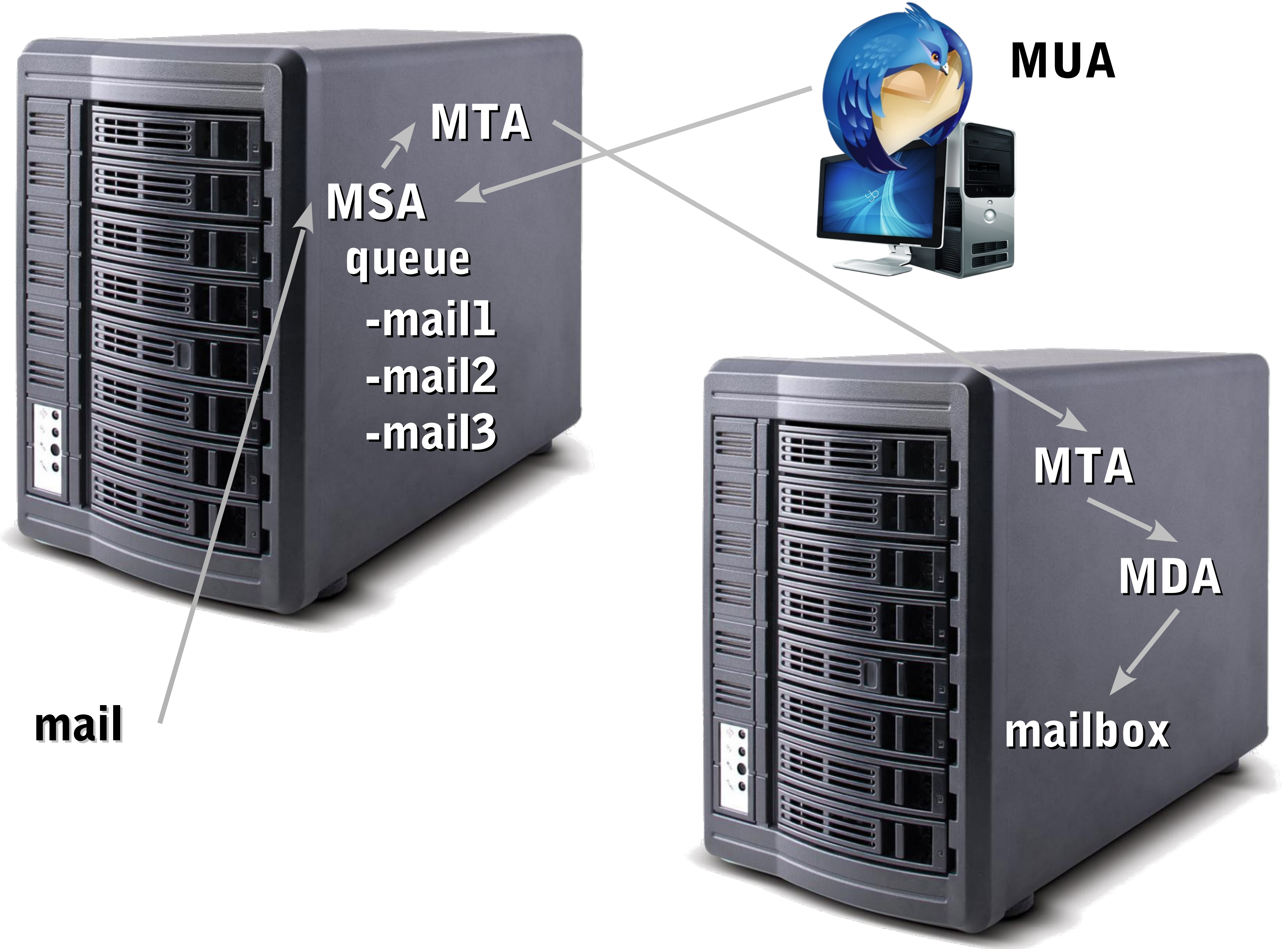
Send Mail Transport Protocol (SMTP)

- 1982 - RFC 821
- 2008 - RFC 5321 (ESMTP)
- TCP ports 25 and 587
- Mail User Agent(MUA)
- Mail Submission Agent(MSA)
- Mail Transfer Agent(MTA)
- Mail Delivery Agent(MDA)



MUA

MTA

MSA

queue

-mail1

-mail2

-mail3

mail

MTA

MDA

mailbox

SMTP commands

- HELO
- EHLO
- MAIL FROM:
- RCPT TO:
- DATA
- RSET
- VRFY
- HELP
- QUIT
- Valid replies (2xx)
- Transient errors(4xx)
- Permanent errors(5xx)

SMTP commands

```
hackman@terion:~$ telnet yuhu.biz 25
Trying 85.14.7.4...
Connected to yuhu.biz.
Escape character is '^]'.
220 blackpearl.yuhu.biz ESMTP Postfix (2.1.1)
HELO
501 Syntax: HELO hostname
HELO yuhu.biz
250 blackpearl.yuhu.biz
```

SMTP commands

```
hackman@terion:~$ telnet yuhu.biz 25
Trying 85.14.7.4...
Connected to yuhu.biz.
Escape character is '^]'.
220 blackpearl.yuhu.biz ESMTP Postfix (2.1.1)
EHLO yuhu.biz
250-blackpearl.yuhu.biz
250-PIPELINING
250-SIZE 30720000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH CRAM-MD5 PLAIN LOGIN DIGEST-MD5
250-AUTH=CRAM-MD5 PLAIN LOGIN DIGEST-MD5
250 8BITMIME
```

SMTP commands

```
hackman@terion:~$ telnet yuhu.biz 25
Trying 85.14.7.4...
Connected to yuhu.biz.
Escape character is '^]'.
HELO yuhu.biz
250 blackpearl.yuhu.biz
MAIL FROM: mm@yuhu.biz
250 Ok
RCPT TO: mm@yuhu.biz
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: testing
test 1
.
250 Ok: queued as 450D1156263C
```

SMTP commands

```
hackman@terion:~$ telnet yuhu.biz 25
Trying 85.14.7.4...
Connected to yuhu.biz.
Escape character is '^]'.
HELO yuhu.biz
250 blackpearl.yuhu.biz
VRFY hackman@yuhu.biz
252 hackman@yuhu.biz
VRFY dsadas@yuhu.biz
550 <dsadas@yuhu.biz>: Recipient address
rejected: User unknown in virtual mailbox table
RSET
250 Ok
quit
221 Bye
```

SMTP

- Retry interval, at least 30min
- Give-up time, at least 4-5 days
- Storage - either Mailbox or Maildir
- Failover setup

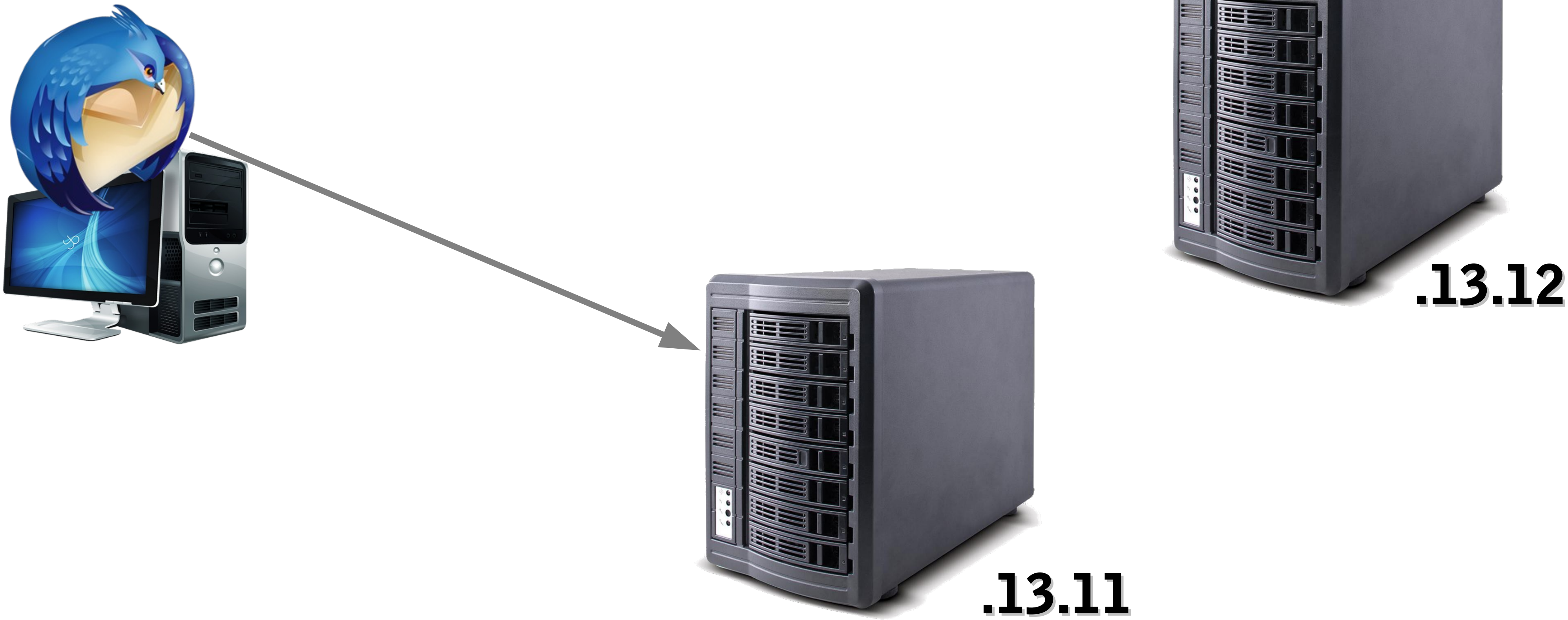
SMTP
Mailbox vs. Maildir

```
mail# ls -1A
Spam
mail-trash
saved-drafts
saved-messages
sent-mail
```

```
mail# ls -1A
camera/
cur/
new/
tmp/
```

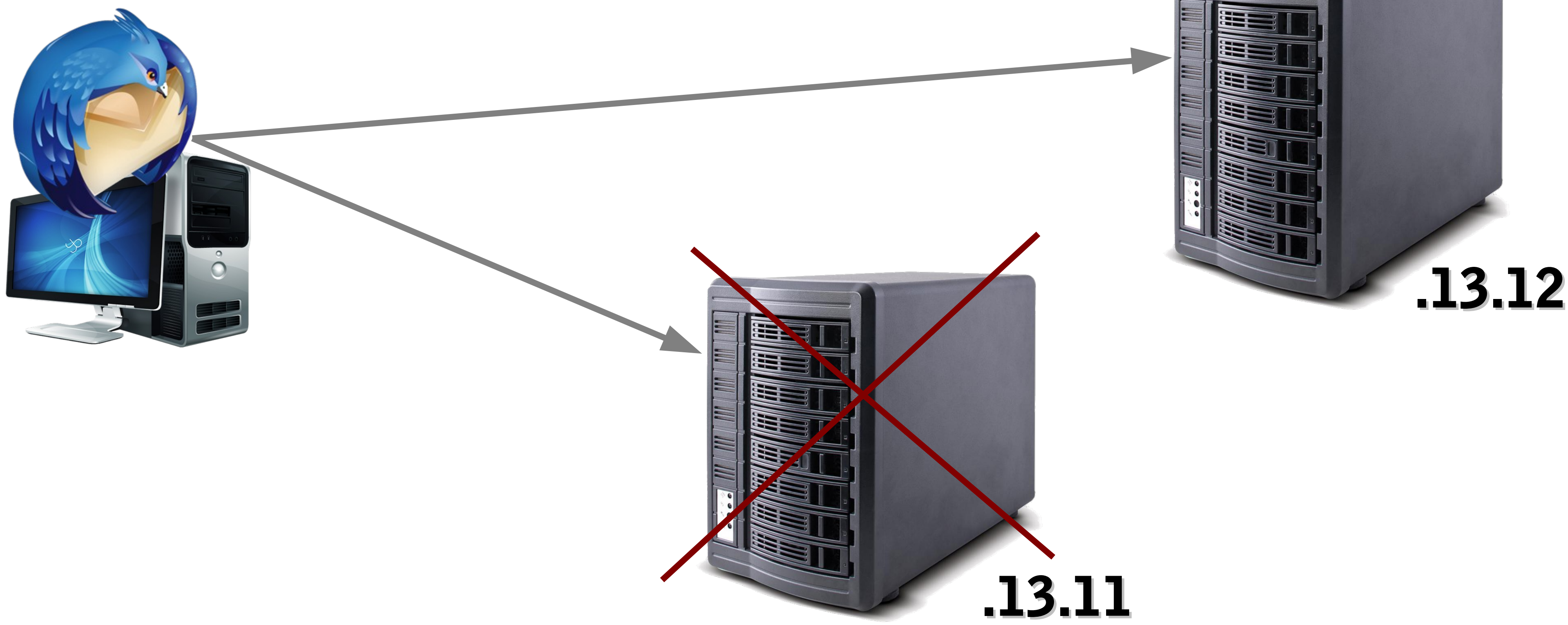
SMTP failover

```
        IN MX 10 mail.example.com.
        IN MX 20 mail2.example.com.
mail    IN A 123.123.13.11
mail2   IN A 123.123.13.12
```



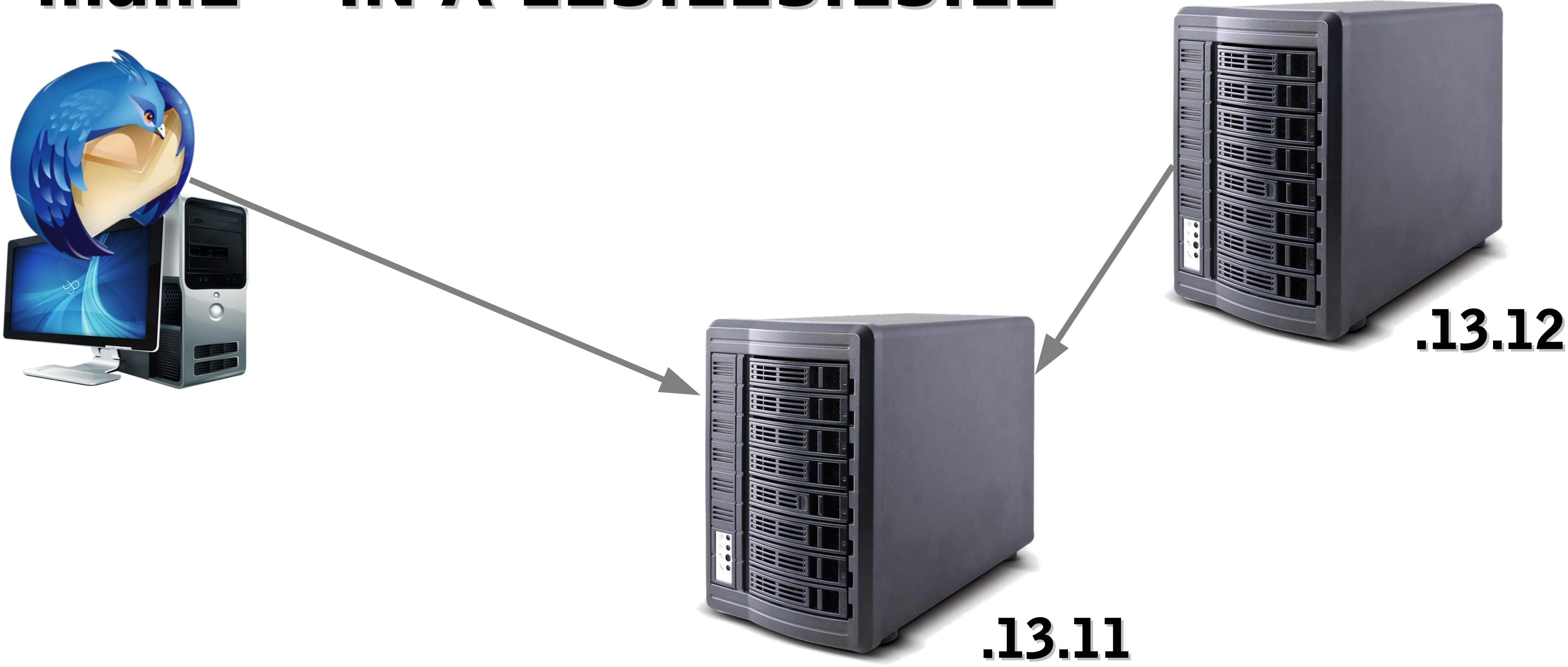
SMTP failover

```
      IN MX 10 mail.example.com.
      IN MX 20 mail2.example.com.
mail  IN A 123.123.13.11
mail2 IN A 123.123.13.12
```



SMTP failover

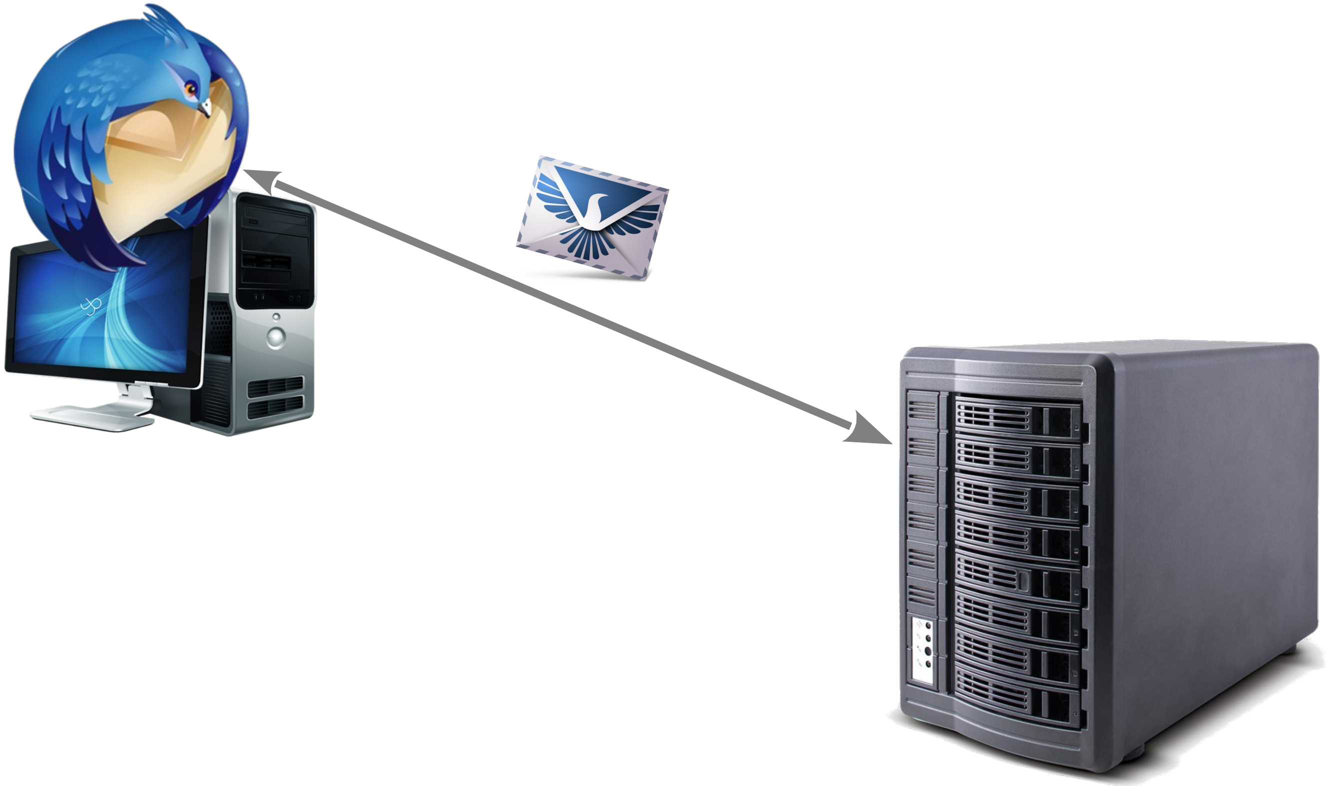
```
        IN MX 10 mail.example.com.
        IN MX 20 mail2.example.com.
mail    IN A 123.123.13.11
mail2   IN A 123.123.13.12
```



Post Office Protocol - POP

- 1984 – POP - RFC 918
- 1985 – POP2 - RFC 973
- 1988 – POP3 - RFC 1081
- 1996 – POP3 - RFC 1939
- TCP ports 110, 995(SSL)

POP3 commands



- USER
- PASS
- LIST
- STAT
- UIDL
- RETR
- DELE
- QUIT
- Valid replies (+OK)
- Negative replies(-ERR)
- Single connection

POP3 commands

```
hackman@BlackPearl: ~$ telnet localhost 110
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
+OK Dovecot ready.
USER userX@yuhu.biz
+OK
PASS Jer0n1m0!
+OK Logged in.
STAT
+OK 1717 21744442
```

POP3 commands

```
LIST
+OK 1717 messages:
1 8482
2 80853
3 33093
4 5543
.....
1715 8060
1716 6558
1717 4615
.
RETR 1717
___mail message here___
.
DELE 1717
+OK Marked to be deleted.
```

Interactive Message Access Protocol - IMAP

- 1988 – IMAP 2 - RFC 1064
- 1991 – IMAP 3 - RFC 1203
- 2003 – IMAP 4 - RFC 3501
  - becomes INTERNET MESSAGE ACCESS PROTOCOL
- 2011 – SRV records – RFC 6186
- 2013 – IMAP 4 - RFC 6858
- TCP port 143, 993(SSL)

Interactive Message Access Protocol - IMAP

- **Support multiple connections**
- **Supports folders**
- **Support pulling only the headers of the e-mail, pull the data on demand**
- **Support mail PUSH(sending mail)**

IMAP SRV records - RFC6186

_submission._tcp.example.com.   SRV 0 1 587 mail.example.com.

_service._proto.name TTL class SRV priority weight port target

- service: the symbolic name of the desired service.
- proto: the transport protocol of the desired service; this is usually either TCP or UDP.
- name: the domain name for which this record is valid.
- TTL: standard DNS time to live field.
- class: standard DNS class field (this is always IN).
- priority: the priority of the target host, lower value means more preferred.
- weight: A relative weight for records with the same priority.
- port: the TCP or UDP port on which the service is to be found.
- target: the canonical hostname of the machine providing the service.

IMAP Basic commands

- a001 login USER PASS
- a001 logout
- a001 select FOLDER
- a001 list "" *
- a001 fetch PARAM
  - ALL/HEADERS/BODY
- a001 delete "Message"
- Valid replies - (a00x OK)
- Negative replies - (a00x BAD or NO)

IMAP

```
hackman@BlackPearl: ~$ telnet localhost 143
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR
LOGIN-REFERRALS ID ENABLE IDLE STARTTLS
AUTH=PLAIN] Dovecot ready.
a001 login userX@yuhu.biz Jer0n1m0!
a001 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR
LOGIN-REFERRALS ID ENABLE IDLE SORT
SORT=DISPLAY THREAD=REFERENCES
THREAD=REFS MULTIAPPEND UNSELECT CHILDREN
NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1
CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES
WITHIN CONTEXT=SEARCH LIST-STATUS QUOTA]
Logged in
```

IMAP

```
a002 list
a002 BAD Error in IMAP command LIST: Invalid
reference.
a003 select inbox
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft
$label2)
* OK [PERMANENTFLAGS (\Answered \Flagged
\Deleted \Seen \Draft $label2 \*)] Flags permitted.
* 1714 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1330989345] UIDs valid
* OK [UIDNEXT 59881] Predicted next UID
* OK [HIGHESTMODSEQ 1] Highest
a003 OK [READ-WRITE] Select completed.
```

IMAP

```
a004 list "" *
* LIST (\HasNoChildren) "." "Spam"
* LIST (\HasNoChildren) "." "INBOX"
a004 OK List completed.
a005 FETCH 1:15 ENVELOPE
* 1 FETCH (ENVELOPE ("Thu, 23 May 2013 07:58:06
+0000" "RE: svn commit: r1484852 - in
/httpd/httpd/trunk: CHANGES
modules/http/http_filters.c"
* 2 FETCH (ENVELOPE ("Thu, 23 May 2013 10:17:56
+0200" {89}......
...
* 15 FETCH (ENVELOPE ..........
a005 OK Fetch completed.
```

Hypertext Transfer Protocol HTTP

- **1995 – HTML 2.0 - RFC 1866**
- **1996 – HTTP/1.0 - RFC 1945**
- **1997 – HTTP/1.1 - RFC 2068**
- **1999 – HTTP/1.1 - RFC 2616**
- **2012 – STATUS codes – RFC 6585**
- **1995 – URI - RFC 1808**
- **2005 – URI - RFC 3986**

- **Uniform Resource Identifier (URI)**

proto :// userinfo @ host : port / path

user : pass

user

Hypertext Transfer Protocol HTTP

- Absolute URI or Path
  - http://x.com/images/srpr/logo4w.png
  - /images/srpr/logo4w.png

- Request methods
  - GET
  - POST
  - HEAD
  - OPTIONS
  - CONNECT

Hypertext Transfer Protocol HTTP

- Request methods
  - GET
  - POST
  - HEAD
  - OPTIONS
  - CONNECT

HTTP

- Request Headers
  - Host
  - Accept-Charset
  - Accept-Encoding
  - Authorization
  - Range
  - Referer
  - User-Agent

HTTP/1.0 vs. HTTP/1.1

- **Methods**
  - **GET**
  - **HEAD**
  - **POST**

- **Methods**
  - **GET**
  - **HEAD**
  - **POST**
  - **OPTIONS**
  - **CONNECT**
  - **PUT**
  - **DELETE**

HTTP/1.0 vs. HTTP/1.1

- Headers
  - Authorization
  - Referer
  - User-Agent

- Headers
  - Host
  - Accept-Charset
  - Accept-Encoding
  - Authorization
  - Range
  - Referer
  - User-Agent

HTTP/1.0 vs. HTTP/1.1

```
hackman@terion:~$ telnet google.com 80
Trying 173.194.39.100...
Connected to google.com.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.0 302 Found
Location: http://www.google.bg/
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Date: Thu, 06 Jun 2013 08:35:46 GMT
Server: gws
Content-Length: 218


Connection closed.
```

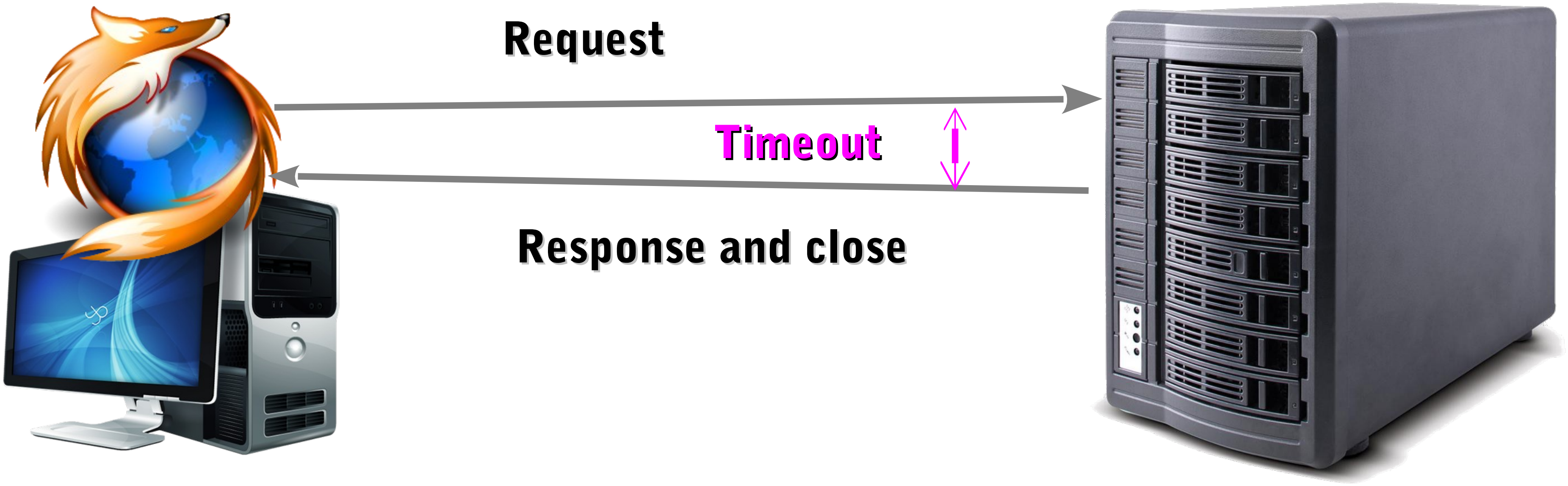
HTTP/1.0 vs. HTTP/1.1

```
hackman@terion:~$ telnet google.com 80
Trying 173.194.39.99...
Connected to google.com.
Escape character is '^]'.
GET / HTTP/1.1
Host: google.com

HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Date: Thu, 06 Jun 2013 08:36:01 GMT
Expires: Sat, 06 Jul 2013 08:36:01 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 219

.......Connection still open.....
```

HTTP OPTIONS

```
hackman@terion:~$ telnet s1 81
Trying 192.168.155.100...
Connected to s1.
Escape character is '^]'.
OPTIONS / HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 06 Jun 2013 15:13:30 GMT
Server: Apache
Allow: GET,HEAD,POST,OPTIONS
Host-Header: 192fc2e7e50945beb8231a492d6a8024
Content-Length: 0
Connection: close
Content-Type: text/html
```

HTTP/1.0 request

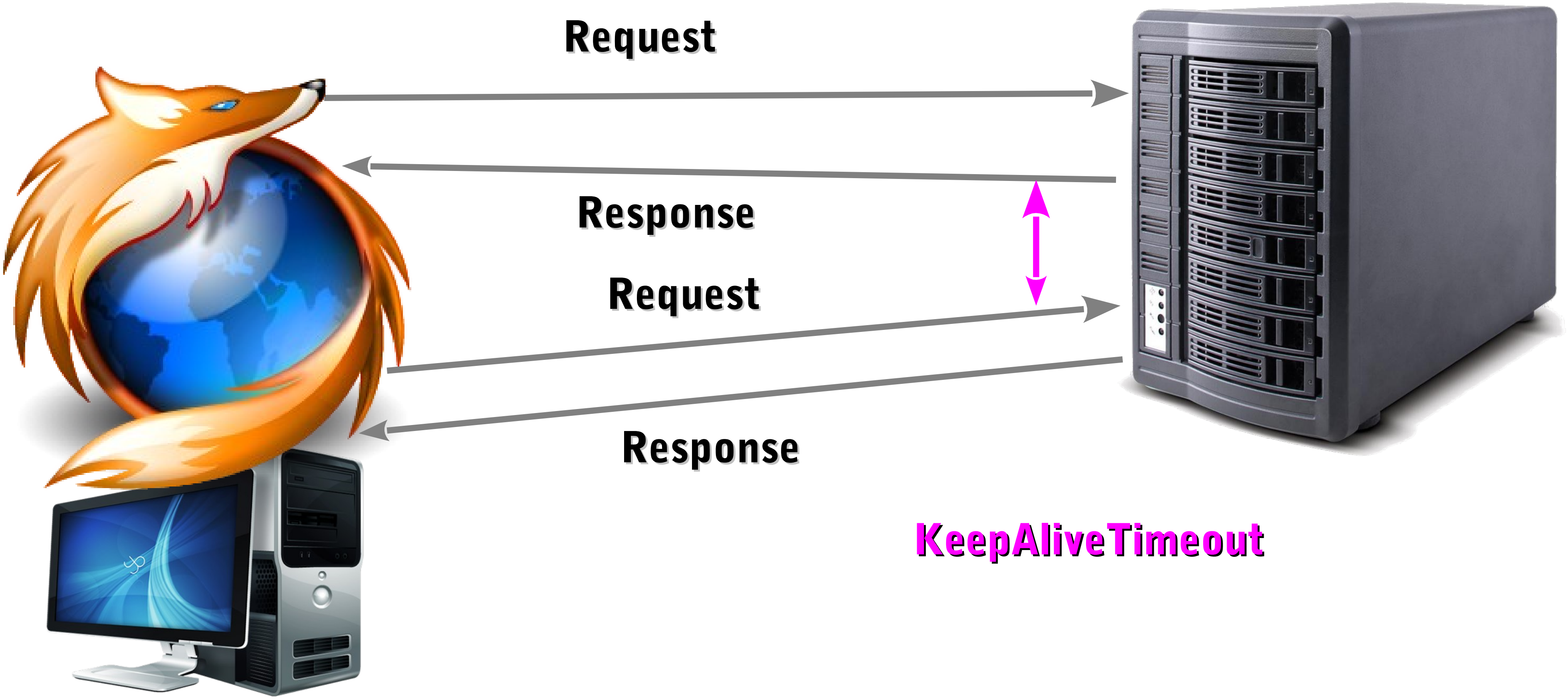


Request

Timeout

Response and close

HTTP/1.1 request



Request

Response

Request

Response

KeepAliveTimeout

HTTP

- **Request with header**
- **Request with cookie**
- **Difference between normal and HEAD requests**