国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1241

(04/2008)

X系列：数据网、开放系统通信和安全性

电信安全

反垃圾信息技术框架

ITU-T X.1241 建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	
业务和设施	X.1-X.19
接口	X.20-X.49
传输、信令和交换	X.50-X.89
网络概貌	X.90-X.149
维护	X.150-X.179
管理安排	X.180-X.199
开放系统互连	
模型和记法	X.200-X.209
服务限定	X.210-X.219
连接式协议规范	X.220-X.229
无连接式协议规范	X.230-X.239
PICS书写形式	X.240-X.259
协议标识	X.260-X.269
安全协议	X.270-X.279
层管理对象	X.280-X.289
一致性测试	X.290-X.299
网间互通	
概述	X.300-X.349
卫星数据传输系统	X.350-X.369
以IP为基础的网络	X.370-X.379
报文处理系统	X.400-X.499
号码簿	X.500-X.599
OSI 组网和系统概貌	
组网	X.600-X.629
效率	X.630-X.639
业务质量	X.640-X.649
命名、寻址和登记	X.650-X.679
抽象句法记法1(ASN.1)	X.680-X.699
OSI 管理	
系统管理协议子集和结构	X.700-X.709
管理通信服务和协议	X.710-X.719
管理信息的结构	X.720-X.729
管理功能	X.730-X.799
安全	X.800-X.849
OSI 应用	
托付、并发和恢复	X.850-X.859
事务处理	X.860-X.879
远程操作	X.880-X.889
ASN.1的一般应用	X.890-X.899
开放分布式处理	X.900-X.999
电信安全	**X.1000-**

欲了解更详细信息，请查阅 *ITU-T*建议书目录。

ITU-T X.1241建议书

反垃圾信息技术框架

摘要

ITU-T X.1241建议书提供了一个反垃圾电子邮件的技术框架。此框架描述了一个反垃圾信息处理域的推荐结构，定义了其中主要模块的功能。框架的关键点是在不同邮件服务器之间建立垃圾电子邮件的共享机制，按照此框架的系统可以通过互连提高效率。

来源

ITU-T第17研究组（2005-2008年）根据世界电信标准化全会（WTSA）第1号决议的程序于2008年4月18日批准了ITU-T X.1241建议书。

关键词

反垃圾信息，电子邮件，互连，垃圾信息，技术框架。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准ITU-T建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

© 国际电联 2009

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

页

1 范围 1
2 参考文件 1
3 定义 1
3.1 其它文件定义的术语 1
3.2 本建议书定义的术语 1
4 缩写词和首字母缩略语 2
5 排印惯例 2
6 反垃圾信息处理域的总体结构 2
6.1 总体结构 2
6.2 参考模型 4
7 反垃圾信息处理域的功能 5
7.1 邮件客户机的功能 5
7.2 邮件服务器的功能 5
7.3 反垃圾信息处理实体的功能 6
7.4 反垃圾信息处理下级实体的功能 6
8 垃圾电子邮件的鉴别 6
8.1 常见垃圾电子邮件的特征 6
8.2 常见的反垃圾邮件规则 7
9 反垃圾电子邮件的方法 8
9.1 关闭open-relay功能 8
9.2 邮件发信权限控制 8
9.3 过滤技术 9
9.4 可追溯性检查 9
10 反垃圾信息处理域之间的互连 10
10.1 顶级处理实体之间的互连 10
10.2 处理实体和处理下级实体之间的互连 11
10.3 处理下级实体和邮件服务器之间的互连 11
参考文献 12

引言

随着基于IP的电信网的发展，大量的电子邮件需要通过IP电信网传送到用户，而同时越练越多的垃圾电子邮件正在互联网网络上泛滥。

电子邮件垃圾成了降低IP电信网业务能力的原因之一，业务提供商不得不花费大量的财力来解决垃圾电子邮件造成的问题，用户也不得不花费时间删除垃圾信息。

一些侦测技术可以用于检测和删除垃圾邮件，但是垃圾信息制造者又能想出躲避侦测的办法，比如伪造成正常的邮件，随机写邮件内容来避免被过滤。因此，我们需要发展一种有效的技术框架去解决垃圾邮件的问题。

不同反垃圾信息解决方案可能使用不同的技术去处理垃圾邮件，这些反垃圾信息技术都在不断发展，所以很难找到一个能长期概括所有反垃圾信息技术的描述。

因此，我们需要建立一个涵盖各种解决方案的开放的框架，这个框架要能够兼容所有的反垃圾信息技术，而不限于某一个具体技术。此框架满足一下需求：

- 能够系统地区分电子邮件是否垃圾信息；
- 能够在多个电子邮件业务系统之间分享反垃圾电子邮件信息；
- 能够提升邮件系统反垃圾信息工具的准确性；
- 确保不同管理域内实体能共享反垃圾邮件信息。

ITU-T X.1241建议书

反垃圾信息技术框架

1 范围

本建议书提供了反信息的技术框架。此框架描述了一个反垃圾信息处理域的推荐结构，定义了其中主要模块的功能。框架的关键点是在不同邮件服务器之间建立垃圾电子邮件的共享机制，按照此框架的系统可以通过互连提高效率。

2 参考文件

无。

3 定义

3.1 其它文件定义的术语

本建议书使用的在其它文件定义的术语如下：

3.1.1 邮件对象[b-IETF RFC 2821]： SMTP 协议传输邮件对象。邮件对象包括信封和内容。

3.1.2 邮件头[b-IETF RFC 2822]：邮件头有着通用的语法结构：域名字，冒号，域主体。

3.2 本建议书定义的术语

本文件定义了如下术语：

3.2.1 反垃圾信息处理域：这是一个独立的系统，它包含反垃圾信息处理实体、反垃圾信息处理下级实体、邮件服务器、邮件客户机。

3.2.2 反垃圾信息处理实体：反垃圾信息处理实体是反垃圾信息处理域的核心，用于收集来自下级的处理实体的垃圾电子邮件信息，建立统一、完整的规则体系，并将这些规则体系下发到下级的处理实体。

3.2.3 反垃圾信息处理下级实体：反垃圾信息处理下级实体连接到一个或多个邮件服务提供商，并从邮件服务器和反垃圾信息设备收集垃圾邮件信息，经过定期分析后上报信息给上级实体。同时，它也定期接收上级实体下发的规则更新，并分发给下级实体。

3.2.4 复合规则：复合规则由两个或两个以上的简单规则组合。

3.2.5 电子邮件：主要是指通过电信网传输电子邮件信息。

3.2.6 垃圾电子邮件：是指通过电子邮件进行的未经收件人请求或许可的电子通信，通常用于特定目的。

3.2.7 规则：规则是一系列的条件和基本动作。规则包括多种形式，如行为、过滤器等。

3.2.8 邮件样本：指按一定规则邮件服务接受的邮件。

3.2.9 **垃圾信息制造者：**指创建和发送垃圾邮件的实体或个人。

4 缩写词和首字母缩略语

本建议书使用如下缩写词和首字母缩略语：

DNS	Domain Name Server	域名服务器
E-mail	electronic mail	电子邮件
ESMTP	Extended Simple Mail Transfer Protocol	扩展的简单邮件传送协议
FTP	File Transfer Protocol	文件传送协议
HTTP	Hypertext Transfer Protocol	超文本传送协议
IMAP4	Internet Message Access Protocol v4	互联网消息访问协议版本4
IP	Internet Protocol	网际协议
POP3	Post Office Protocol v3	邮局协议版本3
RBL	Real-time Blacklist	实时黑名单
SASL	Simple Authentication and Security Layer	简单认证和安全层
SMTP	Simple Mail Transfer Protocol	简单邮件传送协议
URL	Uniform Resource Locator	统一资源定位符

5 排印惯例

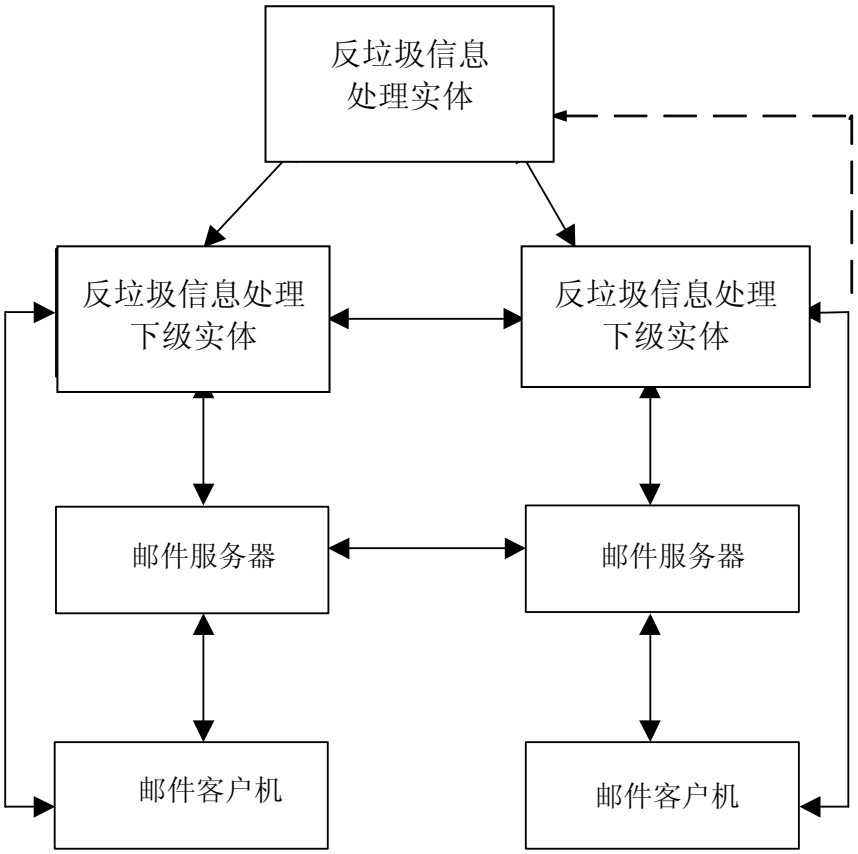
无。

6 反垃圾信息处理域的总体结构

6.1 总体结构

本建议书介绍了框架的组成部分，包括反垃圾信息处理实体、反垃圾信息处理下级实体、邮件服务器和邮件客户机。

这些组成部分之间通过通用消息传送协议进行通信，本节将对各组成部分的性能进行描述。



注 – 实线部分表示反垃圾信息处理域中各组成部分之间交换信息的通道。

图1 – 总体结构

在图1中，反垃圾信息处理实体接收反垃圾信息处理下级实体的报告并向他们下发新的规则。

反垃圾信息处理下级实体须检查来自反垃圾信息处理实体规则的有效性，并进行改进。

邮件客户机是用户直接处理的实体。邮件服务器通过IP电信网传送电子邮件。

邮件客户机将投诉传送给反垃圾信息处理下级实体，特定情况下，邮件客户机可以将投诉直接传送给上级的反垃圾信息处理实体。

6.2 参考模型

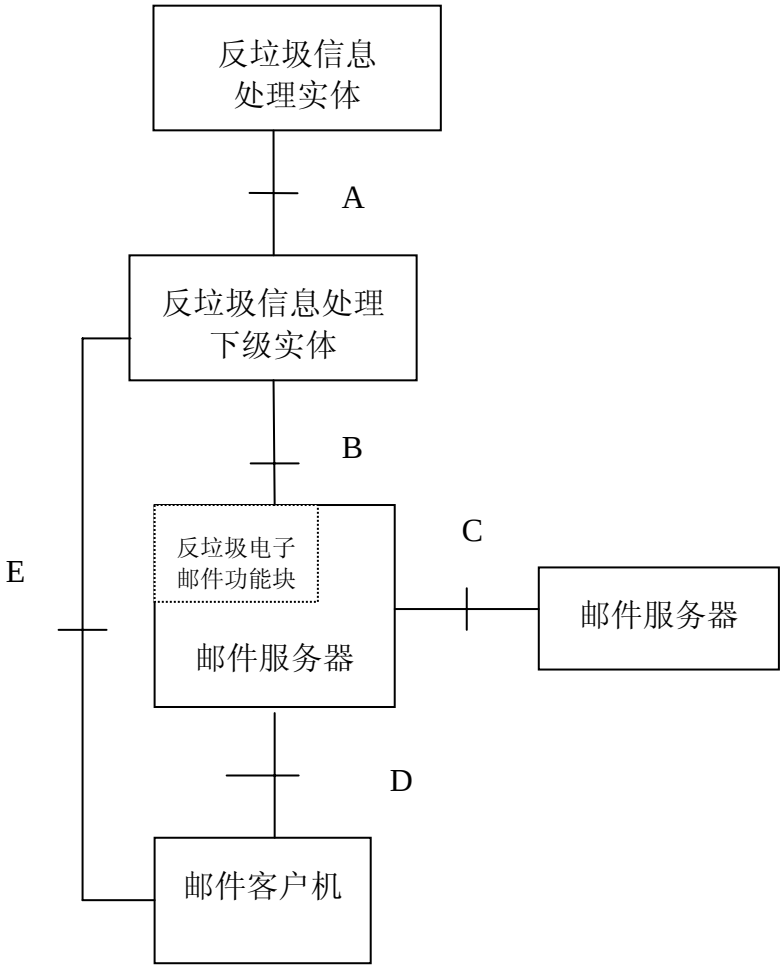


图 2 – 参考模型

接口A在反垃圾信息处理实体与下级实体之间。需要支持FTP文件传输协议和HTTP超文本文件传输协议，举报和反垃圾信息规则信息通过接口A进行传送，规则如“来源IP+URL”可能是复合规则，接口A应支持FTP和HTTP。

接口B位于反垃圾信息处理下级实体与邮件服务器之间，用于传送上报投诉和规则，同样，规则可能是复合规则，如“来源IP+URL”。接口B应支持FTP和HTTP。在特定情况下，邮件服务器可与上级反垃圾信息处理实体直接通信。

接口C在邮件服务器之间，采用SMTP进行消息传送。

接口D在邮件服务器与邮件客户机之间。可采用各种协议传送电子邮件，如POP3、IMAP4。

接口E在邮件客户机与反垃圾信息处理下级实体之间的参考点，邮件客户机可将投诉发送给反垃圾信息处理下级实体。在特定情况下，邮件客户机可将投诉直接发送给上级的反垃圾信息处理实体。在此接口可使用线网络、电话、电子邮件和客户机软件。

7 反垃圾信息处理域的功能

7.1 邮件客户机的功能

邮件客户机有以下功能：

- 邮件客户机除完成邮件收发的一般功能外，还提供了一种帮助用户将垃圾信息投诉发送至反垃圾信息处理实体的机制。电子邮件的接收者仅需根据内容标题或地址判断其是否为垃圾信息，例如，如接收者未同意接收的广告、电子刊物或宣传材料，可通过邮件客户机的机制向反垃圾信息处理实体举报。
- 邮件客户机可以从反垃圾信息处理实体自动下载垃圾信息过滤规则。过滤规则根据邮件客户机上报的投诉，包括单封邮件的大小限制、一段时间内发出的邮件数量、邮件内容的关键词等。根据上报的投诉对过滤规则进行定期更新、通过邮箱用户名、输出IP地址和域名索引。
- 可以提交邮件客户机可将垃圾邮件转发反垃圾信息处理实体作进一步处理或撤销造成误报的一些过滤规则。反垃圾信息处理实体可根据邮件的要求或上报的投诉即时更新过滤规则。
- 邮件客户机可直接过滤垃圾邮件。通常接收者应了解过滤结果，以避免误报问题。

7.2 邮件服务器的功能

邮件服务器有以下功能：

- 实现邮件传送的一般功能后，邮件服务器完成了与其它邮件服务器之间交换电子邮件，或在邮件客户机之间收发邮件的正常活动；同时邮件服务器应禁止开放转发功能，以避免垃圾信息制造者利用其向其它邮件服务器发送垃圾邮件。
- 客户在通过邮件服务器发送邮件之前须通过验证。不同的邮件系统可能使用不同的认证机制，认证部署在邮件服务器和邮件客户机之间。
- 邮件业务提供商可能有一个垃圾信息制造者的黑名单，这个黑名单包括垃圾信息制造者的一些信息（如主机名、域名、电子邮件地址），邮件服务器可以拒绝接收他们发送的邮件。
- 邮件服务器可以回发验证信息到邮件来源（已显示在发件人信息（如DNS、主机名或其它）中）；如果这个验证命令未确认来源的真实性，邮件服务器将拒绝此电子邮件。
- SMTP的一些命令可能被垃圾信息制造者用于猜测邮件服务器的真实账户，邮件服务器禁止EXPN、VRFY等命令。
- 一些广告和宣传电子邮件没有发送者的信息。邮件服务器应自动在电子邮件中加上HTTP的链接，以便于用户提出投诉。
- 邮件服务器通过反垃圾信息技术检测垃圾邮件，同时报告给反垃圾信息处理下级实体，并从它那里下载过滤规则。
- 如检测出垃圾信息，邮件服务器备份原邮件（至少包括源邮件的邮件头），并提交给过滤器。

- 邮件服务器应该提供系统日志和定期备份的邮件服务器统计数据，并提交给反垃圾信息处理下级实体。
- 邮件服务器能够根据不同的规则返回不同的状态代码。
- 邮件服务器能够限制特定电子邮件用户的流量。

7.3 反垃圾信息处理实体的功能

反垃圾信息处理实体具有以下功能：

- 与其它反垃圾信息处理实体的交换过滤规则，可以采用各种协议进行传送，例如FTP和HTTP。
- 保存用户和反垃圾信息处理下级实体举报的垃圾电子邮件的原始信息。
- 向反垃圾信息处理下级实体发布过滤规则，并发出高危邮件警报。
- 反垃圾信息处理实体能够管理和维护过滤规则，通过下列网站可获得这些规则：
  - 受理用户和反垃圾信息邮件处理下级实体举报；
  - 公布官方消息，包括监督和管理情况的信息。

7.4 反垃圾信息处理下级实体的功能

反垃圾信息处理下级实体具有以下功能：

- 接收用户和其他实体垃圾电子邮件的举报；接收反垃圾信息处理实体的过滤规则；
- 保存用户和其它实体举报的垃圾邮件的原始信息（至少包括垃圾邮件的邮件头）。
- 向邮件服务器和邮件客户机发布过滤规则，如有必要，向用户发出高危邮件警报；
- 追溯垃圾信息的来源，收集相关的信息；
- 向上级实体报告垃圾邮件传播和相关信息的状态；
- 根据可疑电子邮件备份生成新的过滤规则，检查并修改已有的过滤规则。可以通过如下网站获得这些规则：
  - 生成用户和邮件服务器的垃圾信息报告；
  - 生成新的过滤规则。

8 垃圾电子邮件的鉴别

本节描述了常见的垃圾电子邮件的特征和判定标准。

8.1 常见垃圾电子邮件的特征

以下是垃圾电子邮件消息通常具有的特征：

- 隐藏或伪造真实的发送者地址。

  信息源字段的“from”或 “sender”中的内容为空或无效。
- 隐藏或伪造电子邮件的真实来源

  标识字段的 “message-id” 为空或无效。

- 发件人是已知垃圾信息制造者

  信息源字段的“from”或 “sender”中包含黑名单中的垃圾信息制造者地址。
- 伪造收件人信息

  收件人字段（“to”）或抄送收件人字段（“cc”）的内容是伪造的或与垃圾信息制造者有关。
- 包含垃圾信息制造者常用的词语

  在主题字段（“subject”）或邮件内容中包含垃圾信息制造者常用的词语。
- 伪造中继信息

  中继域中的 “resent-from”或“resent-sender” 字段的内容是伪造的。
- 伪造跟踪信息

  路径字段中的内容是伪造的。
- 大小不合理

  整个电子邮件、头字段或邮件内容的大小与垃圾电子邮件头字段和邮件内容大小接近。
- 收件人过多

  在某一域中收件人过多。
- 转发跳跃点过多

  路径字段中路径过多。
- 在特定字段中包含发送者IP地址

  信息源字段的“from”或“sender”字段包含有关垃圾信息制造者的信息。
- 特定字段中包含邮件服务器IP地址

  路径字段中的“received”转发字段的resent-from、resent-sender中包含垃圾信息制造者的信息。
- 新垃圾信息

  反垃圾信息处理实体可通过新的垃圾信息样本总结出新特征，并创建相应的过滤规则。

8.2 常见的反垃圾邮件规则

单项规则可以按不同的优先级组合成为复合规则。

邮件服务器在处理垃圾电子邮件时可采用单项和/或复合规则。

8.2.1 常见的基本规则

邮件服务器可以根据下列因素设置标准：

- 信息源字段(“from” 或 “sender”)为空或无效内容。
- 标识字段(“message-id”)是空或无效内容。
- 信息源字段(“from” 或 “sender”) 包含黑名单中给出的关键词。
- 收件人字段 (“to”)或抄件人字段(“cc”)中包含黑名单中给出的关键词。
- 邮件主题 (“subject”)或邮件内容包括给定的关键词。
- 在转发字段 “resent-from” 和“resent-sender” 或路径字段中的内容无法找到真实的信息源信息。

- 邮件整体、头字段或邮件内容的大小（约）等于给定的值。
- 在信息源字段中的 “to”、“cc”和“bcc” 等确定的地址总数超过了邮件服务器给定的限值；或邮件发送的频次超过了邮件服务器给定的限值。
- 路径字段中给出的路径数量超过了邮件服务提供商或域管理员给出的限值。
- 根据信息源字段中的“from”或“sender”信息给出DNS反向解析结果包含在特定黑名单中。
- 路径字段中“received” 或转发字段中的“resent-from”或“resent-reader”之后的DNS反向解析结果包括在特定黑名单中。
- 如果垃圾信息不能用单个规则鉴别，应使用复合规则。

8.2.2 标准的优先级

确定标准的优先级。如果有多个规则都可以匹配同一封电子邮件（称为规则冲突），那么会以优先级最高的规则为准。如果规则的优先级相同，那么应使用冲突优先原则应用的最终规则。应尽量避免规则冲突。

8.2.3 标准的冲突检测

这是一项检测不同指定标准之间是否存在冲突的功能。常见的冲突条件如下所述：

- 当“规则条件”中都包含相同类型的关键字搜索类“简单规则（基本规则）”（如：“主题包含XXX”或“正文前10行解码后包含 XXX”等等），并且“简单规则”中的搜索关键字相同或一个关键字包含另一个关键字。
- “规则条件”中都包含相同类型的IP地址限制类“简单规则”（如：“客户端IP是XXX”等等），并且“简单规则”中指定的IP空间相同或有交集。
- “规则条件”中均包含大小限制类型的“简单规则”，并且大小限制的条件为“XXX大小等于设定值”形式（不可以是大于或小于形式），并且指定的大小值相同。比如：两个规则都包含同一简单规则：“正文大小等于5343字节”。

9 反垃圾电子邮件的方法

防范垃圾电子邮件的主要方法包括关闭邮件服务器 open-relay 功能, 邮件发信权限的控制及过滤技术。防范垃圾电子邮件系统应当支持或可选支持以下方法。

9.1 关闭open-relay功能

Open-relay（开放转发）是指由于邮件服务器不理会邮件发送者或邮件接收者是否为系统所设定的用户，而对所有的入站邮件一律进行转发。通常，若邮件服务器开放没有任何限制的转发功能，则被认为是 open-relay 的。

9.2 邮件发信权限控制

为有效防止非法用户使用邮件服务器：

- 发信用户必须是本服务器的合法用户；

- 邮件服务器应验证发件人IP地址；
- 限制邮件的转发次数，避免垃圾信息的迅速传播；
- 邮件服务器可以对邮件进行来源核实，确保其真实性。

9.3 过滤技术

过滤技术可分为两类：IP地址过滤和邮件内容扫描过滤。

9.3.1 IP地址过滤

IP地址过滤可限制与邮件系统的SMTP进行连接。它的主要属性有IP范围和限制模式。

IP范围包含以下三种：

- 从反垃圾信息处理实体获取的实时IP范围
- 从其它组织过滤规则中获取的实时IP范围
- 自己添加的实时IP范围

限制模式包含：

- 拒绝连接
- 无条件允许连接
- 应限制同一客户端IP在一段时间内与邮件服务器的重复连接

如果某个客户端IP属于给定的IP范围内，应采用限制模式。

9.3.2 邮件内容扫描过滤

过滤规则可由邮件服务器设定，并从反垃圾信息处理实体下载，在特定条件下，过滤规则可由管理员进行修改。

如果某封邮件符合某项规则，该邮件将根据相关行为进行分类。内容扫描规则的行为包括：

- 拒收：抽取特征后，将拒收信息退给发送方。
- 丢弃：对每个无任何行为的命令的正常应答。
- 投递：正常进行投递处理。如果选择了投递那么忽略丢弃的动作。
- 标签：在信头中加入特定的标签。
- 举报：将邮件抽取特征后上报举报中心。
- 缓存：尽可能的保持邮件的原貌，将其转发反垃圾信息处理实体。

9.4 可追溯性检查

有时难以检查邮件发送者是否是合法用户，因为收件服务器不可能得到关于发件服务器的所有信息，也无法为合法用户验证所有信息。

电子邮件可以被分成两类：可追查的和不可追查的。如果没有警告，可追查的垃圾邮件将放入过滤规则。对不可追查的垃圾邮件的处理就比较困难，因为这些邮件通常使用的是假的发送地址。大多数不可追查的邮件都是垃圾邮件，所以检查邮件的可追查性是反垃圾电子邮件的基础，建议采用以下三个步骤：

第一步：实现的要求

- 大多数收件（域名中的“MX”）服务器本身就是发件服务器。

- 大部分独立的收件服务器和发件服务器的IP地址是相邻相近的。
- 其他允许发送邮件的计算机可能与“MX”邮件服务器的IP地址相邻相近
- 部分邮件服务器具有可DNS反解，所得到的结果与用户声称的相同

第二步：可追查公示机制

在电信网上支持认证：

- 确认发件人的邮件域是许可的。
- 确认发件人确实是该邮件域的合法用户。

第三步：可回溯机制

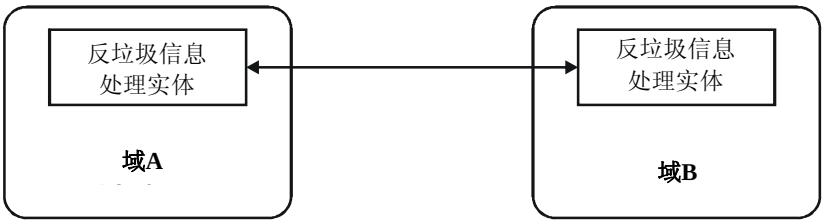
- 可追查服务与可追查检查形成回溯链
- 回溯链具有不可伪造性
- 很容易判别伪造部分和真实的部分

追查系统可自动根据回溯链追查。

10 反垃圾信息处理域之间的互连

当反垃圾信息处理域之间互连时，有三种可选的模式：通过顶级处理实体进行互连，处理实体和下级实体之间的互连以及下级实体和邮件服务器之间的互连。每种可选方式分别适合不同的场景或需求。

10.1 顶级处理实体之间的互连



X.1241(08)_F03

图 3 – 顶级处理实体之间的互连

此互连模式是顶级实体之间的双向互连。两个顶级实体之间仅交换相应规则。如一个实体接收到另一个实体的信息，它将实施特定的机制和流程选择其中有用的规则。

10.2 处理实体和处理下级实体之间的互连

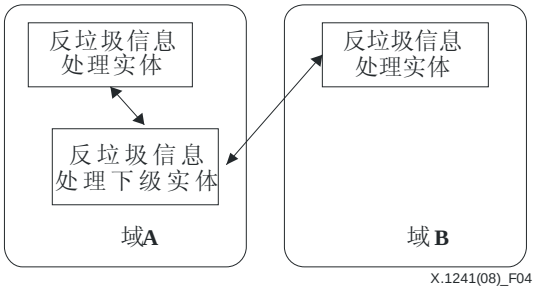


图 4 – 处理实体和处理下级实体之间的互连

此互连模式为处理实体和下级实体之间的双向互连。下级实体应从两个处理实体下载两个过滤规则列表。该下级实体根据所属的邮件服务器上报的可疑邮件样本创建新的规则。它应将规则上报两个实体。

该模式具有一定的安全性，但使下级实体和两个实体之间产生复杂的管理关系。可扩展性会存在问题，并非综合的域间互连。

10.3 处理下级实体和邮件服务器之间的互连

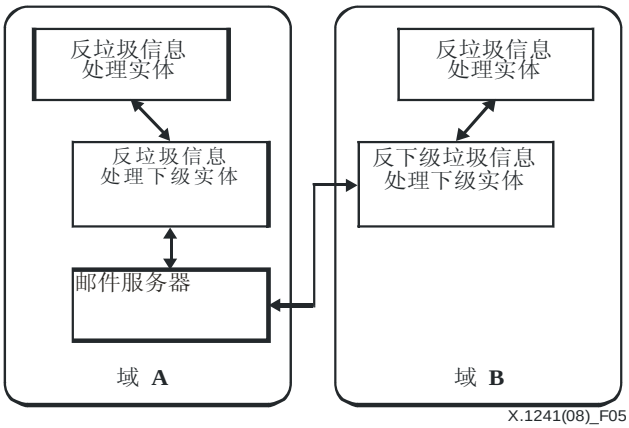


图 5 – 处理下级实体和邮件服务器之间的互连

此互连模式为下级处理实体和邮件服务器之间的双向互连。邮件服务器从下级处理实体下载过滤规则，将垃圾邮件上报给另一域内的下级处理实体。下级处理实体将接收邮件服务器的垃圾邮件报告，并向另一域服务器公布其规则。

该模式在域间易于实现，但域外的邮件服务器可能攻击反垃圾信息系统，所以存在一定的安全问题，该方式同样存在可扩展性问题，并非综合的域间互连。 在第10.1节中定义的模式是安全的，为推荐的互连模式。

参考文献

[b-IETF RFC 1869] IETF RFC 1869 (1995), *SMTP Service Extensions.* <http://www.ietf.org/rfc/rfc1869.txt>

[b-IETF RFC 1939] IETF RFC 1939 (1996), *Post Office Protocol – Version 3.* <http://www.ietf.org/rfc/rfc1939.txt>

[b-IETF RFC 2060] IETF RFC 2060 (1996), *Internet Message Access Protocol – Version 4rev1*. <http://www.ietf.org/rfc/rfc2060.txt>

[b-IETF RFC 2222] IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL).* <http://www.ietf.org/rfc/rfc2222.txt>

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs.* <http://www.ietf.org/rfc/rfc2505.txt>

[b-IETF RFC 2554] IETF RFC 2554 (1999), *SMTP Service Extension for Authentication.* <http://www.ietf.org/rfc/rfc2554.txt>

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol.* <http://www.ietf.org/rfc/rfc2821.txt>

[b-IETF RFC 2822] IETF RFC 2822 (2001), *Internet Message Format.* <http://www.ietf.org/rfc/rfc2822.txt>

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其他多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其他组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	**数据网、开放系统通信和安全性**
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	电信系统使用的语言和一般性软件情况

瑞士印刷
2009年，日内瓦