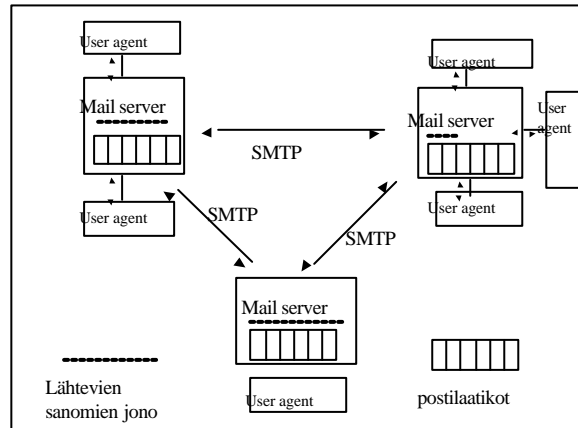


## 2.2. Sähköposti

- **Käyttäjiliitäntä (user agent)**
  - sanomien kirjoittaminen, lukeminen ja lähettäminen
- **Postipalvelin (mail server)**
  - postilaatikot
- **Postiprotokolla SMTP**
  - sanomien toimittaminen lähettäjän postijärjestelmästä vastaanottajan postijärjestelmään
  - sanoman muoto
    - tekstisanoma, MIME-sanoma

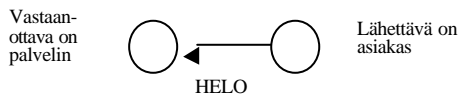
27.9.2001

39



## SMTP (Simple Mail Transfer Protocol)

- **Postipalvelimet käyttävät SMTP-protokollaa sanomien siirtoon**
  - sanoma lähetettävä postipalvelu muodostaa TCP-yhteyden vastaanottajan postipalvelimeen
  - 'kättelyjen' jälkeen siirretään sanomat



27.9.2001

41

### Lähetävä postipalvelin

- muodostaa TCP-yhteyden
- esittelee itsensä
- kertoo lähettäjän ja vastaanottajan
- lähettää sanoman, jos vastaanottava palvelin antaa luvan

### Vastaanottava postipalvelin

- kuuntelee TCP-porttia 25
- hyväksyy yhteydenmuodostuspyynnöt
- vastaanottaa ja siirtää sanomat postilaatikoihin
- palauttaa virheilmoitukset

```
S: 220 helsinki.fi
C: HELO princeton.edu
S: 250 Hello princeton.edu
C: MAIL FROM: <Bob@princeton.edu>
S: 250 <Bob@princeton.edu> OK
C: RCPT TO: <pekka.puupaa@cs.helsinki.fi>
S: 250 <pekka.puupaa@cs.helsinki.fi> OK
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: dataa ... dataa
C: dataa ... dataa
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 princeton.edu closing connection
```

27.9.2001

### • TCP-yhteys on pysyvä

- yhteydellä voidaan lähettää useita sanomia

### • Yhteydellä voidaan lähettää vain ASCII-sanomia

- sanomatekstin lopettaa omalla rivillään irrallisena oleva piste (".") (Tämä on vanha protokolla!)
- "CRLF.CRLF"
- jos sanomassa on binääridataa, esim. kuvia, niin siellä voisi esiintyä irrallinen piste eli CRLF.CRLF => sanoma katkeaa. => binääridata koodataan ASCIIksi siten, ettei siinä esiinny CRLF.CRLF : ää

27.9.2001

44

S: 220 helsinki.fi  
 C: HELO princeton.edu  
 S: 250 Hello princeton.edu  
 C: MAIL FROM: <Bob@princeton.edu>  
 .....  
 S: 250 Message accepted for delivery  
 C: HELO princeton.edu  
 S: 250 Hello princeton.edu  
 C: MAIL FROM: <Alice@princeton.edu>  
 .....  
 S: 250 Message accepted for delivery  
 .....  
 C: QUIT  
 S: 221 princeton.edu closing connection

## Sanoman muoto

<b>To:</b>
CC:
<b>From:</b>
Message-Id:
Received:
Date:
Reply-To:
<b>Subject:</b>

Yleisiä sanoman  
otsakekenttiä  
kentät erotettu  
rivinvaihdolla  
RFC 822 sallii myös omien  
kenttien käytön

27.9.2001

46

## MIME (Multipurpose Internet Mail Extension)

- Alunperin vain tekstisanomia (ASCII)
- nykyisin myös
  - erityyppisiä tekstisanomia
    - Word-dokumentteja
    - kiinankielistä tekstiä
  - ääntä,
  - videota
  - kuvia

27.9.2001

47

## MIME-laajennus

- Lisää kenttiä otsikkoon

MIME-versio:
<b>Content-Transfer-Encoding:</b>
<b>Content-Type:</b>

27.9.2001

48

**From:** alice@crepes.fr  
**To:** bob@hamburger.edu  
**Subject:** Picture of yummy crepe  
**MIME-Version:** 1.0  
**Content-Transfer-Encoding:** base64  
**Content-Type:** image/jpeg  
 (base64 encoded data .....  
 ..... base64 encoded data)

## MIME-sisältötyyppejä

- text/plain; charset=us-ascii
- text/html
- image/gif, image/jpeg, video/mpeg
- application/postscript, application/msword,  
application/octetstream
- **multipart/mixed**

27.9.2001

50

```

Content-Type: multipart/mixed;Boundary=StartOfNextPart
-- StartOfNextPart
Hei Allu,
sinulle kaunis kuva kissastani Villestä.
-- StartOfNextPart
Content-Transfer-Encoding: base64
Content-Type: image/jpeg
base64 encoded data .....
.....base64 encoded data
-- StartOfNextPart
Haluatko muita kuvia!
.

```

- **tyyppien koodaukset siirtoa varten**
  - sähköpostisanomassa saa olla vain ASCII-merkkejä
  - ei esimerkiksi ääkkösiä
- **base64-koodaus**

27.9.2001

52

## Base64-koodaus

- **Sanoman 24 bitin ryhmät jaetaan 6 bitin osiksi, jotka kukin koodataan ASCII-merkiksi => 64 eri vaihtoehtoa**
  - 0-25 = A-Z,
  - 26-51 = a-z,
  - 52-61 = 0-9,
  - 62= +, 63 =/
- Tekstisanoma voidaan koodata myös 7-bitin ASCIIlla.

27.9.2001

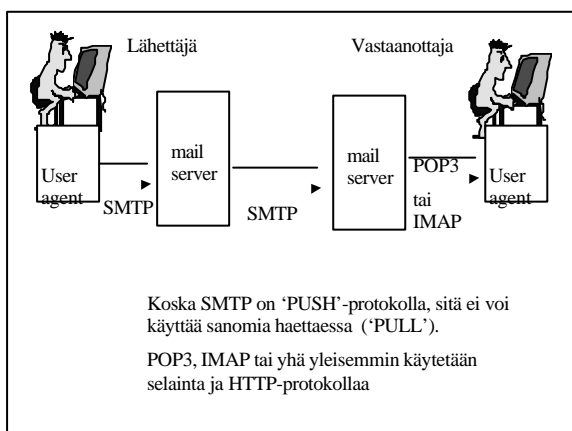
53

## Postinhakuprotokollat (mail access protocols)

- **Käyttäjän postiohjelma siirtää postinhakuprotokollan avulla sanomat postipalvelimen postilaatikoista käyttäjän PC:lle**
  - POP3: yksinkertainen ohjelma, joka siirtää sanomat vastaanottajan PC:lle
  - IMAP: monipuolinen, käyttäjä voi käsitellä postipalvelimen postilaatikkoo kuin se olisi omissa koneessa
- **Entä lähetettäessä?**

27.9.2001

54



## Postiyhdyskäytävä (Mail Gateway)

- **Yleensä postipalvelin ottaa suoraan yhteyttä vastaanottajan postipalvelimeen**
- **välissä voi olla postiyhdyskäytäviä**
  - tallettavat ja toimittavat eteenpäin sanomia
  - yrittävät lähettämistä useita päiviä
  - **Miksi tarvitaan?**
    - ohjaa oikeaan koneeseen: liisa.marttinen@helsinki.fi
    - vastaanottajan kone usein pois päältä

27.9.2001

56

## 2.3. DNS (Domain Name System)

- **Internetin hakemistopalvelu**
- Ihmisten ja ohjelmien käyttämien merkkijonomuotoisten nimien muuttaminen binäärisiksi IP-verkko-osoitteiksi
  - **hydra.cs.helsinki.fi => 218.214.4.29**
- hierarkkinen nimentätapa + hajautettu hakemisto IP-osoitteiden selvittämiseksi
  - **esim. sähköpostiosoitteita, koneiden IP-osoitteita**

27.9.2001

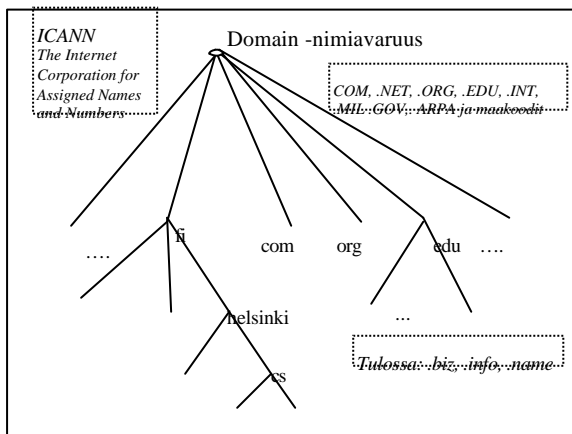
57

## DNS- nimiavaruus

- **Domain (nimihallinta-alue)**
  - maiden tunnuksset
    - fi, fr, de, uk, ...
  - yleiset (yleensä USA)
    - com, edu, gov, int, mil, net, org
  - esimerkkejä:
    - cs.helsinki.fi
    - www.cnn.com
    - www-dept.cs.ucl.ac.u

27.9.2001

58



## IP-nimen selvittäminen

- **sovellusohjelma kutsuu kirjastorutiinia parametrina nimi merkkijonona**
  - esim Unix:ssa `gethostbyname()`
- **kirjastorutiini lähettää UDP-datasähkeen paikalliselle DNS-palvelimelle, joka etsii nimeä vastaavan IP-osoitteen ja palauttaa sen kirjastorutiinille**
  - etsinnässä tarvitaan usein monien palvelimien yhteistyötä

27.9.2001

60

## Nimipalvelimien hierarkia

- **DNS-nimiavaruus jaettu vyöhykkeisiin (zone)**
  - kukin vyöhyke kattaa osan nimipuusta
  - vyöhykkeellä on yksi siitä vastaava nimipalvelija (primary) ja yksi tai useita apunimipalvelijoita (secondary)
- **vyöhykejako on hallinnollinen**
  - tarpeen mukaan nimipalvelijoita vastaamaan omasta alueestaan

27.9.2001

61

## Kysely ensin paikalliselle nimipalvelimelle

- jos nimi on sen vastuulla => **authoritative record**
- jos sillä ei ole mitään tietoa nimestä, se lähettää kyselyn ylimmän tason ns. juurinimipalvelijalle (DNS root server, <http://www.wia.org/pub/rooterv.html>, <ftp://ftp.rs.internic.net/domain/named.root>)
  - esim. Kysely "linda.cs.yale.edu" lähetetään nimipalvelimelle "edu-server.net", joka vastaa vyöhykkeestä "edu".

27.9.2001

62

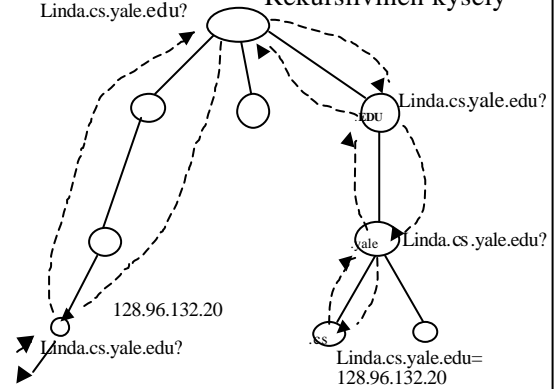
- **Juurinimipalvelin tietää, mikä nimipalvelin on vastuussa kysytystä nimestä**

- tämä on tosin voinut jakaa vastuun joillekin toisille nimipalvelimelle
- mutta tietää, mikä niistä on vastuussa juuri kysytystä nimestä

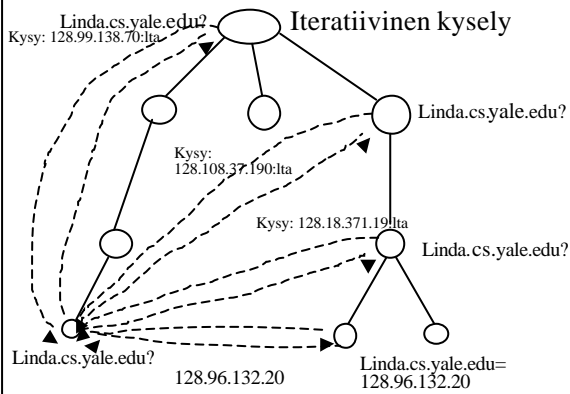
27.9.2001

63

### Rekursiivinen kysely



### Iteratiivinen kysely



### Hakemistotiedot

- **DNS-hakemistotietue (resource record)**

- (nimi, arvo, tyyppi, tietueen elinaika)
- Tyyppi määrää nimen ja arvon merkityksen
  - A-tyyppi
    - koneen domain nimi , arvo on IP-osoite
  - NS-tyyppi
    - domain-nimi, arvo on alueesta vastaavan nimipalvelijan koneen domain-nimi
  - CNAME-tyyppi
    - alias-nimeä vastaava 'kanoninen' nimi
  - MX-tyyppi
    - aliasnimeä vastaava postipalvelin

27.9.2001

66

### DNS-sanomat

Identification	Flags
Number of questions	Number of answers
Number of authority RRs	Number of additional RRs
Questions (name and types for queries)	
Answers (RRs in response to queries)	
Authority (RRs for authoritative servers)	

Additional information

27.9.2001

67

### DNS-välimuisti

- **Suorituskyvyn parantamiseksi nimipalvelijat varastoivat välimuistiinsa DNS-tietueita**
- **ei tarvitse hakea uudestaan**
- **elinaika kertoo voimassaoloajan**

27.9.2001

68