邮件系统中的单元往往会有相互重复的功能，对于初学者的我来说，肯定是需要好好整理归纳的。本文会以传统的邮件收发模式为模型，结合 Postfix 这个邮件服务器实现来说明其结构原理。会穿插一些 DNS 的相关知识，正解和反解对于邮件服务器是比较重要的，对于如何处理垃圾邮件、病毒也有会说明。希望整理出一个适用的小型邮件服务器实例（Webmail+ 密码认证方式管理的客户端）------搭起来 + 垃圾/广告/病毒过滤 + 账户安全性 + 隐私。

邮件组成

- 符合 RFC5322 的邮件头和邮件主体，就邮件头而言：1）针对收信端有：*To* 直接收信者、*Cc* 抄送者、*Bcc* 暗送者等；2）针对发送端有：*From* 最原始发信者、*Sender* 其他发信者、*Reply-To* 设置回信地址非原始地址等。
- 符合MIME规范的非文本附件

明确几个定义

MUA（**Mail User Agent**）：一个用于收发并管理邮件的用户客户端，仅仅在用户运行它的时候才会运作，一般运行在个人电脑（本地）上，当发信时，MUA 会去主动连接 MSA 或者 MTA 以处理用户的发信请求，MSA 和 MTA 都采用了 smtp 协议，但是又有少许不同，比如 MSA 使用的是 587 端口而 MTA 使用的是 25 号端口。现在的验证模式基本不会由邮件服务器来直接管理允许发信者的 IP 地址，因为在公网 IP 资源不够用总是动态分配的情况下，这是不合理的。所以验证的工作会要求 MUA 提供用户名和密码在服务器端校验。当然也有一个非标准的 SSL 加密 smtp 协议，走的是 465 端口，但是兼容性很差，不予考虑。当收信时，信件由 MTA 预先保留到 mailbox 下（一般是以 mbox 格式保存在用户家目录下），当 MDA 检测到 MUA 可以通讯的时候便将信件发送到客户端。客户端下载信件有两种独立的方法：一个是 POP（Post Office Protocol），这种方法每当邮件从服务器下下载下来之后，服务器上不再保留邮件，只能下载一次，意味着不能多终端查看邮件，且无法对邮件标记为已查看、已回复或者已转发；另一种方法是 IMAP（Internet Message Access Protocl），这个可以保留邮件到服务器上，那么上述的弊端就不见了。

MSA（**Mail Submission Agent**）：一个用户接收从 MUA 提交的电子邮件，并协助 MTA 做邮件传递工作的程序。目前很多的 MTA 已经包含了 MSA 的功能,*MSA* 处理发信的请求，*MTA* 处理收信的请求, 这句话我查了很久，还是没有明白它们两个到底是如何分工的，MSA 是否可以不依赖于 MTA 而单独工作，根据目前查到的信息来看，MSA 仅仅是分立出来以获取以下几点好处，本身还是需要依赖 MTA 传递邮件的：

- 因为 MSA 直接与 MUA 交互，所以可以修正邮件的一些格式上的错误，比如日期、邮件 ID、收件人信息等。并且或许可以马上给写信人也就是客户端报告错误而不需要等到 MTA 已经把邮件发送完毕后才发现错误再向写信人报告，我认为这个是非常有用的。
- 很多 ISP 和机构网络环境为了抑制垃圾邮件而限制了连接远程 MTA 上 25 端口的功能，MSA 因为可以使用 587 端口，从而使得网络使用的灵活性大大提升。
- MSA 和 MTA 的分工工作方式可以让 MTA 拒绝邮件转发变得更加简单，只需要将收件人非指向本地服务域名的邮件当作垃圾处理即可。与此同时，MSA 就需要接受发往互联网上任何收件地址的信息，好在可以设置仅接受已经验证过的发信客户端。
- 还有就是 MSA 和 MTA 可以设置不同的策略用于屏蔽垃圾邮件。大多数的 MSA 需要完整的用户名和密码验证，通过这样子的机制就可以很轻易地发现发信者是谁，这样子如果有人发送了垃圾邮件，肯定是要为其负责的。因为在随机域名间建立信赖关系基本上是不可能的，也无法像上述通过用户和密码来验证不同域名间的用户关系（不然这个世界只要一个用户名就可以走天下了），所以被设置为收信的 MTA 就需要建立一个完整的垃圾邮件屏蔽机制（往往依赖本地的一些规则或者第三方的鉴定机构），为了区别垃圾邮件和合法邮件，同时也需要一个排错机制，毕竟系统有时候可能也会因为本地规则不完善或者第三方机构误收录而出错。这一点真的很重要，MSA 和 MTA 分立后可以通过用户名密码验证基本忽略邮件提交程序的垃圾邮件检测。

MTA（Mail Tansfer Agent）：这个可以说是整个邮件系统的核心了，DNS 下的 MX 记录也是指的提供 MTA 服务的主机。MTA 可以从另一个 MTA、一个 MSA 或者直接从 MUA 下获取邮件，通过 SMTP 协议传输邮件。当信件的收件人邮箱并非本机管理的时候，这个邮件就会被转发到另一个 MTA（黑函可能就是这样子出现的），每转发一次，就会在邮件头信息添加一个跟踪记录（Received------服务器地址，越后添加的越靠前）。如何选择下一跳的 MTA 服务器是由 SMTP 协议描述的，不过 MTA 服务器本身也可以指定自定义路由。当 MTA 确定了接收到的邮件就是由自己处理的时候，就会把邮件传递给 MDA 做分发，并记录 Return-Path（用户 @ 服务器地址）到邮件头。Postfix 下针对 MTA 的设置非常多，在构建结构图前，我会先把常用的设置整理一遍。

MDA（Mail Delivery Agent）：在互联网邮件体系中，MTA 是通过它来将邮件分发给各个用户，一般是储存在用户服务器端的 mailbox 中。

MRA（Mail Retrieval Agent）：这个其实是一个技术上的定义说明，并不指代特殊的一个组件，详细的可以看下述的说明图。

Postfix 下常见的设置

关于 Postfix 的结构可以看看这里，看了这个结构说明就可以发现：Postfix 可以实现 MSA、MTA、MRA、MDA 的功能，可以说一个 Postfix 就搞定了，关于 Postfix main.cf 下的配置有几百种，这边仅仅列举重要的，也是学习的一个手段。配置文件 main.cf 内常用的参数设置方式有 4 种：

1. 单一值
2. 通过逗号、``'' 或者空格起行的来分隔设定值
3. 直接将参数放在文件里面后指向指定文件
4. 通过 type:table 这样子的模式来设定值，详细的看Postfix Lookup Table。

mydomain：这个定义的就是本服务器在互联网中属于哪一个域名，默认是 myhostname 值去掉由. 分隔的第一个字符后所得的值，可以不设置。参数设置方法：1

myhostname：这个比较重要，建议采用 FQDN 格式，比如：mail.bekcpear.io。参数设置方法：1

myorigin：这个就是邮件发信地点了，比如在邮件头的 mail from 下显示。一般设置为 myhostname 即可，但是根据官方的文档来看，说如果一个域名下由多台邮件服务器，应该将这个值设置为域名，并做好别名数据库，分别指向不同用户，不是很懂，暂且忽略。

mydestination：定义的是可以被 MDA 分发到的主机，默认值是：`mydestination = $myhostname, localhost.$mydomain, localhost`。针对目的地的用户名是在/etc/passwd 和/etc/alias 这两个文件下设置的，注意虚拟域名有其单独设置的地方，不要在这边设置；备用的 MX 记录也不是设置在这边的。参数设置方法：2/3/4

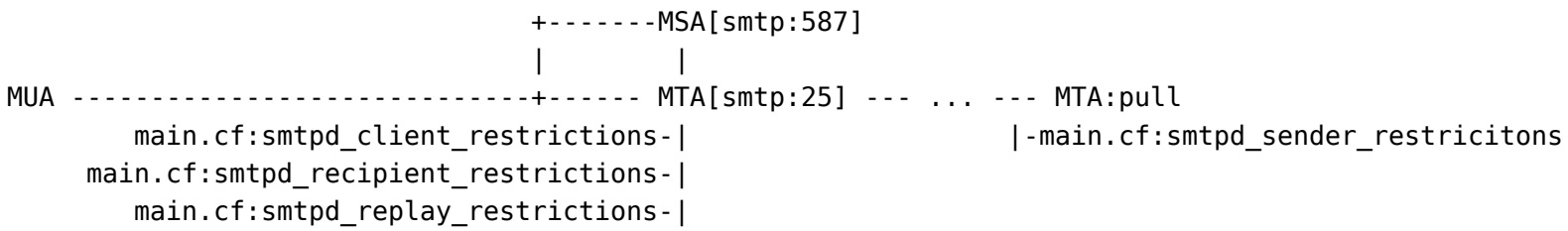
mynetworks：这个很重要，是设置的信任网络，这个设置下的网络地址可以很轻松的通过这个邮件服务器来中转或者发送邮件，所以设置需要注意。设置了这个值之后，会导致 mynetworks_style 的设置失效。所以关于 mynetworks_style 的就不写了。参数设置方法：2/3/4

relay_domains：这个是用于判断邮件的目的域名非本服务器域名时是否属于本参数内，属于了才会对其进行转发，否则就会将有点丢弃。所以猜想是否个人使用的邮件服务器完全没有必要设置 MX 记录，那就可以不涉及本地邮件转发的问题了。详细的实际使用后更新本内容。参数设置方法：2/3/4

smtpd_client_restrictions：用于限制允许连接的客户端，默认是空的就是所有的地址都可以连接。最基本需要设置的是两个值：1）check_client_access

传统 **Mail Server** 结构图解 **(**结合 **Postfix** 设置**)**

从发邮件到目的MTA收件:



目的MTA分发邮件: