

OH2MP Mikko (översättning OH6NT):

## Hur fungerar e-posten?

E-post förmedlas i Internet med hjälp av protokollet SMTP (simple mail transfer protocol, ett slags överenskommet språk). När man sänder e-post, tar **den sändande datorn** kontakt till **e-postserverns** port nr. 25 med hjälp av protokollet TCP (transfer control protocol). Sedan "pratar" den SMTP med servern och e-posten far iväg. I normala fall är e-postservern inte den slutgiltiga mottagaren, utan då tar den med hjälp av MX-information från namntjänstens server reda på till vilken server posten skall skickas vidare.

### Så går SMTP-sessionen:

När den sändande datorn öppnar förbindelsen till e-postservern, säger denna nånting om sig själv, t.ex.:

```
220 post.server.tjingtjong.fi ESMTP Postfix
```

I varje SMTP-svar från servern finns det ett nummer i början som berättar vilket innehåll meddelandet har. Siffror används av samma orsak som i övriga protokoll; de är lättare att läsa maskinellt. 220 i exemplet ovan är en hälsningsfras. Resten av innehållet på raden är serverns namn, protokollet den anser att skall användas (i detta fall ESMTP, dvs. Extended SMTP, en utökad variant). och möjligen serverprogrammets namn och version.

Sedan säger den sändande datorn:

```
HELO min.datamaskin.fi
```

Datorn berättar sitt namn för postservern, eller något annat om den vill ljuga. Det är inte förbjudet att ljuga, även om serverns underhållare i detta skede kunde förbjuda ljugande. I det fallet kunde tyvärr även nyttopost förbli olevererad. Servern svarar genom att hälsa:

```
250 post.server.tjingtjong.fi Hello min.datamaskin.fi
```

Sedan börjar den sändande maskinen den egentliga postförsändelsen:

```
MAIL FROM:<vemsohelst@varsohelst.com>
```

```
250 Ok
```

Den innehåller först avsändarens adress. Den kan också vara falsk, den har endast som uppgift att fungera som returadress ifall posten inte kan levereras eller för felmeddelanden. Servern svarar OK igen.

Här gäller det att observera att denna uppgift inte behöver vara den samma som finns i postens From: -fält. Adressen som ges här ingår i meddelandets första rad efter ordet From (utan kolon) och före datumet. Detta kallas för "Envelope sender" ("kuvertets avsändare") och eventuella returer och felmeddelanden sänds till denna adress om meddelandet inte kan levereras.

Sedan säger den sändande datorn:

```
RCPT TO:<mottag.are@naanstans.fi>
```

```
250 Ok
```

Detta är den adress dit meddelandet levereras. Om servern har tillåtelse att leverera post till den uppgivna adressen svarar den Ok och levererar posten vidare. Om inte, så

svarar den med något felmeddelande. Svaret kan innehålla flera rader om meddelandet har flera mottagare. Mottagarna kan även svara med felmeddelanden, om t.ex. mottagarens adress inte existerar, eller meddelandet av andra orsaker inte kan tas emot. Då returneras meddelandet till avsändaren tillsammans med ett felmeddelande.

Sedan säger den sändande datorn DATA, och då svarar servern okay, låt komma och avsluta meddelandet med en rad som innehåller endast en punkt::

DATA

```
354 End data with <CR><LF>.<CR><LF>
```

Då sänder den sändande datorn alla rubrikrader (headers) och meddelandets innehåll. Mailservern bryr sig inte om innehållet, detta är bara innehåll som inte påverkar postgången på något sätt. T.ex. kan From: eller To: -fälten innehålla **vad som helst**. De kan tom. saknas helt, och ändå förfar man enligt reglerna. Detta betyder att man inte kan lita på innehållet i dessa fält, liksom inte på något annat heller gällande innehållet. Man ska komma ihåg att e-posten utvecklades på den tiden när användarna var närmast endast professorer och forskare vid universiteten. Då fanns inga virusfabrikanter eller spammakare som var till besvär, och det fanns inte någon, ur säkerhetssynpunkt emmentalostiknande, fönsterbaserad niddbild av ett operativsystem från Redmond fullt med säkerhetshål. Om man vill ha säkerhet i e-posthaneringen bör man använda något underskrifts- eller krypteringsprogram, t.ex. PGP.

När meddelandet avslutas med en rad som bara innehåller en punkt, svarar servern:

```
250 Ok
```

När alla meddelanden är översända avslutas förbindelsen till servern med meddelandet QUIT och servern svarar med BYE och TCP-förbindelsen bryts:

QUIT

```
221 Bye
```

Innan servern förmedlar meddelandet vidare till mottagares inbox eller till en annan e-postserver lägger den till en Received-rad blanda meddelandets rubriker (headers). Om man vill granska postgången utgående från dessa headers, skall de alltså läsas i bakvänd ordning. T.ex. i denna session lades följande rubrikrad till:

```
Received: from min.datamaskin.fi [123.123.123.123]
        by post.server.tjingtjong.fi; Mon, 20 Oct 2007 20:00:00 +0300
```

Ibland kan Received-headern innehålla tilläggsinformation, t.ex. ett ID som särskiljer meddelandet eller serverprogrammets namn och versionsnummer. Observera att header-rader som inleds med mellanslag eller tabulator hör till föregående rad. I allmänhet anges i Received-headern den sändande maskinens IP-adress (i exemplet den påhitade adressen 123.123.123.123) som meddelandet mottogs ifrån. Således är det möjligt att utreda den verkliga källan t.ex. för skräppost, fast avsändaren i HELO-meddelandet ljuger om sin adress, eftersom den sändande maskinen finns på den sparade IP-adressen.

## Tilläggsuppgifter

- <http://www.ietf.org/rfc/rfc2821.txt> - definition av SMTP