Bevezetés a DHCP kiszolgáló használatába

TCP/IP alapú hálózatok központi beállítása és karbantartása – avagy ami unalmas, az a számítógép dolga.

Egyszer volt, hol nem volt, volt egyszer egy rendszergazda. Ennek a rendszergazdának egy kisebb helyi hálózatot kellett felügyelnie, főként olyan ügyfélgépekkel, amik azt a bizonyos másik operációs rendszert futtatták. Bár az a másik operációs rendszer felettébb megbízható, egyszer-egyszer mégis előfordult, hogy a türelmetlen felhasználók heves kattintgatásai és az internetről beáramló mérhetetlen mennyiségű kártevő miatt újra kellett telepíteni egy gépet.

Ilyenkor hősünk kezében egy telepítőlemezzel nekiesett a gépnek, és úgy másfél-két óra alatt varázsolt rá egy, a szűz hó érintetlenségének jeleivel büszkélkedő rendszert irodai csomaggal, és néhány fontos alkalmazással. A telepítés folyamata alapvetően nem kifejezetten szórakoztató, jópár szál cigaretta és nem kevesebb csésze kávé is elfogy egy ilyen művelet során. Viszont remek alkalom ez az alkalmazott módszer előnyeinek és hátrányainak mérlegeléséhez.

Történetünk rendszergazdája mérnök lévén, azt latolgatta, hogy vajon a telepítésnek melyik az a része, ami miatt feltétlenül az ő személyes beavatkozása szükséges. Magáról a rendszerről és az alkalmazásokról készíthető egy kép, ami egy írható ***DVD***-n pont elfér. Ennek felmásolását akár még a felhasználókra is rá lehetne bízni – na jó, azért ne essünk túlzásokba. Viszont ott van a hálózat beállításának kérdése, amit kénytelen-kelletlen, kézzel kell elvégezni.

Vagy mégsem? Milyen szép lenne a világ, ha az összes ***TCP/IP*** beállítás, címestül, átjáróstul, ***DNS***-kiszolgálóstul egy helyen, a sokat próbált ***Linux*** kiszolgálón volna, és az ügyfeleknek csak annyit kellene tudniuk, hogy ezeket az információkat le kell kérdezni. Hiszen ez már másnak is eszébe jutott! S ekkor hősünk fél óra alatt feltelepített egy ***DHCP*** kiszolgálót, és azóta élvezi a lustálkodás, valamint a ***bzflag*** édes örömeit.

A tanmese szereplői természetesen a képzelet szüleményei, ennek ellenére mindenkivel előfordulhat, hogy a munkahelyén azért rágják a fülét, mert a vállalati laptopnak látnia kellene az Internetet három telephelyen is, és senki sem akarja (vagy nem tudja) beállítani minden egyes alkalommal, hogy a helyi hálózaton most épp ki az átjáró. Erre a problémára jelent hosszú távú megoldást a ***DHCP***. Nézzük meg közelebbről, hogy mi is ez, és hogyan kell beállítani.

A ***DHCP*** a ***Dynamic Host Configuration Protocol***, azaz a dinamikus állomás beállító protokoll rövidítése. Az ***IETF (Internet Engineering Task Force)*** fejlesztette ki azzal a céllal, hogy egy nagyobb ***IP*** hálózat gépei egy központi helyről kérdezhessék le beállításaikat, ezáltal megkönnyítve a hálózat felügyeletét. A valamivel nagyobb múltra visszatekintő ***BOOTP***-vel visszafelé kompatíbilis, ám sok tekintetben tágabb lehetőségeket biztosít.

Az ***ISC (Internet Systems Consortium)*** által kiadott ***DHCP*** kiszolgáló, valamint ügyfél a jelenleg leginkább támogatott megvalósítás, ezért érdemes ennek a használatában elmélyedni. Kedvenc terjesztésünk, a ***Debian Linux*** csomagkezelőjében, a ***dselect***-ben kalandozva látható, hogy az ***ISC*** kiszolgálójának két változata is elérhető előre fordított csomag formájában. Az egyik a ***dhcp***, a másik a ***dhcp3-server*** nevet viseli. Előbbi a 2-es, míg utóbbi értelemszerűen a 3-as sorozatból származik.

A 3-as változatszámú ***DHCP*** kiszolgáló, illetve a hozzá tartozó ügyfél még tesztelés alatt áll, és a 2-es is igen szép szolgáltatás-választékkal áll rendelkezésünkre, ezért érdemes inkább ezt felrakni. Természetesen a forrásból történő telepítés sem nehéz, mindössze az ***ftp://ftp.isc.org/isc/dhcp/*** címről kell beszerezni a legújabb csomagot, kitömöríteni, majd `./configure && make && make install`. Ez tényleg ennyire egyszerű!

A ***Debian*** csomagleírása szerint a ***DHCP 2***-höz elég egy 2.0.32-es, a 3-ashoz már szükség van egy 2.2-es sorozatú Linux rendszermagra. Ez nem túl erős rendszerkövetelmény, amire azonban feltétlenül oda kell figyelni, az az, hogy a `CONFIG_PACKET` és a `CONFIG_FILTER` be legyen állítva. Ugyanakkor bizonyos 2.1-es sorozatú magokkal még így is gondok lehetnek, emiatt érdemes inkább legalább egy 2.4-es sorozatból származót használni.

Milyen gond származhat a régebbi kernelek használatából? A ***Windows*** korai változatainál, többek között ***Windows 95***-ös ügyfelek esetén, a helyes működéshez a ***DHCP*** kiszolgálónak képesnek kell lennie ***IP*** csomagot küldeni a ***255.255.255.255*** címre. Sajnálatos módon a ***Linux*** az ilyen célállomású IP csomagokat a helyi hálózat üzenetszórási címére irányítja. Így egy közönséges C típusú magánhálózatnál a ***255.255.255.255***-öt átírja ***192.168.0.255***-re.

Bizonyos esetekben ez a probléma megkerülhető. A legegyszerűbb, ha a rendszermag útvonalválasztó táblájába felveszünk egy sort, ami a ***255.255.255.255***-ös állomást a megfelelő hálózati csatolóhoz párosítja:

```
route add -host 255.255.255.255 dev eth0
```

Ez azonban nem mindig jelent gyógyírt a fenti gondra, mert egyes kernel változatok hibaüzenettel utasítják el a megadott *IP* állomásként történő bejegyzését. Még mindig becsaphatjuk a rendszermagot, ha a */etc/hosts* állományba felvesszük nevesítve a címet:

```
# /etc/hosts
255.255.255.255    mindenki
```

Ezután próbáljuk meg kiadni a következő parancsot:

```
route add -host mindenki dev eth0
```

Ha még ez sem válna be, próbálkozzunk az alábbival:

```
route add -net 255.255.255.0 dev eth0
```

Ezúton szeretnék elnézést kérni a – remélhetőleg – tőlem teljesen szokatlan ködös fogalmazásért. A fenti trükköket az *ISC DHCP* kiszolgálójának leírásában olvastam és sem ott, sem más dokumentációban nem találtam arra vonatkozó információt, hogy mikor melyik próbálkozás jelenti a megoldást. Ezért én azt javaslom, hogy mindenki, aki *DHCP* kiszolgáló telepítésére adja a fejét, és még nem frissített legalább 2.4-es változatú kernelre, előbb azt tegye meg.
Ha tűzfallal is rendelkezik leendő linuxos *DHCP* kiszolgálónk, néhány új szempontot figyelembe kell vennünk. Bármely *IP* címről, a 68-as *UDP* kapuról érkező üzenetszórt csomagokat át kell engedni, ha azok a 67-es *UDP* kapura érkeznek. Továbbá az ellentétes irányú kommunikációt hasonlóan engedélyezni kell. Egy tipikus *iptables/netfilter* beállítás lehet az alábbi:

```
iptables -I INPUT 1 -m state –state
➥ESTABLISHED,RELATED -j ACCEPT
iptables -I INPUT 2 -i eth1 -p udp –dport 67 -j
➥ACCEPT
iptables -I OUTPUT 1 -m state –state ESTABLISHED,
➥RELATED -j ACCEPT
```

A fenti példához szükség van az `ip_conntrack` modulra. Ez a három szabály azt eredményezi, hogy a tűzfal az eth1 csatolón, a 67-es *UDP* kapura érkező új kapcsolatokat fogadja el, valamint a kapcsolatkövetésnek köszönhetően az így kiépített kommunikációt engedélyezi. Itt a megszorítást a hálózati csatoló meghatározása jelentette. Fontos, hogy ilyenkor *IP* címre nem lehet szűrni, hiszen az ügyfelek pont azért kapcsolódnak a kiszolgálóhoz!
Nincs más hátra, mint a *DHCP* démon beállító-állományának szerkesztése. Alapértelmezésben */etc/dhcpd.conf* néven találjuk ezt a fájlt. Egy olyan szerver esetében, amelynek feladata mindössze egyetlen alhálózat kiszolgálása, nincs nehéz dolgunk. Tekintsük az alábbi beállítást, és mielőtt továbblépnénk, töprengjünk el azon, hogy mit eredményezhet.

```
# dhcpd.conf
#
option domain-name “lustakeavilag.hu”;
option domain-name-servers dns1, 192.168.0.10;

option subnet-mask 255.255.255.0;
option broadcast-address 192.168.0.255;
option routers szerver;

default-lease-time 86400; # egy nap
max-lease-time 604800;    # egy het

subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.100 192.168.0.199;
}
```

A közönséges szöveges állományban szokás szerint a megjegyzések #-től sorvégéig tartanak. Minden beállítást tartalmazó sor végén pontosvessző áll. Előbb a globális beállítások következnek. Ilyen a `domain-name` paraméter, amely a tartománynevet határozza meg. Egy új ügyfél a *DHCP* kérésre kapott válaszban ezt a tartománynevet fogja látni, kivéve, ha ezt alább felül nem definiáljuk.
A következő `domain-name-servers` paraméterben, amely a *DNS* kiszolgálókat sorolja fel, azt a furcsaságot láthatjuk, hogy épp a névfeloldást végző számítógépre névvel hivatkoztunk. Ha a *DHCP* szerver képes feloldani ezt a nevet, akkor semmi gond, az ügyfélnek már a hozzá tartozó *IP* címet fogja közvetíteni. Ez mindössze a rendszergazdának egy kényelmi szempont, a teljesítményre semmilyen hatással nincs.
A `subnet-mask` az alhálózati maszkot, a `broadcast-address` az üzenetszórás címét adja meg. Az elsőre talán furcsának talált `routers` az átjárókat határozza meg. Természetesen itt is használhatunk neveket, ha azokat a *DHCP* szerver képes feloldani. Érdemes megfigyelni, hogy az eddigi beállításokat mindig egy `option` paraméter előzte meg. Ezek fontos, de a *DHCP* protokoll szerint elhagyható paraméterek. Az option nélkül állók azonban nem.
Ilyen a bérleti idők beállítására szolgáló `default-lease-time` és `max-lease-time`. A bérleti idő azt jelenti, hogy a *DHCP* által szolgáltatott információ bizonyos idő letelte után elévül. Ekkor az ügyfél felelőssége, hogy újra kérje ezeket az információkat. Ugyanakkor az ügyfél a *DHCP* kérésben meghatározhat egy kívánt bérleti időt, ameddig nem kell újabb kérést kiadnia. Ha nem fogalmaz meg ilyen kívánalmat, az alapértelmezett (default) bérletet kapja, ellenkező esetben a felső határig (max) a kiszolgáló megpróbálja kielégíteni a kérést.
Ez a két paraméter másodpercekben van kifejezve. A 86400 másodperc egy napot, a 604800 másodperc pedig egy hetet jelent. Ennyi ideig az ügyfél szabadon használhatja a kapott *IP* címet. Természetesen még a bérlet lejárta előtt bármikor lehetősége van azt megújítani. Ezt *Microsoft Windows 2000* és afölött parancssorban az alábbiakkal lehet elérni:

```
ipconfig /release
ipconfig /renew
```

A `release` elengedi a jelenlegi címet, a `renew` pedig megújítja. A `/all` kapcsolóval pedig a linuxos `ifconfig`-hoz hasonló kimenetet láthatunk a használatban lévő hálózati csatolókról. A példa *dhcpd.conf* végén egy alhálózat meghatározása lát-

ható. A hálózat neve, illetve az alhálózati maszk által azonosított alhálózatban a `range` paraméter segítségével lehet meghatározni azt a tartományt, amelyből az újonnan érkező ügyfeleknek *IP* címet lehet osztani. Egyszerűen egy alsó, illetve egy felső határt szab a felhasználható címeknek.
A fenti beállításokkal már elindulhat a kiszolgáló. Minden ügyfél tudni fogja, hogy melyik tartományba tartozik, kap egy egyedi *IP*-címet, és ha a többi paraméter is helyes, az Internetes szupersztráda által nyújtott korlátlan lehetőségekkel is élhet. Ha mindent jól csináltunk, *IP*-cím ütközéstől sem kell tartanunk a helyi hálózaton.
Ha figyelemmel kísérjük a rendszernaplót, láthatjuk, ahogy az ügyfelek egymás után fordulnak kéréssel a *DHCP* kiszolgálóhoz, és címet is kapnak szépen sorban. Azonban egy ilyen elrendezés esetén a dinamikus IP-cím kiosztás miatt problémás lehet behatárolni, hogy egy adott IP melyik géphez tartozik. Tegyük fel, hogy az egyik ügyfél egy hirtelen ötlettől vezérelve elkezdi *ICMP* üzenetekkel elárasztani a hálózatot. Ahhoz, hogy megtaláljuk, melyik gép volt az, a naplóhoz kell fordulnunk minden esetben.
További gondot jelenthet, hogy ezek után bárki kaphat *IP*-címet, és azonnal látja az egész hálózatot. Egy laptoppal rendelkező betolakodónak csak egy végpontot kell találnia, és máris osztozhat a hálózati erőforrásokon. A *DHCP* protokoll használatakor a hitelesítés egyetlen módja a hálózati kártyák fizikai címének figyelembe vétele. Ez az úgynevezett *MAC*-cím elvileg teljesen egyedi az egész világon és nem lehet két olyan hálózati eszköz, aminek megegyezik a *MAC*-címe.
Fűzzük hozzá meglévő ***dhcpd.conf***-unkhoz az alábbi sorokat:

```
group {
    use-host-decl-names on;
    host gizi {
        hardware ethernet 01:02:03:04:05:06;
        fixed-address 192.168.0.10;
    }
    host bela {
        hardware ethernet 0a:0b:0c:0d:0e:0f;
        fixed-address 192.168.0.20;
    }
}
```

A `group` csupán azt a célt szolgálja, hogy logikai egységbe foglalja a meghatározásokat. Így a paraméterek az összes, a csoportban szereplő elemre érvényesek lesznek. Például a `use-host-decl-names` egy olyan paraméter, amely előírja, hogy az azonosított számítógépek *DHCP* kérésére a számítógép nevét is el kell küldeni a válaszban. Így az ügyfeleknek a saját nevüket sem kell tudniuk, ezt az információt is megkapják a *DHCP* kiszolgálótól.
A `host` egy azonosítható állomást határoz meg. A `gizi` nevűnek a *MAC*-címe `01:02:03:04:05:06`, és a `192.168.0.10` *IP*-cím tartozik hozzá. Ez azt jelenti, hogy a `subnet` meghatározástól függetlenül, ha egy adott fizikai címmel rendelkező hálózati eszközről érkezik a kérés, a megadott IP-címet kell kiosztani. Ezáltal bár csak a szerveren tárolódik az összes hálózati beállítás, a két ügyfél állandó címmel rendelkezik, így könnyebb őket nyomon követni. Továbbá senki más nem bitorolhatja a megadott címeket.

Nagyon fontos, hogy a `subnet`-ben meghatározott tartomány ne érintse a `host`-okban foglaltakat. Ellenkező esetben előfordulhat, hogy egy ismeretlen *MAC*-című gép elfoglalja egy ismert *IP*-jét! Ezzel a módszerrel tehát elérhető, hogy minden ismert számítógép előre megadott, állandó IP címmel rendelkezzen. Adott esetben a `subnet` meghatározástól meg is válhatunk ezek után, de tudnunk kell, hogy ekkor a *DHCP* szerver visszautasít minden ismeretlen kérést.
Ezt figyelembe kell vennünk, ha hálózati kártyát cserélünk valamelyik ügyfélnél, vagy új számítógép érkezik a céghez. Nem mehetünk el szó nélkül a ***Microsoft Networks*** hálózat mellett sem. A ***Netbios*** nevek feloldásához érdemes a tartományvezérlőt ***WINS*** kiszolgálóvá tenni. Ez egy ***Samba*** kiszolgáló esetén egyszerűen az alábbi paraméter segítségével történik:

```
wins support = yes
```

Ezáltal a hálózat tallózása sokkal gyorsabb lesz, feltéve, hogy az ügyfelek tudják, kihez kell fordulni a ***Netbios*** nevekért. Ezt az információt is könnyen közzétehetjük új *DHCP* kiszolgálónkkal, az alábbi módon:

```
option netbios-name-servers 192.168.0.25;
```

A fenti sort a ***dhcpd.conf*** globális beállításai között kell elhelyezni, és egy újraindítás után az ügyfelek a következő *DHCP* kéréskor már a *WINS* kiszolgálóról is értesülni fognak.
Apropó, újraindítás. Jó volna, ha amikor ***dhcpd.conf***-hoz hozzáadunk egy új `host` bejegyzést, nem kellene újraindítani a démont. Erről hosszas viták folytak több levelezőlistán, és sajnos egyelőre nem várható változás ezzel kapcsolatban. Miután külső forrást sem lehet megjelölni a `host` meghatározásoknak, be kell érnünk azzal, hogy minden módosítás után újra kell indítani a `dhcpd`-t.
Ez a rövid leírás mindössze ízelítőül szolgált a *DHCP* lehetőségeinek bemutatására. Az interneten azonban számos jól használható leírás található, ha ez a cikk, illetve a kézikönyv lapok (`man dhcpd`, `man dhcpd.conf`) kevésnek bizonyulnának. Sok sikert a beállításokhoz és kellemes lustálkodást mindenkinek!

Fülöp Balázs (admin@guardware.com)
Imádja a Túró Rudit, a Debian Linuxot és a teheneket. Kedvenc írója Slawomir Mrożek. Leginkább a számítógépes hálózatok biztonsága érdekli. A BME VIK műszaki informatikus szak hallgatója.

KAPCSOLÓDÓ CÍMEK

- http://rfc.net/rfc2131.html
  A DHCP protokoll hivatalos leírása
- http://www.dhcp-handbook.com/dhcp_faq.html
  DHCP gyakran ismételt kérdések
- http://www.isc.org/index.pl?/sw/dhcp/
  Az ISC DHCP honlapja, számos remek linkkel