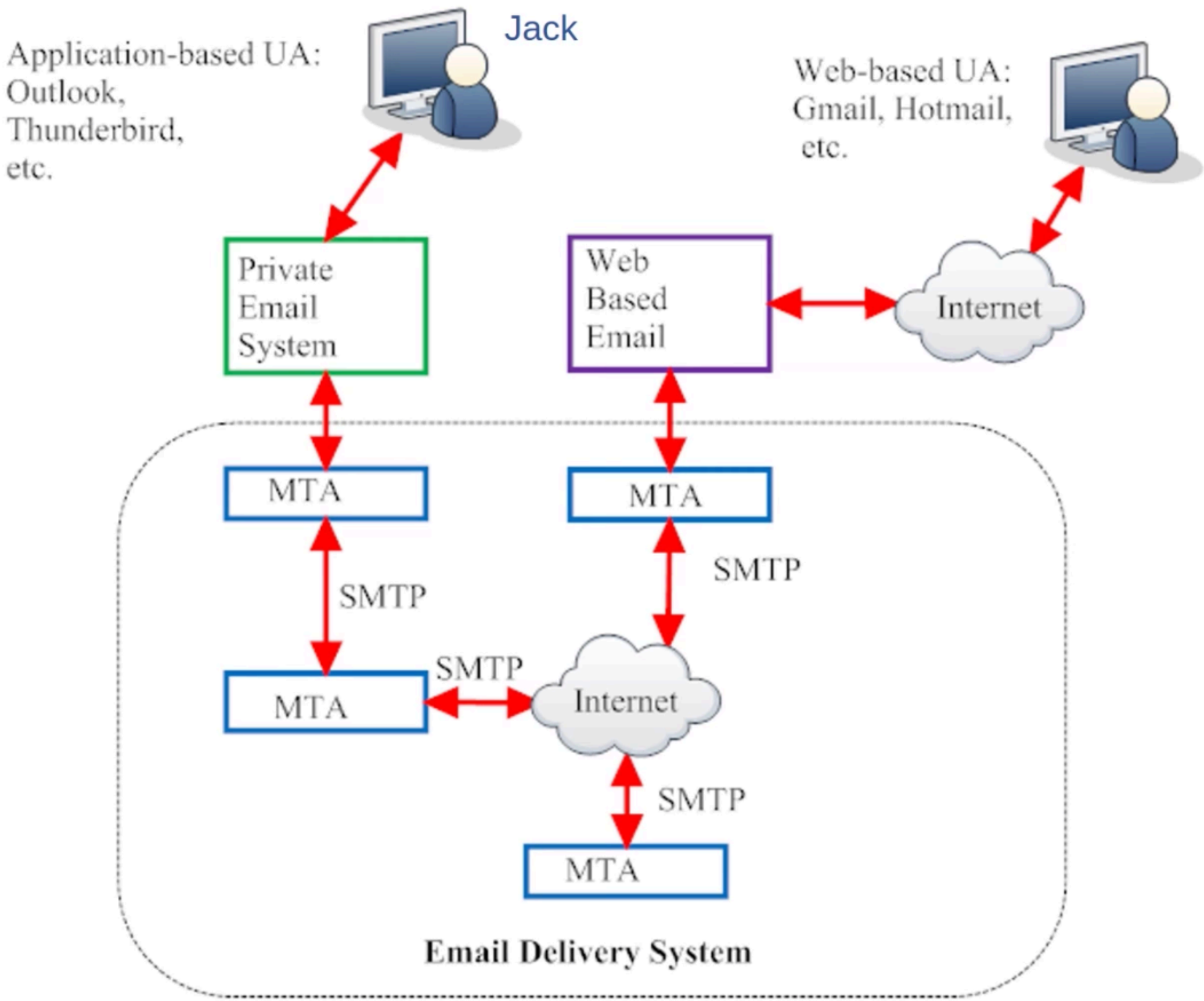
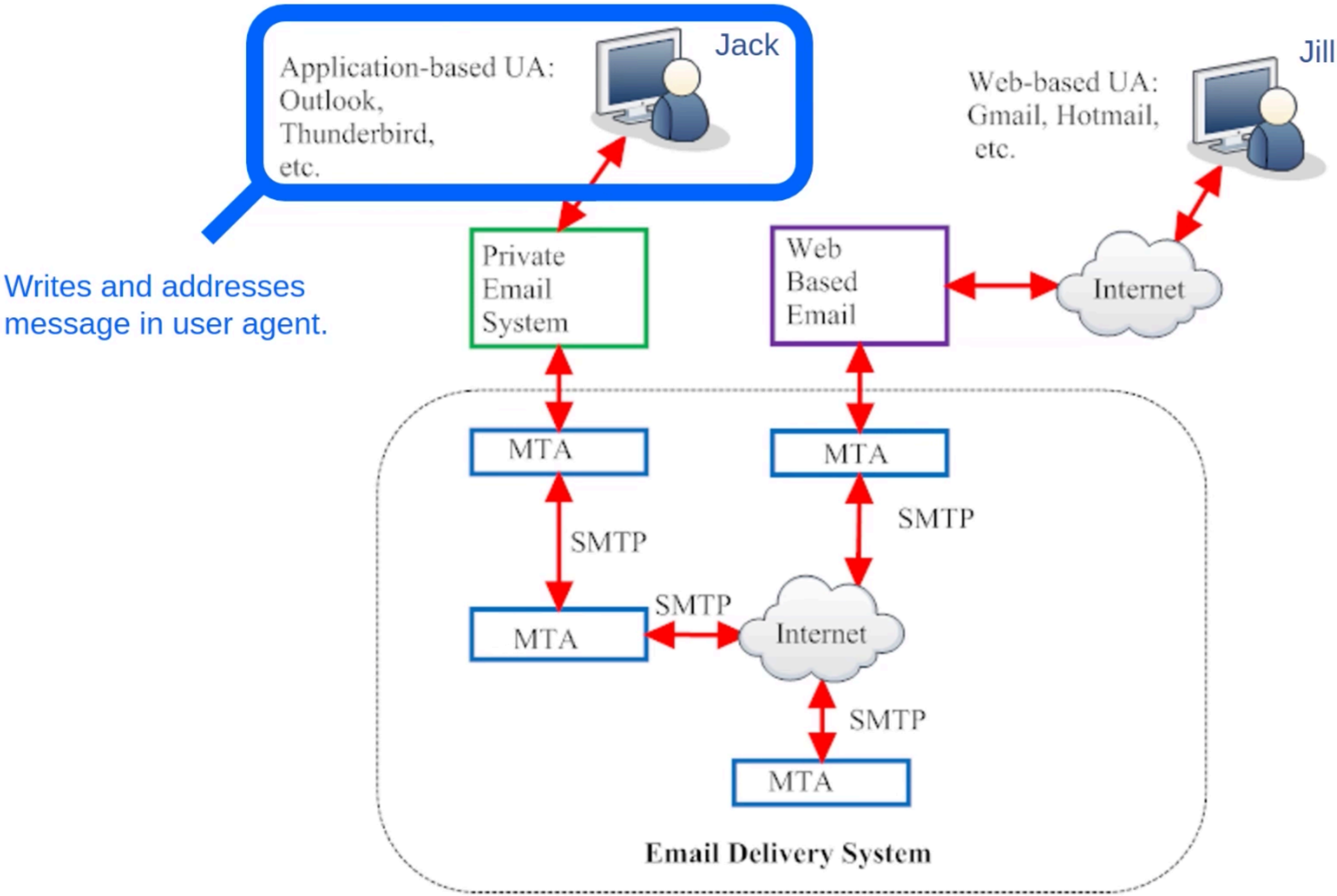
MAIL

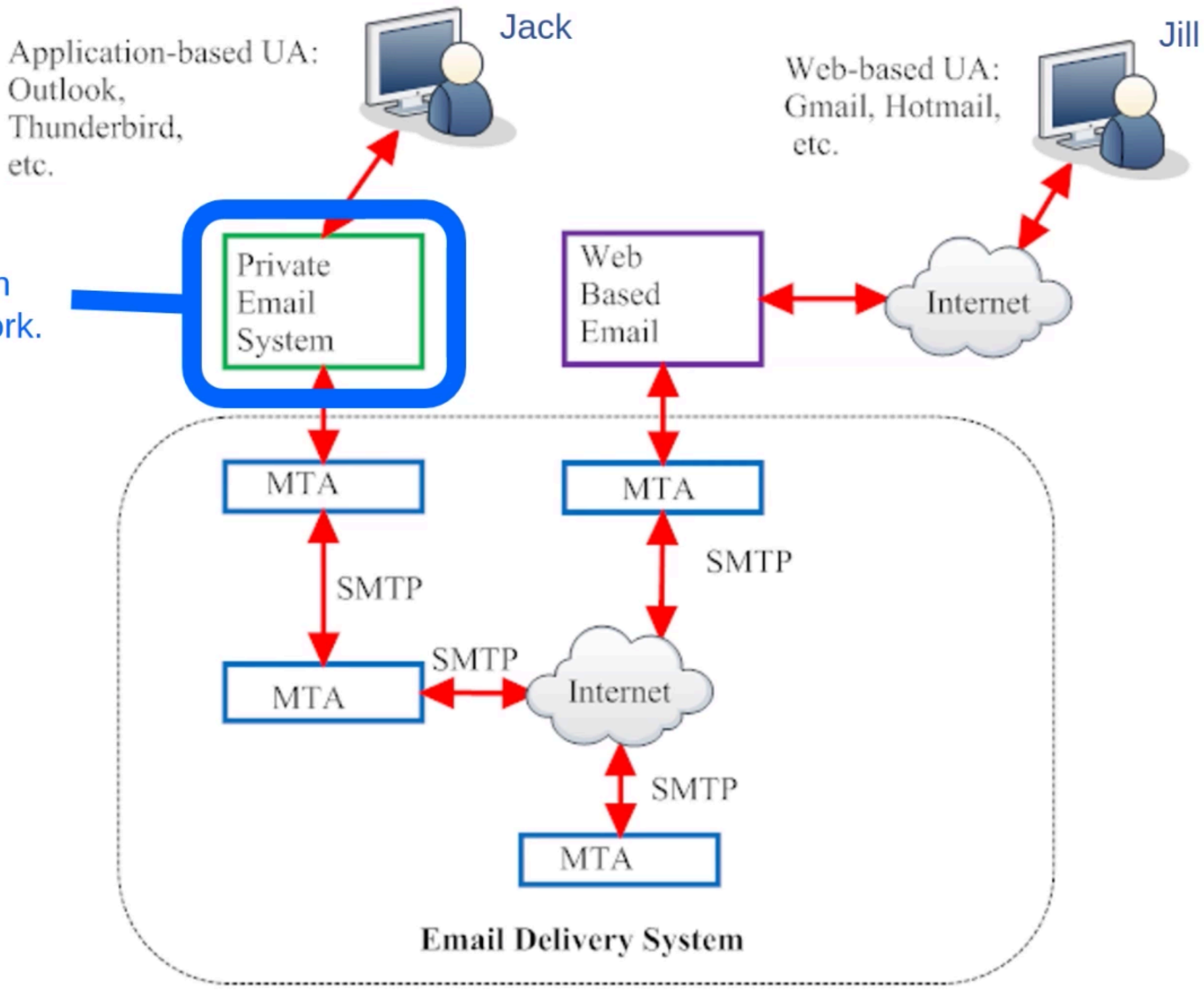
Les 2 27/09/2018

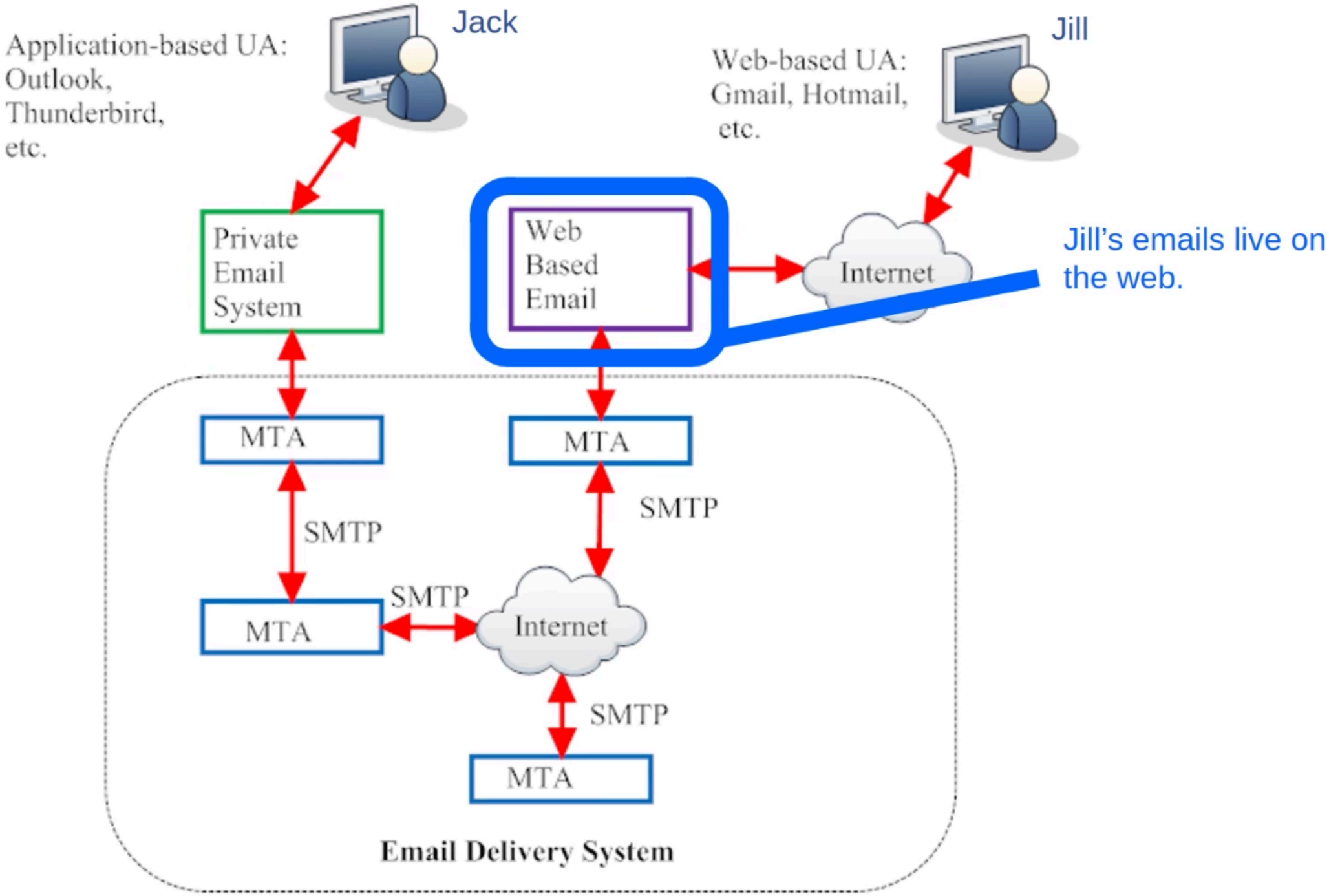
M.DIMA


Jack
Application-based UA:
Outlook,
Thunderbird,
etc.
Web-based UA:
Gmail, Hotmail,
etc.
Private
Email
System
Web
Based
Email
Internet
MTA
MTA
SMTP
SMTP
SMTP
MTA
Internet
SMTP
MTA
Email Delivery System

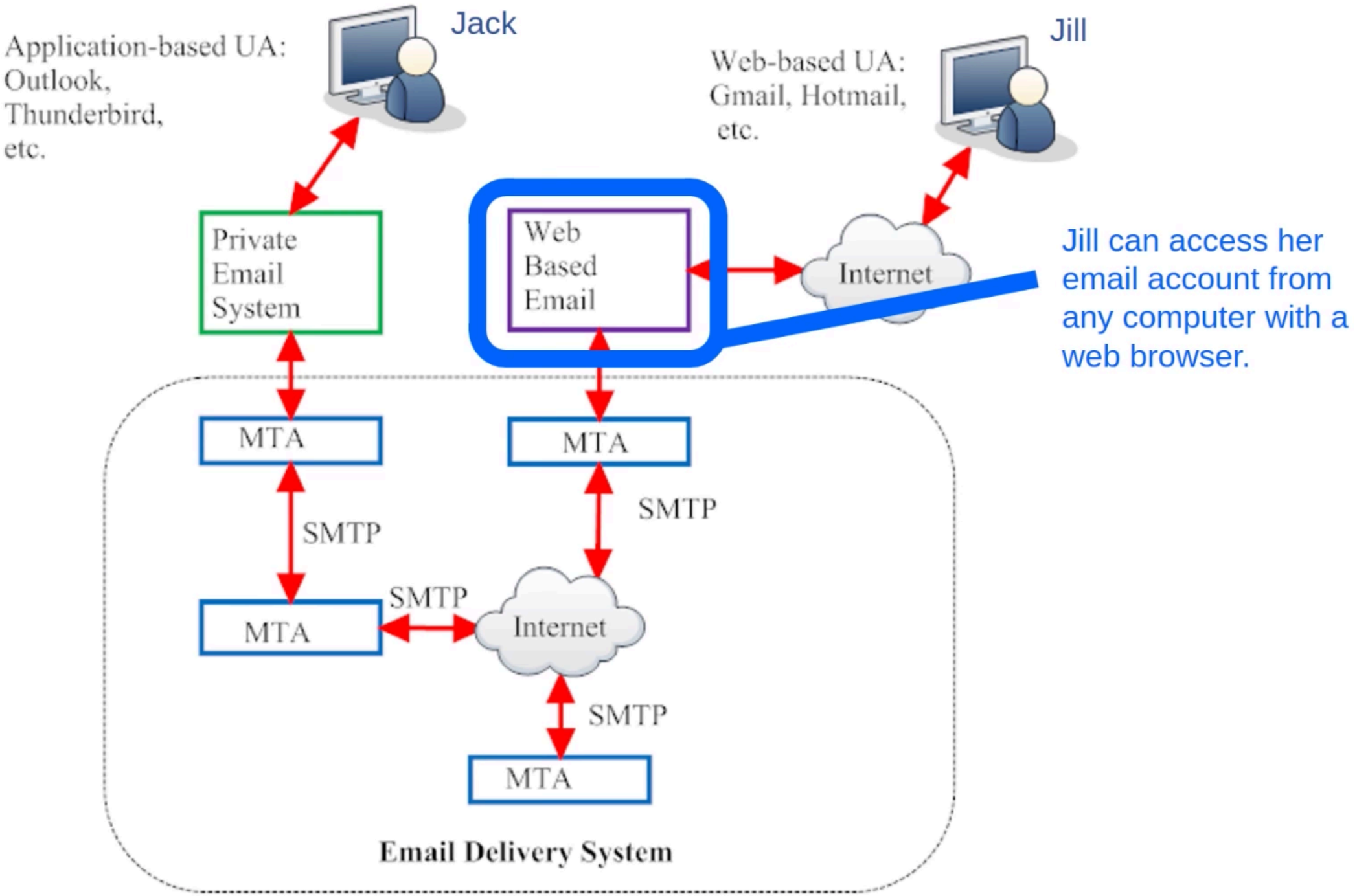

Jack
Application-based UA:
Outlook,
Thunderbird,
etc.
Jill
Web-based UA:
Gmail, Hotmail,
etc.
Writes and addresses
message in user agent.
Private
Email
System
Web
Based
Email
Internet
MTA
MTA
SMTP
SMTP
SMTP
MTA
Internet
SMTP
MTA
Email Delivery System

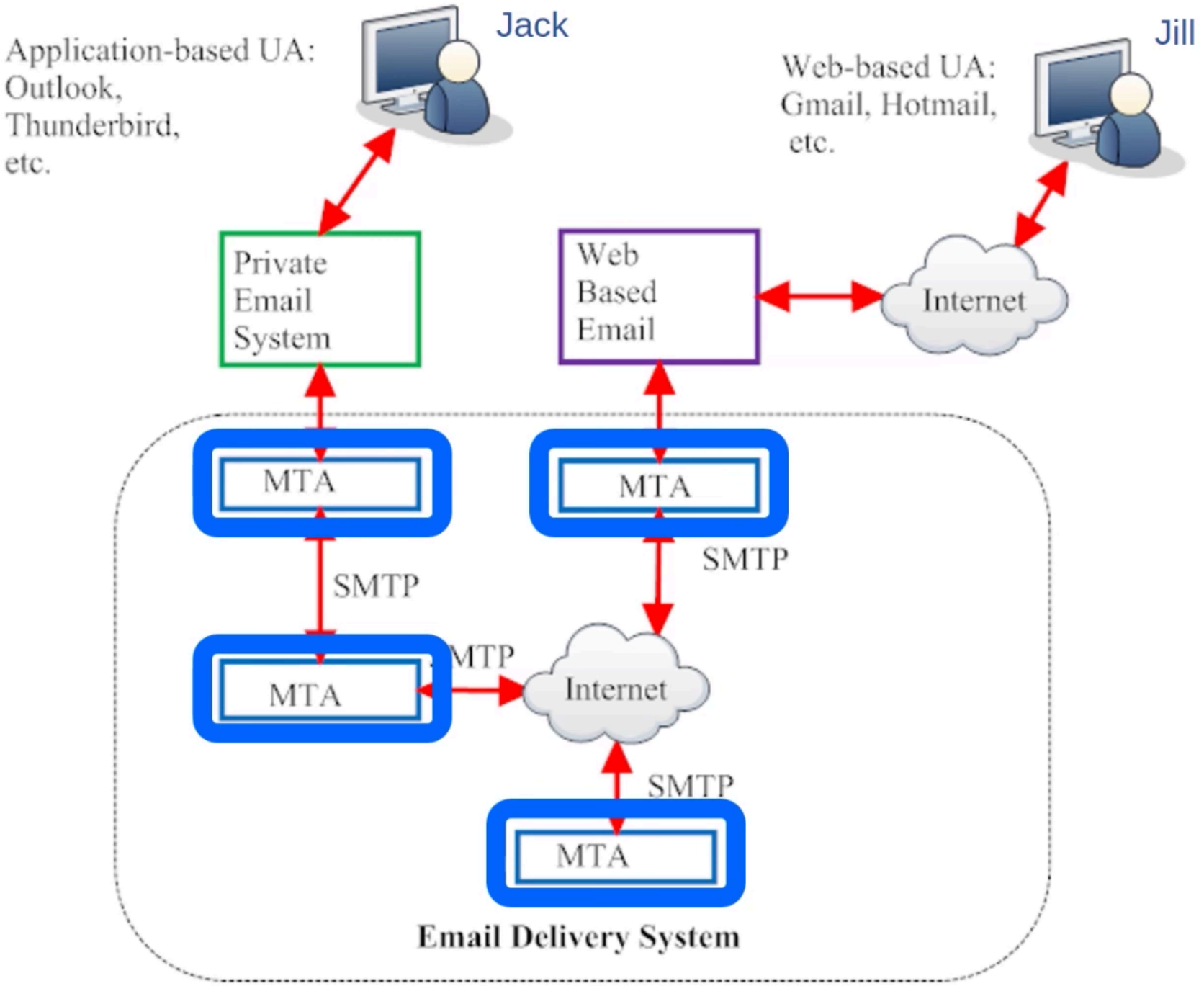
Emails are stored on Jack's private network.

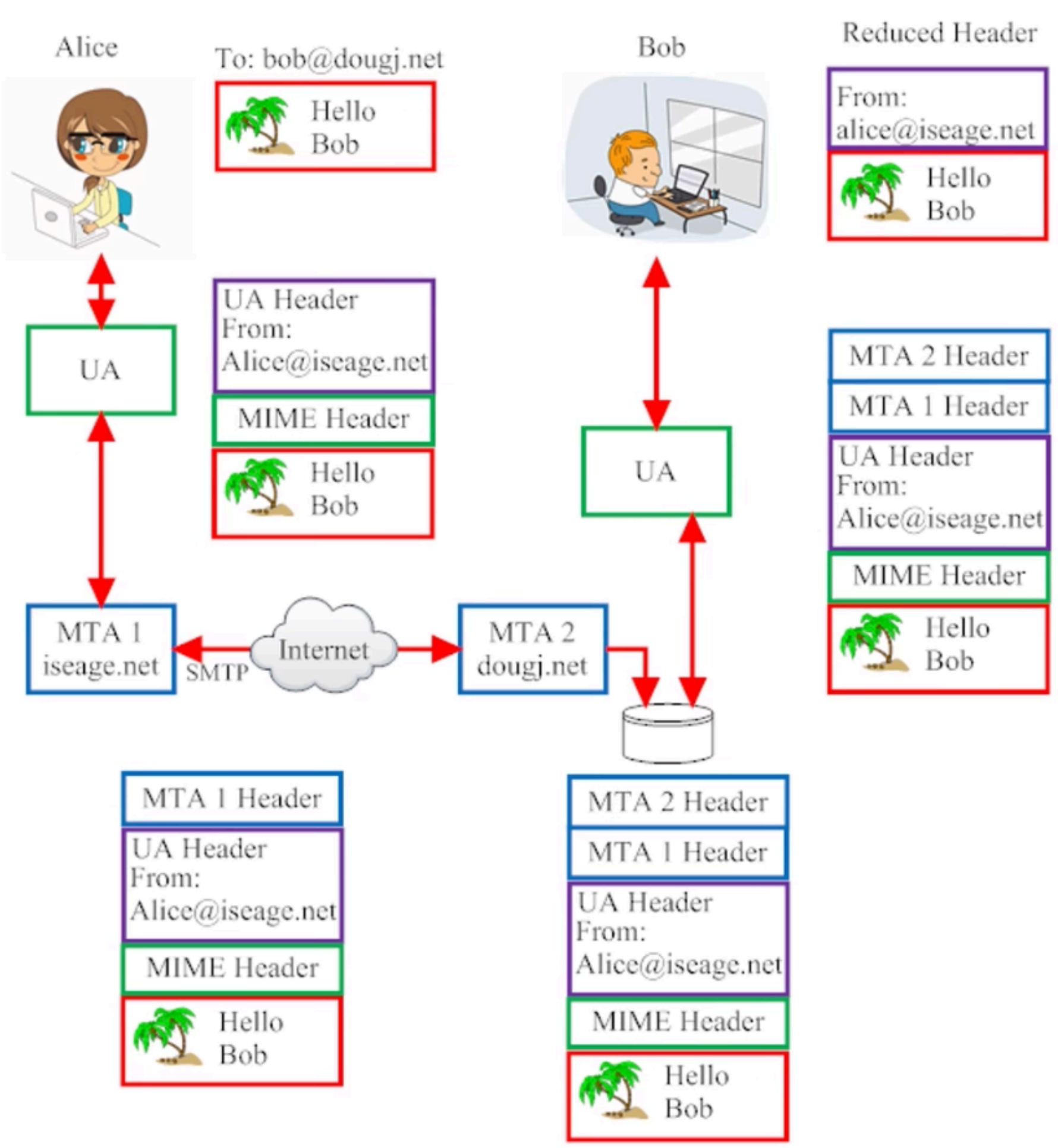



Application-based UA:
Outlook,
Thunderbird,
etc.
Jack
Web-based UA:
Gmail, Hotmail,
etc.
Jill
Private
Email
System
Web
Based
Email
Internet
Jill's emails live on
the web.
MTA
MTA
SMTP
SMTP
SMTP
MTA
Internet
SMTP
MTA
Email Delivery System

Ondertiteling




Application-based UA:
Outlook,
Thunderbird,
etc.
Jack
Web-based UA:
Gmail, Hotmail,
etc.
Jill
Private
Email
System
Web
Based
Email
Internet
MTA
MTA
SMTP
SMTP
MTP
MTA
Internet
SMTP
MTA
Email Delivery System


Alice
To: bob@dougj.net
Hello
Bob
Bob
Reduced Header
From:
alice@iseage.net
Hello
Bob
UA
UA Header
From:
Alice@iseage.net
MIME Header
Hello
Bob
UA
MTA 2 Header
MTA 1 Header
UA Header
From:
Alice@iseage.net
MIME Header
Hello
Bob
MTA 1
iseage.net
SMTP
Internet
MTA 2
dougj.net
MTA 1 Header
UA Header
From:
Alice@iseage.net
MIME Header
Hello
Bob
MTA 2 Header
MTA 1 Header
UA Header
From:
Alice@iseage.net
MIME Header
Hello
Bob

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=F87jySDZnMayyitVxLdHcQNL073DytKRyrRh84GNsI24IRNakn0oOfrC2luliNvdea LGTk3adIrzt+N96GyMseWz8T9xE6O/
sAI16db48q4Iqkd7uOiDvFsvS3CUQlNhybNw8m CH/o8eELTN0zbSbn5Trp0dkRYXhMX8FTAwrH0=
Domainkey-Signature: a=rsa-sha1; c=nofws; d=gmail.com; s=gamma; h=message-id:date:from:to:subject:mime-version:content-type;
b=wkbBj0M8NCUlboI6idKooejg0sL2ms7fDPe1tHUkR9Ht0qr5lAJX4q9PMVJeyjWalH
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 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 bv **smtp.telenet.be**, **smtp.gmail.com**

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

IMAP: mail ontvangen -> draait op poort 143 , mail blijft op de server, encryptie, minder performant bv **imap.telenet.be** **imap.gmail.com**

Exchange mail server

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

Qmail commands:

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