EXPLORATION OF THE DESIGN OF A COMPLEX E-MAIL SYSTEM

Francesco Gennai, Laura Abba, Marina Buzzi CNR, Istituto per le Applicazioni Telematiche

Abstract

The management of an Internet service involves a variety of aspects, ranging from the economic to the technical and organizational. Cost reduction, management simplification and improvement of service quality are the fundamental targets of every Internet service project. In geographically widespread organizations where numerous servers are used in order to implement distributed network services, both costs and human labor for maintenance and management are greatly multiplied. We believe that security and maintenance problems, and thus costs, could be reduced by transferring from a distributed to a centralized service. However, this choice would undermine the flexibility needed by local administrators in order to be able to administer their own services. This paper describes a hybrid service management model (partly centralized, partly distributed) and outlines the results we obtained by applying this model to the e-mail service of our organization.

Keywords

Electronic mail, management, administration, cost, interfaces, security, quality of service.

1. Motivation

IAT (Istituto per le Applicazioni Telematiche) is an Institute of the Italian National Research Council (Consiglio Nazionale delle Ricerche - CNR) located in Pisa. The Italian National Research Council is one of the most important governmental organizations dedicated to the promotion, coordination and regulation of scientific research and technological progress in Italy. CNR carries out its multifaceted institutional activity through the agency of about 330 research units and 18 Research Areas located throughout Italy; it has a permanent staff of more than 8700 people, including research, technical and administrative personnel.

IAT hosts the e-mail service for several Institutes of the Pisa Research Area. In this paper we attempt to analyze e-mail service provision, management and quality assurance issues, based on our experience in the design and implementation of our organization's e-mail service.

The CNR e-mail system is composed of a large set of heterogeneous servers managed by various research units, each organizing its own service autonomously. This heterogeneous environment with multiple servers and no central co-ordination point presents both security and Quality of Service (QoS) problems.

Multiple servers multiply security problems; if not carefully managed, they can become weak security points in the network. Old versions and incorrect configurations of e-mail servers could allow malicious users to gain control of the system.

Furthermore, the growing proliferation of servers on PC platforms can contribute to an increase in the number of active mail servers. An inexpert user may not be aware that an e-mail daemon is active on his system. We have had and still have a lot of spamming activities on CNR servers. Attempts to close "open relays" - multiplied so as to cover a very large number of servers - consume considerable human and economic resources.

The QoS is another important aspect. Today, e-mail service has become a fundamental tool for everyday work. Company productivity can be lowered by service interruptions due to maintenance activities, denial of service problems, etc.

Also, if different mechanisms at different network levels (such as VPN, firewall, traffic filtering by router, etc.) are available to protect data and systems, in the following we focus on security mechanisms that could be activated from the mail server.

2. The e-mail service

In order to design an e-mail service it is necessary to consider the entire project from various angles, that is from both the users' and administrators' points of view.

Users' requirements for QoS include:

- Reliable service;
- Support to mobility;
- Confidentiality of the message content;
- Specific groups of users can ask for added value services in order to satisfy particular needs.

Administrators wish to:

- Decrease maintenance duties (upgrade, monitoring, etc.);
- Simplify administration and management;
- Maintain flexibility and autonomy in e-mail administration;
- Guarantee e-mail system security (according to the security policy defined by the organization);

The two classic approaches to network service management are the centralized and the distributed models. There are pros and cons to both models. The centralized model reduces costs and simplifies system control and maintenance, but leads to a single central point of failure and limits the flexibility and autonomy of peripheral organization units.

On the other hand, although the distributed model increases the flexibility and autonomy of peripheral organization units while minimizing response time to user requests, it requires more hardware/software resources and maintenance, management and monitoring activities. In addition, multiple servers become potential weak security points in the network.

We believe that the best solution is to strike a balance between these two different models.

The idea is to centralize the system management tasks (e.g. system monitoring, upgrading software) while distributing the administration tasks which are typical of peripheral organization units. We call this approach "centralized management with delegated administration" (CMDA).

This approach provides local administrators with the tools to manage their own services. Most products do not support the CMDA model. To enable our product to work in this modality we have developed web-based interfaces as tools for implementing the distributed administration. These interfaces could be implemented by CGI scripts (Common Gateway Interface) which rely on APIs (Application Programming Interfaces) provided by the product.

This model, with respect to a distributed solution, reduces the number of required hw/sw resources and thus of skilled personnel performing management tasks, while still offering a distributed administration of the service in order to best meet user requirements.

Concentrating efforts in managing and monitoring a single or minimal number of servers is an efficient way to reduce costs and to improve security and quality of service.

2.1. Hosting e-mail service

Pisa is home to one of Italy's most prestigious universities, and our first experience in implementing this model began here in 1995. In the collaboration between our institute (at that time we were a part of CNUCE, a CNR Institute located in Pisa) and the University of Pisa, we began hosting mailboxes for 21 of the university's sub-domains.

The idea was to furnish the e-mail service to those university departments which were unable to run their own server, without having to deal with their administration problems (such as mailboxes' naming schema, assignment policies and so on).

An interface with two hierarchical levels of management was developed:

- The first level was intended to manage sub-domain names under the University of Pisa domain name (unipi.it). This enabled the university to add/remove the sub-domain definition on our e-mail system.
- The second level was intended to manage user mailboxes and aliases under each sub-domain (di.unipi.it, etc.).

In order to host the service for university domains, we needed to:

- Route e-mail traffic toward our system (insert a MX record in the DNS system of the university pointing to our mail server) in order to process messages addressed to university people;
- Insert an alias (CNAME record) in the university DNS specifying mail.unipi.it pointing to mail.cnuce.cnr.it. This configuration enables university users to insert a server name belonging to their domain in their client configuration. Actually, in order to have a greater degree of flexibility, the university decided to adopt our model name using different names for different e-mail system components (smtp, pop or imap server), so two additional CNAMEs have been added: pop.unipi.it and smtp.unipi.it pointing respectively to pop.cnuce.cnr.it and smtp.cnuce.cnr.it (at that time the university did not use the IMAP). The adoption of this naming scheme permits movement of different e-mail system components to different systems without the need for client re-configuration. A short time later, this choice proved to be useful; it permitted the university to move the e-mail service from our mail server to their new one in a way completely transparent to the user (only modifying DNS entries).

In order to manage the university domains and mailboxes we developed programs and interfaces based on the Application Programming Interfaces of our e-mail server.

The success of this first experience demonstrated the importance of the CMDA model. Two years later we decided to offer similar service to our own organization (CNR), comprising a large number of institutes situated throughout Italy.

Most of the CNR Institutes have their own e-mail servers, with one person in charge of management tasks. Each institute has an e-mail domain in the following form: institute-acronym.city-code.cnr.it (i.e. ict.pi.cnr.it, ladseb.pd.cnr.it). Since CNR institutes exist for all scientific disciplines, many institutes lack experts in Internet service management; these institutes found the CMDA model very useful.

However, in scientific institutes, people are used to configuring their own mail servers. In order to comprehend the workload required to manage the CNR e-mail service, we scanned the 25 (smtp) port at the CNUCE Institute. As a result, we found out that in an Institute with less than 120 workers, and a centralized e-mail service, there were a total of 52 active smtp servers. Most of these servers were older versions, carelessly configured - occasionally active although not in use. This situation was obviously a weak point in the system's security. Our most difficult task was convincing people to close these servers, and the flexibility of the administration interface helped us to achieve this.

Today all the CNUCE mailboxes are defined on our mail server, and CNUCE smtp servers are either disabled or filtered by a firewall.

In the following paragraphs we describe our management interface and the features offered by our server. Technical details are skipped because they depend on the APIs provided by the e-mail product, the configuration files format, the implementation choices, etc.

2.2 The administration interface

As a development of the first text-oriented interface, we came to use a web interface by which local administrators can manage users, mailboxes, and aliases (in a domain) without encountering further server management problems.

Products which implement and manage network services offer a very large number of options and facilities which can be set across configuration files. Configuration files are sometimes very complex; the same functionality can occasionally be obtained with different configuration parameters. Configuration files render products highly flexible. In contrast, web interfaces to configure and manage the product could reduce the set of possible options, thus losing flexibility. Yet, at the same time, web user interfaces should be user-friendly; whereas increasing flexibility entails increasing the complexity of the interfaces.

It is difficult to obtain simple web interfaces without reducing the configuration options set. But customizing the web interface to be applied to an organization makes a great difference. In this case, a web interface can be used with satisfactory results, since within a specific user application the full generality of the configuration file is not needed.

We designed and implemented the web interface in order to meet the requirements of our organization. For instance, our interface automatically leads the administrator to use our standard address format, thus achieving a satisfactory (for us) level of simplicity in the address. Due to the lack of a central directive for defining the syntax of the e-mail address' local part (the portion prefixing the @ symbol), each CNR organization unit defined its own schema making it impossible to see a homogeneous addressing schema for CNR. Sometimes, users are not able to guess (e.g. after a change of address) the e-mail address of a person belonging to the same organization. We are just now starting to use a LDAP (Lightweight Directory Access Protocol) server [4] [5] [6], in part to promote the adoption of a common addressing schema. The old address will continue to operate as an alias of the new official e-mail address, conforming to the naming schema Firstname.Lastname@cnr-sub-domain [7].

The interface is composed of 4 parts: "local mailboxes", "addresses for remote mailboxes", "aliases" and "distribution list aliases" [Fig. 1].

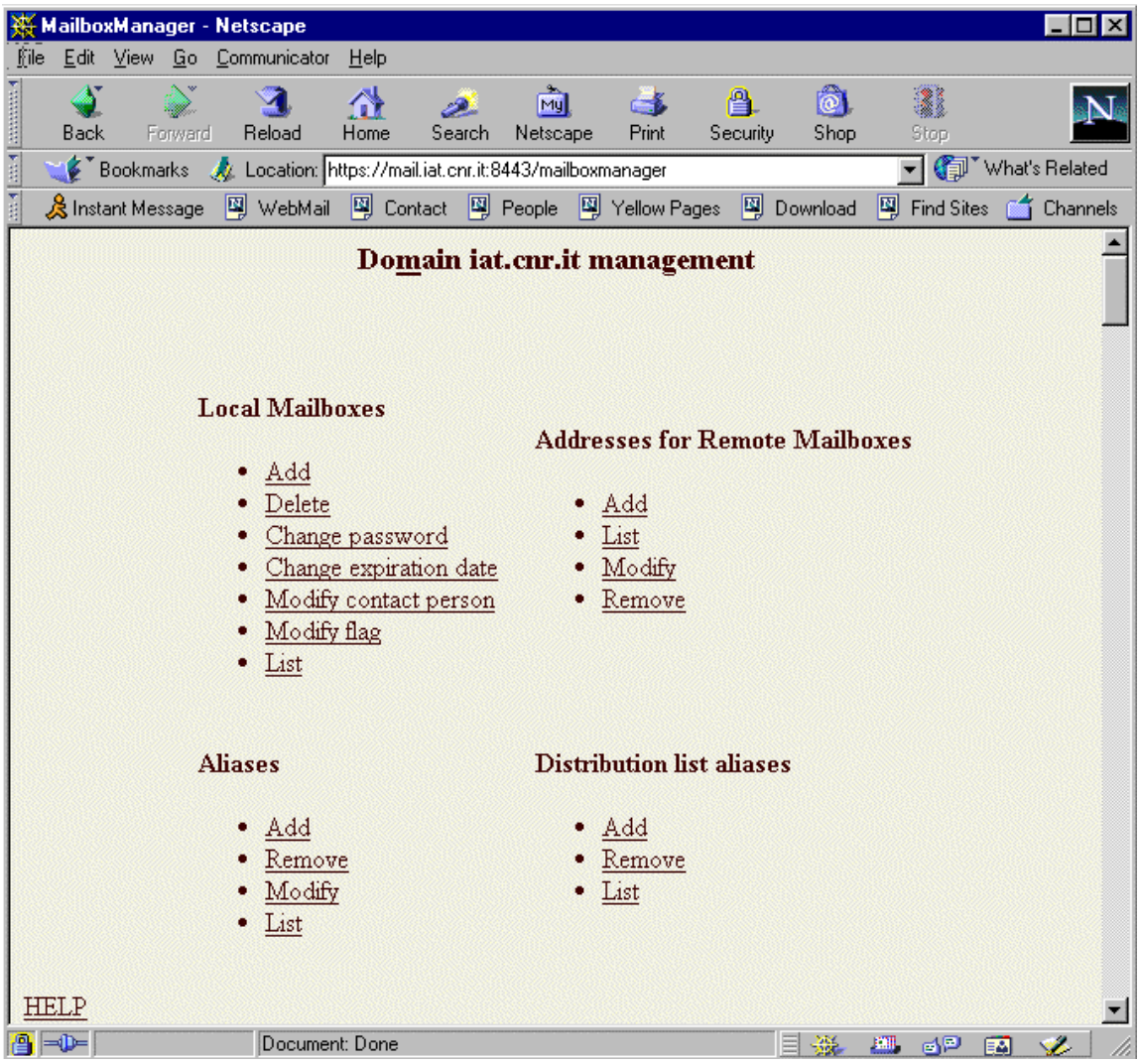

Fig. 1 - Mailbox manager: the administration interface

The first part allows the administrator to add, remove and list mailboxes, and to change both password and user expiration date [Fig. 2]. The interface manages both personal and role addresses.

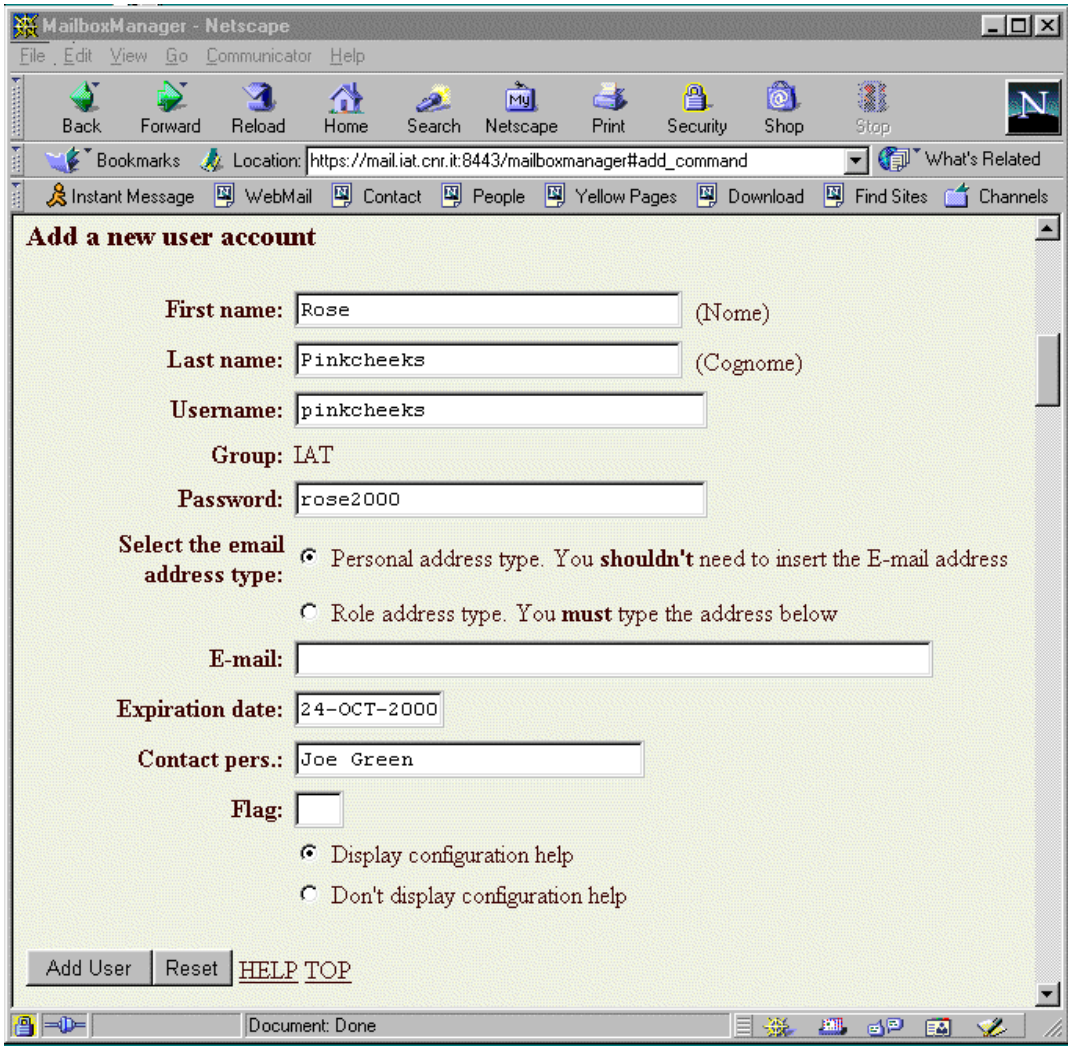

Fig. 2 - iat.cnr.it domain: add a new user

While creating personal mailboxes the web interface requires only the user's first and last name. After that, the CGI process creates the official address in the format Firstname.Lastname@domain and the aliases Initial-of-Firstname.Lastname@domain, Lastname@domain [Fig. 3].

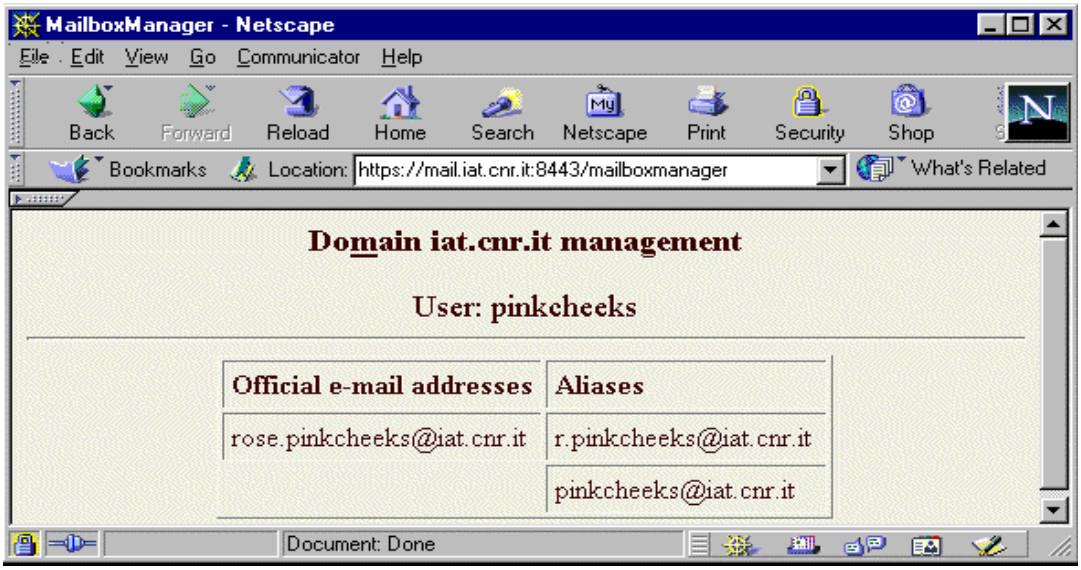

Fig. 3 - iat.cnr.it domain: aliases for the pinkcheeks user

Address ambiguities, due to people sharing the same last name, are automatically resolved by our e-mail product which sends back a delivery notification message (delivery has failed) to inform the sender about the ambiguity and asking him to specify one of the official addresses. This behavior could be obtained interacting with a LDAP server containing users' configurations.

Once the mailbox has been created, one page showing the client configuration (for different products) is shown to the administrator who then can print it for the user [Fig. 4]. We have also developed an extensive on-line help accessible from each interface page.

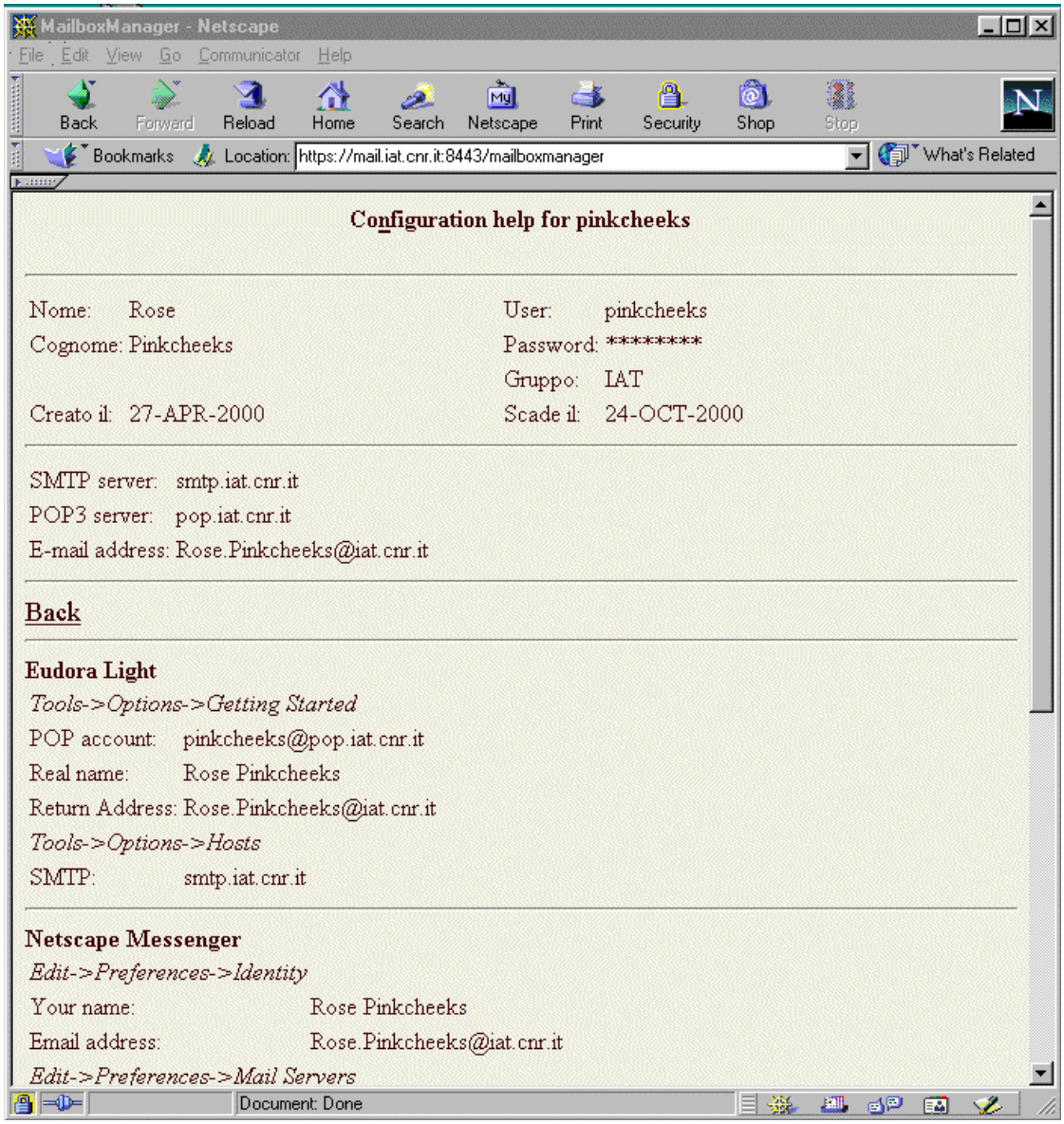

Fig. 4 - the user configuration help

The section "addresses for remote mailboxes" allows definition of an official address (in the selected domain) referring to a remote mailbox. This function is useful when the administrator wishes to be in control of a step-by-step migration process.

The "aliases" section allows administrators to add, remove and list user aliases (local and remote).

Our institute also offers housing for web and mailing lists services (to CNR Institutes). The last section allows the administrator to create, remove or list the aliases required to forward a message sent to a mailing list belonging to the administrator's domain to our list server, located on a different system.

The administration interface is accessible by secure sessions (https). The user authentication is based on ACLs using user and password. On the base of the given values, the CGI script loads the interface's configuration file that enable the administrator to act only over his domains, thus

maintaining operation spaces separated. Figure 2, for instance, shows the administration interface for the domain iat. It is important to observe that the administrator can create mailboxes only within the group IAT. If an administrator manages more than one domain, the interface shows his managed domains in a list box.

The proposed solution is cost-effective since it performs repetitive operations while avoiding human error, and reduces administration and maintenance time. The interface is fairly simple and can be used by individuals without specialized skills.

2.3 The quality of service

Advanced e-mail products (conforming to the IETF standards definition) provide users with a high-quality e-mail service and guarantee interoperability between products by different companies. The distributed administration model permitted us to reduce the effort required to manage and maintain multiple servers and to concentrate our attention on improving the quality of service offered to the end user.

Our server includes:

- The Delivery Status Notifications (DSN) SMTP extension. Since its first release, SMTP (Simple Mail Transfer Protocol [1]), the original protocol for sending e-mail, has been extended with multiple features.

  Different mail servers can support different SMTP extensions. As general rule, e-mail systems not supporting the most important SMTP extensions should not appear on the e-mail backbone because they degrade the quality of service (QoS).

  DSN, for example, is a SMTP extension [2] [3] enabling the client (on behalf of the sender) to require a message delivery status notification, specifying if the message has been delivered or not into the recipient mailbox. Figure 5 shows an example.

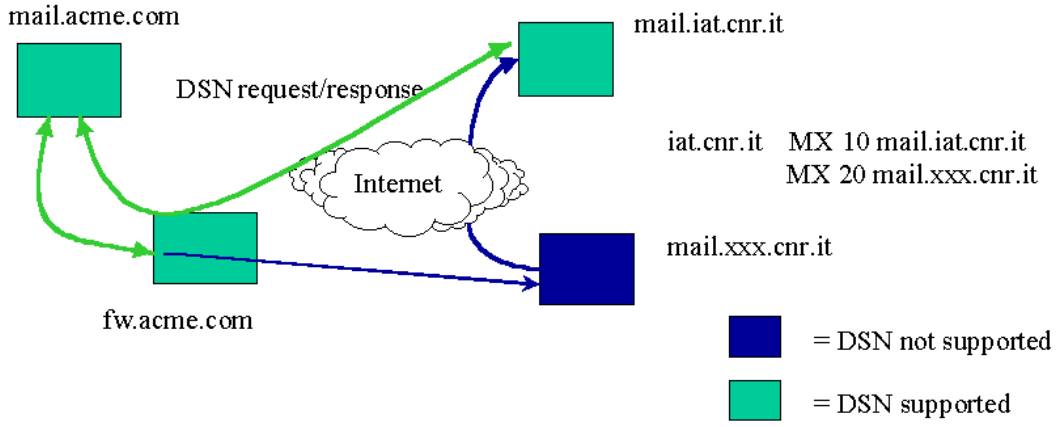

Fig. 5 - Delivery Status Notification example

A user X in domain acme.com sends a message to a user Y in domain iat.cnr.it (asking for a DSN receipt). The message is carrying a DSN request. If the message follows the primary path (through the mail.iat.cnr.it server), the sender will receive the delivery notification message from the destination mail server. If the message follows the secondary path crossing the mail.xxx.cnr.it server (not supporting DNS), the sender will receive a message notification from the intermediate server (fw.acme.com) informing him that the message was forwarded to a system not supporting the DSN extension.

- Secure client-server SMTP, POP and IMAP sessions, using TLS (Transport Layer Security [8] [9] [10] better known as SSL). This security mechanism enables client and server to cipher the transmission channel, thus protecting messages from tampering and eavesdropping. TLS is included as an extension for SMTP, POP and IMAP protocols, and it is supported by a growing number of e-mail clients and servers. We consider this feature to be very important in protecting wide area network connections between clients and servers (as in the case of a centralized service).

We must note that TLS is a transport level security mechanism. Although encryption could be applied during the message transmission (if both the sender and the receiver server support TLS), however, the message stored in the recipient mailbox is not encrypted. In order to have message content confidentiality, the user has to use public key cryptography techniques. Secure e-mail is an end-to-end mechanism.

- SASL (Simple Authentication and Security Layer) support to authenticate SMTP, POP and IMAP sessions. SASL [11] is a specification for adding authentication support to connection-based protocols. This authentication method avoids the transmission of a plain password over the network (using for example CRAM/MD5 mechanism [12]). Again this feature is supported as SMTP, POP and IMAP extension.
- Authentication for SMTP sessions (SMTP extension AUTH [13]). Sometimes anti-relay countermeasures render users unable to work efficiently from external networks. Users are unable to send messages out from their organization, but this limitation is not acceptable for scientific networks.

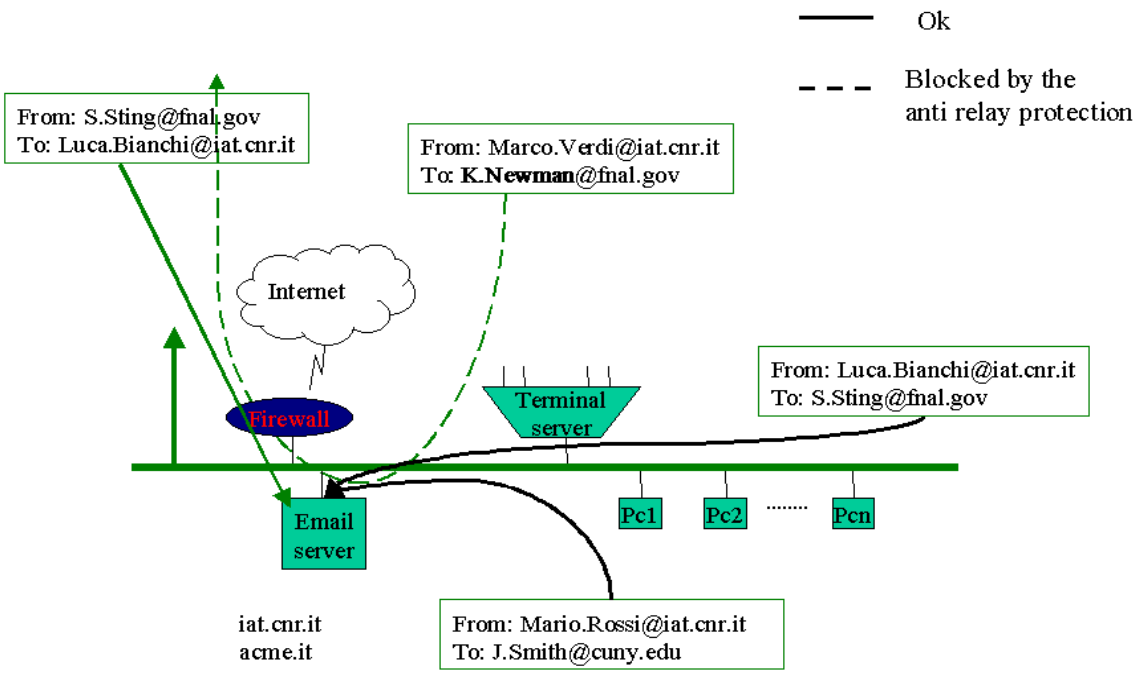

Fig. 6 - Anti-relay configuration

Using the AUTH extension we are able to set an anti-relay configuration that gives our e-mail users the liberty to use our SMTP server from external networks as well. The mail server accepts every message addressed to the local server but requires SMTP client authentication to permit relay from external networks. In this way, CNR users can continue to send messages through our server even when the connection comes from external networks.
Figure 6 shows an example.

- Users coming from the internal network can send message to any Internet user. For example Luca.Bianchi@iat.cnr.it can send a message to S.Sting@fnal.gov.
- External users can send anything to users within the iat.cnr.it domain. S.Sting@fnal.gov can send a message to Luca.Bianchi@iat.cnr.it.
- The system requires user authentication (user and password) for sending messages from external networks to external users. For example, Marco.Verdi@iat.cnr.it (coming from the Internet) must digit his password to be able to send a message to the destination address K.Newman@fnal.gov.

In addition to the anti-spamming configuration (preventing the use of our server as a relay to perform spam activities), in order to reduce the reception of unsolicited messages, care must be taken in the definition of mailing lists. For example when defining a mailing list it is very important to permit only owners to review the list, thus preventing outsiders from stealing e-mail addresses.

When possible sender restrictions (authorized domains, addresses, etc.) help contain this disagreeable phenomenon.

- The mail system permits users to access remote mailboxes via IMAP protocol (Internet Message Access Protocol). The mail server offers both POP (Post Office Protocol) and IMAP access [14] [15]. In particular IMAP permits access to, and manipulation of, electronic mail messages on the server. It includes operations for creating, deleting, and renaming remote mailboxes; checking for new messages; permanently removing messages; setting and clearing message flags. IMAP offers multiple advantages such as the user mobility support and easy implementation of help desk services.
- Our added value e-mail administration web interfaces enable administrators to manage one or more domains in a simple and flexible way. The interface (described in details in the previous paragraph) is accessible via secure sessions, using https.
- In order to increase service feasibility and performance we migrated from a single system to a SCSI cluster consisting of two systems sharing a RAID disk array and performing load balancing. This enables us to perform maintenance activities on one node without any service interruption.
- Finally, we developed software (server side) to furnish added value service to CNR libraries. Specifically, we implemented a selective e-mail/web gateway (for registered users). The proposed solution permits CNR library operators to continue using the e-mail service to send large documents (GIF, JPEG, PDF files), but at the same time overcomes problems that users may encounter when downloading large files with e-mail agents (due to the time-out of the mailbox access protocol). The system, by using a multi-part MIME (Multipurpose Internet Mail Extensions) message [16] [17] [18] [19] [20], is able to extract parts of messages and save them under a web server in order to permit users to download these large objects via http (hypertext transfer protocol). A text/html part is inserted into the original e-mail message in place of every extracted part, to specify to the receiver the URL where the extracted objects are stored [21].

As a future enhancement, we also wish to introduce anti-virus software server side. We believe that a server side control could save time and resources.

3. The service evaluation

To permit the evolution of CNR's e-mail service quality and reliability we need to introduce a new service infrastructure. In fact, it is no longer feasible to continue maintenance of all CNR e-mail servers when today's technologies permits us to restructure the service using only a few "high quality" servers.

Our experience has shown that the CMDA model offers numerous advantages:

- By reducing the number of servers to their technical minimum we can:
  - Facilitate system control and maintenance (e.g. monitoring, debugging, software upgrades) by reducing the number of points to be controlled thus decreasing the global effort sustained by the organization for managing the e-mail service;
  - Reduce security problems;
  - Decrease costs by concentrating the hardware/software and human resources dedicated to managing and monitoring systems in a central location;
- The administration workload is distributed among all organizations, thus implying:
  - The workload for the organization hosting the service does not increase with the number of domains. One of the most interesting features offered by the delegated model is the possibility to get rid of administration duties. This means that by increasing the number of the managed domains the duties of the organization hosting the services are not increased. In our case, we manage 17 domains. At least, we reduced the number of servers from 16 (the official ones) to 1 while maintaining the same number of people for maintenance duty (2).
  - Peripheral organization units maintain their flexibility and autonomy in organizing their services;
  - The response time for satisfying one user request depends on his organization units, such as using a distribution solution;
- The administration interface offers further advantages.
  - It is user friendly, not requiring skilled technicians;
  - It is error-safe: automatic process avoids human error (i.e., when editing configuration files, recompiling configurations, etc);
  - Critical operations are performed by the system, thus preventing local administrator from accessing the system as privileged accounts;
  - It automatically implements the organization's addressing policy.

- An additional advantage is the transparency of the model's implementation. In general we noticed that the transparency of this model - which masks the centralization of the service - helps overcome any bureaucratic problem that might arise in the organization where the model is proposed.

So far we have only discussed the advantages of this model, however, there are a few drawbacks:

- Centralized management leads to a single point of failure. It is very important to use reliable systems and back-up configurations;
- This model's implementation requires a feasible network infrastructure and a guaranteed bandwidth (in order to permit clients who are geographically distant to access and download messages within a short time).
- CGI could represent a weak point in system security. The implementation of the interfaces is very critical. Carelessly developed CGI scripts may enable hackers to penetrate the system. Each parameter passed from client to server should thus be controlled and errors must be carefully managed. Access to the web interfaces can be protected by Access Control Lists (ACL) based on the IP address or user/password. An interesting alternative is the use of client certificates. In addition to these techniques the usual system and network security mechanisms have been added.

In a large organization such as CNR where there is considerable freedom in organizing and managing services it is very difficult to attempt to introduce the model all at once. Lacking a real central authority capable of imposing a solution, the next very important step is to transfer our new vision of the service to the CNR network administrator community.

We have begun seminar activities, introducing new technologies and focusing our attention on the quality of service. In addition, we have initiated discussion of these topics on CNR network administrator mailing lists.

Although it takes time, we have observed the increasing acceptance of our proposal. Since the first proposal of this delegated administration service, a growing number of institutes including some outside our geographical area (IAS - CNR Terni, ITIS - CNR Matera, and IRPEM - CNR Ancona) have decided to move their e-mail service onto our server.

Figures 7, 8 and 9 show the e-mail statistics of the first quarter 2000. The values include the total traffic (incoming, outcoming and the internal) for each managed domain. Figure 9 shows the average number of messages per mailbox (number of messages/number of managed mailbox).

A few months ago, a mail server using our management interfaces was activated in Padua. This server manages domains for the Research Area in Padua.

The CMDA model attempts to reduce the number of servers to their technical minimum. But what is the correct minimal number of servers? The answer varies according to many factors: topological considerations, network backbone performance, geographical distribution of the organization units and security issues can all influence the decisions.

Today, e-mail servers can efficiently manage thousands of users. We think that a possible bottleneck of the model could be network congestion. Network topology and traffic are the most important factors to consider when designing complex e-mail system architectures. For organizations spread over wide areas, additional servers located in different geographical areas are required in order to optimize network traffic.

We believe that three servers might be sufficient for the entire CNR Community - one for Northern Italy, one for Central Italy, and one for Southern Italy. However, political and security reasons related to our organization policy lead to the expansion of this number to one server for each CNR Research Area.

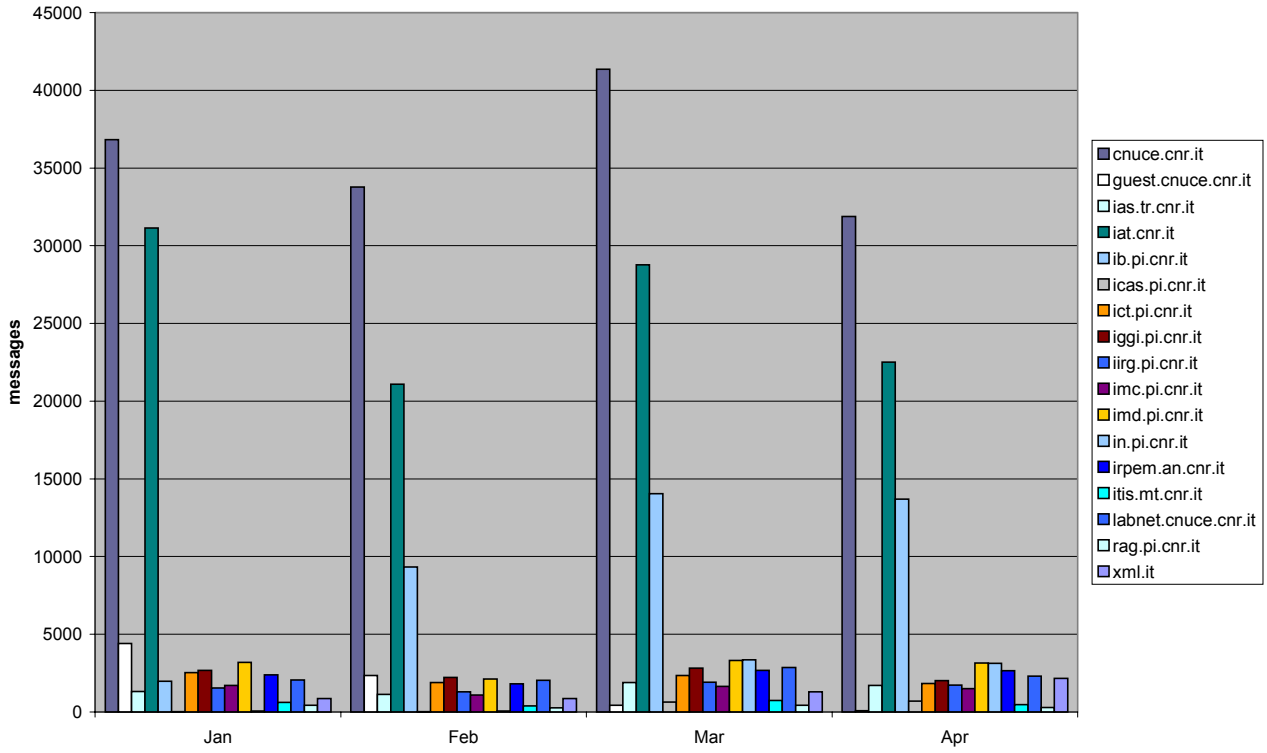

Fig. 7 - Number of messages by domain

This is a simple but effective outsourcing model. The proposed model could be advantageously adopted in medium-to-large organizations with distributed units spread over wide areas (such as Universities, Public Administrations, large companies) and by ISPs (Internet Service Providers) offering value added services to their customers.

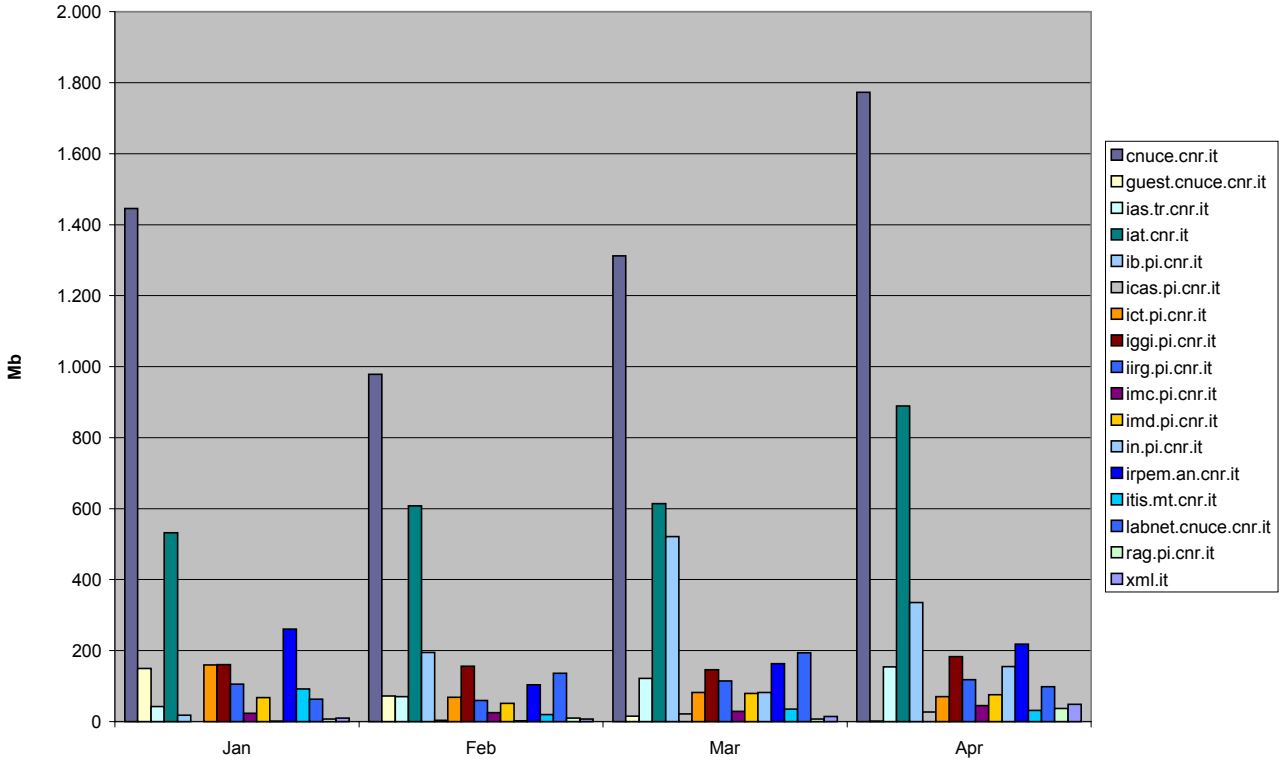

Fig. 8 - Traffic in Mbytes by domain

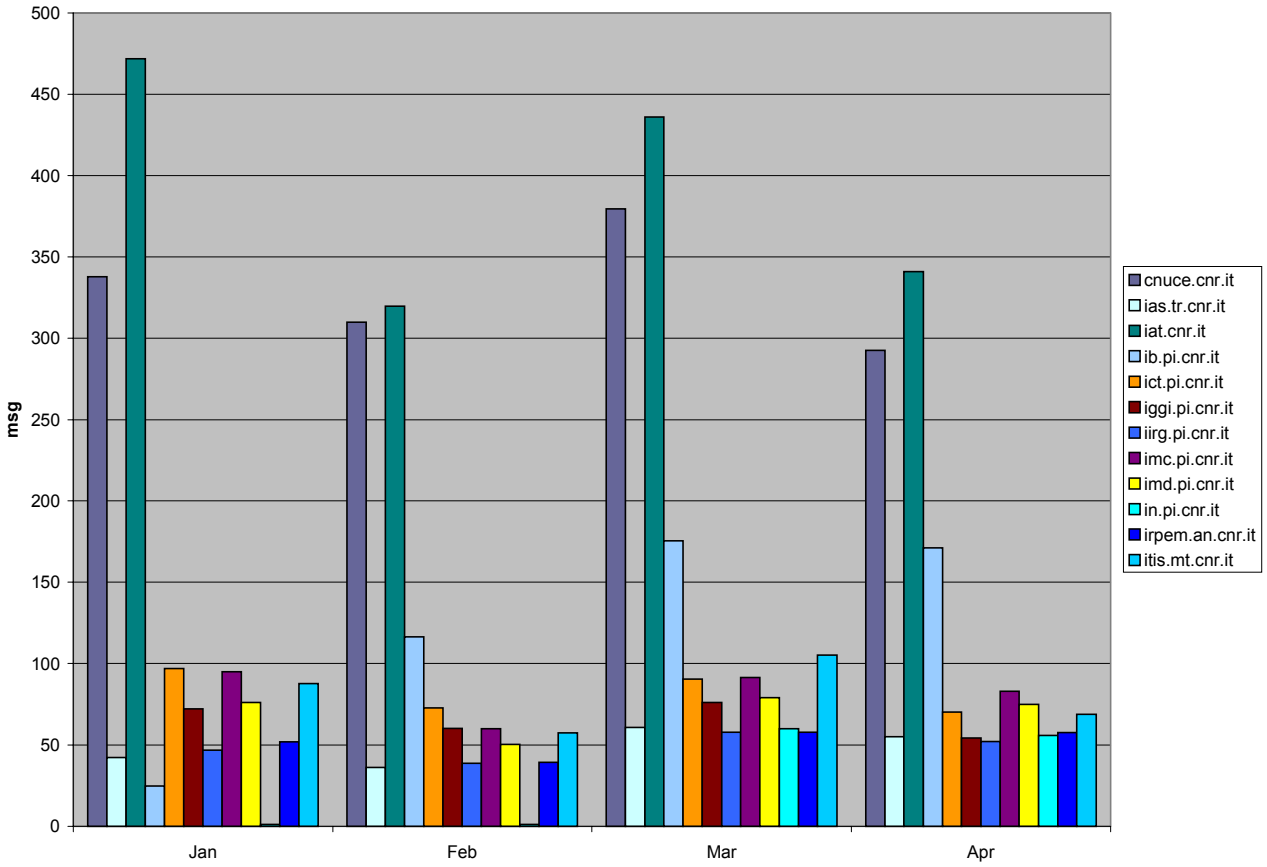

Fig. 9 - Average number of messages per mailbox

4. Conclusions

This paper is an exploration of the design of a complex e-mail system involving a novel management framework. Our experience had shown that:

- The use of products conforming to international standards (in conformity with the latest IETF standards) allows the organization to achieve reliable, flexible, inter-operable and secure e-mail services.
- Investments made when introducing the CMDA model (analyzing systems and user requirements, implementing/maintaining CGI interfaces) are quickly repaid by the consequent reduction in costs. Unskilled personnel could perform administrative duties while the workload is distributed across the peripheral organizational units.

Both these features contribute to increasing the productivity of the organization.

The hosting of services involves, but is not restricted to, web, e-mail and mailing list services. We plan to implement the CMDA model to Domain Name System Services in order to spread all administrative duties over distributed organization units.

References

[1] Jonathan B. Postel, RFC821: Simple Mail Transfer Protocol, August 1982 - ftp://ftp.isi.edu/in-notes/rfc821.txt.

[2] K. Moore, RFC1891: SMTP Service Extension for Delivery Status Notifications, January 1996 - ftp://ftp.isi.edu/in-notes/rfc1891.txt.

[3] K. Moore & G. Vaudreuil, RFC1894: An Extensible Message Format for Delivery Status Notifications, January 1996 - ftp://ftp.isi.edu/in-notes/rfc1894.txt.

[4] M. Wahl, T. Howes, S. Kille, RFC2251: Lightweight Directory Access Protocol (v3), December 1997 - ftp://ftp.isi.edu/in-notes/rfc2251.txt.

[5] Howes, S. Kille, RFC2252: Lightweight Directory Access Protocol (v3), December 1997 - ftp://ftp.isi.edu/in-notes/rfc2252.txt.

[6] M. Wahl, S. Kille, T. Howes, RFC2253: Lightweight Directory Access Protocol (v3), December 1997 - ftp://ftp.isi.edu/in-notes/rfc2253.txt.
[7] D. Crocker, RFC2142: Mailbox Names for Common Services, Roles and Functions, May 1997 - ftp://ftp.isi.edu/in-notes/rfc2142.txt.
[8] T. Dierks, C. Allen, RFC 2246: The TLS Protocol Version 1.0, January 1999 - ftp://ftp.isi.edu/in-notes/rfc2246.txt.
[9] P. Hoffman, RFC2487: SMTP Service Extension for Secure SMTP over TLS, January 1999 - ftp://ftp.isi.edu/in-notes/rfc2487.txt.
[10] C. Newman, RFC 2595: Using TLS with IMAP, POP3 and ACAP, June 1999 - ftp://ftp.isi.edu/in-notes/rfc2595.txt.
[11] J. Myers, RFC2222 Simple Authentication and Security Layer (SASL), October 1997- ftp://ftp.isi.edu/in-notes/rfc2222.txt.
[12] J. Klensin, R. Catoe, P. Krumviede, RFC2195: IMAP/POP AUTHorize Extension for Simple Challenge/Response, September 1997 - ftp://ftp.isi.edu/in-notes/rfc2195.txt.
[13] J. Myers, RFC2554: SMTP Service Extension for Authentication, March 1999 - ftp://ftp.isi.edu/in-notes/rfc2554.txt.
[14] J. Myers & M. Rose, RFC1939: Post Office Protocol - Version 3, May 1996 - ftp://ftp.isi.edu/in-notes/rfc1939.txt.
[15] M. Crispin, RFC 2060: Internet Message Access Protocol -Version 4rev1, December 1996 - ftp://ftp.isi.edu/in-notes/rfc2060.txt.
[16] N. Freed, N. Borenstein RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies, November 1996 - ftp://ftp.isi.edu/in-notes/rfc2045.txt.
[17] N. Freed, N. Borenstein, RFC 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types Novembre 1996 - ftp://ftp.isi.edu/in-notes/rfc2046.txt.
[18] K. Moore, RFC 2047: Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text, November 1996 - ftp://ftp.isi.edu/in-notes/rfc2047.txt.
[19] N. Freed, J. Klensin, J. Postel, RFC 2048: Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures, November 1996 - ftp://ftp.isi.edu/in-notes/rfc2048.txt.
[20] N. Freed, N. Borenstein, RFC 2049: Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples, November 1996 - ftp://ftp.isi.edu/in-notes/rfc2045.txt.
[21] F. Gennai, L. Abba, M. Buzzi, M. G. Balestri, S. Mangiaracina: Experience in implementing a document delivery service - IAT-B4-1999-02, Digital Library 00, July 2-7 San Antonio, Texas.