第31章 Internet Email协议

作者：Neal S. Jamison

本章内容包括：

- 电子邮件
- X.400
- 简单邮件管理协议(SMTP)
- 使用POP和IMAP取回客户邮件
- 高级主题
- 相关RFC文档及其他参考信息

电子邮件是当前最普遍的互联网应用。用户可以使用它给老板发消息或给保险代理人、银行代理或远方的亲人和朋友发消息。毫无疑问，电子邮件改变了人们的通信方式。

31.1 电子邮件

生活离不开人与人之间的交流。电子邮件或简称为伊妹儿是信息时代进行交流最重要的技术；它此刻正在世界各地成百上千的计算机间穿梭。

本节简单介绍电子邮件及其发展历史。讲述使电子邮件的工作标准及制定标准的组织。

31.1.1 电子邮件的历史

互联网最初用于方便科学家与政府技术人员间的通信。虽然电子邮件并不是他们采用的第一种通信方式，但它是通信的终极目标。自从互联之日起，它就孕育了电子邮件传输机制。目前，电子邮件完成大部分数据传输工作。

早期的电子邮件系统仅是将消息拷贝到用户邮箱的程序。那时，用户均使用同一台机器。多用户系统的某个用户使用电子邮件向同一台机器的其他用户发消息。大多数用户都使用cc:mail和其他类似的专用电子邮件系统来执行此项功能。经过一段时期，网关组件的出现允许用户使用一个电子邮件服务器向/从其他电子邮件服务器发送或接收邮件。网关允许不同类型的电子邮件系统相互通信。cc:mail用户可以利用网关向其他组织的Microsoft Mail用户发送消息。但是这些网关仍只能发送和接收专用格式的消息。因此，需要制定标准。

31.1.2 标准及制定标准的组织

电子邮件标准主要有以下两个：X.400，由国际远程通信——通信标准化组织及国际标准化组织制定。简单邮件传输协议(SMTP)，由IETF根据早期的研究及开发成果制定。

31.2 X.400

X.400首先由ITU于1984年制定并于1988年修改，它是复杂、健壮的电子邮件协议。然而，正由于其复杂性，因此目前缺少了厂家支持，因而远不如SMTP普及。因此，本章仅简单介绍

X.400，而对互联网标准SMTP作详细讨论。

邮件术语101

电子邮件中使用少量专门的术语描述邮件系统的组件：

用户代理(User Agent，UA)——运行于用户计算机上的电子邮件客户程序；用于创建和读取邮件消息。

消息传输代理(Message Transfer Agent，MTA)——电子邮件服务器。MTA存储并转发消息。

消息存储(Message Store，MS)——存储消息直到被接收者读取或处理。

X.400消息中可包含结构化的消息和附件。它还可以传送传输术语的属性并在消息中添加值。属性包括：

- 敏感性和重要性级别
- 优先权
- 过期时间
- 发送和接收通知
- 回复时间

与消息的结构类似，X.400取址方式十分复杂。表31-1显示组成X.400地址的常用属性。

表31-1 X.400常见属性

属 性	描 述
G	给定名字
I	初始化
S	姓
Q	家族简写(Jr., Sr.)
CN	通用姓名
O	组织
OU	组织中的部门
P	私人管理域
A	行政管理域
C	国家

示例：

C=US; A=XXX; P=Acme; O=Acme; OU=IT; S=Jamison; G=Neal;

在上述地址中，国家为美国 (C=US)；提供X.400服务的公司或行政管理域为XXX(A=XXX)；私用域为Acme (P=Acme)；组织的雇佣者为Acme(O=Acme)；所在的部门为IT(OU=IT)，名字无需解释。而SMTP地址则简单得多：Jamisonn @ mycompany.com。

目录服务的角色

X.400标准复杂的原因之一是它的地址方案。与SMTP地址(username @ domain.com)不同，X.400地址非常复杂。目录服务包含X.500和轻型目录访问控制协议(LDAP)。这些协议为全局目录指定标准格式。X.400邮件系统可以使用这些目录查看合作者。

关于X.500和LDAP的详细信息参见第16章及RFC 2256或访问国际远程通信组织的主页http://www.itu.int/。

X.400优点和缺陷

X.400的复杂结构使它的优缺点十分鲜明。

优点包括：

- 对于数据复杂性高和/或安全需求高的应用可很好地支持。
- 安全性高。
- 可靠性高。
- 国际标准。

不足之处在于：

- 实现代价高。
- 配置及管理复杂。
- 缺少厂商支持。
- 许多较好的特性(如安全)并未在产品中实现。

关于X.400的详细信息参见国际电信同盟(ITU)的主页http://www.itu.int/。

31.3 简单邮件传输协议(SMTP)

简单邮件传输协议(Simple Mail Transport Protocol，SMTP)是电子邮件的互联网标准。SMTP是应用层协议，通过TCP/IP网络处理消息服务。由互联网工程任务组于1982年定义，目前在RFC 821和822中详述。

SMTP使用TCP端口25。

虽然SMTP是最流行的电子邮件协议，但它缺少像X.400那样丰富的特性。标准SMTP的主要缺陷是不支持非文本消息。

31.3.1 MIME和SMTP

多用途网际邮件扩展协议(Multipurpose Internet Mail Extensions，MIME)扩展了SMTP，它实现了在标准SMTP消息中封装多媒体(非文本)消息的功能。MIME使用Base 64编码方案将复杂文件转化为ASCII。

MIME是相对较新的标准，虽然大多数UA应用都支持MIME，但仍存在少量应用不支持它。如果碰到此种情况，就可能要使用本章将描述的其他编码方法(BinHex或uuencode)。

MIME在RFC 2045-2049中描述。

S/MIME

S/MIME是新的MIME规范，它支持加密消息。S/MIME基于公钥加密机制(RSA)并可有效防止消息被中途截取或伪造。

RSA公钥/私钥认证

根据算法的发明者Rivest、Shamir和Adelman称，RSA提供公钥/私钥加密功能。使用公钥加密的数据只能用私钥进行解密。使用S/MIME，发送方UA使用接收方(远程)用户或UA的公钥加密数据。接收方使用私钥解密获得消息。

关于RSA的详细信息，参见http://www.rsa.com；关于公钥/私钥加密的信息参见站点：http://www.rsa.com/rsalabs/pubs/pkcs/。

S/MIME在RFC 2311和2312中描述。

31.3.2 其他编码标准

编码非ASCII码消息的标准还有多种，最常用的是BinHex和uuencode。

BinHex和Unencode

BinHex表示二进制/十六进制编码，它被认为是Macintosh的MIME版本；Uuencode表示UNIX到UNIX的编码，因为它最初用于UNIX平台，现在它已用于多种非UNIX平台。虽然MIME、uuencode和BinHex有许多不同之处，但它们完成同一个目标——在文本消息中传输非文本文件。用户具体使用哪种方法决定于发送/接收方的邮件UA。幸运的是，目前大多数UA自动完成编码/解码工作。

31.3.3 SMTP命令

SMTP简洁的原因之一是它使用的命令少。表31-2列出了这些命令。

表31-2 RFC 821文档中描述的SMTP命令

命 令	描 述
HELO	呼叫Helo命令向接收者标识发送者，命令必须与发送方主机名结合使用。在扩展协议(ESMTP)使用EHLO命令。详细信息参见本章31.3.5节
MAIL	初始化邮件传输。参数包括“ from ”字段或邮件发送者字段
RCPT	标识邮件接收方
DATA	声明邮件数据开始(消息的主体)。数据可包含128位ASCII代码，并以包含圆点“ . ”的行结束
RSET	中止当前的传输
VRFY	用于确认接收用户
NOOP	无操作命令
QUIT	关闭连接
SEND	使接收主机知道消息必须送到另一个终端
下列命令在RFC 821描述但不是必需的命令：	
SOML	发送或邮寄。通知接收主机消息必须发送到其他终端或邮箱
SAML	发送并邮寄。通知接收主机消息必须发送到其他终端和邮箱
EXPN	用于展开邮件列表
HELP	请求帮助信息
TURN	请求接收主机向发送方主机返回消息

用户可从下面的SMTP示例中看出SMTP命令的语法结构十分简单：

```
220 receivingdomain.com -
    Server ESMTP Sendmail 8.8.8+Sun/8.8.8; Fri, 30 Jul 1999 09:23:01
HELO host.sendingdomain.com
250 receivingdomain.com Hello host, pleased to meet you.
MAIL FROM:<username@sendingdomain.com>
250 <username@sendingdomain.com>... Sender ok.
RCPT TO:<username@receivingdomain.com>
250 <username@receivingdomain.com>... Recipient ok.
DATA
354 Enter mail, end with a ''.'' on a line by itself
Here goes the message.
```

```
.
250 Message accepted for delivery
QUIT
221 Goodbye host.sendingdomain.com
```

结果邮件消息如下所示：

```
From username@sendingdomain.com Fri Jul 30 09:23:39 1999
Date: Fri, 30 Jul 1999 09:23:15 -0400 (EDT)
From: username@sendingdomain.com
Message-Id: <199907301326.JAA13734@mail.receivingdomain.com>
Content-Length: 23

Here goes the message.
```

31.3.4 SMTP状态码

当发送MTA向接收MTA发送SMTP命令时，接收MTA返回特定的状态码使发送者了解命令是否正确执行。表31-3列出RFC 821中描述的状态码。这些状态码按状态分组，其中第一位表示组含义(5XX表示失败，4XX表示临时问题，1XX-3XX表示成功)。

表31-3 SMTP返回码

编 码	描 述	编 码	描 述
211	帮助返回系统状态	500	命令不可识别或语法错
214	帮助信息	501	参数语法错
220	服务准备就绪	502	命令不支持
221	关闭连接	503	命令顺序错
250	请求操作就绪	504	命令参数不支持
251	用户不在本地，转寄到<Path>	550	操作未执行，邮箱不可用
354	开始邮件输入	551	非本地用户
421	服务不可用	552	中止，存储空间不足
450	操作未执行，邮箱忙	553	操作未执行，邮箱名不正确
451	操作中止，本地错误	554	传输失败
452	操作未执行，存储空间不足		

数字编码在RFC中定义，相应的文本具体由邮局长及 MTA管理员定义，以上列出的为RFC文档中建议的含义。

31.3.5 扩展SMTP

SMTP已经证明自己是可靠性高、用途广泛的电子邮件协议，但扩展 SMTP是广泛认可的需求。RFC 1809扩展了SMTP。它并未列出具体的扩展，而只是为增加命令提供了一个框架。例如SIZE命令，扩展SMTP允许接收主机限制接收消息的长度。标准 SMTP不提供此项支持。

当系统连接到一个 MTA，可采用HELO命令的扩展版本 EHLO命令。如果MTA支持扩展SMTP(ESMTP)，它将对此命令作响应。如果不支持 ESMTP，就返回错误消息(500 命令不能识别)使发送方使用SMTP。下面是ESMTP传输的示例：

```
220 esmtpdomain.com -
    Server ESMTP Sendmail 8.8.8+Sun/8.8.8; Thu, 22 Jul 1999 09:43:01
```

```
EHLO host.sendingdomain.com
250-mail.esmtpdomain.com Hello host, pleased to meet you
250-EXPN
250-VERB
250-8BITMIME
250-SIZE
250-DSN
250-ONEX
250-ETRN
250-XUSR
250 HELP
QUIT
221 Goodbye host.sendingdomain.com
```

表31-4描述了常用ESMTP命令。

表31-4 常用ESMTP命令

命 令	描 述
EHLO	HELO的扩展版本
8BITMIME	指明8位MIME传输
SIZE	限制消息的长度

31.3.6 检查SMTP的头

检查SMTP消息的头，可以使用户获取大量有用的信息。不仅可以知道消息的发送者、主题、发送日期及接收者，而且可以看到路由过程中所经过的停止点。 RFC 822指明头中至少需包含发送者(From)、日期和接收者(TO、CC或BCC)。

注意 从技术上说，TO和CC的作用相同。CC(复写纸拷贝)是早期术语，可追溯到文档中打字员输入并用复写纸复制文档的时代。

BCC(隐藏的复写纸拷贝)与前两者不同，虽然 BCC接收者接收消息的方式与 TO和CC接收者相同，但它们没有列在地址列表中。 BCC列表可能对所有 BCC接收者可见，但对于TO和CC接收者，它们是不可见的。

接收邮件的头允许用户在消息到达用户邮箱时对它进行检查。这一功能对解决碰到的邮件问题非常有效。如下例所示：

```
From someone@mydomain.COM Sat Jul 31 11:33:00 1999
Received: from host1.mydomain.com by host2.mydomain.com (8.8.8+Sun/8.8.8)
   with ESMTP id LAA21968 for <jamisonn@host2.mydomain.com]];
   Sat, 31 Jul 1999 11:33:00 -0400 (EDT)
Received: by host1.mydomain.com with Internet Mail Service (5.0.1460.8)
   id <KNJ6NT2Q>; Sat, 31 Jul 1999 11:34:39 -0400
Message-ID: <C547FF20D6E3D111B4BF0020AFF588113101AF@host1.mydomain.com>
From: ''Your Friend'' <someone@mydomain.COM>
To: '''jamisonn@host2.mydomain.com''' <jamisonn@host2.mydomain.com>
Subject: Hello There
Date: Sat, 31 Jul 1999 11:34:36 -0400
```

在示例中，用户可以看出消息发送者为 someone @ mydomain.com。消息从mydomain.com传送到host1。接着，host2从host1上接收到消息，接收者从host2之上读取邮件。在路由过程中的每一个停止点，接收主机都需添加它的头，其中包括日期 /时戳。与上一个示例相比，时戳发生了变化。 host2(接收者主机)报告它接收到消息的时间为 11:33:00，而host1报告的时间为11:34:36，比host2接收到消息的时间还晚1分钟。这是由于系统时钟不一致引起的问题。

31.3.7 SMTP的优势与不足

与X.400，SMTP也有许多优势和不足。

优势在于：

- SMTP十分流行。
- 许多厂商的平台都支持SMTP。
- SMTP便于实现易于管理。
- SMTP地址方案简单。

不足之处在于：

- SMTP功能不足。
- SMTP的安全机制不如X.400。
- 它的简单性限制了其使用。

31.4 使用POP和IMAP取回客户邮件

在Internet邮件刚开始使用时，用户读取邮件必须首先登录到邮件服务器。邮件程序通常都是基于文本的，缺乏对用户有好的界面。为了解决这一问题，出现了一些协议，它们使邮件消息可直接发送到用户桌面电脑。这些 UA取回协议给予工作在多个不同计算机上的用户带来了许多方便。

其中，使用最广泛的协议是邮局协议 (Post Office Protocol，POP)和互联网邮件控制协议 (Internet Mail Access Protocol，IMAP)。

31.4.1 邮局协议(POP)

POP允许本地邮件UA连接MTA并将邮件取回到用户本地系统，用户也在本地机上阅读和响应消息。 POP协议于1984年定义，并于1988年提出了POP2协议。目前的标准是POP3协议。

POP3 UA通过TCP/IP与服务器连接(通常使用端口110)。UA输入用户名和口令(为了方便可将这些信息存入系统，但每次由用户敲入安全性更好)。经过认证后， UA可通过POP3命令取回或删除邮件。

POP3仅仅是接收协议。 POP3 UA使用SMTP向服务器发送邮件。

POP3由RFC 1939定义。

POP3命令

表31-5列出了POP3命令。

表31-5 POP3命令

命 令	描 述
USER	指明用户名
PASS	指明口令
STAT	询问邮箱状态(消息数量，消息大小)
LIST	列出消息索引
RETR	取回指定的消息
DELE	删除指定的消息
NOOP	空操作
RSET	不删除消息(回卷)
QUIT	提交修改并断开连接

31.4.2 互联网邮件访问协议(IMAP)

POP3是将消息取回到用户 UA的最好并且最简单协议。但是，它的简单性导致其缺少许多必要的特性。例如， POP3仅能工作于离线模式，即消息下载到UA时从服务器上删除。

注意 某些POP3的实现支持“伪在线”方，它允许消息留在服务器上。

互联网邮件访问协议(Internet Mail Access Protocol，IMAP)弥补了POP3的不足。它首先于1986年在斯坦福大学被提出。 1987年实现了IMAP2。目前最高版本为IMAP4，并于1994年被接收为互联网标准。IMAP4在RFC 2060中描述，它使用TCP端口143。

IMAP4命令

表31-6列出了RFC 2060中描述的IMAP4命令。

表31-6 IMAP4命令

命 令	描 述	命 令	描 述
CAPABILITY	询问支持功能列表	STATUS	询问邮箱的状态
AUTHENTICATE	指定认证机制	APPEND	往邮箱中添加信息
LOGIN	提供用户名和口令	CHECK	询问邮箱的检查点
SELECT	指明邮箱	CLOSE	提交删除并关闭邮箱
EXAMINE	指定邮箱采用只读方式	EXPUNGE	提交删除
CREATE	创建邮箱	SEARCH	按指定规则为消息寻找邮箱
DELETE	删除邮箱	FETCH	取回指定的消息
RENAME	更改邮箱名	STORE	修改指定消息
SUBSCRIBE	将邮箱加入活跃(可用)列表	COPY	拷贝消息到其他邮箱
UNSUBSCRIBE	从活跃列表中删除邮箱	NOOP	空操作
LIST	列出邮箱	LOGOUT	关闭连接
LSUB	列出订阅邮箱		

31.4.3 POP3与IMAP4的比较

POP3与IMAP4间存在基本差异。用户可根据 UA、自己的MTA及自身需求，决定使用二者中的哪一个，或两者都使用。 POP3的优点在于：

- 非常简单。
- 得到广泛支持。

正由于其简单，POP3也受到许多限制。例如，它仅能支持一个邮箱，消息必须从服务器上删除(虽然许多实现支持“伪在线”模式，使消息可留在服务器上)。

IMAP4有以下优点：

- 认证功能强。
- 支持多个邮箱。
- 可很好地支持断线、在线或断开连接多种模式的操作。

IMAP4的在线模式使用户的UA可从服务上下载消息的一个子集，支持基于特定规则的消息检索和下载等。IMAP4也允许用户或UA在服务器文件夹间移动消息，删除特定的消息。IMAP4非常适合于需要工作在多个不同计算机上的移动用户，或需要访问和维护多个不同邮箱的用户。

IMAP4最大的不足在于缺少UA的支持。但是，这种状况将很快将得到改观。

31.5 高级主题

随着电子邮件的流行，与其相关的主题也日益引起人们的重视。本节介绍与电子邮件用户密切相关的主题。这些主题包括安全、垃圾邮件及其他类型的邮件服务。

安全

正如计算机网络的其他方面一样，电子邮件安全也成为人们关注的焦点。确保邮件安全和可靠的传送所采用的机制十分关键。

1. 加密

如前所述，S/MIME可实现对电子邮件数据的加密。这种加密可以保护数据并确保数据到达目的地。

另一种加密消息的方法是PGP(Pretty Good Privacy)。PGP使用成对的公钥/私钥完成消息的加/解密。发送者用接收者的公用加密数据。接收者使用私钥解密消息。关于PGP的详细信息，参见站点http://www.pgp.com/。

数字签名(又称数字ID)被用于确认消息来自其声称的签名者。数字签名也使用成对密钥。关于数字签名的详细信息参见http://www.verisign.com/client/index.html。

关于电子邮件私有和加密方面的信息请参见RFC文档1421至1424。

2. 内容过滤

电子邮件的内容过滤与防火墙的工作类似。它扫描出入的消息以确保它们符合电子邮件策略管理员及邮局管理员制定的规则。例如某些公司使用此方法防止信息泄露给竞争者。它采用内容过滤禁止某些类型的数据(如草稿或设计文档)发送出去。内容过滤还可以删去敌对消息或垃圾信件、扫描病毒等。

3. 病毒

美国最近发作的梅丽沙病毒使电子邮件病毒再次成为热门话题。虽然通过电子邮件ASCII码文本不可能传输病毒，但将病毒嵌入到电子邮件附件中是完全可能的。梅丽沙宏病毒就是通过此种方法传播的，一旦某台机器感染了此病毒，它将拷贝到该主机电子邮件目录下的所有能找到的邮件地址上去。

梅丽沙病毒提醒电子邮件用户：查杀电子邮件附件中的病毒十分重要。

关于病毒的详细信息，请参阅互联网站点http://www.isoc.org/Internet/issues/viruses/。

4. 伪造

由于SMTP的安全性十分脆弱，伪造电子邮件消息十分简单，用户可以使用 telnet命令连接到SMTP端口，然后像MTA一样发送命令，就可轻松地伪造电子邮件消息。如下例所示：

```
$ telnet mail.mydomain.com 25
Trying...
Connected to mail.mydomain.com.
Escape character is '^]'.
220 mail.mydomain.com - Server ESMTP Sendmail 8.8.8+Sun/8.8.8;
    Fri, 30 Jul 1999 09:23:01
help
214-This is Sendmail version 8.8.8+Sun
214-Topics:
214-    HELO    EHLO    MAIL    RCPT    DATA
214-    RSET    NOOP    QUIT    HELP    VRFY
214-    EXPN    VERB    ETRN    DSN
214-For more info use ''HELP <topic>''.
help mail
214-MAIL FROM: <sender> [ <parameters> ]
214-    Specifies the sender.  Parameters are ESMTP extensions.
214-    See ''HELP DSN'' for details.
214 End of HELP info
helo fakedomain.com
250 mail.mydomain.com Hello  realhost.mydomain.com, pleased to meet you
mail from:<charlatan@fakedomain.com>
250 <charlatan@fakedomain.com>... Sender ok
rcpt to:jamisonn
250 jamisonn... Recipient ok
data
354 Enter mail, end with ''.'' on a line by itself
This is not really from charlatan@fakedomain.com.
.
250 MAA07012 Message accepted for delivery
quit
221 mail.mydomain.com closing connection
Connection closed by foreign host.
$
```

注意，HELO命令后的主机名并不是真实的主机名。发送给用户jamisonn的电子邮件如下所示：

```
From charlatan@fakedomain.com Sun Aug  1 12:18:08 1999
Date: Sun, 1 Aug 1999 12:17:43 -0400 (EDT)
From: charlatan@fakedomain.com
Message-Id: <199908011617.MAA07012@realhost.mydomain.com>
Content-Length: 50
This is not really from charlatan@fakedomain.com.
```

虽然初看起来，它像来自 charlatan @ fakedomain.com的邮件，但检查其头，在 Message-Id行中可以看出真实主机名。

对于想尝试伪造邮件的读者的警告：邮局管理者及管理员可采用专门的登录机制来找出真实的发送者，甚至可避免伪造电子邮件。伪造邮件并不是个好主意，上例仅为了说明它的可能性。

5. 垃圾邮件

用户可能会发现自己的电子邮箱开始与自己的普通邮箱一样充满了垃圾邮件。

垃圾邮件是一个令人头痛的问题。我们的邮箱每天充斥着广告信息、发财指南及其他不想要的信息。我们的电子邮件地址被拍卖或未经本人同意就被共享，从而导致邮箱中充满了垃圾。

一种避免这种烦人消息的方法是使用过滤器。它实际上是邮件UA上的工具，可以使用户删除满足规则的邮件。最常见的规则是读取进入邮箱消息的 SMTP头，查找发送者的地址或邮件的主题是否包含规则中指明的关键字。如果包含，则删除该邮件；否则将邮件保留在邮箱中。

除了上述方法外，用户还可采用其他方法对付垃圾邮件。但这一内容超出了本章讨论的范围。详细信息请访问互联网组织的站点 http://spam.abuse.net或http:// www, isoc.org/ internet /issues/spamming。

6. 匿名电子邮件服务

在互联网上使用匿名涉及道德伦理上的问题。某些人坚持匿名服务，另一些人认为所有的行为都应是可查询的。当然，这一问题在人与人之间的交流上 (如电子邮件)讨论更加热烈。

在互联网上存在许多程序和服务允许用户发送匿名邮件。这些服务通常都利用程序将SMTP头从消息中删去，仅将剩余部分提供给接收者。因此，无法查询它的发送者。同时，也无法回复接收到的消息。

许多高级应用都维护一个保存匿名用户的数据库。每个用户都分配一个 ID，只要数据库安全，邮件发送者可使用ID发送邮件。将ID映射为用户名使接收者可以回复邮件。

另一种匿名邮件服务是通过在线服务和电子邮件提供者实现。这些最近出现的免费电子邮件服务允许用户选择自己的电子邮件用户名。它不要求用户使用自己的真实姓名。因此，用户可以发送匿名邮件。

31.6 相关RFC文档及其他参考信息

表31-7列出了许多电子邮件协议的相关 RFC文档。所有这些文档可从 http://www.cis.ohio-state.edu//htbin/rfc/INDEX.rfc.html上找到。

表31-7 RFC相关文档

RFC	描 述
821	简单邮件传输协议(J.B.Postel, 1982)
822	ARPA互联网文本消息的格式标准(D.H.Crocker, 1982)
1203	交互式邮件控制协议：版本3(J.Rice, 1991)
2196	站点安全手册(B.Fraster, 1997)
1521	MIME(多用途互联网邮件扩充)(N.Borenstein, N.Freed, 1993)
1421	互联网电子邮件私用性增强：第一部分：消息加密与认证过程(J.Linn, 1993)
1422	互联网电子邮件私用性增强：第二部分：密钥管理 (S.Kent, 1993)
1423	互联网电子邮件私用性增强：第三部分：算法、模型和标识(D.Balenson, 1993)
1424	互联网电子邮件私用性增强：第四部分：密钥检定和相关服务(B.Kaliski, 1993)
1939	邮局协议－版本3(M.Rose, 1988)
1869	SMTP服务扩充(J.Klensin et al., 1994)
1652	SMTP服务扩充8位MIME传输(J.Klensin et al., 1995)
1871	SMTP服务扩充：消息大小声明(J.Klensin et al., 1995)
2256	使用LDAPr3 X.500 (96)用户策略简介(M.Wahl, 1997)
2164	使用X.500/LDAP目录支持MIXER地址映射(S.kille, 1988)

下列组织定义电子邮件协议，它们的站点提供丰富的信息。

互联网工程任务组(IETF)：http：//www.ietf.org/

国际标准化组织(ISO)：http://www.iso.ch/

国际电信联盟(ITU)：http://www.itu.int/

31.7 小结

本章详细讲述了互联网邮件协议： SMTP。我们首先简单介绍了电子邮件的历史，然后简单讲述了X.400 —— 功能强大但未被广泛使用的电子邮件协议。接着介绍了 SMTP的命令集、响应码和非文本数据的编码方法。并讨论了两种从邮件传输代理或消息存储中取回邮件的方法：使用POP3和使用功能强大的IMAP4。

本章还讨论了与电子邮件相关的问题。电子邮件的安全问题主要讲述了加密、内容过滤和病毒等。讨论了垃圾邮件产生的原因及解决办法。最后一节给出了与电子邮件相关的 RFC文档，及负责电子邮件协议组织的Web站点。