电子邮件原理

第一章 电子邮件的工作原理

1．互联网 TCP/IP 的基本结构

今 天的互联网（Internet）的原形是 1969 年建立的 APARNET。在互联网发展史上具有决定意义的一件事是在 1983 年 1 月 1 日，APARNET 正式转换成 TCP/IP 协议的网络。正是 TCP/IP 的出现，才使得互联网得以在全世界的范围内迅速发展并具有今天的规模。

根据 TCP/IP 协议，互联网分为 4 层，加上最底层的硬件层一共是 5 层：

物理层：
对 应于网络的基本硬件，这也是 Internet 物理构成，即我们可以看得见的硬件设备，如 PC 机、互连网服务器、网络设备等，必须对这些硬件设备的电气特性 作一个规范，使这些设备都能够互相连接并兼容使用。网络接口层：它定义了将数据组成正确帧的规程和在网络中传输帧的规程，帧是指一串数据，它是数据在网络 中传输的单位。

互联网层：
本层定义了互联网中传输的“信息包”格式，以及从一个用户通过一个或多个路由器到最终目标?quot;信息包"转发机制。

传输层：
为两个用户进程之间建立、管理和拆除可靠而又有效的端到端连接。

应用层：
它 定义了应用程序使用互联网的规程。电子邮件的 SMTP 协议就建立在这一层。Internet 的核心层是网络层和传输层，相应的核心协议是 IP 协议和 TCP 协议。IP 协议的主要功能包括无连结数据报传送 、数据报寻径以及差错处理三部分。IP 协议的特点是点到点的，IP 对等实体间的通信不经过中间机器，对等实体所在的机 器位于同一物理网络，对等机器之间有直接的物理连接。IP 层的主要功能是屏蔽下面物理层的差别，向上一层提供一致的数据格式。所有要传输的数据，被按照一 定的格式分组封装层 IP 数据报，数据报单元通过寻径等机制进行传输，在接收方数据报进行重组，得到最初要传送的数据。由于 IP 协议是不可靠的数据传输协 议，由于网络的拥塞而发生的数据丢失等情况是不可避免的，因此 Internet 还必须有一定的控制重传机制，这就是差错与控制报文协议(ICMP)。尽管计算机通过安装 IP 软件，从而保证了计算机之间可以发送和接收数据，但 IP 协议 还不能解决数据分组在传输过程中可能出现的问题。因此，若要解决可能出现的问题，还需要 TCP 协议来提供可靠的并且无差错的通信服务。TCP 协议被称作一 种端对端协议。这是因为它为两台计算机之间的连接起了重要作用：当一台计算机需要与另一台远程计算机连接时，TCP 协议会让它们建立一个连接、发送和接收数据以及终止连接。传输控制协议 TCP 协议利用重发技术和拥塞控制机制，向应用程序提供可靠的通信连接，使它能够自动适应网上的各种变化。即使在 Internet 暂时出现堵塞的情况下，TCP 也能够保证通信的可靠.Internet 是一个庞大的国际性网络，网路上的拥挤和空闲时间总是交替不定的，加上传送的距离也远近不同，所以传输数据所用时间也会变化不定。TCP 协议具有自动调 整"超时值"的功能，能很好地适应 Internet 上各种各样的变化，确保传输数值的正确。

IP 协议只保证计算机能发送和接收分组数据，而 TCP 协议则可提供一个可靠的、可流控的、全双工的信息流传输服务。虽然 IP 和 TCP 这两个协议的功能不 尽相同，也可以分开单独使用，但它们是在同一时期作为一个协议来设计的，并且在功能上也是互补的。只有两者的结合，才能保证 Internet 在复杂的环境下正常运行。凡是要连接到 Internet 的计算机，都必须同时安装和使用这两个协议，因此在实际中常把这两个协议统称作

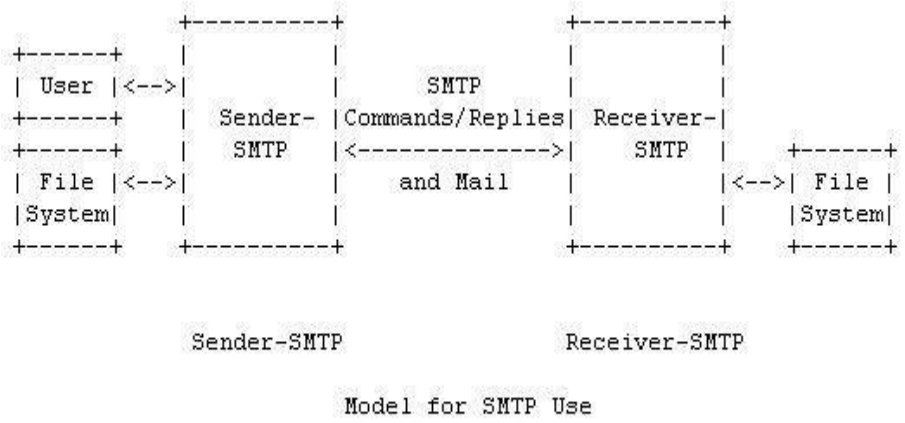
TCP/IP 协议。 TCP/IP 协议除了 TCP 协议和 IP 协议，还包含物理接口和 IP 层之间的 ARP/RARP 协议，应用层的 FTP 协议、SMTP 协议和 BOOTP 协议等，所用的这些协 议构成 Intenet 的 TCP/IP 协议族。

2．SMTP 的基本结构

SMTP （Simple Mail Transfer Protocol）协议是为了保证电子邮件的可靠和高效传送。TCP/IP 协议的应用层中包含有 SMTP 协议，但事实上它与传输系统和机制无关，仅要求一个可靠的数据流通道。它可以工作在 TCP 上，也可以工作在 NCP, NITS 等协议上。在 TCP 上，它使用端口 25 进行传输。SMTP 的一个重要特点是可以在可交互的通信系统中转发邮件。

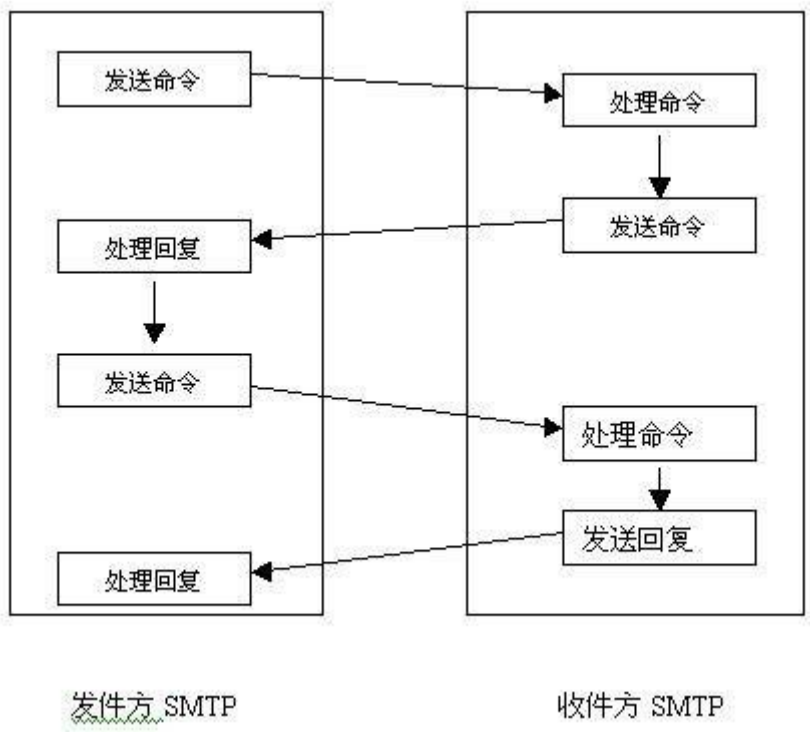
2.1 SMTP 的模型

SMTP 提供了一种邮件传输的机制，当收件方和发件方都在一个网络上时，可以把邮件直传给对方；当双方不在同一个网络上时，需要通过一个或几个中间服务器转发。 SMTP 首先由发件方提出申请，要求与接收方 SMTP 建立双向的通信渠道，收件方可以是最终收件人也可以是中间转发的服务器。收件方服务器确认可以建立连 接后，双发就可以开始通信。下面是 SMTP 的模型示意图。



Model for SMTP Use

发 件方 SMTP 向收件方发处 MAIL 命令，告知发件方的身份；如果收件方接受，就会回答 OK。发件方再发出 RCPT 命令，告知收件人的身份，收件方 SMTP 确认是否接收或转发，如果同意就回答 OK；接下来就可以进行数据传输了。通信过程中，发件方 SMTP 与收件方 SMTP 采用对话式的交互方式，发件方提出要求，收件方进行确认，确认后才进行下一步的动作。整个过程由发件方控制，有时需要确认几回才可以。



为了保证回复命令的有效，SMTP 要求发件方必须提供接收方的服务器及邮箱。邮件的命令和答复有严格的语法定义，并且回复具有相应的数字代码。所有的命令由 ASCII 码组成。命令代码是大小写无关的，如 MAIL 和 mail 、mAIL 是等效的。

2.2 SMTP 的基本命令

SMTP 定义了 14 个命令，它们是：

HELO <SP> <domain> <CRLF>
MAIL <SP> FROM:<reverse-path> <CRLF>
RCPT <SP> TO:<forward-path> <CRLF>
DATA <CRLF>
RSET <CRLF>
SEND <SP> FROM:<reverse-path> <CRLF>
SOML <SP> FROM:<reverse-path> <CRLF>
SAML <SP> FROM:<reverse-path> <CRLF>
VRFY <SP> <string> <CRLF>
EXPN <SP> <string> <CRLF>
HELP [<SP> <string>] <CRLF>
NOOP <CRLF>
QUIT <CRLF>
TURN <CRLF>

其中使得 SMTP 工作的基本的命令有 7 个，分别为：HELO 、MAIL 、RCPT 、DATA 、REST 、NOOP 和 QUIT ．下面分别介绍如下。

HELO--发件方问候收件方，后面是发件人的服务器地址或标识。收件方回答 OK 时标识自己的身份。问候和确认过程表明两台机器可以进行通信，同时状态参量被复位，缓冲区被清空。

MAIL--这个命令用来开始传送邮件，它的后面跟随发件方邮件地址（返回邮件地址）。它也用来当邮件无法送达时，发送失败通知。为保证邮件的成功发送，发件方的地址应是被对方或中间转发方同意接受的。这个命令会清空有关的缓冲区，为新的邮件做准备。

RCPT --这个命令告诉收件方收件人的邮箱。当有多个收件人时，需要多次使用该命令，每次只能指明一个人。如果接收方服务器不同意转发这个地址的邮件，它必须报 550 错误代码通知发件方。如果服务器同意转发，它要更改邮件发送路径，把最开始的目的地（该服务器）换成下一个服务器。

DATA-- 收件方把该命令之后的数据作为发送的数据。数据被加入数据缓冲区中，以单独一行是"<CRLF>.<CRLF>"的行结束数据。 结束行对于接收方同时意味立即开始缓冲区内的数据传送，传送结束后清空缓冲区。如果传送接受，接收方回复 OK。

REST--这个命令用来通知收件方复位，所有已存入缓冲区的收件人数据，发件人数据和待传送的数据都必须清除，接收放必须回答 OK.

NOOP--这个命令不影响任何参数，只是要求接收放回答 OK, 不会影响缓冲区的数据。

QUIT--SMTP 要求接收放必须回答 OK，然后中断传输；在收到这个命令并回答 OK 前，收件方不得中断连接，即使传输出现错误。发件方在发出这个命令并收到 OK 答复前，也不得中断连接。

下面是 SMTP 答复中用到的代码和含义：

500 Syntax error, command unrecognized
[This may include errors such as command line too long]
501 Syntax error in parameters or arguments
502 Command not implemented
503 Bad sequence of commands
504 Command parameter not implemented
211 System status, or system help reply
214 Help message
[Information on how to use the receiver or the meaning of a
particular non-standard command; this reply is useful only to the human user]
220 <domain> Service ready
221 <domain> Service closing transmission channel
421 <domain> Service not available, closing transmission channel
[This may be a reply to any command if the service knows it must shut down]
250 Requested mail action okay, completed
251 User not local; will forward to <forward-path>
450 Requested mail action not taken: mailbox unavailable
[E.g., mailbox busy]
550 Requested action not taken: mailbox unavailable
[E.g., mailbox not found, no access]
451 Requested action aborted: error in processing
551 User not local; please try <forward-path>
452 Requested action not taken: insufficient system storage
552 Requested mail action aborted: exceeded storage allocation
553 Requested action not taken: mailbox name not allowed
[E.g., mailbox syntax incorrect]
354 Start mail input; end with <CRLF>.<CRLF>
554 Transaction failed

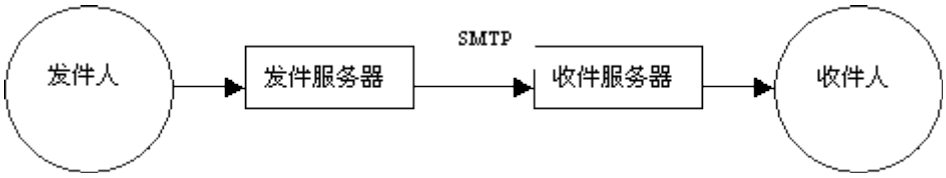
最后，让我们看一个 RFC821 中给出的例子。这封信是 Smith 在主机 Alpha.ARPA 发给主机 Beta.ARPA 上的 Jones,Green 和 Brown.并且假定两台主机在同一个网络上。

S: MAIL FROM:<Smith@Alpha.ARPA>
R: 250 OK
S: RCPT TO:<Jones@Beta.ARPA>
R: 250 OK
S: RCPT TO:<Green@Beta.ARPA>
R: 550 No such user here
S: RCPT TO:<Brown@Beta.ARPA>
R: 250 OK
S: DATA
R: 354 Start mail input; end with <CRLF>.<CRLF>
S: Blah blah blah...
S: ...etc. etc. etc.
S: <CRLF>.<CRLF>
R: 250 OK

邮件最后被对方接受。

3．电子邮件的工作原理

电子邮件与普通邮件有类似的地方，发信者注明收件人的姓名与地址（即邮件地址），发送方服务器把邮件传到收件方服务器，收件方服务器再把邮件发到收件人的邮箱中。如下图所示：



更进一步的解释涉及到以下几个概念:

MUA -- Mail User Agent, 邮件用户代理，帮助用户读写邮件；

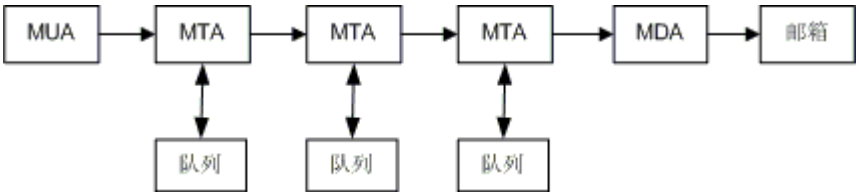
MTA -- Mail Transport Agent, 邮件传输代理，负责把邮件由一个服务器传到另一个服务

器或邮件投递代理；

MDA -- Mail Delivery Agent, 邮件投递代理，把邮件放到用户的邮箱里。

整个邮件传输过程如下：

目前使用的 SMTP 协议是存储转发协议，意味着它允许邮件通过一系列的服务器发送到最终目的地。服务器在一个队列中存储到达的邮件，等待发送到下一个目的地。下一个目的地可以是本地用户，或者是另一个邮件服务器，如下图所示。



如果下游的服务器暂时不可用，MTA 就暂时在队列中保存信件，并在以后尝试发送。

4. 电子邮件的信头结构及分析

4.1 邮件的结构

在最高层，邮件的结构是非常简单的，用户从终端机上看到的邮件格式一般为：

1. From: user1@domain1.com
2. To: user2@domain2.com
3. Subject: Explaination of mail format
4. Date: Thu, 1 Apr 1999. 10:00:00 GMT
5. Hi, Jack
7. This mail is to explain you the mail format
8. - - - -
9. Thanks
10. Bob

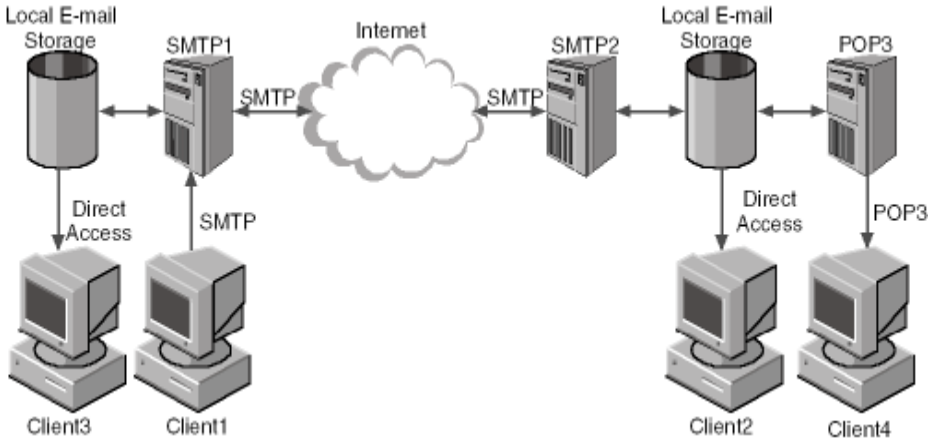
其 中， 1~~4 行称作信件信头(message header) 6~~10 行描述信件要表达的内容，称为信体 (message body)。第

5 行是空行，根据 RFC822 的要求，信头和信体之间必须加入一空行。[i]信头通常包含字段 From, To, Subject 和 Date,有的邮件还包含 cc,bcc 等字段。

4.2 邮件的信头

事实上，邮件在传输过程中，服务器要把它打包成一个数据对象，包括上面的信件和一个信封。邮件的投递是依靠信封上的地址或信封信头（envelop address 或 envelop header），而不是上面讲的信件上的地址。

从 表面上看，一封邮件是从发件人的机器直接传送到收件人的机器，但通常这并不正确，一封邮件发送和接受过程至少要经过四台计算机。参考下图所示。用户通常在 自己的电脑前编写阅读邮件，我们把它叫做客户端 （client 1~~4 ）。大部分组织里，都是用一台专门的机器处理邮件，称作邮件服务器 (SMTP1, SMTP2). 如果用户是从家里拨号上网，那末邮件服务器是 ISP 提供的。



当 某个用户在自己的电脑 Client1 前编写完一个邮件，然后把它发送到他的 ISP 的邮件服务器 SMTP1。此时她的机器已经完成了所有的工作，但邮件服务器 SMTP1 还必须想法把邮件发送到目的地。SMTP1 通过阅读信头或信封上的地址，找到收件认得邮件服务器 SMTP2, 然后与该服务器建立连接，把邮件发到收件人的服务器上，等待收件人来取阅。

下 面我们将通过一个例子说明整个邮件传送过程及邮件的信头变化。假设发件人的名字叫 Sender, email 地址是 sender@domain1.com 使用的电脑名字叫 client1， IP 地址是 [111.11.1.1] (假设的地址)。 收件人的名字叫 receipt, email 地址是 receipt@domain2.com, 使用的电脑的名字叫 client2，IP 地址是 [222.22.2.2] (假设的地址)。当邮件编辑完传送给其邮件服务器 mail.domain1.com 时，邮件的信头格式为：

From: sender@domain1.com

To: receipt@domain2.com

Date: Tue, Mar 18 1998 15:36:24 GMT

X-mailer:Sendmail 8.9.0

Subject: Greetings

当邮件服务器 mail.domain1.com 把邮件传到接收方的服务器 mail.domain2.com 时，接受方服务器会在信头上记录下有关的计算机信息，邮件的信头变成：

Received: from client1.domain1.com (client1.domain1.com [111.11.1.1]) by mail.domain1.com (8.8.5) id 004A21; Tue, Mar 18 1998 15:3 7:24 GMT

From: sender@domain1.com

To: receipt@domain2.com

Date: Tue, Mar 18 1998 15:36:24 GMT

Message-Id: <client1254556544-45556454@mail.domain1.com>

X-mailer:Sendmail 8.9.0

Subject: Greetings

当收件人服务器 mail.domain2.com 把邮件接收并存初下来，等待收件人来阅读时，邮件的信头将会再加入一条记录：

Received: from mail.domain1.com (mail.domain1.com [111.11.1.0]) by mail.domain2.com (8.8.5/8.7.2) with ESMTP id LAA20869; Tue, Mar 18 1998 15:39:44 GMT

Received: from client1.domain1.com (client1.domain1.com [111.11.1.1]) by mail.domain1.com (8.8.5) id 004A21; Tue, Mar 18 1998 15:37:24 GMT

From: sender@domain1.com

To: receipt@domain2.com

Date: Tue, Mar 18 1998 15:36:24 GMT

Message-Id: <client1254556544-45556454@mail.domain1.com>

X-mailer:Sendmail 8.9.0

Subject: Greetings

上面整个记录就将是收件人看到的完整的邮件信头。让我们逐行看一下信头中各行的含义：

Received: from mail.domain1.com (mail.domain1.com [111.11.1.0]) by mail.domain2.com (8.8.5/8.7.2) with ESMTP id LAA20869; Tue, Mar 18 1998 15:39:44 GMT

这封信是从一台自称为 mail.domain1.com 的机器上接收的；这台机器的 IP 地址是[111.11.1.0]，真实名字就是标称名字 mail.domain1.com; 接收方的机器名称是 mail.domain2.com, 运行的邮件服务器是 Sendmail, 版本 (8.8.5/8.7.2) 。接收方机器给邮件的编号是 ESMTP id LAA20869， 接收到的时间是 Tue, Mar 18 1998 15:39:44 GMT。

Received: from client1.domain1.com (client1.domain1.com [111.11.1.1]) by mail.domain1.com (8.8.5) id 004A21; Tue, Mar 18 1998 15:37:24 GMT

这条记录表明信件是由机器 client1.domain1.com (IP 地址是 [111.11.1.1]) 在 Tue, Mar 18 1998 15:37:24 GMT 交给 mail.domain1.com，并赋给编号 id 004A21。

From,TO ,Date 和 Subject 都易于理解，分别指明发件人，收件人，信件编辑日期及信件主题。

Message-Id: <client1254556544-45556454@mail.domain1.com>

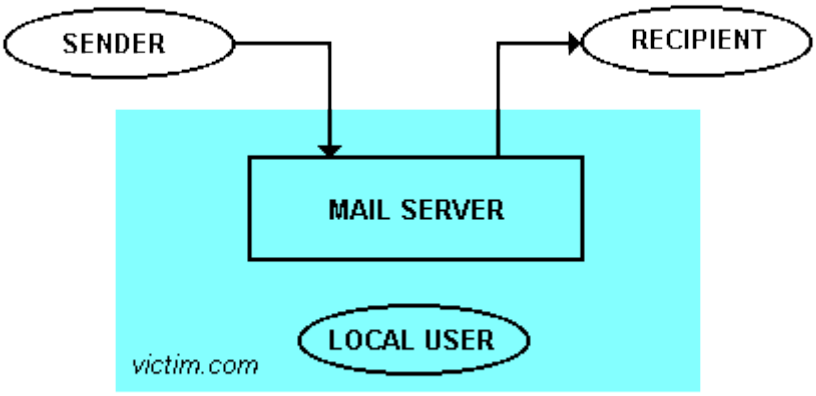
这是由发件方邮件服务器赋给这封邮件的编号。与其它编号不同，这个编号自始至终跟随邮件。

第二章 OPEN RELAY 的原理及测试

1.OPEN RELAY 的原理

由于技术的原因，在 80 年代前，网络还不是很健全，机器之间很少能直接对话发送邮件，人们必须得找出一条有效的连接通路来，然后信件沿着通路一步一步传送到目的地。SMTP 协议中就明确指出当邮件在不同的网络间传送时，需要借助中间服务器的 RELAY。

邮件在收件方和发件方之间会经过毫不相干的第三方服务器，这就是邮件转发 (RELAY)。 如下图所示：



图中的 MAIL SERVER 是可以对要求转发的邮件进行限制的，如只转发来自某个域的邮件或来自于某些 IP 得邮件。如果转发没有任何限制，就被称为 OPEN RELAY 或 THIRD PARTY RELAY。
从 历史上看，relay 曾经发挥过重要作用。而且当时这些工作主要靠手工来做，就像我们今天通过邮局发一封信一样。假如我想从沈阳发一封信件到深圳，我再信封上写好收信地址深 圳，邮局就需要找到定义的运送路线： 沈阳，北京，郑州，长沙，广州，深圳。甚至还要长一些。其中很重要一点是每一个中继站都能很好的理解这封信将被送到哪里，下一个接收站是谁。在电子邮件 里，这就相当于每个中继服务器清楚下一个服务起是谁，这就是邮件的转发。

目前，正常邮件转发已经不再必要，相反，无限制转发常常被发送垃圾邮件的人利用，隐藏真实的邮件来源，让别人以为是从另外的 ISP 发出的信件；同时，也把大量的处理工作转移到别人机器上。
由 于前面提到的历史的原因，最初的绝大多数邮件服务器都允许 OPEN RELAY 的。今天，大部分邮件服务器升级版本已经在缺省设置中关闭了 OPEN RELAY, 如 Sendmail 从 8.9.3 版本开始，Exchange Server 从 5.5 版本开始关闭了 open relay。有的服务器虽然没有相应的升级版本，也都提供了关闭 open relay 的方法，如在 NOTES SERVER 的配置文件 notes.ini 中加入一行：SMTPMTA_REJECT_RELAYS=1。但由于很多服务器管理员的疏忽而没能及时的修补这些安全漏洞，被利用来转发垃圾邮件。

2 如何确认邮件服务器是否 RELAY

假设要测试的 IP 是 202.112.0.0. 可以使用下列命令进行测试，文中的绿色斜题字为测试邮件服务器的反馈信息：

#telnet 202.112.0.0 25
Trying 202.112.0.0...
Connected to 202.112.0.0.
Escape character is '^]'.
220 dns.ccert.edu.cn ESMTP Sendmail 8.11.1/8.11.1; Sat, 30 Jun 2001 21:07:10 +0800
helo mydomain
250 dns.ccert.edu.cn Hello point.ccert.edu.cn [202.112.50.3], pleased to meet you
mail from:nobody@yahoo.com
250 2.1.0 nobody@#yahoo.com... Sender ok
rcpt to:nobody@hotmail.com
550 5.7.1 nobody@hotmail.com... Relaying denied

最后的 Relaying denied 表明该服务器已经安全设置，不会再 relay 无关邮件了。如果显示的结果是下面的样子，这表明服务器可以转发任何人的邮件。

rcpt to:nobody@hotmail.com
250 nobody@hotmail.com... Recipient ok
data
354 Enter mail, end with "." on a line by itself
this is a test of the relay
.

250 VAA00289 Message accepted for delivery

除了用上面的命令行的方法测试外，下面的链接提供了一个测试工具，只需输入 IP 即可。
http://www.abuse.net/relay.html

第三章 垃圾邮件的文化与历史

1. 什么是垃圾邮件

经 常上网的人和经常使用电子邮件的人可能会收到一些莫名其妙的电子邮件，内容大都是一些产品介绍，发财之道等。开始你可能并不在意，删掉了之；但你可能会发 现你还会不断收到类似的邮件，常常令你烦恼不已。这就是我们这里要研究的垃圾邮件。垃圾邮件就是那些你并不希望收到，并且你也没有订阅过，但却被人利用电 子邮件的特点强行塞入你的邮箱的商业广告，产品介绍，发财之道等内容的电子邮件。垃圾邮件一次发给很多人，在 Internet 上同时传送很多副本。

垃 圾邮件和那些强行塞入你家门缝或信箱中的传单又有本质的区别。这些传单的印刷和分发的成本由生产该产品的厂家来承担。而这些电子垃圾邮件的成本却是由你来 支付的。这些垃圾邮件通常是盗用别人的服务器（也可能是你的服务器），使用别人的带宽来传送的。这也就是为是什么垃圾邮件遭到了如此强烈的谴责，而那些散 发传单的人却没有。

2．垃圾邮件的起源与历史

垃圾邮件是 Internet 技术发展的产物。。与其它先进技术一样，在为人类服务的同时，不可避免的被另外一些人用作相反目的。

首 次关于垃圾邮件的记录是 1985 年 8 月一封通过电子邮件发送的链锁信，一直持续到 1993 年。 1993 年 6 月份，在 Internet 上出现了"发财之道（Make Money Fast）"的电子邮件。历史上比较著名的事件是 1994 年 4 月份，Canter 和 Siegel 的法律事务所把一封信发到 6000 多个新闻组，宣传获得美国国内绿卡的法律支持。这是第一次使用 Spam (垃圾邮件)一词，用来描述新闻或电子邮件的主动性发布。同时，垃圾邮件也开始引起了人们的注意和反感。一些触觉敏锐的商人立刻意识到了电子邮件带来的商 机，许多人开始利用电子邮件作商业广告，95 年 5 月有人写出了第一个专门的应用程序 Floodgate，一次可以自动把邮件发给很多人。紧接着在 8 月份，就有人拿两百万个邮件地址出售。垃圾邮件越来越多与商业联系起来，96 年的 4 月份， 人们开始使用 UCE(Unsolicited Commercial Email) 来称呼垃圾邮件，并开始积极想办法阻止垃圾邮件在 Internet 上泛滥。到了 96 年 3 月，有人提出了 SpamBlock 的方法，例如使用 REMOVE.TO.REPLY 的工具来过滤邮件地址。随着过滤垃圾邮件技术的发展以及人们对发送垃圾邮件者的谴责，垃圾邮件的制造者不得不采取更为隐蔽的技术，比如伪造信头中的发件 人，域名，邮件地址等。然而这些方法还是逃不出 IP 的地址的过滤。于是，垃圾邮件的制造者又开始寻找更为安全的做法，97 年 3 月，他们开始把目光转向 OPEN RELAY。OPEN RELAY 是当时解决 Internet 路由的一种很好的方法，当然存在以上安全漏洞。很快，大部分商业垃圾邮件就开始利用别人的服务器使用邮件转发的办法发送。这样做的另一个原因是可以节省邮 件发送者的钱，盗用别人的资源。在过去的几年里，人们已经越来越多的意识到控制 Internet 上垃圾邮件的重要性，世界各地成立了很多组织反对垃圾邮件，如 MAPS,ORBS, SpamCorp. Junckemail.org 等，从技术上，法律上做着努力。

3. 垃圾邮件的分类

垃圾邮件从内容上看，主要是商业广告性质的邮件；另外，由少量政治，团体组织的宣传邮件。
从 邮件的发送形式上看，有直接发送和第三方转发两种。所谓直接发送，就是邮件的发送者使用自己的服务器，IP 地址，自己的网络资源传送这些邮件。对于接收者来说，如果长期收到这样的邮件，可以采取过滤该 IP 地址的办法或者根据邮件内容过滤的方法；但如果只是偶尔 收到，就很难找到有效的方法了。使用这种方法，邮件发送人的真实情况很容易被查出来，因此也很少有人使用。目前使用更多的是使用第三方服务器转发。当然大 多都是未经该服务器管理员同意情况下使用的。由于历史的原因，Internet 上有很多服务器可以转发第三方邮件。对于这种垃圾邮件，只要关闭有关服务器的转发功能就可以了。

4．我们为什么要反对垃圾邮件

在 讨论这个问题之前，让我们看一下为什么会有人采用这种方式做广告。总结一下，大致归于两点原因：低成本和易于匿名。发送 10 万封电子邮件的成本低于 200 美圆，花 100 美圆就可以买到 100 万个邮件地址列表。一个业余的邮件广告人只需要一台普通的电脑，一个 Internet 帐户加上一个免费的邮件客户端软 件就足够了。更为专业一点的，投资几百美圆就可以买到专门的应用软件，每小时可以发送 25 万个邮件，并且自动伪装了邮件的信头；并且还可以不断的从 WEB 上截获邮件地址。由于低廉的成本，即使只有很少很少的部分得到了反馈，就足以支付这些费用了，比起昂贵的其它方式的广告自然很划算。然而，事实上成本低只 是针对于那些用邮件做广告的人，其他的成本由 ISP 和收件人承担了。

另外，从整个 Internet 的资源利用来看，目前带宽资源还比较有限。垃圾邮件里的信息几乎没有什么价值，每次发送上万，百万，甚至上亿份，占用了大量的带宽资源，严重时甚至拥塞整 个 Internet 链路，中断 Internet 的部分线路的运营。 这是 ISP 和服务器管理员所不希望看到的。据 CAUCE 组织统计，消除垃圾邮件可为全世界小型企业和个人每年节省 940 万美圆。

其次，从个人用户来看，垃圾邮件浪费了人们的大量时间。一般人们需要至少 10 秒钟时间来判断是否为垃圾邮件，如果每天收到几十份垃圾邮件，就得花大约十分钟的时间来处理它们，实在是比较痛苦的事情。

垃 圾邮件也威胁网络的安全，特别是那些利用别人的服务器转发邮件的情况。今年 3 月份，我们就收到两起来自 CERNET 用户的有关事故报告。其中一个是网络管 理员发现他们的服务器在以每秒 60 封的速度转发邮件，占用了大量的系统资源，其他正常运作被迫终止。另外一起是管理员发现出国流量突然增加，一查发现该服务器转发了 200 万封国外的来源不名的邮件，而且发现时还在转发。

从法律的角度来看，发送垃圾邮件属于言论自由的滥用，不但得不到法律的支持，相反，很多地方正积极之制定相关法律来禁止垃圾邮件。

5. 世界垃圾邮件状况

正如上一节讲到的，垃圾邮件并不受人们的欢迎。从垃圾邮件的产生之初，人们就开始了反垃圾邮件的工作，并取得了一定的进展。我们不妨回顾一下过去的几年中取得的进展：

95.7 在英语中开始使用 spam 以此来表示垃圾邮件，表明垃圾邮件已成为一个正式的课题；

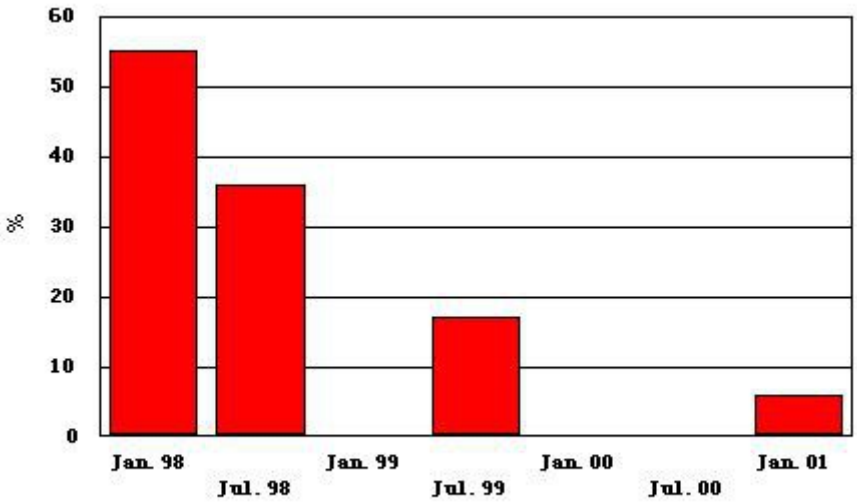
95.10~11，行业内开始使用专门的邮件账户 abuse@domain 来讨论垃圾邮件，并开始出现所谓的黑名单，把一些已知的发送垃圾邮件的 IP 列入其中，人们可以用来过滤垃圾邮件；

97.5 CAUCE (Coalition Against Unsolicited Commercial E-mail) 组织成立，倡议建立法律来同垃圾邮件做斗争；

98.4 Interner 协会 ISOC (Internet Society) 召开会议专门讨论了垃圾邮件；

99.2 发布了 RFC2502, Anti-Spam Recommendations for SMTP MTAs, 标志垃圾邮件已正式成为 Internet 的重要研究课题。

另 外一种比较办法用 OPEN RELAY 服务器的数量。以美国 IMC（Internet Mail Consortium）组织在美国的统计结果来看，OPEN RELAY 服务器数量已有 1998 年的 55% 迅速下降到 2001 年初的 6% 左右。 如下图所示 ：



在其他国家和地区，状况虽然不会有这样好，但随着越来越多的人们意识到垃圾邮件的危害，随着相关技术的不断成熟，网络安全意识的不断提高，垃圾邮件的活动空间将越来越小。

6 世界著名的反垃圾邮件组织

世 界各地成立了许多组织开展反垃圾邮件的工作。目前几个著名的组织有 MAPS,ORBS, SpamCorp 等，他们从技术角度着手解决垃圾邮件，他们都各自维护了一个发送或转发垃圾邮件的数据库，帮助用户过滤垃圾邮件。另外，CAUCE 等组织则积极推动建立相 关的法律体系以彻底清除垃圾邮件。

7 垃圾邮件支持者

目 前大量发送垃圾邮件的主要是一些中小企业，以此来进行广告商业宣传。同时，也有一些大的组织机构出于自己的商业目的而支持垃圾邮件。据 Spamhaus 统计，90% 的垃圾邮件来自于知名的盈利机构 ，Spamhoue 收集了 100 多家主要的支持垃圾邮件的 ISP, 其中甚至包括著名的跨国公司。 有的公司甚至把支持垃圾邮件作为自己的经营策略。还有一些公司是专门提供发送垃圾邮件的应用程序。正因为如此，才增加了禁止垃圾由邮件的难度。目前，一些 公司主要从以下几个方面从事或支持垃圾邮件，尽管他们不一定直接发送这些邮件：

制作并销售具有特殊功能的垃圾邮件发送软件，这些软件具有"隐蔽功能"，能够逃避普通的过滤器；
制作和销售从网络上截获 email 地址的工具；
销售从网络上获取的 email 地址列表；
销售具有发送垃圾邮件特征的服务，媒体或软件；
提供发送垃圾邮件的商业服务；
为垃圾邮件的制造者提供防攻击（bulletproof）的服务；
提供到以上站点的链接或把链接转向以上站点。
目前，有 656 个上述网站被 Spamhaus 记录并仍在从事支持垃圾邮件的行为，3149 个站点被关闭或被迫停止类似业务。