kernel` kapcsolókkal indítva a flashmemória egyes részeit letárolja (a CFE területen van a router MAC címe is, és ez felel a kernel betöltéséért). A `-backup:cfe`, illetve `-backup:nvram` parancsokkal érdemes elmentenünk a kritikus memóriarészeket, ha később valamit tényleg elrontunk, legyen hova visszatérni.

Az égetéshez a `-flash:cfe` és a `-flash:nvram` parancsokat adjuk ki a `wrt54g.exe` után, a működő routerre pedig a TFTP-s módszerrel töltjük fel a firmware-t, a teljes memória égetése a JTAG módszerrel nagyon lassú. Fontos, hogy a parancsok kiadása előtt húzzuk ki a routert, majd a csatlakoztatás után nyomjunk Entert – a hardverben aktív a watchdog, amely egy idő után, ha a firmware nem válaszol, automatikusan újraindítja a routert. Ha nem bekapcsolás után kezdjük az írást, ez hibát fog okozni.

DD-WRT alternatívák

Emlékezzünk meg a sokat megélt, de nem mindenképpen kiemelkedő ingyenes firmware-ekről, amelyek a DD-WRT alternatívái lehetnek. A Linksys eredeti kiadásától alig különbözik a *HyperWRT*, ebben a plusz szinte csak a kimenő teljesítmény emelése. A *Freeman* a fizetősnek indult *Talisman* firmware „feltöréseként” terjedt el, tudása szinte azonos a *HyperWRT*-ével. Igazi csemege az *OpenWRT*, aki komolyan ért a Linuxhoz, az az ingyenesen hozzáférhető csomagok alapján készítheti el az *OpenWRT*-n alapuló egyedi firmware-ét. Aki egyszerűsége és nagy tudásra vágyik, annak természetesen a DD-WRT a legmegfelelőbb.



TP-LINK®

Behálózuk a világot.



Super G & Kiterjesztett Hatótáv™ 54/108Mbps vezeték nélküli Router

- 108M vezeték nélküli LAN Router, 2.4GHz
- 802.11g/b, beépített 4-portos Switch-csel
- 108M Super G™ technológia
- 2x-3x Kiterjesztett Hatótáv™ technológia
- forgatható SMA Antenna



Super G & Kiterjesztett Hatótáv™ 54/108Mbps vezeték nélküli USB Adapter

- IEEE 802.11g WLAN USB Adapter
- Super G™, akár 54/108Mbps átvitel teljes 802.11b kompatibilitás
- Kiterjesztett Hatótáv™, akár 9x nagyobb, mint a normál vezeték nélküli adaptereknél



Super G & Kiterjesztett Hatótáv™ 54/108Mbps vezeték nélküli PCMCIA Adapter

- IEEE 802.11g WLAN PCMCIA Adapter
- Super G™, akár 54/108Mbps átvitel teljes 802.11b kompatibilitás
- Kiterjesztett Hatótáv™, akár 9x nagyobb, mint a normál vezeték nélküli adaptereknél



6dBi 2.4GHz beltéri asztali Yagi Antenna

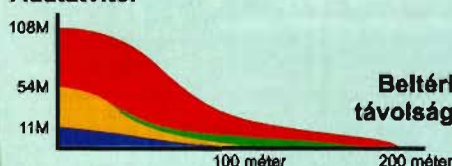
- Frekvencia távolság: 2.4GHz - 2.5GHz
- Sugárzási irány: kétirányú
- Jel erősség (csúcsérték): 6dBi
- Kábel hossz: 100cm
- Csatlakozó: SMA közvetlen dugó/fordított



Kábel/DSL Router beépített 4/8 portos Switch DDNS felügyelet, 802.1X

- 4/8 db 10/100Mbps LAN port
- 1 db 100Mbps Auto-Negotiation WAN RJ45 port
- Beépített tűzfal IP cím szűréssel
- Domain Name és MAC cím szűrés
- Felhasználói adminisztráció, webcím szűrés

Adatátvitel



- Hagyományos 802.11b eszköz
 - Hagyományos 802.11g eszköz
 - TP-LINK vezeték nélküli eszköz 2x-3x kiterjesztett hatótávval
 - TP-LINK vezeték nélküli eszköz 2x-3x kiterjesztett hatótávval és 108M Super G-val
- A beltéri távolság függ a működési környezettől is.

Kiemelt Importőr:

Mercury Impex
felnevünk a vevőinkkel

1131 Budapest, Dolmány u. 14. tel.: 221-3020 fax: 221-4254
www.mercurycomputer.hu mercury.hungary@ahol.com

Router iskola 8.

A Computer Panoráma magazin 2007-es router iskolájának befejező részét közöljük e mellékletben; bemutatjuk a különleges hálózati eszközöket.

Szerző: Köhler Zsolt

Hálózati különlegességek

Korábban már megemlítettük, hogy a Linksys WRT-54G-re telepíthető DD-WRT firmware valóban sokoldalúvá teszi néhány ezer forintba kerülő routerünket, arról azonban nem szóltunk, hogy milyen különlegességet tartogat az adóteljesítmény növelésén kívül.

Vissza a DD-WRT-hez

A LAN és WAN oldalon aktiválhatjuk a teljeskörű QoS funkciókat, amelyeket alkalmazás (portcím) alapján rendezhetünk sorba, de a prioritás MAC vagy IP cím, netán Ethernet port szerint is megadható. A szabályzás az összes feltételt egyszerre vizsgálja, ráadásul kétféle prioritáskezelési módszer közül választhatunk.

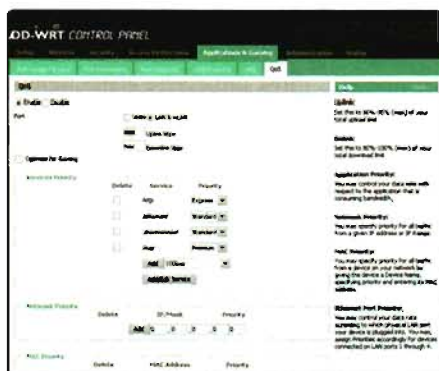
A LAN oldalon virtuális LAN (VLAN) hálózatokat alakíthatunk ki, így még akár egy nagyobb céges hálózat alapjaként is használhatjuk az igen olcsó routert, emellett szól az is, hogy két 100 megabites Ethernet portot a szerver számára összehozhatunk (Link Aggregation).

A biztonságot a szokásos tűzfal növeli, amely minden hozzáférést naplóz, a felhasználók, szolgáltatások engedélyezése/tiltása akár napok és órák szerint is beállítható. A felhasználók munkaidőben nem, azon kívül viszont korlátlanul cseveghetnek, letölthetnek – hogy csak egy egyszerű példát említsünk. A tűzfalat hatékony „rejtő” szolgáltatások segítik, amelyek a kliensek mellett a routeren futó DNS szerver károkozó céllal történő azonosítását is meg tudják akadályozni (pl. DNS Masq).

A vezeték nélküli szolgáltatások sokat bővültek, a WDS-beli üzemeltetés, az IPv6 és a WMM támogatás is természetes, no meg a WPA2 Radius-hitelesítésű (TKIP és AES) titkosítás is. Mivel a WRT-54G két antennás, az adminisztrációs felületen azt is megadhatjuk, hogy a két antenna közül

melyik legyen adó és vevő. Ez akkor különösen fontos, ha csak egy nagyobb antennánk van; azt a vevő oldalra kapcsoljuk, az adó teljesítményét pedig „szoftverből” növeljük meg.

Előnyös, hogy a router indulásakor az általunk megadott linuxos utasításokat végre tudja hajtani, így egy ritkán felbukkanó probléma néhány utasítás beírásával orvosolható.



A piacon alig van olyan router, amellyel pontosabban tudnánk a QoS-t konfigurálni (DD-WRT)



A DD-WRT pontosan annyi információval lát el, amennyire szükségünk van (Wireless)

De ez még mind semmi! A DynDNS-szerű szolgáltatások ellenőrzésére bekapcsolhatjuk a loopback funkciót, így a belső hálózatunkról ellenőrizhetjük, hogy a szolgáltatás működik-e. Más routereknél ezt az esetek nagy részében csak kívülről ellenőrizhetjük.

A DD-WRT olyan modullal is kiegészíthető, amellyel a routerben lévő flashmemória szabad részét a firmware



A DD-WRT segítségével a házilag beépített SD kártyaolvasó is használható



Ki gondolná, hogy az alig két éves cég már hazánkban is terjeszkedik? A router a képen nem véletlenül is ismerős

további programok futtatására, a tőlük kapott adatok tárolására tudja használni. Ehhez JFFS2 (*Journaling Flash File System 2*) fájlrendszert használ, amelyet nem csak a beépített memórián, hanem az egyszerű házi barkács megoldással beépíthető MMC/SD kártyaolvasón is használhatunk.

A kártyaolvasó nem csak ezért érdekes, hanem azért is, mert a rajta lévő fájlokat a beépített Samba FS szerverrel meg is oszthatjuk. Mivel az ASUS WL-500g támogatott, az USB-re csatlakoztatott külső tárat megoszthatjuk a szerverrel.

A DD-WRT azért is szimpatikus, mert a routerrel hotspotok is készíthetők, ehhez pedig a szintén linuxos és természetesen ingyenes, nagy sikerű *ChilliSpot* ad segítséget. Ezzel akár nyílt, akár jelszóval védett és hitelesítést igénylő hozzáférések is készíthetők. A működéséhez szükség van egy, a belső hálózatra kötött webszerverre, amelyre a WLAN hálózatra csatlakozott és böngészőt indító kliensek automatikusan átirányítódnak. A hitelességüket igazoló felhasználók ezután már szabadon használhatják az internetet, természetesen úgy, hogy egymást nem látják a hálózaton.

Végül, de nem utolsósorban a DD-WRT forgalmi adatokat tud szolgáltatni az adminisztrátori gépre telepített RFlow programnak.

Arról, hogyan lehet pontosan konfigurálni, kiépíteni egy speciálisabb rendszert, a www.dd-wrt.com oldalon találhatunk angol nyelvű információkat, a fórumokban feltett kérdésre pedig szívesen válaszolnak. Mint mindig, itt sem árt, ha előtte átbogarászuk a különféle kérdéseket és válaszokat.

Egyszerű különlegességek

A boltokban routerszerű konfigurációt igénylő, routolást nem végző hálózati eszközökből elég nagy a kínálat. Azoknak, akik elvégezték iskolánkat, nem okoz gondot majd a beállítás. A készülékek egy része tökéletesen egyszerű, mint például a nyomtatószerverek: ezek gyakorlatilag pontosan úgy működnek, mint a nyomtatókba épített változatok, és fordítást végeznek az Ethernet és az USB között. Azon túl, hogy a meghajtóprogramot telepítjük, semmilyen más teendőnk nincs.

Pontosan ilyen a *WLAN Repeater*, amelyet csak be kell kapcsolnunk és elhelyezni valahol a WLAN hálózatunk

Végy egy 3G mobilkártyát, és tedd be egy jó WLAN routerbe! Az eredmény a Linksys WRT-54G3G



Az egyszerű jelismétlőt csak energiával kell ellátni, máris kibővíti WLAN területünket

hatókörzetében. A hozzá érkező rádiós csomagokat megismétli, ezáltal lassítja a hálózatot, a távolban lévő kliens viszont gond nélkül csatlakozhat. Akkor, ha a WLAN hálózaton titkosítást használunk, a repeater adminisztrációs felületén vagy a hozzá adott programmal be kell állítanunk a korábban ismertetett opciókkal.

Több router támogatja a repeater üzemmódot, amelyet inkább irodai környezetben használhatunk, esetenként pedig a beépített nyomtatószerver is alapfelszereltség. Fontosnak tartjuk megjegyezni, hogy a routeren lévő USB port a legtöbb esetben csak nyomtatószerver, másra nem használható – vásárlás előtt erről mindenképpen meg kell győződnünk.

Fejlett hardverek

Néhány éve a routerek nem számítottak különleges terméknek, de amint elterjedt az internet, a gyártók egyre inkább az



otthoni felhasználókra kezdtek koncentrálni. Így először az otthoni játékosokkal lépést tartva jelent meg a *D-Link DGL-4300 GamerLounge* routere, amely nem csak intelligens QoS-sel, de a LAN oldalon gigabites portokkal is rendelkezik. Az egyszerű konfigurációk, különös tekintettel a QoS-re, ma is hódítanak, az *ASUS GigaX 1105N* például ebben is versenyre kell a *D-Link* routerével.

Aztán ott vannak az üzleti felhasználásra szánt készülékek, mint például a székházak közötti kapcsolat kiépítésére specializált routerek, amelyek G.SHDSL protokoll szerint akár 2,3 megabit/s sebességű kapcsolatot tudnak létrehozni (pl. *Zyxel P-791*). A Zykel kínálatában egyébként már most sorakoznak a VDSL/VDSL2 routerek, amelyek 50-100 megabit/s sebességet biztosítanak – megfelelő szolgáltató esetén.

A VPN routerek ma már külön kategóriát képviselnek, és jellemzően 2-10 egyidejű VPN csatorna kezelését végzik a szokásos tűzfal biztosítása mellett.

Elsősorban a kritikus üzleti felhasználók számára lesznek hasznosak a 3G (HSDPA) routerek, amelyek 3G/UMTS hálózatra terelik a WAN forgalmat. A GSM modemmel kiegészíthető WRT54G3G a fokozatos átállásban segít, hiszen még hagyományos DSL hálózatokhoz is tud csatlakozni, ám dedikált 3G-s routert is kaphatunk a *D-Link DIR-451* képében.

Speciális funkciók

Az otthoni felhasználók sikertermékei a BitTorrent hálózatot használó routerek, illetve NAS-ok. Elsőnek az *ASUS WL-500W* jelent meg a piacon, de ma már kaphatunk olyan otthoni NAS-t, amely hálózati (esetleg WLAN) médialejátszóként háttértárként használható: a *D-Link DNS-323/313* azon túl, hogy az iTunes is le tudja játszani a rajta lévő zenéket, a letöltést is átvesszi a PC-től. Utóbbi a BitTorrent hálózat (seedel is!) mellett a Gnutella, eDonkey és eMule hálózatokat is használni tudja. Mint ahogyan egyre többen állnak át a nyílt, de legalább Linux alapú firmware-ekre, úgy fog egyre több ezekhez hasonló funkció megjelenni a többi gyártónál is.

Az egyszerű kezelhetőség a legfőbb szempont, amelyet az új otthoni routerek tervezésekor figyelembe vesznek.

Amíg ezek az egyszerű, sokoldalú készülékek népszerűvé válnak, addig is kívánjuk minden kedves olvasónknak a Router iskolában tanultak sikeres alkalmazását!