Verkonhallinta ja hakemistot

Markus Peuhkuri

2004-01-29

Luennon aiheet

- Verkonhallinta
- Nimipalvelu
  - 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

Perinteinen verkonvalvonta

- Niin kauan kuin kaikki toimii ei tehdä mitään
- Kun vika tai häiriö tulee:
  - selvitettään häiriön laajuus
    1. "toimiiko sinulla"
    2. "toimiiko yhteys muualle"
  - mitataan/tutkitaan järjestelmää
  - korjataan epäilty vika
  - hommat seis kunnes korjattu, μ-tuki juoksee
- Ei tarjoa historiatietoa
- Ei tietoa liikenteestä
- Hallittavien laitteiden määrä tukihenkilöä kohti kasvanut
  $\Rightarrow$ 1 CPU / 200 käyttäjää $\Rightarrow$ 300 CPU / 200 käyttäjää
- Ihmiset kalliita, laitteet monimutkaisia: operaattorille saattaa olla halvempaa yliprovisoida verkko kuin ottaa käyttöön osaavaa henkilöstöä vaativia palvelunlaadun takaavia menetelmiä.

Toiminnallinen arkkitehtuuri

Hallittavat kohteet [1] Tarkkailua tarvitsevat

- laitteet
- järjestelmät
- muut

Esimerkiksi reitittimet, keskittimet, päätelaitteet, palvelimet, sovellukset (tietokannat, viestintäsovellukset (sähköposti).

Elementtienhallintajärjestelmä [2] hallitsee tiettyä osaa verkosta, “verkonhallintasovellus”

Hallintajärjestelmien hallinta [3] yhdistää eri hallintajärjestelmien tiedot, esim. hälytysten yhdistäminen

Käyttöliittymä “työkalu”, näyttää

- hälytykset realiajassa
- historiatietoa, muutoskäyrät
- raportit

Verkonhallinnan osa-alueet (OSI: FCAPS)

Vikojen hallinta (*Fault* mgmt)

- tunnistaminen
- eristäminen
- korjaaminen

Toteutetaan kyselyillä, testeillä ja reporttien analysoinnilla. Tämä osa on suunniteltava huolellisesti tai verkko kuormittuu tarpeettomasti.

Kokoonpanon hallinta (*Configuration* mgmt)

Ehkä tärkein osa verkonhallintaa: et voi hallita, jos et tiedä mitä hallitset. Sisältää komponenttien

- nimeäminen
- ominaisuudet
- tilat

Kuvaus verkosta ja laitteista.

Laskenta (*Accounting*)

Usein ei yksityisissä tietokoneverkoissa käytössä, operaattorille tärkeä.

Suorituskyvyn hallinta (*Performance* mgmt)

- verkon taloudellisuus riippuu suorituskyvyn hallinnasta: tiedetään, mitä kohtaa tulee kehittää seuraavaksi
- etäyhteyksillä erityisesti mahdollisuudet suuriin säästöihin
- ei yleensä hyvin tuettu hallintajärjestelmissä

Turvallisuuden hallinta (*Security* mgmt)

- vain oikeilla käyttäjillä pääsy tiettyyn resussiin
- hälytykset epäonnistuneista autentikoinneista
- myös fyysinen turvallisuus[4]

[1] Managed Objects
[2] Element Management Systems (EMS)
[3] Manager of Managers Systems MoM
[4] Murtosuojaus, palohälytykset, vesihälytykset, lämpötila…

Velotus (chargeback)

Osa laskentaa, veloitetaan vain käytetyistä resusseista

Järjestelmänhallinta (systems management)

Myös muiden kun verkkolaitteiden hallinta samassa; osa “business process streamlining”.

Kulujen hallinta (cost management)

Paneutuu hallittavien laitteiden

- luotettavuuteen
- toimintakelpoisuuteen
- hallittavuuteen

Verkon käyttökulut määräytyvät:

- ylläpitokustannuksista
- vikojen välisestä ajasta (MTBF: Mean Time Between Failure)
- korjausajasta (MTTR: Mean Time To Repair)

TNM-verkonhallinta

- ITU-T:n verkonhallintakonsepti[5]
- Kehitetty vuodesta 1985 lähetien, suositus M.3xxx
- Tukeutuu vahvasti OSI hallintaan
- Hyödyllinen myös Internetin hallintaan
- Komponentit:

  televerkko (telecommunication network) hallittava järjestelmä

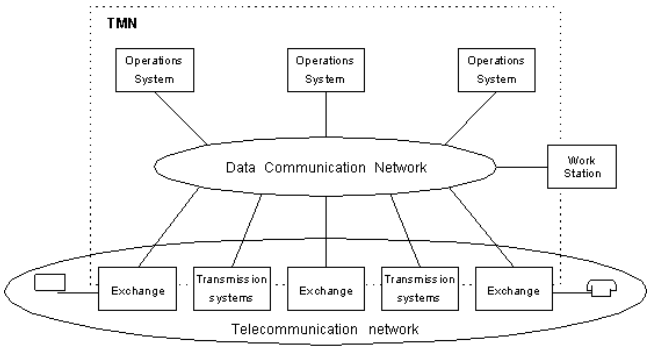
  toimintajärjestelmät (operations system) hoitavat suurimman osan hallintatoimista, joko manuaalisesti tai automaattisesti
  voivat toimia myös yhdessä toteuttaakseen toiminnon

  työasema (work station) mahdollistaa operaattoreille pääsyn hallintatietoon käyttöliittymästä

  tietoliikenneverkko (data communication network) välittää tietoa televerkon, toimintajärjestelmien ja työasemien välillä

TNM:n suhde verkkoon

- “Erillinen verkko, joka liittyy televerkkoon useissa pisteissä”



[5]Telecommunications Management Network

TNM: looginen kerroksellinen arkkitehtuuri

- Usein tarvetta esittää asiat hierarkisesti eri abstraktiotasoilla
- “Vastuumalli”

Elementtihallintakerros Yksittäisten laitteiden ja ohjelmistojen hallinta, esim.

- laitevikojen havainnointi
- tehonkulutuksen mittaus
- lämpötilan tarkkailu
- resussien (CPU-teho, puskurit, jonot) käytön mittaus
- tilastotietojen keräys
- ohjelmistopäivitukset

Verkonhallintakerros Laitteiden välisen toiminnan hallinta, esim.

- verkon topologisen kuvan luominen
- tietoliikennepolkujen määrittäminen laadun takaamiseksi asiakkaalle
- reititystaulujen muokkaus
- linkkinen kuormituksen tarkkailu
- verkon suorituskyvyn optimoiminen
- virheiden havaitseminen

Palvelunhallintakerros Verkon käyttäjien havaitsemien ilmiöiden hallinta, esim.

- palvelun laadun hallinta (QoS: viive, hukka,. . .)
- laskenta
- käyttäjien luominen ja poisto
- osoitteiden hallinta

Liiketoiminnanhallintakerros Asettaa tavoitteet muille kerroksille

SNMP-arkkitehtuurin toteustarpeet [10]

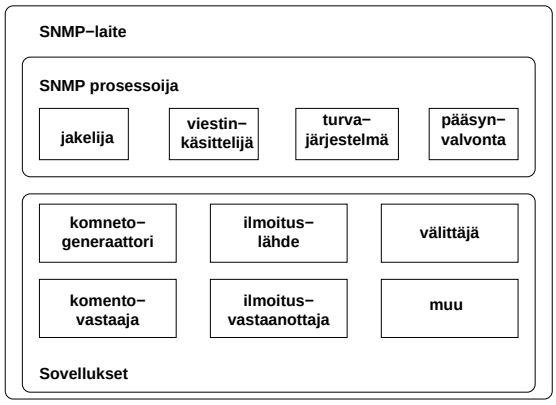
- Yksinkertaiset komentovastaimet (agentit)
- Välityssovelluket (välitysagentti)
- Komentorivipohjaiset tapahtumat
- Välitason hallinta-asemat
- Hallinta-asemat

SNMPv3 [21]

- SNMPv2* ja SNMPv2u yhdistettynä, kehitys alkanut 1997
- Viitekehyksen ja mekanismien erityttäminen
  - manager $\Leftrightarrow$ agent muuttuu sovelluksiksi
  - eri osien standardointi erillisinä

  $\Rightarrow$tavoitteena joustavampi määrittely

SNMPv3 viitekehys



SNMP prosessoija (SNMP Engine)[4]

jakelija (dispatcher) viestien välittäjä

1. PDU:t sovelluksille ja sovelluksilta
2. PDU:t viestinkäsittelijälle
3. SNMP-viestit verkkon ja verkosta

viestinkäsittelijiä (message processing subsystem) SNMP-viestien käsittely

1. dekoodaus vastaanotossa
2. kodaus lähetyksessä

eri modulit eri SNMP-versioille

turvajärjestelmä (security subsystem) huolehtii viestien autentikoinnista ja salauksesta

pääsynvalvonta (access control subsystem) kontrolloi tunnistetujen pääsyä muuttujiin

Sovellukset (Applications) toteuttavat eri tehtävät, laitteeseen voidaan ottaa vain sen tarvitsemat sovellukset. [13]

komentogeneraattori (command generator) käynnistää Get*- ja Set-pyynnöt sekä käsittelee vastaukset niihin

komentovastaaja (command responder) vastaanottaa Get*- ja Set-pyynnöt pääsynvalvonnan avulla ja vastaa niihin

ilmoituslähde (notification originator) lähettää Trap- tai Inform-viestejä havaintojen perusteella, huolehdittava oikeista SNMP-versioista ja turvaparametreistä.

ilmoitusvastaanottaja (notification receiver) vastaanottaa ilmoitusviestit ja kuittaa Inform-viestit

välittäjä (proxy forwarder) välittää SNMP-viestit eteenpäin

muu muita mahdollisia soveluuksia

Web-pohjainen hallinta

- Web-selain: yleinen käyttöliittymä
  $\Rightarrow$ point-and-click
- HTTP-protolla & HTML yksinkertainen
- HTTP-palvelin verkkolaitteessa
  - yksinkertainen toteuttaa
  - helppokäyttöisempi verrattuna komentrivipohjaiseen
  - ei skaalaudu
- Web-selain käyttöliittymänä
  - SNMP-protokolla taustalla
  - käyttöliittymä toteutettu selaimella ja Javalla
  - hallinnan ja monitoroinnin hajauttaminen

Hakemistopohjainen verkko (Directory Enabled Networking)

- Verkkoelementtien lisäksi myös hallittava
  - verkkoresusseja
  - sovelluksia
  - käyttäjiä
- Tiedot tallennettava hakemistoon
  - tieto tallennettu hajautetusti
  - tieto haettavissa ominaisuuden, esimerkiksi nimen perusteella ns. White Pages, tai luokittelun, esimerkiksi lajin perusteella ns. Yellow Pages, perusteella
  - yksi sisäänkirjautuminen palveluihin, resusseihin ja sovelluksiin
  - sijaintiriippumaton hallinta ja käyttö
  - tiedon replikointi
    $\Rightarrow$ tieto saatavissa läheltä
- SNMP keskittynyt kuvaamaan verkon dynamista tietoa

DEN-komponentit

Hakemisto (Directory) tallentaa tiedot järjestelmästä

- LDAP-pohjainen [20]
- yhteiskäyttö DNS:n kanssa [15]

Toimintapalvelin (Policy server) mahdollistaa "toimintaperusteiset verkot"

- konfiguroi verkon käyttäjälle
- muuttaa asetuksia dynamisesti
  - viive
  - kaistanleveys
  - oikeudet
- WBEM[6] CIM[7]-XML käyttää standardikomponentteja

  xmlCIM välittää CIM-viesti

  HTTP kuljetusmenetelmänä

Verkonhallinta IP-verkoissa aktiivisilla menetelmillä

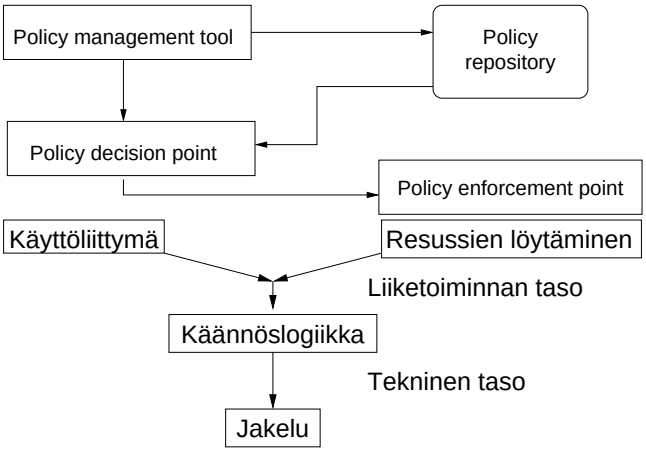
- Hallittavien laitteiden määrä kertaluokkaa isompi kuin POTS-verkoissa
- Keskitetyn ratkaisun ongelmat korostuvat
- Monimutkaisissa järjestelmissä viive tai kaistanleveys rajoittaa hallintaa, koska halutun hallintatapahtuman toteuttaminen kysely-vastaus -menetelmällä voi vaatia suuren määrän viestejä.
- Ratkaisuvaihtoehdot
  - aktiiviset verkot (active network)
    - aktviivinen paketti suoritetaan verkkolaitteissa
  - ohjelmoitavat verkot (programmable networks)
    - CORBA, Java RMI...
  - liikkuvat agentit (mobile agents)
    - laitteesta toiseen siirtyvä (tai replikoiva) ohjelma tekee hallintatoimet, mahdollisesti keskenään kommunikoiden.

[6] Web-Based Enterprise Management
[7] Common Information Model

Menettelytapapohjainen verkonhallinta

Policy-based management

- Luotu helpottamaan suurten laitemäärien hallintaan
- Jos … Niin … -säännöt
  - liiketoimintatason säännöt
  - toimintakuri yhdistää liiketoimintatarpeen ja sen totetuttavan tekniikan
- Laite-, laiteryhmä- ja verkkolaajuisia



Käyttöliittymä liiketoimitatason sääntöjen syöttäminen

Resussien löytäminen verkkolaitteiden ja -topologian inventointi

Käännöslogikka tarkistaa sääntöjen keskinäisen eheyden ja toteuttamiskelpoisuuden ja muuntaa säännöt teknisiksi

Jakelu hoitaa laitekohtaisen konfiguroinnin. On mahdollista, että verkon eri laitteet tukevat eri hallintamenetelmiä (esim. komentorivi, snmp, konfigurointitiedosto, web-pohjainen). Jakelu huolehtii siitä, että kukin laite konfiguroidaan sillä tavalla kuin on mahdollista.

Siis *MITÄ* hallintaa

- SNMP kevyt, toimii huonoissa verkko-olosuhteissa
- HTTP(TCP)-pohjaiset pystyvät siirtämään suuria tietomääriä
- Ohjelmoitavuus mahdollistaa monimutkaiset operaatiot ja prosessoinnin optimoinnin
- Menettelypohjaisuus skaalautuvuuden suuriin ja moniulotteisiin verkkoihin

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:  postel@venera.isi.edu
Subject:  re: IEN-116 nameserver
Date:  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) [15, 16]
   - 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`, korkeat vaatimukset [3]
   - nimipalvelun käynnistystieto, mutta itseasiassa nimipalvelimelle riittää tietää yhdenkin toisen *luotettavan* nimipalvelimen osoite.
   - Viimeaikoina useiden DDoS-hyökkäysten kohteina
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
  ⇒ 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 [18]

  .com kaupallisille yrityksille, nykyään erittäin laajaksi paisunut, noin 21 miljoonaa piiriä (esim. `sun.com`, `whitehouse.com`)

  .net alunperin verkko-operaattoreille tarkoitettu, nykyään sisältää mitä tahansa (esim. `uusitupa.net`), noin 3,6 miljoonaa

  .org erilaisia organisaatioita, jotka eivät sovellu muihin ryhmiin – tai ole saaneet `.com`-piiriä (esim. `eff.org`, `debian.org`, `amnesty.org`, `metso.org`), noin 2,6 miljoonaa

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

- Uudet, 2001-02 voimaan tulleet piirinimet (tilanne 2003-01-09, lukumäärät osin 2002-09-31)

  .aero lentoyhtiöiden käyttöön – Societe Internationale de Telecommunications Aeronautiques SC, (SITA); 2.600 kpl

  .biz yritystoimintaa varten – JVTeam, LLC; 770.000

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

  .info rajoittamton – Afilias, LLC, 950.000

  .museum museot – Museum Domain Management Association, (MDMA): 600 kpl 2. tason piirinimiä

  .name yksityishenklöille 3. tasolla `john.doe.name` – Global Name Registry, LTD: 86.000

  .pro "ammattilaiset", esim. `johnDoe.med.pro` – RegistryPro, LTD; ei vielä toiminnassa

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 (38.000)
    - hakijan kauppa-, yhdistys- tai säätiörekisteriin merkitty nimi
    - tavaramerkkirekisteriin merkitty sanamerkki
    - julkisyhteisölle joko tämän nimi, nimen lyhenne tai julkista tehtävää kuvaava muu lyhenne
    - tunnuksen ennakkotarkastuksesta luovutaan syyskussa 2003; hakijan huolehdittava, että ei loukkaa toisen oikeuksia

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

    Japani, jp yrityksen tulee toimia Japanissa ja transliteroinnin oltava oikein

    Tuvalu, tv (470.000)

    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. Ensisijainen nimipalvelin voi olla myös piilotettu eli se ei vastaa ulkopuolisiin kyselyihin vaan ainoastaan antaa julkisten nimipalvelimien hakea tiedot.

Sisältää kaikki piirin nimipalvelutiedot *(primary nameserver)*

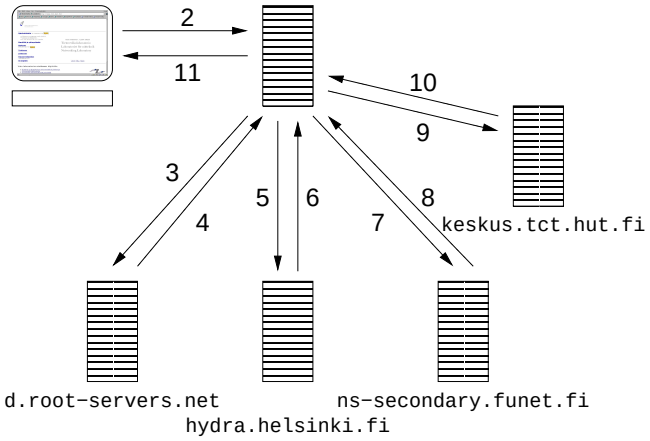
toissijainen nimipalvelin hakee tiedot ensisijaiselta palvelimelta käynnistyksen yhteydessä, määritellyin aikavälein tai kun ensisijainen nimipalvelin ilmoittaa muutoksesta. Kullakin alueella tulisi olla vähintään kaksi nimipalvelinta: tyypillisesti yksi ensisijainen nimipalvelin ja yksi toissijainen. 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.

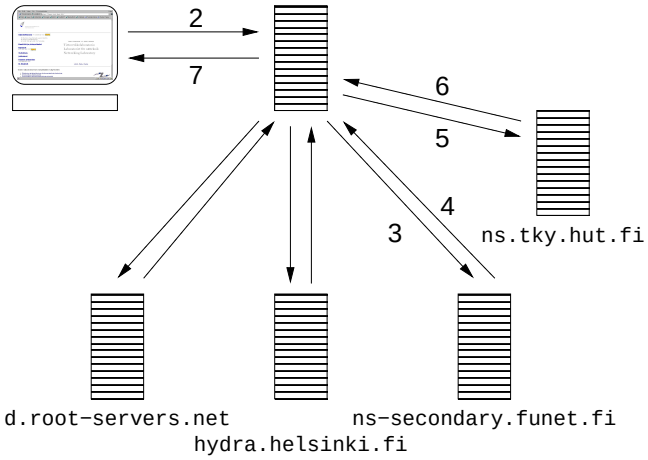


1. Käyttäjä kirjoittaa selaimeen `www.tct.hut.fi` ja painaa enter
   ⇒ selain kysyy kirjastolta `www.tct.hut.fi`:n osoitetta
2. Ratkaisijakirjasto muodostaa nimipalvelukyselyn ja lähettää sen määritellylle nimipalvelimelle *rekursiivisena* kyselynä
3. Nimipalvelin ei tiedä vastausta, joten se tekee *iteratiivisen* 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

  DNAME alipuun uudelleenohjaus, hyödyllinen esimerkiksi käänteisen nimipalvelun yhteydessä, missä `in-addr.arpa`-puu operaattorin osoiteavaruuden osalta siirtää esim. `in-addr.isp.example` ja tästä edelleen asiakkaille. Hyöty erityisesti IPv6-verkoissa. [6]

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

  MX postinvälityksestä huolehtiva kone, voidaan määritellä suosituimmuusjärjestys

  PTR osoitin nimeen

  AAAA IPv6 osoite (ns. nibble-format, poistuva)

  A6 IPv6 osoite bittikenttiin [5] perustuva hierarkinen määrittely

  RP vastuuhenkilö

LOC laitteen koordinaatit

TXT vapaamuotoista tekstiä, esimerkiksi organisaation täydellinen nimi ja sijainti

SIG julkisiin avaimiin perustuva allekirjoitus, joko yksittäisten tietueiden tai koko transaktion [1]

TSIG jaettuun salaisuuteen perustuva allekirjoitus, jota voidaan käyttää organisaation sisällä tietueiden ja kyselyiden autentikointiin. Nopeampi laskea kuin SIG. [19]

KEY avain, jolla voidaan tarkistaa SIG-tietueet [1] tai käyttää muihin tarkoituksiin (TLS, sähköposti, IPSec). Avaimia voi olla useilla algoritmeillä (RSA/MD5, Diffie-Hellman, DSA, RSA/SHA-1). Suositellaan, että eri tarkoituksia varten on erilliset avaimet.

CERT sertifikaatti, esim. PKIX, SPKI, PGP avainten varmistamiseen. [2]

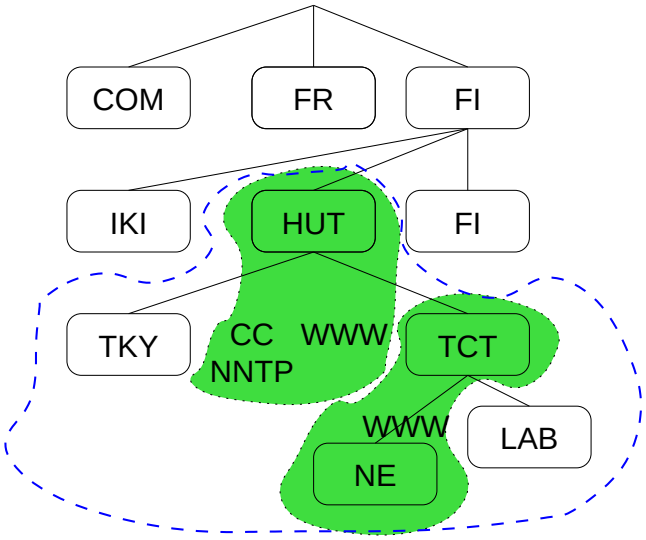
luokka: käytännössä vain Internet-luokka, mahdollista määritellä erillisiä nimiavaruuksia

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 *(domain)* on haara DNS-puusta

alue *(zone)* 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 [7]
- 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)

  `microsoft.com`:n nimipalvelimet (2001-01):

```
DNS5.CP.MSFT.NET        internet address = 207.46.138.12
DNS7.CP.MSFT.NET        internet address = 207.46.138.21
DNS6.CP.MSFT.NET        internet address = 207.46.138.20
DNS4.CP.MSFT.NET        internet address = 207.46.138.11
```

- Yksittäisen asiakkaan vaikea toteuttaa
- Toissijainen nimipalvelu “kevyt” palvelu
  ⇒ helposti lisäarvoa asiakkaalle
- Asiakkaalla edelleen oma hallinta

Nimipalvelun turvallisuus

- Nimipalvelutiedot kriittisiä verkon turvalliselle toiminnalle
  - sähköpostien ohjaus
  - yhteyksien ohjaus (salasanojen kaappaus, man-in-midle)
- Avaimet (SSL, TLS, SSH, IPSec) tuovat jonkin verran turvaa

- Välimuistin saastuttaminen

  ns.innocent.example: `1.0.0.10.in-addr.arpa IN PTR ?` ⇒ns.evil.example
  ns.evil.example ⇒ns.innocent.example:

1.0.0.10.in-addr.arpa	IN	PTR	trap.evil.example
bank.example	IN	NS	ns.evil.example
www.bank.example	IN	A	middlebox.evil.example
company.example	IN	NS	ns.evil.example
company.example	IN	MX	1 mailrecord.evil.example

- Vaikeasti havaittamissa

Nimipalvelun kehitys

- Juuripalvelun selkeyttäminen [3]
- Turvallisuus heikkoa
  - nimipalvelutietojen allekirjoittaminen[1]
- Avainjakelu
- DNS yleiskäyttöisenä hakemistona, ei välttämättä järkevää: DNS on suunniteltu nimi-osoitemuunnoksiin.
- IPv6
- enum: puhelinnumeron muuntaminen DNS-nimeksi
- Merkistön laajentaminen, Microsoft ajaa mutta rikkoo monta asiaa [12]
  - sähköposti
  - reititys (reitityspolitiikkatietokannat)
  - verkonhallinta (SNMP)
  - sertifikaatit (TLS, IPSec)

DNSSEC

- Nimipalvelutiedot autentikoimattomia
  - aluetiedostoissa (ts. authoratiivisilla palvelimilla)
  - välimuistissa
  - verkossa

  ⇒useita mahdollisuuksia väärentää

Palvelujen hakeminen

- Perinteisesti “oletetut nimet”
  - nntp, news
  - smtp, mail
  - www, http, home
- Ei vakiintunutta käytäntöä
- Ei vaihtoehtoisia palvelimia, vrt. MX-tietueet
- SRV [9]
  - yleistys MX-tietueile
  - `_ldap._tcp.example.com` kysyy TCP-protokollaa tukevat LDAP-palvelimet `example.com`-piirille
  - vastauksena lista, joissa tietuilla on

prioriteeti kuten MX-tietueissa, pienempiarvoinen koetettava ensin

paino määrää valintatodennäköisyyden saman prioriteetin tietueiden kesken. Tällä on mahdollista jakaa liikennettä eri suhteissa eri palvelimien kesken. Tätä ei kuitenkaan voi käyttää dynaamiseen kuormanjakoon ilman, että nimipalvelun välimuistitoiminta turmeltuu.

portti kuljetusprotokollan (TCP, UDP) portti, mihin yhteydenmuodostus tapahtuu. Vähentää tarvetta päivittää `/etc/services`-tiedostoa (tai vastaava) uusien palvelujen myötä.

kohde koneen DNS-nimi, joka tarjoaa palveluja. Tähän nimeen voi liittyä useita osoitetietueita, joka suositellaan palautettavaksi samassa kyselyssä. Nimi ei voi olla alias (CNAME). Mikäli palvelua ei tarjota, kohde on "." (juuri).

```
$ORIGIN example.com ;$
_ssh._tcp SRV 0 10 22 fast.example.com.
          SRV 0  1 22 slow.example.com.
          SRV 10 0 24 old.example.com.
```

ENUM

- Puhelinnumeron muuntaminen URI:ksi [14, 8]
- E.164-muotoinen numero numeroittain pisteillä erotettuna käänteisessä järjestyksessä `e164.arpa`-juureen.
- esim. +358-9-451 2467
  ⇒ 7.6.4.2.1.5.4.9.8.5.3.e164.arpa
- Saadun NAPTR-tietueen avulla selvieteään pyyntöä vastaava URI, esimerkiksi sähköpostiosoite, SIP-osotie tai toinen puhelinnumero.
- Useita poliittisia ongelmia
  - salaiset numerot: kyselyitä voidaan helposti tehdä tuhat sekunnissa; muutamassa tunnissa saadaan käytyä koko Helsingin numeroavaruus.
  - luettelotieto arvokasta

```
$ORIGIN 1.5.4.9.8.5.3.e164.arpa. ;$
   IN NAPTR 100 10 "u" "sip+E2U" "!^.*$!sip:info@hut.fi!" .
   IN NAPTR 102 10 "u" "mailto+E2U" "!^.*$!mailto:info@hut.fi!" .
   IN NAPTR 102 12 "u" "tel+E2U" "!^.*$!tel:+358694511!" .
7.6.4.2 IN NAPTR 100 10 "u" "mailto:+E2U" "!^.*$!mailto:puhuri@netlab.hut.fi" .
```

LDAP-hakemistopalvelu

- Kevytversio X.500:sta, alunperin yhdyskäytävä kevyiltä asiakkailta täysimittaiseen X.500-tietokantaan (DAP-protkolla). Nykyään joitakin laajennuksia verrattuna X.500:aa. [20]
- Ei ole sopiva
  - relatiotietokannan korvikkeeksi
  - tiedolle, jota kirjoitetaan usein
  - laajoille data-alkioille
  - DNS: korvaavaksi
- On
  - puumainen tietorakenne attribuutti-arvopareja
  - tiedoissa voidaan käyttää pääsynvalvontaa (SASL: Simple Authentication and Security Layer [17])
  - tietoa voidaan osoittaa URI:lla[11]
- Sopii

  - sovelluskohtaisten hakemistojen yhdistämiseen
  - käyttäjien autentikointiin: sama tietokanta toimii sekä puhelinluettelona että autentikointitietokantana
  - taustatietokannaksi esim. DNS:lle
- Windows Active Directory $\approx$ LDAP

Yhteenveto

- Verkonhallinta vaikuttaa operaattorin työvoimakuluihin
- DNS lisää verkon käyttäjäystävällisyyttä
  - "helppo" palvelu
  - paljon politiikkaa
  - turvallisuus (ehkä) paranee

Viitteet

[1] D. Eastlake 3rd. 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, RFC3007, RFC3008, RFC3090, RFC3226, RFC3445, RFC3597, RFC3655, RFC3658) (Obsoletes RFC2065). URL:`http://www.ietf.org/rfc/rfc2535.txt`.

[2] D. Eastlake 3rd and O. Gudmundsson. Storing Certificates in the Domain Name System (DNS). Request for Comments RFC 2538, Internet Engineering Task Force, March 1999. (Internet Proposed Standard). URL:`http://www.ietf.org/rfc/rfc2538.txt`.

[3] 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`.

[4] J. Case, D. Harrington, R. Presuhn, and B. Wijnen. Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). Request for Comments RFC 2572, Internet Engineering Task Force, April 1999. (Internet Draft Standard) (Obsoleted by RFC3412) (Obsoletes RFC2272). URL:`http://www.ietf.org/rfc/rfc2572.txt`.

[5] M. Crawford. Binary Labels in the Domain Name System. Request for Comments RFC 2673, Internet Engineering Task Force, August 1999. (Experimental) (Updated by RFC3363, RFC3364). URL:`http://www.ietf.org/rfc/rfc2673.txt`.

[6] M. Crawford. Non-Terminal DNS Name Redirection. Request for Comments RFC 2672, Internet Engineering Task Force, August 1999. (Internet Proposed Standard). URL:`http://www.ietf.org/rfc/rfc2672.txt`.

[7] 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`.

[8] P. Faltstrom. E.164 number and DNS. Request for Comments RFC 2916, Internet Engineering Task Force, September 2000. (Internet Proposed Standard). URL:`http://www.ietf.org/rfc/rfc2916.txt`.

[9] A. Gulbrandsen, P. Vixie, and L. Esibov. A DNS RR for specifying the location of services (DNS SRV). Request for Comments RFC 2782, Internet Engineering Task Force, February 2000. (Internet Proposed Standard) (Obsoletes RFC2052). URL:`http://www.ietf.org/rfc/rfc2782.txt`.

[10] D. Harrington, R. Presuhn, and B. Wijnen. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. Request for Comments RFC 3411, Internet Engineering Task Force, December 2002. (Internet Standard) (Obsoletes RFC2571) (Also STD0062). URL:`http://www.ietf.org/rfc/rfc3411.txt`.

[11] T. Howes and M. Smith. The LDAP URL Format. Request for Comments RFC 2255, Internet Engineering Task Force, December 1997. (Internet Proposed Standard) (Updated by RFC3377) (Obsoletes RFC1959). URL:http://www.ietf.org/rfc/rfc2255.txt.

[12] IAB, L. Daigle, and ed. A Tangled Web: Issues of I18N, Domain Names, and the Other Internet protocols. Request for Comments RFC 2825, Internet Engineering Task Force, May 2000. (Informational). URL:http://www.ietf.org/rfc/rfc2825.txt.

[13] D. Levi, P. Meyer, and B. Stewart. SNMPv3 Applications. Request for Comments RFC 2273, Internet Engineering Task Force, January 1998. (Internet Proposed Standard) (Obsoleted by RFC2573) (Obsoletes RFC2263). URL:http://www.ietf.org/rfc/rfc2273.txt.

[14] M. Mealling and R. Daniel. The Naming Authority Pointer (NAPTR) DNS Resource Record. Request for Comments RFC 2915, Internet Engineering Task Force, September 2000. (Internet Proposed Standard) (Updates RFC2168) (Obsoleted by RFC3401, RFC3402, RFC3403, RFC3404). URL:http://www.ietf.org/rfc/rfc2915.txt.

[15] 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.

[16] 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, RFC2136, RFC2181, RFC2137, RFC2308, RFC2535, RFC2845, RFC3425, RFC3658) (Obsoletes RFC0973, RFC0882, RFC0883) (Also STD0013). URL:http://www.ietf.org/rfc/rfc1035.txt.

[17] J. Myers. Simple Authentication and Security Layer (SASL). Request for Comments RFC 2222, Internet Engineering Task Force, October 1997. (Internet Proposed Standard) (Updated by RFC2444). URL:http://www.ietf.org/rfc/rfc2222.txt.

[18] 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.

[19] P. Vixie, O. Gudmundsson, D. Eastlake 3rd, and B. Wellington. Secret Key Transaction Authentication for DNS (TSIG). Request for Comments RFC 2845, Internet Engineering Task Force, May 2000. (Internet Proposed Standard) (Updates RFC1035) (Updated by RFC3645). URL:http://www.ietf.org/rfc/rfc2845.txt.

[20] M. Wahl, T. Howes, and S. Kille. Lightweight Directory Access Protocol (v3). Request for Comments RFC 2251, Internet Engineering Task Force, December 1997. (Internet Proposed Standard) (Updated by RFC3377). URL:http://www.ietf.org/rfc/rfc2251.txt.

[21] B. Wijnen, D. Harrington, and R. Presuhn. An Architecture for Describing SNMP Management Frameworks. Request for Comments RFC 2571, Internet Engineering Task Force, April 1999. (Internet Draft Standard) (Obsoleted by RFC3411) (Obsoletes RFC2271). URL:http://www.ietf.org/rfc/rfc2571.txt.