



Aalto-yliopisto
Teknillinen korkeakoulu

Miten Internet toimii

Tuomas Aura

T-110.2100 Johdatus tietoliikenteeseen
kevät 2010

Outline

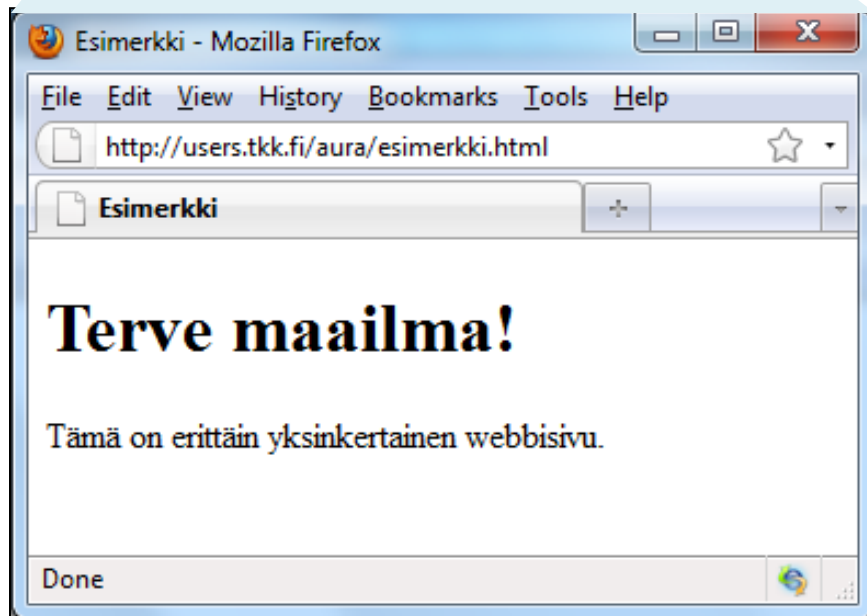
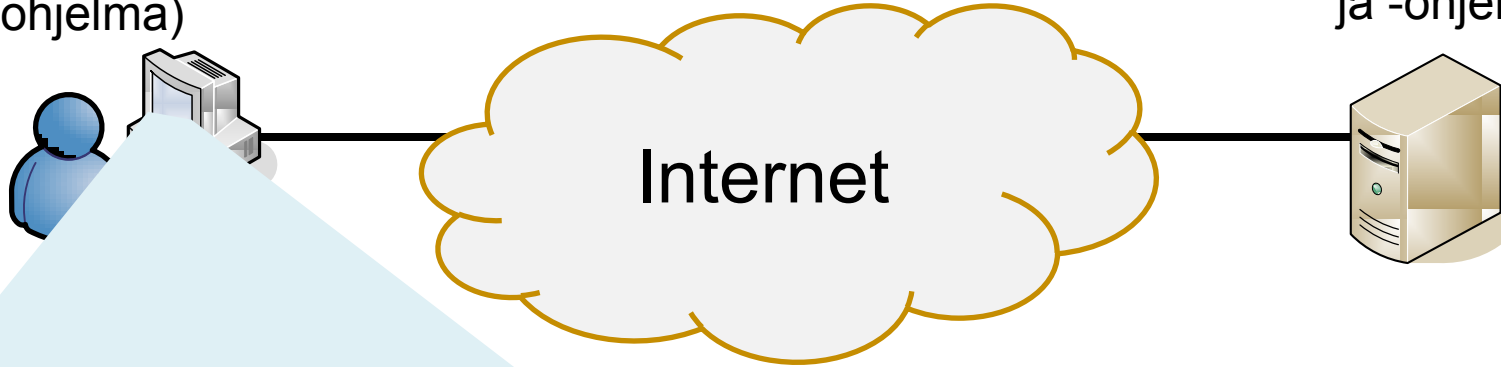
1. Esimerkki 1: nettiselailu
2. Esimerkki 2: sähköposti
3. Internetin protokollapino

ESIMERKKI 1: NETTISELAILU

Asiakas
(käyttäjä,
työasema ja
selainohjelma)

Nettiselailu

Palvelin
(palvelinkone
ja -ohjelma)

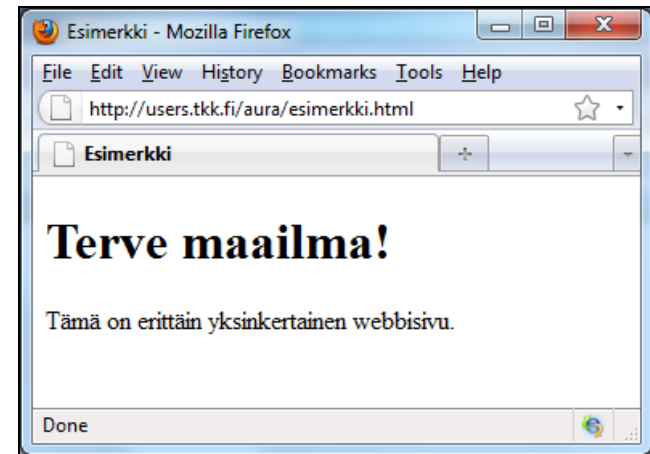


- **Asiakas/palvelin-malli**
- **Nimiarvaruus: URL**

<http://users.tkk.fi/aura/esimerkki.html>

Tiedon muoto

- Tietokoneiden käsittelemä tieto on **määrämuotoista**
- Esim. HTML = hypertekstin merkintäkieli



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
'http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd'>
<html xmlns='http://www.w3.org/1999/xhtml'
xml:lang='fi'>
  <head>
    <title>Esimerkki</title>
  </head>
  <body>
    <!-- Aika simppeliä -->
    <h1>Terve maailma!</h1>
    <p>Tämä on erittäin yksinkertainen webbisivu.</p>
  </body>
</html>
```

Sivun esimerkki.html
lähdekoodi

Protokolla

- Tiedon siirtoon palvelimen ja asiakkaan välillä pitää sopia **yhteyskäytäntö eli protokolla**:
 - lähetettävät viestit ja niiden otsakkeet
 - tilakone: kuka lähettää mitä ja milloin
 - tiedon muoto
 - siirtotie
- Esim. HTTP = hypertekstin siirtoprotokolla
- Protokollista sovitaan **standardointiorganisaatioissa**: IETF, W3C, Oasis, ISO, IEEE, 3GPP, ITU,...

HTTP

Selaimelta palvelimelle:

GET /aura/esimerkki.html HTTP/1.1 ←

Host: users.tkk.fi

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.7) Gecko/20091221 Firefox/3.5.7

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

HTTP-pyyntö

HTTP-pyynnön
otsakkeet

Palvelimelta selaimelle:

HTTP/1.x 200 OK ←

Date: Sun, 17 Jan 2010 12:57:12 GMT

Server: Apache/2.2.9 (Unix)

Last-Modified: Sun, 17 Jan 2010 12:51:31 GMT

Etag: "35ab82-158-47d5bb227dca9:458ab883a0bc0"

Accept-Ranges: bytes

Content-Length: 344

Keep-Alive: timeout=

Connection: Keep-Alive

Content-Type: text/html

HTTP-vastaus

HTTP-vastauksen
otsakkeet

Tyypillinen
asiakas/palvelin-
protokollan
rakenne: pyyntö
ja vastaus

Data(HTML)

<!DOCTYPE html PUBLIC

'http://www.w3.org

<html xmlns='http://

<head>

<title>Esimerkki

</head>

<body>

<!-- Aika simppeä -->

<h1>Terve maailma!</h1>

<p>Tämä on erittäin yksinkertainen verkkosivu.</p>

</body>

</html>

HTTP

Selaimelta palvelimelle:

```
GET /aura/esimerkki.html HTTP/1.1
Host: users.tkk.fi
User-Agent: Mozilla/5.0 (Windows; U; Windo
Accept: text/html,application/xhtml+xml,ap
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;c
Keep-Alive: 300
Connection: keep-alive
```

```
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="fi">
  <head>
    <title>Esimerkki</title>
  </head>
  <body>
    <!-- Aika simppeä -->
    <h1>Terve maailma!</h1>
    <p>Tämä on erittäin yksinkertainen webbisivu.</p>
  </body>
</html>
```

Data (HTML)

HTTP

Selaimella palvelimella:

HTTP/1.x 200 OK

Date: Sun, 17 Jan 2010 12:57:12 GMT

Server: Apache/2.2.9 (Unix)

Last-Modified: Sun, 17 Jan 2010 12:51:31 C

Etag: "35ab82-158-47d5bb227dca9;458ab883a0

Accept-Ranges: bytes

Content-Length: 344

Keep-Alive: timeout=15, max=100

Connection: Keep-Alive

Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1

'http://www.w3.org/TR/xhtml11/DTD/xhtml11

<html xmlns='http://www.w3.org/1999/xhtml

HTTP

Selaimelta palvelimelle:

GET /aura/esimerkki.html HTTP/1.1 ←

Host: users.tkk.fi

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.7) Gecko/20091221 Firefox/3.5.7

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

HTTP-pyyntö

HTTP-pyynnön
otsakkeet

Palvelimelta selaimelle:

HTTP/1.x 200 OK ←

Date: Sun, 17 Jan 2010 12:57:12 GMT

Server: Apache/2.2.9 (Unix)

Last-Modified: Sun, 17 Jan 2010 12:51:31 GMT

Etag: "35ab82-158-47d5bb227dca9;458ab883a0bc0"

Accept-Ranges: bytes

Content-Length: 344

Keep-Alive: timeout=15, max=100

Connection: Keep-Alive

Content-Type: text/html

HTTP-vastaus

HTTP-vastauksen
otsakkeet

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"

'http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd'>

<html xmlns='http://www.w3.org/1999/xhtml' xml:lang='fi'>

<head>

<title>Esimerkki</title>

</head>

<body>

<!-- Aika simppeä -->

<h1>Terve maailma!</h1>

<p>Tämä on erittäin yksinkertainen verkkosivu.</p>

</body>

</html>

Data(HTML)

Siirtoprotokolla

- Kuinka HTTP-protokollan viestit siirretään asiakkaan ja palvelimen välillä?

Vastaus: HTTP käyttää viestien siirtoon
TCP-protokollaa

TCP:n tarjoama palvelu

- TCP toteuttaa **kaksisuuntaisen tavuvirran** asiakkaan ja palvelimen välillä
 - Palvelin odottaa yhteyksiä; asiakas avaa yhteyden
 - Kumpikin kirjoittaa ja lukee tavuja virrasta



- Palvelut on numeroitu: HTTP-palvelinohjelma odottaa yhteyksiä **porttinumeroissa** 80
- **Telnet**-ohjelmalla TCP:tä voi käyttää käsin

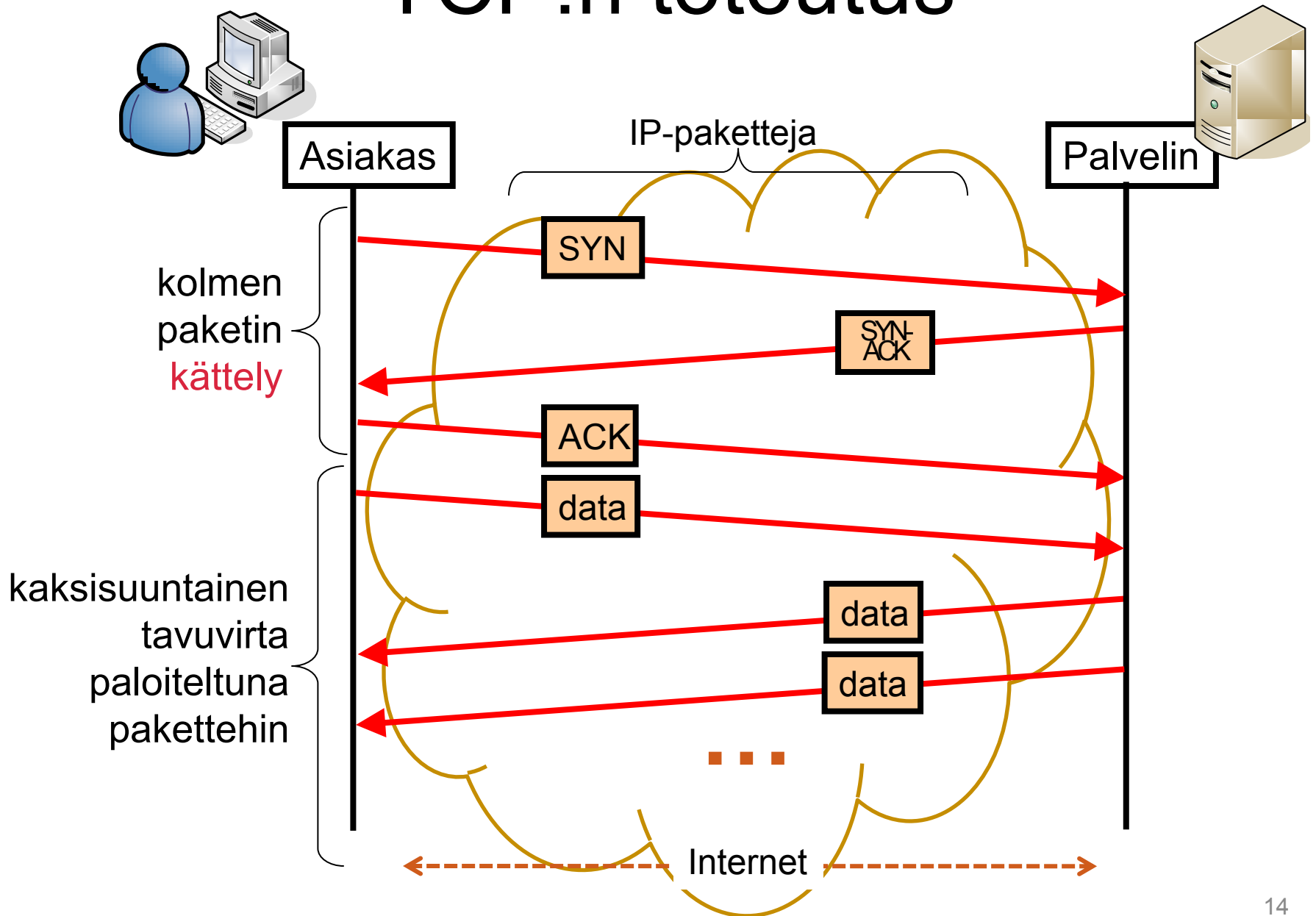
Protokollapino ja rajapinnat

- Miten TCP siirtää tavuvirran asiakkaan ja palvelimen välillä?

Vastaus: TCP jakaa tavuvirran lohkoihin ja lähettää lohkot IP-paketeissa

- Protokollat muodostavat **pinon**, jossa kukin käyttää alemman kerroksen palveluja
 - HTTP käyttää TCP:tä, TCP käyttää IP:tä
- Kerrosten välillä on **rajapinta**
 - TCP **Socket API** — ohjelmointirajapinta sovelluksia varten

TCP:n toteutus



IP:n tarjoama palvelu

- IP siirtää tietopaketteja kahden Internettiin yhdistetyn koneen (host) välillä
 - Paketin koko yleensä alle 1500 tavua
- Kullakin koneella on IP-osoite
 - Esim. 130.233.194.61
- Periaate: Jokaisella koneella on oma IP-osoite ja mikä tahansa kone voi lähettää paketteja mille tahansa koneelle

Paketit verkossa

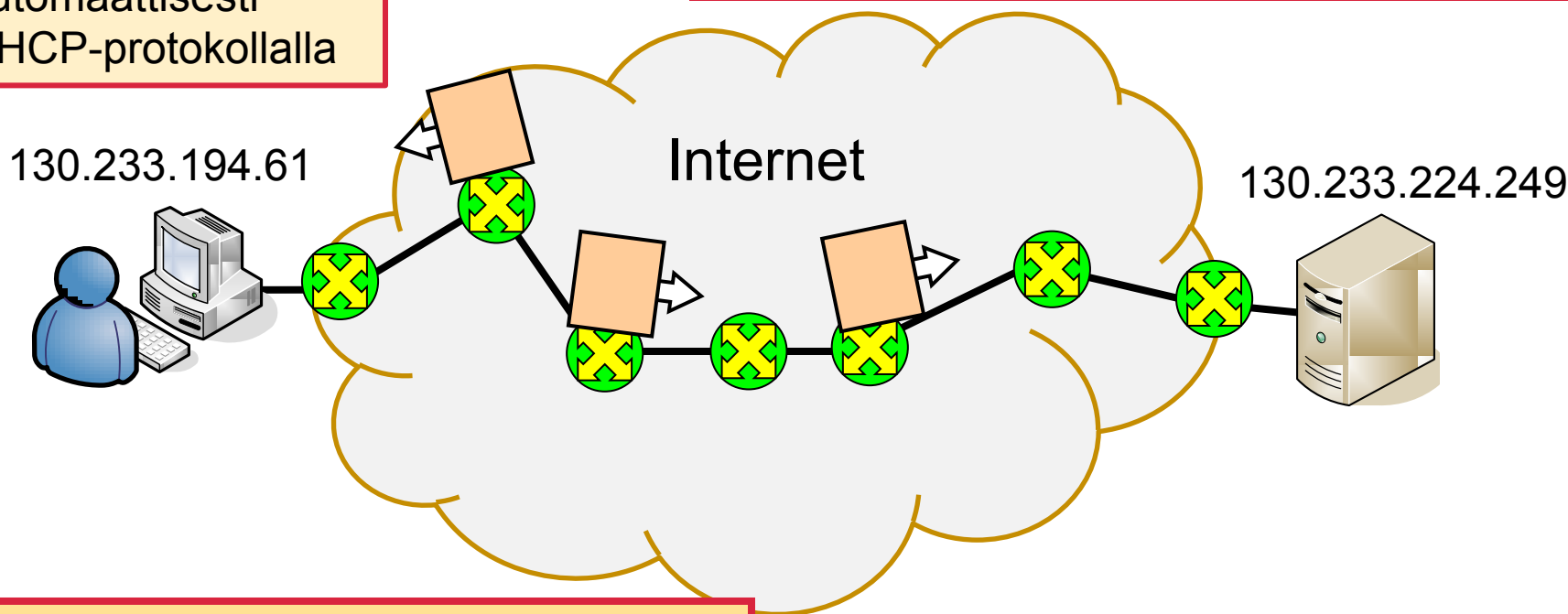
Esimerkin paketit (**Wireshark**):

Time	Source IP	Destination IP	Protocol	Ports	Details
5.722	130.233.194.61	130.233.224.249	TCP	52079 > 80	SYN
5.725	130.233.224.249	130.233.194.61	TCP	80 > 52079	SYN, ACK
5.725	130.233.194.61	130.233.224.249	TCP	52079 > 80	ACK
5.725	130.233.194.61	130.233.224.249	HTTP	52079 > 80	GET /aura/esimerkki.html HTTP/1.1
5.726	130.233.224.249	130.233.194.61	TCP	80 > 52079	ACK
5.737	130.233.224.249	130.233.194.61	HTTP	80/1.1 200	OK (text/html)
5.938	130.233.194.61	130.233.224.249	TCP	52079 > 80	ACK
20.746	130.233.224.249	130.233.194.61	TCP	80 > 52079	FIN, ACK
20.747	130.233.194.61	130.233.224.249	TCP	52079 > 80	ACK
32.521	130.233.194.61	130.233.224.249	TCP	52079 > 80	FIN, ACK
32.522	130.233.224.249	130.233.194.61	TCP	80 > 52079	ACK

IP-reititys

Asiakaskone löytää lähimmän reitittimen ja saa oman IP-osoitteen automaattisesti DHCP-protokollalla

Reitittimet kuljettavat IP-paketteja vastaanottajan IP-osoitteeseen

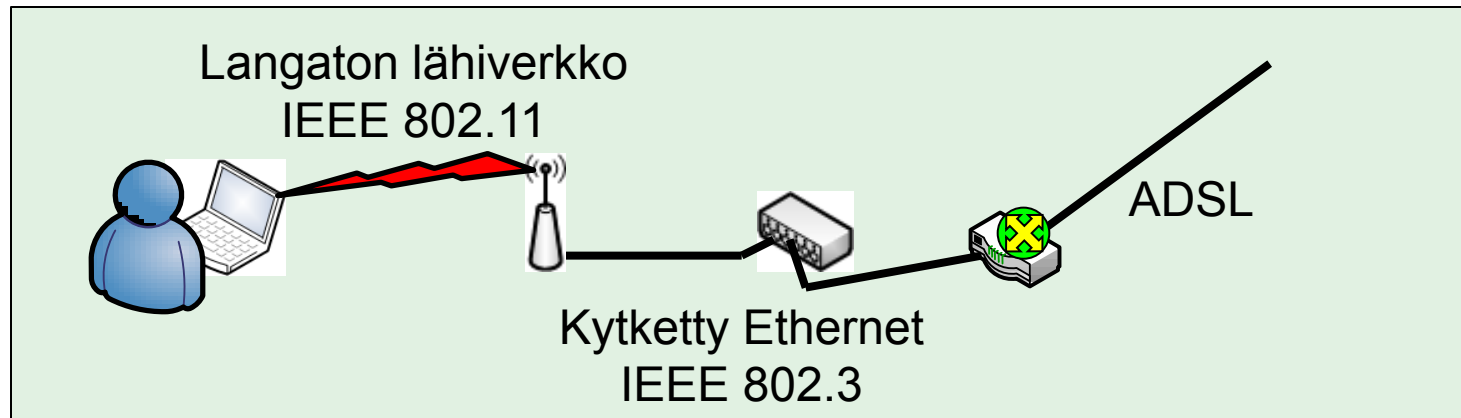


Kunkin koneen tarvitsee tietää vain oma lähin reititin

Linkkikerroksen palvelu

- Miten asiakas- ja palvelinkone siirtävät IP-paketin lähimmälle reitittimelle?
- Miten reititin siirtää tiedon seuraavalle reitittimelle?
- Miten tavut koneen muistista lähetetään fyysisenä signaalina?

Vastaus: **Linkkikerros** toteuttaa IP-pakettien siirron fyysisen linkin yli



Linkkikerroksen toteutus

- Linkkikerros siirtää IP-paketteja fyysisen siirtotien kuten **radioyhteyden, kuparikaapelin tai kuidun** yli
- Kone tai reititin liittyy linkkiin verkkokortilla, jolla on **MAC-osoite**
- IP-paketit kapsuloidaan **kehyksiin**
- Kehysten bitit **koodataan** fyysiseksi signaaliksi
- Linkkikerroksen toteutuksia:
 - Ethernet, WLAN, GPRS
 - DSL, kaapelimodeemi
 - MPLS, ATM

ESIMERKKI 2: SÄHKÖPOSTI

Webmail

<https://webmail.tkk.fi/>

Mail :: Opetus/T-110.4200 Tietoturva - Mozilla Firefox

File Edit View History Bookmarks Tools Help

tkk.fi https://webmail3.tkk.fi/index.php?Horde=41029921573f7c3752d4360b8d6ce093

Mail :: Opetus/T-110.4200 Tietoturva

Open Folder T-110.4200 Tietoturva

Inbox Empty Trash New Message Folders Search Fetch Mail Options Problem Help Log out

Quota status: 337.97MB / 1024.00MB (33.01%)

Opetus/T-110.4200 Tietoturva 1 to 3 of 3 Messages

Select Mark as: Move | Copy Messages to

Delete | Forward | View Messages

	#	Date	From	Subject [Thread]	Size
☐	3	8 Oct 2009	Timo Kiravuo	Re: Laitoin kalvot Noppaan	3 KB
☐	2	6 Oct 2009	Timo Kiravuo	Keskiviikon SSL T1 14-16	3 KB
☐	1	9 Jun 2009	Timo Kiravuo	tietoturva syksy 2009 T-110.4200 kehitysajatuksia	3 KB

Unseen Answered Important Deleted Draft Personal

Done

Dynaaminen HTML

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
```

<!-- Horde: Copyright 2000-2006, The Horde Project. Horde is under the LGPL. -->

```
<!-- Horde Project: http://horde.org/ -->
```

```
<!-- GNU Library Public License: http://www.fsf.org/copyleft/lgpl.html -->
```

```
<html lang="en-US" id="sidebar-frame"><head>
```

```
<script type="text/javascript" src="/js/horde.js?Horde=714099321573f7c375fa436013d6ce093"></script>
```

```
<script type="text/javascript"
```

src="/services/javascript.php?Horde=714099321573f7c375fa436013d6ce093&file=popup.js&app=imp"></script>

```
<script type="text/javascript" src="/js/httpclient.js?Horde=714099321573f7c375fa436013d6ce093"></script>
```

```
<script type="text/javascript" src="/js/hidden.js?Horde=714099321573f7c375fa436013d6ce093"></script>
```

<title>Horde</title>

```
<link href="/themes/graphics/favicon.ico" rel="SHORTCUT ICON" />
```

```
<link href="/themes/screen.css" rel="stylesheet" type="text/css" />
```

```
<link href="/themes/bluwhite/screen.css" rel="stylesheet" type="text/css" />
```

</head>

```
<body class="sidebar">
```

<

<div class="clear"> </div>

</div>

<div id="sidebarPanel">

```
<script type="text/javascript"
```

```
src="/services/javascript.php?Horde=714099321573f7c375fa436013d6ce093&file=tree.js&app=horde"></script>
```

```
<script type="text/javascript">
```

```
n_horde_menu['horde'] = new Array();
```

```
n horde menu['horde']['label'] = 'Horde';
```

```
n horde menu['horde']['expanded'] = ";
```

```
n_horde_menu['horde']['url'] = '/login.php?Horde=714099321573f7c375fa436013d6ce093';
```

```
n horde menu['horde']['icon'] = '/themes/graphics/horde.png';
```

```

n_borde = menu["borde"]["condic"] = ""

```

Otteita palvelun webmail.tkk.fi
-lähdekoodista

Dynaaminen HTML

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
```

```
<!-- Horde: Copyright 2000-2006, The Horde Project. Horde is under the LGPL. -->
```

```
<!-- Horde Project: http://horde.org/ -->
```

```
<!-- GNU Library Public License: http://www.fsf.org/copyleft/lgpl.html -->
```

```
<html lang="en-US" id="sidebar-frame"><head>
```

```
<script type="text/javascript" src="/js/horde.js?Horde=714099321573f7c375fa436013d6ce093"></script>
```

```
<script type="text/javascript" src="/js/horde.js?Horde=714099321573f7c375fa436013d6ce093"></script>
```

```
src="/services/javascript.php?Horde=714099321573f7c375fa436013d6ce093&file=tree.js&app=horde"></script>
```

```
<script type="text/javascript" src="/js/hideable.js?Horde=714099321573f7c375fa436013d6ce093"></script>
```

```
<script type="text/javascript" src="/js/hideable.js?Horde=714099321573f7c375fa436013d6ce093"></script>
```

```
<title>Horde</title>
```

```
<link href="/themes/graphics/favicon.ico" rel="SHORTCUT ICON" />
```

```
<link href="/themes/screen.css" rel="stylesheet" type="text/css" />
```

```
<link href="/themes/bluewhite/screen.css" rel="stylesheet" type="text/css" />
```

```
</head>
```

```
<body class="sidebar">
```

```
<div id="expandedSidebar" style="overflow:hidden">
```

```
<div id="menu" style="overflow:hidden">
```

```
<span class="leftFloat" id="themelogo">
```

```
&nbsp; </span>
```

```
<span class="leftFloat" id="logopad">&nbsp; </span>
```

```
<div class="clear">&nbsp; </div>
```

```
</div>
```

```
<span id="expandButton" class="rightFloat"><a href="#" onclick="toggleMenuFrame(); return false;" title="Collapse Sidebar"></span>
```

```
<div id="sidebarPanel">
```

```
<script type="text/javascript">
```

```
src="/services/javascript.php?Horde=714099321573f7c375fa436013d6ce093&file=tree.js&app=horde"></script>
```

```
<script type="text/javascript">
```

```
n_horde = 0;
n_horde = 0;
n_horde = 0;
n_horde = 0;
n_horde = 0;
n_horde = 0;
```

```
var extraColsLeft = 0;
```

```
var extraColsRight = 0;
```

```
var n_horde_menu = new Array();
```

Otteita palvelun webmail.tkk.fi
-lähdekoodista

- Nykyaikaiset verkkosivut ovat interaktiivisia Javascript-ohjelmia, jotka kommunikoivat käyttäjän ja palvelimen kanssa

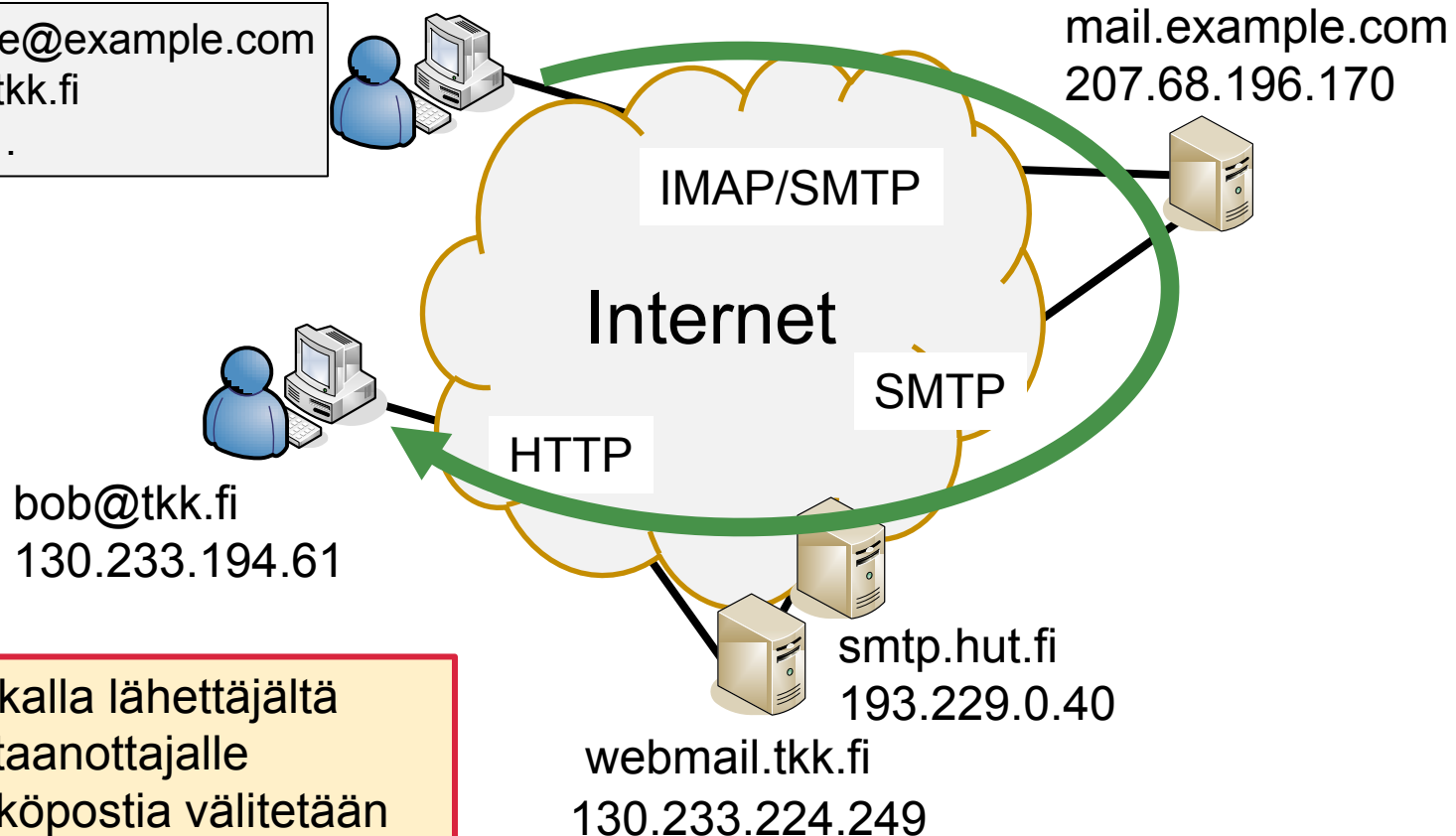
```
onclick="toggleMenuFrame(); return false;"
```

Internetin sähköposti

alice@example.com
192.168.1.33

mail.example.com
207.68.196.170

From: alice@example.com
To: bob@tkk.fi
Subject: ...



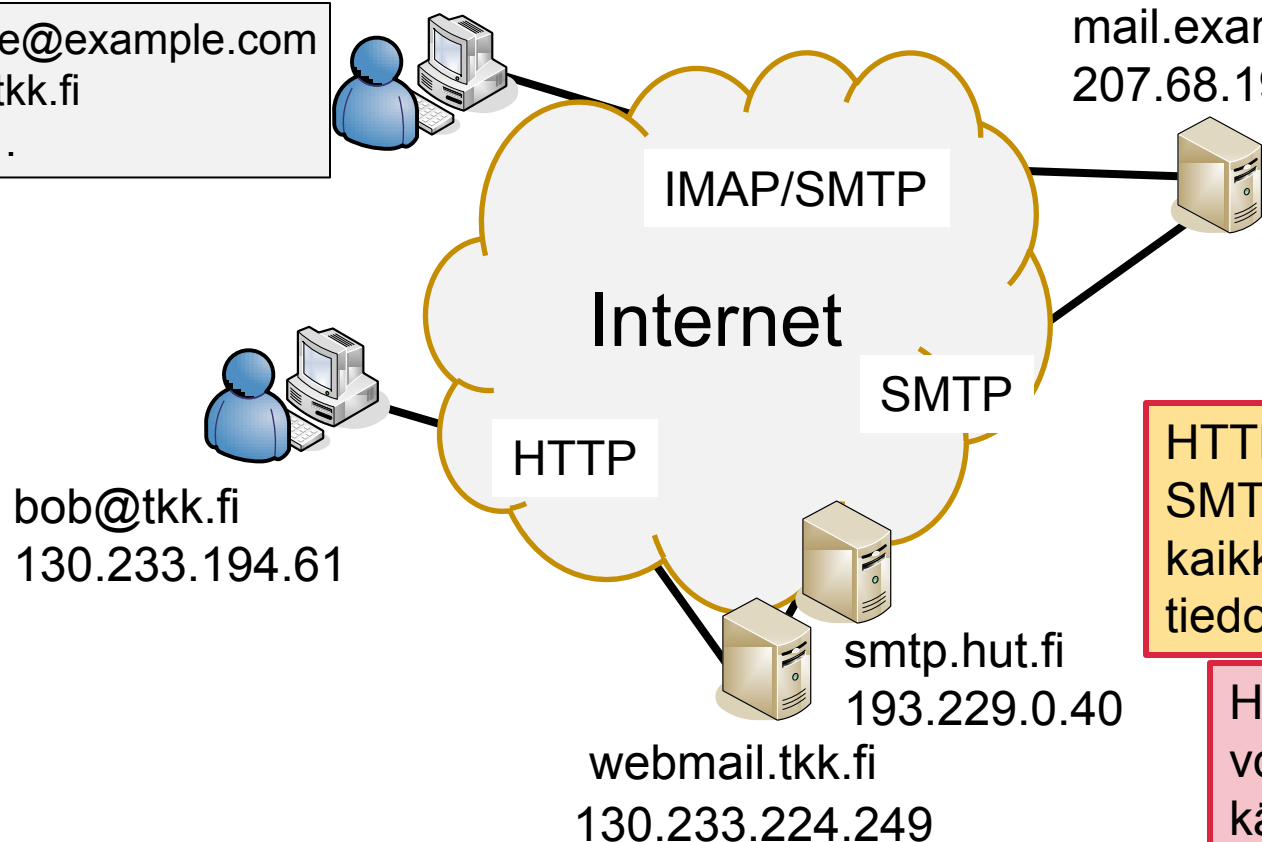
Matkalla lähettäjältä vastaanottajalle sähköpostia välitetään useilla eri protokollilla useiden eri koneiden ja organisaatioiden välillä

Internetin sähköposti

alice@example.com
192.168.1.33

mail.example.com
207.68.196.170

From: alice@example.com
To: bob@tkk.fi
Subject: ...



HTTP, IMAP ja SMTP käyttävät kaikki TCP:tä tiedon siirtoon

HTTP ja IMAP voidaan suojata käyttämällä SSL:ää

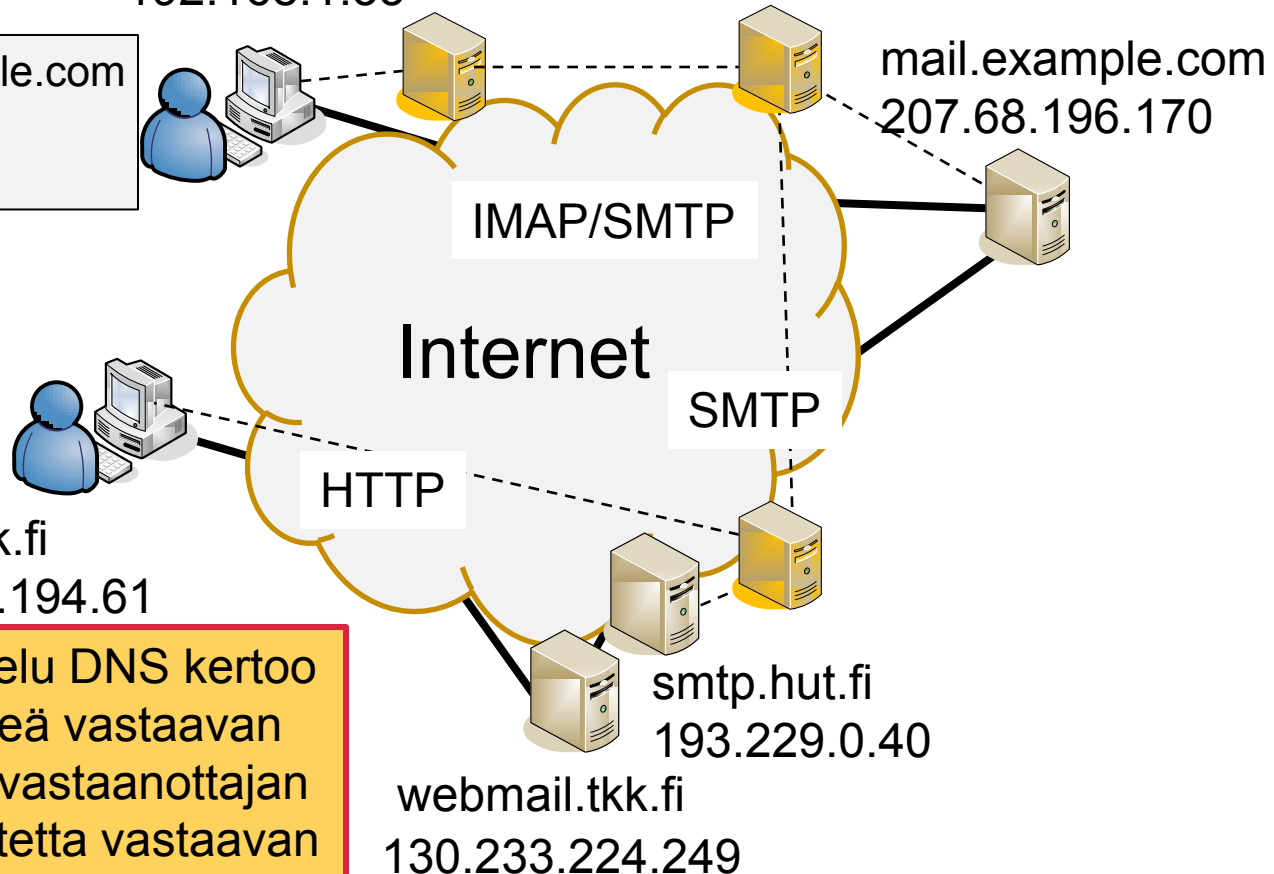
Tietoturva

- Siirrettävän tiedon luottamuksellisuus ja aitous voidaan suojata kryptografisesti
- HTTP^S tarkoittaa, että tieto asiakkaan ja palvelimen välillä on salattu ja todennettu SSL-protokollalla
 - SSL tarjoaa sovelluksille rajapinnan *turvalliseen* tavuvirran siirtoon
 - SSL käyttää tavuvirran siirtoon TCP:tä

Internetin sähköposti

alice@example.com
192.168.1.33

From: alice@example.com
To: bob@tkk.fi
Subject: ...



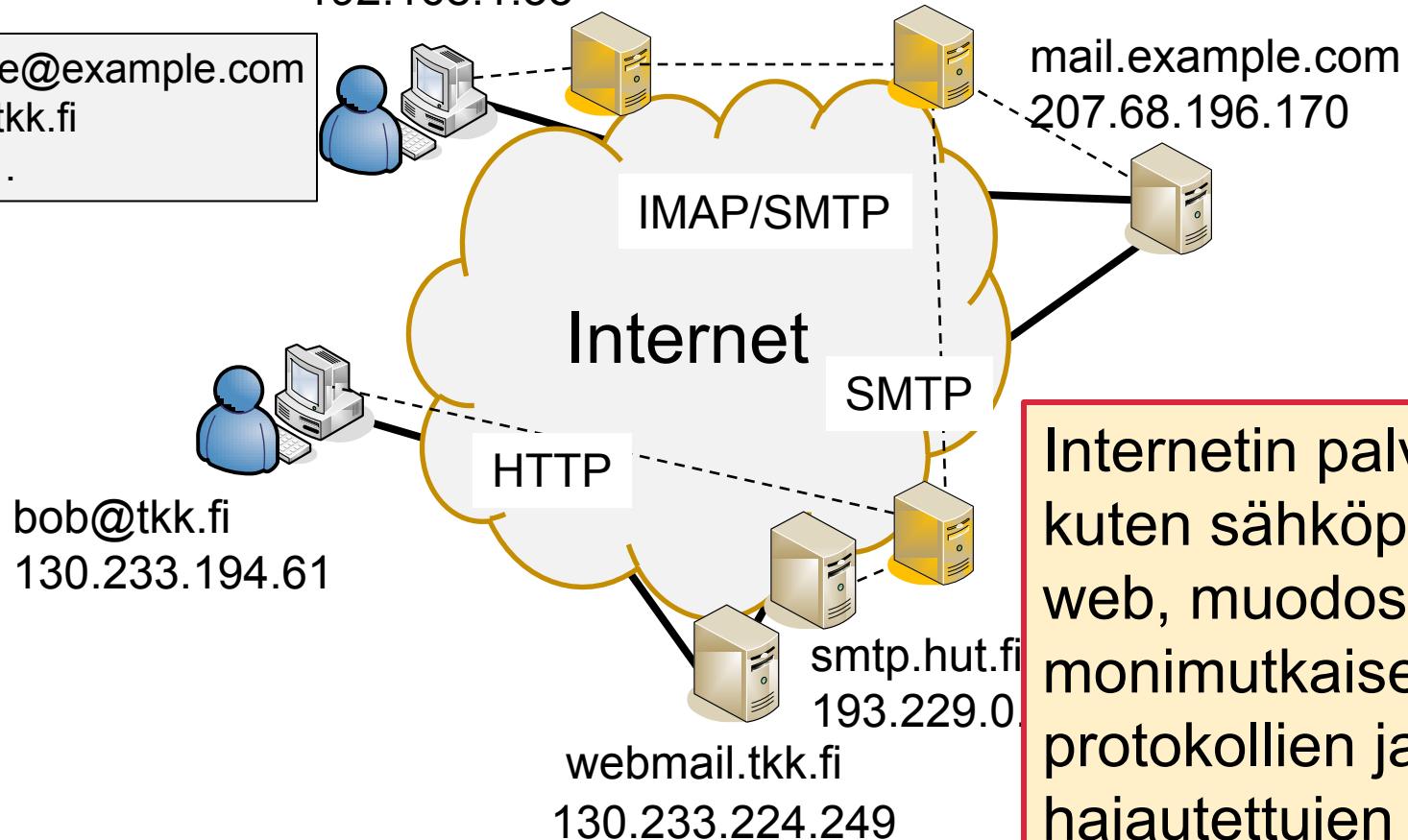
Hakemistopalvelu DNS kertoo palvelimen nimeä vastaavan IP-osoitteen ja vastaanottajan sähköpostiosoitetta vastaavan SMTP-palvelimen nimen

DNS-protokolla ei käytä sanomiensa siirtoon TCP:tä vaan UDP:tä

Internetin sähköposti

alice@example.com
192.168.1.33

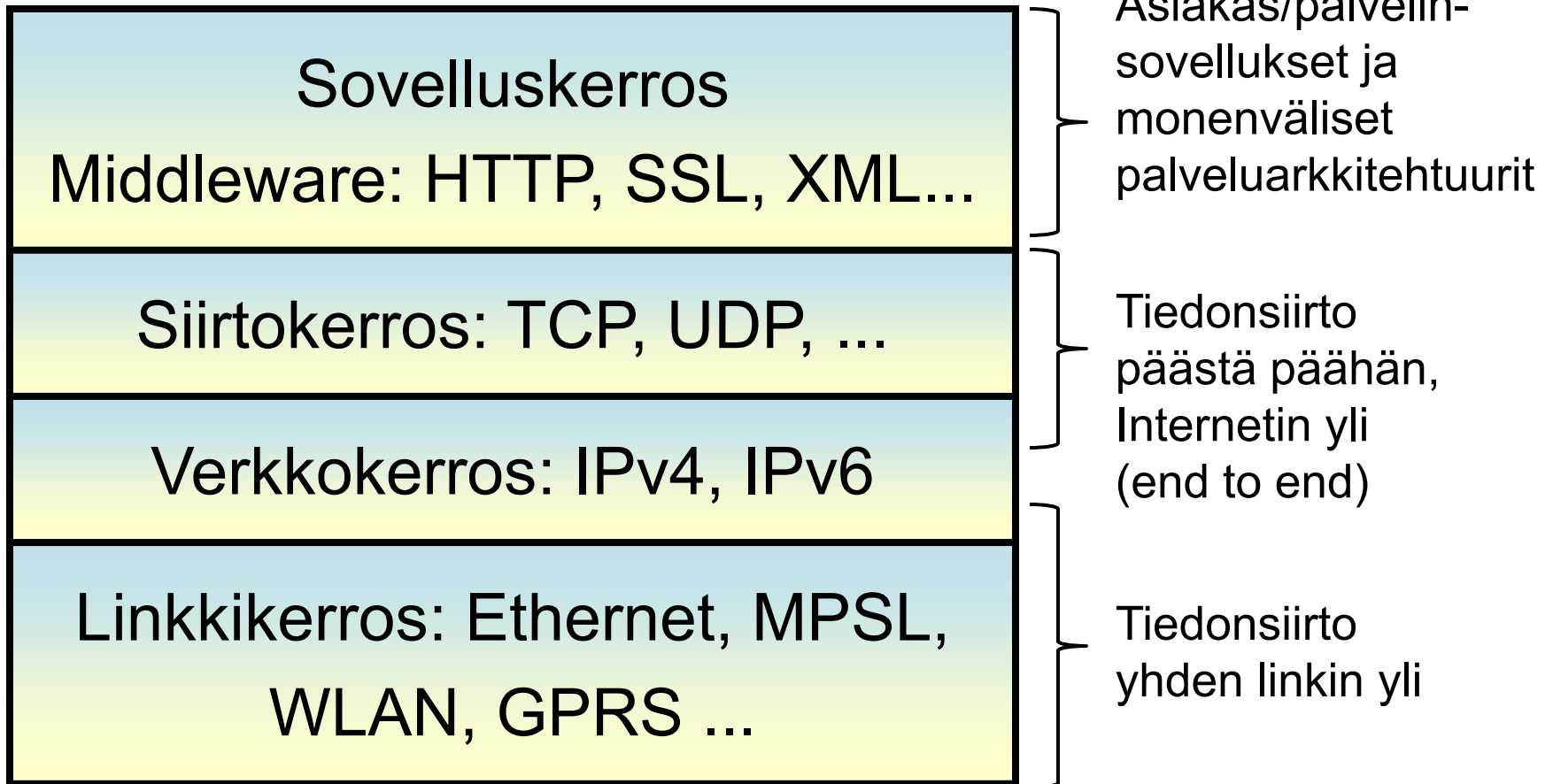
From: alice@example.com
To: bob@tkk.fi
Subject: ...



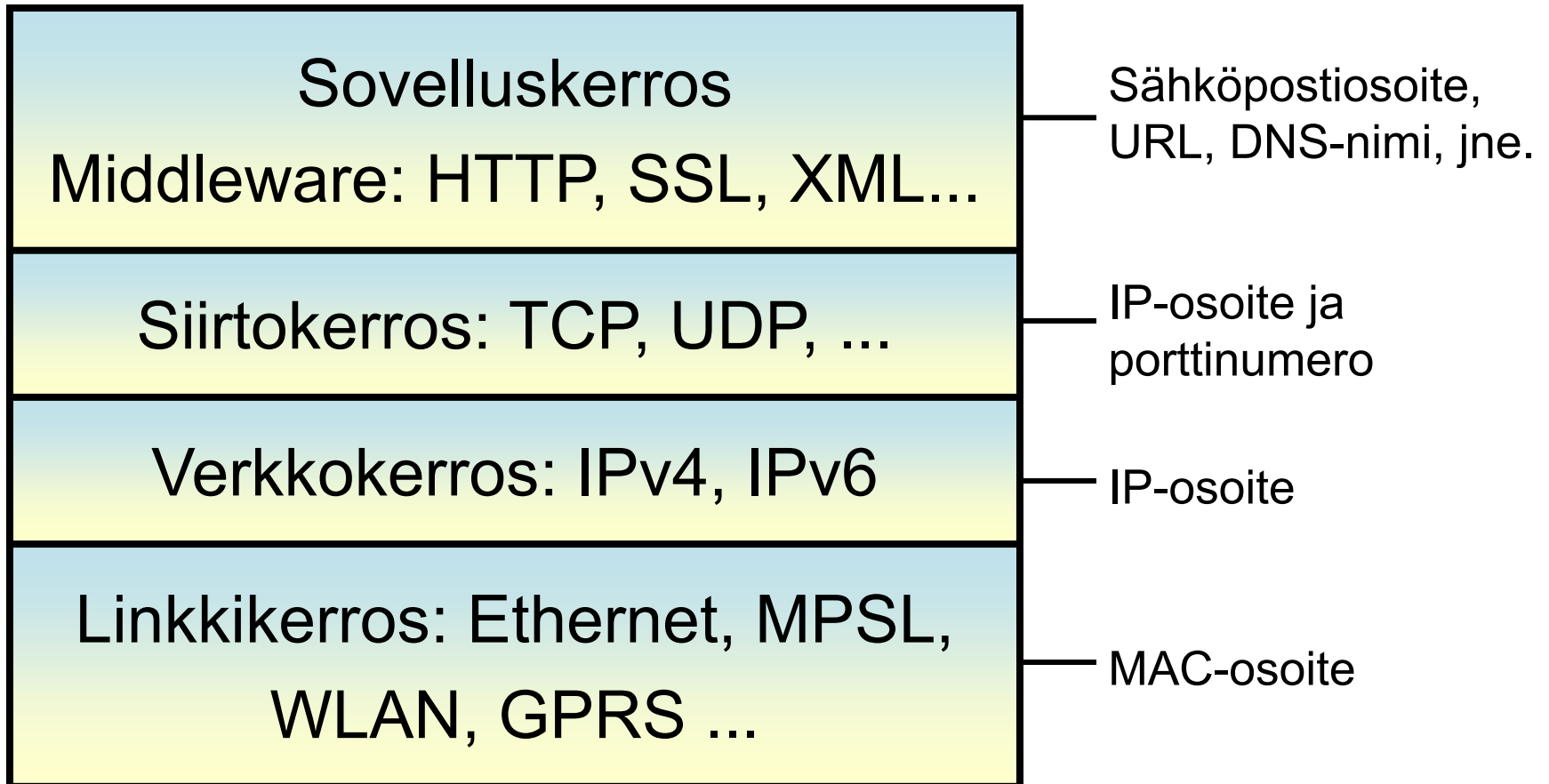
Internetin palvelut, kuten sähköposti ja web, muodostavat monimutkaisen protokollien ja hajautettujen palvelinten vyyhdin

INTERNET-PROTOKOLLAPINO

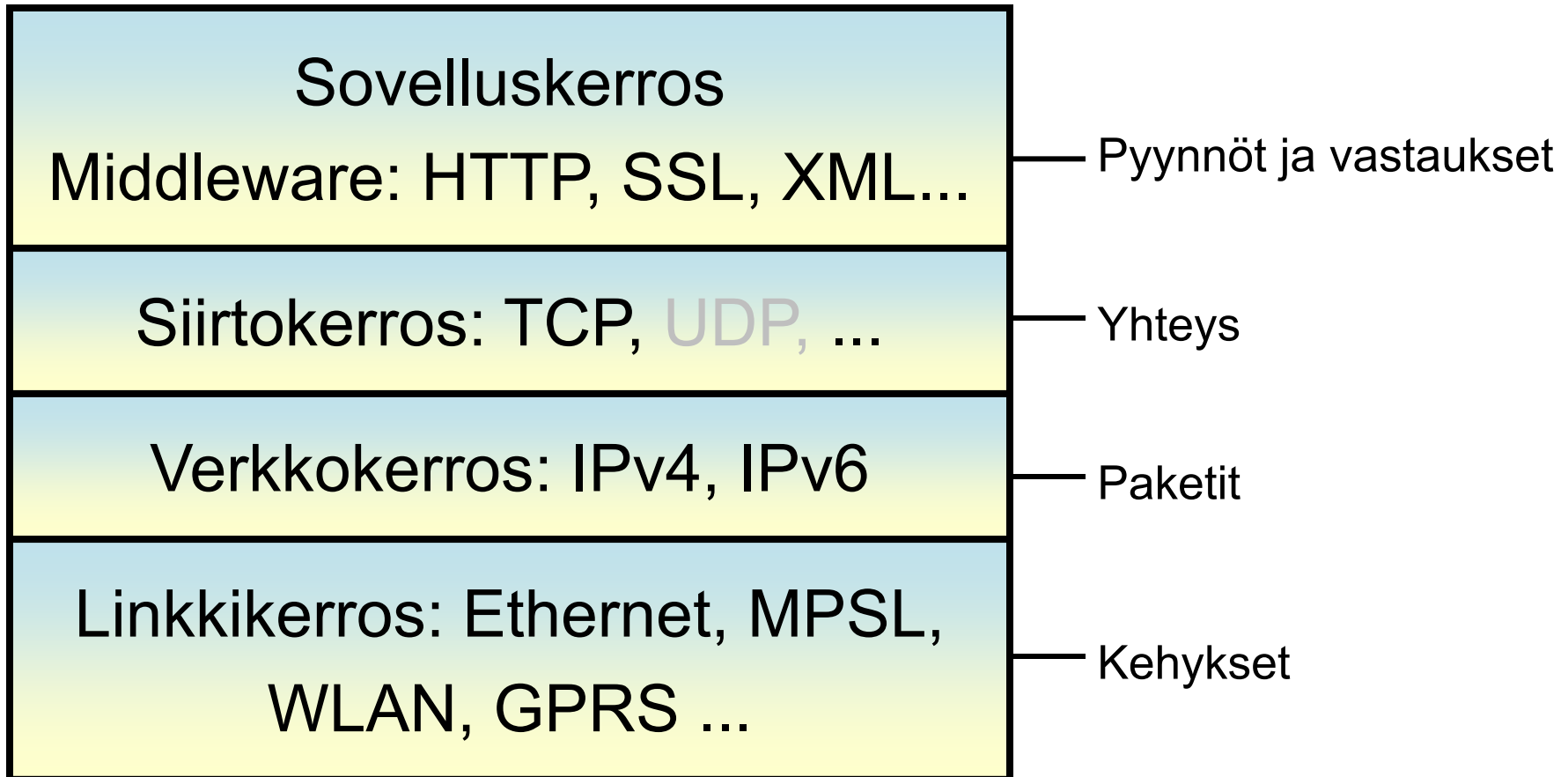
TCP/IP-protokollapino



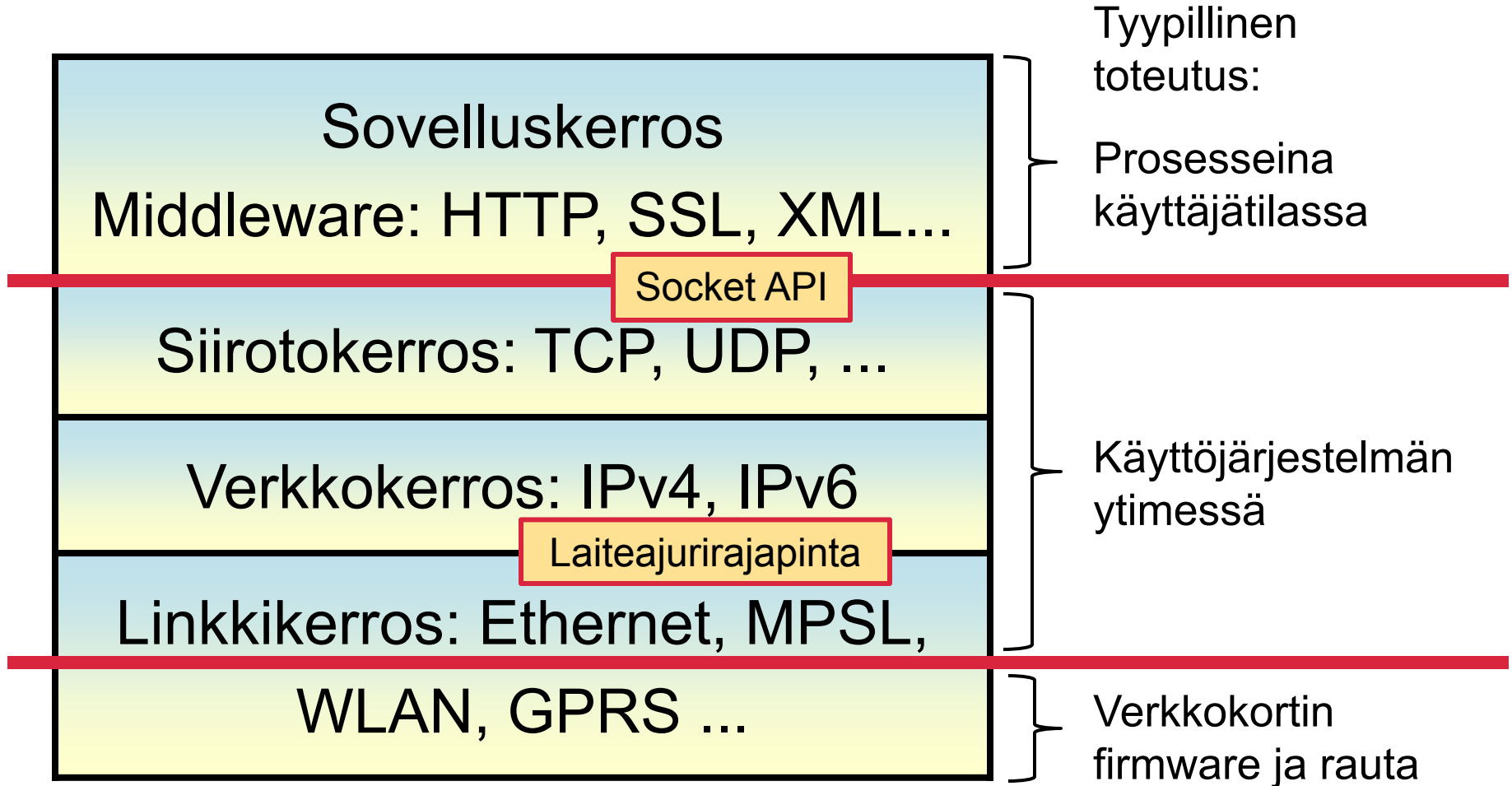
Nimiavaruudet



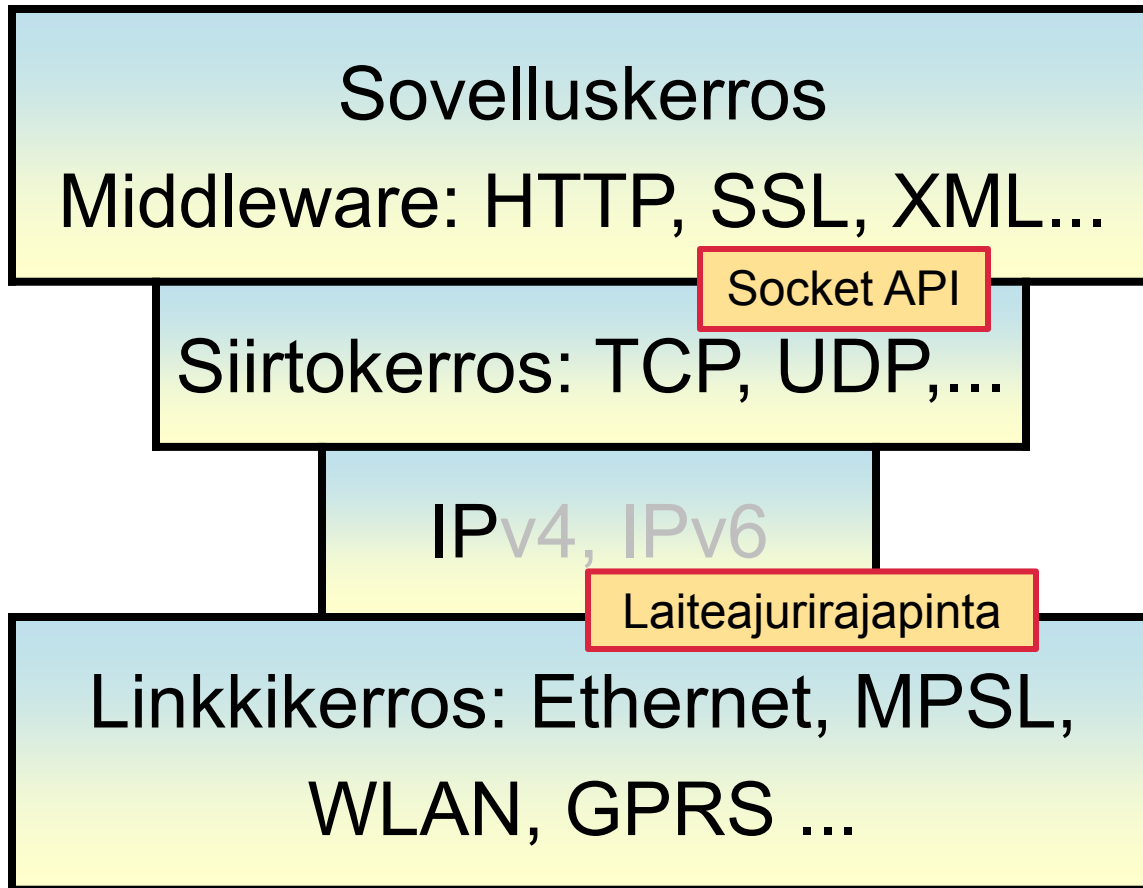
Viestien muoto



Toteutus ja rajapinnat



Tiimalasimalli



Alun perin vain yksi verkkokerroksen protokolla ja kaksi siirtokerroksen protokollaa

Rajapinnat tekevät uusien sovellusten ja linkkityyppien lisäämisen helpoksi

Kurssin luennot

- Aloitus: Miten Internet toimii, Tuomas Aura
- Web 2.0 ja uudet sovellustekniikat, Tancred Lindholm
- Sovelluskerros: WWW, email, socket API, Tancred Lindholm
- Tietoturvan perusteet, Tuomas Aura
- Salaustekniikat, Tuomas Aura
- Kuljetuskerros, TCP, Matti Siekkinen
- Verkkokerros, IP, Matti Siekkinen
- Linkkikerros, Ethernet ja WLAN, N.N.
- Tiedonsiirron perusteet, N.N.
- Puhelinverkot, Antti Ylä-Jääski
- Soluverkot, Antti Ylä-Jääski
- Tele- ja tietoverkon laskutus, Sakari Luukkainen
- Liiketoiminta verkkoympäristössä, Sakari Luukkainen
- Yhteenveto/kertaus, Antti Ylä-Jääski ja Tuomas Aura