



# TurboMail 电子邮件系统

TurboMail® SYSTEM SOLUTION

## 系统解决方案

龙源电力集团股份有限公司

(Linux平台3000用户适用)

广州拓波软件科技有限公司

电话：020-38921969 38395469 85509396

传真：020-38921969

地址：广州市天河区天河路242号丰兴广场B座1906

网址：[www.turbomail.org](http://www.turbomail.org)



## 目录

拓波软件科技有限公司简介 .....	- 6 -
资质证书 .....	- 7 -
设计篇 .....	- 8 -
一. 硬件配置 .....	- 8 -
二. 服务器部署 .....	- 10 -
2.1 单台服务器部署 .....	- 10 -
2.2 双机热备方案部署 .....	- 10 -
2.3 内网外网隔离部署 .....	- 14 -
2.4 辅助说明 .....	- 14 -
三. 高级中继解决方案 .....	- 16 -
四. 系统稳定安全方案 .....	- 19 -
五. 邮件管理全局方案 .....	- 24 -
5.1 邮件监控 .....	- 24 -
5.2 邮件审核 .....	- 26 -
5.3 邮件跟踪 .....	- 30 -
5.4 邮件归档 .....	- 30 -
六. 设计构架 .....	- 39 -
6.1 底层坚固、高度稳定 .....	- 40 -
6.2 容易管理、维护 .....	- 40 -
6.3 增加设备简单、有效 .....	- 40 -



6.4 多级权限管理，支持企业全面发展.....	41
6.5 高度模块化，模块之间最小耦合.....	41
6.6 提供与其它系统直接的接口 .....	41
6.7 应用层二次开发、部署简单方便.....	42
七. 系统安全 .....	43
7.1 邮件系统核心安全设计 .....	43
7.2 数字签名和传输数据加密 .....	43
7.3 易于管理、配置 .....	44
7.4 其它技术优势 .....	45
八. 邮件备份及恢复 .....	46
九. 带宽评估 .....	46
十. 存储硬件配置 .....	47
产品篇 .....	49
一. 产品优势介绍 .....	49
二. 技术架构 .....	51
2.1 九层反垃圾引擎 .....	52
2.2 内嵌杀毒引擎 .....	56
2.3 模块化、高扩展性 .....	57
2.4 邮件全文检索 .....	58
2.5 最小内核技术 .....	58
2.6 多线程远程投递 .....	58



2.7 支持多种操作系统 .....	58
2.8 支持主流标准协议 .....	58
2.9 支持主流数据库 .....	58
2.10 分布式并行处理 .....	59
2.11 独立队列处理 .....	59
2.12 前端系统与 MTA 系统隔离 .....	59
2.13 集群高速管理认证技术 .....	59
2.14 抗灾难能力和恢复技术 .....	59
2.15 智能邮件安全管理技术 .....	60
2.16 大容量 .....	60
2.17 高速度 .....	60
三. Turbomail 功能模块.....	61
3.1 普通用户功能 .....	61
3.2 域管理员功能 .....	62
3.3 后台管理员功能 .....	68
<b>培训篇</b> .....	131
一. 系统管理员培训 .....	131
二. 操作培训 .....	132
<b>服务篇</b> .....	136
一. 服务承诺 .....	136
二. 服务支持体系的构成 .....	136



拓波软件-企业通信系统专业研发商  
TurboMail-电子邮件专家

2.1 电话支持中心 .....	- 136 -
2.2 定期巡查服务 .....	- 136 -
三. 故障等级设定 .....	- 137 -



## 拓波软件科技有限公司简介

广州拓波软件科技有限公司的前身 TurboMail 工作室成立于 2002 年，是专业研发电子邮件系统、企业即时通讯和短信平台的组织机构。经过三年的研发，在 2005 年，TurboMail 工作室正式发布 1.0.2 版本 TurboMail 邮件服务器软件，并成为国内最大的邮件服务器软件 OEM 开发商，为国内知名的邮件系统供应商提供产品。2007 年 TurboMail 工作室正式转为实体公司，正式开展自主品牌 TurboMail 的销售。

广州拓波软件科技有限公司的创始团队来自华南理工大学，依托华南理工大学的优势，聚集了一群软件开发高级人才专注于企业通信相关软件产品的研发。公司视产品性能，功能和服务为自己的生命，秉承“行胜于言”的所训以及“技术服务社会”企业理念，以 100%客户满意度为产品合格标准，坚持实施自主创新战略、品牌战略和产学研一体化战略，实现企业的可持续发展，为打造一流的科技企业而努力。

公司拳头产品 TurboMail 邮件服务器在中国国内企业用户群中享有盛誉。经过八年的发展与积累，TurboMail 已经拥有超过 1000 家忠实的客户，客户们的鼎力支持，鞭策着拓波不断升级技术和完善产品。

客户的需求是拓波的发展动力，拓波始终以客户的需求为根本出发点，用扎实的技术实力解决企业客户有关邮件的一切问题和达成企业用户对邮件方面的各种功能需求。TurboMail 以开放的技术架构，在国内整合了几十家二次开发伙伴，为各行各业客户提供个性化需求。

邮件是一个古老而又永恒的互联网基本功能，拓波已积累的数百家邮件系统架设案例的经验，能为客户未雨绸缪的处理许多潜在问题，解除用户未知的烦恼，使得邮件系统成为企业通信真正核心。

**TurboMail 以技术研发为根本，以客户需求为源泉，以服务支持为保障**



资质证书





## 设计篇

### 一. 硬件配置

服务器功能指标:

网络层功能	<ol style="list-style-type: none"><li>1. 网络地址阻断: 控制特定的地址、端口</li><li>2. 最大连接数控制</li><li>3. 最大连接频率控制</li><li>4. 邮件路由控制</li></ol>
协议层功能	<ol style="list-style-type: none"><li>1. 支持协议: pop2、pop3、sdps、imap、apop</li><li>2. 邮件发送数量控制</li><li>3. 指定邮件监控</li><li>4. 邮件转发控制 (smtp relay)</li></ol>
应用层功能	<ol style="list-style-type: none"><li>1. 同步频率设置</li><li>2. 邮件备份</li><li>3. 多域同步</li><li>4. 信头重写</li><li>5. 公共邮箱</li><li>6. 邮件过滤插件</li></ol>



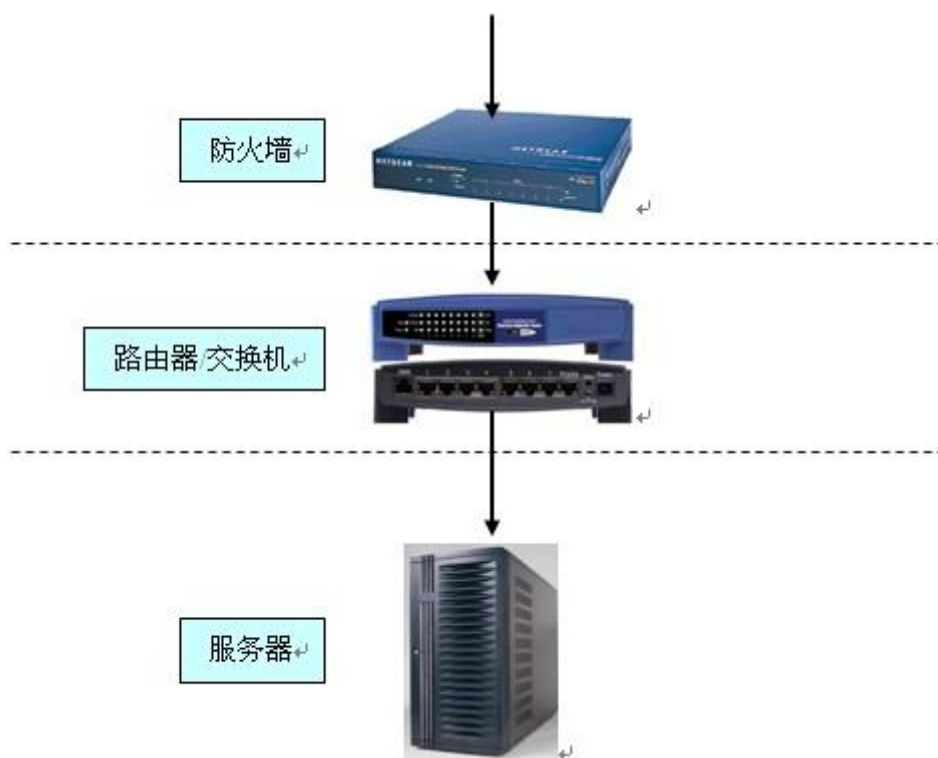


操作系统	Windows 各版本、Linux 各版本、freebsd、Solaris、Aix、HP-UX
硬件配置	CPU: 英特尔至强四核处理器, 2.83GHz x 2 内存: 4G 硬盘: 2.5T 网卡: 1 块千兆网卡
应用软件	Turbomail 企业版 V4.3.0

## 二. 服务器部署

以下是三种常见的部署方案。根据“龙源电力集团股份有限公司”的实际使用要求，我们建议采用双机热备的方案进行部署搭建，保证 7x24 小时的系统稳定运行。

### 2.1 单台服务器部署

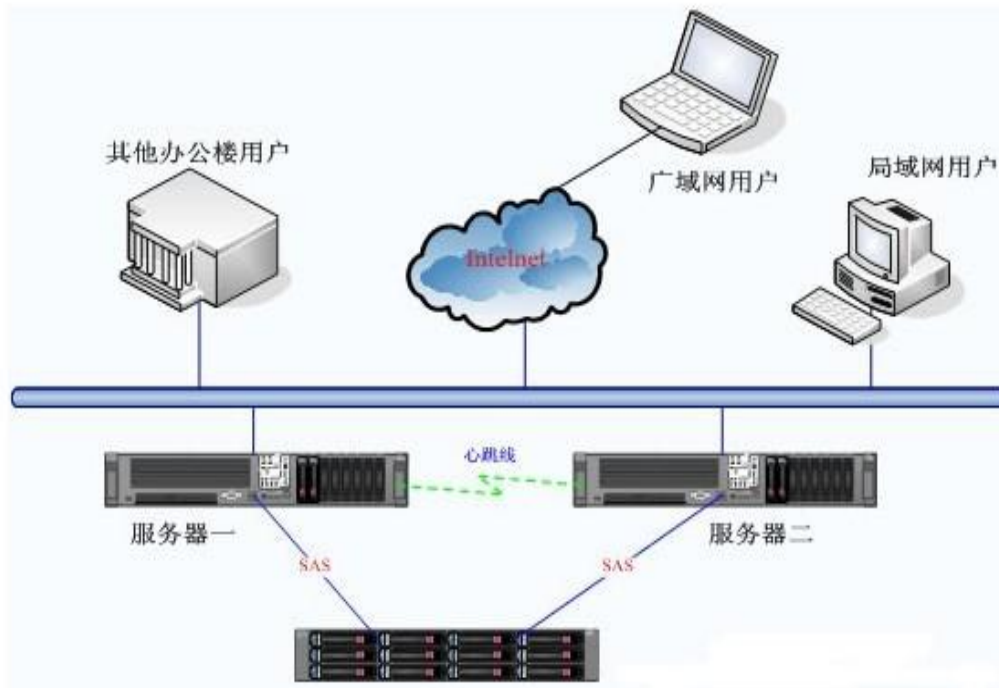


### 2.2 双机热备方案部署

双机热备针对的是服务器的临时故障所做的一种备份技术，通过双机热备，来避免长时间的服务中断，保证系统长期、可靠的服务。以前，企业为了避免服务器故障产生数据丢失等现象，会利用 RAID 技术和数据备份技术。但是数据备份只能解决系统出现问题后的恢复。我们知道，无论是硬件还是软件问题，都会造成邮件服务的中断，而 RAID 及数据备份技术恰恰就不能解决避免服务中断的问题。

要恢复服务器，再轻微的问题或者强悍的技术支持，服务器都要中断一段时间，对于一些需要随时实时的用户而言，丢失邮件就等于丢失金钱，损失可大可小，这类用户是很难忍受服务中断的。因此，就需要通过双机热备，来避免服务中断，保证系统长期、可靠的服务。

## 1) 基于共享存储设备的双机热备



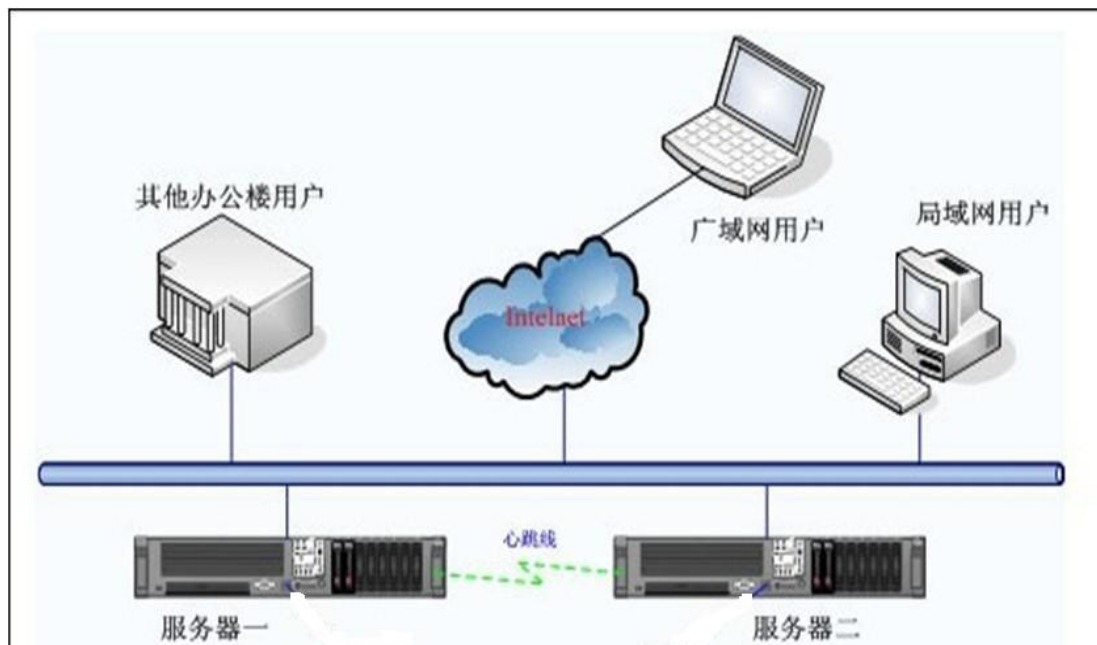
基于存储共享的双机热备是双机热备中最标准方案。对于这种方式，采用两台服务器（邮件系统同时运行在两台服务器上），使用共享的存储设备磁盘阵列（邮件系统的数据都存放在该磁盘阵列中）。两台服务器可以采用互备、主从、并行等不同的方式。在工作过程中，两台服务器将以一个虚拟的 IP 地址对外提供服务，依工作方式的不同，将服务请求发送给其中一台服务器承担。同时，服务器通过心跳线(目前往往采用建立私有网络的方式)侦测另一台服务器的工作状况。当一台服务器出现故障时，另一台服务器根据心跳侦测的情况做出判断，并进行切换，接管服务。对于用户而言，这一过程是全自动的，在很短时间内完成，从而对业务不会造成影响。由于使用共享的存储设备，因此两台服务器使用的实际上是一样的数据，由双机或集群软件对其进行管理。

**优点：**对于共享方式，数据库放在共享的存储设备上。当一台服务器提供服务时，直接在存储设备上读写。

而当系统切换后，另一台服务器也同样读取该存储设备上的数据。它可以在无人值守的情况下提供快速的切换，保证不会有数据丢失现象。

**缺点：**增加了存储设备的投资，对于有实力的企业，可优先考虑该方式。

## 2) 基于软件管理的双机热备



纯软件的方式，通过镜像软件，将数据可以实时复制到另一台服务器上，这样同样的数据就在两台服务器上各存在一份，如果一台服务器出现故障，可以及时切换到另一台服务器。

### 优点：

- ① 节约投资。
- ② 不受距离的限制：两台服务器不需受 SCSI 电缆的长度限制（光纤通道的磁盘阵列也不受距离限制，但投资会大得多）。这样，可以更灵活地部署服务器，包括通过物理位置的距离来提高安全性。

### 缺点：

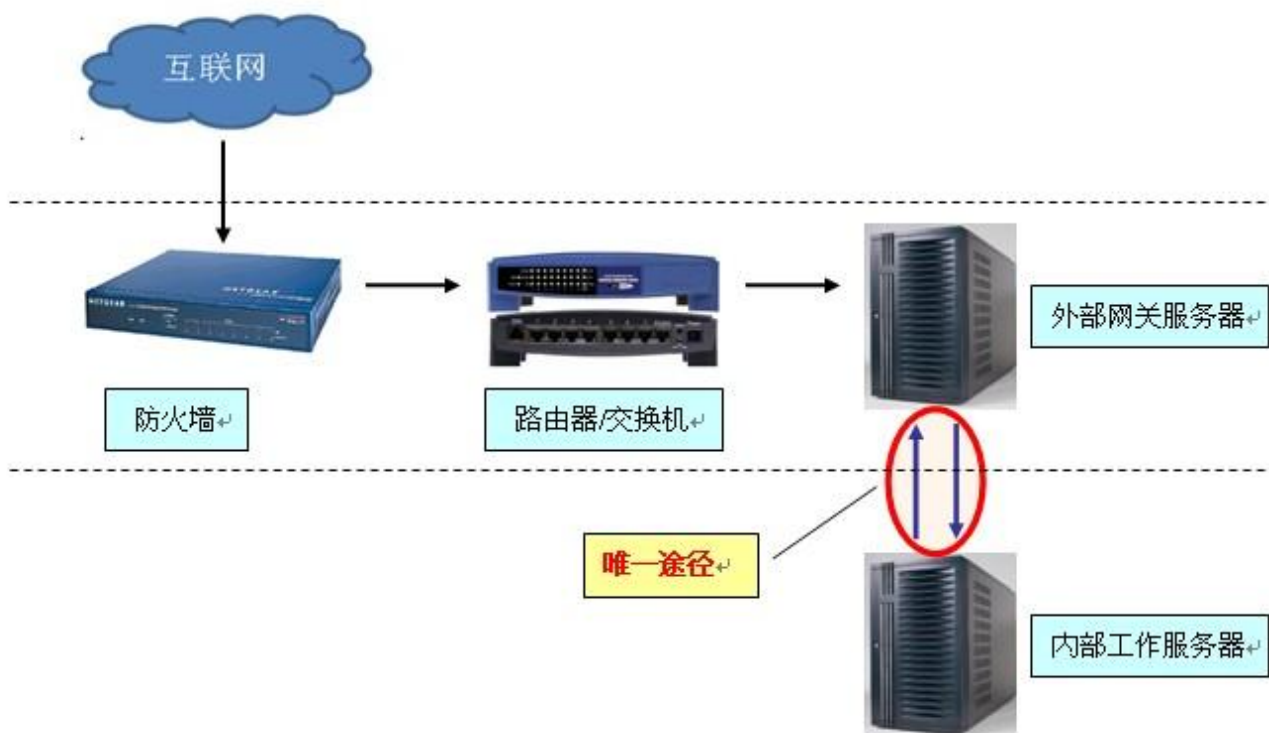
- ① 可靠性相对较差，两服务器间的数据实时复制是一个比较脆弱的环节。
- ② 一旦某台服务器出现中断，恢复后还要进行比较复杂的数据同步恢复。并且，这个时段系统处于无保护状态。
- ③ 没有事务机制，由于其复制是在文件和磁盘层进行的，复制是否成功不会影响数据库事务操作，因此有出现数据不完整变化的情况，这个存在着相当的风险。



软件存在在维护和未知 BUG 等因素，所以我们并不建议客户采取这种方式进行双机热备。目前 Turbomail 的客户中需要采用双机热备的使用者绝大多数都是利用“磁盘阵列”这种基于共享存储设备的方式，而且截止现在，尚未发现报修或者需要维护的情况。

## 2.3 内网外网隔离部署

随着网络技术和因特网技术的成熟和高速发展，电子邮件已逐渐成为最受网民青睐的一种交流方式，越来越多的企事业单位开始组建属于自己的邮件服务器。同时，为了保证邮件数据的安全性，杜绝外网病毒的攻击，很多企业都会加用防火墙。但大家都知道，防火墙不是万能的，黑客可多种手段绕过防火墙的阻挡，侵入内网窃取数据或破坏数据，以致损失惨重。针对要求高安全性的客户，就可以考虑使用内外网物理隔离的方案来组建邮件系统。



“内/外网隔离部署方案”的主要特点如下：

- 内部服务器与外部环境实行隔离，从逻辑层面就保证了系统运营的安全性。
- 外部网关服务器作为内部与外部进行邮件数据沟通的唯一途径，可控性极高。
- 网络攻击只能前进到外部网关服务器，无法入侵内部工作服务器。如外部服务器因病毒等原因出现故障，则内外网之间的通讯终止，有效保护工作系统的正常运营。
- 所有的数据信息均保存在内部工作服务器，所以，网络攻击/人为/或自然灾害等因素导致外部网关服务器失效，都不会损害或影响用户的各种数据信息，保证零数据丢失。



拓波软件-企业通信系统专业研发商  
TurboMail-电子邮件专家

- 外部服务器上部署的 Turbomail 软件网关实现反病毒/反垃圾功能，并司职邮件监控、邮件跟踪等邮件管理模块，与内网系统有效组合，双管其下。
- 外部服务器软件系统与内部服务器软件系统均由拓波公司自主研发，在设计每个环节就保证系统的集成性，这一点是其他任何一款邮件系统软件都无法比拟。



### 三. 高级中继解决方案

近年来，广大用户对邮件系统的反馈，出现最多的抱怨就是与大型的邮件服务提供商，特别是国外的，例如 hotmail、yahoo、sina 之间的通信障碍，经常无法将正常邮件发送出去给这些邮箱。甚至在中国国内，都经常会发生邮件投递失败的情况。究其原因主要是因为中国的垃圾邮件过度泛滥（如下图），大量的 IP 和邮箱域名进入了国际邮件组织的黑名单（如 Spamhaushuo、FortiGuard 等），中国用户发出的邮件被当成垃圾邮件被自动屏蔽。



邮件的顺利快速收发是一个邮件系统最基本和最重要的功能，邮件收发不顺严重影响着使用者的工作效率，是否保证通邮，是判断一套邮件系统是否可用的基本条件。Turbomail 始终将自己定位在专业的邮件系统研发供应机构，拆耗巨资在亚洲（香港）、欧洲（法国）、大洋洲（澳大利亚）、美洲（美国）分别设立了高级中转服务器。广州拓波软件科技有限公司在国际服务器设备的投入，以及国际邮件市场的战略定位，保证了 Turbomail 邮件系统的国际邮件收发。

除了上述的硬件资源对国际邮件的保障之外，我们的软件是依照如下思路配合中继服务器工作的。

1、邮件系统将首先对用户发出的邮件进行筛选分类，对不同类别的邮件使用不同的邮件中转服务，针对不同类型的邮件巧妙的利用不同的“可靠”的邮件系统帐号进行中转。

2、同时对所有中继邮箱进行排序，当使用第一个中继邮箱仍然无法成功投递后，系统自动转用下一个中继邮箱进行投递。全球网状的服务器布局，保证用户顺利的发送邮件。

3、下面呈现的是高级中继模块的部分截图，供阅览，更多优势细节请测试体验。





### 投递服务 红色参数表示该参数在服务器重启后才生效

系统设置 <==

最大投递线程数	<input type="text" value="25"/>	(最大值为1024, 小于或等于零表示使用默认值32)
投递尝试间隔时间	<input type="text" value="480"/>	秒 (小于或等于零表示使用默认值600)
最大投递尝试次数	<input type="text" value="16"/>	(小于或等于零表示使用默认值32)
投递间隔增加率	<input type="text" value="0"/>	(小于或等于零表示使用默认值16)
外发绑定IP	<input type="text"/>	
网络连接超时	<input type="text" value="0"/>	(小于或等于零表示使用默认值30)
投递失败是否转入用户Exception文件夹	<input type="checkbox"/>	
对中转邮件执行过滤规则	<input type="checkbox"/>	
记录发件会话明细	<input checked="" type="checkbox"/>	
HELO命令模式	<input type="text" value="使用各域设置helo域名"/>	

### 外发邮件中继设置

中继使用方式	<input type="text" value="当正常发送失败后, 使用中继"/>	
根据判断条件, 使用中继	<input checked="" type="checkbox"/>	
中继判断条件	<input type="text" value="中继判断条件列表"/>	
正常发送失败判断条件	<input type="text" value="正常发送失败判断条件列表"/>	
中继帐号列表	<input type="text" value="中继帐号列表"/>	
中继最大投递尝试次数	<input type="text" value="0"/>	小于或等于零表示使用默认值3
中继最大同时投递数	<input type="text" value="0"/>	小于或等于零表示不限制
<input type="button" value="保存"/> <input type="button" value="取消"/>		

### 编辑中继判断条件

中继判断条件类型	<input type="text" value="收件域"/>	
满足条件	<input type="text" value="hotmail.com"/>	(IP可有两种格式: 1. 单个ip地址, 2. 一个网段, IP/Mask, 如: 192.168.168.0/255.255.255.0)
<input type="button" value="保存"/> <input type="button" value="取消"/>		



**中继判断条件列表**

系统设置 <== 投递服务 <==

增加

中继判断条件类型	满足条件	删除
收件域	hotmail.com	
收件域	163.com	
收件域	sina.com	

#### 四. 系统稳定安全方案

Turbomail 系统支持多种杀毒引擎，并且内置著名的开源杀毒引擎 ClamAV，对邮件类病毒具有 99.9% 的杀灭能力，同时支持嵌入式杀毒和网关杀毒自动定时更新病毒特征库，用户可设置为每 3 小时自动在线升级。

自主研发的九层反垃圾邮件内嵌式引擎，根据不同垃圾邮件特点采用不同技术，综合分析垃圾邮件，同时为每种特征打上垃圾分值，根据综合评分判断是否为垃圾邮件，真正做到准确率高，误杀率低，垃圾邮件拦截率为 98% 以上。

Turbomail 系统同时支持发信认证 (smtp-auth)、黑名单和系统级垃圾邮件过滤功能，为用户邮箱提供三重保护功能。用户可以随时从国内外反垃圾邮件组织获得黑名单列表文件，导入邮件系统。从而使邮件管理员从被动变为主动。turbomail 系统黑名单功能支持模糊匹配，可以屏蔽一个域如 @usa.com，也可以只屏蔽域内的一个用户如 spam@usa.com。提供多种方式的垃圾邮件过滤功能，避免邮件服务器成为垃圾邮件中转站。



##### 第一层：网络控制层

经验分析，发送垃圾邮件的服务器一般都会同时大批量的向某些域的多个帐号发送垃圾邮件，对于这些发送垃圾邮件方式，可通过设定一定网络访问频率控制进行有效的阻隔，turbomail 提供了两种设置方式对付这种攻击，并可自动把发送垃圾邮件的 IP 归为垃圾 IP (SpamIP) 列表。

通过 smtp 服务层把明显的发送垃圾邮件的 smtp 连接拒绝，大大减轻后台投递系统和反垃圾引擎的负载。

通过统计分析，我们发现很多发送垃圾邮件的 smtp 连接具有以下特点。

1、同一 IP 同时的 smtp 连接数非常大。



2、同一 IP 一段时间，smtp 连接频率非常大。

一般出现这两种情况，都表示源发件人非常有可能发送垃圾邮件。

通过设置以下这两个参数可控制这类型的 smtp 连接，从而截断发送垃圾邮件的源头：

#### 1、系统设置—》SMTP 服务—》一分钟内同一 IP 允许访问次数

同时设置：

系统设置—》SMTP 服务—》启用智能反垃圾 IP 功能参数，把符合以上两个条件的 IP 地址自动加入系统的智能反垃圾 IP 列表中（SmartSpamIP），当以后系统碰到这些 IP 的连接的时候，直接拒绝。

可通过：

系统监控—》智能反垃圾 IP 列表

查看系统目前智能反垃圾 IP 列表

注意：

当互联网是经过反垃圾网关再接入邮件系统的情况，由于邮件系统的所有 smtp 连接都来自反垃圾网关，所以基于 SmtP 服务反垃圾不再起作用，这是需要把以上两个参数设为-1，以免系统 smtp 服务故障。

#### 第二层：来源分析

根据垃圾邮件发送者 IP 的地理位置，与 APNIC 的 IP 信息库核对结果，看来源是否真实，如果真实则通过，否则可能为可疑邮件，由于 IP 来源无法伪装，所以这个反垃圾策略比较有效。

#### 第三层：黑名单

通过黑名单，turbomail 系统设置屏蔽任何一个 IP，一个网段；也可以屏蔽任何一个发信人，一个域。

实时黑名单(RBL)主要通过利用互联网公开的 rbl 资源判断垃圾邮件的可能性。目前 RBL 一般都通过 DNS 查询的方式提供对某个 IP 或域名是否是垃圾邮件发送源的判断。另外，由于国外大多数 rbl 都对来自中国的 ip 有“歧视”，所以我们并不能完全依靠 rbl 来判断一封邮件是否是垃圾邮件，只能根据 rbl 查询结果判断邮件是否垃圾邮件的可能性。可设置以下参数定制 rbl：



RBL 服务器地址	<input type="text" value="xbl.spamhaus.org"/>
DNS 查询类型	<input type="text" value="A"/>
得分	<input type="text" value="3.0"/>
匹配表达式	<input type="text" value="127\.\d+\.\d+\.[45]"/>
描述	<input type="text"/>
<input type="button" value="保存"/> <input type="button" value="取消"/>	

RBL 服务器，指定 RBL 查询域名后缀。

DNS 查询类型，根据具体的 RBL 要求指定 DNS 查询记录类型。

匹配表达式，指定 RBL 查询结果的匹配模式，表达式格式采用 perl 正则表达式，如果为空，则表示如果可查到 RBL 结果，就表示符合条件。

目前所知比较有效的 RBL 服务器为：

xbl.spamhaus.org

bl.spamcop.net

cbl.anti-spam.org.cn

cdl.anti-spam.org.cn

#### 第四层：灰名单

灰名单技术源于：<http://www.greylisting.org/>。

灰名单技术其基本假设是：病毒和垃圾邮件，通常都是一次性的，如果遇到错误，不会重试。

一些发垃圾邮件的软件，这些软件基本上都不会对邮件服务器返回的错误做出任何重试，而只是简单的在日志里记录发送失败而已。而病毒引发的邮件风暴则更加不会识别邮件服务器返回的错误，因为这些病毒仅仅是简单的发送邮件，发送时根本不理睬服务器的状态。

Greylist 的设计大体上是基于一种重试的原则，即第一次看到某个 IP 要想给某个收件人发信，那么它将简单的返回一个临时错误（4xx），并拒绝此请求，正常的邮件服务器都会在一段时间内（如半小时）重发一次邮件。greylist 发现还是刚才同样的 ip 地址和收件人，认为此 ip 是来自合法服务器的，予以放行。如果是



非正常的邮件,那么或者将永远也不再进行重试,或者会疯狂重试,但由于间隔太近,而遭拒绝。因此,greylist 只要设置一个合适的放行间隔,就可以在很大程度上对这类垃圾邮件有着良好的免疫能力。greylist 的一大特点就是不会丢信,正规的邮件服务器认为 4xx 错误只是临时性、软性的错误,会隔一段时间重试,因此邮件还是可以投递成功。但 greylist 的一大缺点即使延迟 (delay),延迟从几分钟到几个小时不等。对于一些对邮件及时性很强的客户,greylist 可能不是一个很好的选择。

### 第五层: 趋势分析

趋势分析原理为,所有垃圾邮件都有目标指向,比如:卖药广告邮件都会在邮件内容里指定卖药的电话、邮件或网站,如果不指定这些信息,发送垃圾邮件也就没有意义了。趋势分析法就是通过分析邮件里的电话、邮件或网站链接内容,通过匹配判断他的指向从而判断邮件是否是垃圾邮件。

### 第六层: 邮件来源判断

主要通过分析邮件的来源,如:发件人 ip,发件人,发件域,等内容,来判断垃圾邮件的可能性。

### 第七层: SpamFilter 内容过滤

通过邮件内容关键字分析,可为符合内容分析结果的邮件打上相应的垃圾邮件评分。这类规则的判断条件类似系统的过滤规则。可参考过滤规则设定来设定过滤评分内容,同时我们也会通过收集客户反馈的垃圾邮件特点整理成规则内容,定期通知客户更新。

### 第八层: SpamAssassin 引擎

SpamAssassin 是一个由 Apache 开发的一个著名的反垃圾引擎,turbomail 邮件系统完整的集成了 SpamAssassin 反垃圾引擎。

邮件系统提供了一个名为 SA-Server 的 SpamAssassin 反垃圾服务器,邮件系统通过把需要进行反垃圾分析的邮件提交给 SA-Server 进行分析。

SA-Server 在 Windows 平台上可通过 SA\_Server 服务启动,在 Unix/Linux 平台上可通过 sa/sa\_server.sh 脚本启动。

SA-Server 默认端口为 8700,可通过直接修改 sa/sa\_server.pl 修改这个端口。

可通过邮件管理系统中的,反垃圾\反病毒一》反垃圾引擎设置 中的 SpamAssassin 中的相关设置进行



SA-Server 的服务配置。

其中：

启用 SpamAssassin ， 指定是否启动 SpamAssassin 反垃圾检查

SpamAssassin 服务器地址，指定 SA-Server 服务器地址，默认为本机。

SpamAssassin 服务端口，指定 SA-Server 服务器端口，默认为 8700。

最大 SpamAssassin 检查线程数，指定最大的连接 SA-Server 服务数，可根据系统的复杂进行适当调整。

### **第九层：TMspamcheck 引擎**

垃圾广告商总是在想方设法的绕开上述拦截与屏蔽方式，“作案”手段不时更改，Turbomail 通过定期巡查以及与客户建立沟通制度，广泛搜集现行的各类垃圾邮件，并逐个分析，将垃圾邮件源列入 TMchecklist，所有的正式客户都将得到同步更新的服务，再度查杀漏网之“邮”。



## 五. 邮件管理全局方案

### 5.1 邮件监控

为了防止单位的员工通过电子邮件方式，将企业的核心资料外泄出去，TurboMail 邮件服务器软件针对这一需求研发了严密又易用的邮件监控功能，有效的保证工作邮箱的安全使用，对意外情况进行先期预防。

**全面监控：**对所选邮箱的所有收件或者发件进行监控；

**条件监控：**根据发件人、收件人、主题、附件名、正文、收发时间、是否含附件等目标设置过滤条件，对满足条件的邮件进行监控。

**查找/删除邮件：**管理员或者域管理员根据邮件帐号、邮件主题、发件人、收件人、时间对本系统或本域的邮件进行搜索，从而执行删除工作。

这两个监控方式可以单独使用，也可以搭配起来使用。

一，对所选邮箱的所有收件或者发件进行监控

- 1，管理员登陆管理员帐号，选择邮件监控功能
- 2，选择发送邮件监控或者接收邮件监控，编辑监控邮箱
- 3，设置完毕，被监控邮箱的发件将全部备份到接受监控邮箱的收件箱内。

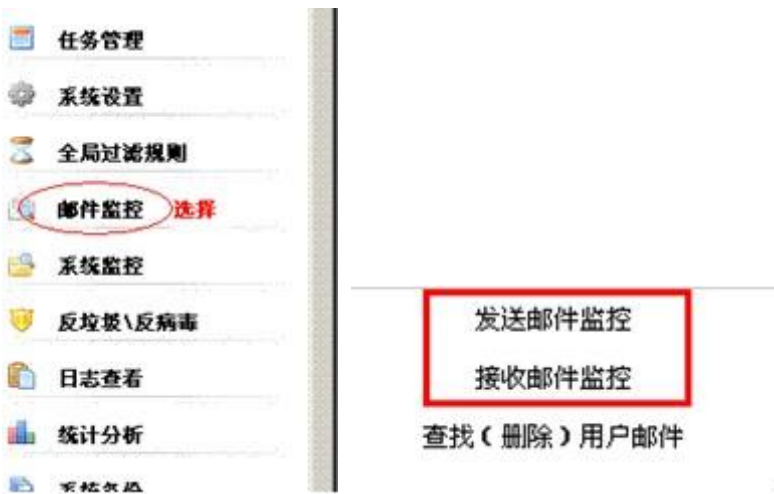
二，设置过滤条件，监控部分邮件

- 1，管理员登陆管理员帐号，选择全局过滤规则
- 2，选择接收过滤或者发送过滤
- 3，编辑过滤规则，设置监控邮箱

三，管理员或者域管理员对本系统或者本域下的用户的邮件进行搜索，删除邮件。

**部分截图：**





### 增加邮件监控

规则名称:

被监控发件人:  选择系统用户

(如有多个,可用分号分隔";")

接收监控邮件邮箱:

编辑过滤规则 (系统接收过滤规则)

启用该规则

规则名称:  输入过滤规则名称

到达的所有邮件

满足以下条件的邮件 (各条件为“与”关系)

**设置邮件监控的条件**

**规则设置**

发件人:   检查原编码

收件人:   检查原编码

主题:   检查原编码

附件名:  价格  检查原编码

内容:   检查原编码

其他邮件头字段1:    检查原编码

其他邮件头字段2:    检查原编码

\* 规则是否包含邮件头字段:

邮件长度:   字节

邮件发送时间: 

邮件接收时间: 

是否包含附件:

**执行操作**

不执行以后规则

拒绝接收

执行自定义动作

发送到

转发到其它邮箱  输入监控邮箱, 被监控的邮件将备份到该收件箱内

自动回复

## 5.2 邮件审核

系统管理员可以先行设置每项业务的审核邮箱，通常可以设置为一个部门的主管或者经理。比如销售经理可以对旗下所有销售员的进出邮件进行监控和审核，对订单信息确认无误后才允许发送或接收，保证业务信息的安全与准确。

- 系统管理员或者域管理员任意设立审核人与被审核人；
- 可根据发件人、收件人、主题、附件名、内容、邮件大小、邮件时间、是否含附件等条件做设定过滤条件，设置需要审核的邮件；
- 可以选择对接收邮件或者发出邮件进行审批；
- 可以对部门邮件和组织邮件进行群体审批；
- 审核人能收到待办审核的提醒，及时处理相关事项；

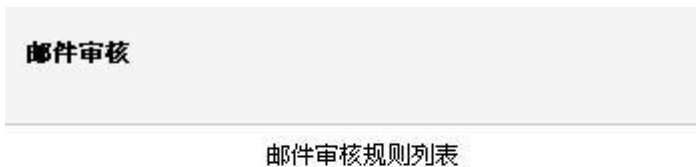


- 审核功能能与短信提醒和手机邮箱配合使用，保证紧急事情能够得到及时处理，降低隐性风险和损失；

通过灵活的审核功能，可以强化企业对员工邮箱的管理，进一步避免公司的机密信息外泄。

## 邮件审核功能的设置与使用

1、添加邮件审批帐号，进入管理员左边列表的邮件审核如下图：



2、点击“邮件审核规则列表”如下图：

规则名称	判断条件	审核人	修改日期	编辑	删除
接收邮件审核	to:ad@turbomail.org.cn	admin@turbomail.org.cn	2009-8-6 10:41:27		
发送邮件审核	from:user@turbomail.org.cn	admin@turbomail.org.cn	2009-8-6 10:46:30		

点击“增加”添加审核人地址和被审核人地址

**规则名称:** 接收邮件审核

启用该规则

到达的所有邮件

满足以下条件的邮件 (各条件为“与”关系)

来源IP:

收件人IP:

发件人:  发件人地址所发的邮件都会通过审核人发送后才发出去

收件人:  ad@turbomail.org.cn 输入接收邮件人地址发往此地址的邮件都会先到审核人邮箱等待审核之后才会收到

主题:

附件名:

内容:

字符集:

其他邮件头字段1:

其他邮件头字段2:

判断是否包含邮件头字段:

邮件长度:   字节

邮件发送时间:   
(时间格式: YYYY-MM-DD HH:mm:SS~YYYY-MM-DD HH:mm:SS)

邮件接收时间:   
(时间格式: YYYY-MM-DD HH:mm:SS~YYYY-MM-DD HH:mm:SS)

是否包含附件:

**审核人**  接收或发送审核通过些用户审核后能收到或发出

3、审核规则建好后，被审核人发送或接收邮件时，登录审核人邮箱，左边多出“待审批邮件”此功能，如有需要待办的审批邮件，将会得到提醒，并弹出提示框。





待审批邮件 (admin@turbomail.org.cn) 共4封邮件 第 1--4 封

全部选择

附件	选择	发件人	收件人	主题	日期	审批时间	长度(字节)
	<input type="checkbox"/>	user@turbomail.org	cnad@turbomail.org	nto ad <small>点击主题进行审批</small>	2009年08月06日 10:47:22		684
	<input type="checkbox"/>	user@turbomail.org	cnad@turbomail.org	接收邮件审核	2009年08月06日 10:45:13	2009年08月06日 10:46:03	906
	<input type="checkbox"/>	user@turbomail.org	cnad@turbomail.org	发送审核邮件	2009年08月06日 10:42:44	2009年08月06日 10:42:55	706
	<input type="checkbox"/>	user@turbomail.org	cnad@turbomail.org	邮件审核功能邮件	2009年08月06日 10:39:32	2009年08月06日 10:40:21	710

全部选择

4、点击主题进入内容查看内容是否通过，通过就击“审批”即可

**(已审批)**  
审批时间: 2009年08月06日 10:42:55

<< >>

发件人	"user" <user@turbomail.org.cn> [加入地址簿] [加入黑名单] [加入白名单]
收件人	<ad@turbomail.org.cn>
抄送	
日期	2009-8-6 10:42:44
主题	发送审核邮件
附件	

fafafa

经过审批的邮件，将会以收件人的邮箱作为目的地进行投递。

以上举例的是发送邮件的审核，同理，收取邮件的步骤也是要收件经过审核邮箱，一旦审核邮箱确认通过，最终收件人才能收取发件人投递过来的邮件。

邮件审核功能可以根据使用者的需要灵活配置，开启某些功能，关闭某些功能都是纯 Web 界面的简单操作，如果存在设置方面的疑问或有其他建议， 敬请联系拓波技术支持。



### 5.3 邮件跟踪

TurboMail 邮箱用户对发出的给其他邮箱的邮件，可以实时跟踪对方的收件情况。针对系统内的邮件，能跟踪到是否查看、何时查看、是否转发等等更详细的信息。

同时，为了便利用户使用此功能，在邮件跟踪模块，用户可以设置对邮件主题进行清晰或模糊查找；也可以设定开始时间和结束时间进行查找。

详细情况						
序号	时间	主题	收件人	目前状态	是否删除	详细情况
1	2009-3-16 10:40:40	TurboMail的邮件跟踪功能测试	a2	已回复	未删除	发送成功
2	2009-3-16 10:36:29	TurboMail的邮件跟踪功能测试	a2@a.com	未读	未删除	发送成功

### 5.4 邮件归档

邮件归档是指对邮件数据进行在线归档、分类管理、长期保留并允许实时搜索和访问，主要是针对海量数据的应用，是对数据进行有效的迁移和管理。数据的保存时限由用户自己决定，只要有足够的存储空间，任何的数据信息都可以永久保存。

Turbomail 邮件归档功能开启后，系统对所有进出邮件进行归档备份，任何一封被误删的邮件都能恢复到用户的邮箱。即使用户执行彻底删除，邮件仍已被备份，仍能轻松检索调出，邮件归档功能就像是一个持续运作的复印机，来往所有邮件全部被复印留底。归档同时并即时产生索引，一对一锁定目标性索引，节省用户空间。即使在突然断电的情况下，系统也能保全邮件数据。

部分截图：





归档邮件列表 共21封邮件 第 1--21 封

收件帐号: admin@turbomail.org.cn 日期: 至: (格式: 时间格式: YYYY-MM-DD) 内容: 搜索

全部选择

附件	选择	发件人	收件人	主题	归档类型	日期	长度(字节)
	<input type="checkbox"/>	admin@turbomail.org.cn	causer@turbomail.org.cn	邮件跟踪	发送	2009-7-31 14:44:12	0
	<input type="checkbox"/>	admin@turbomail.org.cn		邮件跟踪	接收	2009-7-31 14:44:12	0
	<input type="checkbox"/>	admin@turbomail.org.cn	causer@turbomail.org.cn	邮件跟踪	发送	2009-7-31 14:37:58	0
	<input type="checkbox"/>	admin@turbomail.org.cn		邮件跟踪	接收	2009-7-31 14:37:58	0



## 六. 数据迁移介绍说明

### 6.1 用户信息

导入说明:

Turbomail 支持文本格式用户数据导入, 文本格式用户数据要求如下:

1. 文件为文本文件, 并且是 GB2312 或者 GBK 编码格式保存。
2. 每行为一条用户记录, 记录之间用回车换行分隔
3. 每行记录为用户字段, 字段直接用空格或者 TAB 分隔, 顺序如下:

域 用户名 密码 最大空间 最多邮件数 昵称 单位 部门 地址 电话 手机 城市 省 邮编 国家

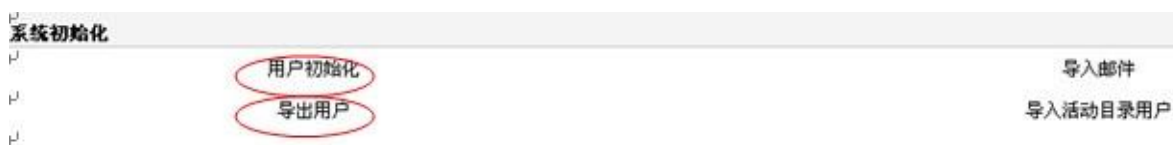
Test.com adm 888 102400 -1 王五 中国移动 研究院 天河路 85xxx 1390xxx 广州 广东 510000 中国

注意:

- 1) 邮箱大小为 K 字节表示。
- 2) 在导入用户之前, 请先创建域, 域空间大小、域用户默认邮箱大小应该适合导入的用户。
- 3) 昵称之后的用户信息为可选项, 可以不必导入。

导入操作步骤:

如果身份为“系统管理员”, 则进入“系统设置”点击“用户初始化”



如果身份为“域管理员”, 则进入“用户管理”点击“导入用户”





**用户管理** (分配用户数:无限制 分配空间:无限制M 已有用户数:12)

进入用户初始化界面

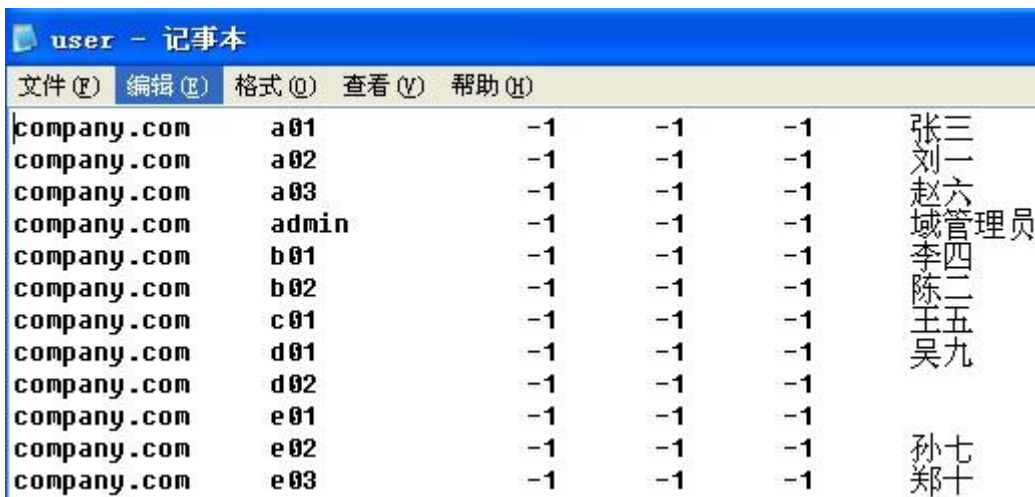
**用户初始化**

用户文件格式说明:  
1.文件为文本文件  
2.每行记录表示一用户记录  
3.用户记录格式:  
**域名 用户名 密码 最大空间 最多邮件数 网络硬盘空间 昵称**

编码:    当前用户文件:

序号	域	用户名	昵称	最大
----	---	-----	----	----

点击浏览，选择导入文件，注意为文本文件，每行记录表示一个用户，每个项目之间以空格隔开，如下：



先上传，接下来导入。

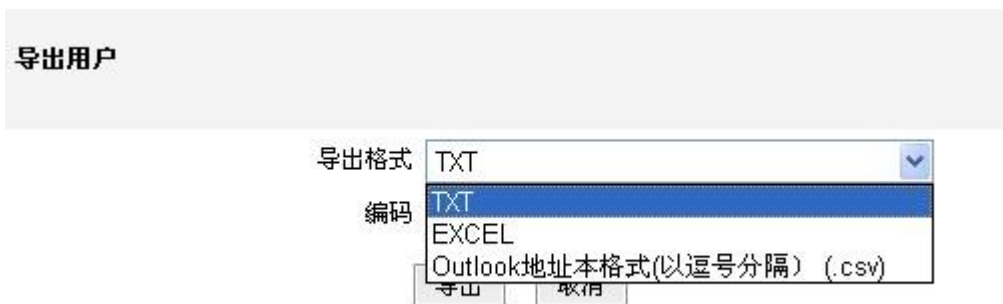


点击“确定”后，导入成功

序号	域	用户名	昵称	最大空间(K)	最多邮件数
1	company.com	sd1	张三	-1	-1
2	company.com	sd2	刘一	-1	-1
3	company.com	sd3	赵六	-1	-1
4	company.com	admin	域管理员	-1	-1
5	company.com		李四	-1	-1
6	company.com		陈二	-1	-1
7	company.com		王五	-1	-1
8	company.com		吴九	-1	-1
9	company.com	sd2		-1	-1
10	company.com	sd1		-1	-1



导出操作步骤：



选择用户导出的文件格式，可以为 txt、xls 或者 csv。

选择编码，可以为 GBK 或者 UFT-8。

点击导出，设置文件存放路径，确定即可。

## 6.2 邮件数据

Turbomail 邮件系统内的所有进出邮件及其数据均保存在“\turbomail\accounts”目录下，用户如需要做数据迁移，直接复制拷贝该目录即可。



### 导入邮件

系统设置 <==

原邮件系统类型

原邮件存储目录

默认域

需导入的用户

自动生成不存在的用户

自动生成用户的默认密码

可用以下三类格式:  
1. 为空,则表示导入所有用户邮件。  
2. 域名,表示导入指定域的用户。  
3. 用户邮件地址,表示导入特定的用户。

Turbomail 支持多种邮件系统邮件数据的导入。Qmail、Cyrus IMAP、Mdaemon、Sendmail、Oldmail、POP3、Vernal、Igenus、Foxmail、Iemail、Foundir、OldJD、Winmail、Cmail、Winwebmail、Formail、Postfix、RedhatMail、Archive、Redflag、春气香邮件服务器、方标邮件服务器、Exchange、Domino Lotus 格式邮件可以直接指定路径、指定域、指定用户导入。



Turbomail 还支持 POP3 导入, 如果您的邮件系统不在上面之列, 可以在批量导入用户之后, 通过 POP3 协议导入邮件。



## 七. 附件传输及网络存储

### 7.1 大容量大空间

管理员可以针对全局、某个域、或者是单个用户进行精确的空间分配。

启用SMTP服务	<input checked="" type="checkbox"/>
启用POP3服务	<input checked="" type="checkbox"/>
启用IMAP4服务	<input checked="" type="checkbox"/>
启用WEB服务	<input checked="" type="checkbox"/>
<b>最大空间</b>	<input type="text" value="-1"/> M(负数表示无限制)
最多邮件数	<input type="text" value="-1"/> (负数表示无限制)
<b>启用网络硬盘</b>	<input checked="" type="checkbox"/>
<b>最大分配网络硬盘空间</b>	<input type="text" value="-1"/> M(负数表示无限制)
启用短信服务	<input type="checkbox"/>
启动彩信服务	<input checked="" type="checkbox"/>
启动即时通讯服务	<input checked="" type="checkbox"/>

用户登陆邮箱后提示邮箱空间的截图如下：

自定义文件夹	<input type="text"/>	<a href="#">新建文件夹</a>
邮箱总容量信息:(无限制)	<input type="text"/>	已用： <b>856.19M</b> (0%) 剩余：无限制 (100%)
邮件总数量信息:(无限制)	<input type="text"/>	已用： <b>350</b> (0%) 剩余：无限制(100%)

### 7.2 大附件超速上传

Turbomail 邮件系统采用最新的 ajax upload 超速上传技术，附件上传速度改善三倍以上。为需要经常性传输附件的使用者提供了极大的便利。



配合批量上传和高级媒体多窗口界面，使用者可以在高速上传附件的同时，浏览邮件并同时编写新邮件，无需等待。时间统筹规划，为企业节省了宝贵的时间。



### 7.3 网络硬盘

管理员在设置用户开启网络硬盘的同时也可以分配网络空间的大小，向网络硬盘上传文件同样采用的是最快的 ajax upload 新技术



分配空间:无限制 已使用空间:44.29M 文件总数:13 剩余空间:无限制

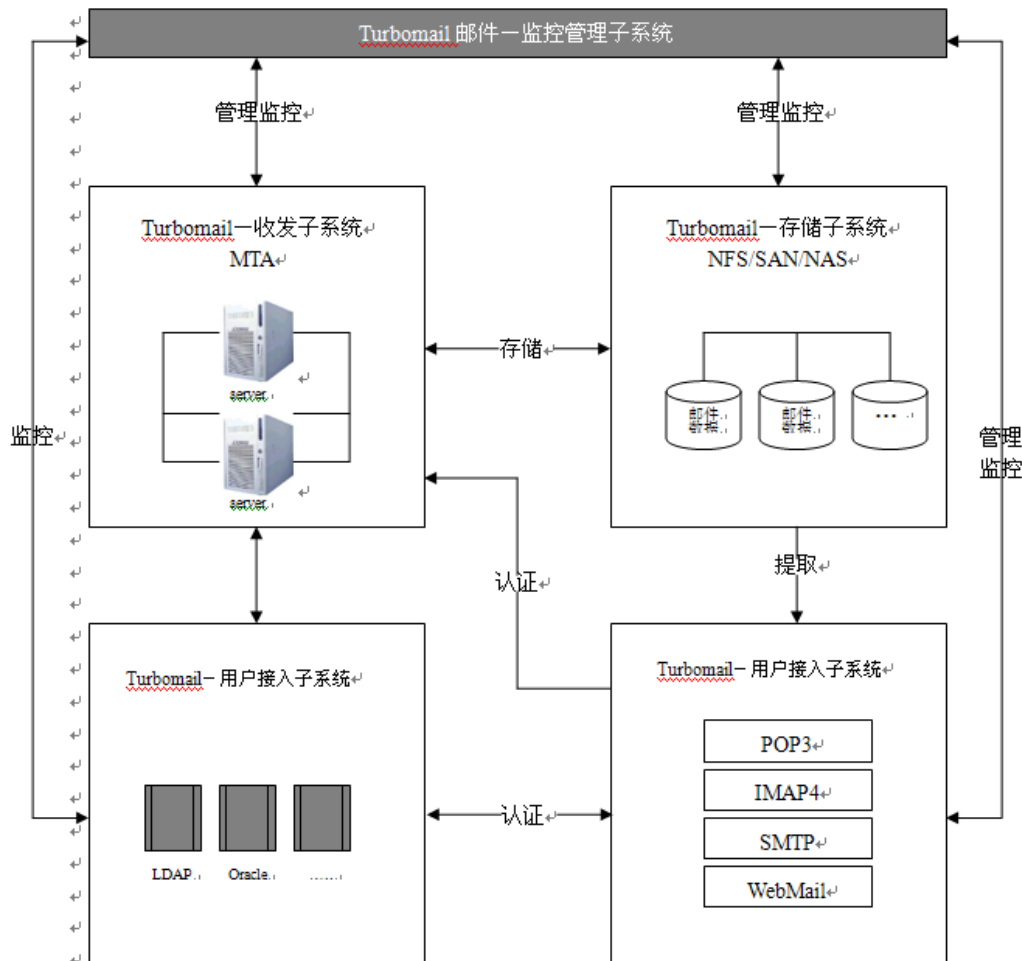
当前路径:/

	文件名	大小	类型	修改日期
<input type="checkbox"/>	公告扫描件.jpg	1.72M	文件	2009-10-22 14:37:05
<input type="checkbox"/>	██████████.doc	186K	文件	2009-10-22 14:39:33
<input type="checkbox"/>	██████████.doc	134K	文件	2009-11-17 17:14:46
<input type="checkbox"/>	二次开发JAVA.rar	332K	文件	2009-11-20 14:59:52
<input type="checkbox"/>	二次开发包NET文件.rar	65K	文件	2009-11-20 15:01:31
<input type="checkbox"/>	Turbomail产品手册v4.2.0.pdf	2.06M	文件	2009-11-26 16:40:18
<input type="checkbox"/>	TurboMail功能特点.pdf	202K	文件	2009-11-26 16:40:49
<input type="checkbox"/>	广州拓波软件科技有限公司介绍.pdf	251K	文件	2009-11-26 16:43:16
<input type="checkbox"/>	Turbomail售后服务说明.pdf	170K	文件	2009-11-26 16:43:33
<input type="checkbox"/>	TurboMail邮件系统用户手册.pdf	14.91M	文件	2009-12-08 09:52:36
<input type="checkbox"/>	TurboMail邮件系统域管理员手册.pdf	8.71M	文件	2009-12-08 09:56:15
<input type="checkbox"/>	通用方案.rar	7.01M	文件	2009-12-25 18:19:44
<input type="checkbox"/>	Turbomail邮件系统性能指标-压力测试报告.doc	127K	文件	2010-01-04 19:06:51
<input type="checkbox"/>	全选/取消全选			

## 八. 设计构架 (支持二次开发)

Turbomail®邮件系统五大功能模块逻辑关系图



面对国内巨大的用户群体，邮件系统的高可用性、高可扩展性是极其重要的。Java 在跨平台、开放性、扩展性方面具有先天优势，因此，基于 J2EE 构建大容量的邮件应用系统也就成为很好的技术选择。

邮件系统在当今社会，作为一种基础通讯平台，已经不单纯是简单收发邮件，而是成为互联网各种应用的核心，承载越来越重要的应用。中国人口众多，上网人数逐年剧增，使用邮件也日益频繁。邮件系统从建成的那一天起，就面临升级的压力。如何设计一个结构良好的大容量邮件系统，对于系统稳定性、可靠性，对于日后的升级维护有着至关重要的作用。

Turbomail®作为一个在邮件领域不断成长的产品，最终希望打造一个坚固的、高度可扩展的、容易管理维护的大容量分布式邮件系统。在设计时，我们主要考虑如下方面：



## 8.1 底层坚固、高度稳定

为保证系统的稳定可靠，需要在硬件、操作系统、核心 MTA、应用层在内的每一个环节都稳定可靠才行。硬件通常选取知名品牌服务器，稳定性、可靠性都有保障，差别不大。

操作系统选择 windows, Linux, FreeBSD 或者 Unix，针对邮件系统的特点，内核需要特殊调整：如打开文件数 (open files)、stack size、max user processes 等。除了操作系统核心外，系统只加载必须的软件，屏蔽一切不要的服务端口。

应用层我们选取 Apache+tomcat。Apache 久负盛名、久经考验，tomcat 背后有 IBM/SUN 支持，最重要的是 tomcat5 支持应用层负载均衡 (Load Balance)。另外，java 作为一种面向对象的编程语言，最能体现软件工程思想，有一系列的 UML 设计工具、集成开发环境、应用服务器可以选择。JAVA 语言已经是企业应用开发的实际标准语言。邮件系统应用层可以根据用户的反馈信息进行个性化二次开发，如果基于 java 开发，很容易找到相关人才。这样缩短开发周期、节省开发成本、降低维护难度。Google 很多服务是基于 java 开发的。当然，java 也有执行效率低的缺点，但随着硬件速度的提升，单只程序运行速度的劣势很容易被良好的设计模式优势取代。

## 8.2 容易管理、维护

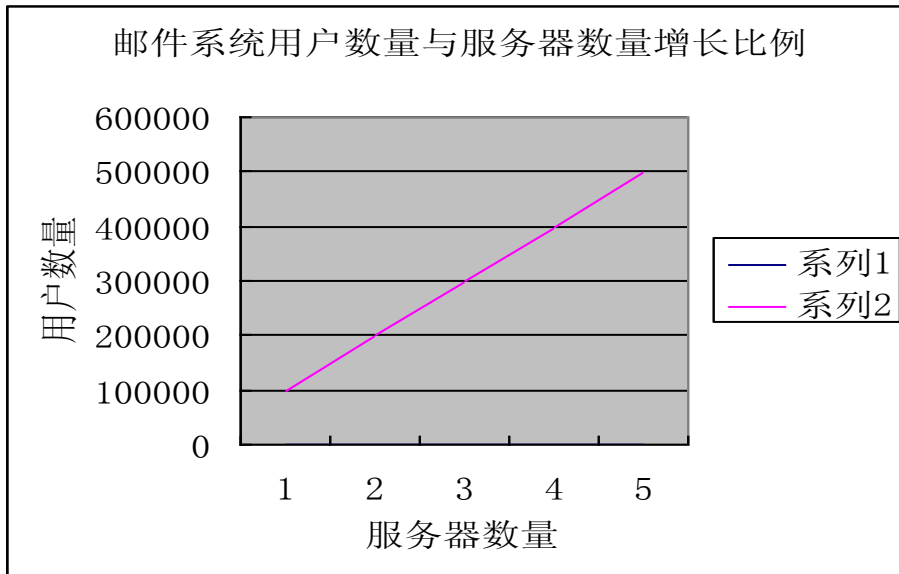
系统结构复杂之后，必然会带来管理维护上的麻烦。我们的设计思想是希望通过统一的一个管理控制界面，让系统管理员对每台服务器的运行状况、负载情况、流量了如指掌；同时通过一个管控界面，可以远程控制服务器启动、关闭，对服务进程远程启动、停止，对流量调配。当出现异常时，系统自动通过短信通知到管理人员的手机上。

## 8.3 增加设备简单、有效

系统扩展性是衡量系统设计好坏的一个重要指标。好的系统能够通过简单添置硬件、软件做少许配置即可满足需要。我们设计的是让用户数量的增长和邮件服务器数量呈线性关系。由于 PC 服务器的硬件成本比较低，以一台高性能 PC 服务器 3 万元人民币计算，如果作为 SMTP 服务器可以支撑 15 万用户，作为 POP 服务器可以支撑 30 万用户，作为存储服务器，可以支撑 3 万用户。

在保证系统稳定可靠的同时，能够最大地降低成本。降低成本有 2 个途径，一是最大限度利用硬件，二是避免使用高端的存储备份设备、负载均衡设备、四层交换机等。





#### 8.4 多级权限管理，支持企业全面发展

大容量邮件系统，不仅仅是个人用户，还有企业用户。不同用户群体的需求是不同的。针对不同用户群，提供不同的服务套餐，无疑是市场营销重要手段。而这，需要有技术上做保障才行。turbomail 系统应用层采用 java 技术，无疑是体现用户需求的最佳技术手段。

作为运营商，要有丰富权限管理体系，使邮件系统的每一个管理环节严紧、严密。

#### 8.5 高度模块化，模块之间最小耦合

模块化程度的高低，可以体现的系统的成熟度。充分利用开源宝库中的免费资源，将优秀的开源项目经过改良、优化，会搭建出优秀的系统。不赞成完全从底层开发。

模块之间通过标准接口通讯，耦合程度尽可能小，这样，即使出问题也不会影响全局。最重要的是，系统扩展性大大增强。如可以随时将病毒扫描过滤模块升级，或者将垃圾邮件过滤模块升级，其它模块无需做任何改动。

#### 8.6 提供与其它系统直接的接口

提供多种二次开发接口：单点登录、手机 WAP 访问、邮件读写二次开发、用户操作 API、组织机构管理、地址本二次开发等，TurboMail 拥有大量与 OA 系统、ERP 系统，PDM 系统等的集成经验。



## 8.7 应用层二次开发、部署简单方便

邮件系统的生命力来自客户的需求，只有不断满足客户需求，推陈出新，与时俱进，才会不断有新的用户加入。根据用户需求进行二次开发，这是必不可少的。二次开发必须简单，方便。Turbomail 通过统一的二次开发接口 Turbo-Maillet 实现服务端应用的扩展。



## 九. 系统安全

Turbomail 系统广泛用在电子政务、OA 项目中，安全是 Turbomail 系统的主要特点之一。安全性主要体现在如下方面：

### 9.1 邮件系统核心安全设计

邮件系统内核采用自主研发、自主知识产权的 MTA。turbomail 系统标准版、企业版 MTA 采用 C/C++ 开发，和操作系统紧密结合，在稳定性和效率方面，取得最佳平衡点。虽然有很多比较成熟的 MTA，但 turbomail 系统采用自主研发邮件通讯底层的技术路线，主要出于长远发展考虑：邮件内核好比是汽车发动机，只有掌握邮件内核，才能将最新的研究成果和技术应用于邮件内核，才会有一颗强健的心，给邮件应用层不断提供澎湃的动力。如果构建在别人的内核之上，邮件系统的扩展等会受到很多制约，邮件系统底层如果不能持续改进、完善，那么这个邮件系统的生命力是有限的，能够实现的功能也是有限的。目前国内有些厂商，采用破解国外 imail、mdaemon 等邮件系统另外加一套中文的 webmail 界面低价销售，采用这样的系统，一旦出现问题，国内的厂商不掌握核心技术和核心代码，很难解决，严重者所有的邮件帐户信息和邮件数据将无法挽回。这种损失，有时候不是用钱来衡量的。另外一些厂商基于 qmail 和 postfix 开发邮件系统，一般厂商也没有实力改造邮件内核，邮件系统的发展和功能拓展很多依赖于开源社区，各个补丁包之间难以完全兼容，因此依赖于此的邮件系统也很难有长足的发展。

1)、turbomail 系统在 TCP/IP 网络层实现 smtp client 并发连接限制和发送频率限制。很多邮件系统不稳定，是因为没有此功能，导致通过垃圾邮件字典攻击者瞬间发送大量的垃圾邮件所致。比如 netscape message server、exchange、domino mail server 都是这个原因导致服务崩溃。

2)、turbomail 系统内嵌 clamav 杀毒引擎、八层反垃圾邮件引擎，都是能够自动升级、自动更新病毒库和垃圾邮件规则库的，另外反垃圾邮件还有智能学习功能，管理员可以通过一批垃圾邮件和非垃圾邮件训练系统对垃圾邮件的识别率。内嵌反病毒反垃圾邮件模块，一方面可以提高效率，另外一方面，对于判定为垃圾邮件的邮件，turbomail 系统自动投递到普通用户的垃圾邮件箱，同时存放到管理员的垃圾邮件列表，供管理员进一步处理。

### 9.2 数字签名和传输数据加密

基于先进 PKI-CA 的安全机制，采用标准的 SMTP/SSL、POP3/SSL、S/MIME 协议，满足企业、军队、企业、个人在 Internet 上安全收发电子邮件的需求，保证信息传递的安全。Turbomail 邮件的加密安全性能特点：



✓ 数据加密功能

对邮件进行高强度的加密和解密以实现数据的保密

✓ 抗抵赖功能

邮件的数字签名（鉴别）实现发件人认证和不可抵赖

返回带数字签名的回执实现收件人不可抵赖

✓ 防篡改功能

完整性校验功能防止信息传输过程中被篡改

✓ 访问控制功能

通过安全邮件代理和证书来实现对用户强身份认证，给用户划分不同权限规则检验功能。通过安全邮件代理对邮件进行过滤。

✓ 日志和审计功能

通过分级日志系统来记录系统日志，并进行审计。

✓ 证书管理功能

提供用户管理、更新联系人和证书功能

用 RSA 密钥算法，支持标准 PKI—CA 系统

支持国密办批准认可的加密算法

✓ 支持多种硬件密码平台

采用公开密钥和对称密钥相结合的密钥体系

### 9.3 易于管理、配置

管理员只要通过浏览器，就能配置 DNS、内外部邮件服务器 ip、内外部邮件服务器域名、同步方式、同步频率、用户管理、邮件列表管理等，用户可以轻松建立 intranet 应用环境。用户可以通过 WEB 方式或邮件客户端软件收发邮件。并可以通过浏览器设置邮件过滤、转发、屏蔽、自动回复、pop 收信，极大地适应了用户



在不同环境和条件下的需求，使非专业人员也可以迅速部署邮件系统。

#### 9.4 其它技术优势

- ① 可做 DNS 反向查询
- ② 可限定发送频率和同一 ip 最大连接数
- ③ 登录失败后自动延时登录，可防止非法用户用连续密码尝试方式去破解邮箱
- ④ 自定义服务欢迎信息
- ⑤ 队列中的邮件是以文件形式存放在磁盘中，即使断电也不会丢数据
- ⑥ 用户分组管理，便于对分组用户的邮件收发进行精准控制
- ⑦ 全局过滤规则
- ⑧ 强大的反垃圾邮件功能
- ⑨ 完备的分级日志功能
- ⑩ 系统备份功能
- ⑪ 邮件系统监控功能
- ⑫ 单目录部署功能
- ⑬ 完备的二次开发接口
- ⑭ 单点登录，sso 统一认证接口
- ⑮ 邮件全文检索
- ⑯ 根据附件名查找邮件
- ⑰ 智能垃圾邮件过滤训练功能
- ⑱ 支持手机邮件
- ⑲ 内置邮件归档功能



## 十. 邮件备份及恢复

Turbomail 邮件系统的用户数据和邮件保存在单一目录 accounts 下，用户可通过指定特定的存储路径，把邮件存储在适当的硬盘空间中。

同时邮件系统数据的备份和恢复也只需针对这个目录进行即可。

## 十一. 带宽评估

Turbomail 邮件系统 1000 用户配置说明（峰值系数设为 4 倍）

### 互联网接入带宽

（根据每用户每天收发 20 封 200K 邮件计算）

#### 1. SMTP/POP3 请求：

$200\text{K}(\text{邮件}) * 20 \text{封} * 1000(\text{用户}) = 4\text{Gbyte} = 40\text{Gbit} / 86400(24 \text{小时} * 60 \text{分钟} * 60 \text{秒}) = 0.463\text{Mbit} / 0.6(\text{以太网带宽利用率}) = 0.772\text{Mbit} * 4(\text{带宽峰值比例}) = 3.08\text{M}$ 。

#### 2. WEB MAIL 请求：

$200\text{K} * 20 \text{封} * (\text{页面请求}) * 1000 \text{用户}(\text{实际通过 WEB 方式访问比例 } 3/10) = 1.2\text{Gbyte} = 12\text{Gbit} / 86400(24 \text{小时} * 60 \text{分钟} * 60 \text{秒}) = 0.13889\text{Mbit} / 0.6(\text{以太网带宽利用率}) = 0.2315\text{M} * 4(\text{带宽峰值比例}) = 0.926\text{M}$ 。

#### 3. 建议：

1000 用户 Internet 接入带宽为  $3.08\text{M} + 0.926\text{M} = 4\text{M}$

3000 用户 Internet 接入带宽为 12M



## 十二. 存储硬件配置

参数项目	参数值	编号
每用户存储量	1000M	A
用户平均存储率（经验值）	20%	B
系统存储率(Raid 5)	80%	D

计算项目	公式	计算值	编号
每用户平均存储需求	A*B	200M	C
每用户存储需求	C/D	250M	E

用户数量	实际邮件容量	总和
3000	250MB	约 750G

## 十三. 工程实施进度表

序号	项目	时间	工时	人员配备
1	硬件调试		1 天	1 人
2	系统安装 反垃圾病毒功能部署 系统监控调试		0.5 天	1 人



3	用户迁移		0.5 天	1 人
4	安全测试		1 天	1 人
5	操作配训		1 天	1 人
6	系统交接		0.5 天	1 人
总用时			4.5 天/人	





## 产品篇

### 一. 产品优势介绍

Turbomail 电子邮件系统是分布式、大容量、高可用电子邮件系统。采用 J2EE 开放技术架构，具有很好的可靠性、可扩展性。目前广泛用于各地电子政务网站、IDC 及各地行业门户网站。特点如下：

1. 完全自主研发、自主知识产权的 MTA（内核）；
2. 支持完全 Web 操作；（有些邮件系统是必须在一个机器上）
3. 垃圾邮件学习功能；（识别垃圾邮件，智能计算）
4. 自主设计 8 层反垃圾引擎，有效过滤垃圾邮件（拦截率高达 96%），误杀率低
5. 内嵌反垃圾、反病毒网关；（可自行设置 2 小时—3 天升级一次）
6. 支持 AJAX 界面，可多窗口操作，写邮件，读邮件同时进行
7. 树状公共地址簿；可通过部门和组设置，轻松群发邮件。
8. 部门管理机制和权限设立机制，可各部门自行管理本部门用户，也可统一管理。
9. 特别的组用户控制，除了普通组管理，更可以设置组可见度，是否发信需要审批等精细功能。
10. 支持 UTF-8 编码（多语言）；支持日文、俄文、韩文、繁体等语言文字；
11. 邮件关键字、内容全文检索，内置 lucence 搜索引擎，输入关键字后，能自动搜索发信人、主题、邮件正文、邮件附件名，快速查询；这是目前国内其他邮件系统所没有的。
12. Windows/Linux/Unix/Solaris/Aix 等多平台支持，切换系统零数据损失；
13. 布署 5 分钟内完成，可指定数据存储位置，维护方便；手动/自动备份，操作简便。
14. 短信模块（短信提醒、通知、时间、内容都能设定）；
15. 支持多域名和分级管理；
16. 提供在线注册（申请）功能，提供手动、命令行、批量建立用户帐号功能、在线存储文件和地址簿功能；
17. 可以通过 WEB 方式按日、月及用户进行精确详细统计及分析；



18. 提供与其它邮件系统兼容和用户信息迁移功能;
19. 完善的二次开发接口; 方便系统集成等开发。
20. 严谨的语言架构 (C 语言);
21. 成熟、稳定, 并有六年以上实际运营时间;
22. 有 100 万用户以上的实际应用经验及省级用户;
23. 支持分布式部署, 统一用户列表, 无单点故障的邮件服务。对于跨地域的大型集团尤其推荐。
24. 底层内核精简, 性能优秀。并发量大, 处理速度极快。单机并发量可达 20000 用户。
25. 实时系统监控, 方便发现、排查问题, 获得统计讯息。
26. 用户邮箱监控和镜像, 邮件审批, 对特殊的企业内外的邮箱地址进行监督。
27. 邮件归档, 所有进出邮件都会被备份到备份邮件中, 即使用户执行彻底删除, 邮件仍已被备份, 仍能轻松检索调出。
28. 邮件跟踪, 实时跟踪邮件发送状态。
29. 图形的用户流量报告, 详细统计每个邮件地址的发件和收件数量, 支持按条件查询生成报告;
30. 支持高级中继传输、加密传输, 海外中转服务器服务, 轻松解决国内外通信的线路问题、IP 问题、网关防火墙问题。



## 二. 技术架构

### (一) turbomail 邮件系统技术架构优势



turbomail 邮件系统 WEB 应用采用 J2EE 技术架构，有许多优势：

- 面向对象的网络编程语言，支持跨平台应用
- 开放的技术架构，100 多家大型 IT 厂商支持
- 跨平台，支持异构网络连接
- 安全性、可靠性好
- 对 XML, WebService 支持较好
- 安全性好
- 开发周期短
- 最好的 Object Oriented 语言：重用性，功能延展性
- 丰富的标准应用库
- 可靠性高

面对国内巨大的用户群体，邮件系统的高可用性、高可扩展性是极其重要的。Java 在跨平台、开放性、扩展性方面具有先天优势，因此，基于 J2EE 构建大容量的邮件应用系统也就成为很好的技术选择。



## (二) turbomail 的主要技术特点

### 2.1 九层反垃圾引擎

内嵌九层反垃圾邮件引擎，自动更新垃圾邮件规则库，垃圾邮件拦截率为 98%以上。

Turbomail 系统同时支持发信认证(smtp-auth)、黑名单和系统级垃圾邮件过滤功能，为用户邮箱提供三重保护功能。用户可以随时从国内外反垃圾邮件组织获得黑名单列表文件，导入邮件系统。从而使邮件管理员从被动变为主动。turbomail 系统黑名单功能支持模糊匹配，可以屏蔽一个域如@usa.com，也可以只屏蔽域内的一个用户如 spam@usa.com。

提供多种方式的垃圾邮件过滤功能，避免邮件服务器成为垃圾邮件中转站。

垃圾邮件过滤方法：九层垃圾邮件防护



#### 第一层：网络控制层

经验分析，发送垃圾邮件的服务器一般都会同时大批量的向某些域的多个帐号发送垃圾邮件，对于这些发送垃圾邮件方式，可通过设定一定网络访问频率控制进行有效的阻隔，turbomail 提供了两种设置方式对付这种攻击，并可自动把发送垃圾邮件的 IP 归为垃圾 IP (SpamIP) 列表。

通过 smtp 服务层把明显的发送垃圾邮件的 smtp 连接拒绝，大大减轻后台投递系统和反垃圾引擎的负载。

通过统计分析，我们发现很多发送垃圾邮件的 smtp 连接具有以下特点。

- 1、同一 IP 同时的 smtp 连接数非常大。
- 2、同一 IP 一段时间，smtp 连接频率非常大。



一般出现这两种情况，都表示源发件人非常有可能发送垃圾邮件。

通过设置以下这两个参数可控制这类型的 smtp 连接，从而截断发送垃圾邮件的源头：

#### 1、系统设置—》SMTP 服务—》一分钟内同一 IP 允许访问次数

同时设置：

系统设置—》SMTP 服务—》启用智能反垃圾 IP 功能参数，把符合以上两个条件的 IP 地址自动加入系统的智能反垃圾 IP 列表中（SmartSpamIP），当以后系统碰到这些 IP 的连接的时候，直接拒绝。

可通过：

系统监控—》智能反垃圾 IP 列表

查看系统目前智能反垃圾 IP 列表

注意：

当互联网是经过反垃圾网关再接入邮件系统的情况，由于邮件系统的所有 smtp 连接都来自反垃圾网关，所以基于 SmtP 服务反垃圾不再起作用，这是需要把以上两个参数设为-1，以免系统 smtp 服务故障。

#### 第二层：来源分析

根据垃圾邮件发送者 IP 的地理位置，与 APNIC 的 IP 信息库核对结果，看来源是否真实，如果真实则通过，否则可能为可疑邮件，由于 IP 来源无法伪装，所以这个反垃圾策略比较有效。

#### 第三层：黑名单

通过黑名单，turbomail 系统设置屏蔽任何一个 IP，一个网段；也可以屏蔽任何一个发信人，一个域。

实时黑名单(RBL)主要通过利用互联网公开的 rbl 资源判断垃圾邮件的可能性。目前 RBL 一般都通过 DNS 查询的方式提供对某个 IP 或域名是否是垃圾邮件发送源的判断。另外，由于国外大多数 rbl 都对来自中国的 ip 有“歧视”，所以我们并不能完全依靠 rbl 来判断一封邮件是否是垃圾邮件，只能根据 rbl 查询结果判断邮件是否垃圾邮件的可能性。可设置以下参数定制 rbl：



RBL 服务器地址	<input type="text" value="xbl.spamhaus.org"/>
DNS 查询类型	<input type="text" value="A"/>
得分	<input type="text" value="3.0"/>
匹配表达式	<input type="text" value="127\.\d+\.\d+\.[45]"/>
描述	<input type="text"/>
<input type="button" value="保存"/> <input type="button" value="取消"/>	

RBL 服务器，指定 RBL 查询域名后缀。

DNS 查询类型，根据具体的 RBL 要求指定 DNS 查询记录类型。

匹配表达式，指定 RBL 查询结果的匹配模式，表达式格式采用 perl 正则表达式，如果为空，则表示如果可查到 RBL 结果，就表示符合条件。

目前所知比较有效的 RBL 服务器为：

xbl.spamhaus.org

bl.spamcop.net

cbl.anti-spam.org.cn

cdl.anti-spam.org.cn

#### 第四层：灰名单

灰名单技术源于：<http://www.greylisting.org/>。

灰名单技术其基本假设是：病毒和垃圾邮件，通常都是一次性的，如果遇到错误，不会重试。

一些发垃圾邮件的软件，这些软件基本上都不会对邮件服务器返回的错误做出任何重试，而只是简单的在日志里记录发送失败而已。而病毒引发的邮件风暴则更加不会识别邮件服务器返回的错误，因为这些病毒仅仅是简单的发送邮件，发送时根本不理睬服务器的状态。

Greylist 的设计大体上是基于一种重试的原则，即第一次看到某个 IP 要想给某个收件人发信，那么它将简单的返回一个临时错误（4xx），并拒绝此请求，正常的邮件服务器都会在一段时间内（如半小时）重发一次邮件。greylist 发现还是刚才同样的 ip 地址和收件人，认为此 ip 是来自合法服务器的，予以放行。如果是



非正常的邮件，那么或者将永远也不再进行重试，或者会疯狂重试，但由于间隔太近，而遭拒绝。因此，greylist 只要设置一个合适的放行间隔，就可以在很大程度上对这类垃圾邮件有着良好的免疫能力。greylist 的一大特点就是不会丢信，正规的邮件服务器认为 4xx 错误只是临时性、软性的错误，会隔一段时间重试，因此邮件还是可以投递成功。但 greylist 的一大缺点即使延迟（delay），延迟从几分钟到几个小时不等。对于一些对邮件及时性很强的客户，greylist 可能不是一个很好的选择。

### 第五层：趋势分析

趋势分析原理为，所有垃圾邮件都有目标指向，比如：卖药广告邮件都会在邮件内容里指定卖药的电话、邮件或网站，如果不指定这些信息，发送垃圾邮件也就没有意义了。趋势分析法就是通过分析邮件里的电话、邮件或网站链接内容，通过匹配判断他的指向从而判断邮件是否是垃圾邮件。

### 第六层：邮件来源判断

主要通过分析邮件的来源，如：发件人 ip ，发件人，发件域，等内容，来判断垃圾邮件的可能性。

### 第七层：SpamFilter 内容过滤

通过邮件内容关键字分析，可为符合内容分析结果的邮件打上相应的垃圾邮件评分。这类规则的判断条件类似系统的过滤规则。可参考过滤规则设定来设定过滤评分内容，同时我们也会通过收集客户反馈的垃圾邮件特点整理成规则内容，定期通知客户更新。

### 第八层：SpamAssassin 引擎

SpamAssassin 是一个由 Apache 开发的一个著名的反垃圾引擎，turbomail 邮件系统完整的集成了 SpamAssassin 反垃圾引擎。

邮件系统提供了一个名为 SA-Server 的 SpamAssassin 反垃圾服务器，邮件系统通过把需要进行反垃圾分析的邮件提交给 SA-Server 进行分析。

SA-Server 在 Windows 平台上可通过 SA\_Server 服务启动，在 Unix/Linux 平台上可通过 sa/sa\_server.sh 脚本启动。

SA-Server 默认端口为 8700，可通过直接修改 sa/sa\_server.pl 修改这个端口。

可通过邮件管理系统中的，反垃圾\反病毒一》反垃圾引擎设置 中的 SpamAssassin 中的相关设置进行



SA-Server 的服务配置。

其中：

启用 SpamAssassin ， 指定是否启动 SpamAssassin 反垃圾检查

SpamAssassin 服务器地址，指定 SA-Server 服务器地址，默认为本机。

SpamAssassin 服务端口，指定 SA-Server 服务器端口，默认为 8700。

最大 SpamAssassin 检查线程数，指定最大的连接 SA-Server 服务数，可根据系统的复杂进行适当调整。

### **第九层：TMspamcheck 引擎**

垃圾广告商总是在想方设法的绕开上述拦截与屏蔽方式，“作案”手段不时更改，Turbomail 通过定期巡查以及与客户建立沟通制度，广泛搜集现行的各类垃圾邮件，并逐个分析，将垃圾邮件源列入 TMchecklist，所有的正式客户都将得到同步更新的服务，再度查杀漏网之“邮”。

## **2.2 内嵌杀毒引擎**

turbomail 系统支持多种杀毒引擎，并且内置著名的开源杀毒引擎 ClamAV，对邮件类病毒具有 99.9% 的杀灭能力，同时支持嵌入式杀毒和网关杀毒自动定时更新病毒特征库。

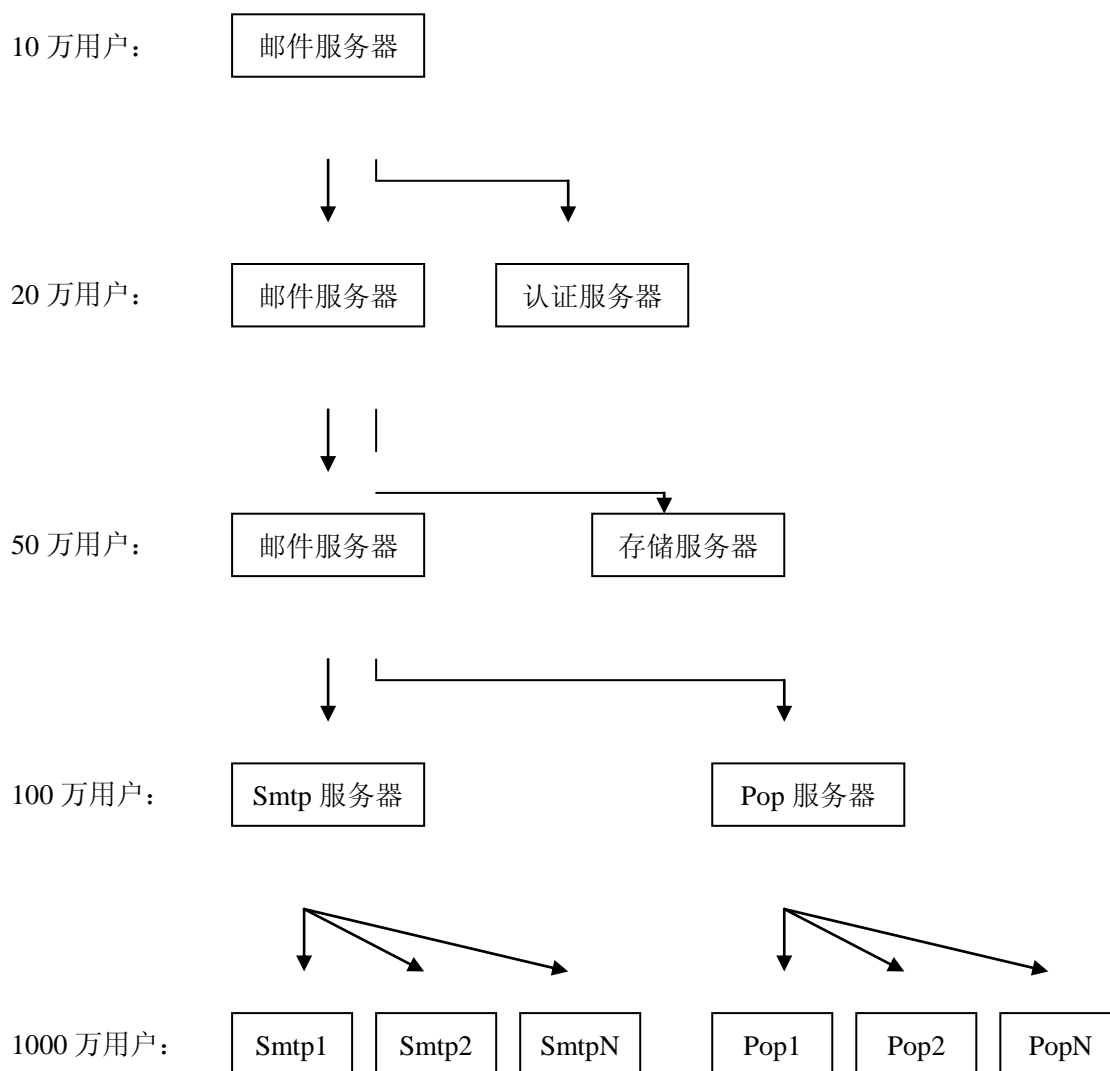




### 2.3 模块化、高扩展性

基于 turbomail 系统可以构建单服务器邮件系统和上千万用户的集群邮件系统。本着功能单一化、高度模块化的设计原则，turbomail 系统分为：收发模块、用户认证模块、邮件存储模块、用户接入模块等，既可以运行在一台服务器上，又可以分别运行在不同的机器上，共同完成整个电子邮件系统的功能。如果需要的话，每一种模块还可以再拆分在不同的服务器上运行实现负载分担，因此系统可以根据需要和用户的使用模式进行定制。这种结构所支持的用户量有比较大的灵活性。当邮件系统用户增加时，可以实现无缝升级和平滑过渡。最多可以支持到几千万以上用户。

如下图所示：





## 2.4 邮件全文检索

在邮件全文检索方面，turbomail 系统采用 lucence 技术，输入关键字后，能自动搜索发信人、主题、邮件正文、邮件附件名，这是目前国内其他邮件系统所没有的。另外，最有突破的是，邮件全文检索不会随着邮件数的增多(如几千,几十万封邮件),搜索时间不会增长，搜索时间一般都可控在几百毫秒以内。

## 2.5 最小内核技术

turbomail 系统设计上保证内核最小化，保证系统运行稳定、可靠；

## 2.6 多线程远程投递

多线程并发投递数动态可调，可以根据网络的带宽和主机性能随时调整，保证高效的投递速度和 100%的资源利用；

## 2.7 支持多种操作系统

Windows NT/2000/2003/2008, Linux, Solaris, Aix, HP-UX

## 2.8 支持主流标准协议

通讯协议：SMTP、ESMTP、POP3、IMAP、LDAP、MIME、DNS 等；

安全协议：SSL、PGP、VPN、DES 等

存储技术：SAN、NAS、NFS 等

## 2.9 支持主流数据库

关系数据库：支持 Oracle、Mysql、Sybase、SqlServer、DB2 等数据库。

(注：turbomail 安装包默认支持文本数据存储格式，支持其它各种数据库，不需要购买相应插件。)

目录数据库：LDAP



## 2.10 分布式并行处理

系统采用模块化设计、具有良好的封装性,使系统具有强大的扩展性。邮件核心系统和邮件前端(Webmail)系统可以运行在不同的主机上,可以将软件的不同模块,如收发模块、用户认证模块、邮件存储模块、用户接入模块等,分别运行在不同的机器上,共同来完成整个电子邮件系统的功能。如果需要的话,每一种模块还可以再拆分在不同的服务器上运行,实现负载分担,因此系统可以根据需要和用户的使用模式进行定制。

这种结构所支持的用户量有比较大的灵活性。用这种结构的系统可以支持到几百万以上的用户。最为著名的Hotmail 站点所采用的就是多台机器分布式并行操作的方式。通过多机集群技术,使运营商能够在处理海量邮件的发送、管理和存储。根据负载流量管理,运营商可以掌握系统的负荷状况,并根据业务发展需求来添加服务器。这种系统可以支持上百万乃至上千万的用户。

## 2.11 独立队列处理

当由于外界因素导致系统故障时,邮件队列处理失败的邮件将存储在缓冲区内。系统将继续利用其他工作正常的主机接管整个系统事务,直到故障排除,再将暂时存储的队列继续进行处理。

## 2.12 前端系统与 MTA 系统隔离

前端 Webmail 系统与核心系统分离,使系统具有良好的封装性、安全性和可扩展性。邮件核心系统与前端 Webmail 系统相分离,邮件用户不能直接访问邮件核心系统。由于系统的良好封装性,运营商可以将邮件核心系统放在防火墙后面,大大降低邮件系统被攻击的风险。

另一方面,随着运营商网络服务业务的发展,运营商可以灵活配置前端 Webmail 系统的功能。并可以通过增加 Webmail 系统主机获取更强的 Web 访问负载能力。

## 2.13 集群高速管理认证技术

高速邮件用户管理/认证方式与系统本身紧密结合,随着运营商服务的发展,用户管理可以随着邮件系统一同进行扩大,发展为分布并行式处理。所以,即便邮件用户发展到非常庞大的数量,系统依然能够以很快的速度对访问用户进行身份识别验证,对邮件用户进行管理。

## 2.14 抗灾难能力和恢复技术

系统通过分布式并行处理技术将服务中断风险降到最低限度,当集群服务器中某些服务器发生故障后,系



统其他服务器依然能够工作，并且接管故障服务器的工作，直到故障排除，再将工作移交回去。当机房发生重大意外事故（例如停电）的时候，系统邮件队列将保存在队列缓存中，当系统恢复工作后，邮件队列完全恢复，不会因此导致正在处理得邮件丢失。

## 2.15 智能邮件安全管理技术

turbomail 系统还提供了智能邮件过滤技术，通过大量分析研究国际 internet 上的垃圾邮件特征，系统能够智能识别垃圾邮件，无须各级管理员干预，自动将垃圾邮件拒之门外。并且实时监测系统收发的每个邮件，防止邮件内藏有恶意文件。从而提高了系统安全性并大大降低了系统维护的工作量。同时系统还采用 IP 记录跟踪技术，及时屏蔽黑客恶意行为，防止黑客采用机器人进行恶意破坏。（著名的 Hotmail 遭受的攻击事件导致系统严重瘫痪就是采用这类手段）

## 2.16 大容量

在一个中等规模的系统可以投递大约百万封邮件，甚至在一台 PC 服务器一天上能处理超过 20 万封邮件，起支持并行投递。支持邮件并行投递，同时可以投递大约 200 封邮件。采用 QMTP (Quick Mail Transfer Protocol) 来加速邮件的投递。

## 2.17 高速度

turbomail 系统集群版本把用户数据库挂接到高性能的 MYSQL 数据库上，利用 MYSQL 数据库速度快、安全性强和可远程访问的特点，保证了系统可以迅速从上百万的用户中找到所需投递的邮件存放服务器与特定的用户邮箱，使邮件系统在进行用户验证时的速度大大提高，满足大量用户同时访问。



### 三. Turbomail 功能模块

#### 3.1 普通用户功能

- 支持 outlook, foxmail 等邮件客户端, 并可共享地址簿
- 支持抄送和密送功能
- 定时发送邮件
- 高级多媒体编辑功能
- 收件人邮箱无需填全, 系统自动识别邮箱地址或昵称
- 自动回复, 自动转发
- POP3 收件
- 多个个人签名档
- 邮件回执
- 邮件发送优先级选择
- 邮件可选按不同要素进行排序
- 公共地址簿, 个人地址簿, 层级式管理
- 自建文件夹对邮件分类管理
- 过滤规则设置, 设置条件做邮件过滤, 从而对邮件执行相应操作, 如拒收, 发送短消息, 转到某文件夹, 转发等
- 设定个人垃圾邮件黑名单与白名单
- 网络硬盘
- 日程安排
- 移动书签



- 邮件全文搜索
- 发送邮件短信提醒收件人
- 邮件到达短信通知自己
- 手机登录邮箱，收发邮件
- 视频邮件，语音邮件

### 3.2 域管理员功能

#### 1. 用户管理

新增、编辑用户	可设置用户名，用户类型（普通用户，域管理用户），昵称，SMTP/POP3/IMAP4/WEB/SMS 功能控制，外发权限设置，最大空间/邮件数限制，发送邮件/SMS 频率控制，用户别名，有效期，允许发送附件大小，网络硬盘控制等等
删除用户	可用复选框，一次删除多个用户，删除用户时用户邮件也一并删除
查找用户	可根据用户名、域、各用户属性做为关键字模糊查找
浏览用户	可分页浏览显示用户列表；可浏览用户邮箱空间情况
导入用户	可导入用户文件，并列表显示所导入的用户清单
导出用户	可导出 txt、excel、Outlook 地址本格式的用户文件

#### 2. 用户组管理

用户组管理	可创建用户组，删除用户组，编辑用户组，浏览用户组
-------	--------------------------



	用户组是一个特殊的邮箱，给这个邮箱发信，组内的每个用户都可以收到，组内用户可以是系统内用户，也可以是系统外用户
	可设定用户组的属性：可选择接收所有邮件、只接收同一域下用户发来的邮件、只接收系统内投递的邮件、只接收通过用户验证后发送的邮件、只接收组内用户的邮件、只接收特定发件人的邮件、来自组管理员的邮件
	可选择是否保存邮件副本，即指定是否在用户组保存邮件的副本
	可选择是否替换接收人地址，指定是否把邮件头的接收人替换成真实的组成员邮件地址

### 3. 域地址本

功能	增加、删除、编辑地址以及目录，分为域地址簿和个人地址簿
域地址本	域级公共地址本只有域内的用户可以使用
个人地址本	个人编辑使用

### 4. 域信息

域信息	显示该域相关信息：域名、分配空间、分配用户数、已有用户数、已有空间、状态、域到期时间、是否允许用户自由注册、是否启用 smtp/pop3/imap/WEB，是否只能发本域邮件、最大空
-----	---



	间、最多发送邮件数
--	-----------

## 5. 公告

增加公告	增加新的公告，可文字编辑，插入图片、链接等
删除公告	删除不需要的公告
刷新公告	刷新显示最新发布公告列表

## 6. 域网络硬盘

域网络硬盘	显示网络硬盘中所有的文件列表、分配空间、已使用空间、文件总数、剩余空间、当前路径
上传	上传文件到网络硬盘
新建文件夹	建立新文件夹

## 7. 任务管理

用户注册申请	显示当前新用户注册申请信息列表，可以选择批准、删除、刷新操作
--------	--------------------------------

## 8. 日志查看





域操作日志	显示域操作日志列表，可按开始时间和截止时间进行查找，也可根据内容进行模糊查找
用户日志	显示用户日志列表，可按邮件账号、日志类型（Webmail、SMTP、POP3、IMAP、XMPP）、开始时间和截止时间进行查找，也可根据内容进行模糊查找

## 9. 域过滤规则

过滤范围	对域内所有用户都起作用
规则设置	可分别设置域接收过滤规则、域发送过滤规则。规则可根据来源 IP、收件人 IP、发件人所属部门、收件人所属部门、发件人、接收人、主题、附件名、邮件内容、邮件长度、邮件头字段、邮件发送时间、邮件接收时间、是否包含附件等条件进行判断
执行操作	不执行以后规则、拒绝接收、发送到指定文件夹、转发到指定邮箱、自动回复、发送短信、发送彩信等相应操作

## 10. 域中继设置

域中继列表	显示已经添加的域中继列表
增加	可根据收件人或者收件域编辑中继判断条件



### 11. 域邮件监控

发送邮件监控	可增加、编辑或者删除规则，编辑选项有规则名称、被监控发件人、接收监控邮件邮箱
接收邮件监控	可增加、编辑或者删除规则，编辑选项有规则名称、被监控收件人、接收监控邮件邮箱
查找（删除）用户邮件	可根据邮件账号、主题、发件人、收件人、日期进行搜索用户邮件

### 12. 域邮件审核

邮件审核规则列表	增加、编辑审核规则，可根据来源 IP、收件人 IP、发件人所属部门、收件人所属部门、发件人、接收人、主题、附件名、邮件内容、邮件长度、邮件头字段、邮件发送时间、邮件接收时间、是否包含附件等条件进行设置
接收邮件审核	增加、编辑接收邮件审核规则，可根据来源 IP、收件人 IP、发件人所属部门、收件人所属部门、发件人、接收人、主题、附件名、邮件内容、邮件长度、邮件头字段、邮件发送时间、邮件接收时间、是否包含附件等条件进行设置

### 13. 域黑名单

黑名单管理	增加、删除黑名单
-------	----------



	新增黑名单 IP 地址（两种格式：单个 IP 地址、一个网段）
	新增黑名单域名
	新增黑名单邮件地址

#### 14. 域白名单

白名单管理	增加、删除白名单
	新增白名单 IP 地址（两种格式：单个 IP 地址、一个网段）
	新增白名单域名
	新增白名单邮件地址



### 3.3 后台管理员功能

#### 1. 用户管理

增加、编辑用户	可设置用户名，用户类型（普通用户，域管理员），昵称，SMTP/POP3/IMAP4/WEB/SMS 功能控制，外发权限设置，最大空间/邮件数限制，发送邮件/SMS 频率控制，用户别名，有效期，允许发送附件大小，网络硬盘控制，启用短信、彩信、即时通讯服务控制，个人信息设置
删除用户	可用复选框，一次删除多个用户，删除用户时用户邮件也一并删除
查找用户	可根据用户状态、用户名、域、各用户属性作为关键字模糊查找
浏览用户	可分页浏览显示用户列表；可浏览用户邮箱空间情况
批量修改用户	可根据一定条件进行批量用户的属性修改
重建辅助用户数据库	刷新并重新加载用户数据库
重建全文索引	重新刷新全文索引

#### 2. 用户组管理

用户组管理	可创建用户组，删除用户组，编辑用户组，浏览用户组，根据用户组状态、用户组名、域、昵称等属性查找用户组
	用户组是一个特殊的邮箱，给这个邮箱发信，组内的每个用户都可以收到，组内用户可以是系统内用户，也可以是系统外用户



	可设定用户组的属性：可选择接收所有邮件、只接收同一域下用户发来的邮件、只接收系统内投递的邮件、只接收通过用户验证后发送的邮件、只接收组内用户的邮件、只接收特定发件人的邮件、只接受来自组管理员的邮件
	可选择发件是否需要审批，组员加入方式，可见度，是否保存邮件副本（即指定是否在用户组保存邮件的副本）
	可选择是否替换接收人地址，指定是否把邮件头的接收人替换成真实的组成员邮件地址

### 3. 公共地址本

功能	增加、删除、编辑地址以及目录，导入、导出、刷新地址本，可根据用户名称、邮件地址、手机号码、电话号码查找用户，分为公共地址簿和个人地址簿
公共地址簿	分为系统级地址簿和域级公共地址簿，系统级公共地址簿由系统管理员维护，系统内所有用户都可以使用；域级公共地址簿只有域内的用户可以使用
个人地址簿	个人编辑使用



#### 4. 域管理

新增域	可设置域名、HELO 域名、总分配空间数、用户数、是否为默认域、状态、域到期时间、启用短信彩信服务，如果域到期是否禁用该域，域日发信数量，域发送邮件频率，最大可建用户组数，是否允许域级邮件监控、邮件审批，是否允许域级黑名单、白名单，是否禁用域外发中继，启用域网络硬盘，启用即时通讯功能，是否允许用户注册，是否启用 smtp/pop3/imap/WEB 服务，是否只能发邮件到本域
修改域	变更 HELO 域名、总分配空间、用户数、是否为默认域、是否允许用户自由注册、是否启用 smtp/pop3/imap, 是否只能发本域邮件、每个用户最大空间、每个用户最多发送邮件数等等域的相关信息
设定域过滤规则	可根据发件人、收件人、主题、附件名、邮件内容、邮件大小、邮件头字段、邮件发送时间设定域的过滤规则，满足条件后可执行 4 种动作：拒收、转发指定邮件夹、转发其他邮箱、自动回复邮件
删除域	删除域将删除域下所有用户和邮件
重置所有用户已用空间	重新刷新所有用户的已用空间
从目录生成域信息	从目录结构生成域信息
清除所有用户邮件索引	清除所有用户邮件的索引数据

#### 5. 组织部门管理

组织部门管理	按层级编辑组织、部门以及下级单元，将所有用户按照层级进行分组
--------	--------------------------------



	并进行分别管理，可设立部门管理员，同时可为每个部门指定一个邮件帐户，发送到这个帐号的邮件同时也会转发给部门内所有人
	可增加、删除、编辑组织、部门或者部门人员

## 6. 任务管理

用户注册申请	显示当前新用户注册申请信息列表，可以选择批准、删除、刷新操作
--------	--------------------------------

## 7. 系统设置

一般参数设置	设定用户验证方式：文本文件、中心认证（数据库）、中心认证（LDAP）、中心认证（简单 LDAP）、中心认证（AD）
	设定接收错误信息的帐户、接收系统建议账号
	错误退信附件格式：不包含原邮件、包含原邮件作附件（但去除原邮件附件）、
	设定日志记录层次：所有、错误信息、一般信息、底层信息、调试信息
	设定邮件最小容量告警值
	设定自动清除垃圾/病毒软件时间间隔
	设定自动定时发送邮件间隔



设定清除 postmaster@root 超过（小时）之前的邮件
设定清除超过（天）之前的日志
设定清除超过（天）之前的邮件流量日志
设定系统默认字符集
设定邮件存储目录
设定备份存储目录
选择是否启用文本用户缓存
设定文本用户缓存时间
设定记录用户级日志
设定启用邮件状态追踪
选择不使用日志缓冲功能
选择是否记录邮件流量
选择用户级过滤规则执行模式：默认是（最后）发送到用户收件箱
选择操作系统字节序：最低位字节在最前、最高位字节在最前





	设定用户修改接口类
	设定邮件导入转换器实现类
	输入 API 访问用户名
	输入 API 访问密码
	设定令牌验证密码
	自定义邮件处理接口类
	新邮件到达处理接口类
	WEB 用户验证接口类
投递服务系统	设定最大投递线程数
	设定投递尝试间隔时间
	设定最大尝试投递次数
	设定投递间隔增加率
	设定外发绑定 IP
	设定网络连接超时值
	选择投递失败是否转入用户 Exception 文件夹



	选择对中转邮件是否执行过滤规则
	选择是否记录发件会话明细
	选择 HELO 命令模式：使用各域设置 HELO 域名、使用默认域 HELO 域名
	选择中继的使用方式：不使用、投递失败时使用、总是使用
	设定根据判断条件，是否使用中继
	编辑中继判断条件列表
	编辑正常发送失败判断条件列表
	编辑中继账号列表
	设定中继最大投递尝试次数
	设定中继最大同时投递数
SMTP 服务	选择服务端口，可以绑定多个 IP，设置端口号，是否使用 SSL/TLS
	设定 SMTP 欢迎信息
	设定服务器 IP
	选择是否启用 SMTP 验证



选择是否启用 SMTP 强制验证
设定不做 SMTP 验证的 IP: 单个 IP 或者一个网段
设定 SMTP 验证最大尝试次数
设定最大 SMTP 服务线程
设定端口最大侦听数
设定最大 RCPT 命令数
设定最大 MTA 跳转数
设定 SMTP 客户连接超时时间
设定读取命令超时时间
设定邮件最大体积
设定 SMTP 服务最小允许存储空间
设定 SMTP 最小允许内存
设定一次会话允许最大命令数
设定最大无效命令书
选择是否检查发件邮箱地址域名有效性



选择是否允许邮件中转
设定连续发送相同邮件控制次数
选择是否允许 VRFY 命令
选择是否允许 ETRN 命令
选择是否禁止 RSET 重复发送
选择是否允许空的发送者
选择 SMTP 中继网关
选择允许中继地址
选择“mail from”与“from”不一致处理方式：允许转发、拒绝转发、替换邮件头的 from 字段为 mail from 字段
选择收件人空间不足致处理方式：直接拒绝、发送提示信
设定 DNS 服务器
选择如果不存在 MX 记录，是否使用 A 记录
设定一分钟内同一 IP 允许访问次数
设定同一 IP 最大同时访问数



	选择是否启用智能反垃圾 IP 功能
	选择是否启用防止伪装发送地址邮件
	选择是否启用同域发给同域需要验证
	选择是否记录会话明细
	选择是否允许使用 nobody@root 邮箱
POP3 服务器	选择 POP3 服务端口
	设置 POP3 欢迎信息
	设定登录错误间隔延时值
	设定最大 POP3 服务线程
	设定端口最大侦听数
	设定 POP3 客户连接延时值
	设定读取命令超时时间
	设定 POP3 验证最大尝试次数
	设定验证前最大可执行命令数
	设定最大无效命令数



	设定 POP3 服务最小使用内存
	设定一分钟同一 IP 允许访问次数
	设定同一 IP 最大同时访问数
	是否记录会话明细
	设定最大 POP3 收件服务线程
	设定 POP3 收信服务执行间隔
IMAP4 服务器	设定服务端口列表
	设置 IMAP4 欢迎信息
	设定登录错误间隔延时值
	设定最大 IMAP4 服务线程
	设定端口最大侦听数
	设定 IMAP4 客户连接超时值
	设定读取命令超时时间
	设定验证前最大可执行命令数
	设定最大无效命令数



	设定最大无效命令数
	设定一分钟内同一 IP 允许访问次数
	设定同一 IP 最大同时访问数
队列系统	设定扫描间隔时间
	设定队列文件系统层级
本地处理服务	设定最大本地投递线程
webmail 参数	设定允许 Web 上传的最大附件大小
	设定会话非活动超时值
	选择窗口显示模式：嵌入窗口、弹出窗口
	选择是否记录客户端 MAC 地址（适用于 IE）
	选择是否直接生成注册用户
	选择是否允许注册时选择组织部门
	设定 URI 编码集
	设定发送定制信息线程扫描间隔
	选择发送回执方式：需用户确认、自动回执



选择添加编辑附件方式：传统方式、同一页面方式、同时添加多个附件方式
选择发件页面是否显示密送
选择显示发件人友好名称
选择显示收件人友好名称
选择是否允许非登录查看邮件
设定非登陆查看邮件 URL 前缀
设定匿名发件帐号
选择 WAP 是否允许下载附件
选择是否启动自动输入提示
选择是否允许用系统用户昵称发信
选择是否自动提醒新邮件
选择是否提醒后需要签收邮件
选择是否缓存邮件索引
选择是否允许个人地址本从系统用户添加





	选择是否允许域地址本从系统用户添加
	选择是否允许个人导出组织部门列表
	选择是否地址本只显示所属子部门
	设定登陆显示的域名
	设定只允许普通用户通过那些哪些 IP 访问
	设定管理员通过哪些 IP 访问
	选择是否允许用户自己注销
	选择是否启用视频邮件
	选择是否启用音频邮件
	选择是否启用公告功能
	设定邮件列表列出公告数
CTRL 服务	设定服务端口
	设定最大线程
	设定客户端连接超时值
	设定端口最大侦听数



	输入用户名和密码以供确认
	设定许可访问 IP
	设定 CTRL 服务器 IP
数据库参数	设定 DB 驱动程序类名
	设定连接 URL
	输入数据库用户名及密码以供确认
	设定最大连接数
	设定空闲超时
	设定检出超时
	设定最大检出数
网络访问控制	选择网络访问控制类型：SMTP、POP3、Sendmail、IMAP4
	增加：设定名称，设置判断条件类型和控制动作
	编辑网络访问控制：名称，设置判断条件类型和控制动作
证书管理	选择域
	设定密钥长度



	设定有效期
	设定国家、省、城市、组织、部门
短信设置	选择是否启动短信功能
	设置 SMS 实现发送类
	设置短信发送频率
	设置失败后重发次数
	设置串口号、波特率、短信中心号码、短信最大长度
	短信发送测试，输入测试手机号码和短信内容
彩信设置	选择是否启动彩信功能
	设置网关 IP、网关端口、服务器 URL、MMS 发送实现类
	彩信发送测试
网络硬盘设置	选择是否启用网络硬盘功能
	设置允许上传最大文件大小
	选择是否启用公共网络硬盘
数据库参数	设置 DB 驱动程序类名



	设置连接 URL
	输入数据库用户名及密码以供确认
	设置最大连接数
	设定空闲超时值
	设定检出超时值
	设定最大检出数
LDAP 参数	设定 LDAP 服务器名
	设定 LDAP 服务器端口
	设定 BASE DN
	输入管理员 DN 及密码以供确认
	设置查询 DN 格式
	设定保存密码的属性
	设定密码格式
认证中心	设定认证服务器地址
	输入用户名及密码以供确认



	输入服务器端口
Plugin 服务	设置 Plugin 服务 IP
	设定 Plugin 服务器端口
	设定连接超时值
分布式服务	节点管理：增加、编辑、删除节点
	设置本节点 IP
	设置服务端口
	设置客户端连接超时值
	设置端口最大侦听数
	设定服务器端最大线程数
	输入用户名和密码以供确认
	设置许可访问 IP
	选择是否启用分布式服务端
	选择是否允许通过分布式服务转发邮件
	设置客户端最大线程数



	选择是否启用分布式客户端
虚拟域	可设置多个虚拟域
	增加、编辑、删除虚拟域
邮件模板	可设置多个邮件模板
	增加、编辑、删除邮件模板
	设定模板名称、主题及内容
TcpServer 服务	选择是否启动 TcpServer
	设定 TcpServer 服务器 IP
	设定 TcpServer 服务器端口
	设定最大线程数
	设定连接超时
	设定许可访问 IP
XMPP（即时通讯）服务	是否启动 C2S 服务
	设置 XMPP C2S 服务端口列表
	设定最大 C2S 线程数



	设定 C2S 端口最大侦听数
	设定 C2S 连接超时时间
	设定 C2S 会话超时时间
	选择是否记录发件会话明细
归档服务	选择是否启动归档服务
	设定归档文件存放路径
	设定每个归档文件大小
	设定归档索引间隔时间值
用户初始化	导入用户文件，文件为文本文件
导入邮件	选择原邮件系统类型
	设定原邮件存储目录
	设定默认域
	设定需导入的用户
	选择是否自动生成不存在的用户
	选择是否自动生成用户的默认密码



导出用户	选择需要导出的域、导出格式和编码格式，进行导出
导入活动目录用户	导入活动目录用户

## 8. 全局过滤规则

过滤范围	对系统内所有用户都起作用
规则设置	可分别设置系统接收过滤规则、系统发送过滤规则。规则可根据来源IP、收件人IP、发件人所属部门、收件人所属部门、发件人、接收人、主题、附件名、邮件内容、邮件长度、邮件头字段、邮件发送时间、邮件接收时间、是否包含附件等条件进行判断
执行操作	不执行以后规则、拒绝接收、发送到指定文件夹、转发到指定邮箱、自动回复、发送短信、发送彩信、执行 Plugin (Java 处理类) 等相应操作

## 9. 邮件监控

发送邮件监控	可增加、编辑或者删除规则，编辑选项有规则名称、被监控发件人、接收监控邮件邮箱
接收邮件监控	可增加、编辑或者删除规则，编辑选项有规则名称、被监控收件人、接收监控邮件邮箱
查找（删除）用户邮件	可根据邮件账号、主题、发件人、收件人、日期进行搜索用户





	邮件
--	----

## 10. 邮件审核

邮件审核规则列表	增加、编辑审核规则，可根据来源 IP、收件人 IP、发件人所属部门、收件人所属部门、发件人、接收人、主题、附件名、邮件内容、邮件长度、邮件头字段、邮件发送时间、邮件接收时间、是否包含附件等条件进行设置
----------	--

## 11. 归档服务

归档邮件搜索	支持一般搜索和高级搜索，高级搜索包括发件账号、收件账号、主题、发件人、收件人、内容、附件名、日期和归档类型（即所有、接受、发送）
归档邮件列表	显示归档邮件列表，可根据收件账号、日期或者内容进行搜索

## 12. 系统监控

Webmail 在线用户	查看当前在线的 webmail 用户
邮件队列查看	查看系统的邮件就绪队列和重发队列，并可手工删除队列里指定邮件
SMTP 当前活动会话查看	查看当前活跃的 SMTP 会话，和会话状况



POP3 当前活动会话查看	查看当前活跃的 POP3 会话，和会话状况
IMAP4 当前活动会话查看	查看当前活跃的 IMAP4 会话，和会话状况
远程投递当前活动会话查看	查看当前活跃的 Sendmail 会话，和会话状况
XMPP C2S 服务当前活动会话查看	查看当前的 XMPP C2S 服务对话
智能反垃圾 IP 列表	查看、增加、删除系统垃圾 IP
web 服务器信息	查看 Tomcat 服务器的环境
系统信息	查看系统安装目录和版本号
系统警告信息	查看系统警告信息，如：注册码到期信息

### 13. 反垃圾\反病毒设置

反垃圾参数设置	选择是否启用 RBL 反垃圾查询
	设定 RBL 服务地址
	选择是否启用 RWL 白名单查询
	设定 RWL 服务地址



	选择是否对发送者 IP 进行 DNS 反向解析
	选择是否验证 HELO 域名有效性
黑名单	增加、删除黑名单
	新增黑名单 IP 地址，两种格式:单个 IP 地址，一个网段
	新增黑名单域名
	新增黑名单邮件地址
白名单管理	增加、删除白名单
	新增白名单 IP 地址，两种格式:单个 IP 地址，一个网段
	新增白名单域名
	新增白名单邮件地址
反垃圾引擎	选择启用反垃圾引擎
	设置同域内互发邮件也使用反垃圾引擎
	设置外发邮件也使用反垃圾引擎
	设置系统内用户互发邮件不经过反垃圾过滤
	设置标记为可能垃圾邮件值



设置标记主题前缀
设置判定为垃圾邮件值
设置垃圾邮件主题前缀
设置判定为系统自动删除值
设置垃圾邮件处理帐号
设置最大判断邮件大小
选择是否启用趋势分析
选择是否启用灰名单
设置灰名单开始阻隔时间值
设置灰名单超时时间值
选择是否启动来源分析
设置反向域名匹配级数
编辑可疑反向域名列表
设定可疑反向域名加分值
选择是否如果 IP 有反向记录则可信



编辑可信反向域名列表
设置 MX 记录不存在评分值
这是发件人格式不正确评分值
设置收件人不匹配评分值
设置发件人与收件人相同评分值
选择是否启用 SpamFilter
垃圾邮件内容评分规则，可根据邮件发件人、接收人、主题、附件名、邮件内容、邮件长度、邮件头字段、邮件发送时间等条件进行判断，并做垃圾邮件评分
设置邮件来源评分规则，可对邮件的来源 IP，域名，邮件地址进行垃圾邮件评分
设置黑名单（RBL）规则列表
设置内容 RBL 规则列表，可根据各种 RBL 进行垃圾邮件评分
选择是否启用白名单
设定白名单内容规则列表，包括发件人、收件人、主题、附件名、内容、其他邮件头字段、判断是否包含邮件头字段、邮件长度、邮件发送时间、邮件接收时间



	增加、编辑邮件来源白名单，包括 IP 地址、域名、邮件地址
垃圾邮件样本测试	测试垃圾邮件样本
垃圾邮件报告列表	显示发件人、收件人、主题、类型、日期、长度
	选择删除或重新发送垃圾邮件
ClamAV 反病毒引擎设置	选择启用 ClamAV
	选择是否记录反病毒明细日志
	选择同域内互发邮件也使用 ClamAV
	设置最大判断邮件大小
	设置病毒邮件处理帐号
	设置病毒库自动升级间隔
	设置升级失败尝试次数
	设定病毒库版本信息查询地址
设定病毒库下载地址	
病毒邮件报告列表	显示发件人、收件人、主题、类型、日期、长度
	选择删除或重新发送垃圾邮件



#### 14. 公告

增加公告	增加新的公告，可文字编辑，插入图片、链接等
删除公告	删除不需要的公告
刷新公告	刷新显示最新发布的公告列表

#### 15. 公共网络硬盘

公共网络硬盘	显示网络硬盘中所有的文件列表、分配空间、已使用空间、文件总数、剩余空间、当前路径
上传	上传文件到网络硬盘
新建文件夹	建立新文件夹

#### 16. 日志查看

系统日志	显示各种日志类型，如：系统信息、IMAP、POP3、SMTP、本地处理服务等，可按日志类型、日志记录层次、开始时间、截止时间、错误号、内容进行日志查找
域操作日志	显示域操作日志列表，可按开始时间和截止时间进行查找，也可根据内容进行模糊查找



用户日志	显示用户日志列表,可按邮件账号、日志类型(Webmail、SMTP、POP3、IMAP、XMPP)、开始时间和截止时间进行查找,也可根据内容进行模糊查找
------	--

## 17. 统计分析

流量统计	可根据多种条件进行查找统计,包括发件人、发件域、收件人、收件域、是否模糊匹配、统计类型(即远程投递、本地投递、POP3、SMTP、黑名单阻隔、病毒邮件、垃圾邮件)、分组类型(分为按发件人统计、按发件域统计、按收件人统计、按收件域统计)、开始和截止时间
邮件流量统计图	根据月份进行正常邮件、垃圾邮件与病毒邮件的统计
短信发送查询	根据发件人、手机进行查询,可选模糊匹配,查询类型包括明细查询、按手机统计、按发送人统计,还可按时间进行查询

## 18. 系统备份

系统备份	可选择备份用户地址本、用户邮件内容和用户网络硬盘内容,还可上传备份
------	-----------------------------------

## 19. 注册码管理

注册码管理	输入域名、许可域名数、用户数、注册码
-------	--------------------





## 20. 邮件

收邮件	显示系统收件箱，可以进行刷新、删除、把选中邮件移到文件夹等操作
发邮件	编辑邮件并发送邮件，可以上传附件、使用网络硬盘、定时发送邮件等
地址本	增加、删除、编辑地址以及目录，分为公共地址本、域地址本和个人地址本，并显示系统内各部门结构
邮件搜索	可进行一般搜索或高级搜索，其中高级搜索包括主题、发件人、收件人、内容、附件名、日期和文件夹
文件夹	包括收件箱、草稿箱、已发送邮件、回收站、异常邮件、垃圾邮件、病毒邮件，可选择刷新、删除、把选中邮件移动到文件夹等操作
定时发送邮件	对于定时发送邮件可选择刷新、删除操作
网络硬盘	显示网络硬盘文件列表、上传文件到网络硬盘、新建文件夹等

## 21. 设置

个人设定	设定默认值：每页显示邮件数、发送的邮件默认保存到“已发送邮件”、发送邮件需要回执、保存邮件客户端发送的邮件、发送邮件默认编码、登陆显示页、自动清除垃圾/病毒时间间隔
------	--



	等；设置个人相关信息：昵称、电话、手机、邮编、国家、省、地址等；设置三种个性化签名档
修改密码	修改登录密码
文件夹管理	删除文件夹、文件夹改名、增加文件夹
过滤规则设置	对当前用户起作用
	可根据来源 IP、收件人 IP、发件人、接收人、主题、附件名、邮件内容、字符集、其他邮件头字段、邮件长度、邮件发送时间、邮件接收时间、是否包含附件等组合条件执行相应的过滤作用
	拒绝接收、发送到指定文件夹、转发到指定邮箱、自动回复、发送短信、发送彩信
POP3 收信	设定 POP3 服务器地址、端口、用户名、密码
	选择发送到指定文件夹
	选择接收邮件后，是否删除 POP3 服务器上的邮件
	选择该服务器是否要求安全连接（SSL）
自动转发	选择启用自动转发
	设置转发到的邮箱



	选择是否保存副本在本地邮箱
自动回复	选择启用自动回复
	编辑回复内容
黑名单	个人黑名单设置，包括 IP 地址、域名和邮件地址
白名单	个人白名单设置，包括 IP 地址、域名和邮件地址
短信短语	编辑常用短信短语，包括标题和内容

## 22. 系统意见

系统意见	编辑系统意见并发送，包括意见主题和意见内容
------	-----------------------

## 23. 用户管理

增加、编辑用户	可设置用户名，用户类型（普通用户，域管理员），昵称，SMTP/POP3/IMAP4/WEB/SMS 功能控制，外发权限设置，最大空间/邮件数限制，发送邮件/SMS 频率控制，用户别名，有效期，允许发送附件大小，网络硬盘控制，启用短信、彩信、即时通讯服务控制，个人信息设置
删除用户	可用复选框，一次删除多个用户，删除用户时用户邮件也一并删除



查找用户	可根据用户状态、用户名、域、各用户属性做为关键字模糊查找
浏览用户	可分页浏览显示用户列表；可浏览用户邮箱空间情况
批量修改用户	可根据一定条件进行批量用户的属性修改
重建辅助用户数据库	刷新并重新加载用户数据库
重建全文索引	重新刷新全文索引

## 24. 用户组管理

用户组管理	可创建用户组，删除用户组，编辑用户组，浏览用户组，根据用户组状态、用户组名、域、昵称等属性查找用户组
	用户组是一个特殊的邮箱，给这个邮箱发信，组内的每个用户都可以收到，组内用户可以是系统内用户，也可以是系统外用户
	可设定用户组的属性：可选择接收所有邮件、只接收同一域下用户发来的邮件、只接收系统内投递的邮件、只接收通过用户验证后发送的邮件、只接收组内用户的邮件、只接收特定发件人的邮件、只接受来自组管理员的邮件
	可选择发件是否需要审批，组员加入方式，可见度，是否保存邮件副本（即指定是否在用户组保存邮件的副本）
	可选择是否替换接收人地址，指定是否把邮件头的接收人替换成真实



	的组成员邮件地址
--	----------

## 25. 公共地址本

功能	增加、删除、编辑地址以及目录，导入、导出、刷新地址本，可根据用户名称、邮件地址、手机号码、电话号码查找用户，分为公共地址簿和个人地址簿
公共地址簿	分为系统级地址簿和域级公共地址簿，系统级公共地址簿由系统管理员维护，系统内所有用户都可以使用；域级公共地址簿只有域内的用户可以使用
个人地址簿	个人编辑使用

## 26. 域管理

新增域	可设置域名、HELO 域名、总分配空间数、用户数、是否为默认域、状态、域到期时间、启用短信彩信服务，如果域到期是否禁用该域，域日发信数量，域发送邮件频率，最大可建用户组数，是否允许域级邮件监控、邮件审批，是否允许域级黑名单、白名单，是否禁用域外发中继，启用域网络硬盘，启用即时通讯功能，是否允许用户注册，是否启用 smtp/pop3/imap/WEB 服务，是否只能发邮件到本域
修改域	变更 HELO 域名、总分配空间、用户数、是否为默认域、是否允许用户自由注册、是否启用 smtp/pop3/imap, 是否只能发本域邮件、每个用户最大空间、每个用户最多发送邮件数等等域的相关信息



设定域过滤规则	可根据发件人、收件人、主题、附件名、邮件内容、邮件大小、邮件头字段、邮件发送时间设定域的过滤规则，满足条件后可执行 4 种动作：拒收、转发指定邮件夹、转发其他邮箱、自动回复邮件
删除域	删除域将删除域下所有用户和邮件
重置所有用户已用空间	重新刷新所有用户的已用空间
从目录生成域信息	从目录结构生成域信息
清除所有用户邮件索引	清除所有用户邮件的索引数据

## 27. 组织部门管理

组织部门管理	按层级编辑组织、部门以及下级单元，将所有用户按照层级进行分组并进行分别管理，可设立部门管理员，同时可为每个部门指定一个邮件帐户，发送到这个帐号的邮件同时也会转发给部门内所有人
	可增加、删除、编辑组织、部门或者部门人员

## 28. 任务管理

用户注册申请	显示当前新用户注册申请信息列表，可以选择批准、删除、刷新操作
--------	--------------------------------

## 29. 系统设置



一般参数设置	设定用户验证方式：文本文件、中心认证（数据库）、中心认证（LDAP）、中心认证（简单 LDAP）、中心认证（AD）
	设定接收错误信息的帐户、接收系统建议账号
	错误退信附件格式：不包含原邮件、包含原邮件作附件（但去除原邮件附件）、
	设定日志记录层次：所有、错误信息、一般信息、底层信息、调试信息
	设定邮件最小容量告警值
	设定自动清除垃圾/病毒软件时间间隔
	设定自动定时发送邮件间隔
	设定清除 postmaster@root 超过（小时）之前的邮件
	设定清除超过（天）之前的日志
	设定清除超过（天）之前的邮件流量日志
	设定系统默认字符集
	设定邮件存储目录
	设定备份存储目录



选择是否启用文本用户缓存
设定文本用户缓存时间
设定记录用户级日志
设定启用邮件状态追踪
选择不使用日志缓冲功能
选择是否记录邮件流量
选择用户级过滤规则执行模式：默认是（最后）发送到用户收件箱
选择操作系统字节序：最低位字节在最前、最高位字节在最前
设定用户修改接口类
设定邮件导入转换器实现类
输入 API 访问用户名
输入 API 访问密码
设定令牌验证密码
自定义邮件处理接口类
新邮件到达处理接口类





	WEB 用户验证接口类
投递服务系统	设定最大投递线程数
	设定投递尝试间隔时间
	设定最大尝试投递次数
	设定投递间隔增加率
	设定外发绑定 IP
	设定网络连接超时值
	选择投递失败是否转入用户 Exception 文件夹
	选择对中转邮件是否执行过滤规则
	选择是否记录发件会话明细
	选择 HELO 命令模式：使用各域设置 HELO 域名、使用默认域 HELO 域名
	选择中继的使用方式：不使用、投递失败时使用、总是使用
	设定根据判断条件，是否使用中继
	编辑中继判断条件列表
	编辑正常发送失败判断条件列表



	编辑中继账号列表
	设定中继最大投递尝试次数
	设定中继最大同时投递数
SMTP 服务	选择服务端口，可以绑定多个 IP，设置端口号，是否使用 SSL/TLS
	设定 SMTP 欢迎信息
	设定服务器 IP
	选择是否启用 SMTP 验证
	选择是否启用 SMTP 强制验证
	设定不做 SMTP 验证的 IP: 单个 IP 或者一个网段
	设定 SMTP 验证最大尝试次数
	设定最大 SMTP 服务线程
	设定端口最大侦听数
	设定最大 RCPT 命令数
	设定最大 MTA 跳转数
	设定 SMTP 客户连接超时时间



设定读取命令超时时间
设定邮件最大体积
设定 SMTP 服务最小允许存储空间
设定 SMTP 最小允许内存
设定一次会话允许最大命令数
设定最大无效命令书
选择是否检查发件邮箱地址域名有效性
选择是否允许邮件中转
设定连续发送相同邮件控制次数
选择是否允许 VRFY 命令
选择是否允许 ETRN 命令
选择是否禁止 RSET 重复发送
选择是否允许空的发送者
选择 SMTP 中继网关
选择允许中继地址



	选择“mail from”与“from”不一致处理方式：允许转发、拒绝转发、替换邮件头的 from 字段为 mail from 字段
	选择收件人空间不足致处理方式：直接拒绝、发送提示信
	设定 DNS 服务器
	选择如果不存在 MX 记录，是否使用 A 记录
	设定一分钟内同一 IP 允许访问次数
	设定同一 IP 最大同时访问数
	选择是否启用智能反垃圾 IP 功能
	选择是否启用防止伪装发送地址邮件
	选择是否启用同域发给同域需要验证
	选择是否记录会话明细
	选择是否允许使用 nobody@root 邮箱
POP3 服务器	选择 POP3 服务端口
	设置 POP3 欢迎信息
	设定登录错误间隔延时值



	设定最大 POP3 服务线程
	设定端口最大侦听数
	设定 POP3 客户连接延时值
	设定读取命令超时时间
	设定 POP3 验证最大尝试次数
	设定验证前最大可执行命令数
	设定最大无效命令数
	设定 POP3 服务最小使用内存
	设定一分钟同一 IP 允许访问次数
	设定同一 IP 最大同时访问数
	是否记录会话明细
	设定最大 POP3 收件服务线程
	设定 POP3 收信服务执行间隔
IMAP4 服务器	设定服务端口列表
	设置 IMAP4 欢迎信息



	设定登录错误间隔延时值
	设定最大 IMAP4 服务线程
	设定端口最大侦听数
	设定 IMAP4 客户连接超时值
	设定读取命令超时时间
	设定验证前最大可执行命令数
	设定最大无效命令数
	设定最大无效命令数
	设定一分钟内同一 IP 允许访问次数
	设定同一 IP 最大同时访问数
队列系统	设定扫描间隔时间
	设定队列文件系统层级
本地处理服务	设定最大本地投递线程
webmail 参数	设定允许 Web 上传的最大附件大小
	设定会话非活动超时值



	选择窗口显示模式：嵌入窗口、弹出窗口
	选择是否记录客户端 MAC 地址（适用于 IE）
	选择是否直接生成注册用户
	选择是否允许注册时选择组织部门
	设定 URI 编码集
	设定发送定制信息线程扫描间隔
	选择发送回执方式：需用户确认、自动回执
	选择添加编辑附件方式：传统方式、同一页面方式、同时添加多个附件方式
	选择发件页面是否显示密送
	选择显示发件人友好名称
	选择显示收件人友好名称
	选择是否允许非登录查看邮件
	设定非登陆查看邮件 URL 前缀
	设定匿名发件帐号



选择 WAP 是否允许下载附件
选择是否启动自动输入提示
选择是否允许用系统用户昵称发信
选择是否自动提醒新邮件
选择是否提醒后需要签收邮件
选择是否缓存邮件索引
选择是否允许个人地址本从系统用户添加
选择是否允许域地址本从系统用户添加
选择是否允许个人导出组织部门列表
选择是否地址本只显示所属子部门
设定登陆显示的域名
设定只允许普通用户通过那些哪些 IP 访问
设定管理员通过哪些 IP 访问
选择是否允许用户自己注销
选择是否启用视频邮件





	选择是否启用音频邮件
	选择是否启用公告功能
	设定邮件列表列出公告数
CTRL 服务	设定服务端口
	设定最大线程
	设定客户端连接超时值
	设定端口最大侦听数
	输入用户名和密码以供确认
	设定许可访问 IP
	设定 CTRL 服务器 IP
数据库参数	设定 DB 驱动程序类名
	设定连接 URL
	输入数据库用户名及密码以供确认
	设定最大连接数
	设定空闲超时



	设定检出超时
	设定最大检出数
网络访问控制	选择网络访问控制类型：SMTP、POP3、Sendmail、IMAP4
	增加：设定名称，设置判断条件类型和控制动作
	编辑网络访问控制：名称，设置判断条件类型和控制动作
证书管理	选择域
	设定密钥长度
	设定有效期
	设定国家、省、城市、组织、部门
短信设置	选择是否启动短信功能
	设置 SMS 实现发送类
	设置短信发送频率
	设置失败后重发次数
	设置串口号、波特率、短信中心号码、短信最大长度
	短信发送测试，输入测试手机号码和短信内容



彩信设置	选择是否启动彩信功能
	设置网关 IP、网关端口、服务器 URL、MMS 发送实现类
	彩信发送测试
网络硬盘设置	选择是否启用网络硬盘功能
	设置允许上传最大文件大小
	选择是否启用公共网络硬盘
数据库参数	设置 DB 驱动程序类名
	设置连接 URL
	输入数据库用户名及密码以供确认
	设置最大连接数
	设定空闲超时值
	设定检出超时值
	设定最大检出数
LDAP 参数	设定 LDAP 服务器名
	设定 LDAP 服务器端口



	设定 BASE DN
	输入管理员 DN 及密码以供确认
	设置查询 DN 格式
	设定保存密码的属性
	设定密码格式
认证中心	设定认证服务器地址
	输入用户名及密码以供确认
	输入服务器端口
Plugin 服务	设置 Plugin 服务 IP
	设定 Plugin 服务器端口
	设定连接超时值
分布式服务	节点管理：增加、编辑、删除节点
	设置本节点 IP
	设置服务端口
	设置客户端连接超时值



	设置端口最大侦听数
	设定服务器端最大线程数
	输入用户名和密码以供确认
	设置许可访问 IP
	选择是否启用分布式服务端
	选择是否允许通过分布式服务转发邮件
	设置客户端最大线程数
	选择是否启用分布式客户端
虚拟域	可设置多个虚拟域
	增加、编辑、删除虚拟域
邮件模板	可设置多个邮件模板
	增加、编辑、删除邮件模板
	设定模板名称、主题及内容
TcpServer 服务	选择是否启动 TcpServer
	设定 TcpServer 服务器 IP



	设定 TcpServer 服务器端口
	设定最大线程数
	设定连接超时
	设定许可访问 IP
XMPP（即时通讯）服务	是否启动 C2S 服务
	设置 XMPP C2S 服务端口列表
	设定最大 C2S 线程数
	设定 C2S 端口最大侦听数
	设定 C2S 连接超时时间
	设定 C2S 会话超时时间
	选择是否记录发件会话明细
归档服务	选择是否启动归档服务
	设定归档文件存放路径
	设定每个归档文件大小
	设定归档索引间隔时间值



用户初始化	导入用户文件，文件为文本文件
导入邮件	选择原邮件系统类型
	设定原邮件存储目录
	设定默认域
	设定需导入的用户
	选择是否自动生成不存在的用户
	选择是否自动生成用户的默认密码
导出用户	选择需要导出的域、导出格式和编码格式，进行导出
导入活动目录用户	导入活动目录用户

### 30. 全局过滤规则

过滤范围	对系统内所有用户都起作用
规则设置	可分别设置系统接收过滤规则、系统发送过滤规则。规则可根据来源IP、收件人IP、发件人所属部门、收件人所属部门、发件人、接收人、主题、附件名、邮件内容、邮件长度、邮件头字段、邮件发送时间、邮件接收时间、是否包含附件等条件进行判断
执行操作	不执行以后规则、拒绝接收、发送到指定文件夹、转发到指定邮箱、



	自动回复、发送短信、发送彩信、执行 Plugin (Java 处理类) 等相应操作
--	---

### 31. 邮件监控

发送邮件监控	可增加、编辑或者删除规则，编辑选项有规则名称、被监控发件人、接收监控邮件邮箱
接收邮件监控	可增加、编辑或者删除规则，编辑选项有规则名称、被监控收件人、接收监控邮件邮箱
查找（删除）用户邮件	可根据邮件账号、主题、发件人、收件人、日期进行搜索用户邮件

### 32. 邮件审核

邮件审核规则列表	增加、编辑审核规则，可根据来源 IP、收件人 IP、发件人所属部门、收件人所属部门、发件人、接收人、主题、附件名、邮件内容、邮件长度、邮件头字段、邮件发送时间、邮件接收时间、是否包含附件等条件进行设置
----------	--

### 33. 归档服务

归档邮件搜索	支持一般搜索和高级搜索，高级搜索包括发件账号、收件账号、主题、发件人、收件人、内容、附件名、日期和归档类型（即所有、接受、发送）
--------	--





归档邮件列表	显示归档邮件列表，可根据收件账号、日期或者内容进行搜索
--------	-----------------------------

### 34. 系统监控

Webmail 在线用户	查看当前在线的 webmail 用户
邮件队列查看	查看系统的邮件就绪队列和重发队列，并可手工删除队列里指定邮件
SMTP 当前活动会话查看	查看当前活跃的 SMTP 会话，和会话状况
POP3 当前活动会话查看	查看当前活跃的 POP3 会话，和会话状况
IMAP4 当前活动会话查看	查看当前活跃的 IMAP4 会话，和会话状况
远程投递当前活动会话查看	查看当前活跃的 Sendmail 会话，和会话状况
XMPP C2S 服务当前活动会话查看	查看当前的 XMPP C2S 服务对话
智能反垃圾 IP 列表	查看、增加、删除系统垃圾 IP
web 服务器信息	查看 Tomcat 服务器的环境
系统信息	查看系统安装目录和版本号
系统警告信息	查看系统警告信息，如：注册码到期信息



### 35. 反垃圾\反病毒设置

反垃圾参数设置	选择是否启用 RBL 反垃圾查询
	设定 RBL 服务地址
	选择是否启用 RWL 白名单查询
	设定 RWL 服务地址
	选择是否对发送者 IP 进行 DNS 反向解析
	选择是否验证 HELO 域名有效性
黑名单	增加、删除黑名单
	新增黑名单 IP 地址，两种格式:单个 IP 地址，一个网段
	新增黑名单域名
	新增黑名单邮件地址
白名单管理	增加、删除白名单
	新增白名单 IP 地址，两种格式:单个 IP 地址，一个网段
	新增白名单域名
	新增白名单邮件地址



反垃圾引擎	选择启用反垃圾引擎
	设置同域内互发邮件也使用反垃圾引擎
	设置外发邮件也使用反垃圾引擎
	设置系统内用户互发邮件不经过反垃圾过滤
	设置标记为可能垃圾邮件值
	设置标记主题前缀
	设置判定为垃圾邮件值
	设置垃圾邮件主题前缀
	设置判定为系统自动删除值
	设置垃圾邮件处理帐号
	设置最大判断邮件大小
	选择是否启用趋势分析
	选择是否启用灰名单
	设置灰名单开始阻隔时间值
设置灰名单超时时间值	



选择是否启动来源分析
设置反向域名匹配级数
编辑可疑反向域名列表
设定可疑反向域名加分值
选择是否如果 IP 有反向记录则可信
编辑可信反向域名列表
设置 MX 记录不存在评分值
这是发件人格式不正确评分值
设置收件人不匹配评分值
设置发件人与收件人相同评分值
选择是否启用 SpamFilter
垃圾邮件内容评分规则，可根据邮件发件人、接收人、主题、附件名、邮件内容、邮件长度、邮件头字段、邮件发送时间等条件进行判断，并做垃圾邮件评分
设置邮件来源评分规则，可对邮件的来源 IP，域名，邮件地址进行垃圾邮件评分



	设置黑名单（RBL）规则列表
	设置内容 RBL 规则列表，可根据各种 RBL 进行垃圾邮件评分
	选择是否启用白名单
	设定白名单内容规则列表，包括发件人、收件人、主题、附件名、内容、其他邮件头字段、判断是否包含邮件头字段、邮件长度、邮件发送时间、邮件接收时间
	增加、编辑邮件来源白名单，包括 IP 地址、域名、邮件地址
垃圾邮件样本测试	测试垃圾邮件样本
垃圾邮件报告列表	显示发件人、收件人、主题、类型、日期、长度
	选择删除或重新发送垃圾邮件
ClamAV 反病毒引擎设置	选择启用 ClamAV
	选择是否记录反病毒明细日志
	选择同域内互发邮件也使用 ClamAV
	设置最大判断邮件大小
	设置病毒邮件处理帐号
	设置病毒库自动升级间隔



	设置升级失败尝试次数
	设定病毒库版本信息查询地址
	设定病毒库下载地址
病毒邮件报告列表	显示发件人、收件人、主题、类型、日期、长度
	选择删除或重新发送垃圾邮件

### 36. 公告

增加公告	增加新的公告，可文字编辑，插入图片、链接等
删除公告	删除不需要的公告
刷新公告	刷新显示最新发布公告列表

### 37. 公共网络硬盘

公共网络硬盘	显示网络硬盘中所有的文件列表、分配空间、已使用空间、文件总数、剩余空间、当前路径
上传	上传文件到网络硬盘
新建文件夹	建立新文件夹



### 38. 日志查看

系统日志	显示各种日志类型，如：系统信息、IMAP、POP3、SMTP、本地处理服务等，可按日志类型、日志记录层次、开始时间、截止时间、错误号、内容进行日志查找
域操作日志	显示域操作日志列表，可按开始时间和截止时间进行查找，也可根据内容进行模糊查找
用户日志	显示用户日志列表，可按邮件账号、日志类型（Webmail、SMTP、POP3、IMAP、XMPP）、开始时间和截止时间进行查找，也可根据内容进行模糊查找

### 39. 统计分析

流量统计	可根据多种条件进行查找统计,包括发件人、发件域、收件人、收件域、是否模糊匹配、统计类型（即远程投递、本地投递、POP3、SMTP、黑名单阻隔、病毒邮件、垃圾邮件）、分组类型（分为按发件人统计、按发件域统计、按收件人统计、按收件域统计）、开始和截止时间
邮件流量统计图	根据月份进行正常邮件、垃圾邮件与病毒邮件的统计
短信发送查询	根据发件人、手机进行查询，可选模糊匹配，查询类型包括明细查询、按手机统计、按发送人统计，还可按时间进行查询



#### 40. 系统备份

系统备份	可选择备份用户地址本、用户邮件内容和用户网络硬盘内容，还可上传备份
------	-----------------------------------

#### 41. 注册码管理

注册码管理	输入域名、许可域名数、用户数、注册码
-------	--------------------

#### 42. 邮件

收邮件	显示系统收件箱，可以进行刷新、删除、把选中邮件移到文件夹等操作
发邮件	编辑邮件并发送邮件，可以上传附件、使用网络硬盘、定时发送等
地址本	增加、删除、编辑地址以及目录，分为公共地址本、域地址本和个人地址本，并显示系统内各部门结构
邮件搜索	可进行一般搜索或高级搜索，其中高级搜索包括主题、发件人、收件人、内容、附件名、日期和文件夹
文件夹	包括收件箱、草稿箱、已发送邮件、回收站、异常邮件、垃圾邮件、病毒邮件，可选择刷新、删除、把选中邮件移动到文件夹等操作
定时发送邮件	对于定时发送邮件可选择刷新、删除操作
网络硬盘	显示网络硬盘文件列表、上传文件到网络硬盘、新建文件夹等





### 43. 设置

个人设定	设定默认值：每页显示邮件数、发送的邮件默认保存到“已发送邮件”、发送邮件需要回执、保存邮件客户端发送的邮件、发送邮件默认编码、登陆显示页、自动清除垃圾/病毒时间间隔等；设置个人相关信息：昵称、电话、手机、邮编、国家、省、地址等；设置三种个性化签名档
修改密码	修改登录密码
文件夹管理	删除文件夹、文件夹改名、增加文件夹
过滤规则设置	对当前用户起作用
	可根据来源 IP、收件人 IP、发件人、接收人、主题、附件名、邮件内容、字符集、其他邮件头字段、邮件长度、邮件发送时间、邮件接收时间、是否包含附件等组合条件执行相应的过滤作用
	拒绝接收、发送到指定文件夹、转发到指定邮箱、自动回复、发送短信、发送彩信
POP3 收信	设定 POP3 服务器地址、端口、用户名、密码
	选择发送到指定文件夹
	选择接收邮件后，是否删除 POP3 服务器上的邮件
	选择该服务器是否要求安全连接（SSL）



自动转发	选择启用自动转发
	设置转发到的邮箱
	选择是否保存副本在本地邮箱
自动回复	选择启用自动回复
	编辑回复内容
黑名单	个人黑名单设置，包括 IP 地址、域名和邮件地址
白名单	个人白名单设置，包括 IP 地址、域名和邮件地址
短信短语	编辑常用短信短语，包括标题和内容

#### 44. 系统意见

系统意见	编辑系统意见并发送，包括意见主题和意见内容
------	-----------------------

#### 45. 退出

退出	安全退出系统
----	--------



## 培训篇

### 一. 系统管理员培训

序号	培训内容		参加人
1	Email 系统基本原理	Internet 邮件系统	系统管理员
		基本网络协议	
		电子邮件系统传送过程	
		电子邮件技术名义解释	
2	Linux 基础培训		
3	传统电子邮件系统的局限		
4	turbomail 系统介绍	系统结构	
		系统效率	
		对公共协议的支持	
		对平台的支持	
		垃圾信件的处理	
		邮件列表	
		虚拟主机和虚拟域	
		Web Mail	



		系统的可扩展性	
		系统的可管理性	
		支持 Unified Messaging	
		系统安全讲解	
		流行电子邮件系统技术分析	
5	电子邮件系统评估准则		

详细培训参见《turbomail 系统管理员培训手册》

## 二. 操作培训

序号	培训内容		参加人
1	系统管理员功能	多域管理：增加域、修改域、删除域、暂停域	系统管理员
		域空间管理	
		域用户数管理	
		计费管理	
		消息通知发布系统	
		自动报警系统	



		自动备份恢复系统	
		反垃圾引擎	
		病毒防护系统	
		系统监控	
		短信模块配置	
		邮件监控、邮件审批配置	
		组织机构管理配置	
		邮件归档配置	
		MMS 彩信手机 Email 发送的照片显示功能	
		公告功能	
		邮件列表管理、定时批量发信	
2	域管理员 功能	用户管理：增加、删除、修改、暂停、恢复	域管理员
		用户邮箱大小设置	
		域用户批处理开户/数据导入导出	
		用户注册信息修改	
		用户密码修改	



		域公告功能	
		域白名单，域黑名单	
		域过滤规则	
		域邮件监控、域邮件审批	
		邮件列表管理	
		用户别名管理	
3	普通用户 功能	邮箱申请（可选）	普通用户
		修改密码	
		收邮件	
		发邮件	
		读信、回复、转发、彩信照片发送	
		邮箱管理	
		地址本管理	
		视频邮件，语音邮件	
		邮件跟踪	
		短信功能	



	手机邮箱	
	邮件搜索	
	邮件设置	备份邮件
		屏蔽垃圾邮件
		个人签名
		参数设置
		过滤器
		POP 邮件账号
		自动回复
	自动转发	
4	邮件系统监控	系统管理员
5	其它邮件系统使用	普通用户

详细培训参见《turbomail 系统用户培训手册》



## 服务篇

### 一. 服务承诺

针对 turbomail 产品，我们公司一年内免费为客户免费升级并提供免费的服务，一年后，如果继续需要技术服务则收取邮件系统造价的 20%。

技术支持服务是指保障 TurboMail 邮件系统稳定运行所必要的技术服务，包括系统漏洞修补、邮件收发屏蔽解决、系统重装、数据迁移等，服务方式为远程服务和现场服务。在远程技术手段（如 SSH、远程桌面、QQ 远程协助）解决不了的情况下，拓波工程师需根据故障等级的响应时限，提供现场服务。技术支持热线 7x24 小时值班。

### 二. 服务支持体系的构成

#### 2.1 电话支持中心

提供 7\*24 小时热线电话（020-38921969，13928708886），并建立大客户档案，工程师在线提供技术问题咨询和故障诊断。远程在线诊断和故障排除。

对于电话咨询解决不了的问题，经用户授权我们可通过电话或 Internet 远程登录到用户网络系统进行的故障诊断和故障排除。

**【注】**对于购买 turbomail 软件产品用于内部网的客户，工程师不能远程直接登陆诊断的，可以通过电话、传真、Email、论坛、MSN 等方式指导对方完成故障诊断和故障排除。在远程不能解决的情况下，拓波公司工程师在 48 小时内赶到现场解决。

#### 2.2 定期巡查服务

提供的全方位网络技术服务，包括对用户的定期巡查制度，即定期远程诊断，采用先进的网络检测与分析工具对系统进行诊断，提出系统优化建议与措施。专人进行客户支持。

**【注】**定期巡查工作由拓波公司协助完成。巡查时间为一年一次。

服务等级以及划分





### 三. 故障等级设定

严格按照故障等级划分标准，将邮件系统的故障划为四级

一级故障：现有的网络停机，或对最终用户的业务运作有重大影响

二级故障：现有网络的的操作性能严重降级，或由于网络性能失常严重影响用户业务运作。

三级故障：网络的操作性能受损，但大部分业务运作仍可正常工作。

四级故障：在产品功能、安装或配置方面需要信息或支持，对用户的业务运作几乎没有影响。

优先级的划分及处理

一级优先权：拓波公司将全天候调集所有必要的资源来排除故障，在 4 小时内提供解决方案或替代方法。

二级优先权：拓波公司将全天候调集所有必要的资源来排除故障，在 12 小时内提供解决方案或替代方法。

三级优先权：拓波公司将全天候调集所有必要的资源来排除故障，一般在 5 天内提供解决方案或替代方法。

四级优先权：拓波公司将全天候调集所有必要的资源来排除故障，一般在 7 天内提供解决方案或替代方法。