Consulta registro mx del servidor DNS

DNS Query Results

Step 1

We are at the first step. All DNS queries, if not previously cached (and we do NOT cache), starts from the root servers.

Also please note that, as all or many of the root servers has anycast ip addresses, it's impossible to determine their locations just only by their ip addresses. This situtation is most likely the same for the next step. All gTLD and ccTLD nameservers are also required to have their ip addresses advertised as anycast. So basically, it is hard to say where these nameservers are.

h.root-servers.net [128.63.2.53] (Fort Huachuca, Arizona, United States 🇺🇸)   🕐 17.44 ms

```
;;Authority
➡ com. 172800 IN NS a.gtld-servers.net
➡ com. 172800 IN NS b.gtld-servers.net
➡ com. 172800 IN NS c.gtld-servers.net
➡ com. 172800 IN NS d.gtld-servers.net
➡ com. 172800 IN NS e.gtld-servers.net
➡ com. 172800 IN NS f.gtld-servers.net
➡ com. 172800 IN NS g.gtld-servers.net
➡ com. 172800 IN NS h.gtld-servers.net
➡ com. 172800 IN NS i.gtld-servers.net
➡ com. 172800 IN NS j.gtld-servers.net
➡ com. 172800 IN NS k.gtld-servers.net
➡ com. 172800 IN NS l.gtld-servers.net
➡ com. 172800 IN NS m.gtld-servers.net
```

🗔 We got referrals from **h.root-servers.net**

Step 2

Step 2

We've got referrals (a.gtld-servers.net, b.gtld-servers.net, c.gtld-servers.net, d.gtld-servers.net, e.gtld-servers.net, f.gtld-servers.net, g.gtld-servers.net, h.gtld-servers.net, i.gtld-servers.net, j.gtld-servers.net, k.gtld-servers.net, l.gtld-servers.net, m.gtld-servers.net) from queries on previous step. We'll query them now, until we got an authoritative result

i.gtld-servers.net [192.43.172.30] (United States 🇺🇸)   84.60 ms

```
;;Authority
gmail.com. 172800 IN NS ns1.google.com
gmail.com. 172800 IN NS ns2.google.com
gmail.com. 172800 IN NS ns3.google.com
gmail.com. 172800 IN NS ns4.google.com
```

We got referrals from **i.gtld-servers.net**

Step 3

We've got referrals (ns2.google.com, ns1.google.com, ns3.google.com, ns4.google.com) from queries on previous step. We'll query them now, until we got an authoritative result

ns1.google.com [216.239.32.10] (Mountain View, California, United States 🇺🇸)   23.37 ms

```
;;Answer
gmail.com. 3600 IN MX 10 alt1.gmail-smtp-in.l.google.com
gmail.com. 3600 IN MX 20 alt2.gmail-smtp-in.l.google.com
gmail.com. 3600 IN MX 30 alt3.gmail-smtp-in.l.google.com
gmail.com. 3600 IN MX 40 alt4.gmail-smtp-in.l.google.com
gmail.com. 3600 IN MX 5 gmail-smtp-in.l.google.com
;;Additional
alt1.gmail-smtp-in.l.google.com. 300 IN A 64.233.186.26
alt2.gmail-smtp-in.l.google.com. 300 IN A 74.125.138.26
alt3.gmail-smtp-in.l.google.com. 300 IN A 64.233.166.26
alt4.gmail-smtp-in.l.google.com. 300 IN A 173.194.65.26
gmail-smtp-in.l.google.com. 300 IN A 64.233.171.26
```

We got authoritative results from **ns1.google.com**

Mediante comando nslookup:

```
Administrador: C:\Windows\system32\cmd.exe - nslookup  - 194.179.1.100

C:\Users\eugenio>nslookup - 194.179.1.100
Servidor predeterminado:  100.red-194-179-1.static.ccgg.telefonica.net
Address:  194.179.1.100

> set q=mx
> gmail.com
Servidor:  100.red-194-179-1.static.ccgg.telefonica.net
Address:  194.179.1.100

Respuesta no autoritativa:
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google
.com

alt1.gmail-smtp-in.l.google.com internet address = 64.233.161.27
alt1.gmail-smtp-in.l.google.com AAAA IPv6 address = 2a00:1450:4010:c08::1b
gmail-smtp-in.l.google.com       internet address = 173.194.66.26
gmail-smtp-in.l.google.com       AAAA IPv6 address = 2a00:1450:400c:c03::1a
alt3.gmail-smtp-in.l.google.com internet address = 74.125.203.27
alt3.gmail-smtp-in.l.google.com AAAA IPv6 address = 2404:6800:4008:c03::1a
alt4.gmail-smtp-in.l.google.com internet address = 173.194.72.26
alt4.gmail-smtp-in.l.google.com AAAA IPv6 address = 2404:6800:4008:c01::1a
alt2.gmail-smtp-in.l.google.com internet address = 74.125.130.27
alt2.gmail-smtp-in.l.google.com AAAA IPv6 address = 2404:6800:4003:c01::1b
>
```
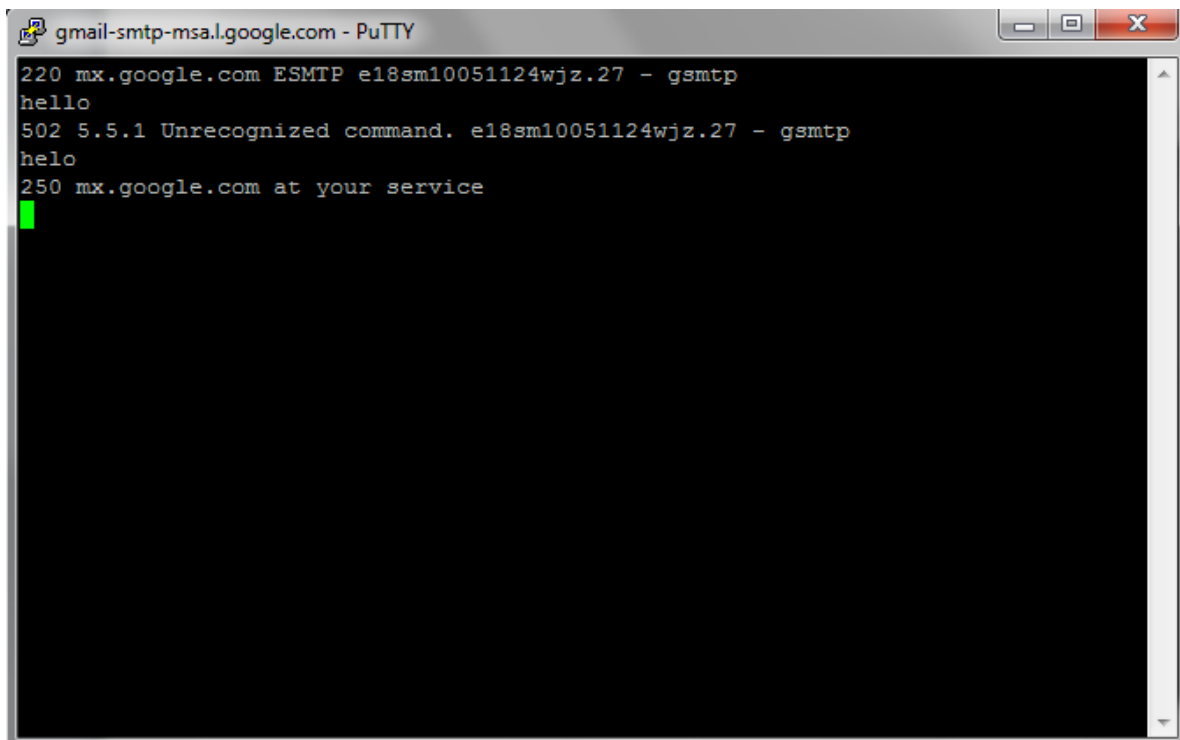
Conexión remota telnet smtp.google.com puerto 25:
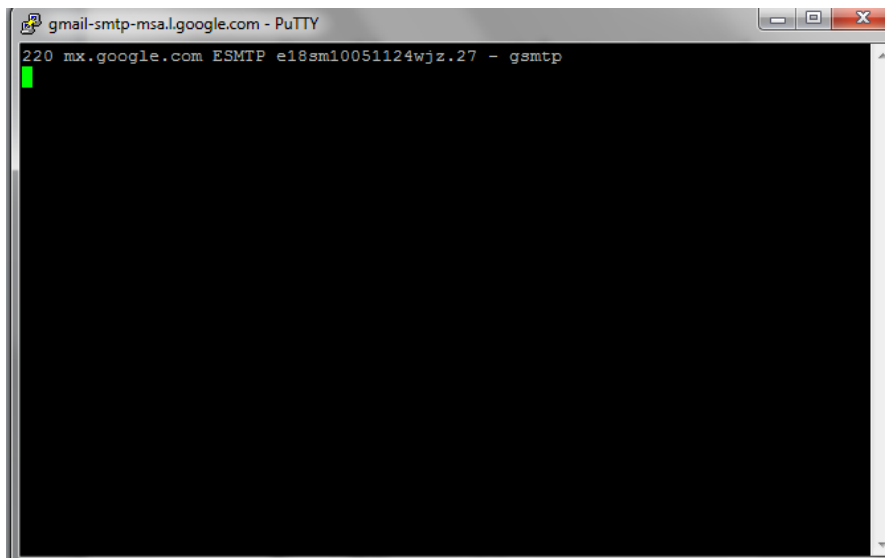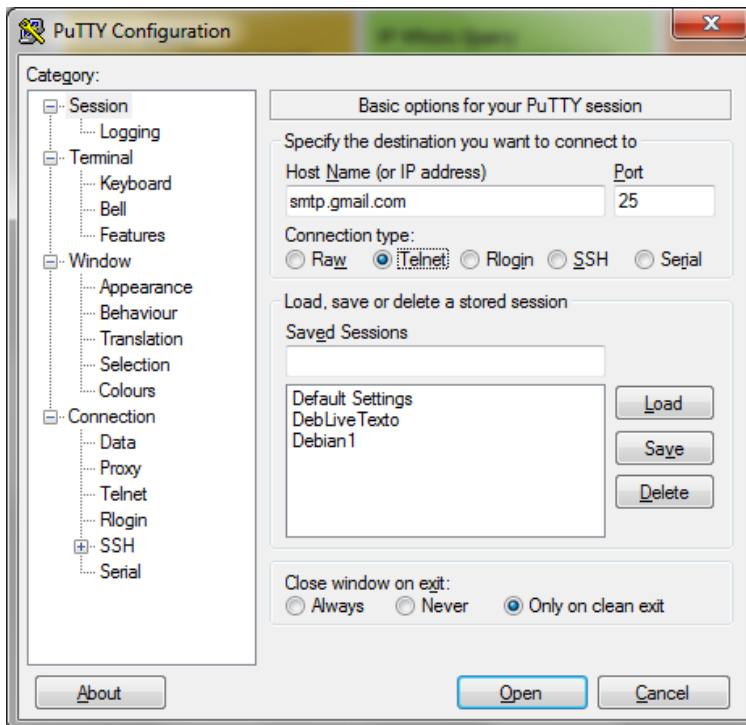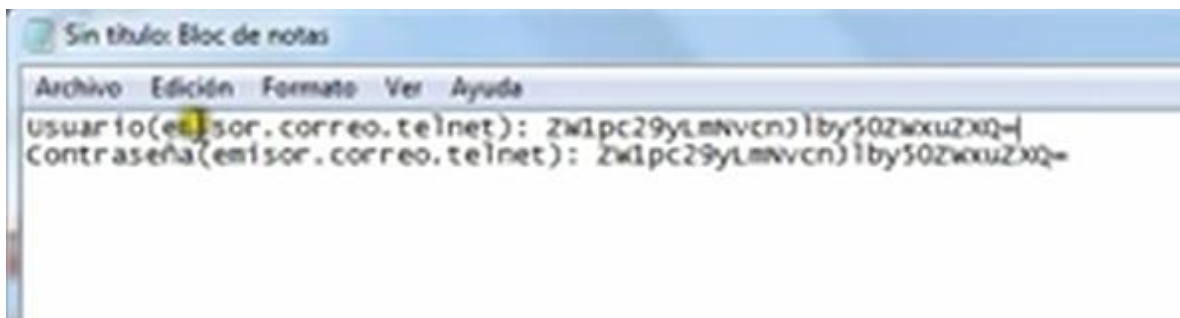
```
gmail-smtp-msa.l.google.com - PuTTY
220 mx.google.com ESMTP e18sm10051124wjz.27 - gsmtp
hello
502 5.5.1 Unrecognized command. e18sm10051124wjz.27 - gsmtp
helo
250 mx.google.com at your service
```

Ejemplo de conexión mediante telnet con usuario en gmail:


```
Sin título: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
usuario(emisor.correo.telnet): ZW1pc29yLmNvcn)lby5OZWxuZXQ=
Contraseña(emisor.correo.telnet): ZW1pc29yLmNvcn)lby5OZWxuZXQ=
```

```
Telnet smtp.gmail.com

220 mx.google.com ESMTP x4sm76474061eef.10
ehlo
250-mx.google.com at your service, [84.127.8.89]
250-SIZE 35882577
250-8BITMIME
250-AUTH LOGIN PLAIN XOAUTH
250-ENHANCEDSTATUSCODES
250 STARTTLS
auth login
334 VXNlcm5hbWU6
ZW1pc29yLmNvcnJlby50ZWxuZXQ=334 UGFzc3dvcmQ6
ZW1pc29yLmNvcnJlby50ZWxuZXQ=235 2.7.0 Accepted
MAIL FROM:<emisor.correo.telnet@gmail.com>
250 2.1.0 OK x4sm76474061eef.10
RCPT TO:<receptor.correo.telnet@gmail.com>
250 2.1.5 OK x4sm76474061eef.10
DATA
354  Go ahead x4sm76474061eef.10
From:emisor.correo.telnet
To:receptor.correo.telnet
Subject:Prueba correo electronico mediante TELNET

Estamos probando el correo electronico mediante TELNET.
.
250 2.0.0 OK 1335212294 x4sm76474061eef.10
```

Servicio de correo de Linux

Enviar un correo desde el usuario *ftp1* al usuario *usuario* dentro de la propia máquina.

```
usuario@profesor:~$ su ftp1
Contraseña:
ftp1@profesor:/home/usuario$ mail
No mail for ftp1
ftp1@profesor:/home/usuario$ mail from usuario@profesor.2asir.net
Subject: Prueba de correo
Esto es una prueba de correo
.
Cc:
ftp1@profesor:/home/usuario$
```

Si ahora me logeo como usuario

```
usuario@profesor: ~

Debian GNU/Linux 7
profesor login: usuario
Password:
Last login: Thu Jan 29 13:00:16 CET 2015 from 192.168.4.16 on pts/0
Linux profesor 3.2.0-4-486 #1 Debian 3.2.46-1+deb7u1 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
usuario@profesor:~$ mail
Mail version 8.1.2 01/15/2001.  Type ? for help.
"/var/mail/usuario": 1 message 1 new
>N  1 ftp1@profesor.2as  Thu Jan 29 13:02   15/574    Prueba de correo
&
```

Para ver el correo:

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have mail.
usuario@profesor:~$ mail
Mail version 8.1.2 01/15/2001.  Type ? for help.
"/var/mail/usuario": 1 message 1 new
>N  1 ftp1@profesor.2as  Thu Jan 29 13:02   15/574    Prueba de correo
& ?
& 1
Message 1:
From ftp1@profesor.2asir.net Thu Jan 29 13:02:00 2015
Envelope-to: usuario@profesor.2asir.net
Delivery-date: Thu, 29 Jan 2015 13:02:00 +0100
To: from@profesor.2asir.net, usuario@profesor.2asir.net
Subject: Prueba de correo
From: ftp1@profesor.2asir.net
Date: Thu, 29 Jan 2015 13:01:59 +0100

Esto es una prueba de correo

&
```

Cunado me salgo del interfaz de lectura del correo

```
Esto es una prueba de correo

& quit
Saved 1 message in /home/usuario/mbox
usuario@profesor:~$
```

Guarda dicho mensaje en el fichero *mbox* de la carpeta personal de usuario. Si vemos el contenido de dicho fichero:

```
usuario@profesor:~$ cat /home/usuario/mbox
From ftp1@profesor.2asir.net Thu Jan 29 13:02:00 2015
Return-path: <ftp1@profesor.2asir.net>
Envelope-to: usuario@profesor.2asir.net
Delivery-date: Thu, 29 Jan 2015 13:02:00 +0100
Received: from ftp1 by profesor.2asir.net with local (Exim 4.80)
        (envelope-from <ftp1@profesor.2asir.net>)
        id 1YGnnL-0000k5-Oy; Thu, 29 Jan 2015 13:01:59 +0100
To: from@profesor.2asir.net, usuario@profesor.2asir.net
Subject: Prueba de correo
Message-Id: <E1YGnnL-0000k5-Oy@profesor.2asir.net>
From: ftp1@profesor.2asir.net
Date: Thu, 29 Jan 2015 13:01:59 +0100
Status: RO

Esto es una prueba de correo
```

O ver el fichero de correos de usuario:

```
usuario@profesor:~$ cat /var/mail/usuario
From ftp1@profesor.2asir.net Thu Jan 29 13:02:00 2015
Return-path: <ftp1@profesor.2asir.net>
Envelope-to: usuario@profesor.2asir.net
Delivery-date: Thu, 29 Jan 2015 13:02:00 +0100
Received: from ftp1 by profesor.2asir.net with local (Exim 4.80)
        (envelope-from <ftp1@profesor.2asir.net>)
        id 1YGnnL-0000k5-Oy; Thu, 29 Jan 2015 13:01:59 +0100
To: from@profesor.2asir.net, usuario@profesor.2asir.net
Subject: Prueba de correo
Message-Id: <E1YGnnL-0000k5-Oy@profesor.2asir.net>
From: ftp1@profesor.2asir.net
Date: Thu, 29 Jan 2015 13:01:59 +0100

Esto es una prueba de correo

usuario@profesor:~$
usuario@profesor:~$
```

¿Quién permite todo esto en Debian?

Lo hace el servicio exim4

```
usuario@profesor:~$ ps -aux |grep exim
warning: bad ps syntax, perhaps a bogus '-'?
See http://gitorious.org/procps/procps/blobs/master/Documentation/FAQ
101       2589  0.0  0.0   7400    952 ?        Ss   12:58   0:00 /usr/sbin/exim4
 -bd -q30m
usuario   3247  0.0  0.0   3564    832 pts/1    S+   13:16   0:00 grep exim
usuario@profesor:~$
```

Vemos en que puertos trabaja exim4:

```
root@profesor:/home/usuario# netstat -atunp |grep exim
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
2589/exim4
tcp6       0      0 ::1:25                  :::*                    LISTEN
2589/exim4
root@profesor:/home/usuario#
```

Conexión telnet desde la cuenta de usuario al servidor exim 4 en la dirección 127.0.0.1 por el puerto 25.

```
usuario@profesor:~$ telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 profesor.2asir.net ESMTP Exim 4.80 Thu, 29 Jan 2015 13:20:58 +0100
helo
501 Syntactically invalid HELO argument(s)
helo profesor.2asir.net
250 profesor.2asir.net Hello localhost [127.0.0.1]
mail from: <eugenio@hola.com>
250 OK
rcpt to: <usuario@profesor.2asir.net>
250 Accepted
data
354 Enter message, ending with "." on a line by itself
esto es una prueba desde telnet
.
250 OK id=1YGo80-0000qw-2T
```

Vemos el resultado en la cuenta de usuario, saliendo de la sesión telnet:

```
quit
221 profesor.2asir.net closing connection
Connection closed by foreign host.
Tiene correo nuevo en /var/mail/usuario
usuario@profesor:~$
```

Veamos el correo con el comando mail:

```
usuario@profesor:~$ mail
Mail version 8.1.2 01/15/2001.  Type ? for help.
"/var/mail/usuario": 1 message 1 new
>N  1 eugenio@hola.com    Thu Jan 29 13:23    15/543
& 1
Message 1:
From eugenio@hola.com Thu Jan 29 13:23:45 2015
Envelope-to: usuario@profesor.2asir.net
Delivery-date: Thu, 29 Jan 2015 13:23:45 +0100
From: eugenio@hola.com
Date: Thu, 29 Jan 2015 13:23:45 +0100

esto es una prueba desde telM-Cnet

&
```

Vemos los logs del exim:

```
root@profesor:/home/usuario# cat /var/log/exim4/
mainlog     rejectlog
root@profesor:/home/usuario# cat /var/log/exim4/mainlog
2013-09-18 12:07:03 exim 4.80 daemon started: pid=2340, -q30m, listening for SMT
2015-01-29 13:01:59 1YGnnL-0000k5-Oy <= ftp1@profesor.2asir.net U=ftp1 P=local S
=393
2015-01-29 13:02:00 1YGnnL-0000k5-Oy ** from@profesor.2asir.net: Unrouteable add
ress
2015-01-29 13:02:00 1YGnnL-0000k5-Oy => usuario <usuario@profesor.2asir.net> R=l
ocal_user T=mail_spool
2015-01-29 13:02:00 1YGnnM-0000kA-7y <= <> R=1YGnnL-0000k5-Oy U=Debian-exim P=lo
cal S=1234
2015-01-29 13:02:00 1YGnnL-0000k5-Oy Completed
2015-01-29 13:02:00 1YGnnM-0000kA-7y => ftp1 <ftp1@profesor.2asir.net> R=local_u
ser T=mail_spool
2015-01-29 13:02:00 1YGnnM-0000kA-7y Completed
2015-01-29 13:21:09 rejected HELO from localhost [127.0.0.1]: syntactically inva
lid argument(s): (no argument given)
2015-01-29 13:23:45 1YGo80-0000qw-2T <= eugenio@hola.com H=localhost (profesor.2
asir.net) [127.0.0.1] P=smtp S=376
2015-01-29 13:23:45 1YGo80-0000qw-2T => usuario <usuario@profesor.2asir.net> R=l
ocal_user T=mail_spool
2015-01-29 13:23:45 1YGo80-0000qw-2T Completed
2015-01-29 13:28:56 Start queue run: pid=3312
2015-01-29 13:28:56 End queue run: pid=3312
root@profesor:/home/usuario#
```

Vamos a intentar mandar un email a una cuenta de correo fuera del servidor:

```
usuario@profesor:~$ mail erincon@iesmiravent.es
Subject: prueba correo desde linux exim
esto es una prueba desde exim
.
Cc:
usuario@profesor:~$ mail
Mail version 8.1.2 01/15/2001.  Type ? for help.
"/var/mail/usuario": 1 message 1 new
>N  1 Mailer-Daemon@pro  Thu Jan 29 13:40   38/1442  Mail delivery failed: retur
&
```

```
Message 1:
From MAILER-DAEMON Thu Jan 29 13:40:42 2015
Envelope-to: usuario@profesor.2asir.net
Delivery-date: Thu, 29 Jan 2015 13:40:42 +0100
X-Failed-Recipients: erincon@iesmiravent.es
Auto-Submitted: auto-replied
From: Mail Delivery System <Mailer-Daemon@profesor.2asir.net>
To: usuario@profesor.2asir.net
Subject: Mail delivery failed: returning message to sender
Date: Thu, 29 Jan 2015 13:40:42 +0100

This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its
recipients. This is a permanent error. The following address(es) failed:

  erincon@iesmiravent.es
    Mailing to remote domains not supported

------ This is a copy of the message, including all the headers. ------

Return-path: <usuario@profesor.2asir.net>
Received: from usuario by profesor.2asir.net with local (Exim 4.80)
:
```

```
------ This is a copy of the message, including all the headers. ------

Return-path: <usuario@profesor.2asir.net>
Received: from usuario by profesor.2asir.net with local (Exim 4.80)
        (envelope-from <usuario@profesor.2asir.net>)
        id 1YGoOn-0000sr-TV
        for erincon@iesmiravent.es; Thu, 29 Jan 2015 13:40:41 +0100
To: erincon@iesmiravent.es
Subject: prueba correo desde linux exim
Message-Id: <E1YGoOn-0000sr-TV@profesor.2asir.net>
From: usuario <usuario@profesor.2asir.net>
Date: Thu, 29 Jan 2015 13:40:41 +0100

esto es una prueba desde exim
```

Vemos que nos manda un mensaje de error. Si vemos el log

```
2015-01-29 13:40:41 1YGoOn-0000sr-TV <= usuario@profesor.2asir.net U=usuario P=l
ocal S=426
2015-01-29 13:40:42 1YGoOn-0000sr-TV ** erincon@iesmiravent.es R=nonlocal: Maili
ng to remote domains not supported
2015-01-29 13:40:42 1YGoOo-0000sv-Ia <= <> R=1YGoOn-0000sr-TV U=Debian-exim P=lo
cal S=1294
2015-01-29 13:40:42 1YGoOn-0000sr-TV Completed
2015-01-29 13:40:42 1YGoOo-0000sv-Ia => usuario <usuario@profesor.2asir.net> R=l
ocal_user T=mail_spool
2015-01-29 13:40:42 1YGoOo-0000sv-Ia Completed
```