

# Project EmailNG

## *Next Generation Email System*

Project EmailNG is an upgrade project of our mail systems which were installed in 2004 in their current form. Along with upgrading the existing systems new functionality and options are implemented to reflect the technological advances of the last years. EmailNG depends entirely on FOSS and makes use of the CS Dept. virtualization and consolidated storage systems.

Apart from the infrastructure being used and the time spent on implementing the project there are no other costs. The system is custom built using entirely internal technological knowledge and dependent entirely on the CS support personnel for support and maintenance (and the FOSS community of course).

**The “Email administrator manual” should be read along with this document to understand the installation details. Here we describe the project steps. Description of the system and installation details are provides in the Administrator manual.**

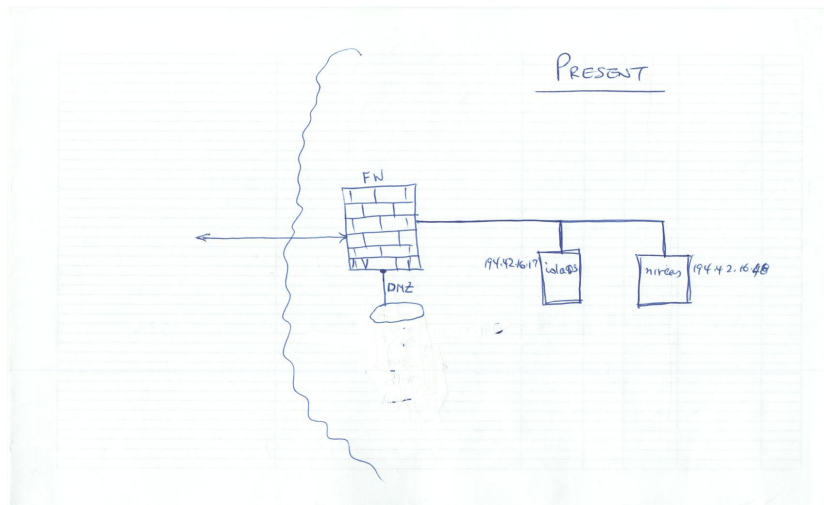
## Features

- Advanced capabilities fit for a diverse community
- Expandability at all levels (Storage, IMAP, SMTP, SPAM and VIRUS control)
- Multilevel security (system, email, DMZ)
- E-Mail client independence supporting almost all IMAP, POP and Webmail clients
- Robustness, availability, fault tolerance built into the original design
- User control – users can customize their message delivery experience (filters, SPAM control etc)
- Support for advanced and entry level users
- Support for mobile devices and clients
- No down time maintenance operations
- Minimal cost with FOSS and off the shelf hardware. Uses widely available and tested FOSS software.
- Based on widely accepted protocol standards (RFC) for all the software
- Vendor independence. No vendor lock in. Built with local technology knowledge and experience.

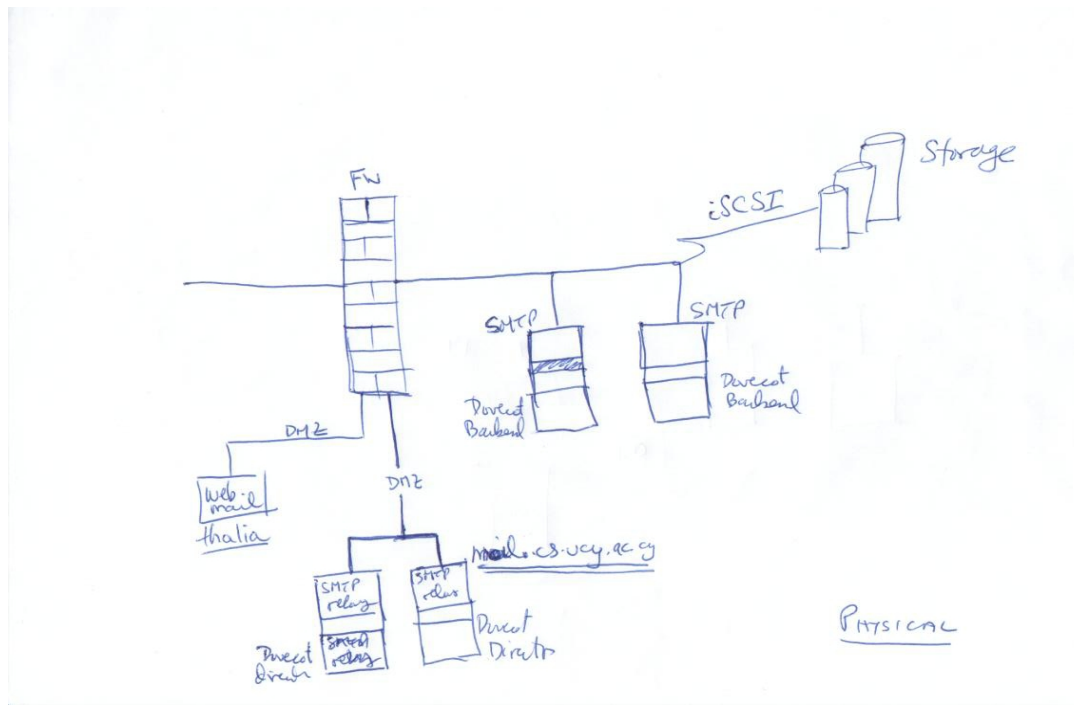
## Why Change?

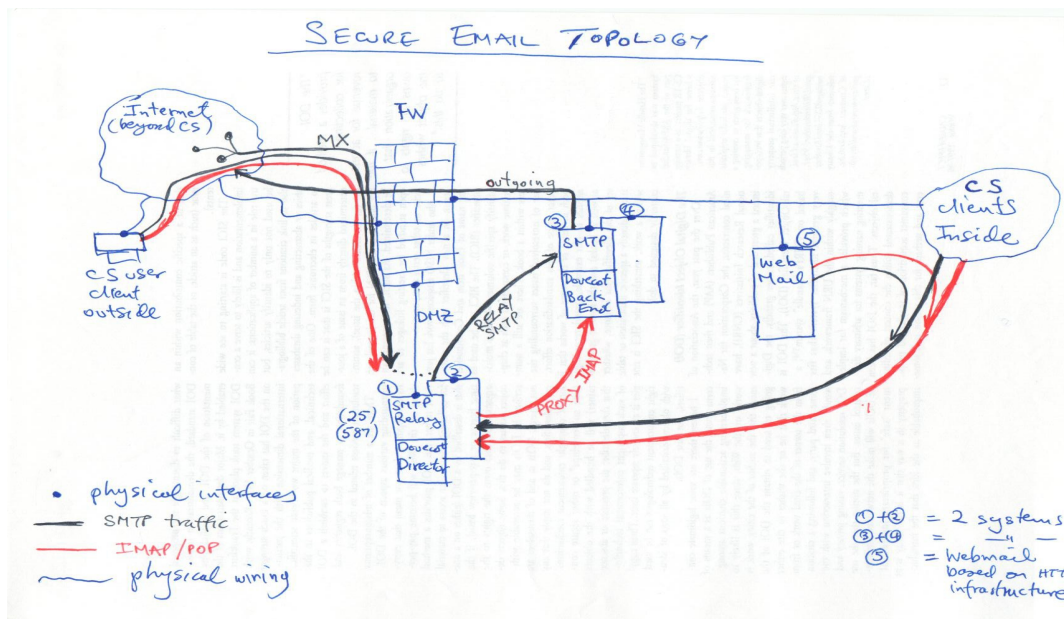
- There is a pressing need for a system upgrade of software and hardware
- security challenges have increased and the current status does not address even the basic threats that exist today
- provide better availability in line with dept. requirements both during normal operations but also during maintenance operations
- enhance the user functionality by allowing the user to better control his/her environment
- better mobile systems support

## Current Status



## Future Status





**Objectives:**

1. Create a robust, fault tolerant upgrade of the existing system
2. Upgrade of software and take advantage of new features in software
3. Change from the MailScanner software to the Amavisd-new system
4. Make use of our extensive virtual server platforms and our consolidated storage
5. Take advantage of our LDAP installation to centralize and streamline the email system authentication and user profiles
6. Improvements on
  - a) Security
  - b) Efficiency (storage, processing speed)
  - c) User capabilities and UI
7. The following areas will be affected:

Area	Short description
User Quota	<ul style="list-style-type: none"> <li>• implement Dovecot based quota with the ability to enforce from LDAP settings rather than fs quota</li> <li>• over quota management</li> <li>• user monitoring</li> </ul>
Message Storage	<ul style="list-style-type: none"> <li>• Integration with consolidated storage systems at CS</li> <li>• Multiple location message storage</li> <li>• synchronization with dsync</li> <li>• migration to the more efficient mbox message storage format</li> </ul>
Message format	<ul style="list-style-type: none"> <li>• Change from maildir to Dovecot mbox</li> </ul>
Better filtering	<ul style="list-style-type: none"> <li>• Use a standards based filter engine (sieve)               <ul style="list-style-type: none"> <li>◦ clients will be affected</li> </ul> </li> </ul>
Better user experience	<ul style="list-style-type: none"> <li>• Message filter setup from within the clients</li> <li>• individual quota monitoring</li> <li>• over quota management</li> </ul>
Fault tolerance, resilience	<ul style="list-style-type: none"> <li>• Multiple message servers (virtual machines)</li> <li>• ability for the system to survive server failures</li> <li>• automatic redirection of mail traffic and users to surviving</li> </ul>

	<ul style="list-style-type: none"> <li>servers</li> <li>automatic storage synchronization on two servers</li> </ul>
Performance	<ul style="list-style-type: none"> <li>Separation of user activity from back end server activity</li> </ul>
Better SPAM control	<ul style="list-style-type: none"> <li>Use of amavisd</li> <li>Multilevel filtering</li> <li>Server side filters and options (before queue-after queue filtering)</li> </ul>
User filters (spam and message mgmt)	<ul style="list-style-type: none"> <li>Server side user filters with Sieve</li> </ul>
User management	<ul style="list-style-type: none"> <li>Integration with LDAP services</li> </ul>
Security/SMTSPS	<ul style="list-style-type: none"> <li>Greatly enhance security by designing the whole system around using the DMZ with inside and outside facing servers</li> <li>Login with encrypted channel to SMTP when submitting messages for delivery (SASL authentication)</li> </ul>
Shared Mailboxes	<ul style="list-style-type: none"> <li>Internal Lists or Announcements</li> </ul>

## Project Overall Flow

This is an overview and plan. Not a complete action list. See the section “Project Time Flow” below for a detailed action list and the Appendix for a detailed action account and notes.

How to install, configure the systems, enable and protect services is described in the “Email Administrator Manual”.

The project takes a phased approach where the general flow is:

1. PHASE I: Primary IMAP network (theano, gorgo)
    1. priority is give to the primary IMAP network setup (since this will provide substantial improvement in user experience right from the start)
    2. Experiment with new features (mail alt locations, dsync to mbox format)
  2. PHASE II: Primary SMTP services network (theano, gorgo)
  3. PHASE III: Secondary IMAP network
  4. PHASE IV: Aecondary SMTP services network
  5. PHASE V: Message storage format, security, tuning, final checks
    1. Message storage format change to mbox
    2. Security enhancements
    3. tuning
  6. PHASE VI: External systems integration
    1. Mailing list manager
    2. Pine on ADA
    3. caching DNS
- Primary and secondary IMAP/SMTP networks function simultaneously and do not have priority over each other. Here the terms are used for reference only.
- It should be noted that where ever we mention IMAP we really mean both IMAP and POP3 since we support both protocols.**
- **See also the ADDENDUM on user names, groups and aliases. This was added after project**

start when it was realized that our names,groups, aliases system needed a major overhaul.

- **NO EMAIL SERVICE DISRUPTION IS EXPECTED**

## Project Time Flow

### PRE-REQUISITES:

1. Check and verify that at least one storage device to be used is ready to accept load
  1. hermes (nfs) -> argo -> /Mail (is already available)
  2. orpheas (nfs) -> argo -> /Mail (will be available soon as a final location)
  3. orpheas (nfs) -> NetApp -> /MailAlt (will be available soon)

### PHASE I: PRIMARY IMAP SET-UP (Expected Duration: 20 days)

#### 2. THEANO – IMAP proxy #1

1. Install and secure OS - CentOS
  - A) iptables, fail2ban, secure at the firewall, set up monitoring
2. Compile and/or Install basic IMAP software
  - A) Dovecot
  - B) Configure IMAP proxy (director #1) to proxy to either NIREAS/IMAP or IOLAOS/IMAP based on user and or user-group. This is an initial state to test the director service.

#### 3. GORGO – IMAP back end #1

1. Install and secure OS - CentOS
  - A) iptables, fail2ban, secure at the firewall, set up monitoring
2. Compile and/or Install basic IMAP software – Dovecot (Ref.: Setting up Dovecot)
3. Configure to become a back end IMAP server
4. enable LDAP authentication.
5. LDAP schema for users directly accessed by IMAP.
  - A) Why not through PAM for password authentication
  - B) MUST be direct for extra fields (is this true? Must be verified)
6. Install the Sieve extension - filtering
7. Enable IMAP Quota

#### 4. Expire NIREAS/IMAP only – keep NIREAS/SMTP for now

- A) Reconfigure THEANO to proxy to the new IMAP back end (GORGO)
- B) Disable IMAP on NIREAS
- C) mail.cs.ucy.ac.cy should point to theano.cs.ucy.ac.cy
- D) MX records should remain as is (iolaos, nireas)

#### 5. GORGO – NewFiler/MailAlt – Optional Activity

1. Convert message store from maildir to mbox by using dsync
  - This is sort of a backup process

- TO actually make use of the /MailAlt requires the ability to individually set the location of message repositories

### **MILESTONE #1:**

**Successful operation of Dovecot as an IMAP server, proxy/director on theano and back end on gorgo means that PHASE I is finished and we have a complete usable IMAP mail environment based on the new objectives.**

### **PHASE II: PRIMARY SMTP SET-UP (Expected Duration: 20 days)**

6. THEANO – SMTP External Relay #1
  1. Enable SMTP services
    - A) (Compile), install and configure Postfix as a relay
    - B) Relay SMTP traffic to IOLAOS, NIREAS
    - C) *SPAM/VIRUS control – AMAVISD*
      - I. *AMAVISD*
      - II. *CLAMAV set up*
      - III. *SPAMASSASSIN set up*
7. GORGO - SMTP Internal Back End #1
  1. (Compile), install and configure Postfix as a back-end
  2. *Dovecot needs to be configured here to enable its LDA/LMTP to enable the LDA delivery and Postfix to make use of it*
  3. *Configure Sieve global filters to replace procmail*
  4. *Add new MX record with higher priority on GORGO*
  5. *Demote NIREAS MX record to a very low priority (MX priorities are now GORGO, IOLAOS, NIREAS)*
  6. *mail-out.cs.ucy.ac.cy (???)*
8. THEANO – Reconfigure to Relay to: IOLAOS, GORGO now

### **MILESTONE #2:**

**Proper operation of both SMTP relay #1 and SMTP back end #1 allows bringing the new systems on-line (with an additional MX record). It also allows, as second step, transfer of existing system (nireas, iolaos SMTP) functionality to the new systems. At this point NIREAS is free of mail services but kept as backup in case we discover problems.**

### **PHASE III: SECONDARY GROUP IMAP SET-UP (Expected Duration: 15 days)**

9. ELYSSO – IMAP proxy #2
  1. Install and secure the OS - CentOS
    - A) Iptables, fail2ban, secure at the firewall, set up monitoring
  2. Compile, install, configure basic IMAP software - Dovecot
  3. Enable IMAP proxy/director #2
    - A) Proxy to GORGO and IOLAOS for now
10. MIRTO – IMAP back end #2

1. Install and secure OS - CentOS
    - A) iptables, fail2ban, secure at the firewall, set up monitoring
  2. Compile and/or Install basic IMAP software - Dovecot
  3. Configure to become a back end IMAP server #2
  4. Install the Sieve extension – user filtering
  5. enable LDAP authentication
11. Expire IOLAOS/IMAP only – keep IOLAOS/SMTP for now
- A) Reconfigure THENO, ELYSSO to proxy to the new IMAP back ends #1, #2 (GORGO, MIRTO)
  - B) Disable IMAP on IOLAOS
  - C) mail.cs.ucy.ac.cy should now point to theano.cs.ucy.ac.cy and elysson.cs.ucy.ac.cy
  - D) MX records should remain as is (gorgo, iolaos, nireas)

#### **PHASE IV: SECONDARY GROUP SMTP SET-UP (Expected Duration: 15 days)**

##### 12. ELYSSO – SMTP External Relay #2

1. Enable SMTP services
  - A) (Compile), install and configure Postfix as a relay
  - B) Relay SMTP traffic to GORGO, IOLAOS
  - C) SPAM/VIRUS control – AMAVISD
    - I. AMAVISD
    - II. CLAMAV set up
    - III. SPAMASSASSIN set up

##### 13. MIRTO - SMTP Internal Back End #2

1. (Compile), install and configure Postfix as a back-end
2. Dovecot needs to be configured here to enable its LDA/LMTP to enable the LDA delivery and Postfix to make use of it
3. Configure Sieve global filters to replace procmail
4. SPAM/VIRUS control – AMAVISD
  - A) CLAMAV set up
  - B) SPAMASSASSIN set up
5. Add new MX record for MIRTO
  - A) MX records priority now GORGO, MIRTO, IOLAOS
  - B) Remove NIREAS MX record (NIREAS is now dead for email. Thank you – more than 10 years of service!!)
6. mail-out.cs.ucy.ac.cy (???)

##### 14. THEANO – Reconfigure to SMTP relay to: GORGO and MIRTO now

#### **PHASE V:**

#### **MDBOX MESSAGE STORE CONVERSION, TUNING, SECURITY ENHANCEMENTS, FINAL CHECKS (Expected Duration: 20 days)**

##### 15. Convert message store to mbox message format

1. DSYNC – Replicate message storage to a secondary storage area

2. Enable "alternative" location for Dovecot
16. Tuning of systems – Final Configurations – SMTP
  1. Remove IOLAOS MX record (IOLAOS is now dead for email)

### **MILESTONE #3:**

#### **mdbox conversion**

### **PHASE VI: The Further Work Phase**

**(Some of these actions are not in the Project Plan. Some are also noted for further investigation as a wish list))**

#### 17. FURTHER ENHANCEMENTS

##### 1. Mailing lists management

A) csall etc

B) project mailing lists

C) ad-hoc mailing lists – user defined – announce

*Current setup: mailing lists are directed to <list>@listserver.cs.ucy.ac.cy directly. This also works with theano for the time being since it uses the same virtual-users set up. (13/01/2014)*

D) Aliases – investigate how aliases can be used in cases where no real users are needed – ex. conferences where the email eventually goes to a real account or accounts (16/01/2014)

#### 18. SPF record checking for incoming traffic on the SMTP relays.

##### 1. SPF DNS RR for cs.ucy.ac.cy

##### 2. SPF breaks .forward (!!) -- see how to fix with SRS or ditch SPF (!!)

#### 19. Unresolved Issues on which no decision has been made

##### 1. pine on ADA

##### 2. caching DNS (on outgoing SMTP)

#### 20. Investigate POLICYD for POSTFIX to battle the most nasty of SPAM and attack vectors. (16/01/2014)

#### 21. Should there be internal MX records on in.cs.ucy.ac.cy (in which the internal mail servers are) such that forwarding from the relays but also transmission from internal systems like listserver can direct to local servers in a fault tolerant manner?

#### 22. how to solve the problem of external relays access to internal users so that we reject messages destined to non-existent users on the border NOT inside. (16/01/2014)

##### 1. see postfix verify(8)

#### 23. Full Text indexing support from Dovecot (27/01/2014)

#### 24. Limit the number of messages a user can send

##### 1. smtpd\_recipient\_limit = 20 (;;)

##### 2. smtpd\_recipient\_overshoot = 10 (;;)



## Appendix: Activity Schedule

d – working day (estimate)

- Notes may need to be transferred to the user or admin manual

- **Where ever IMAP is mentioned we really mean both IMAP/POP3.**

- Yellow highlights contain issues that need to be revisited.

**Official Start: 09/12/2013**

**Expected Delivery: +90 working days (approx. End of April 2014).**

Systems will be put on line as they become fully functional in a phased approach.

Time	System	What	Notes	Done
<b>PHASE I: PRIMARY IMAP SET-UP (+20d total)</b>				
+3d	THEANO	- Install and secure OS with all already standard methods (see Linux install and security in wiki)	Checked	11/12/2013
		- iptables, fail2ban, secure, firewall - check further the VLAN security	This should be revisited on the final check-out and in line with future DMZ mods.	11/12/2013
+7d	THEANO	- compile and install dovecot	Due to a problem with IOLAOS hanging at random:	12/12/2013
		- Dovecot configuration as a front-end proxy #1	* this was slightly modified to go directly to gorgo which was already a live IMAP server also (see below) removing load from nireas and bypassing the unstable iolaos. Proxying is currently static and should be modified when the secondary IMAP is available.	12/12/2013
		- configure IMAP proxy to NIREAS/IOLAOS based on user/group (50/50).	* also decided to redirect RC to theano to bypass the unstable iolaos as soon as the theano/gorgo IMAP couple are ready and as a testing ground.	12/12/2013
+10d	GORGO	- Install and secure OS with all already standard methods (see Linux install and security in wiki)	Checked	12/12/2013
		- iptables, fail2ban, secure, firewall - check further the VLAN security	This should be revisited on the final check-out and in line with future DMZ mods.	12/12/2013
+15d	GORGO	- compile and install Dovecot 2.2.x	Checked	12/12/2013
		- Dovecot configuration as a back end #1	Checked	12/12/2013
		- enable LDAP authentication	* authentication is via SSSD/PAM to LDAP	12/12/2013

		- install the Sieve extension	* managesieve installed BUT cannot be used since proxying of this protocol MUST be enabled on THEANO-proxy – postponed until after installation of GORGO	12/12/2013 Proxying functional on 16/01/2014
		- install/enable IMAP quota	Checked	12/12/2013
		- Test for stand alone operation	Checked	12/12/2013
		-Test proper proxying from THEANO	** static proxying ** This should be changed when the whole system is in operation	12/12/2013
<b>Due to problems with IOLAOS being unstable decided to jump to PHASE II and postpone actions here until IOLAOS/SMTP is replaced. (12/12/2013)</b>				
+18d	LDAP	- set up of LDAP mail schema (kekkos)	** See temporary arrangement #1 below	16/01/2014
		- enable IMAP to receive user info from LDAP		
+20d	NIREAS	- reconfigure THEANO to proxy to the new GORGO/IMAP back end	Checked	12/12/2013
		- expire NIREAS IMAP – keep NIREAS/SMTP	postponed	18/06/2014
		- mail.cs.ucy.ac.cy should point to THEANO	postponed	18/06/2014
		- MX remain as (iolaos, nireas)	MX (see also below)	06/02/2014
+22d	GORGO/ NewFiler	- convert message store from maildir to mbox by using dsync manually	Postponed as a last feature test	
		- this is actually a backup process on the message store level		
		- NOTE: using the mail alt feature of Dovecot requires the ability to individually set the message location		
		- This is experimental at this stage and meant to test the concept		
<b>MAILSTONE #1:</b>				
TEST all above functionality for				
<ul style="list-style-type: none"> <li>• dovecot proxying</li> <li>• dovecot operation</li> <li>• quota</li> <li>• sieve</li> <li>• LDAP schema</li> <li>• conversion from maildir to mbox</li> </ul>				
Completed at 27/01/2014 except				
1. LDAP schema				
2. conversion from maildir to mbox				
which is postponed for later due to urgency with IOLAOS.				

PHASE II: PRIMARY SMTP SET-UP (+20d total)				
+27d	THEANO	- Enable SMTP services	Checked	13/01/2014
		- Compile, install, configure Postfix as a relay #1	Checked	13/01/2014
		- relay SMTP traffic to IOLAOS, NIREAS	Due to problems with IOLAOS, GORGO was set up to replace it (see below) and relaying is to GORGO. Note: 1) relaying is done on internally destined traffic, other traffic is sent to its destination 2) TLS v.1 (STARTTLS) has been enabled also for SMTP auth. 3) Relaying is done using the LMTP protocol	13/01/2014
		- install, configure AMAVISD to do CLAMAV, SPAMASSASSIN scans		OK
+32d	GORGO	- enable SMTP services	Checked	13/01/2014
		- compile install, configure Postfix as SMTP Internal back end #1	Checked	13/01/2014
		** enable Dovecot LDA/LMTP (required for delivery to message store by Postfix) – change from PROCMAIL	Checked Note: 1) PROCMAIL is not enabled. Sieve installed but not verified. 2) aliases and virtual users (ex mailing lists need to be properly set up as per existing method)	13/01/2014 Checked 06/04/2014
			Sieve/Managesieve -Sieve installed - managesieve proxying from theano checked - clients enabled ** further configuration and tuning possible with sieve plug ins etc	16/01/2014
		- add new MX record with higher priority than NIREAS	added MX weight 300 for theano which is the lowest priority. This should be changes eventually.	17/01/2014
			MX for theano (mail3) now 150 (between IOLAOS and NIREAS).	06/02/2014
+34d	NIREAS	- Demote NIREAS MX record to least priority  ** MX priorities are now GORGO- THEANO, IOLAOS, NIREAS	theano 100 iolaos 100 nireas 200	11/02/2014
+36d	DNS	Mail-out.cs.ucy.ac.cy this should be obsoleted eventually and just use mail.cs.ucy.ac.cy which should point to theano, elysso.		

+40d	THEANO	- reconfigure to relay to IOLAOS, GORGO	This was changed at +7d to bypass IOLAOS	27/01/2014
<b>MILESTONE #2</b> <b>Test all above</b> <b>- at this stage we have a complete system (IMAP/SMTP services) except the fault tolerant part</b> - complete functionality testing is done here. <ul style="list-style-type: none"> <li>- SMTP delivery</li> <li>- IMAP proxying</li> <li>- IMAP and SMTP back ends</li> <li>- sieve/managesieve (including proxying)</li> <li>- LDAP schema working</li> <li>- auxiliary systems (quota, sieve)</li> </ul> <b>- begin writing the user manual</b>				
<b>PHASE III: SECONDARY IMAP SET-UP (+15d total)</b>				
+43d	ELYSSO	- Install and secure OS with all already standard methods (Linux install and security in wiki - iptables, fail2ban, secure, firewall - check further the VLAN security	Checked  This should be revisited on the final check-out and in line with future DMZ mods.	28/01/2014
+45d	ELYSSO	- compile and install dovecot - configure IMAP proxy #2 to GORGO/IOLAOS based on user/group (50/50).	Checked  mirto has also been set up to which proxying is done	21/02/2014
+50d	MIRTO	- Install and secure OS with all already standard methods (Linux install and security in wiki - iptables, fail2ban, secure, firewall - check further the VLAN security	Checked  This should be revisited on the final check-out and in line with future DMZ mods.	21/02/2014
+52d	MIRTO	- compile and install Dovecot 2.2.x - Dovecot configuration as back end #2 - enable LDAP authentication  - install the Sieve extension  - install/enable IMAP quota	Checked Checked  * authentication is via SSSD/PAM to LDAP  * sieve and managesieve installed  Checked  ** static proxying ** This should be changed when the whole system is in operation	07/03/2014
+55d	IOLAOS	- expire IOLAOS/IMAP  - reconfigure THEANO, ELYSSO to proxy to the new IMAP back ends #1 #2 (GORGO, MIRTO)	Checked  See temporary arrangement 5 below	07/03/2014
+55d	DNS	- mail.cs.ucy.ac.cy should now point to theano.cs.ucy.ac.cy and elyso.cs.ucy.ac.cy  - MX records should remain as is (GORGO, IOLAOS, NIREAS) theano, elyso, nireas	Postponed  Checked	18/06/2014  02/04/2014
<b>PHASE IV: SECONDARY SMTP SET-UP (+15d total)</b>				

+57d	ELYSSO	<ul style="list-style-type: none"> <li>- SMTP External Relay #2</li> <li>- Enable SMTP services</li> <li>- Compile, install, configure Postfix as a relay #2</li> <li>- relay SMTP traffic to GORGO, IOLAOS</li> <li>- install, configure AMAVISD to do CLAMAV, SPAMASSASSIN scans</li> </ul>	<p>Checked</p> <p>Checked.</p> <p>IOLAOS not used. Relaying to GORGO only.</p> <p>Checked.</p>	11/02/2014
+60d	MIRTO	<ul style="list-style-type: none"> <li>- Internal Back end #2</li> <li>- enable SMTP services</li> <li>- compile install, configure Postfix as SMTP Internal back end #2</li> <li>- ** enable Dovecot LDA/LMTP (required for delivery to message store by Postfix) – change from PROCMAIL</li> </ul>	<p>Checked</p> <p>Checked</p> <p>Checked</p> <p>Checked</p> <p>See also notes at +32d for gorgo</p>	07/03/2014
+65d	DNS	- add new MX record for MIRTO elyso	Checked	07/03/2014
		- MX records now: GORGO, MIRTO, IOLAOS theano, elyso, nireas	Checked	07/03/2014
		- remove NIREAS MX record	Postponed	28/07/2014
		<b>(NIREAS now dead!!)</b> - mail-out.cs.ucy.ac.cy (???)	<p>Postponed</p> <p><b>It was decided at this stage that the names and aliases system needed a major upgrading subproject. See the ADDENDUM.</b></p> <p><b>Only after the completion of this critical subproject we will proceed with completing the pending tasks.</b></p>	05/05/2014
+70d	THEANO	- reconfigure to SMTP relay to GORGO, MIRTO	Checked. See also temporary arrangement #5 below.	02/04/2014
<b>PHASE V: NewFiler and MDBOX change (+10d)</b>				
+75d	GORGO MIRTO	<ul style="list-style-type: none"> <li>- Dovecot dynamic synchronization (DSYNC)</li> <li>- test manual synchronization for proper operation (from</li> <li>- set up DSYNC for on line synchronization (</li> </ul>	Postponed	
+78d	GORGO MIRTO	- make use of newfiler instead and in addition to of hermes NFS		
+80d	DNS	- remove MX record for IOLAOS (ioloas now dead for email)	Checked	07/03/2014
<b>PHASE VI: Additional Work – Tuning (+10d)</b>				
+83d		Postfix Policyd		

+85d		Mailing list management		
+88d		Dovecot mail alt feature		
+90d		SPAM config with outside SPAM DBs	checked	28/07/2014
+91d		User manual		
+92d		Dovecot deduplication		

RC = Roundcube

### Temporary Arrangements

1. In order enable delivery to aliases/groups/lists the current set-up of /etc/mailaliases was transferred to gorgo/mirto. This enables us to check other aspects of the system before setting up new systems like LDAP for this. This will be changed once a final decision is made on how to reconfigure this part. (rsync from nireas) (16/01/2014).
2. overquota.users installed on SMTP relays (theano, elyso) to block mail to overquota user. This needs to be improved to allow for temporary overquota. (Dovecot policies). (17/02/2014)
3. On nireas: there is a script (sendfile) that is used by crontab to send the overquota users file to theano, elyso every hour. (25/02/2014)  
  
There is also a sendmailaliases file that sende the /etc/aliases data on nireas and /etc/mailalaises directory to gorgo, mirto
4. On nireas relayhost=[mail3.cs.ucy.ac.cy] which means ALL email destined to locations OTHER than cs.ucy.a.ccy goes to theano (mail3) first for relaying. This is an interim arrangement before complete nireas shutdown.
5. Related to #4: Also all email destined to cs.ucy.ac.cy is forwarded to mail3 via the transport method. (20/03//2014)
6. As temporary arrangement that helps the debug phase: systems are kept in couples (theano/gorgo, elyso/mirto) ie theano will relay and proxy to gorgo, elyso will relay and proxy to mirto. Eventually this should be improved so that it will be possible for any front-end to use any of the back end systems both in relay and in IMAP/managesieve proxying. (07/03/2014)

## Appendix B: Bugs, Unresolved issues, Additional work

This catalogs issues and bugs (of lesser importance than the actual project) that need to be resolved. It also catalogs additional work that SHOULD be considered after the main project is seriously brought on-line.

No.	Date	Issue	Notes	Resolved
001	13/01/2014	Theano - postfix (2.10) does not stop/start properly on reboot – not in chkconfig --list		31/01/2014
002	13/01/2014	Jan 13 16:32:07 theano postfix/tlsmgr[4179]: warning: request to update table btree:/var/spool/postfix/smtpd_tls_cache in non-postfix directory /var/spool/postfix Jan 13 16:32:07 theano postfix/tlsmgr[4179]: warning: redirecting the request to postfix-owned data_directory /usr/local/var/lib/postfix		18/06/2014
003	13/01/2014	11117561 3069 Mon Jan 13 17:35:26 andreas.kasenides@cs.ucy.ac.cy (host gorgo.in.cs.ucy.ac.cy[10.16.1.113] said: 550 5.1.1 <junkone@cs.ucy.ac.cy>: Recipient address rejected: User unknown in local recipient table (in reply to RCPT TO command))  junkone@cs.ucy.ac.cy	Fix relays (theano) so that they do not accept/forward mail for non existent users.  Related to 023	
004	16/01/2014	/usr/local/etc/postfix/bounce.cf should be fixed on internal servers to not advertise *.in.cs.ucy.ac.cy systems when bouncing non-deliverable messages ** should we also examine the bounce system also		
005	20/01/2014	Jan 20 03:38:35 theano postfix/smtpd[25502]: warning: dict_nis_init: NIS domain name not set - NIS lookups disabled	??	
006	24/01/2014	Should we create a separate filesystem (LV) for /var/spool/amavis? This is used as a quarantine space and potentially can be overflown with the result of the OS becoming unavailable (filling /var)		
007	28/01/2014	Fine tune iptables. Ssh should be allowed only from some hosts (/etc/hosts.allowed etc)		
008	30/01/2014	Jan 30 10:29:01 theano dovecot: imap-login: Debug: Ignoring unknown passdb extra field: nopassword Jan 30 10:29:01 theano dovecot: imap-login: Invalid certificate: self signed certificate: /OU=Computer Science Department/CN=mail.cs.ucy.ac.cy/emailAddress=postmaster@cs.ucy.ac.cy		
009	31/01/2014	Protection of internal mailing lists	/usr/local/etc/postfix/access	

			needs to be checked again and fine tuned	
010	31/01/2014	With Postfix >2.10 there is also smtpd_relay_restrictions in addition to smtpd_recipient_restrictions. Since theono/elysso are actually relays we need to look at this change more carefully		
011	09/02/2014	Currently over quota rejection happens at the back end systems (gorgo, mirto with overquota.users) which is not ideal. This can be improved by rejecting at the relay instead. Makes no sense to accept message for user just to find out at the back end that he/she is over quota. See <a href="http://sys4.de/en/blog/2013/04/08/postfix-do-vecot-mailbox-quota/">http://sys4.de/en/blog/2013/04/08/postfix-do-vecot-mailbox-quota/</a>		
012	11/02/2014	Consider nullmailer to replace postfix set up on machines doing send only.		
013	19/02/2014	1. Investigate further the permissions on the control and index directories of Dovecot in /sys-data/dovecot in our case. Seems to be a problem with 707 permissions for it to work. 2. Also check permissions for log files. Seems to be a problem there too.		
014	27/02/2014	If we do Dovecot/Director and the user gets directed to a different server then there is a problem with the subscriptions file since currently CONTROL:/sys-data/dovecot and the subscriptions are local. 1) should we change locations of subscriptions to \$HOME? PROBLEM: What happens to over quota users in this case? 2) synchronize CONTROL with dsync? 3)What happens with mbox message storage		
015	27/02/2014	Need to check the correct permissions for Dovecot CONTROL directories {control, indexes}		
016	02/04/2014	Issues with names and aliases: In order for the system to work well ie to reject messages during the SMTP session to non-existent users or over quota users external relays need access to the users DB ie LDAP. Not a very good idea for external systems (this is related to #011 above).		
017	07/04/2014	Related to #016, #011. Aliases, groups, lists etc is a major problem from the old system since, essentially the same practice of aliases, is defined in	Needs to be fixed before proceeding to defining LDAP procedures for aliases.	



		various places: /etc/aliases, /etc/mailaliases, /etc/postfix/virtual-users. This needs to be fixed.		
018	07/04/2014	/Mail/common/Mail/scripts/cleanup-Mail running on hermes. This needs to be transferred to the mail servers (back-end) and be updated.		
019	12/05/2014	There are at least two cases producing backscatter: 1. Names, aliases, groups, lists and the quota system: It is necessary that the same front-end server resolve names (ex. <a href="mailto:grid@cs.ucy.ac.cy">grid@cs.ucy.ac.cy</a> resolves to several names) and check for quota since as is a currently setup grid is resolved by gorgo while quota is checked by theano&gorgo with the result of <a href="mailto:grid@cs.ucy.ac.cy">grid@cs.ucy.ac.cy</a> passing through theano and then rejected by gorgo -> backscatter. This is related to the aliases,groups,lists set-up. 2. .forward – since .forward files are not visible by the front-end servers the resolution is done on back end and a possible non-delivery (ex. Overquota, wrong user) leads to a reject -> backscatter		
020	14/05/2014	Restarting sssd on gorg, mirto may create problems since during the restart any email that arrives may be returned with 550 User not found. Verify. Possible solutions: 1. stop postfix first 2. restart sssd 3. start postfix		
021	19/05/2014	Access Control: students etc should not have access to internal mailing lists like csall etc.		
022	22/05/2014	Logrotate seems to still have problems with Dovecot logs on gorgo, mirto		
023	22/05/2014	Is there a problem with the .forward mechanism when forwarding from one user to another that is banned/overquota etc. Check the flow of messages. This should not be a problem if transport->*.cs.ucy.ac.cy flows to theano/elysso The .forward problem: 1. message to a valid user ex. Grid 2. passes to back-ends for delivery 3. grid/.forward -> nstyl (nstyl not deliverable because of over quota) 4. gets stuck in queue 5 produces backscatter to the original sender (not grid)  TEMP: this has been fixed by for ex <code>\cspitsil,  "/usr/sbin/sendmail -oi -f <a href="mailto:cspitsil@cs.ucy.ac.cy">cspitsil@cs.ucy.ac.cy</a> <a href="mailto:cspitsil@cytanet.com.cy">cspitsil@cytanet.com.cy</a>"</code>		
024	22/05/2014	Starting and stopping of services on mail servers, especially back-ends.		

		<p>1. Is there a particular order</p> <p>2. what happens if sssd stops</p> <p>SOLUTIONS (maybe):</p> <p>1. interim – stop first all mail services (postfix, dovecot) before any other services.</p> <p>2. sssd should not be started on mail servers. Accounts should be accessed directly to LDAP or files ie with two servers.</p>		
025	22/05/2014	<p>Monitoring:</p> <p>1. How to check for SMTP receive ability of ALL servers.</p> <p>2. How to check for IMAP ability ie users are able to log into the machines and perform actual receive</p>	Theano, elysso	
026	26/06/2014	<p>Noticed that with Thunderbird if</p> <p>1. I delete a folder</p> <p>2. then I force director to proxy me to a different server (ex. From gorgo to mirto) I can see the deleted folder in read-only mode (grey)</p> <p>3. I can also deleted folders like CentOS^announce instead of the usual folder hierarchy.</p> <p>Need to Verify.</p>		
027	28/07/2014	<p>Planetlab machines are able to inject email to the system. This should be disabled at the net interface (DMZ)</p>	<p>Disabled in access.db for now</p> <p>Also in IPTABLES for theano, elysso</p>	
028	28/07/2014	<p>On theano:/usr/local/etc/postfix/main.cf</p> <p>smtpd_sasl = inet: gorgo.....:12345</p> <p>should change to 10001 as with elysso</p>		
029	04/09/2014	<p>Roundcube -&gt;theano, smtp-&gt;\$mydomain</p> <p>Horde -&gt; mail.cs, smtp -&gt;\$mydomain</p> <p>Should these stay like this?</p>		

## ADDENDUM on names, groups, aliases

This section describes the steps in upgrade our approach to user names, groups and aliases. It was decided mid-project that this diversion was necessary to create the basis for the final target which is to move most of operation to LDAP.

It is understood that:

- there are LDAP based groups (ex. CSALL) that need to move to the new system
- there are file based groups (temporary or small number of users)
- there are MAILMAN bases mailing lists (groups)
- there are aliases to users of at least two different forms for each user

Preliminary decisions:

1. CS users have:
  - a regular user name (given by LDAP creation of the account – we do not have users that receive only mail and are not on the systems)
  - have an alias of the form <lastname.firstname>@cs.ucy.ac.cy
  - have an additional alias of the user's choice provided no conflict exists
  - \*\*\* most users also have an alias of the form <lastname.firstname>@ucy.ac.cy which DOES NOT involve our mail systems
2. It was decided that the procedures of creating groups and aliases on nireas will see an overhaul first to create a file basis before going to LDAP
3. The overhauled files will be used on the new systems as an intermediate step
4. Last step will be moving the files-based system to LDAP as much as possible.

What the changes involve:

- [<lastname.firstname>@cs.ucy.ac.cy](mailto:<lastname.firstname>@cs.ucy.ac.cy) 
  - make virtual-user\_access obsolete – there is no reason to allow users beyond the dept. To have (essentially) a virtual account on CS domain of the form remoteuser@cs.ucy.ac.cy.

### Files based plan (intermediate solution to LDAP final)

On front end systems:

- On front end systems (thano, mirto) there are no local users on the system (no LDAP configuration)
- /etc/aliases used only for OS users, so it is static and does not need to change
- /usr/local/etc/postfix/access - reject/permit (also individual users)
- UCY-virtual-users - UCY aliases as forwarded to us from YPS.

These names are created by YPS and are given to us by them and follow the official way of creating aliases.

- CS-virtual-users - CS aliases as defined by us
- CS-mailing-lists - CS custom mailing lists
- CS-mailman-lists - CS mailing lists (mailman)

### On back-end systems:

XX

### Names and Aliases Subproject

No.	Date	Issue	Notes	Resolved
001	21/07/2014	Clean up of all files on nireas as described above such that each file contains appropriate and unique names/aliases		28/07/2014
002	21/07/2014	Enable cleaned files on new system (transfer by cron for now)		28/07/2014
003	28/07/2014	Enable simple LDAP aliases (a one to one correspondence and one to many for one level groups) to work along the files based ones	Checked OK. LDAP now configured as a <u>secondary</u> options after traditional alias files. <b>STILL OPEN to become primary</b>	04/09/2014
004	28/09/2014	Transfer the /etc/aliases groups to LDAP		
005	28/07/2014	Enable group of groups (mutlilevel groups ex. Alumni -> alumni01 -> <users>		
006				