PPPoE 原理、应用及改进建议*

徐霖洲，丘海明
（中山大学电子与通信工程系，广东 广州 510275）

摘 要：PPPoE (point to point protocol over ethernet) 作为宽带驻地网接入一种有效方法，不但可以防止 IP 盗用，还有利于开展多服务、速率限制和按时按流量计费等多方面应用。然而，PPPoE 本身也有着其安全局限性有待克服。就 PPPoE 的应用场合及工作原理指出其潜在安全问题，并且提出改进方案。

关键词：PPPoE (point to point protocol over ethernet)；接入集中器；PAP 认证；CHAP 认证
中图分类号：TN915.08 **文献标识码**：A **文章编号**：0529-6579 (2002) 06-0111-03

在宽带驻地网（尤其是以太网）的接入中，多个用户通过一个设备（例如以太网中的交换机或者 ADSL 中的 DSLAM 等）统一连接到 ISP 所在网络。因此，需要一种协议能够像用于拨号服务的 PPP (point to point protocol) 一样，提供接入控制和计费等功能。

PPPoE (point to point protocol over ethernet) 满足了上述要求，在这种模型中，各主机利用其自己的 PPP 堆栈，各用户有着自己的逻辑接口，因此，就可以按用户（而不是基于某个地方）来进行接入控制，计费和开展多类型服务。

1 宽带驻地网用户接入要解决的问题

IP 地址盗用是宽带驻地网用户接入要解决的首要问题，非法用户把自己的 IP 和 MAC 地址修改成与合法用户一模一样，冒充合法用户就能使用网络资源，而且运营商难以察觉。采用 MAC 地址表的方式对与用户直接相连的交换机各端口进行锁定虽然可以防止盗用，但在大中型网络中，对众多分布在不同地方的交换机的每个端口作绑定，管理性差，同时，价格问题也是一个考虑因素[1]。

多服务类型将更有利于运营商吸引用户，某些应用在内部网中实现往往比从 Internet 中下载要方便和容易得多，如视频点播等。一些用户可能愿意交更多的钱，而享受到特别的服务，例如更快的接入速度，访问运营商在内部网所设的视频服务器等。如果能够区分不同用户所允许的服务类型，运营商就能够按用户要求开展相关服务，从而吸引更多的用户。

PPPoE 是基于以太网的点对点通讯协议，它通过用户认证的方法有效地解决了上述问题，而且对运营商来说，在现有局域网基础上不必花费巨资来做大面积改造。因此，PPPoE 在宽带驻地接入中比其他协议更具有优势，已经是最佳选择方案。

2 PPPoE 的工作原理

PPPoE 有两个进程：发现进程和 PPP 会话进程。在发现进程中，主机必须找到并选定一个接入集中器（access concentrator）。当发现进程顺利完成，主机和选定的 AC 之间就有了用于在以太网中建立点对点连接的信息。进入 PPP 会话进程后，主机和 AC 之间为 PPP 虚拟接口分配资源，就基本上和 PPP 工作原理一样。

2.1 有关帧结构[2,3]

以太网的帧中，有一个 16 位的类型字段。在发现进程中，该字段为 0x8863；在 PPP 会话进程中则为 0x8864。

在 PPPoE 的以太网帧中，有效载荷字段如图 1 所示：

版本 (4 位)	类型 (4 位)	编码 (8 位)	会话 ID 号 (16 位)
长度 (16 位)			有效载荷

图 1 PPPoE 数据包结构

Fig. 1 PPPoE packet structure

有效载荷字段可以包含 0 或者多个 TAG，其结构如图 2：

TAG 类型 (16 位)	TAG 长度 (16 位)
TAG 值 ···	

图 2 TAG 结构

Fig. 2 TAG structure

TAG 类型和 TAG 值如表 1 所示。

* 收稿日期：2002 - 06 - 03
作者简介：徐霖洲（1978 年生），男，硕士研究生；通讯联系人：丘海明；E-mail：truejce @163.net

表 1 TAG 说明

Tab. 1 TAG details

TAG 类型	TAG 值	说明
0x0000	无	表示后面再没有 TAG（不一定要有）为了向后兼容所以定义
0xf0101	服务名称	如 ISP 名字、服务等级和 QoS 等
0x0102	AC 名称	可以是 AC 的 MAC 地址（UTF - 8 字符串表示）或者普通名称等
0x0103	Host - Uniq	主机用它来把 PADI 或 PADR 和 AC 的 PADO 或 PADS 联系起来
0x0104	AC - Cookie	AC 使用它来防止服务攻击
0x0105	运营商细节	运营商的一些信息
0x0110	中继会话 ID	在发现进程的数据包中用来表示中间代理，只能有一个
0x0201	服务名称错误	服务名称不可靠或请求被拒绝
0x0202	AC 系统错误	AC 在处理请求时出现错误
0x0203	一般错误	出现无法恢复的错误且没有其他表示错误的 TAG

2.2 发现进程[2,3] 发现进程有 4 个步骤，当进程完成后，主机和选定的 AC 间确定了 PPPoE 的会话 ID 号和对方 MAC 地址，使用这两个参数来唯一确认一个 PPPoE 会话。

第 1 步，主机发 PADI（PPPoE active discovery initiation）数据包。目的 MAC 地址为广播地址，编码字段为 0x09，会话 ID 号字段为 0x0000。PADI 数据包必须包含一个服务名称的 TAG，说明主机要请求的服务。

第 2 步，AC 用 PADO（PPPoE active discovery offer）数据包来响应 PADI 数据包。目的 MAC 地址为发 PADI 数据包主机的 MAC 地址，编码字段为 0x07，会话 ID 字段依然为 0x0000。PADO 数据包必须包含一个 AC 名称 TAG 和一个与 PADI 数据包相同的服务名称 TAG，如果 AC 可以提供更多的服务，它就可以在 PADO 数据包中加入其他的服务名称 TAG，如果不能为 PADI 提供服务，那么它将不会发 PADO 数据包作响应。

第 3 步，主机发 PADR（PPPoE active discovery request）数据包。主机可能收到不仅一个的 PADO。主机会选定其中一个 PADO。然后，主机就会发 PADR 数据包。目的 MAC 地址为所选 AC 的 MAC 地址，编码字段为 0x19，会话 ID 号字段仍是 0x0000。PADR 必须至少包含一个服务名称的 TAG，说明要请求的服务。

第 4 步，AC 发 PADS（PPPoE active discovery session-confirmation）数据包。当 AC 收到 PADR 数据包后，它就会准备开始 PPP 会话。AC 为 PPPoE 会话生成一个唯一的会话 ID 号，用于 PADS 数据包中的会话 ID 号字段，并发 PADS 数据包响应 PADR。目的 MAC 地址为发 PADR 数据包的主机的 MAC 地址，编码字段为 0x65。PADS 中同样要有一个服务名称的 TAG。如果 AC 无法响应 PADR 中的服务名称 TAG，PADS 中就会有一个服务名称错误的 TAG，且会话 ID 号字段为 0x0000。

当 AC 发出确认包以后，就开始进入 PPP 会话进程。当会话建立后，主机和 AC 都可以通过发 PADT（PPPoE active discovery terminate）数据包中断会话。目的 MAC 地址为对方的 MAC 地址，编码字段为 0xa7，会话 ID 号字段指出要中断的会话。

2.3 PPP 会话进程 一旦 PPPoE 会话开始，数据都以 PPP 封装而发送，其工作方式与 PPP 基本一样。具体可参阅文献[4]，此时，编码字段为 0x00，会话 ID 号字段为发现进程中获得的会话 ID 号并且始终保持一致，而 PPPoE 中的有效负载不再是 TAG，而是以 PPP 协议 ID 开头的 PPP 帧。

3 PPPoE 安全问题及其改进方案

PPPoE 的最大问题是它甚少考虑到安全性。

PPPoE 只在防止 DOS（denial of service）攻击方面作了一些措施，而且只可以一定程度地防止 DOS 攻击。更严重的是，PPPoE 在防止伪装 AC 方面没有任何安全措施。

由于 PPPoE 没有对 AC 的选择作出规定，用户如果错误的选择了伪装 AC 并与之建立连接，将造成安全性的问题。即使用户静态指定了 AC，伪装者也可以成对地修改伪装 AC 的 IP 和 MAC 地址，使人难以察觉。

例如，如果有人（假设此人叫 Tom）也架设一台 PPPoE 服务器，并使用无加密功能的 PAP 认证。由于现有的 PPPoE 在默认条件下，同时支持 PAP 和 CHAP 的认证方式，当合法用户错误选择了 Tom 的 AC 建立 PPP 会话，在要求认证时，客户端软件就会以明文的形式发送账号和密码发送给 Tom。Tom 就获得了用户的账号和密码[5]。

当然，在这个例子中，可以假设所有用户都有充分的网络知识和安全意识，即使在网络使用正常

的情况下，用户都去会关心自己是否强制使用了有加密功能的 CHAP 作认证，保证没有使用 PAP（因为不作强制并不影响用户使用网络）。这样，Tom 或许无法窃得用户的账号和密码了。但实际上，大部分用户连 PAP 和 CHAP 是什么都不知道[5]。

但是，如果 Tom 架设伪装 PPPoE 服务器的目的不是为了盗取账号和密码呢？Tom 也可以使用 CHAP，而且无论认证成功与否都使用户可以连接上他的伪装 AC，并且通过 NAT 等技术使用户能够通过伪装 AC 正常上网，进而监视用户数据而获得用户某些私隐信息。

即没有一个机制使得用户在发现进程中选择 AC 的时候发现网络中可疑的 AC。重新制定新的 PPPoE 标准来克服这个问题无疑是不合成本的，因此，需要一种在现有 PPPoE 基础上，在不改变原有流程和数据包结构的基础上作出改进的方案。

针对这点，提出 PPPoE 如下改进方案，其关键思想在于利用发现进程中的 TAG 字段，定义一种用于验证 AC 的 TAG 类型，并且通过使用单向散列函数的方法对 AC 做出验证。

(1) 主机发 PADI 时，除了服务名称 TAG 后，还要添加一个用于加密了类型的 TAG，TAG 值为一个伪随机数 Rh。

(2) 运营商架设的多个 AC 都有一个相同的伪随机数 Ra 作为密钥，当收到 PADI 时，各 AC 会用 Ra 和 Rh 作单向散列运算，得 E（Ra，Rh），并把它作为 PADO 的一个加密类型的 TAG 值发送。

(3) 伪装 PPPoE 服务器不知道 Ra，而且 PADO 也不是以广播的形式发送，因此，它无法轻易地获取 E（Ra，Rh）值，只能随便发送 E’填充该 TAG 字段。

(4) 主机接收 PADO 时，若发现两个不同的加密的 TAG 值时，就会发出警告，通知用户可能有人架设了伪装服务器。

这样做可以在一定程度上防止伪装，至少 Tom 要想继续伪装就得想个法子去截获 E（Ra，Rh），并在自己的 PADO 中加入该 E（Ra，Rh）的 TAG 则不会被发现。然而，可以再改进上面的做法以打消 Tom 的念头。

(1) 运营商架设 AC 都使用一个互不同伪随机数 Ra1、Ra2 ……作为自己密钥，并且把 Ra1、Ra2 ……作为密钥列表保存在每台 AC 的数据库中。

(2) 主机发 PADI 时，添加一个用于加密了类型的 TAG，TAG 值为一个伪随机数 Rh。

(3) 各 AC 在收到 PADI 时，会用自己的密钥 Rax（x 可能为 1、2 ……）和 Rh 作单向散列运算，分别得到 E（Rax，Rh），并把它作为自己 PADO 的一个加密类型的 TAG 值发送。

(4) 主机接收 PADO 时，若发现有两个相同的加密 TAG 值时，即发警告通知用户可能存在伪装服务器。这样即使 Tom 截获了某个 E（Rax，Rh）也无济于事。

(5) 主机选定 AC 后，向各个发 PADO 的 AC 都送一个确认包，里面有所选定的 AC 的 E（Rax，Rh）值。

(6) 各 AC 分别用 Ra1、Ra2 ……和 Rh 运算，看是否得到 E（Rax，Rh），若不能，则发警告通知用户可能存在伪装服务器。

参考文献：

[1] 张亮. 如何防止宽带网络地址被盗用[J]. 通信世界，2002(11):56.

[2] RFC 2516 ——A Method for Transmitting PPP Over Ethernet (PPPoE),February 1999.

[3] RFC 2119 ——Key words for use in RFCs to Indicate Requirement Levels,March 1997.

[4] RFC 1661 ——The Point - to - Point Protocol (PPP),July 1994.

[5] RFC 1994 ——PPP Challenge Handshake Authentication Protocol (CHAP),August 1996.

PPPoE’s Principle, Application and Improved Suggestion

XU Lin-zhou, QIU Hai-ming

(Department of Electronics and Communication Engineering,
Sun Yat-sen(Zhongshan) University, Guangzhou 510275, China)

Abstract: PPPoE is an effective access method of broadband network. It can prevent ip address from being stolen and benefit access controlling, but it has some disadvantages and secure leak for PPPoE. Its application and principle are introduced and then some suggestion for improvement is proposed.

Key words: PPPoE; AC; PAP; CHAP