

Internettechnologie MAIL

Les 5 17/10/2019

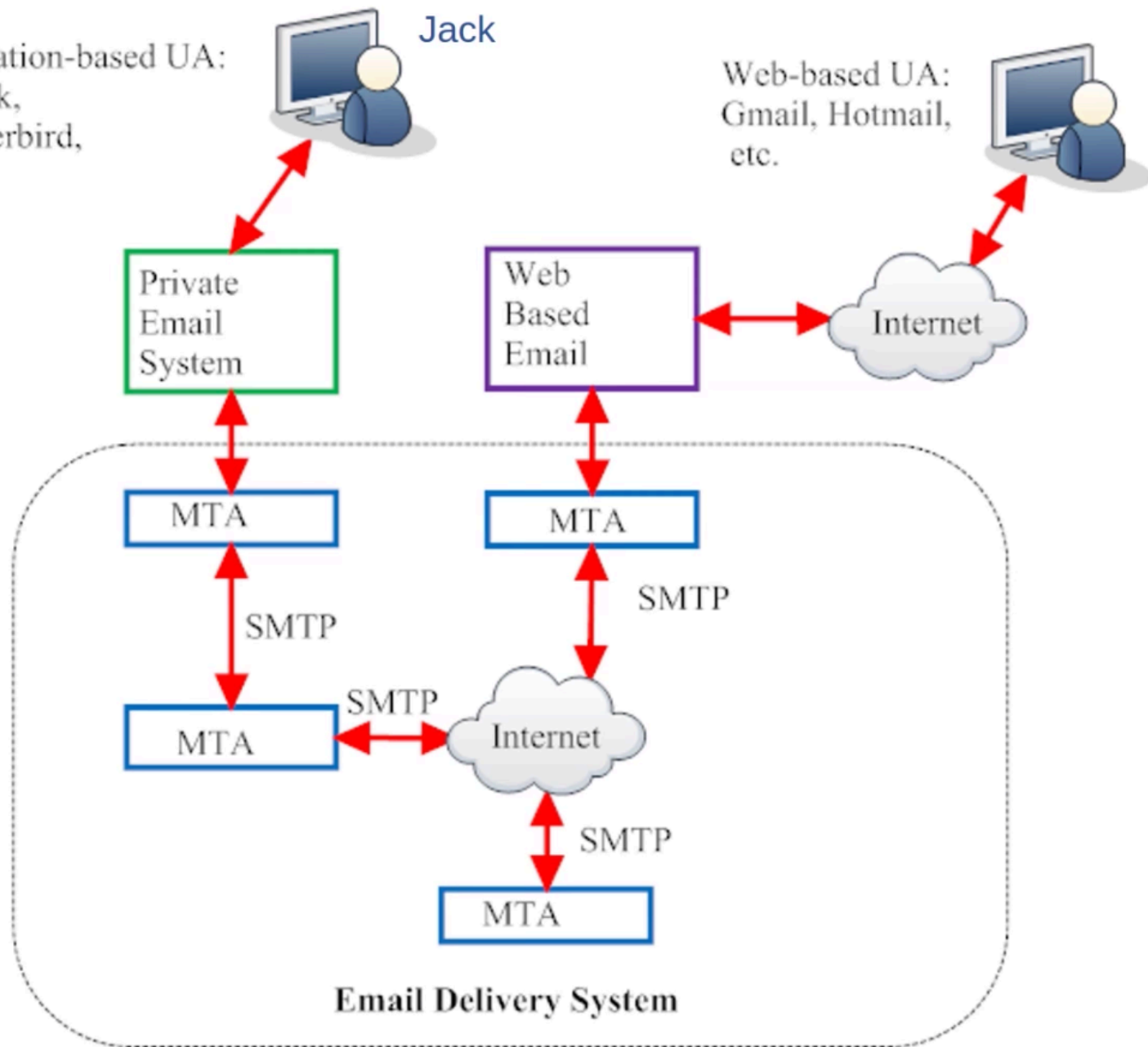
M.DIMA



Application-based UA:
Outlook,
Thunderbird,
etc.

Jack

Web-based UA:
Gmail, Hotmail,
etc.



Wat is een mda?

MDA staat voor Mail Delivery Agent (ook bekend als Local Delivery Agent, LDA). Het gaat om software die de lokale aflevering (niet het versturen) van e-mailberichten op je server aan e-mailadressen op die server verzorgt. Een MDA heeft als het ware de rol van postbode en een MTA de rol van het postkantoor.

[DirectAdmin](#)-, [Plesk](#)- en [cPanel](#)-VPS'en komen vaak standaard met Dovecot als MDA (en [MTA](#)).

De meest gebruikte MDA's zijn:

- [Microsoft Exchange Server](#)
- Dovecot (Linux)

Enkel Microsoft Exchange Server kan worden gebruikt voor zowel het versturen als ontvangen van e-mail. Voor het versturen wordt bij Linux gebruik gemaakt van een MTA zoals Exim of Postfix.

Wat is een mta?

Een MTA (Mail Transfer Agent) is software die het **versturen** van e-mailberichten verzorgt van de ene computer, naar een andere computer. Je kunt een MTA zien als een postkantoor voor e-mail, waarbij een **MDA** de rol van postbode heeft. Andere termen waaronder vaak MTA's worden aangeduid zijn mail servers of mail exchangers.

De meest gebruikte MTA's zijn:

- **Microsoft Exchange Server**
- Postfix
- Exim
- Sendmail

De laatste drie worden gebruikt voor Linux voor het versturen van e-mail. DirectAdmin en cPanel gebruiken Exim en Plesk Postfix. Van de bovenstaande MTA's zorgt enkel Microsoft Exchange Server voor zowel het versturen (MTA) als ontvangen (MDA) van e-mail. Voor ontvangst wordt doorgaans een aparte MDA gebruikt.

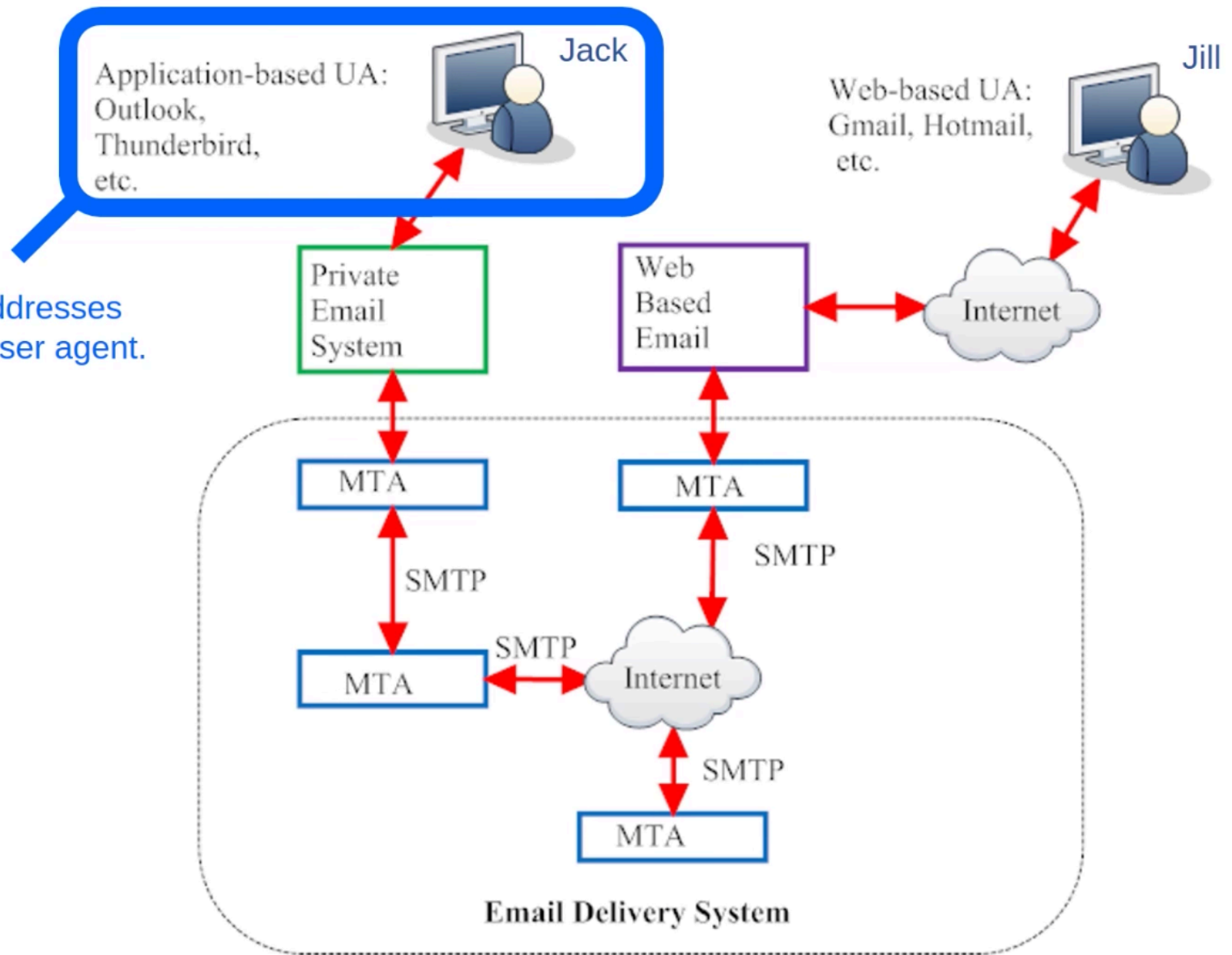
mta vervolg

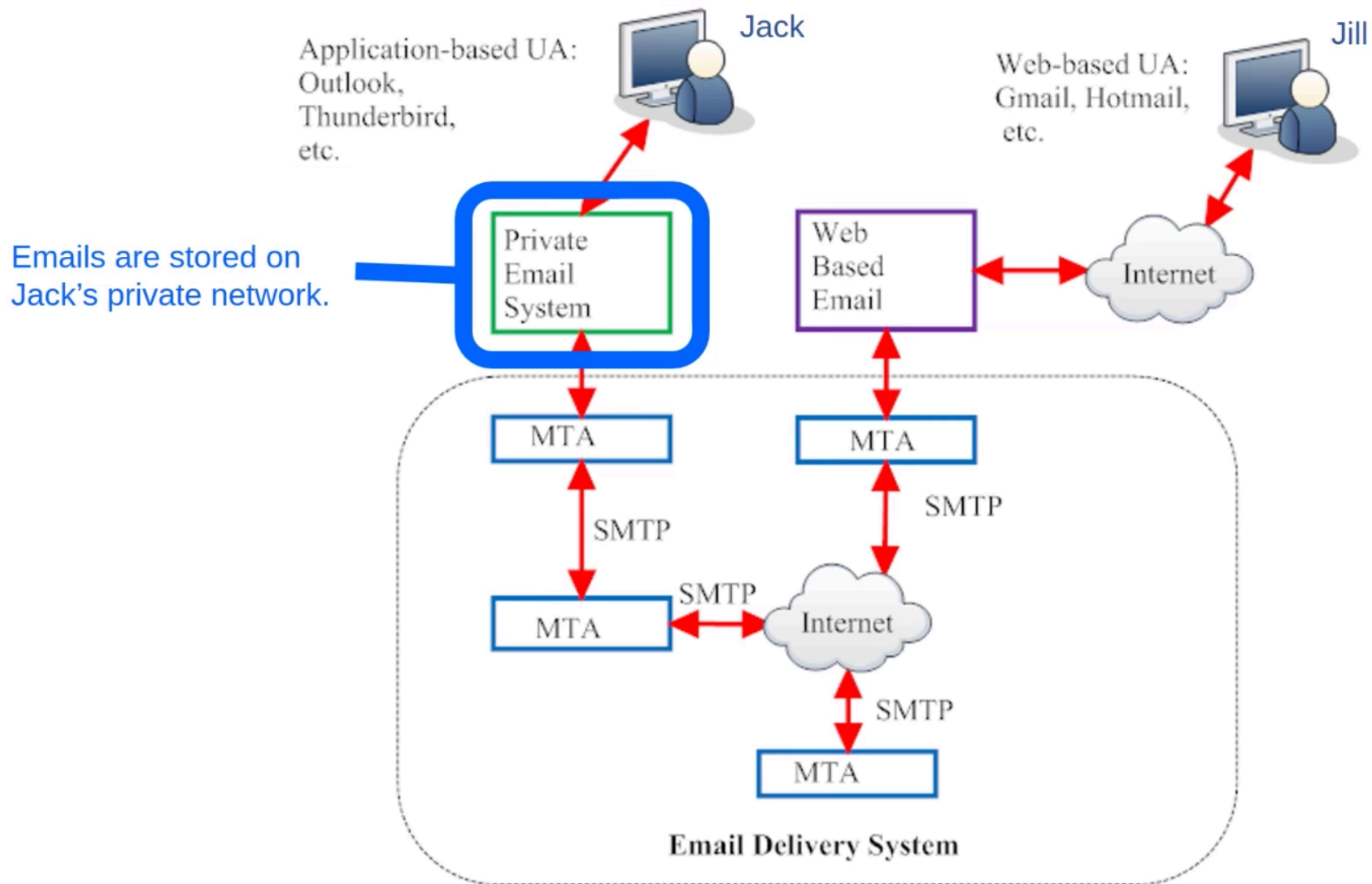
De VPS-mailservice

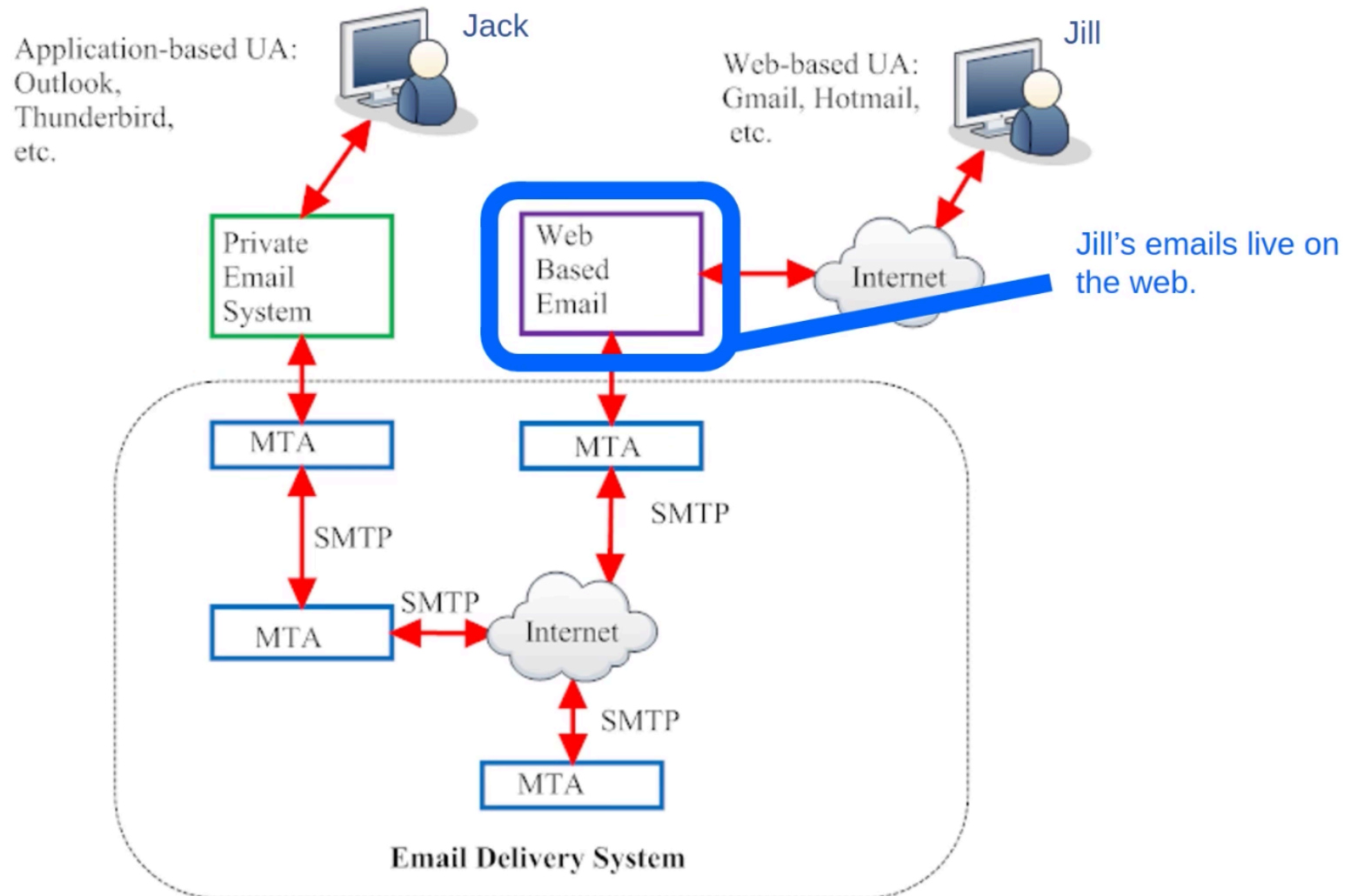
Een [VPS-mailservice](#) is geen MTA en kan **niet** op zichzelf mail versturen. Om de VPS-mailservice te gebruiken is dus een MTA nodig.

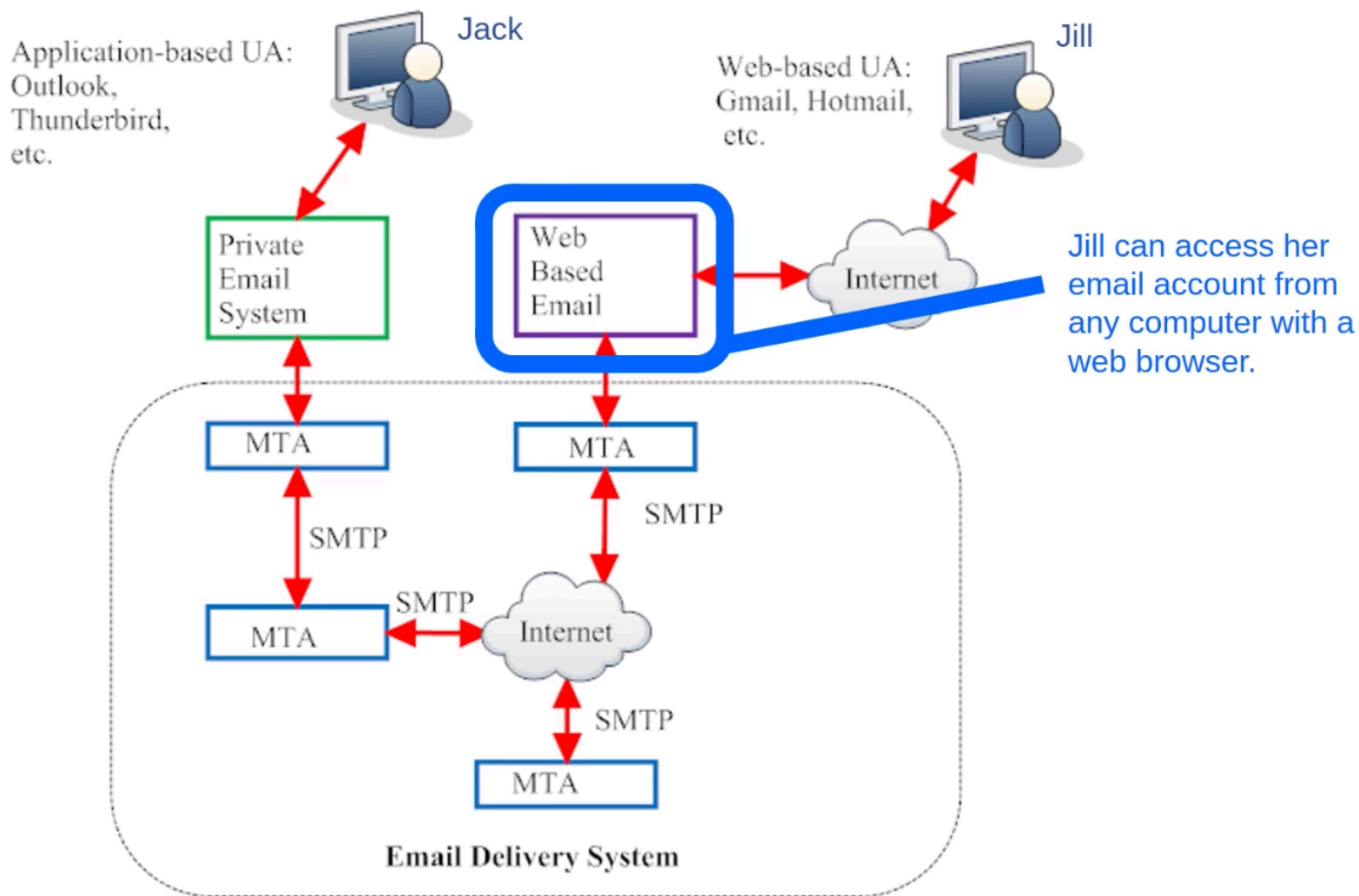
[DirectAdmin](#)-, [Plesk](#)- en [cPanel](#)-VPS'en komen vaak standaard met een MTA en [MDA](#) (Mail Delivery Agent). Voor alle losstaande OS'en moet een MTA eerst geïnstalleerd en geconfigureerd worden.

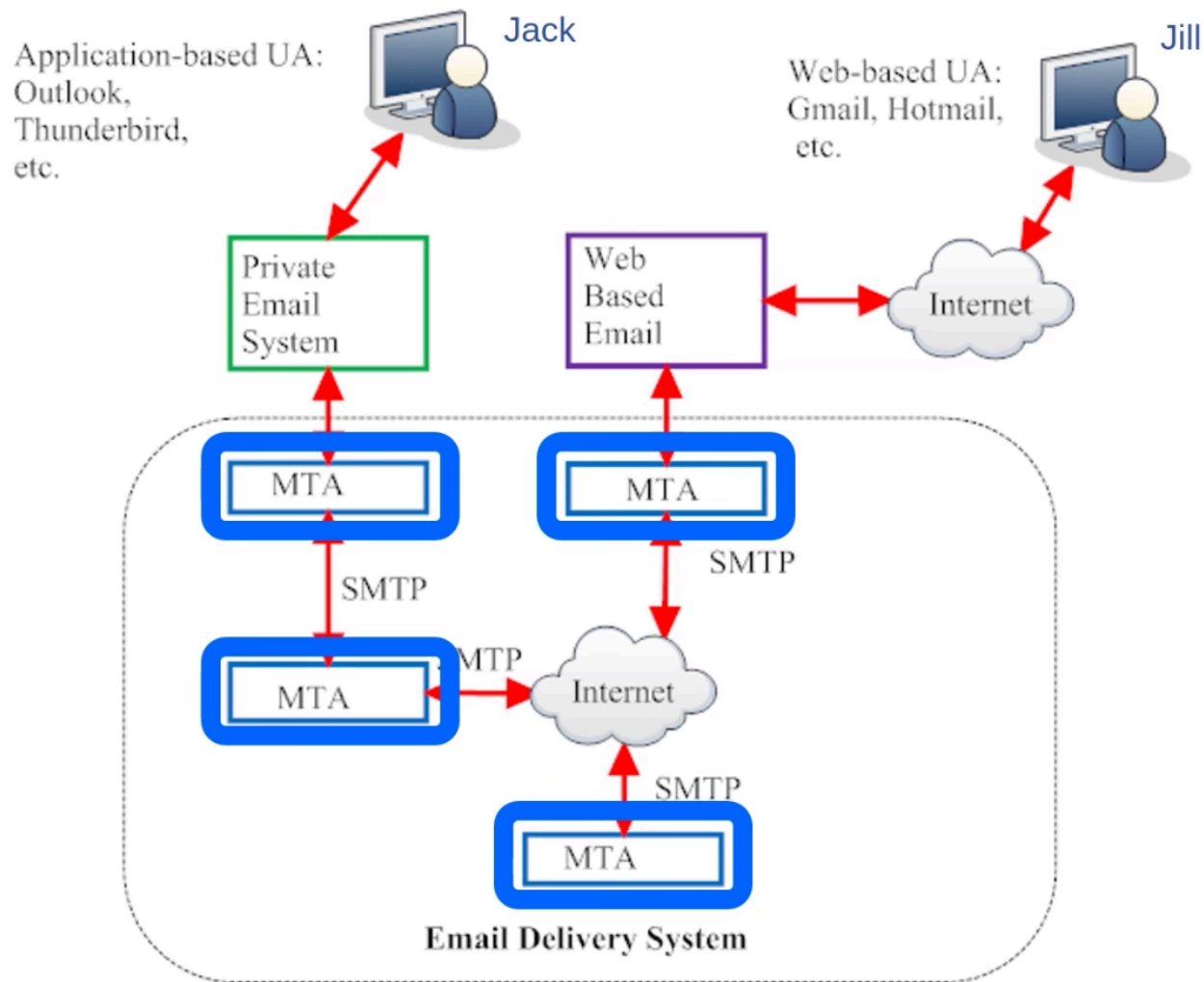
Writes and addresses message in user agent.

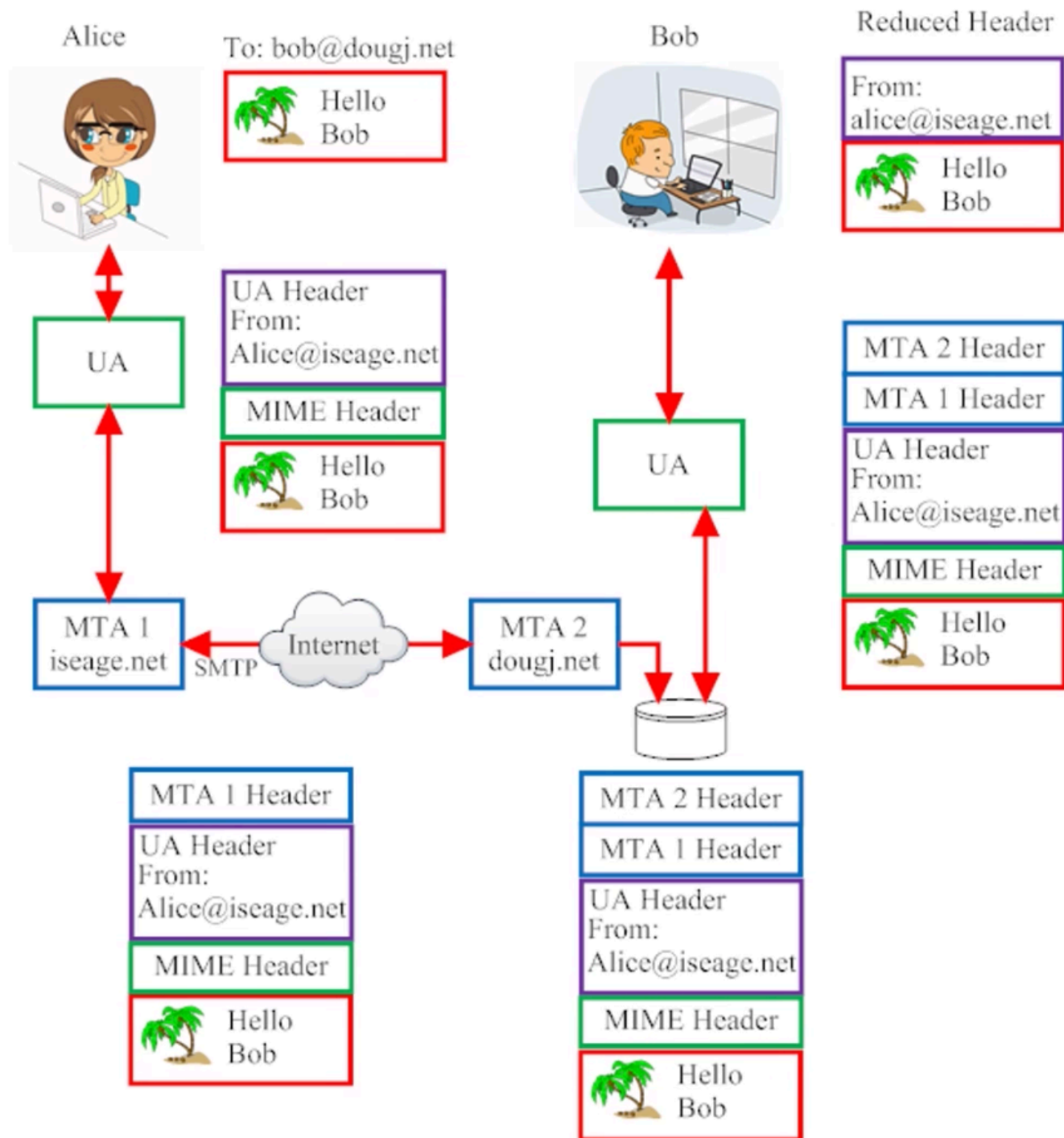












E-mail Headers

From: Media Temple user (mt.kb.user@gmail.com)
Subject: article: How to Trace a Email
Date: January 25, 2011 3:30:58 PM PDT
To: user@example.com
Return-Path: <mt.kb.user@gmail.com>
Envelope-To: user@example.com
Delivery-Date: Tue, 25 Jan 2011 15:31:01 -0700
Received: from po-out-1718.google.com ([72.14.252.155]:54907) by cl35.gs01.gridserver.com with esmtp (Exim 4.63) (envelope-from <mt.kb.user@gmail.com>) id 1KDoNH-0000f0-RL for user@example.com; Tue, 25 Jan 2011 15:31:01 -0700
Received: by po-out-1718.google.com with SMTP id y22so795146pof.4 for <user@example.com>; Tue, 25 Jan 2011 15:30:58 -0700 (PDT)
Received: by 10.141.116.17 with SMTP id t17mr3929916rvm.251.1214951458741; Tue, 25 Jan 2011 15:30:58 -0700 (PDT)
Received: by **10.140.188.3** with HTTP; Tue, 25 Jan 2011 15:30:58 -0700 (PDT)
Dkim-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=gamma; h=domainkey-signature:received:received:message-id:date:from:to :subject:mime-version:content-type; bh=+JqkmVt+sHDFIGX5jKp3oP18LQf10VQjAmZAKl1lspY=; b=F87jySDZnMayyitVxLdHcQNL073DytKRyRh84GNsl24IRNakn0oOfrC2luliNvdea LGTk3adlrzt+N96GyMseWz8T9xE6O/sAl16db48q4lqkd7uOiDvFsvS3CUQINhybNw8m CH/o8eELTN0zbSbn5Trp0dkRYXhMX8FTAwrH0=
Domainkey-Signature: a=rsa-sha1; c=noews; d=gmail.com; s=gamma; h=message-id:date:from:to:subject:mime-version:content-type; b=wkbBj0M8NCUIbol6idKooejg0sL2ms7fDPe1tHUKR9Ht0qr5IAJX4q9PMVJeyjWalH 36n4qGLtC2euBJY070bVra8IBB9FeDEW9C35BC1vuPT5XyucCm0hulbE86+uiUTXCkaB 6ykquzQGCEr7xPacMJqVfXDkHo3H61HM9oCQM=
Message-Id: <c8f49cec0807011530k11196ad4p7cb4b9420f2ae752@mail.gmail.com>
Mime-Version: 1.0
Content-Type: multipart/alternative; boundary="----=_Part_3927_12044027.1214951458678"
X-Spam-Status: score=3.7 tests=DNS_FROM_RFC_POST, HTML_00_10, HTML_MESSAGE, HTML_SHORT_LENGTH version=3.1.7
X-Spam-Level: ***
Message Body: This is a KnowledgeBase article that provides information on how to find email headers and use the data to trace a email.

<https://mediatemple.net/community/products/dv/204643950/understanding-an-email-header>

From

- This displays who the message is from, however, this can be easily forged and can be the least reliable.

Subject

- This is what the sender placed as a topic of the email content.

Date

- This shows the date and time the email message was composed.

To

- This shows to whom the message was addressed, but may not contain the recipient's address.

Return-Path

- The email address for return mail. This is the same as "Reply-To:".

Envelope-To

- This header shows that this email was delivered to the mailbox of a subscriber whose email address is user@example.com.

Delivery Date

- This shows the date and time at which the email was received by your (mt) service or email client.

Received

- The received is the most important part of the email header and is usually the most reliable. They form a list of all the servers/computers through which the message traveled in order to reach you. The received lines are best read from bottom to top. That is, the first "Received:" line is your own system or mail server. The last "Received:" line is where the mail originated. Each mail system has their own style of "Received:" line. A "Received:" line typically identifies the machine that received the mail and the machine from which the mail was received.
Dkim-Signature & Domainkey-Signature
- These are related to domain keys which are currently not supported by (mt) Media Temple services. You can learn more about these by visiting: <http://en.wikipedia.org/wiki/DomainKeys>.

Message-id

- A unique string assigned by the mail system when the message is first created. These can easily be forged.

Mime-Version

- Multipurpose Internet Mail Extensions (MIME) is an [Internet standard](http://en.wikipedia.org/wiki/MIME) that extends the format of [email](#). Please see <http://en.wikipedia.org/wiki/MIME> for more details.

Content-Type

- Generally, this will tell you the format of the message, such as html or plaintext.

X-Spam-Status

- Displays a spam score created by your service or mail client.

X-Spam-Level

- Displays a spam score usually created by your service or mail client.

Message Body

- This is the actual content of the email itself, written by the sender.



Enkele begrippen

Spoofing: de headers aanpassen zodat het lijkt alsof de mail van iemand anders komt

MUA: Mail user agent (programma om mail binnen te halen bv Outlook, Thunderbird)

SMTP: Simple Mail Transfer Protocol. Protocol dat gebruikt onder de MTA's om met elkaar te communiceren.

MTA: Mail transfer agent: mail server. bv. Sendmail, Postfix, Exchange, Qmail

MDA: Mail delivery agent: programma dat de mails routeert. Meestal gekoppeld aan MTA.

MIME: Multipurpose Internet Mail Extensions. Is een internet standaard dat formaat van mail uitbreidt. (niet enkel tekst)

POP3: Post Office Protocol

IMAP: Interactive Mail Access Protocol

MX-Record: Een MX-record (Mail eXchange-record) is een gegevenstype in het Domain Name System (DNS). Het bevat de naam van de computer die e-mailverkeer voor het betreffende domein afhandelt.

Ontvangen en versturen

SMTP: mail versturen -> draait op poort 25 (465) bv smtp.telenet.be,
smtp.gmail.com

POP3: mail ontvangen -> draait op poort 110 (995), geen encryptie, mail wordt gedownload bv pop3.telenet.be pop.gmail.com

IMAP: mail ontvangen -> draait op poort 143 (993), mail blijft op de server, encryptie, minder performant bv imap.telenet.be imap.gmail.com
Simultane connecties mogelijk

Exchange mail server

<https://www.youtube.com/watch?v=jb98hlOaeL4>

Qmail commands:

<http://www.qmail.org/qmail-manual-html/man8/>

Mail versturen en ontvangen via decommandline (telnet)

Telnet - SMTP Commando's (mail versturen dmv telnet)

Om dit te verwezenlijken heb je 3 vereisten:

1. een actieve internetverbinding
2. het adres van een mailserver die relaying toestaat—gewoonlijk aangeboden door een ISP (bv. mail.domein.ext)
3. een geldige mailadres(bv.mail@domein.ext)

Begin met een verbinding te maken vanaf jouw computer naar de mailserver.

```
telnet mail.domain.ext 25
```

Je zou iets moeten krijgen in de trant van:

```
Trying ????.????.????.???...  
Connected to mail.domain.ext.  
Escape character is '^]'.  
220 mail.domain.ext ESMTP Sendmail ?version-number?; ?  
date+time+gmtoffset?
```

- Eerst moet je opgeven waarvandaan je de email verstuurt:
- `HELO local.domain.name` – maak je niet druk om je lokale domeinnaam hoewel het de juiste fully qualified domain name moet zijn zoals de buitenwereld die ziet. De mailserver dient je op je woord te geloven volgens RFC822-RFC1123.

Dit geeft als resultaat:

```
250 mail.domain.ext Hello local.domain.name [loc.al.i.p], pleased to meet you
```

Geef nu je emailadres op:

- `MAIL FROM: mail@domain.ext`
- zou volgende melding moeten opleveren:
- `250 2.1.0 mail@domain.ext... Sender ok`
- Indien niet zie mogelijke problemen

Geef nu het adres van de bestemming (recipient) op:

```
RCPT TO: mail@otherdomain.ext
```

zou volgende melding moeten opleveren:

```
250 2.1.0 mail@otherdomain.ext... Recipient ok
```

Indien niet zie mogelijke problemen.

- Om je bericht op te stellen begin je met het commando

DATA

Wil je een onderwerp voor je bericht, geef dan op:

Subject:-vermeld je onderwerp hier-

- Druk vervolgens twee keer op de ENTER-toets (nodig om conform te zijn met RFC 882)
- Vervolgens kan je de 'bodytekst' van je bericht (bv.
hallo mail@otherdomain.ext from mail@domain.ext)
- Om de mailserver te verwittigen dat het bericht volledig is voeg een "." op een afzonderlijke regel.
De mailserver zou dan moeten antwoorden met zoiets als
250 2.0.0 ???????? Message accepted for delivery
- Met het QUIT commando sluit je de sessie af. De mailserver zal dit bevestigen met zoiets als:
221 2.0.0 mail.domain.ext closing connection Connection closed by
foreign host.

Mogelijke problemen

501 nouser@nosuchplace.here... Sender domain must exist

- Het domein vanwaar je verstuurt moet bestaan

503 Need MAIL before RCPT

- Een bestemming werd opgegeven voor de zender.

550 mail@domain.ext... Relaying Denied

- De mailserver weigert de mail te relayeren voor you, hier kunnen verscheidene redenen voor bestaan vanwaar de meest typische oa. zijn:

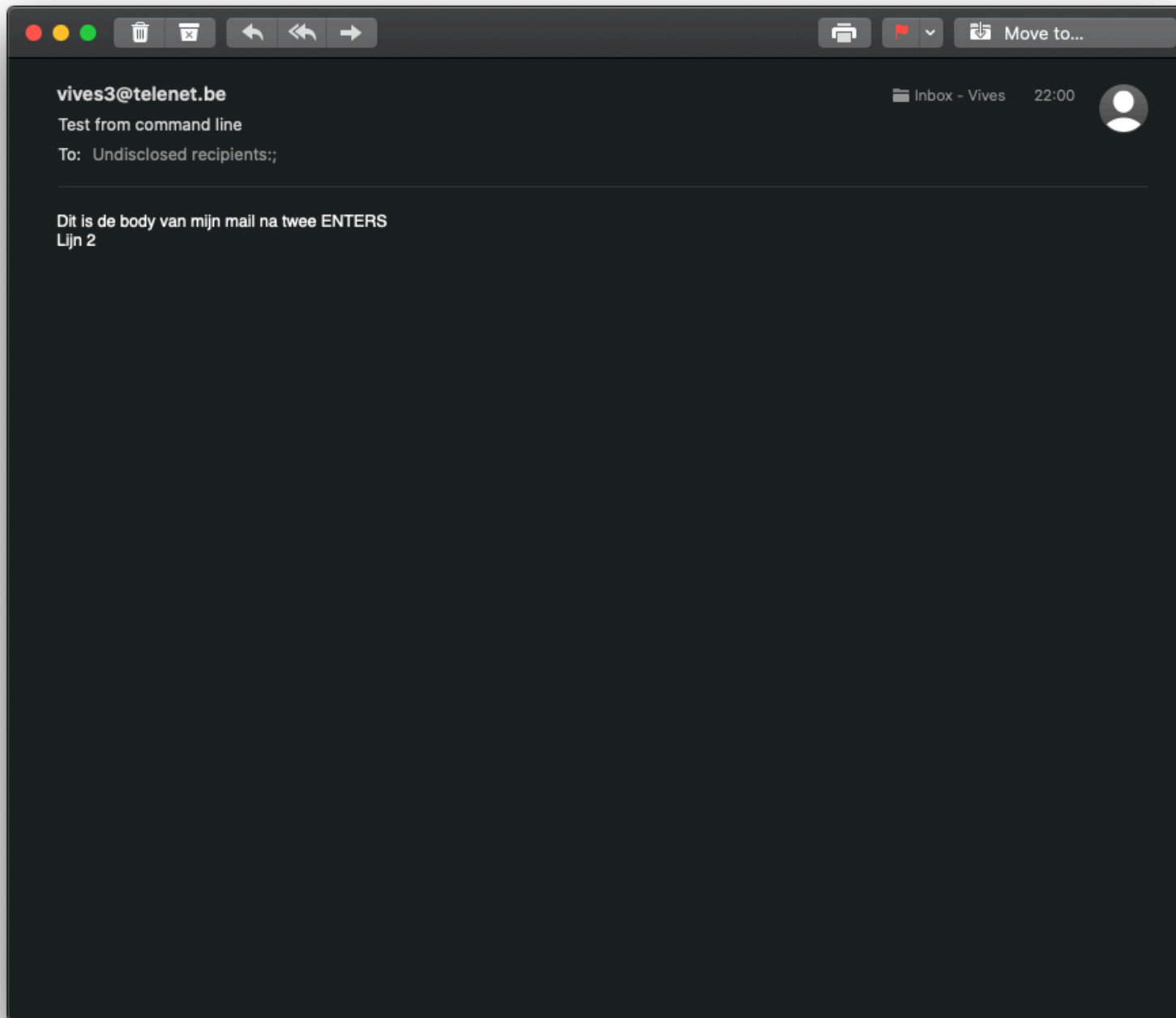
- – de internetverbinding gebeurt niet via deze provider en/of
- – geen email adres gebruiken dat door de eigenaar van de server werd aangeboden.

Enkele watchouts:

1. indien je te snel typt, zal hij soms de tekst niet herkennen (eigenaardig!)
2. de backspace toets werkt niet met bepaalde telnetclients (al lijkt dit niet zo)

```
[diMilan~ $telnet smtp.telenet.be 25
Trying 195.130.132.11...
Connected to smtp.telenet.be.
Escape character is '^]'.
220 andre.telenet-ops.be bizsmtp ESMTP server ready
HELO local.vives.be
250 andre.telenet-ops.be hello [178.119.1.226], pleased to meet you
MAIL FROM: vives3@telenet.be
250 2.1.0 <vives3@telenet.be> sender ok
RCPT TO: milan.dima@vives.be
250 2.1.5 <milan.dima@vives.be> recipient ok
DATA
354 enter mail, end with "." on a line by itself
Subject: Test from command line

Dit is de body van mijn mail na twee ENTERS
Lijn 2
.
250 2.0.0 Message accepted for delivery (EKxC2100L4saP3E01KyXnc)
QUIT
```



Telnet POP

Om dit te verwezenlijken heb je 4 vereisten:

1. een actieve internet verbinding
2. het adres van je pop mailserver(bv.mail.domein.ext)
3. Je gebruikersnaam
4. Je paswoord

Begin met een verbinding te maken vanaf jouw computer naar de mailserver.

```
telnet mail.domain.ext 110
```

Je zou iets moeten krijgen in de trant van:

```
Trying ????.????.????.???... Connected to mail.domain.ext.  
Escape character is '^]'.  
+OK ready
```


- Log dan in als volgt:

USER user@domainname.ext

- Dit geeft vervolgens iets als:

+OK Password required for userName.

- Geef het password op:

PASS passW0rd

- Hierna krijg je een melding of er mail is.

+OK userName has ? visible messages (? hidden) in ?????
octets.

- Indien dit niet zo is, ga dan naar mogelijke problemen.

- Om een lijst te krijgen van emails die wachten op ophaling gebruik je het `LIST` commando, dit zal ook het numerieke id van je berichten vermelden(bv. 1 of 2 enz....)
- Wil je de inhoud bekijken van een bericht typ dan `RETR` + het id nummer van het bericht (bv. `RETR 1`).
- Om een bericht te verwijderen gebruik je `DELE`+ het id nummer van het bericht (bv. `DELE 1`).
- Om je mailbox te verlaten en de verbinding te sluiten gebruik je `QUIT`

Mogelijke problemen

-ERR [AUTH] Password supplied for "userName" is incorrect.

- Het opgegeven password was niet datgene dat de server verwachtte, hertyp het, en indien dat niet lukt, kijk dan na of het correcte password gebruikt.

-ERR [AUTH] PAM authentication failed for user "userName": Authentication failure (7)

- Je mailbox kon niet correct opgedeeld worden in afzonderlijke emails, er is mogelijks nog een restant van een bericht overgebleven – Vraag je ISP om je mailbox manueel te bewerken en uit te kijken naar lege regels boven de headers.

452 4.4.5 Insufficient disk space; try again later

- De mailserver kan de tijdelijke bestanden nodig om je mail op te halen niet wegschrijven- vraag je ISP om het schijfgebruik en de toewijzing op de server na te kijken.

-ERR [SYS/TEMP] Unable to copy mail spool file, quota exceeded (122)

- The mailserver cannot create a temporary file needed to allow you access to your mailbox as you've run out of your space allocation - Try to reduce the amount of disk space you are using on that server (this quota may be shared between your mail, web and userspace), alternatively contact your ISP to increase your quota.

-ERR [IN-USE] /???/???/.userName.pop lock busy! Is another session active? (11)

- The mailbox is currently in use by another connection or an old connection has terminated uncleanly - This will deal with itself

Overquota locking file '/???/???/???/userName.lock'; lock proceeding anyway

Unable to process From lines (envelopes) in /???/???/???/userName; change recognition mode or check for corrupted mail drop.

- The mailbox cannot be split into separate messages because the pop server cannot recognise distinct boundaries or the boundaries do not include the whole mailbox

- Enkele watch-outs:

1. indien je te snel typt, zal hij soms de tekst niet herkennen (eigenaardig!)
2. de backspace toets werkt niet met bepaalde telnetclients (al lijkt dit niet zo)

SMTP Commando's

- HELO
 - MAIL FROM: • RCPT TO:
 - DATA
 - RSET
 - QUIT
 - HELP
-
- introduce yourself • specify sender
 - specify recipient
 - body of message • reset
-
- quit the session
 - help on commands

```
mbpt — telnet pop.telenet.be 110 — 80x24
[diMilan~ $telnet pop.telenet.be 110
Trying 195.130.132.12...
Connected to pop.telenet.be.
Escape character is '^]'.
+OK POP3 ready
USER vives3@telenet.be
+OK
PASS XXXX
+OK server ready
LIST
+OK 1 messages
1 4776
.
TOP 1 4776
```

```

mbpt — telnet pop.telenet.be 110 — 80x62
TOP 1 4776
+OK message top follows
Return-Path: milan.dima@vives.be
Received: from jules.telenet-ops.be (LHL0 jules.telenet-ops.be)
  (2a02:1800:120:4:0:0:f00:c) by zcsnocm111.telenet-ops.be with LMTP; Wed, 16
  Oct 2019 22:05:30 +0200 (CEST)
Received: from edge.vives.be ([193.190.147.132])
  by jules.telenet-ops.be with bizsmtp
  id EL5W2101D2rdaCH01L5W3g; Wed, 16 Oct 2019 22:05:30 +0200
X-Spamcause: gggfuggvucfvtghtrrhhoucdtuddrgeudedrjeehgddugeekucetufdoteggodetrfd
otffvucfrrrhhohfhhlhgvmeuthgvhlghvnhgvthdrsggvnecuaeagrihlohthumuceftddtneecunec
ujfigurhephffvufhtffkfhghjhtggesrgdtmhertddtjeenucfhrhohmhepofhilhgrnhcuffhimhg
ruceomhhilhgrnrhdruhghimgrsehvihhvghsrdgsvgeqneucukfhppeduleefrdduledtrddugeejrdd
ufedvpddutddrudelvdrrjedurddvdpdhfvgektedmmegutgektgemvgejleejmeekvgegleemleekhee
lnecurfgrrrhgrmhhep1hnhvghthpeduleefrdduledtrddugeejrddufedvdpdhvghlohepvvgughgvrdh
viihvghsrdgsvgdpmhgrihhlhfhrohmpmehmihlgrhnrduiuhmrgesvhhivghvshdrsggvpdhrtgh
pthhtohepvhhivghvshfsehtvghlvghnvhghtrdgsvglenucevlhushhtvghruthiigvpedt
Delivered-To: vives3@telenet.be
Received: from DC-EXCH19MBX-02.vivesnet.be (10.192.64.91) by edge.vives.be
  (193.190.147.132) with Microsoft SMTP Server (version=TLS1_2,
  cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256) id 15.1.1779.2; Wed, 16
  Oct 2019 22:05:29 +0200
Received: from DC-EXCH19MBX-02.vivesnet.be (2a02:2c40:70:3200::91) by
  DC-EXCH19MBX-02.vivesnet.be (2a02:2c40:70:3200::91) with Microsoft SMTP
  Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
  15.2.464.5; Wed, 16 Oct 2019 22:05:30 +0200
Received: from DC-EXCH19MBX-02.vivesnet.be ([fe80::dc8c:e797:8e49:9859]) by
  DC-EXCH19MBX-02.vivesnet.be ([fe80::dc8c:e797:8e49:9859%7]) with map1 id
  15.02.0464.005; Wed, 16 Oct 2019 13:05:30 -0700
From: Milan Dima <milan.dima@vives.be>
To: "vives3@telenet.be" <vives3@telenet.be>
Subject: Re: Test from command line
Thread-Topic: Test from command line
Thread-Index: AQHVhFxFV05+frjaDYEmfELIZmX/hdqdeJr2A
Date: Wed, 16 Oct 2019 20:05:30 +0000
Message-ID: <672FD25E-523B-4815-B090-7AD600DCEEF1@vives.be>
References: <20191016220012.EKxC2100L4saP3E01KyXnc@andre.telenet-ops.be>
In-Reply-To: <20191016220012.EKxC2100L4saP3E01KyXnc@andre.telenet-ops.be>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
x-originating-ip: [10.192.71.2]
Content-Type: multipart/alternative;
  boundary="_000_672FD25E523B4815B0907AD600DCEEF1vivesbe_"
MIME-Version: 1.0
Return-Path: milan.dima@vives.be

--_000_672FD25E523B4815B0907AD600DCEEF1vivesbe_
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: base64

UkVQTfkgdm1hIFVzZXIgdWlbnQNCg0KDQrigJQNCg0KTWlsYW4rG1tYQ0KDQoNCK9uIDE2IE9j
dCAYMDE5LCBhdCAyMjowMwgm12ZXZzQHR1bGVuZXQuYmU8bWfPbHRvOnZpdmVzM0B0ZWxlbmV0
LmJlP1B3cm90ZToNCg0KRGl0IGlzIGRlIGJvZHKgdmFuIG1pam4gbWfPpCBuYSB0d2V1IEV0VEVS
Uw0KTG1qb1AyDQoNCg==

--_000_672FD25E523B4815B0907AD600DCEEF1vivesbe_
Content-Type: text/html; charset="utf-8"
Content-ID: <743B50F46D6E924A8271C559E73FE15F@vives.be>
Content-Transfer-Encoding: base64

```

POP commando's

- USER • enter user ID
- PASS • enter password
- QUIT • quit POP server
- LIST • list messages
- RETR • retrieve message
- DELE • delete message
- TOP • show top x lines of a message

Extra links

- Spamscore van je mail adres: <https://www.mail-tester.com/>
- Exchange server installeren / configureren <https://www.youtube.com/watch?v=jb98hlOaeL4>
- Understanding mail headers: <https://mediatemple.net/community/products/dv/204643950/understanding-an-email-header>
- Set Up Postfix + Dovecot on Ubuntu 18.04 <https://www.youtube.com/watch?v=Jeod07TdYkc>
- Postfix basics: <https://help.ubuntu.com/community/PostfixBasicSetupHowto>
- Postfix + Dovecot: <https://www.digitalocean.com/community/tutorials/how-to-set-up-a-postfix-e-mail-server-with-dovecot>

Opdracht

- Installeer lokaal postfix en Dovecot op je lokale Linux Distro
- Zie Toledo Opdracht MTA [Link](#)
- Deadline **23/10/19 8:30**