Description

http://www.netkit.org/

contact@netkit.org

A. Cecchetti, G. Di Battista, M. Patrignani, M. Pizzonia, M. Rimondini

Version

2.3

Author(s)

A. Cecchetti, G. Di Battista, M. Patrignani, M. Pizzonia, M. Rimondini

E-mail

contact@netkit.org

Web

http://www.netkit.org/

Description

configuring e-mail servers, sending and receiving e-mails
copyright notice

- All the pages/slides in this presentation, including but not limited to, images, photos, animations, videos, sounds, music, and text (hereby referred to as “material”) are protected by copyright.
- This material, with the exception of some multimedia elements licensed by other organizations, is property of the authors and/or organizations appearing in the first slide.
- This material, or its parts, can be reproduced and used for didactical purposes within universities and schools, provided that this happens for non-profit purposes.
- Information contained in this material cannot be used within network design projects or other products of any kind.
- Any other use is prohibited, unless explicitly authorized by the authors on the basis of an explicit agreement.
- The authors assume no responsibility about this material and provide this material “as is”, with no implicit or explicit warranty about the correctness and completeness of its contents, which may be subject to changes.
- This copyright notice must always be redistributed together with the material, or its portions.
pine copyright notice

- This lab makes use of the mail user agent pine, which is a registered trademark of the University of Washington
- Licensing information about pine can be found at http://www.washington.edu/pine/
the dns name hierarchy (revised)
zones (revised)

zones

served by dnsroot

served by dnsorg.org

served by dnsnet.net

served by dnsnano.nanoinside.net

served by dnslug.lugroma3.org

served by dnsnano.nanoinside.net
zones

- some domains (nodes) manage mail users

- guest@lugroma3.org
- guest@nanoinside.net
- guest@nanoinside.net
- guest@lugroma3.org
mail exchangers

- each domain allowing users must have at least one Mail eXchanger (MX)
- a mail exchanger is the server in charge of collecting incoming mails for a specific domain (e.g., lugroma3.org)
mail exchangers

- in order to know which is the mail exchanger for a domain:
  - find the name server (NS) for the zone in which the node (=domain) falls
  - ask the NS which is the mail exchanger (MX) for the domain
incoming mail

- users sit anywhere in the network and start a software (Mail User Agent) that allows to connect to mail servers and manage incoming/outgoing mails
  - examples: Outlook, Pine, Mozilla, Thunderbird, ...

![Diagram showing the connection between host1, host2, host3, host4, domain, zone, and user@domain]
incoming mail

- the incoming mail server may coincide with the mail exchanger for its domain
- users must authenticate on the incoming mail server in order to get their incoming mails
incoming mail

- the protocols used to transfer incoming mail are
  - POP3 (*Post Office Protocol*, port 110)
    - allows to get mail from the inbox
  - IMAP (*Interactive Mail Access Protocol*, port 143)
    - allows to handle remote mail folders as if they were local
outgoing mail

- a Mail Transfer Agent is a server acting as an outgoing mail dispatcher
- users choose an MTA (accepting their outgoing mails) as their outgoing mail server
outgoing mail

- in general, users do not need to authenticate on MTAs
- the protocol used to transfer outgoing mail is SMTP (Simple Mail Transfer Protocol, port 25)
incoming and outgoing mail servers

- the incoming mail server and the outgoing mail server may be the same host
configuring a mail service (user side)

- configuring a mail user agent consists of
  - specifying an incoming mail server (plus the authentication information)
  - specifying an outgoing mail (SMTP) server
in this lab...

...and usually in the real world...

...domains and zones coincide
in this lab...

- ...and usually in the real world...
  - ...domains and zones coincide
  - ...the name server for the zone is also the mail exchanger for the domain

```
guest@lugroma3.org
```

```
host1  host3  lugroma3  host4  host5
```

```
MX  NS
```

```
dnslug
```

```
MTA
```

© Computer Networks Research Group Roma Tre
in this lab...

...and usually in the real world...

- ...domains and zones coincide
- ...the name server for the zone is also the mail exchanger for the domain
- ...the user sits in front of a pc inside the domain

© Computer Networks Research Group Roma Tre
in this lab...

...and usually in the real world...
  ...the incoming mail server is the mail exchanger for the domain
in this lab...

- ...and usually in the real world...
  - ...the incoming mail server is the mail exchanger for the domain
  - ...the outgoing mail server is the mail exchanger for the domain

```
host5

guest@lugroma3.org
```

© Computer Networks Research Group Roma Tre
step 1 – network topology

- flat, largely orthogonal to the DNS hierarchy
step 1 – dns (zone) hierarchy

- ""
  - org
    - lugroma3
      - pc1
        - served by dnsorg.org
    - served by dnsroot
  - net
    - served by dnsnet.net
    - nanoinside
      - pc2
        - served by dnsnano.nanoinside.net
  - abc
    - domain name

- domain name: abc
- served by: dnsnet.net
- served by: dnsorg.org
- served by: dnsroot
- served by: dnsnano.nanoinside.net
- served by: dnsslug.lugroma3.org
- served by: dnsorg.org
- served by: dnsroot

netkit – [ lab: email ]

last update: Apr 2007

© Computer Networks Research Group Roma Tre
**step 2 – checking the configuration**

The configuration of the PCs consists of the following information:

<table>
<thead>
<tr>
<th></th>
<th>pc1</th>
<th>pc2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name server</strong></td>
<td>192.168.0.11 dnslug.lugroma3.org</td>
<td>192.168.0.22 dnnano.nanoinside.net</td>
</tr>
<tr>
<td><strong>/etc/resolv.conf</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>incoming mail server</strong></td>
<td>192.168.0.11 imap.lugroma3.org pop.lugroma3.org</td>
<td>192.168.0.22 imap.nanoinside.net pop.nanoinside.net</td>
</tr>
<tr>
<td><strong>outgoing mail server</strong></td>
<td>192.168.0.11 mail.lugroma3.org</td>
<td>192.168.0.22 mail.nanoinside.net</td>
</tr>
</tbody>
</table>
step 2 – checking the configuration

- the configuration of the mail transfer agents consists of (at least):
  - the specification of the local domain
    - if the recipient of a mail is inside the local domain, the mta does not forward the mail any further
  - relaying settings
    - an mta forwarding mails between a domain and another performs relaying
    - since our mail users are located inside two different domains (lugroma3.org and nanoinside.net), relaying must be enabled
step 2 – checking the configuration

- the configuration of the name servers is the same as in the dns lab

```
served by
dnsroot

served by
dnsorg.org

served by
dnsnet.net

served by
dnsnano.nanoinside.net
```

```
served by
dnsroot

served by
dnsorg.org

served by
dnsnet.net

served by
dnsnano.nanoinside.net
```
step 3 – starting the lab

- upon launching the lab
  - 7 virtual machines are started
  - all the network interfaces are configured
  - name servers are automatically configured and started
  - mtas are automatically configured and started
  - muas are automatically configured

```bash
user@localhost:~$ cd netkit-lab_email
user@localhost:~/netkit-lab_email$ lstart
```
step 4 – involved software

- **mua**: pine*
- **mta**: exim4
- **name server**: bind
- **pop/imap server**: ipop3d, imapd (handled by inetd)

*©1998-2005 University of Washington
step 4 – involved software

- start pine on \texttt{pc1}

\begin{verbatim}
\texttt{pc1:~# pine \} }
\end{verbatim}

- pine asks you for a password
  - that is the password to login on the incoming mail server
  - the password is "\texttt{guest}"
step 4 – involved software

- investigate the configuration of pine

Copyright 1989-2005. PINE is a trademark of the University of Washington.
step 4 – involved software

- investigate the configuration of pine

This is the Setup screen for Pine. Choose from the following commands:

(E) Exit Setup:
   This puts you back at the Main Menu.

(P) Printer:
   Allows you to set a default printer and to define custom print commands.

(N) Newpassword:
   Change your password.

(C) Config:
   Allows you to set many features which are not turned on by default. You may also set the values of many options with that command.

Press 'C'
step 4 – involved software

- investigate the configuration of pine

```

PINE 4.64 MAIN MENU
Folder: INBOX  No Messages

personal-name = Root user on PC1
user-domain = lugroma3.org
smtp-server = mail.lugroma3.org
nntp-server = <No Value Set>
inbox-path = {imap.lugroma3.org/user=guest}inbox
incoming-archive-folders = <No Value Set>
pruned-folders = <No Value Set>
default-fcc = <No Value Set: using "sent-mail">
default-saved-msg-folder = <No Value Set: using "saved-messages">
postponed-folder = <No Value Set: using "postponed-msgs">
read-message-folder = <No Value Set>
form-letter-folder = <No Value Set>
literal-signature = <No Value Set>
signature-file = <No Value Set: using ".signature">
feature-list =

Help E Exit Setup P Prev PrevPage A Add Value X Print
C [Change Val] N Next Spc NextPage D Delete Val W WhereIs

```
step 4 – involved software

- investigate the configuration of pine

![PINE 4.64 main menu with configuration settings]

- personal-name = Root user on PC1
- user-domain = lugroma3.org
- smtp-server = mail.lugroma3.org
- nntp-server = <No Value Set>
- inbox-path = {imap.lugroma3.org/user=guest}inbox
- incoming-archive-folders = <No Value Set>
- pruned-folders = <No Value Set>
- default-fcc = <No Value Set: using "sent"
- default-saved-msg-folder = <No Value Set:
- postponed-folder = <No Value Set:
- read-message-folder = <No Value Set:
- form-letter-folder = <No Value Set:
- literal-signature = <No Value Set:
- signature-file = <No Value Set:
- feature-list = <No Value Set:

This is a descriptive name identifying the sender; the recipient will see it in the “From” field.
step 4 – involved software

- investigate the configuration of pine

name of the local domain
step 4 – involved software

- investigate the configuration of pine

outgoing (SMTP) mail server; note that no authentication is needed
step 4 – involved software

- investigate the configuration of pine

PC1

PINE 4.64 MAIN MENU
Folder: INBOX No Messages

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>personal-name</td>
<td>Root user on PC1</td>
</tr>
<tr>
<td>user-domain</td>
<td>lugroma3.org</td>
</tr>
<tr>
<td>smtp-server</td>
<td>mail.lugroma3.org</td>
</tr>
<tr>
<td>nntp-server</td>
<td>&lt;No Value Set&gt;</td>
</tr>
<tr>
<td>inbox-path</td>
<td>{imap.lugroma3.org/user=guest}inbox</td>
</tr>
<tr>
<td>incoming-archive-folders</td>
<td>&lt;No Value Set&gt;</td>
</tr>
<tr>
<td>pruned-folders</td>
<td>&lt;No Value Set&gt;</td>
</tr>
<tr>
<td>default-folder</td>
<td>&lt;No Value Set: using &quot;sent&quot;</td>
</tr>
<tr>
<td>default-saved-messages</td>
<td>&lt;No Value Set: using &quot;saved&quot;</td>
</tr>
<tr>
<td>location of the incoming mailbox; syntax: {server_name/protocol/user=username}folder_name</td>
<td></td>
</tr>
</tbody>
</table>
  - server_name: name/address of the incoming mail server
  - protocol: (optional) may be imap or pop3 (default: imap)
  - username: (optional) login name on the incoming mail server
  - folder_name: should be inbox
step 4 – involved software

- investigate the configuration of pine

- note that
  - the only available mail user account is guest
  - the only available local user account on the pcs is root

- hence
  - mail sent from the pcs has a sender address of the form root@
  - replying to it would result in sending a mail to an invalid mail user
step 4 – involved software

- investigate the configuration of pine
- solution
  - create a local guest account on the pcs and use it to send mail, or...
  - ...configure pine to automatically include a correct Reply-To address in the sent mail
- in this lab we choose the second solution
step 4 – involved software

- investigate the configuration of pine

use the address in the Reply-To header value (instead of From) to answer e-mails
step 4 – involved software

- investigate the configuration of pine

```
[ ] unselect-will-not-advance
[ ] use-current-dir
[ ] use-regular-startup-rule-for-stayopen-folders
[ ] use-subshell-for-suspend
initial-keystroke-list = <No Value Set>
default-composer-hdrs = <No Value Set>
customized-hdrs = Reply-To: guest@lugroma3.org
viewer-hdrs = <No Value Set>
viewer-margin-left = <No Value Set: using "0">
viewer-margin-right = <No Value Set: using "4">
quote-suppression-threshold = <No Value Set: using "0">
saved-msg-name-rule =
    Set     Rule Values
    --------
    () by-from
    () by-nick-of-from
```

address to be placed in the **Reply-To** header (note that the header name must be included as well)
step 4 – involved software

- move on to machine `dnslug`
- check for the running servers:

```bash
dnslug:~# ps ax
```

<table>
<thead>
<tr>
<th>PID</th>
<th>TTY</th>
<th>STAT</th>
<th>TIME</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>243</td>
<td>?</td>
<td>Ss</td>
<td>0:00</td>
<td>/usr/sbin/named</td>
</tr>
<tr>
<td>250</td>
<td>?</td>
<td>Ss</td>
<td>0:00</td>
<td>/usr/sbin/exim4 -bd -q30m</td>
</tr>
<tr>
<td>256</td>
<td>?</td>
<td>Ss</td>
<td>0:00</td>
<td>/usr/sbin/inetd</td>
</tr>
<tr>
<td>259</td>
<td>tty0</td>
<td>Rs</td>
<td>0:00</td>
<td>-bash</td>
</tr>
<tr>
<td>260</td>
<td>vc/1</td>
<td>Ss+</td>
<td>0:00</td>
<td>-bash</td>
</tr>
<tr>
<td>298</td>
<td>tty0</td>
<td>R+</td>
<td>0:00</td>
<td>ps ax</td>
</tr>
</tbody>
</table>

dnslug:~# ▶

name server (bind)

mail transfer agent

pop3 and imap servers (handled by inetd)
step 4 – involved software

- the name server is configured in the same way as for the dns lab, apart from some additional MX and A records

```
dnslug:~# less /etc/bind/db.org.lugroma3
... @       IN      NS      dnslug.lugroma3.org.
@       IN      MX 5    mail.lugroma3.org.
dnslug  IN      A       192.168.0.11
pc1     IN      A       192.168.0.111
imap    IN      A       192.168.0.11
pop     IN      A       192.168.0.11
mail    IN      A       192.168.0.11
```

/etc/bind/db.org.lugroma3
step 4 – involved software

- the name server is configured in the same way as for the dns lab, apart from some additional MX and A records

```
@       IN      NS      dnslug.lugroma3.org.
@       IN      MX 5      mail.lugroma3.org.
dnslug          IN      A       192.168.0.11
pc1             IN      A       192.168.0.111
imap            IN      A       192.168.0.11
pop             IN      A       192.168.0.11
mail            IN      A       192.168.0.11
```

mail.lugroma3.org is the mail exchanger for domain lugroma3.org (@)

a preference value (lower is better)

imap.lugroma3.org, pop.lugroma3.org, and mail.lugroma3.org are the same host
step 4 – involved software

the name of the mail exchanger for a given domain can be retrieved by querying the DNS.

- type of record to look for
- find the MX for domain nanoinside.net
- get a terse answer
- preference value

PC:

```
pc1:~# dig MX nanoinside.net +short
5 mail.nanoinside.net.
```

netkit – [ lab: email ]
step 4 – involved software

- the mta (exim4) is configured as follows:

```
dnslug:~# less /etc/exim4/exim4.conf
...
ifndef MAIN_LOCAL_DOMAINS
MAIN_LOCAL_DOMAINS = @:localhost:lugroma3.org
.endif
domainlist local_domains = MAIN_LOCAL_DOMAINS

ifndef MAIN_RELAY_TO_DOMAINS
MAIN_RELAY_TO_DOMAINS = nanoinside.net
.endif
domainlist relay_to_domains = MAIN_RELAY_TO_DOMAINS

ifndef MAIN_RELAY_NETS
MAIN_RELAY_NETS = 192.168.0.0/24
.endif
hostlist relay_from_hosts = 127.0.0.1 : :::1 : MAIN_RELAY_NETS
```

domains for which mail is accepted (not further relayed); this is the list of domains for which this host must be considered the final destination
step 4 – involved software

the mta (exim4) is configured as follows:

dnslug:~# less /etc/exim4/exim4.conf
...
ifndef MAIN_LOCAL_DOMAINS
MAIN_LOCAL_DOMAINS = @:localhost:lugroma3.org
.endif
domainlist local_domains = MAIN_LOCAL_DOMAINS

ifndef MAIN_RELAY_TO_DOMAINS
MAIN_RELAY_TO_DOMAINS = nanoinside.net
.endif
domainlist relay_to_domains = MAIN_RELAY_TO_DOMAINS

ifndef MAIN_RELAY_NETS
MAIN_RELAY_NETS = 192.168.0.0/24
.endif
hostlist relay_from_hosts = 127.0.0.1 : ::::1 : MAIN_RELAY_NETS

domains to which we accept to relay (forward) mail
step 4 – involved software

- the mta (exim4) is configured as follows:

```bash
dniud:~# less /etc/exim4/exim4.conf
...
ifndef MAIN_LOCAL_DOMAINS
MAIN_LOCAL_DOMAINS = @:localhost:lugroma3.org
endif
domainlist local_domains = MAIN_LOCAL_DOMAINS

ifndef MAIN_RELAY_TO_DOMAINS
MAIN_RELAY_TO_DOMAINS = nanoinside.net
endif
domainlist relay_to_domains = MAIN_RELAY_TO_DOMAINS

ifndef MAIN_RELAY_NETS
MAIN_RELAY_NETS = 192.168.0.0/24
endif
hostlist relay_from_hosts = 127.0.0.1 : :: : MAIN_RELAY_NETS
```

subnet(s) *from* which we accept to relay mail
step 4 – involved software

- Whenever a connection request to port 110 (pop3) or 143 (imap) arrives, inetd launches the appropriate daemon on the fly to service it.

```bash
dnslug:~# less /etc/inetd.conf
...  
#:MAIL: Mail, news and uucp services.
pop3 stream tcp nowait root /usr/sbin/tcpd /usr/sbin/ipop3d
imap stream tcp nowait root /usr/sbin/tcpd /usr/sbin/imapd
```

/etc/inetd.conf
step 4 – involved software

Whenever a connection request to port 110 (pop3) or 143 (imap) arrives, inetd launches the appropriate daemon on the fly to service it.

```
# MAIL: Mail, news and uucp services.
pop3    stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin pop3    stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/tcpd /usr/sbin/tcpd
```

Service name (must exist in /etc/services)
step 4 – involved software

- Whenever a connection request to port 110 (pop3) or 143 (imap) arrives, inetd launches the appropriate daemon on the fly to service it.

```
dnslug:~# less /etc/inetd.conf
...
#:MAIL: Mail, news and uucp services.
pop3  stream  tcp  nowait  root  /usr/sbin/tcpd /usr/sbin/pop3d
imap  stream  tcp  nowait  root  /usr/sbin/tcpd /usr/sbin/imapd
```

socket type (stream, dgram, etc.)
step 4 – involved software

- whenever a connection request to port 110 (pop3) or 143 (imap) arrives, inetd launches the appropriate daemon on the fly to service it.
step 4 – involved software

- whenever a connection request to port 110 (pop3) or 143 (imap) arrives, inetd launches the appropriate daemon on the fly to service it.

```
# MAIL: Mail, news and uucp services.
pop3    stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/pop3d
imap    stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/imapd
```

only applicable to datagram sockets
step 4 – involved software

Whenever a connection request to port 110 (pop3) or 143 (imap) arrives, inetd launches the appropriate daemon on the fly to service it.

```
# MAIL: Mail, news and uucp services.
pop3    stream    tcp    nowait    root    /usr/sbin/tcpd 
    /usr/sbin/pop3d
imap    stream    tcp    nowait    root    /usr/sbin/tcpd 
    /usr/sbin/imapd
```

(name of the user who starts the daemon; change it to run services with restricted privileges)
step 4 – involved software

Whenever a connection request to port 110 (pop3) or 143 (imap) arrives, inetd launches the appropriate daemon on the fly to service it.

```
dnslug:~# less /etc/inetd.conf
... ...
#:MAIL: Mail, news and uucp services.
pop3 stream tcp nowait root /usr/sbin/tcpd /usr/sbin pop3 ...
imap stream tcp nowait root /usr/sbin/tcpd /usr/sbin/imapd ...
```

Daemon name: `tcpd` (is a wrapper providing logging and simple access control capabilities)
step 4 – involved software

- this lab has two mail exchangers
  - mail.lugroma3.org
  - imap.lugroma3.org
  - pop.lugroma3.org
  - mail.nanoinside.net
  - imap.nanoinside.net
  - pop.nanoinside.net

- both of them manage users

- the pop and imap servers running on the mxs provide access to the mailboxes of the users

- a “guest” user account is defined on both mxs
  - password: guest

```
$ cat /etc/passwd | grep guest
guest:x:1000:1000:Guest Account,,,:/home/guest:/bin/bash
```


step 5 – sending an e-mail

- place yourself on **dnsroot** (or whichever other machine, not including **pc1** and **pc2**)
- start tcpdump

```
dnsroot:~# tcpdump -i eth0 -t -q port domain or port smtp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link type EN10MB (Ethernet), capture size 96 bytes
```

- use less verbose output
- filter out other traffic
- suppress timestamps

- place yourself on **pc1**
- start pine (password: **guest**) and compose an e-mail to **guest@lugroma3.org** (see the following slides...)
step 5 – sending an e-mail

PC1

PINE 4.64 MAIN MENU

Folder: INBOX No Messages

? HELP - Get help using Pine
C COMPOSE MESSAGE - Compose and send a message
I MESSAGE INDEX - View messages in current folder
L FOLDER LIST - Select a folder to view
A ADDRESS BOOK - Update address book
S SETUP - Configure Pine Options
Q QUIT - Leave the Pine program

Copyright 1989-2005. PINE is a trademark of the University of Washington.
step 5 – sending an e-mail

To : guest@nanoinside.net
Cc :
Attchmnt:
Subject : Test message

----- Message Text -----
This is a test message.
Goodbye ;-)
step 5 – sending an e-mail

- sending a mail raises several events
step 5 – sending an e-mail

pc1 looks for the address of the outgoing mail server (mail.lugroma3.org)
step 5 – sending an e-mail

pc1 sends the mail to the mta

pc1 sends the mail to the mta
step 5 – sending an e-mail

the mta looks for the mail exchanger for domain nanoinside.net
step 5 – sending an e-mail

PC1 → DNSLUG → SMTP → DNSNANO → PC2

The MTA relays the mail to the mail exchanger (mail.nanoinside.net)
step 5 – sending an e-mail

the mail lies on **dnssnano**, waiting for the user to get it
step 5 – sending an e-mail

The mail lies on `dnsnano`, waiting for the user to get it.
step 5 – sending an e-mail

dnsnano:

```
# cat /var/spool/mail/guest
From root@lugroma3.org Fri Apr 20 15:10:41 2007
Return-path: <root@lugroma3.org>
Envelope-to: guest@nanoinside.net
Delivery-date: Fri, 20 Apr 2007 15:10:41 +0200
Received: from [192.168.0.11] (port=4902 helo=dnslug)
    by dnsnano with esmtp (Exim 4.50)
    id 1Hessr-00004N-OW
    for guest@nanoinside.net; Fri, 20 Apr 2007 15:10:41 +0200
Received: from [192.168.0.111] (port=3119 helo=pc1.lugroma3.org)
    by dnslug with esmtp (Exim 4.50)
    id 1Hessr-00004O-7M
    for guest@nanoinside.net; Fri, 20 Apr 2007 15:10:41 +0200
Date: Fri, 20 Apr 2007 15:10:41 +0200 (CEST)
From: Root user on PC1 <root@lugroma3.org>
X-X-Sender: root@pc1
Reply-To: guest@lugroma3.org
To: guest@nanoinside.net
Subject: Test message
Message-ID: <Pine.LNX.4.64.0704201510200.254@pc1>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII; format=flowed

This is a test message.
Goodbye ;-)```
step 5 – sending an e-mail

dnsnano:~# cat /var/spool/mail/guest
From root@lugroma3.org Fri Apr 20 15:10:41 2007
Return-path: <root@lugroma3.org>
Envelope-to: guest@nanoinside.net
Delivery-date: Fri, 20 Apr 2007 15:10:41 +0200

Received: from [192.168.0.11] (port=4902 helo=dnslug)
  by dnsnano with esmtp (Exim 4.50)
  id 1Hessr-00004N-OW
  for guest@nanoinside.net; Fri, 20 Apr 2007 15:10:41 +0200
Received: from [192.168.0.111] (port=3119 helo=pc1.lugroma3.org)
  by dnslug with esmtp (Exim 4.50)
  id 1Hessr-000040-7M
  for guest@nanoinside.net; Fri, 20 Apr 2007 15:10:41 +0200

Date: Fri, 20 Apr 2007 15:10:41 +0200 (CEST)
From: Root user on PC1 <root@lugroma3.org>
X-X-Sender: root@pc1
Reply-To: guest@lugroma3.org
To: guest@nanoinside.net
Subject: Test message
Message-ID: <Pine.LNX.4.64.0704201510200.254@pc1>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US

This is a test message.
Goodbye ;-)

Each mta traversed by the message adds its own header to it
step 5 – sending an e-mail

```
dnsnano:~# cat /var/spool/mail/guest
From root@lugroma3.org Fri Apr 20 15:10:41 2007
Return-path: <root@lugroma3.org>
Envelope-to: guest@nanoinside.net
Delivery-date: Fri, 20 Apr 2007 15:10:41 +0200
Received: from [192.168.0.11] (port=4902 helo=dnslug)
  by dnsnano with esmtp (Exim 4.50)
  id 1Hessr-00004N-0W
  for guest@nanoinside.net; Fri, 20 Apr 2007 15:10:41 +0200
Received: from [192.168.0.111] (port=3119 helo=pc1.lugroma3.org)
  by dnslug with esmtp (Exim 4.50)
  id 1Hessr-00004O-7M
  for guest@nanoinside.net; Fri, 20 Apr 2007 15:10:41 +0200
Date: Fri, 20 Apr 2007 15:10:41 +0200 (CEST)
From: Root user on PC1 <root@lugroma3.org>
X-X-Sender: root@pc1
Reply-To: guest@lugroma3.org
To: guest@nanoinside.net
Subject: Test message
Message-ID: <Pine.LNX.4.64.0704201510200.254@pc1>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII; format=flowed

This is a test message.
Goodbye ;-)```
step 5 – sending an e-mail

```
dnsnano:~# cat /var/spool/mail/guest
From root@lugroma3.org Fri Apr 20 15:10:41 2007
Return-path: <root@lugroma3.org>
Envelope-to: guest@nanoinside.net
Delivery-date: Fri, 20 Apr 2007 15:10:41 +0200
Received: from [192.168.0.11] (port=4902 helo=dnslug)
    by dnsnano with esmtp (Exim 4.50)
    id 1Hessr-00004N-0W
    for guest@nanoinside.net; Fri, 20 Apr 2007 15:10:41 +0200
Received: from [192.168.0.111] (port=3119 helo=pc1.lugroma3.org)
    by dnslug with esmtp (Exim 4.50)
    id 1Hessr-00004O-7M
    for guest@nanoinside.net; Fri, 20 Apr 2007 15:10:41 +0200
Date: Fri, 20 Apr 2007 15:10:41 +0200 (CEST)
From: Root user on PC1 <root@lugroma3.org>
X-X-Sender: root@pc1
Reply-To: guest@lugroma3.org
To: guest@nanoinside.net
Subject: Test message
Message-ID: <Pine.LNX.4.64.0704201510200.254@pc1>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII; format=flowed

This is a test message.
Goodbye ;-)```
step 6 – receiving an e-mail

- restart tcpdump on dnsroot with a different filter

```
dnsroot:~# tcpdump -i eth0 -t -q port domain or port imap
```

- place yourself on pc2
- start pine and check for incoming messages (see the following slides... )
step 6 – receiving an e-mail
step 6 – receiving an e-mail

select the **inbox** folder
step 6 – receiving an e-mail

select the message
step 6 – receiving an e-mail

Date: Mon, 3 Apr 2006 21:48:26 +0200 (CEST)
From: Root user on PC1 <root@lugroma3.org>
Reply-To: guest@lugroma3.org
To: guest@nanoinside.net
Subject: Test message

This is a test message.
Goodbye ;-)

netkit – [ lab: email ]
step 6 – receiving an e-mail

- receiving a mail activates different protocols
step 6 – receiving an e-mail

pc2 looks for the address of the incoming mail server (imap.nanoinside.net)
step 6 – receiving an e-mail

pc2 authenticates within the incoming mail server
step 6 – receiving an e-mail

pc1

dnslug

dnsnano

pc2

IP pc2.nanoinside.net.4599 > dnsnano.nanoinside.net.imap2: tcp 0
IP dnsnano.nanoinside.net.imap2 > pc2.nanoinside.net.4599: tcp 0
IP pc2.nanoinside.net.4599 > dnsnano.nanoinside.net.imap2: tcp 0
IP dnsnano.nanoinside.net.imap2 > pc2.nanoinside.net.4599: tcp 156
IP pc2.nanoinside.net.4599 > dnsnano.nanoinside.net.imap2: tcp 0
IP pc2.nanoinside.net.4599 > dnsnano.nanoinside.net.imap2: tcp 29
...

pc2 retrieves remote folder information and gets the mail
step 7 – a typical smtp session

```
pc1:~# telnet mail.lugroma3.org smtp
```

© Computer Networks Research Group Roma Tre

netkit – [ lab: email ]

last update: Apr 2007
step 7 – a typical smtp session

```
pc1:~# telnet mail.lugroma3.org smtp
220 dnsnano ESMTP Exim 4.50 Mon, 03 Apr 2006 22:08:51 +0200
EHLO pc2.nanoinside.net
250-dnsnano Hello pc2.nanoinside.net [192.168.0.222]
250-SIZE 52428800
250-PIPELINING
250 HELP
RSET
250 Reset OK
MAIL FROM:<root@nanoinside.net>
250 OK
RCPT TO:<guest@nanoinside.net>
250 Accepted
```

sent

netkit – [ lab: email ]

last update: Apr 2007
step 7 – a typical smtp session

DATA
354 Enter message, ending with "." on a line by itself
Date: Mon, 3 Apr 2006 22:08:51 +0200 (CEST)
From: Root user on PC2 <root@nanoinside.net>
X-X-Sender: root@pc2
Reply-To: guest@nanoinside.net
To: guest@nanoinside.net
Subject: Test message
Message-ID: <Pine.LNX.4.64.0604032208330.264@pc2>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII; format=flowed

This is a test message.
Goodbye ;-)

.

250 OK id=1FQVM3-00004q-6A
QUIT
221 dnsnano closing connection

sent  received
step 7 – a typical imap session

pc2:~# telnet imap.nanoinside.net imap
step 7 – a typical imap session

```
pc2:~# telnet imap.nanoinside.net imap
* OK [CAPABILITY IMAP4REV1 LITERAL+ SASL-IR LOGIN-REFERRALS AUTH LOGIN]
00000000 AUTHENTICATE LOGIN
 + VXNlcBOYW1lAA==
Z3V1c3Q=
 + UGFzc3dvcmQA
Z3V1c3Q=
00000000 OK [CAPABILITY IMAP4REV1 LITERAL+ IDLE NAMESPACE MAILBOX-REFERRALS BINARY UNSELECT SCAN SORT THREAD REFERENCES THREAD ORDEREDSUBJECT MULTIAPPEND] User guest authenticated
```

© Computer Networks
Research Group Roma Tre
step 7 – a typical imap session

```
00000001 SELECT inbox
* 1 EXISTS
* 1 RECENT
* OK [UIDVALIDITY 1144093711] UID validity status
* OK [UIDNEXT 4] Predicted next UID
* FLAGS (\Answered \Flagged \Deleted \Draft \Seen)
* OK [PERMANENTFLAGS (\* \Answered \Flagged \Deleted \Draft \Seen)]
Permanent flags
* OK [UNSEEN 1] first unseen message in /var/spool/mail/guest
00000001 OK [READ-WRITE] SELECT completed
00000002 FETCH 1 FLAGS
* 1 FETCH (FLAGS (\Recent))
00000002 OK FETCH completed
```
step 7 – a typical imap session

pc2

00000003 FETCH 1 (UID ENVELOPE BODY.PEEK[HEADER.FIELDS (Newsgroups Content-MD5 Content-Disposition Content-Language Content-Location resent-to resent-date resent-from resent-cc resent-subject List-Help List-Unsubscribe List-Subscribe List-Post List-Owner List-Archive Followup-To References)] INTERNALDATE RFC822.SIZE FLAGS)
* 1 FETCH (UID 3 ENVELOPE ("Mon, 3 Apr 2006 22:19:59 +0200 (CEST)" "Test message" ("Root user on PC1" NIL "root" "lugroma3.org")) ("Root user on PC1" NIL "root" "lugroma3.org")) (NIL NIL "guest" "lugroma3.org") (NIL NIL "guest" "nanoinside.net")) NIL NIL NIL "<Pine.LNX.4.64.0604032219450.264@pc1>") BODY[HEADER.FIELDS (NEWSGROUPS CONTENT-MD5 CONTENT-DISPOSITION CONTENT-LANGUAGE CONTENT-LOCATION RESENT-TO RESENT-DATE RESENT-FROM RESENT-CC RESENT-SUBJECT LIST-HELP LIST-UNSUBSCRIBE LIST-SUBSCRIBE LIST-POST LIST-OWNER LIST-ARCHIVE FOLLOWUP-TO REFERENCES)] {2}

INTERNALDATE " 3-Apr-2006 22:20:00 +0200" RFC822.SIZE 834 FLAGS (\Recent))
00000003 OK FETCH completed

00000004 FETCH 1 (BODYSTRUCTURE FLAGS)
* 1 FETCH (BODYSTRUCTURE ("TEXT" "PLAIN" ("CHARSET" "US-ASCII" "FORMAT" "flowed") NIL NIL "7BIT" 40 3 NIL NIL NIL NIL) FLAGS (\Recent))
00000004 OK FETCH completed
step 7 – a typical imap session

00000005 FETCH 1 BODY[1]
  * 1 FETCH (BODY[1] {40}
This is a test message.
  Goodbye ;-) )
)
  * 1 FETCH (FLAGS (\Recent \Seen))
00000005 OK FETCH completed
00000006 NOOP
00000006 OK NOOP completed
00000007 LOGOUT
  * BYE dnsnano IMAP4rev1 server terminating connection
00000007 OK LOGOUT completed
exercises

- create a new user account (e.g., with `adduser`) on `dnssnano`
- send an e-mail from `pc1` to that account
- change the configuration of pine on `pc2` to login on the incoming mail server with the new account
- receive the e-mail from `pc2`
exercises

■ reply to the mail you have just sent
■ sniff a smtp/imap/pop3 session, save packet data to file and examine it with a graphical packet dissector (e.g., ethereal)
■ send an e-mail by using a telnet to the outgoing mail server
■ receive an e-mail by using a telnet to the incoming mail server