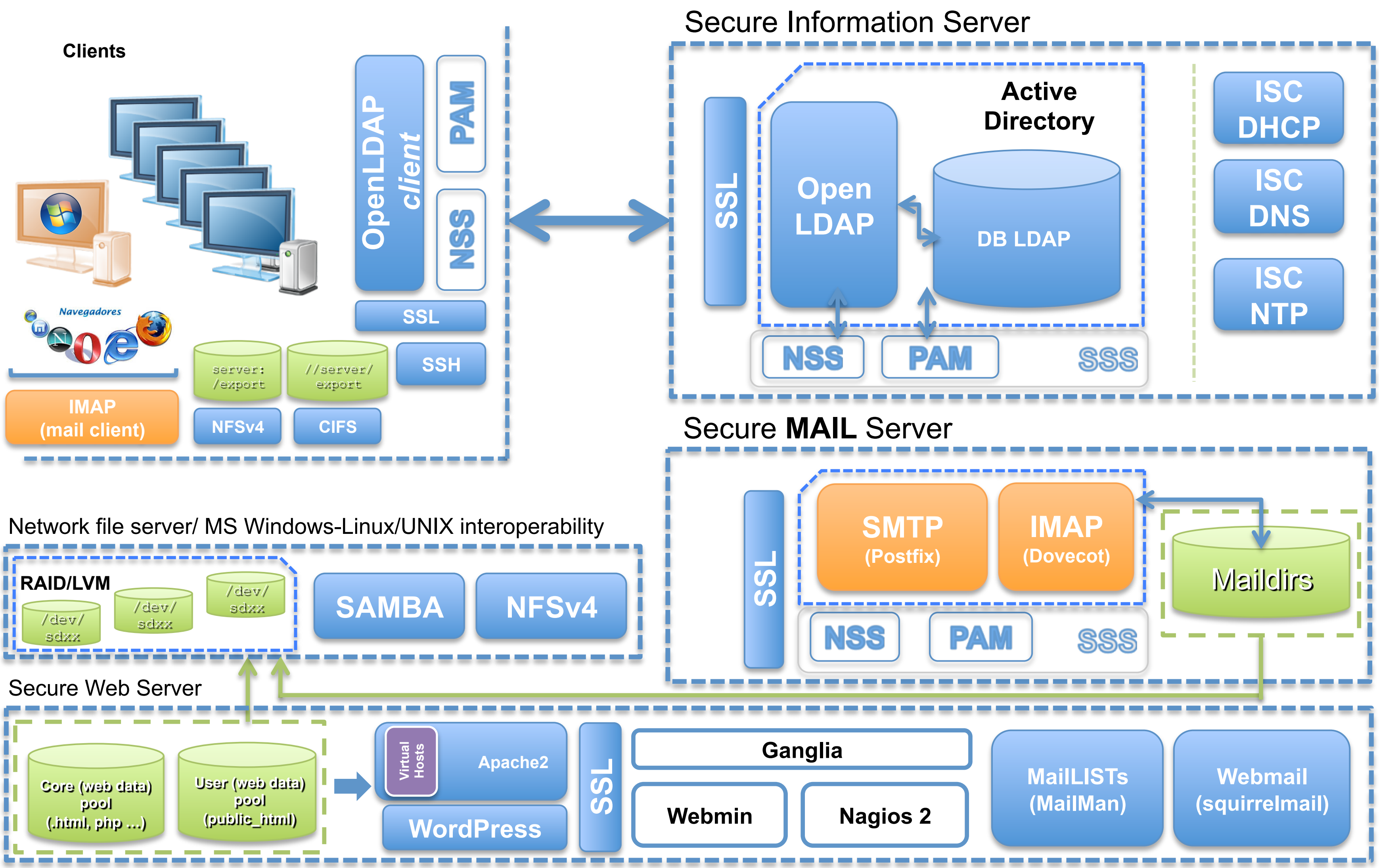
Computer System Design and Administration

Topic 11. Secure e-Mail service: SMTP Postfix, IMAP Dovecot (over SSL)

José Ángel Herrero Velasco

Department of Computer and
Electrical Engineering

Puzzle

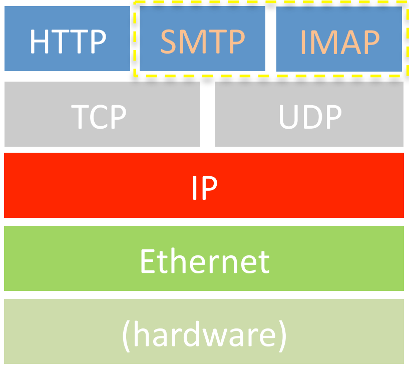


José Ángel Herrero Velasco

Target: e-Mail services

- Deployment and development of an INTERNET *secure* **e-MAIL service** based on SMTP/IMAP protocols:
  - Sending mail using **SMTP** protocol: *Postfix.*
  - Receiving mail using **IMAP** protocol: *Dovecot.*
  - Management of Maildrop: *Maildirs.*
  - MUA-MTA secure communication (*encrypted*): **TLS/SSL.**
- Installation, configuration and start up of a **Webmail** client:
  - Roundcube.
  - Mailmain.

The e-Mail system



TCP/IP stack

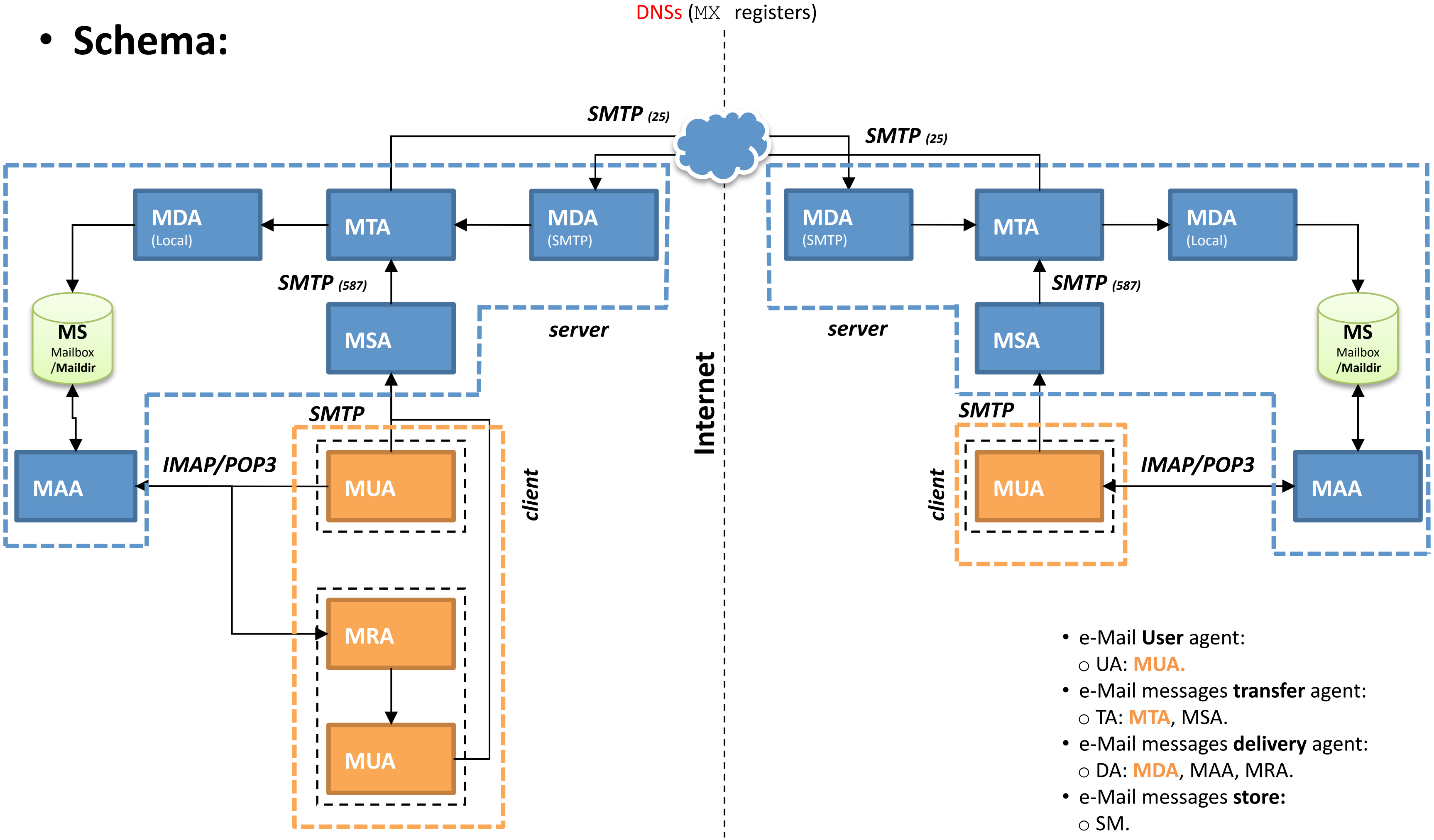
- **Definitions and basics:**
  - E-Mail: the **electronic** mail system:
    - **Network service** that enables 2 users from different computers to **send** and **receive (exchange)** digital messages.
    - Historically, one of the most greatly used systems in the Internet:
      - **Social networks, SMS, WhatsApp ... push e-Mail service into the *"old technology"* category.**
    - **Universal standard** for on-line communications.
  - e-Mail **messages:**
    - Transfer element between e-mail partners (Sender / Receiver):
      - **RFC 5322, RFC 2045 and RFC 2049 (MIME).**
      - **Based and composed of:**
        - » *Encapsulated:*
          - Required by **SMTP protocol.**
        - » *Header:*
          - Divided by *fields*: **`From, To, Subject, CC, CCO`**…
        - » *Body:*
          - It can contain plain text only, HTML format, media elements, etc.
          - It allows *"attach"* user files.
  - e-Mail **address:**
    - Set of words that identifies an **email user address.**
    - User name (NIC) + **@** + network supplier name (FQDN).

The e-Mail system

- **History:**
  - Internet Predecessor:
    - With the first computers, the possibility of storing information and being able to communicate with each other through a computer network, "comes" the idea of **exchanging information.**
  - 1965. "Compatible Time-sharing System" (**CTSS**) from **MIT** *(Operative system):*
    - Informal methods of using this to pass messages were developed and expanded.
  - **1971.** Sending the first story e-Mail (SNDMSG/READMAIL systems) between two contiguous machines:
    - By Ray Tomlinson (Ministry of Defense USA):
      - **Who creates the "@" symbol too.**
    - *Username ←→ hostname.*
  - 1972. Unix *mail* program and **Mailbox** development.
  - 1973. 75% of the ARPANET traffic is composed of emails.
  - 1982. RFCs for ARPANET e-mail **transfer** system are published (MTA):
    - RFC 821 → e-Mail transfer protocol → **SMTP.**
    - RFC 822 → e-Mail message format → MIME.
  - 1984. RFCs for e-mail **delivery** protocol are published (MDA):
    - POP1 was specified in RFC 918 (1984), POP2 by RFC 937 (1985) and **POP3** originated with RFC 1081 (1988):
      - **e-Mail delivery protocol over TCP/IP.**
    - **IMAP4** RFC3501 (1991):
      - **e-Mail remote maildrop protocol.**
  - …
- **At present**, drastic reduction in the use of this mode of communication:
  - Inappropriate use (**SPAM**):
    - 72% of the e-Mail circulating over the internet is SPAM (2014).
  - **Mobile device** development.
  - Communication systems such as **SMS**, **WhatsApp** and even **social networks.**

The e-Mail system: Architecture

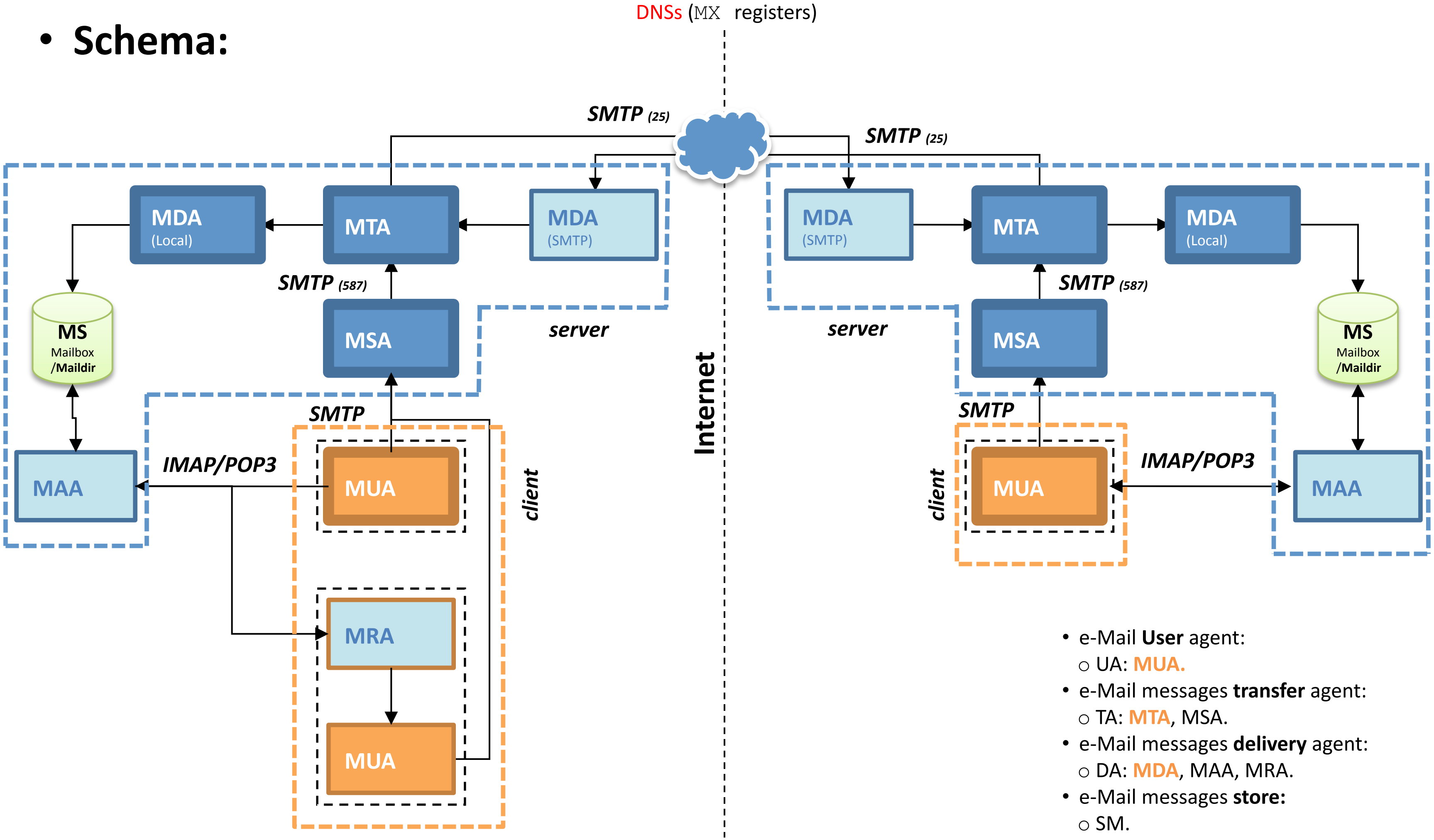
- **Schema:**



- e-Mail **User** agent:
  - UA: MUA.
- e-Mail messages **transfer** agent:
  - TA: MTA, MSA.
- e-Mail messages **delivery** agent:
  - DA: MDA, MAA, MRA.
- e-Mail messages **store:**
  - SM.

The e-Mail system: Architecture

- **Schema:**



- e-Mail **User** agent:
  - UA: MUA.
- e-Mail messages **transfer** agent:
  - TA: MTA, MSA.
- e-Mail messages **delivery** agent:
  - DA: MDA, MAA, MRA.
- e-Mail messages **store:**
  - SM.

The e-Mail system: Components

- **Underlying components:**
  - Server:
    - **MTA** (e-Mail transfer agent) → **Postfix** cleanup, sendmail…:
      - **Pre-processes and routes *incoming* mail to the local MDA (SMTP).**
      - **May route the *outgoing* mail to "Internet" MTA-to-(remote) MDA.**
    - **MSA** (e-Mail submission agent) → **Postfix** postdrop+pickup, sendmail-msa:
      - **Accepts *outgoing* mail from the MUA (client) (SMTP).**
      - **Prepares and delivers the mail to the MTA (SMTP) and authenticates MUA/user (if it's necessary).**
    - **MDA** (e-Mail delivery agent) → **Postfix** local, procmail…:
      - **Accepts the *incoming* mail from the remote MTA.**
      - **Delivers mail to:**
        - Mailbox/Maildir MS (**SMTP**).
        - *(destination-local)* MTA (**SMTP**).
    - **MAA** (e-Mail access agent) → Courier IMAPD, **Dovecot IMAP:**
      - **Detects (new) messages from the maildrop *(Mailbox/Maildir)* and makes them available to the MRA (POP3/IMAP).**
      - **Stores *outgoing* e-mail and authenticates MUA/user.**
    - **MS** (Massages store):
      - **Manages the e-mail store.**
  - Client:
    - **MUA** (e-Mail user agent) → Thunderbird, Outlook, Mail (OSX)…:
      - **Writes e-mail and sends to the MTA (SMTP).**
      - **Reads e-mail delivered by MDA (POP3/IMAP) to the MS through the MRA.**
    - **MRA** (e-Mail retrieval agent) → Thunderbird , Fetchmail:
      - **Retrieves e-mail from the MAA.**
      - **Makes mail available to the MUA (POP3/IMAP).**

The e-Mail system: Operation

- **Operation:**

1. **Writing** new mail [**MUA**]:

SMTP

- The user (**sender**) writes a new message using the MUA.
- MUA deposits it to the MSA and stores it in the MS through the MAA.

2. **Pre-processing** mail [**MSA**]:

- User (sender) **authentication.**
- Sending message using the sender MTA.
- Reports to the MUA.

3. **Sending** the mail to its destination [**MTA**]:

SMTP

- The message is sent from sender MTA.
- The MTA (sender):
  - Validates the intercollectors.
  - Applies mail filter (Anti-SPAM).
  - Re-writes the message header .
- Selects and sends the message to the local MDA of the **recipient** (SMTP):
  - *Routing the message.*

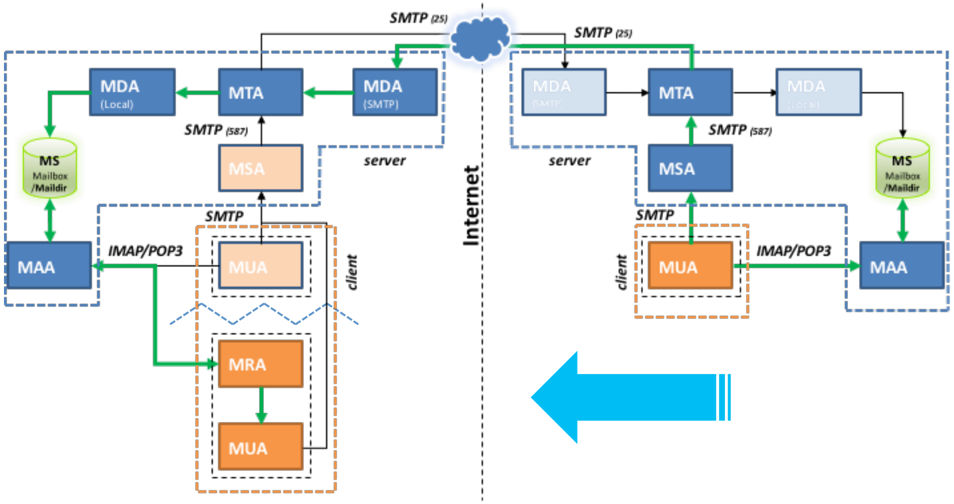
4. **Receipt** of the mail at destination (1) [**MDA**]:

- Receives and sends again the message to the (**local**) MDA of the recipient (SMTP).

5. **Receipt** of the mail at destination (2) [**MTA**]:

SMTP

- The message arrives at the destination user's MTA.
- The MTA (recipient):
  - Validates the intercollectors.
  - Applies mail filter (Anti-SPAM).
  - Re-writes the message header.
- Selects and sends the message to the (**local**) MDA of the recipient.



6. **Receipt** of the mail at destination (3) [**MDA** (local)]:

- Delivers the message to the local store (MS) maildrop (Mailbox/Maildir).

7. **Detecting** a new mail in destination [**MAA**]:

- Validates (**authentication**) user (destination).
- Delivers the message to the MRA.

POP/ IMAP

8. **Reading** the received message [**MUA**]

- Receives mail (message) from the MRA.
- Presents the message to destination user.

The e-Mail system: Integration

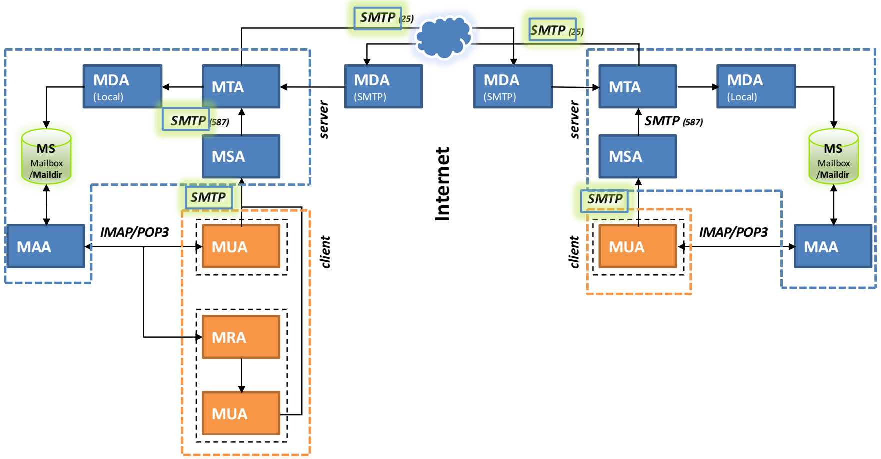
- **DNS service:**
  - It is an essential piece of the global e-Mail system operation in *the Internet:*
    - It enables sending e-mail messages between SMTP servers:
      - **From the MUA to MTA.**
      - **Between MTAs on the Internet (SMTP relays).**
  - It's necessary to configure the *"authoritative zone"* server (bind9) from the MTA local network:
    - The MTA FQDN must be registered in the DNS as a `MX` register (**M**ail e**X**chage):
      - **Redirects all mail from the domain to your MTA server.**

The e-Mail protocols: SMTP

- **SMTP** (**S**imple **M**ail **T**ransfer **P**rotocol):
  - Enables **transferring e-Mail messages among servers** through peer-to-peer connection:
    - RFC 2821, RFC 5321…
    - Used to:
      - **Transfer digital messages (shipping and receiving) among servers (not clients).**
    - Used by the MTA, MSA, MDA and MUA components.
    - Very simple protocol (essentially) **UNSECURE.**
      - **MTA origin → MTA destination:…"Here's a message; please deliver it to user@your.domain".**
      - **MTA destination → MTA origin:… "Ok".**
      - **Unidirectional channel.**
    - Extended (**Enhanced**) version: **ESMTP** RFC 1869:
      - **MIME 8bits, SMTP AUTH, UTF8…**
  - Over TCP/IP (default port: **25**).
  - Operates by executing **commands:**
    - Between partners.
    - Commands:
      - **`HELO`; identifies the connecting host if speaking SMTP.**
      - **`MAIL FROM`; initiates a mail transaction (envelope sender).**
      - **`RCPT TO`; identifies envelope recipient(s).**
      - **`DATA`; begins the message body.**
      - **`QUIT`; ends the exchange and closes the connection.**
      - **`SEND`; sends a message to a user's terminal. Instead of a mailbox.**
      - **…**
  - Supports:
    - Secure (encrypted) communications: TLS/SSL (**SMTPs**):
      - **Puerto 465.**
  - Provides:
    - Authentication:
      - **PLAIN, CRAM-MD5, LDAP, GSSAPI - Kerberos (SASL)…**
  - **Limitations on receiving messages (destination):**
    - On clients, delivery and access to the user mail is managed by other protocols: **POP/ IMAP.**

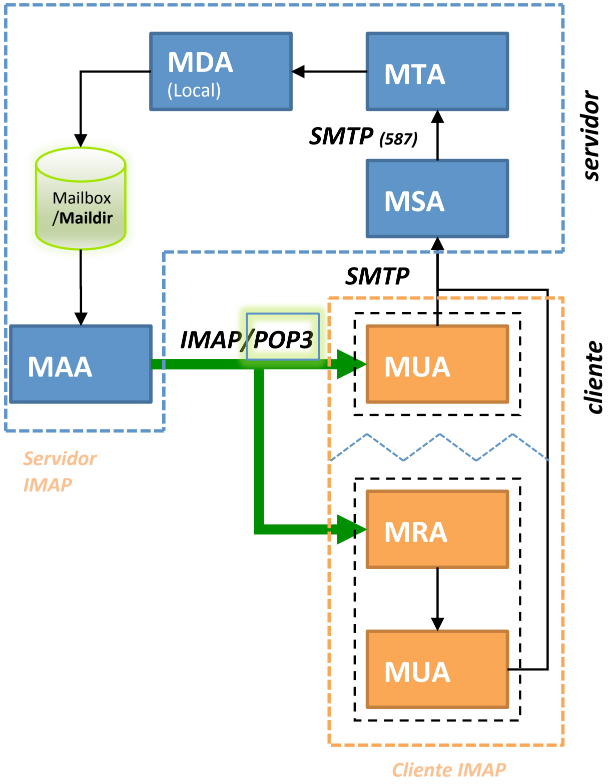
Security?!?!?

→ *SPAM source*



The e-Mail protocols: POP3

- **POP3** (**P**ost **O**ffice **P**rotocol):
  - Enables e-Mail clients **to retrieve the e-Mail messages** from a remote SMTP server:
    - RFC 1939…
    - *download-and-delete* requirements for access to remote mailboxes.
    - Versions: POP1, POP2 and **POP3.**
    - It is used by the MUA component.
  - Operates under **intermittent or slow connection** conditions:
    - E-Mail user doesn't need to be permanently connected.
    - E-Mail *remains* accessible in MUA despite being disconnected:
      - **E-Mail messages are removed from server (by default).**
    - TCP/IP port: **110** (by default).
  - Operates by executing **commands** too (like SMTP protocol):
    - Between partners (MUA-MAA).
    - Commands:
      - **`USER <name>;` defines the user name for access to a maildrop.**
      - **`PASS <password>;` defines the password string for access to a maildrop.**
      - **`STAT;` provides 'drop-listing' status of the maildrop.**
      - **`LIST;` provides 'scan-listing' summary of messages in the maildrop.**
      - **`RETR <number>;` retrieves a message from the maildrop.**
      - **`TOP <number> <lines>;` displays the header and the number of Required message lines by specifying the number.**
      - **`DELE <number>;` mark the msg as deleted from the maildrop.**
      - **`RSET;` resets all messages that are marked as deleted to unmarked. (current connection).**
      - **`QUIT`; terminates the session.**
  - Provides:
    - User authentication (required!!!):
      - **PLAIN (USER/PASS commands), APOP (MD5), LDAP, GSSAPI - Kerberos (SASL)…**
  - Supports:
    - Secure (encrypted) communications: TLS/SSL (**POPs**):
      - **TCP port 995.**
    - …



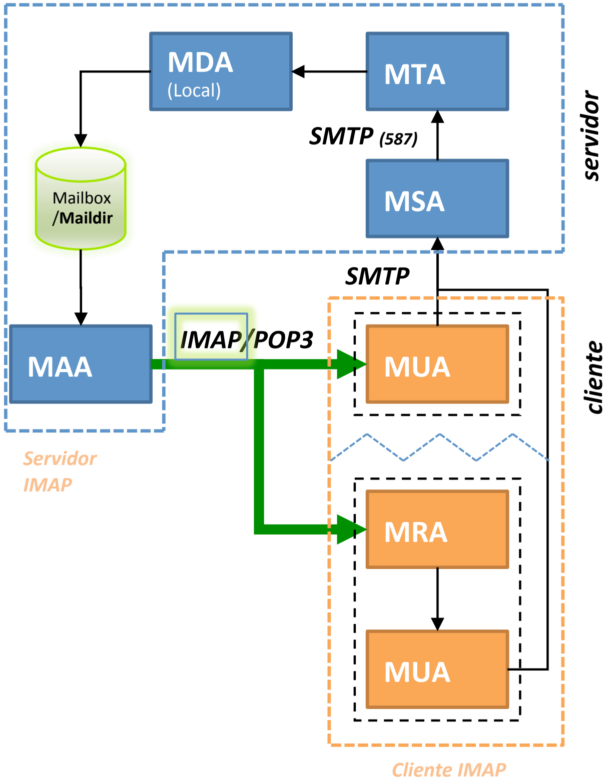
The e-Mail protocols: IMAP4

- **IMAP4** (**I**nternet **M**essages **A**ccess **P**rotocol):
  - Enables e-Mail clients **to receive the e-Mail messages** from an IMAP server:
    - By manipulation of the **remote maildrop (MAILBOX/MAILDIRS)** by **multiple email clients:**
    - **You do not need to download mail locally!!!:**
      - **Headers only.**
      - **→ Allows the client app to delete messages "partially".**
    - RFC 1730, RFC 3501…
    - It is used by the MUA component (like POP3 protocol).
  - Operates under **permanent connection** conditions:
    - Takes advantage of Internet Interconnection Networks:
      - **On-line and off-line modes of operation.**
    - **Immediately detects** new mail.
    - TCP/IP port: **143** (by default).
  - Operates by executing **commands** too (like SMTP and POP3 protocols):
    - Between partners (MUA-MAA).
    - Commands:

      `ANY STATE:`
      - `Capability;` **gets server capability.**
      - `Logout.`
      - `noop;` **use to check for new mail and to prevent connection timeout.**

      `NON-AUTHENTICATED STATE:`
      - `Authenticate;` **auth mechanism (SASL auth).**
      - `Login;` **user/passw.**

      `AUTHENTICATED STATE:`
      - `Append;` **adds message to specific mailbox.**
      - `Create;` **new mailbox.**
      - `Delete;` **deletes mailbox.**
      - `Examine;` **selects in read only mode.**
      - `List;` **list of mailbox names.**
      - `Lsub;` **list of mailboxes user is subscribed.**
      - `Rename.`
  - Provides:
    - User authentication (required!!!):
      - **PLAIN, CRAM-MD5, GSSAPI, LDAP (SASL)…**
  - Supports:
    - Secure (encrypted) communications: TLS/SSL (**IMAPs**):
      - **TCP port 993.**
    - …



The e-Mail message format: MIME

- **MIME** (**M**ultipurpose **I**nternet **M**ail **E**xtensions):
  - Specifications and conventions that are used **to exchange** digital messages and files through the Internet:
    - MIME is a specification for enhancing the capabilities of standard Internet communications:
      - **Specially, used by the e-Mail system:**
        - » SMTP.
        - » HTTP as well.
    - Transfer using different **languages** and **alphabets.**
    - Defined by IETF:
      - **RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 and RFC 2077.**
  - MIME is intended to resolve SMTP problems concerning e-Mail message content, size…
  - In **e-Mail system,** it is used to **encode** the data *text formats* and **attach** *files* (including virus) into mail:
    - Body **for e-Mail messages:**
      - **US-ASCII only *(7 bits):***
        - » ASCII limitations → Sizes, number of languages supported…
      - **Multi-media: image, audio and video messages.**
      - **Multi-fonts…**
    - MIME headers:
      - **MIME-Version.**
      - **Content-Type:**
        - » e-Mail Message content:
          - Text/plain.
        - » e-Mail message multipart (tree).
      - **Content-Transfer-Encoding:**
        - » Methods for representation of binary types (ASCII):
          - **7 bits**, base64, 8 bits, binary...
      - **Encoded-Word.**
  - In the E-mail system:
    - All MUA/MAA () support MIME.

The e-Mail message format: Structure

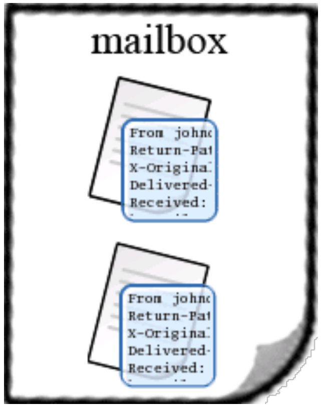
- **The envelope:**
  - From **SMTP** dialog.
  - TCP/IP stack (application level).
- **The headers:**
  - Message metadata.
  - Specified in RFC 2822.
- **The body of the message:**
  - Sequence of ASCII characters.
  - Separated from body by CRLF.
- **Syntax:**
  - Message ::= headers CRLF body
  - headers ::= header headers | e
  - header ::= name ":" value CRLF.

```
Return-Path: andjo@ida.liu.se
Delivery-Date: Fri May 14 08:38:34 2004
Received: from diag7.ida.liu.se (diag7.ida.liu.se [130.236.177.217])
    by portofix.ida.liu.se (8.12.11/8.12.11) with ESMTP id i423760;
    Fri, 14 May 2004 08:38:31 +0200 (MEST)
Received: (from andjo@localhost)
    by diag7.ida.liu.se (8.12.10+Sun/8.12.10/Submit) id i401197;
    Fri, 14 May 2004 08:38:31 +0200 (CEST)
Date: Fri, 14 May 2004 08:38:31 +0200
From: Andreas Johansson <andjo@ida.liu.se>
To: David Byers <davby@ida.liu.se>
Cc: pjn@ida.liu.se
Subject: Re: =?ISO-8859-1?Q?N=E4tverksproblem?=
Message-Id: <20040514083831.495c66a2.andjo@ida.liu.se>
In-Reply-To: <41r7togybd.fsf@obel19.ida.liu.se>
References: <41r7togybd.fsf@obel19.ida.liu.se>
Organization: =?ISO-8859-1?Q?Link=F6pings?= universitet
X-Mailer: Sylpheed version 0.9.6 (GTK+ 1.2.10; sparc-sun-solaris2.9)
Mime-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
X-Virus-Scanned: clamd / ClamAV 0.70, clamav-milter 0.70j
X-Spam-Flag: NO
X-Scanned-By: milter-spamc/0.15.245 ( [130.236.177.25]); pass
```

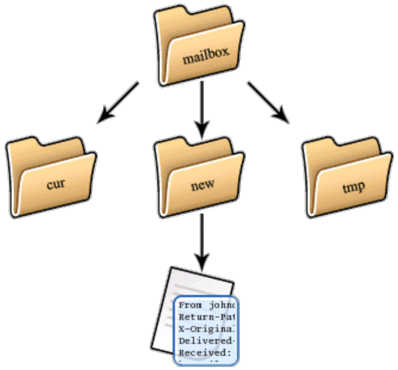
CRLF → Line feed (**LF**) and carriage return (**CR**).

Maildrop management: Mailbox vs. MAILDIR

- **Mailbox:**
  - *Maildrop* **by default** for the e-Mail system:
    - Universal system.
  - It is a **single file:**
    - All mail is stored in a **single file.**
    - `/var/spool/mail/$USERNAME`, `$HOME/mbox`
  - Problems:
    - **File corruptions:**
      - **2 or more processes simultaneously accessing e-Mail messages.**
      - **Never use it on NFS!!!**
    - File **locks.**



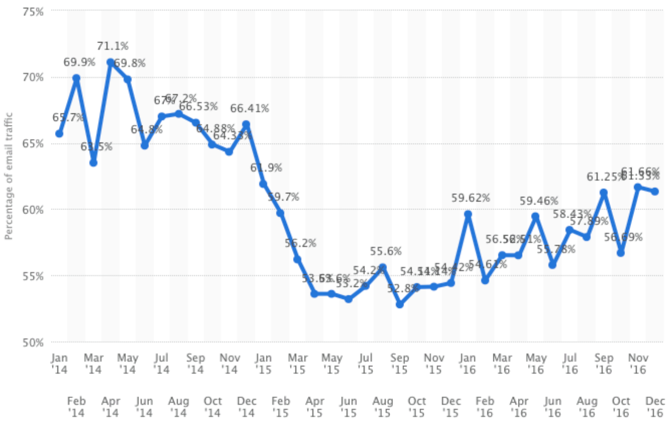
- **Maildir:**
  - It is a directory (**tree**):
    - Each message → One new (unique) file.
    - `$HOME/Maildir/{cur, new, tmp}`
  - No lock.
  - Operation:
    1. The MDA delivers a new email message:
       A) A new (unique) file is created in `$HOME/Maildir/tmp` directory.
       B) The message content is stored in that file.
    2. When delivery is over, that file is moved to:
       A) `$HOME/Maildir/new` directory.
    3. When client (MAA/MUA) reads the message, that file is moved to:
       A) `$HOME/Maildir/cur` directory.
       B) The "read" *flag* of that file is.



The SPAM

- **SPAM:**
  - **Unsolicited** or **undesired** electronic messages by receiver ☹:
    - Unsolicited **commercial** communications.
    - Mass mailing of unsolicited messages (of whatever nature).
  - More than 60% of the **global e-Mail traffic** in the INTERNET is SPAM:
    - Generation by automatic systems (machines).
    - Using "*misconfigured*" SMTP servers.
  - This causes:
    - **User discomfort.**
    - **Security** problems:
      - **Source of virus.**
      - **Fraud *(phishing).***
    - **Performance** decrease in MTAs:
      - **Huge volumes of "bad" mail.**
- It is fundamentally due to the *weakness* of e-Mail systems & protocols (**SMTP**):
  - It is necessary to provide secure channels:
    - Sender authentication (SMTP auth).
    - Encrypted communication (SSL).

Global **SPAM volume** as percentage of total e-mail traffic from January 2014 to December 2016, by month.



Source: statista.com.

MTA/MDA deployment: Postfix

- **Installation (server):**
  - Debian:
    - **Core:**

```
$ apt-get install postfix mailutils maildir-utils
```

Tools to manage *MAILDIRS structures.*

  - Pre-configuration:
    - *"Internet Site":*
      - **Server itself is responsible for distributing the messages to their recipients.**
    - *"Internet with smarthost":*
      - **Server sends the messages to another SMTP server.**

- **Initial checking:**
  - Check the mail ***logs:***

```
$ tail -100 /var/log/mail.log
$ tail -100 /var/log/mail.err
```

  - Check the **network connections** and opened TCP/UDP ports:

```
$ netstat –atup
$ telnet <hostname> 25
```

MTA/MDA configuration: Postfix

- Server *(daemon)* **configuration:**

  `$ vi /etc/postfix/master.cf`

  – Every line of this file corresponds to an **instance** of the mail server:
    - "*daemons*" process.

  – **`service name`:**
    - Instance Name.
    - The service name syntax depends on the service type as described next.

  – **`type`:**
    - **Inet** (TCP/IP sockets), **unix** (unix-domain sockets), fifo, pass…

  – **`private`** (default: yes):
    - Whether or not access is restricted to the mail system.

  – **`unpriv`** (default: yes):
    - Whether the service runs with root privileges or as the owner of the Postfix system.

  – **`chroot`** (default: yes):
    - Whether or not the service runs *chrooted* to the mail queue directory.

  – **`wakeup`** (default: never):
    - Number of seconds the system postpones the start of the instance.

  – **`maxproc`** (default: 100):
    - Max. number of processes running simultaneously per server instance.

  – **`command + args`:**
    - UNIX command that executes the server instance according to `args`.

  → (more details in: **`$ mas 5 master`**).

MTA/MDA configuration: Postfix

- **Service *(core)* configuration:**

  ```
  $ vi /etc/postfix/main.cf
  ```

  - Syntax:
    - *Key = value.*
    - Regular expressions:
      - **POSIX.**
      - **PCRE.**
  - File divided into **sections** about:
    - Server.
    - E-mail message writing (mail):
      - **Incoming/outgoing e-Mails.**
    - E-Mail processing *(filtering).*
    - Access control:
      - **Restrictions.**

You can configurate it using `postconf` command.

MTA/MDA configuration: Postfix

- Service *(core)* configuration:

  `$ vi /etc/postfix/main.cf`

  - **`myhostname`** **=:** the FQDN of the e-Mail server.
  - **`myorigin`** **=:** the Internet **domain** name of this mail system (`mydomain`).
  - **`mydestination`** **=:** the list of domains that are delivered via the $ local_transport mail delivery transport.
  - **`mynetworks`** **=:** the list of "trusted" remote SMTP clients that have more privileges than "strangers".
  - **`relayhosts`** **=:** the next-hop destination of non-local mail.
  - **`inet_interfaces`** **=:** the network interface addresses that this mail system receives mail on.
  - **`alias_maps = hash:<file>`:** pre-formatted file (**`portmap`**) that contains the alias databases that are used for local delivery.
  - **`home_mailbox`** **=:** optional pathname of a mailbox file relative to a local user's home directory.
  - *# TLS/SSL:*
    - **`smtp_use_tls = <yes/no>`:** use TLS when a remote SMTP server announces STARTTLS support, otherwise send the mail in the clear.
    - **`smtpd_tls_sert_file = <file>`:** PATH to the SSL certificate for the SMTP service.
    - **`smtp_tls_key_file = <file>`:** PATH to the SSL key for the SMTP service.
  - *# Access control (Optional):*
    - **`smtpd_helo_restrictions`** **=:** optional restrictions that the Postfix SMTP server applies in the context of a client `HELO` command.
    - **`smtpd_recipient_restrictions`** **=:** optional restrictions that the Postfix SMTP server applies in the context of a client `RCPT TO` command, after smtpd_relay_restrictions.
    - **`smtpd_sender_restrictions`** **=:** optional restrictions that the Postfix SMTP server applies in the context of a client `MAIL FROM` command.

MTA/MDA configuration: Postfix

- **Operation:**
  - **Configuration checking:**
    - `$ postconf`
  - **Start and stop** of the e-Mail service (Postfix):
    - `$ service postfix {start|stop|restart|reload|flush|check|abort|force-reload}`
    - `$ postfix reload`
  - **Service checking:**

```
user1@cliente:~$ telnet server-05 25
Trying 192.168.0.15...
Connected to server-05.localdomain.
Escape character is '^]'.
220 server-05.localdomain ESMTP Postfix (Debian/GNU)
EHLO server-05
250-server-05.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

MAA deployment: Dovecot

- **Installation:**
  - Debian:
    - **Core:**

```
$ apt-get install dovecot-imapd
                  dovecot-gssapi
                  dovecot-…
```

- **Initial check:**
  - Take a look at ***log*** files:

```
$ tail -100 /var/log/syslog
```

  - Check the **network connections** and ports:

```
$ netstat -atup
$ telnet <hostname> 143
```

MAA configuration: Dovecot

- **Syntax:**
  - ALL configuration files in Dovecot service show the same syntax:
    - Basic:

      ```
      Key = value
      ```

    - Section:

      ```
      section optional_name {
        section_setting_key = section_setting_value
        subsection optional_subname {
          subkey = subvalue
        }
      }
      ```

    - Files included: (external):
      - `!include file.conf`
    - Filters.
    - …

- **Server *(daemon)* configuration:**

  ```
  $ vi /etc/dovecot/conf.d/10-master.conf
  ```

  - It establishes, for each entry {}, a service instance (sockets) associated to the user authentication and its configuration parameters:
    - **`inet_listener`:**
      - Service name.
      - IP address.
      - TCP port.
      - …
  - Example:

    ```
    service imap-login {
      inet_listener imap {
        port = 143
      }
    ```

MAA configuration: Dovecot

- Service *(core)* configuration:
  - 100 % of configuration is distributed into several files:

    `$ vi /etc/dovecot/dovecot.conf`

    - **Main** configuration file *(deprecated).*
    - Only certain aspects remain as:
      - **Service protocols and TCP/IP ports.**
      - **Dictionaries `key=value lists`.**
      - **The rest of the configuration is linked by "include" clauses:**
        - To external files.
        - *auth-xxx.**ext**.*

→ Samples of configuration files in:

```
$ cd /usr/share/doc/dovecot-core/example-config/)
```

MAA configuration: Dovecot

- Service *(core)* configuration:
  - 100 % of configuration is distributed into several files:
    $ cd /etc/dovecot/conf.d/
  - 10-mail.conf:
    - Mailbox locations and namespaces:
      - mail_location = location for users' mailboxes.
        - » maildir:~/Maildir
        - » mbox:~/mail:INBOX=/var/mail/%u
      - namespace inbox {inbox = yes}: define multiple mailboxes locations.
  - 10-auth.conf:
    - Authentication processes: **KERBEROS:**
      - auth_realms = REALM name in Kerberos (downer).
      - auth_gssapi_hostname = hostname of dovecot server for kerberos.
      - auth_krb5_keytab = path to kerberos keytab (GSSAPI mechanism).
      - auth_mechanisms = authentication mechanisms enabled to dovecot (plain login digest-md5 anonymous gssapi…).
    - Authentication processes: **LDAP:**
      - auth_mechanisms = login.
      - !include auth-ldap.conf.ext.
  - auth-ldap.conf.ext (/etc/dovecot):
    - LDAP specification:
      - uris = DAP URIs to use. You can use this instead of hosts list.
      - dn = distinguished Name - the username used to login to the LDAP server ad admin (cn=admin).
      - dnpass = password for LDAP server, if dn is specified (ldap).
      - tls_ca_cert_file = TLS cert/key is used only if LDAP server requires a client certificate.
      - tls_require_cert = valid values: never, hard, demand, allow, try (demand).
      - ldap_version = LDAP protocol version to be used. Likely 2 or 3.
      - base = LDAP base for users. %variables can be used here (people).
      - user_attrs = see http://wiki2.dovecot.org/UserDatabase/ExtraFields.
  - 10-ssl.conf:
    - SSL settings:
      - ssl = <yes/no>: enable/disable ssl mechanism.
      - ssl_key = <: PATH to ssl key file.
      - ssl_cert = <: PATH to ssl service certificate file.

MAA configuration: Dovecot

- Service *(core)* configuration:
  - 100 % of configuration is distributed into several files:
    `$ cd /etc/dovecot/conf.d/`
  - `10-logging.conf:`
    - Log events destinations.
  - `15-lda.conf:`
    - LDA specific settings (also used by LMTP).
  - `15-mailboxes.conf:`
    - Mailbox definitions.
  - `20-imap.conf:`
    - IMAP protocol specific settings.
  - `90-acl.conf:`
    - Mailbox access control lists.
  - `90-quota.conf:`
    - Quota limits definitions for Mailboxes.

Load order in:

```
dovecot.conf:
     !include conf.d/*.conf
```