A névkiszolgálókról

A névkiszolgálók az Internet (egyik) alapkövének számítanak, jó kiszolgálóprogramot találni azonban nem egyszerű. Vizsgáljuk meg, hogy pontosan mi a DNS szerepe, és milyen kiszolgálóprogramok közül választhatunk, amelyek megfelelnek a követelményeknek.

A névkiszolgálóknak alapvetően két dolgot kell tudniuk: IP- (hálózati) címekhez nevet és a nevekhez hálózati címeket rendelniük. Az emberek könnyebben jegyezhetik meg neveket, mint számsorozatokat, ezért az Interneten is nevek alapján tájékozódunk. A számítógépek viszont a neveket nem ismerik, csak a számokat, amelyek a kívánt célállomáshoz irányítják ügyfélgépek kéréseit. Ezt folyamatot, azaz a nevek IP-címekre való leképezését ***névfeloldásnak*** nevezik. Nagyon röviden ebből áll a névkiszolgálók szerepe. Tekintsük át, miként osztályozhatjuk a kiszolgálókat működésük szerint:

Gyorstár: az ügyfelek számára a már feloldott nevekhez tartozó IP-számokat tárolja, hogy a névfeloldás folyamata gyorsabb legyen.

Rekurzív névkiszolgáló: nem rendelkezik a hiteles információval, azaz nem ennél a kiszolgálónál találhatók meg az adatok a tartományról. Ha gyorstárában az adat fellelhető, akkor visszaadja. Ellenkező esetben egy másik kiszolgáló felé irányít, amely meg tudja mondani, hová kell fordulni a válaszért, de legalábbis közelebb jutunk hozzá.

Hiteles (authoriative) névkiszolgáló: az a névkiszolgáló, amely az adott zónát – a keresett tartomány is ebben található – karbantartja, tehát nála van az elsődleges adat. Ha az a cím, amit az ügyfél keres, még egyetlen gyorstárban sem található meg, a keresés végül ide jut el.
Egy névfeloldás – például ➲ http://www.linux.hu cím keresésénél – a következőképpen néz(het) ki:

- Az ügyfél az előtte lévő gyorstárat lekérdezi, hogy a névhez tartozó cím elérhető-e.
- Ha a gyorstár nem találta meg az adatot, az első rekurzív névkiszolgálóig jut el.
- Ez a névkiszolgáló, ha az adat nincs a birtokában, a központi (root) kiszolgálók címét adja meg.
- A kérés az egyik központi kiszolgálóhoz jut, ahonnan visszajön, hogy honnan szerezhető adat a .hu tartományhoz.
- Az újabb kiszolgáló nem tud felvilágosítást adni a linux.hu tartományról, azonban meg tudja mondani, hogy ki a tartomány felelőse.
- A linux.hu-ért (is) felelős kiszolgáló meg tudja mondani, hogy hol található meg a ➲ www.linux.hu.
- A gyorstár az adatot visszaadja az ügyfélnek.
- Az ügyfél eljut a keresett helyre.

Bár a folyamat hosszúnak tűnhet, a mindennapi életben tapasztalhatjuk, hogy nem ennyire rossz a helyzet, hiszen a weboldalak gyorsan bejönnek, a levelek sebesen letöltődnek. Mindez nagy mértékben annak köszönhető, hogy csaknem minden szolgáltató alkalmaz gyorstárakat, ezzel is csökkentve a hálózati terhelést és gyorsítva a forgalmat. Mint mindennek, ennek is megvan a maga rossz oldala. Elég csak arra gondolni, hogy ha levélkiszolgálónkon pont IP-címet váltunk, egy napig biztosan akadozva érkeznek a levelek, mert – amíg a gyorstáruk nem frissül – a nem a saját zónánkat karbantartó szolgáltatók mögött lévő ügyfelek nem fognak minket elérni.
A névkiszolgálóknak van még egy különleges fajtája. Sokan vannak, akik szolgáltatásokat szeretnének futtatni a gépükön, azonban állandó IP-címmel nem rendelkeznek, ami viszont szükséges hozzá. Számukra a dinamikus névkiszolgálók jelenthetnek megoldást. A használathoz szükség van egy többé-kevésbé állandó vonalra: ez azt jelenti, ajánlott, hogy a dinamikusan kiosztott IP-cím csak 1-2 naponta változzon. A dinamikus névkiszolgálók ugyanis nagyon kis időközönként frissítik az adatokat, például négyóránként. Ekkor az összes nagyobb névkiszolgáló is rá lesz kényszerítve, hogy ha a tárolt adat érvényessége már lejárt a gyorstárban, a hiteles kiszolgálót megkérdezze a pillanatnyi IP-címről. A cím tárolása a következőképpen történik: a változó című gépeken egy ügyfélprogram fut, mely jelenti, hogy az általunk használni kívánt névhez jelenleg milyen IP tartozik. Ilyen nemzetközi kiszolgáló a DynDNS.org is. Akár saját magunk is kialakíthatunk ilyen szolgáltatásokat. Hogy mi kell hozzá? A BIND, egy `ddt-server` elnevezésű kiszolgálóprogram és PostgreSQL adatbázis. Az ügyfeleknek pedig a `ddt-client` programot kell futtatniuk, ha az adatokat át akarják adni a kiszolgálónak. A `ddt-server` adatbázisban tárolja a felhasználók adatait és jelenlegi címüket, és ebből frissíti fel a BIND beállítófájljait. Debian alatt e környezet kialakításához minden csomag megtalálható.
A kiszolgálókat azonban – ha egy adott tartományra nézve vizsgáljuk a szerepüket – másként is osztályozhatjuk:

Elsődleges névkiszolgáló: egy adott tartományért felel, a tartományon belüli IP-cím-név hozzárendelés első számú meghatározója.

Másodlagos névkiszolgáló: a másodlagos névkiszolgáló feladata, hogy az elsődleges kiesése esetén is mindenki lekérdezhesse a tartomány(ok) gépeihez tartozó címeket, illetve neveket. Csak átveszi az adatokat az elsődleges kiszolgálóról, a tartományokat beállító fájlokban semmilyen változtatás nem kerül érvényesítésre, tehát semmiféleképpen nem térhet el az elsődleges névkiszolgálótól.

A névkiszolgálás másik fontos tulajdonsága, hogy a hálózaton lévő számítógépeket feladat szerint is megkülönbözteti. Közülük minden tartománynak kötelező bizonyos bejegyzésekkel (rekordokkal) rendelkeznie – a zónákat ilyen rekordok alkotják. Nézzük át a legfontosabbakat!

- A rekord – egy hálózati számítógép és a nevéhez rendelt IP-cím. Ilyen A rekord például a www.lsc.hu vagy a mail.linux.hu hálózati név is a hozzájuk tartozó IP-számmal együtt.
- PTR rekord – a reverz rekord, amely azt mutatja meg, hogy egy hálózati címhez mely nevek tartoznak. Sok szolgáltatás gyakran visszaellenőrzi, hogy ez a név megegyezik-e azzal, amelyet a kapcsolódást kezdeményező gép IP-címéhez viszonyítva a kapcsolódó alkalmazás mondott, vagyis ha én a `192.168.0.12`-es IP-címről jövök és azt állítom magamról, hogy a gép neve ***tigris.intranet***, de visszaellenőrzéskor kiderül, hogy a `192.168.0.12`-es címhez a ***malacka.intrane***t név tartozik, a kiszolgálóprogram megtagadhatja a szolgáltatást, feljegyezheti ezt a naplóba stb.
- NS – a hozzárendelt zóna (tartomány) névkiszolgálójára mutat.
- MX – egy adott tartománynak mi a levélkiszolgálója, hova kell küldeni a leveleket. Számok állnak mellette, melyek a preferenciát jelzik. Érdekesség, hogy ebben az esetben minél kisebb a szám, annál nagyobb elsőbbséget élvez a hozzá tartozó számítógép. Ha tehát a ***mailszerver.hu*** tartományra levél érkezik, akkor a levelek először a 0-s MX rekorddal rendelkező ***mx.lsc.hu*** számítógép felé irányulnak. Ha a gépet vagy a rajta futó levélkiszolgálót nem lehet elérni, az ügyfelek a 10-es MX rekorddal rendelkező ***pooh.lsc.hu***-nak próbálják a leveleket eljuttatni.
- CNAME – „becenév”. A szakirodalom a fenti megoldás helyett inkább több A rekord használatát javasolja egy IP-címre – tehát inkább mutasson A rekorddal ugyanarra az IP-címre a ***www.lsc.hu*** és a ***www.mailszerver.hu***, ahelyett, hogy hivatalosan az egyik kapja meg az IP-címet, a másik pedig csak hivatkozik a másik nevére, hogy így oldódjon fel az IP-cím.

A programválasztékról

BIND

Ez a kiszolgáló hosszú múltra tekinthet vissza és rossz a megítélése. Mai napig az alapértelmezett névkiszolgáló a telepítéseknél, de ehhez a nagy vetélytárs, a `djbdns` felhasználói szerződésének is köze van. A BIND legújabb, 9-es változatát az alapoktól újraírták és nem foltozták, mint tették azt a 4-es változatból kiinduló 8-as esetében. A beállítása kicsit nehézkes és nagyon kényes a formai dolgokra. A Sendmail után talán ebben lehet a legtöbb biztonsági hibát találni. A 9-es változat sokáig hibátlannak tűnt, a későbbiek folyamán azonban ebben is „szeplőkre” bukkantak, bár közel sem olyan súlyosra, mint az előző változatokban. Ezek ellenére nagyszámú szabványt támogat és törekszik a biztonságra, jó példa erre a hitelesített DNS-válaszok bevezetésének próbája is. Ebben a kiépítésben a DNS-kiszolgálók ugyanúgy egy tanúsítvánnyal rendelkeznének, mint a webkiszolgálók, ily módon biztosítva, hogy a válasz jó. Biztonsági hibái mellett memóriahasználata sem a legkiemelkedőbb, de ezen is próbálnak javítani, eredmény egyelőre nem annyira látszik, viszont biztató jelek is megfigyelhetők a fejlődésében. Teljes körű megoldást nyújt a gyorstártól a hiteles (authoritative) névkiszolgálásig, több grafikus és weben keresztül használható beállítóprogram is elérhető hozzá. DNS & BIND címmel könyvet is olvashatunk a témában a
➲ http://www.isc.org/products/BIND/ címen.

DJBDNS

A Qmail levélkiszolgáló írója által írt névkiszolgáló, amelyet a szerző – szerénységéhez illően – saját magáról nevezett el. A BIND-tól alapjaiban eltér, kétségbe vonva a másik programban alkalmazott módszereket, és követendő útnak a szabványok – amelyeket nagyrészt valóban az ISC, a BIND-ot fejlesztőcég alkalmazottai írtak – elvetését tartja. A program maga biztonságos, az általa használt memória mennyisége állítható, a beállítófájl formátuma egyszerűbb a BIND-énál. Sajnálatos módon a fejlesztő senki véleményét nem hajlandó meghallgatni – ez a ***véleményem*** – és elég kellemetlen a stílusa. Az alkalmazás maga azonban kitűnő, bár van, aki felhasználási szerződési okok miatt nem használja. Nyílt, de bizonyos értelemben nem szabad program. Többen is írtak hozzá bővítményeket, amelyek hivatalosan nem kerülhetnek bele az alkalmazásba, illetve a módosításokkal együtt nem is terjeszthetők – a fentebb említett fejlesztői hozzáállás és felhasználási szerződésbeli gondok miatt. Teljes körű megoldást nyújt a gyorstártól a hivatalos névkiszolgálásig. Webalapú beállítófelület és számos egyéb hasznos eszköz is elérhető hozzá.
➲ http://www.djbdns.org

MaraDNS

Fejlesztésének kezdete a BIND gyengélkedése és a `djbdns` felhasználási szerződés gondjai miatt kezdődött el. Beállítóállománya kísértetiesen hasonlít a `djbdns`-ére. Az egyetlen érv, amit fel lehet hozni ellene, az, hogy még nem sokan használják, így nem létezik a széles körű használatból adódó kipróbálás és hibakeresés előnye. Megbízhatóan működik és teljes körű szolgáltatást képes nyújtani, továbbá a felhasználási szerződéseket is figyelembe vevő felhasználókat is maradéktalanul kielégíti.
➲ http://www.nsmarad.org

Webalapú és grafikus beállítóprogramok

A Webmin webalapú beállítófelülettel a BIND 8-as változatához rendelkezik.
➲ http://www.webmin.com
A MyWebDNS a BIND beállításához használható webes eszköz. Előnye – szerintem – az, hogy a beállításokat MySQL-ben tartja, így ha a teljes adatbázist biztonsági másolatként használt gépre replikáljuk, egy esetlegesen fellépő hiba esetén az eredeti állapot sokkal könnyebben visszaállítható. Az Apache kiszolgálón kívül szükséges telepíteni a PHP-t és a MySQL-t is.
➲ http://mywebdns.sourceforge.net/
Az ANK_djbdns a `bjdbdns`-hez készített webalapú beállító eszköz. Ennek is előnyére válik, hogy a beállításokat adatbázisban tartja. Apache-n és MySQL-en kívül Apache-perl szükséges hozzá.
➲ http://www.nobol.com.br/dns/index.html

Remélem, írásom által kicsit jobban kiismerhetővé vált az Internet, és mindenki ki tudja választani az általa legjobbnak tartott alkalmazást. Én személy szerint a djbdns-re esküszöm, bár vannak vele kapcsolatban – nem a felhasználási szerződéssel összefüggő – kifogásaim. Jelenleg a MaraDNS-t próbálom ki, hogy mennyire bírja a terhelést. Amint érdemlegeset tudok róla nyilatkozni, ígérem, megteszem.

Deim Ágoston (ago@lsc.hu)
Kedveli a sört, szereti a futást és imádja Szabó Lőrinc verseit. Nem hisz vakon egyik rendszerben sem. Vonzódik a BSD-hez is. Tagja az LME-nek és a MBE-nek. Mottója: a gép nem lehet fontosabb az embernél.