Domain Name System

Markus Peuhkuri

2001-01-25

Luennon aiheet

- Miksi ja miten nykyinen nimipalvelu
- DNS-rakenne
- Piirinimien hankkiminen
- Nimipalvelu käytännössä

Kirjasta kappaleet

- The Evolution of Names and the Domain Name System, s. 76–84
- Domain Name Services, s. 412 – 420
- Domain Name Management, s. 593 – 594

Nimipalvelun tarve

- Verkko-osoitteet numeroita
  - kiinteä pituus tai maksimipituus
    - puhelinverkossa max. 15 numeroa
    - ATM (OSI NSAP) 20 oktettia (160 bittä)
    - IPv4 32 bittiä, IPv6 128 bittiä
  - optimoitu reititystä varteen
    $\Rightarrow$ sisältävät tietoa verkon rakenteesta
    $\Rightarrow$ muutos verkossa voi muuttaa osoitetta
  - eivät sisällä helposti muistettavaa logiikkaa
- Nimet ihmisille ja *myös sovelluksille* helpompia
  - looginen rakenne
  - nimi ei ole sidoksissa tiettyyn laitteeseen tietyssä verkossa
  - muistettava
  - oletuksia, esimerkiksi `www`, `ns`, `smtp`

Internetin nimipalvelun kehitys

1. Aluksi litteä nimiavaruus, nimissä ei mitään erityistä rakennetta tai logiikkaa
   - keskitetty lista Stanfordin tutkimuskeskuksessa
   - kopiointi kaikkiin koneisiin
   - koneiden määrän lisääntyessä
     (a) päivitystiheys kasvoi
     (b) tiedoston koko kasvoi
     (c) kopiointiin useammille koneille

⇒kuormitusongelma

2. IEN-116 nimipalvelu
   - sidoksissa verkon rakenteeseen: alkuperäisiin A-, B- ja C-luokan verkkoihin
   - ei skaalautunut suurelle organisaatiomäärälle

```
From: {\em postel@venera.isi.edu}
Subject: {\em re: IEN-116 nameserver}
Date: {\em Tue, 21 Jun 88 14:58:10 PDT }

It is my hope that all IEN-116 name servers will die soon.
(Actually, i wanted to believe they were all already dead.)
Long live the Domain Name System.

--jon.
```

3. Piirinimijärjestelmä (DNS: Domain Name System) [4, 5]
   - puurakenne
     ⇒ hierrarkinen, delegoitava
   - erossa verkon fyysisestä rakenteesta

Tiedostopohjainen nimipalvelu

- Alkuperinen `hosts.txt` edelleen tuettu, esimerkiksi UNIX™-järjestelmissä `/etc/hosts`
- Varalta nimipalvelun toimimattomuuden varalta
- Päivityksestä huolehdittava

  Joissakin järjestelmissä voidaan määrittää esimerkiksi `/etc/resolv.conf` tiedoston avulla, käytetäänkö ensisijaisesti `hosts`-tiedostoa vai nimipalvelua.

Nimipalvelun toiminta

Nimipalvelu on hajautettu tietokanta verkossa olevista koneista ja niiden nimistä.

1. Sovellusohjelma kysyy käyttöjärjestelmän selvittäjältä (resolver) nimeä vastaavaa IP-osoitetta
2. Selvittäjä kysyy asiaa siihen konfiguroidulta nimipalvelimelta, joita voi olla määritelty useita: mikäli ensimmäinen ei vastaa kysytään toiselta jne.
3. Nimipalvelin etsii tietoa ensin omasta käteismuistista ja tarvittaessa kysyy muilta nimipalvelimilta
4. Saatuaan kysytyn tiedon, palautetaan tieto kysyvälle koneelle, joka edelleen välittää sen sovellusohjelmalle

Nimiavaruuden rakenne

- Puumainen rakenne

1. Juuri "."
   - 13 kpl juuripalvelimia `a ...m.root-servers.net`
   - nimipalvelun käynnistystieto, mutta itseasiassa nimipalvelimelle riittää tietää yhdenkin toisen nimipalvelimen osoite.
2. Ylimmän tason piirinimet

   gTLD (Generic Top-Level Domain) yleiset piirinimet `com`, `org`...

   ccTLD (Country Code Top-Level Domain) ISO 3166 2-alpha -koodit (`fi`, `us`, `se`, `au`, `at`, `ee`...

3. Organisaatiotyyppi
   - käytössä joissain maissa esim. UK, Australia, Israel, Japani
   - `com` tai `co`, `edu` tai `ac` ...
4. Organisaation piirinimi
   - lyhenne (`hut`, `pjoy`)
   - tavaramerkki, aputoiminimi
   - virallinen nimi (`suomensarjakuvaseura`)
5. Organisaation alipiiri
   - organisaatioon tai maantieteelliseen jakoon perustuva
   - helpottaa suuren organisaation hallintaa
   - mahdollisesti useita tasoja
6. Laitetunniste
   - laitteen nimi (`hostname`)
   - piirissä yksikäsitteinen

- kukin osanimi enintään 63 merkkiä
- kaikki osat yhteensä (ml. välissä olevat pisteet) 255 merkkiä
- sallitut merkit A-Z, 0-9 ja "-"
- isot ja pienet kirjaimet samanarvoisia

Täydellinen piirinimi (FQDN: Fully Qualified Domain Name)

`laite(.aliorg)*.organisaatio(.tyyppi)?.TLD`

- Muodostuu laitenimestä ja piirinimestä

laitenimi	`www`
piirinimi	`tct.hut.fi`
FQDN	`www.tct.hut.fi`

- Luetaan oikealta vasemalle

  Aikoinaan (1980-luvun lopulla) Iso-Britanian JANET-verkossa FQDN kirjoitettiin päinvastaisessa järjestyksessä eli vasemalta oikealle. Joissain vanhoissa dokumentessa voi törmätä osoitteisiin, jotka ovat tyyppiä `user@uk.ac.example`; tämän voi muuttaa nykymuotoon kääntämällä järjestyksen `user@example.ac.uk`.

- Laitetta voidaan osoittaa
  - täydellisellä piirinimellä
  - laitenimellä mahdollisesti täydennettynä osittaisella piirinimellä, esimerkiksi TKK:n alueella `www.tct` vie koneelle `www.tct.hut.fi` kun taas `www` vie koneelle `www.hut.fi`, ellei kokeilla jonkun alipiirin alueella.

Yleiset päätason piirinimet (gTLD)

- Alunperin Internet Yhdysvaltain sisällä käytettäväksi
  $\Rightarrow$ USA-keskeiset määrittelyt

  .gov USA:n hallituksen organisaatiot (esim. `fbi.gov`, `whitehouse.gov`)

  .mil USA:n armeijan käyttöön (esim. `af.mil`)

  .edu pääasiassa yhdysvaltalaiset yliopistot (esim. `mit.edu`, `harward.edu`)

- Myöhemmin laajennettu kansainväliseksi [6]

.com kaupallisille yrityksille, nykyään erittäin laajaksi paisunut, noin 1,6 miljoonaa piiriä (esim. `sun.com`, `whitehouse.com`)

.net alunperin verkko-operaattoreille tarkoitettu, nykyään sisältää mitä tahansa (esim. `uusitupa.net`), noin 150.000

.org erilaisia organisaatioita, jotka eivät sovellu muihin ryhmiin – tai ole saaneet `.com`-piiriä (esim. `eff.org`, `debian.org`, `amnesty.org`, `metso.org`), noin 150.000

.int kansainvälisille, valtioiden välisillä sopimuksilla perustetuille organisaatioille (esim. `un.int`, `itu.int`, `nato.int`, 47 kappaletta)

- Uudet, 2001Q2 voimaan tulevat piirinimet,

.aero lentoyhtiöiden käyttöön – Societe Internationale de Telecommunications Aeronautiques SC, (SITA)

.biz yritystoimintaa varten – JVTeam, LLC

.coop yhteistoiminnallisille yrityksille – National Cooperative Business Association, (NCBA)

.info rajoittamton – Afilias, LLC

.museum museot – Museum Domain Management Association, (MDMA)

.name yksityishenklöille 3. tasolla `john.doe.name` – Global Name Registry, LTD

.pro "ammattilaiset", esim. `johnDoe.med.pro` – RegistryPro, LTD

Piirinimien hankkiminen

- Yleiset päätason piirinimiet
  - useita rekisteröijiä
  - hinnat vaihtelevat
  - lista `http://www.icann.org`

  Alunperin `.com`, `.net` ja `.org` piirinimien jako oli InterNIC:n yksinoikeus. Tämä varma (USD 35/vuosi/nimi) tulonlähde herätti kovasti kritiikkiä ja vuoden 1999 alusta lähtien on ollut muitakin rekisteröijiä.

- Maakohtaiset piirinimet
  - eri maissa erilaisia käytäntöjä

    Suomi, fi varsin tiukat säännöt (10.000)
    - hakijan kauppa-, yhdistys- tai säätiörekisteriin merkitty nimi
    - tavaramerkkirekisteriin merkitty sanamerkki
    - julkisyhteisölle joko tämän nimi, nimen lyhenne tai julkista tehtävää kuvaava muu lyhenne

    `http://www.thk.fi/suomi/internet/abc.htm`

    Japani, jp yrityksen tulee toimia Japanissa ja transliteroinnin oltava oikein

    Tuvalu, tv (37)

    Tonga, to "ostettu" maakoodi, vapaasti rekisteröitävissä (2.500)

Nimipalvelun komponentit

ratkaisija käyttöjärjestelmässä oleva kirjasto, joka tarjoaa sovellusrajapinnan ja kysyy tiedot määritellyltä nimipalvelimelta, joka on läheisessä verkossa. Ratkaisija lähettää rekursiivisen pyynnön ts. pyytää nimipalvelijaa ratkaisemaan kyselyn loppuun saakka. Ratkaisija ei yleensä pidä omaa välimuistia. *(resolver)*

ensisijainen nimipalvelin kullakin piirillä yleensä yksi, joskin isoilla piireillä (kuten juurella) voi olla useita ensisijaisia nimipalvelimia. Näiden synkronoinnista tulee huolehtia.

Sisältää kaikki piirin nimipalvelutiedot *(primary nameserver)*

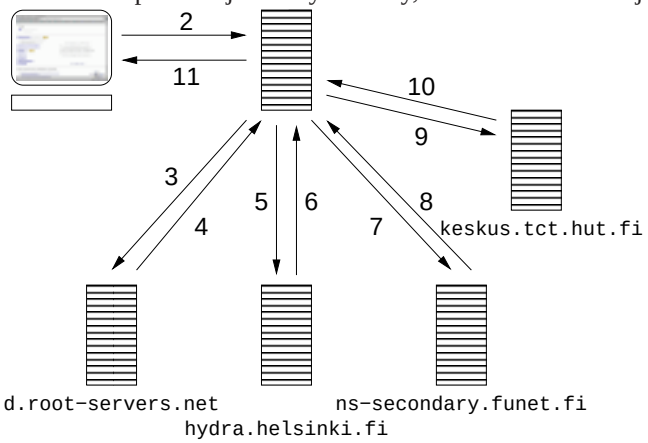
toissijainen nimipalvelin hakee tiedot ensisijaiselta palvelimelta käynnistyksen yhteydessä tai kun ensisijainen nimipalvelin ilmoittaa muutoksesta. Kullakin alueella tulisi olla vähintään kaksi nimipalvelinta: tyypillisesti yksi ensisijainen nimipalvelin ja yksi toissijainen. Ulkopuoliselle ensi- ja toissijainen nimipalvelin eivät eroa mitenkään. *(secondary nameserver)*

välimuistinimipalvelin ei toimi minkään piirin nimipalvelimena vaan selvittää ja vastaa asiakkaiden kyseilyihin. Ensi- ja toissijaiset nimipalvelimet toimivat usein myös välimuistipalvelimina. *(caching name server)*

välitysnimipalvelin toimii kuten välimuistinimipalvelin, mutta antaa tuntemattomat kyselyt selvitettäväksi toiselle nimipalvelimelle. Tarpeen esimerkiksi suojatussa verkossa, josta ei voida suoraan liikennöidä. Auttaa myös jakamaan kuormaa. Asiakkaan verkon oma nimipalvelin voidaan konfiguroida kyselemään ensisijaisesti ISP:n nimipalvelimelta, jolloin välimuistista saadaan suurin hyöty. *(forwarding name server)*

Nimen selvitys: `www.tct.hut.fi`

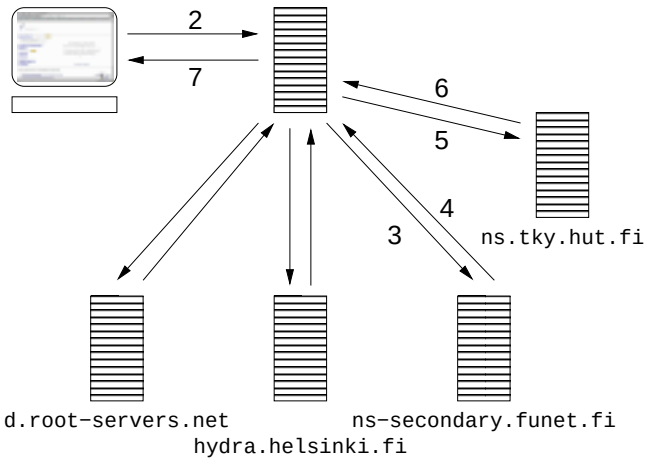
Oletus: nimipalvelin juuri käynnistetty, ei tiedä muuta kuin juuripalvelimet.



1. Käyttäjä kirjoittaa selaimeen `www.tct.hut.fi` ja painaa enter
   $\Rightarrow$ selain kysyy kirjastolta `www.tct.hut.fi`:n osoitetta
2. Ratkaisijakirjasto muodostaa nimipalvelukyselyn ja lähettää sen määritellylle nimipalvelimelle *rekursiivisena* kyselynä
3. Nimipalvelin ei tiedä vastausta, joten se tekee *iteratiivisen* kyselyn yhdelle juurinimipalvelimista. Joihinkin nimipalvelinohjelmistoihinon mahdollista määritellä, missä päin osoiteavaruutta olevilta palvelimilta ensisijaisisti kysytään.
4. Juurinimipalvelin ei tiedä vastausta kyselyyn, mutta sensijaan palauttaa listan `fi`-piirin nimipalvelimista
5. Nimipalvelin kysyy `www.tct.hut.fi`:n osoitetta yhdeltä näistä
6. Vastauksena tulee lista `hut.fi`-piirin nimipalvelimista
7. Nimipalvelin kysyy `www.tct.hut.fi`:n osoitetta yhdeltä näistä
8. Vastauksena tulee lista `tct.hut.fi`-piirin nimipalvelimista
9. Nimipalvelin kysyy `www.tct.hut.fi`:n osoitetta yhdeltä näistä
10. Vastauksena tulee tieto, että `www.tct.hut.fi` on `130.233.154.176`

Nimen selvitys: `www.tky.hut.fi`

Oletus: kysely tapahtuu kohta edellisen kyselyn jälkeen (tietueet edelleen voimassa)



1. Käyttäjä kirjoittaa selaimeen `www.tky.hut.fi` ja painaa enter
   ⇒ selain kysyy kirjastolta `www.tky.hut.fi`:n osoitetta
2. Ratkaisijakirjasto muodostaa nimipalvelukyselyn ja lähettää sen määritellylle nimipalvelimelle *rekursiivisena* kyselynä
3. Nimipalvelin ei tiedä vastausta, mutta se tietää, mitkä ovat `hut.fi`-piirin nimipalvelimet. Se lähettää *iteratiivisen* kyselyn yhdelle näistä.
4. Vastauksena tulee lista `tky.hut.fi`-piirin nimipalvelimista
5. Nimipalvelin kysyy `www.tky.hut.fi`:n osoitetta yhdeltä näistä
6. Vastauksena tulee tieto, että `www.tky.hut.fi` on `130.233.16.2`

Mitä nimipalvelussa on

- Tietue muodostuu

  nimi: avain, minkä perusteella haetaan

  arvo: haettu arvo

  tyypistä: miten nimi-arvo -pari tulkitaan

  A IPv4 osoite

  NS piirin nimipalvelin

  CNAME nimi aliakselle, esim. `www.tct.hut.fi` ⇒`keskus.tct.hut.fi` Aliasta *ei voi* käyttää esim. MX-kentässä

  HINFO tietoa koneesta, esim. käyttöjärjestelmä. Nykyään harvemmin käytetty tietoturvasyistä.

  MX postinvälityksestä huolehtiva kone, voidaan määritellä suosituimmuusjärjestys

  PTR osoitin nimeen

  AAAA IPv6 osoite

  RP vastuuhenkilö

  LOC laitteen koordinaatit

  TXT vapaamuotoista tekstiä, esimerkiksi organisaation täydellinen nimi ja sijainti

  SIG allekirjoitus

  KEY avain

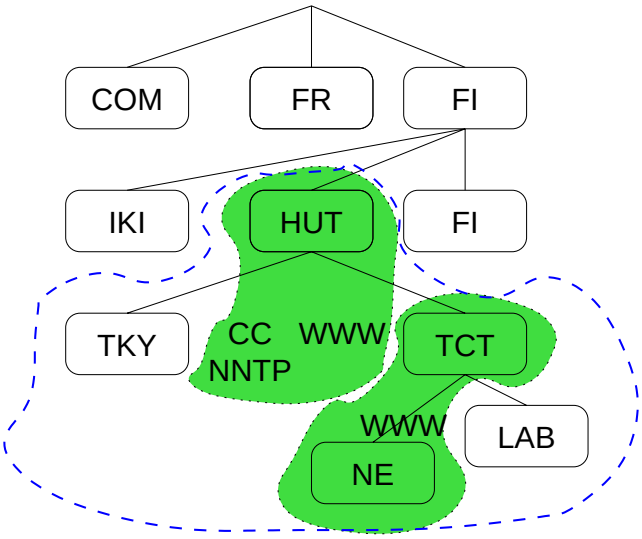
  luokka: käytännössä vain Internet-luokka, mahdollista määritellä erillisiä nimiavaruuksia

  elinikä: kuinka kauan tieto on voimassa, tarpeen välimuistin tominnan kannalta

Aluetiedostot

```
tct.hut.fi IN SOA keskus.tct.hut.fi. puhuri.tct.hut.fi. (
        101008602 ; serial number
        10800 ; Refresh 3 hours
        3600 ; Retry 1 hour
        604800 ; Expire 1 week
        86400 ) ; TTL 1 day

        IN NS keskus.tct.hut.fi. ; primary name server
        IN NS ns1.hut.fi. ; first secondary
        IN NS ns2.hut.fi. ; second secondary

        IN MX 10 keskus ; primary mail server
        IN MX 20 smtp-1.hut.fi. ; backup
        IN MX 20 smtp-2.hut.fi. ; second backup

keskus  IN A 130.233.154.176
        IN MX 10 keskus

www     IN CNAME keskus
smtp    IN CNAME keskus

kytkin.ne IN A 10.0.0.1
```

Alueen ja piirin ero



piiri on haara DNS-puusta

alue on osa (tai kokonaan) piiriä

Alipiirit voivat kuulua samaan alueeseen tai ne voivat olla erillisenä piirinä.

Nimen selvttäminen osoitteesta

- IP-osoitteilla ja nimillä ei keskinäistä riippuvuutta
- Oltava erillinen hierarkia IP-osoitteille: `in-addr.arpa`
- Jos halutaan tietää `130.233.154.148` vastaava nimi, kysytään `148.154.233.130.in-addr.arpa` PTR-tyyppi
- Delegointi tavurajalta helppo, muutenkin onnistuu aliaksia käyttäen [3]

- Käänteinen nimipalvelu “turvaa” palvelut, eräät palvelimet kieltäytyvät yhteyksistä koneilta, joille ei löydy käänteistä nimipalvelua.
- Tarvittaessa kysytään molemmin päin:
  - Yhteys koneelta `10.9.2.3`
  - `3.2.9.10.in-addr.arpa` ⇒`dial-3.example.net`
  - `dial-3.example.net` ⇒`10.9.2.3` ⇒*OK*

Nimipalvelu operaattorin palveluna

- Nimipalvelulta vaaditaan suurta luotettavuutta

  Jos jonkun piirin nimipalvelimista mikään ei vastaa tai antaa vääriä vastauksia, tästä seuraa yleensä ongelmia, erityisesti sähköpostin välituksen suhteen.
- Yksittäsen vian (verkkolaite, kaapeli, palvelin) ei tulisi aiheuttaa nimipalvelun pysähtymistä
  ⇒ palvelimet eri puolille verkkoa (sekä maantieteellisesti että topologisesti)

  Esimerkiksi Suomen `.fi`-juuren nimipalvelimien sijoituspaikat:
  - Helsinki (x2)
  - Espoossa
  - Amsterdam (NL)
  - Fairfax (VI, USA)
  - Houston (TX, USA)

  `yahoo.com`:n nimipalvelimien kaupungit:
  - Sunnyvale (CA, USA)
  - Lontoo (UK)
  - Santa Clara (CA, USA)
- Yksittäisen asiakkaan vaikea toteuttaa
- Toissijainen nimipalvelu “kevyt” palvelu
  ⇒ helposti lisäarvoa asiakkaalle
- Asiakkaalla edelleen oma hallinta

Nimipalvelun kehitys

- Juuripalvelun selkeyttäminen [1]
- Turvallisuus heikkoa
  - nimipalvelutietojen allekirjoittaminen[2]
- Avainjakelu
- DNS yleiskäyttöisenä hakemistona, ei välttämättä järkevää: DNS on suunniteltu nimi-osoitemuunnoksiin.
- Merkistön laajentaminen, Microsoft ajaa mutta rikkoo monta asiaa

Yhteenveto

- DNS lisää verkon käyttäjäystävällisyyttä
- “Helppo” palvelu
- Paljon politiikkaa
- Turvallisuus (ehkä) paranee

Viitteet

[1] R. Bush, D. Karrenberg, M. Kosters, and R. Plzak. Root Name Server Operational Requirements. Request for Comments RFC 2870, Internet Engineering Task Force, June 2000. (Best Current Practice) (Obsoletes RFC2010) (Also BCP0040). URL:`http://www.ietf.org/rfc/rfc2870.txt`.

[2] D. Eastlake. Domain Name System Security Extensions. Request for Comments RFC 2535, Internet Engineering Task Force, March 1999. (Internet Proposed Standard) (Updates RFC2181, RFC1035, RFC1034) (Updated by RFC2931). URL:`http://www.ietf.org/rfc/rfc2535.txt`.

[3] H. Eidnes, G. de Groot, and P. Vixie. Classless IN-ADDR.ARPA delegation. Request for Comments RFC 2317, Internet Engineering Task Force, March 1998. (Best Current Practice) (Also BCP0020). URL:`http://www.ietf.org/rfc/rfc2317.txt`.

[4] P.V. Mockapetris. Domain names - concepts and facilities. Request for Comments RFC 1034, Internet Engineering Task Force, November 1987. (Internet Standard) (Updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC2065, RFC2181, RFC2308, RFC2535) (Obsoletes RFC0973, RFC0882, RFC0883) (Also STD0013). URL:`http://www.ietf.org/rfc/rfc1034.txt`.

[5] P.V. Mockapetris. Domain names - implementation and specification. Request for Comments RFC 1035, Internet Engineering Task Force, November 1987. (Internet Standard) (Updated by RFC1101, RFC1183, RFC1348, RFC1876, RFC1982, RFC1995, RFC1996, RFC2065, RFC2181, RFC2136, RFC2137, RFC2308, RFC2535, RFC2845) (Obsoletes RFC0973, RFC0882, RFC0883) (Also STD0013). URL:`http://www.ietf.org/rfc/rfc1035.txt`.

[6] J. Postel. Domain Name System Structure and Delegation. Request for Comments RFC 1591, Internet Engineering Task Force, March 1994. (Informational). URL:`http://www.ietf.org/rfc/rfc1591.txt`.