Exercises — Application — DNS

Martin Heusse

june 12th, 2007

1 Sending an email

We consider a mail sending attempt. We display bellow the concatenated ”data” sections of a number of TCP segments. “>” and “<” signs tell if the data is going to or coming from the server.

```
<220 heka.imag.fr ESMTP Sendmail 8.13.7/8.13.4/ImagV2.1.pm; Fri, 5 Jan 2007 18:24:09 +0100
>EHLO [129.88.38.134]
<250-heka.imag.fr Hello tome.imag.fr [129.88.38.134], pleased to meet you
<250-ENHANCEDSTATUSCODES
<250-PIPELINING
<250-EXPN
<250-VERB
<250-8BITMIME
<250-SIZE
<250-DSN
<250-ETRN
<250-AUTH GSSAPI DIGEST-MD5 CRAM-MD5
<250-DELIVERBY
<250 HELP
>MAIL FROM:<Martin.Heusse@imag.fr>
<250 2.1.0 <Martin.Heusse@imag.fr>... Sender ok
>RCPT TO:<Spirou@champignac.fr>
<250 2.1.5 <Spirou@champignac.fr>... Recipient ok
>DATA
<354 Enter mail, end with ”.” on a line by itself
>Mime-Version: 1.0
>Content-Transfer-Encoding: quoted-printable
>Message-Id: <F30B1679-AC3D-43B1-853C-ABCCD6B20525@imag.fr>
>Content-Type: text/plain; charset=ISO-8859-1; delsp=yes; format=flowed
>To: Spirou@champignac.fr
>From: Martin Heusse <Martin.Heusse@imag.fr>
>Subject: =?ISO-8859-1?Q?Votre_v=E9hicule?=
>Date: Fri, 5 Jan 2007 18:24:06 +0100
>
>Dear mister Spirou, your car is in the way.
>
>Thank you for moving it.
>Yours,
>M. Heusse
>
>
>.
```

Similar to http headers

end!

7 server -> client

8 client -> server

+ 7 SYN, SYNACK, ACK
Fin, Ack, Fin, Ack

20 packets at least

```
<250 2.0.0 l05HO9Z3022145 Message accepted for delivery
>QUIT
<221 2.0.0 heka.imag.fr closing connection
```

at least?

1. How many packets the server and client exchanged in both direction ? Do not forget packets that do not carry any information.
2. Do you think it's possible to send an e-mail that does not bear the actual receiver's address? Do you often use this functionality? How? → Mailing lists, CCi
3. Why is there no "`content-length`" field (that you would find in the MIME formatting in http)? What replaces it?

A few minutes later I get a message saying:

```
[...]
The original message was received at Fri, 5 Jan 2007 18:25:32 +0100 (CET)
from [IPv6:2001:660:5301:26:214:22ff:fe09:b6f8]

   ----- The following addresses had permanent fatal errors -----
<spirou@champignac.fr>
    (reason: 550 Host unknown)
[...]
```

4. What operations did the server carry out? What protocols and what servers were involved?

(1) MX query for champignac.fr → No answer
(2) email server (carrefour) queries MX for imag.fr
which DNS server was queried?
→ NS for fr
→ NS for champ...
(if domain does exist)

2 DNS

Explain the different times observed for executing the commands bellow:

how long?

```
> time host -t a www.gov.uz
www.gov.uz has address 91.212.89.21

real 0m0.610s
user 0m0.003s
sys 0m0.005s
```

~ 610 ms -

```
> time host -t a www.gov.uz
www.gov.uz has address 91.212.89.21

real 0m0.011s
user 0m0.003s
sys 0m0.005s
```

60 times faster!
→ effect of DNS cache on the server

```
[Here, some time has passed]

> time host -t a www.gov.uz
www.gov.uz has address 91.212.89.21
```

~800 ms → full DNS resolution
recursive

```
real 0m0.774s
user 0m0.003s
sys 0m0.006s

> time host -t a www.gov.uz
www.gov.uz has address 91.212.89.21
real 0m0.011s
user 0m0.003s
sys 0m0.005s

> time host -t a xxx.gov.uz
Host xxx.gov.uz not found: 3(NXDOMAIN)
real 0m0.201s
user 0m0.003s
sys 0m0.004s
```

www.gov.uz is in cache

~~timeout~~

200 ms ?

DNS server (NS) for uz
DNS server for gov.uz
} are in cache

↳ queried directly —

xxx.com.uz would ~~[illegible]~~ take 400 ms or so (provided that com.uz exists ...)