XV. FIATAL MŰSZAKIAK TUDOMÁNYOS ÜLÉSSZAKA

Kolozsvár, 2010. március 25-26.

AZ INTERNET EGYIK ALAPPILLÉRE - A DNS MŰKÖDÉSE

FRIED Zoltán

Abstract

The DNS servers invisible carry out their job in order to ensure unhindered access to Internet services, fault-tolerant, and last but not least, be more humane. Operation of this service is often a mystery even for system administrators.

Key words:

DNS, internet

Összefoglalás

A DNS szerverek láthatatlanul végzik a dolgukat annak érdekében, hogy az internetes szolgáltatások elérhetősége akadálymentes, hibatűrő, és nem utolsósorban emberibb lehessen. Ezen szolgáltatás működése nagyon sok informatikus számára is gyakran rejtély.

Kulcsszavak:

DNS, internet

1. Bevezetés

A DNS (Domain Name System) szolgáltatásra azért van szükség, mert az emberek nem szeretnek számok sorozatával (ipv4/ipv6) hivatkozni például egy weboldal megnézéséhez, vagy bármilyen más az interneten keresztül elérhető erőforrás használatához. Az internet működtetéséhez elengedhetetlen a használata, mert a hálózati alkalmazások, szolgáltatásokat futtató számítógépeket csak az IP cím ismeretében lehet beazonosítani. Hovatovább az internet gyakorlatilag „megszűnne létezni” a DNS szerverek leállítása esetén. Hétköznapi példával élve erre a funkcióra leginkább a telefonkönyv vagy a mobiltelefon névjegyzéke hasonlít.

2. DNS szerverek feladata, felépítése

Elsősorban az IP címeknek és a hozzájuk rendelt domainnevek oda-vissza konvertálását végzik. A lényege egy hierarchikus körzetalapú névkiosztási séma, és az azt megvalósító szintén hierarchikus osztott adatbázisrendszer kialakításában rejlik [1], [2].

A DNS rendszert 1983-ban Paul Mockapetris alakította ki, akkor az RFC 882 és az RFC 883 specifikáció írta le a felépítését és működését. Mára mindkét specifikációt újabb váltotta fel (RFC 1034 és RFC 1035), sok egyéb tulajdonsággal egészítették ki az új igényeknek megfelelően. Mivel a DNS rendszer nagyon stabil, és megbízható, egyre több funkciót integráltak bele. A legismertebb DNS szerver megvalósításokat a [3] szakirodalom tartalmazza. A DNS szerverek az 53-as porton alapvetően UDP protokollon kommunikálnak egymással, kivéve az AXFR szolgáltatástípust (4. fejezet), amely esetben a TCP protokoll a használatos.

2.1. A domainnevek felépítése

A domainnevek szerkezete fa struktúrájú. A fa leveleit címkéknek nevezzük. Egy domainnév címkék láncolatából áll. A címke karakterláncolat, csak az angol ABC betűit, számokat valamint kötőjelet tartalmazhat (a kötőjel nem lehet az utolsó karakter) [4]. A domaint alkotó címkéket egy-egy ponttal választjuk el egymástól. A domainnevet ponttal zárjuk le. A hétköznapi használatban ezt a pontot elhagyhatjuk. Egy hibátlan teljes domainnév – FQDN (Fully Qualified Domain Name) például a *www.wikipedia.com*. (az utolsó pont is a domainnévhez tartozik) [5].

A domainnév az öt alkotó összes ponttal együtt legfeljebb 255 karakterből állhat. A domainnevet mindig jobbról balra olvassuk, és ilyen sorrendben értelmezzük. Ez azt is jelenti, hogy minél inkább jobbra áll egy címke a domainnévben, annál feljebb áll a fastruktúrában. A domainnév jobb szélén álló pont választja el a címkét az első hierarchiai szinttől, a gyökértől (root) [15]. Ezt az első szintet Top Level Domain-nek (TLD) nevezik [5]. Ezeket a TLD-ket két nagy csoportra oszthatjuk: az általánosra mint például: com, gov, org, net, edu stb, és országcódokat tartalmazó csoportra mint például: hu, eu, en stb. (1. ábra)

A domainnév azon részét, amely a hierarchia második szintjén helyezkedik el second-level domainnak (SLD) hívjuk [5]. SLD például a wikipedia.com vagy a banki.hu. Az SLD a domainnév azon legkisebb része, amelyhez már IP cím rendelhető, és egyértelműen meghatározhat egy elérhető erőforrást az interneten.

1. ábra. Példa a domainnevek hierarchikus rendszerére [10]

2.2. A root szerverek

A root szerver a DNS névben a név végére tett pont jelképezi. A root szerverek arra hivatottak, hogy informáljanak arról, hogy a domainnevet melyik domain szervereknél kell keresni [6]. Jelenleg 13 root DNS szerver létezik a világon, amelyek más és más területen elhelyezkedő TLD-kért felelnek. Ezeket az ABC nagy betűivel nevezték el (A-M) [7], földrajzi elhelyezkedésüket az 2. ábra mutatja.

2.3. Autoritatív, primary és secondary névszerverek, glue rekord

A DNS szerverek ismertetése esetén tisztázni kell az autoritatív szerver fogalmát. Egy DNS szerver autoritatívnak „gondolja magát” egy domain zóna esetében, ha rendelkezik egy olyan adatbázissal a domain zónáról, amelyben a zóna tartalma megtalálható. Mások autoritatívnak „gondolják” – a DNS szerver autoritatív egy másik DNS szerver szempontjából – ha a hierarchiában felette álló szerverek (a feloldandó domainnév a név hierarchiában felette álló részeiért felelős szerverek) hozzá delegálnak

(irányítanak) egy domainre vonatkozó kérdéseket [8].

A névszolgáltatás folyamatosságának biztosítása érdekében egy domain regisztrálását csak akkor végzik el a hatóságok, ha minimum két különböző szervert adunk meg a regisztrálandó domainhez tartozó zóna autoritativ szervereként. Ezért megkülönböztetünk elsődleges (primary), és másodlagos (secondary) névszervereket. Természetesen egy zónához rendelhetünk 3, 4 vagy több névszervert is, ami természetesen lehet elsődleges és másodlagos is.

Glue (ragadvány) rekordnak nevezzük a zónától idegen "A" rekordot. Előfordul, hogy a delegált zóna egyik névszervere éppen a zónában van, de mégis szükség van arra, hogy egy vagy több szinttel feljebb a hierarchiához tartozó zónában is felvegyük a névszerver "A" rekordját, különben sosem fogjuk megtudni a névszerver IP címét. Tipikusan ezt használják a root szerverek esetében is.

2. ábra. DNS root szerverek fizikai elhelyezkedése a földön [7]

3. A DNS szerverek működése

Minden DNS szerver nyilvántart egy gyorsító tárat, cache-t a már korábban feloldott kérdések alapján a domainnév SOA rekordjának TTL mezőjében meghatározott ideig. A példa kedvéért keressük a `www.banki.hu` IP címét.

- Amennyiben a helyi cache-ben nincs a válasz, küldünk egy kérdést az egyik root DNS szervernek (amelyeknek a címét a telepítéskor a DNS szerver megkapja). Az egyszerűség kedvéért nevezzük ezt a szervert *root*-nak. A root szerverek IP címait a "." kérdésre adott válaszban kapjuk.

- A *root* szerver a saját nyilvántartása (zona file) alapján megmondja, hogy melyik TLD szerveret kérdezzünk meg. Hívjuk ezt a szerveret *tld*-nek. A TLD a példa esetében a "hu.", a kért névszerver legyen például az "ns.nic.hu."

- Megkérdezzük a *tld*-t a keresett domain SLD részéért felelős DNS szerver címéről. Hívjuk ezt a szerveret *sld*-nek. Az SLD a példa esetében a "banki.hu.", a kért névszerver legyen például az "donat.banki.hu."

- Megkérdezzük a *sld*-t az általunk érdekelt domain erőforrásrekord értékéről. Ha nem tudja a választ, akkor közli velünk hogy melyek azok a szerverek, amelyek a zónadefinícióért felelnek vagyis hol találjuk az autoritativ szervereket. Abban az esetben ha a választ tudja, közli az autoritativ szerverek neveit, valamint, hogy mennyi ideig javasolt azt megjegyeznünk (TTL).

4. A DNS szerverek szolgáltatástípusai

- Autoritativ DNS (lásd: 2.3. fejezet).
- Rekurzív vagy cache-elő DNS: Ez a szolgáltatás a DNS-fa rekurzív bejárását végzi a kliensek kérdési alapján, és az eredményeket cache-eli a későbbi gyorsabb kiszolgálás érdekében.
- Zónatranszfer (AXFR): Ez a szolgáltatás az autoritativ szerver egy zóna adatainak replikálását végzi az primary szerverről a secondary szerverek felé.
- Függvénykönyvtár: A DNS-sel kapcsolatos funkciók megvalósítását tartalmazza, hogy ne kelljen minden programban egyenként implementálni azokat.

A fenti típusok közül a DNS szerver zónáról zónára különbözőeket is szolgáltathat. A DNS szerver egy zónája szempontjából lehet primary, egy másik zónája szempontjából secondary. A kérdésekre adott válasz szempontjából megkülönböztethetünk megbízható és nem megbízható alkalmazásoktól (az alkalmazás IP címe alapján) származó kérdéseket is. Tegyük fel, hogy a DNS szerver mellett működik egy MTA is. Ennek az MTA-nak a DNS szerver kiszolgálja a rekurzív kérdéseket (lát), de például az internetről származó kérdésekre csak autoritativ válaszokat ad (láttat), a rekurzív kérdésekre nem válaszol.

5. A delegációs rendszer törékenysége

Az DNS rendszer hierarchikus felépítése egy kapcsolati rendszert képvisel. Ez egy tipikus megvalósítása a hálós elrendezésű rendszereknek. Egy-egy csomópontjának kiesése esetén is működőképes, így a szolgáltatás minősége egy cseppet sem romlik. Ez a helyzet mindaddig fennáll, amíg egy csomópontját át nem veszi egy rossz szándékú támadó. Amikor ez megtörténik, akkor sem az egész rendszer omlik össze, hanem csak azok a kliensek kapnak hamis IP címet, akik valamilyen módon kapcsolatba kerülnek a megtámadott csomóponttal. A szerverek száma viszonylag egyszerűen növelhető. A hálós, hierarchikus felépítés miatt AKÁR több száz DNS szerver biztonságosságán múlhat egy-egy domain helyes működése [9].

Irodalom

- [1] Andrew S. Tanenbaum: Számítógép-hálózatok, Panem Könykiadó Kft, 3. kiadás, 662.oldal, ISBN 963 545 213 6, 1999
- [2] Pásztor Miklós: Az internet DNS; <http://szabilinux.hu/dns/index.html>
- [3] Wikipédia: Comparison of DNS server software, 2009.05.04., http://en.wikipedia.org/wiki/Comparison_of_DNS_server_software
- [4] Network Working Group: Domain names - implementation and specification, RFC1035, 2.3.1. bekezdés, November 1987
- [5] Wikipédia: Domain Name System, 2009.05.31., http://hu.wikipedia.org/wiki/Domain_Name_System
- [6] Wikipédia: DNS root zone, 2009.04.09., http://en.wikipedia.org/wiki/DNS_root_zone
- [7] Wikipédia: Root nameserver, 2009.05.24, 02:36, http://en.wikipedia.org/wiki/Root_nameserver
- [8] Korn Andras: A DNS működése, 2007.09.21., https://unixlinux.tmit.bme.hu/A_DNS_működése
- [9] D. J. Bernstein: The 200 trusted .com servers, 2000 <http://cr.yp.to/dnscache/bugtraq/20000123114946-2072-qmail@cr-yp-to>
- [10] Andrew S. Tanenbaum: Számítógép-hálózatok, Panem Könykiadó Kft, 3. kiadás, 7.25. ábra, ISBN 963 545 213 6, 1999

Fried Zoltán, informatikus

Munkahely: UniCredit Leasing Kft., Magyarország, 1016 Budapest, Hegyalja út 7-13.

E-mail: kolozsvar@deirf.hu