

RFC2516 A Method for Transmitting PPP Over Ethernet (PPPoE)  
在以太网上传输 PPP 的方法 (PPPoE)

组织: 中国互动出版网 (<http://www.china-pub.com/>)

RFC 文档中文翻译计划 (<http://www.china-pub.com/compters/emook/aboutemook.htm>)

E-mail: [ouyang@china-pub.com](mailto:ouyang@china-pub.com)

译者: Hlp(hlp, [huangliuqi@hotmail.com](mailto:huangliuqi@hotmail.com))

译文发布时间: 2001-4-9

版权: 本中文翻译文档版权归中国互动出版网所有。可以用于非商业用途自由转载, 但必须保留本文档的翻译及版权信息。

Network Working Group

Request for Comments: 2516

Category: Informational

L. Mamakos

K. Lidl

J. Evarts

UUNET Technologies, Inc.

D. Carrel

D. Simone

RedBack Networks, Inc.

R. Wheeler

RouterWare, Inc.

February 1999

## 在以太网上传输 PPP 的方法 (PPPoE)

(RFC2516 A Method for Transmitting PPP Over Ethernet (PPPoE))

### 本备忘录状态

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

### 版权声明

Copyright (C) The Internet Society (1999). All Rights Reserved.

### 摘要

点到点协议(PPP, 参考文献[1])提供在点到点连路上传送多协议数据报的标准方法。本文档描述在以太网上建立 PPP 会话以及封装 PPP 数据报的方法。

### 可行性

本说明书试图提供 PPP 所定义的工具, 如链路控制协议(Link Control Protocol, LCP), 网络层控制协议(Network-layer Control Protocols, NCP), 认证以及其它机制。这些功能要求在通信双方之间存在点到点的关系, 而不是在以太网和其他多访问环境中所出现的多点关系。

本规范可用于同一个以太网上的多个主机通过一个或多个跨接(桥接)的调制解调器向多个目的主机开放其 PPP 会话。主要用于宽带远程访问技术, 即访问服务的提供者希望通过提供一个桥接的拓扑结构从而保持 PPP 会话摘要。

本文档描述的 PPPoE 是 RedBack Networks, RouterWare, UUNET 及其它厂商所采用的在以太网上封装 PPP 的方法。

## 目录

1. 简介 .....	3
2. 约定 .....	3
3. 协议总述 .....	3
4. 净载数据 .....	4
5. DISCOVERY 阶段 .....	5
5.1 PPPoE Active Discovery Initiation 数据包 (PADI) .....	5
5.2 The PPPoE Active Discovery Offer 数据包 (PAD0) .....	6
5.3 The PPPoE Active Discovery Request 数据包 (PADR) .....	6
5.4 The PPPoE Active Discovery Session-confirmation 数据包 (PADS) .....	6
5.5 THE PPPOE ACTIVE DISCOVERY TERMINATE 数据包 (PADT) .....	6
6. PPP 会话阶段 .....	7
7. LCP 方面的考虑 .....	7
8. 其它方面的考虑 .....	7
9. 安全方面的考虑 .....	8
10. 致谢 .....	8
11. 参考文献 .....	8
附录 A .....	8
附录 B .....	10
作者地址 .....	11
完整的版权通告 .....	12



## 1. 简介

现代访问技术有几个互相冲突的设计目标。人们想通过相同的以顾客为前提的访问设备（接入设备）来连接到远程站点上的多个主机，同时提供与拨号上网（使用 PPP）类似的访问控制和支付功能。在很多访问技术（接入技术）中，把多个主机连接到以顾客为前提的访问设备（接入设备）的最经济的方法就是通过以太网。另外，还想尽量保持设备的低成本同时要求不改变或很少改变其配置。

以太网上的 PPP (PPPoE) 提供通过简单桥接访问设备（接入设备）把一个网络的多个主机连接到远程访问集中器的功能。使用该模型，每一个主机使用自己的 PPP 协议栈，呈现给用户的还是熟悉的用户接口，访问控制、支付以及服务类型（type of service）都能基于每一个用户，而不是基于站点。

为了提供以太网上的点到点连接，每一个 PPP 会话必须知道远程通信对方的以太网地址，并建立一个唯一的会话标识符。PPPoE 包含一个（以太网地址）发现协议来提供这个功能。

## 2. 约定

本文当中出现的关键词**必须** (MUST), **不允许** (MUST NOT), **必需** (REQUIRED), **应该** (SHALL), **不应** (SHALL NOT), **应该** (SHOULD), **不应该** (SHOULD NOT), **推荐** (RECOMMENDED), **可以** (**可能**, MAY), 以及**可选** (OPTIONAL), 按参考文献[2]解释。中译版本将对这些关键词加粗并加上红色突出显示。

## 3. 协议总述

PPPoE 分为两个阶段，即 Discovery（地址发现）阶段和 PPP 会话阶段。当某个主机希望发起一个 PPPoE 会话时，它必须首先执行 Discovery 来确定对方的以太网 MAC 地址并建立起一个 PPPoE 会话标识符 SESSION\_ID。虽然 PPP 定义的是端到端的对等关系，Discovery 却是天生的一种客户端-服务器关系。在 Discovery 的过程中，主机（作为客户端）发现某个访问集中器（Access Concentrator，作为服务器），根据网络的拓扑结构，可能主机能够跟不止一个的访问集中器通信。Discovery 阶段允许主机发现所有的访问集中器并从中选择一个。当 Discovery 阶段成功完成之后，主机和访问集中器两者都具备了用于在以太网上建立点到点连接所需的所有信息。

Discovery 阶段保持无状态（stateless）直到建立起一个 PPP 会话。一旦 PPP 会话建立，主机和访问集中器两者都**必须**为一个 PPP 虚拟接口分配资源。



## 4. 净载数据

这里定义了下面所示的数据包格式。**payload** 的内容将在 Discovery 和 PPP 的章节中描述。

以太网的帧格式如下所示：

0								1							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
DESTINATION_ADDR (6 个字节)															
SOURCE_ADDR (6 个字节)															
ETHER_TYPE (2 个字节)															
payload ... ..															
CHECKSUM															

**DESTINATION\_ADDR** 域是一个以太网单播目的地址或者以太网广播地址(0xffffffff)。  
对于 Discovery 数据包来说, 该域的值是在 Discovery 章节中定义的单播或者多播地址。对于 PPP 会话流量来说, 该域**必须**是 Discovery 阶段已确定的通信对方的单播地址。

**SOURCE\_ADDR** 域**必须**包含源设备的以太网 MAC 地址。

**ETHER\_TYPE** 设置为 0x8863 (Discovery 阶段) 或者 0x8864 (PPP 会话阶段)。

PPPoE 的以太网 payload 如下所示：

0								1								2								3							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
VER				TYPE				CODE								SESSION_ID															
LENGTH																payload . . . . .															

**VER** 域为 4 位, PPPoE 规范的本版本**必须**设置为 0x1。

**TYPE** 域为 4 位, PPPoE 规范的本版本**必须**设置为 0x1。

**CODE** 域为 8 位, 其定义在后面的 Discovery 和 PPP 会话章节分别指定。

**SESSION\_ID** 域为 16 位, 是一个网络字节序的无符号值。其值在后面 Discovery 数据包中定义。对一个给定的 PPP 会话来说该值是一个固定值, 并且与以太网 SOURCE\_ADDR 和 DESTINATION\_ADDR 一起实际地定义了一个 PPP 会话。值 0xffff 为将来的使用保留, **不允许**使用。

**LENGTH** 域为 16 位。该值 (网络字节序) 表明了 PPPoE 的 payload 长度。不包括以太网头部和 PPPoE 头部的长度。

## 5. Discovery 阶段

Discovery 阶段由 4 个步骤组成。完成之后通信双方都知道了 PPPoE **SESSION\_ID** 以及对方以太网地址，它们共同定义了唯一的 PPPoE 会话。这些步骤包括：主机广播一个（会话）发起数据包（以请求建立链路），一个或多个访问集中器发送提供（服务）数据包，主机发送单播会话请求数据包以及选中的访问集中器发送确认数据包。当主机接收到该确认数据包后，它就可以进入 PPP 会话阶段。访问集中器发送确认数据包后，它就可以进入到 PPP 会话阶段。

Discovery 阶段所有的以太网帧的 **ETHER\_TYPE** 域都设置为 0x8863。

PPPoE 的 **payload** 部分包含 0 个或多个 TAG。一个 TAG 是一个 TLV(type-length-value) 结构，定义如下：

0								1								2								3								
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	4	1	2	3	4	5	6	7	8	9	0	1
TAG_TYPE																TAG_LENGTH																
TAG_VALUE   ...   ...																																

**TAG\_TYPE** 域为 16 位值（网络字节序），附录 A 列出了各种 TAG\_TYPE 和 TAG\_VALUE。

**TAG\_LENGTH** 域为 16 位，是无符号值（网络字节序），表明 TAG\_VALUE 的字节数。

如果收到的 discovery 数据包中包含未知的 TAG\_TYPE, 则



## 5.2 The PPPoE Active Discovery Offer 数据包(PADO)

如果访问集中器能够为收到的 PADI 请求提供服务, 它将通过发送一个 PADO 数据包来做出应答。**DESTINATION\_ADDR** 为发送 PADI 的主机的单播地址, **CODE** 域为 0x07, **SESSION\_ID** 域**必须**设置为 0x0000。

PADO 数据包**必须**包含一个类型为 AC-Name 的 TAG (包含了访问集中器的名字), 与 PADI 中相同的 Service-Name, 以及任意数目的类型为 Service-Name 的 TAG 表明访问集中器提供的其它服务。如果访问集中器不能为 PADI 提供服务, 则**不允许**用 PADO 作响应。

## 5.3 The PPPoE Active Discovery Request 数据包(PADR)

由于 PADI 是广播的, 主机可能收到不止一个 PADO, 它将审查接收到的所有 PADO 并从中选择一个。可以根据其中的 AC-Name 或 PADO 所提供的服务来作出选择。然后主机向选中的访问集中器发送一个 PADR 数据包。其中, **DESTINATION\_ADDR** 域设置为发送 PADO 的访问集中器的单播地址, **CODE** 域设置为 0x19, **SESSION\_ID** **必须**设置为 0x0000。

PADR **必须**包含且仅包含一个 TAG\_TYPE 为 Service-Name 的 TAG, 表明主机请求的服务, 以及任意数目其他类型的 TAG。

## 5.4 The PPPoE Active Discovery Session-confirmation 数据包(PADS)

当访问集中器收到一个 PADR 数据包, 它就准备开始一个 PPP 会话。它为 PPPoE 会话创建一个唯一的 **SESSION\_ID** 并用一个 PADS 数据包来给主机作出响应。**DESTINATION\_ADDR** 域为发送 PADR 数据包的主机的单播以太网地址, **CODE** 域设置为 0x65, **SESSION\_ID** **必须**设置为所创建好的 PPPoE 会话标识符。

PADS 数据包包含且仅包含一个 TAG\_TYPE 为 Service-Name 的 TAG, 表明访问集中器已经接受的该 PPPoE 会话的服务类型, 以及任意数目的其他类型的 TAG。

如果访问集中器不喜欢 PADR 中的 Service-Name, 那么它**必须**用一个带有类型为 Service-Name-Error 的 TAG (以及任意数目的其它 TAG 类型) 的 PADS 来作出应答。这种情况下, **SESSION\_ID** **必须**设置为 0x0000。

## 5.5 The PPPoE Active Discovery Terminate 数据包(PADT)

这种数据包可以在会话建立以后的任意时刻发送, 表明 PPPoE 会话已经终止。它可以由主机或访问集中器发送, **DESTINATION\_ADDR** 域为单播以太网地址, **CODE** 域设置为 0xa7, **SESSION\_ID** **必须**表明终止的会话, 这种数据包不需要任何 TAG。

当收到 PADT 以后, 就不允许再使用该会话发送 PPP 流量了。在发送或接收到 PADT 后, 即使是常规的 PPP 结束数据包也**不允许**发送。PPP 通信双方**应该**使用 PPP 协议自身来结束 PPPoE 会话, 但在无法使用 PPP 时**可以**使用 PADT。



## 6. PPP 会话阶段

一旦 PPPoE 会话开始, PPP 数据就像其它 PPP 封装一样发送。所有的以太网数据包都是单播的。ETHER\_TYPE 域设置为 0x8864。PPPoE 的 **CODE 必须** 设置为 0x00。PPPoE 会话的 **SESSION\_ID 不允许** 发生改变, **必须** 是 Discovery 阶段所指定的值。PPPoE 的 **payload** 包含一个 PPP 帧, 帧始于 PPP **Protocol-ID**。

附录 B 中给出了数据包的一个实例。

## 7. LCP 方面的考虑

**推荐** 使用 Magic Number LCP 配置选项, 不推荐使用协议域压缩 (Protocol Field Compression, PFC) 选项。**不允许** 实现请求使用下面的任何一个选项, 对此 **必须** 作出拒绝:

Field Check Sequence (FCS) Alternatives,  
Address-and-Control-Field-Compression (ACFC),  
Asynchronous-Control-Character-Map (ACCM)

协商后 (PPPoE) 的最大接收单元 (MRU) **不允许** 超过 1492。因为以太网的最大净载为 1500 字节, 而 PPPoE 头部为 6 个字节, PPP Protocol-ID 为 2 个字节, 所以 PPP 的 MTU **不允许** 超过 1492。

**推荐** 访问集中器不时向主机发送回声请求 (Echo-Request) 数据包, 以确定会话的状态。否则如果主机在没有发送结束请求 (Terminate-Request) 数据包的情况下终止会话, 则访问集中器将无法得知该会话已经“死去”。

当 LCP 结束的时候, 主机和访问集中器 **必须** 停止使用该 PPPoE 会话。如果主机希望开始另一个 PPP 会话, 则它 **必须** 重新进入 PPPoE Discoverey 阶段。

## 8. 其它方面的考虑

如果主机在一段指定时间内没有收到 PADO 数据包, 它 **应该** 重发其 PADI 数据包并把等待的间隔加倍。按所期望的次数重复这个动作。主机在等待接收 PADS 数据包时, **应该** 采用类似的定时机制, 只是主机重新发送的是 PADR 数据包。在重发指定次数后 (还没有收到 PADO), 主机 **应该** 重新发送 PADI。

本文档中的 **ETHER\_TYPE** (0x8863, 0x8864) 已经被 IEEE 指定专用于以太网上的 PPP (PPPoE), 使用这两个值和 PPPoE VER (版本) 域将唯一标识本协议。

本文档始终使用 UTF-8 (参考文献[5]) 而不是 ASCII。UTF-8 支持所有 ASCII 字符集同时允许国际字符集。参见参考文献[5]。



## 9. 安全方面的考虑

为了防止拒绝服务攻击 (Denial of Service, 简称 DOS), 访问集中器可以使用类型为 AC-Cookie 的 TAG。访问集中器**应该**能够根据 PADR 的 SOURCE\_ADDR 来重新产生具有唯一性的 TAG\_VALUE。使用这种方法, 访问集中器可以确保 PADI 的 SOURCE\_ADDR 确实是可到达的, 并对该地址的并行会话数进行限制。使用什么样的算法并没有指定, 留给实现细节自己选择。对主机 MAC 地址使用 HMAC(参考文献[3])就是一个例子, (在进行 HMAC 密码散列时)使用的是仅有访问集中器知道的密码。虽然 AC-Cookie 对防止某些 DOS 有用, 但它不能防止所有的 DOS 攻击, 访问集中器可以使用其它的方法来保护。

很多访问集中器不希望提供信息表明为未认证实体提供什么服务。在这种情况下, 访问集中器应该使用下面两种策略之一: 它**应该**根据请求中的 Service-Name 标签不拒绝该请求, 并返回收到的 TAG\_VALUE; 或者**应该**仅接受带有 TAG\_LENGTH 为 0 (表明任意服务) 的 Service-Name 标签的请求。**推荐**使用前一种方案。

## 10. 致谢

本文档建立在几个论坛所讨论概念的基础上, 包括 ADSL 论坛。还从 RFC 1661, RFC 1662 以及 RFC 2364 中借用了很多内容。

## 11. 参考文献

- [1] Simpson, W., Editor, “点到点协议 (PPP)”, STD 51, RFC 1661, July 1994
- [2] Bradner, S., “RFC 中表明条件级别的关键词”, BCP 14, RFC 2119, March 1997.
- [3] Krawczyk, H., Bellare, M. and R. Canetti, “HMAC:消息认证的密钥散列”, RFC2104, February 1998.
- [4] Reynolds, J. and J. Postel, “指定值”, STD 2, RFC 1700, October 1994. 参见: <http://www.iana.org/numbers.html>
- [5] Yergeau, F., “UTF-8, ISO 10646 的一种转换”, RFC 2279, January 1998.

## 附录 A

### TAG\_TYPE 和 TAG\_VALUE

0x0000 End-Of-List

该 TAG 表明表中没有其它 TAG 了。该 TAG 的 TAG\_LENGTH 必须总是 0。不要求使用该标签, 存在是为了向后兼容。

0x0101 Service-Name

该 TAG 表明后面紧跟的是服务的名称。TAG\_VALUE 是不以 NULL 结束的 UTF-8 字符串。当 TAG\_LENGTH 为 0 时, 该 TAG 用于表明接受任何服务。使用 Service-Name 标签的例



子是表明 ISP(Internet 服务提供商)或者一类服务或者服务的质量。

#### 0x0102 AC-Name

该 TAG 表明后面紧跟的字符串唯一地表示了某个特定的访问集中器。它可以是商标、型号以及序列号等信息的集合,或者该访问集中器 MAC 地址的一个简单的 UTF-8 表示。它不以 NULL 来结束。

#### 0x0103 Host-Uniq

该 TAG 由主机用于把访问集中器的响应 (PADO 或者 PADS) 与主机的某个唯一特定的请求联系起来。**TAG\_VALUE** 是主机选择的长度和值为任意的二进制数据。它不能由访问集中器解释。主机**可以**在 PADI 或者 PADR 中包含一个 Host-Uniq 标签。如果访问集中器收到了该标签,它**必须**在对应的 PADO 或者 PADS 中不加改变的包含该标签。

#### 0x0104 AC-Cookie

该 TAG 由访问集中器用于防止拒绝服务攻击(见“安全方面的考虑”)。访问集中器**可以**在 PADO 数据包中包含该 TAG。如果主机收到了该标签,它**必须**在接下来的 PADR 中不加改变的包含该标签。**TAG\_VALUE** 是长度和值任意的二进制数据,不能由主机解释。

#### 0x0105 Vendor-Specific

该 TAG 用来传送厂商自定义的信息。**TAG\_VALUE** 的头 4 个字节包含了厂商的识别码,其余字节尚未定义。厂商识别码的高字节为 0,低 3 个字节为网络字节序的厂商的 SMI 网络管理专用企业码,如“定义值 RFC”(参考文献[4])中定义的那样。

**不推荐**使用该 TAG。为了确保互操作性,实现**可以**悄悄的忽略 Vendor-Specific TAG。

#### 0x0110 Relay-Session-Id

该 TAG 可由中继流量的中间代理加入到 Discovery 数据包中。**TAG\_VALUE** 对主机和访问集中器都是晦涩难懂的 (paque)。如果主机或访问集中器收到该 TAG,则它们**必须**在所有的 Discovery 数据包中包含该 TAG 以作为响应。所有的 PADI 数据包必须保证足够空间来加入 **TAG\_VALUE** 长度为 12 字节的 Relay-Session-Id 标签。

如果 Discovery 数据包中已经包含一个 Relay-Session-Id 标签,则**不允许**再加入该标签。这种情况下,中间代理**应该**使用该现有的 Relay-Session-Id 标签。如果它不能使用现有的标签,或者没有足够空间来增加一个 Relay-Session-Id 标签,那么它应该向发送者返回一个 Generic-Error 标签。

#### 0x0201 Service-Name-Error

该 TAG(典型的有一个长度为零的数据部分)表明了由于某种原因,没有理解所请求的 Service-Name。如果有数据部分,并且数据部分的头一个字节非 0,那么它**必须**是一个可打印的 UTF-8 字符串,解释请求被拒绝的原因。该字符串**可以**不以 NULL 结束。

#### 0x0202 AC-System-Error

该 TAG 表明了访问集中器在处理主机请求时出现了某个错误。(例如没有足够资源来创建一个虚拟电路。PADS 数据包中可以包含该标签。

如果有数据,并且数据的第一个字节不为 0,那么(数据)必须是一个可打印的 UTF-8 字符串,该字符串解释了错误的性质。该字符串**可以**不以 NULL 结束。

#### 0x0203 Generic-Error

该 TAG 表明发生了一个错误。当发生一个不可恢复的错误并且没有其它合适的 TAG 时,它可被加到 PADO, PADR 或 PADS 数据包中。如果出现数据部分,那么数据**必须**是一个 UTF-8 字符串,解释错误的性质。该字符串**不允许**以 NULL 结束。



### PADI 数据包:

0								1								2								3							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
0xffffffff																															
0xffff																Host_mac_addr															
Host_mac_addr (续)																															
ETHER_TYPE = 0x8863																v = 1				t = 1				CODE = 0x09							
SESSION_ID = 0x0000																LENGTH = 0x0004															
TAG_TYPE = 0x0101																TAG_LENGTH = 0x0000															

0								1								2								3							
1	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Host_mac_addr																															
Host_mac_addr (续)																Access_Concentrator_mac_addr															
Access_Concentrator_mac_addr (续)																															
ETHER_TYPE = 0x8863																v = 1				t = 1				CODE = 0x07							
SESSION_ID = 0x0000																LENGTH = 0x0020															
TAG_TYPE = 0x0101																TAG_LENGTH = 0x0000															
0x47								0x6f								0x20								0x52							
0x65								0x64								0x42								0x61							
0x63								0x6b								0x20								0x2d							
0x20								0x65								0x73								0x68							
0x73								0x68								0x65								0x73							
0x68								0x6f								0x6f								0x74							

0								1								2								3							
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Access_Concentrator_mac_addr																															
Access_Concentrator_mac_addr(c)																Host_mac_addr															
Host_mac_addr (cont)																															
ETHER_TYPE = 0x8864																v = 1				t = 1				CODE = 0x00							
SESSION_ID = 0x1234																LENGTH = 0x????															
PPP_PROTOCOL = 0xc021																PPP payload . . . . .															



## 作者地址

Louis Mamakos  
UUNET Technologies, Inc.  
3060 Williams Drive  
Fairfax, VA 22031-4648  
United States of America  
EMail: louie@uu.net

Kurt Lidl  
UUNET Technologies, Inc.  
3060 Williams Drive  
Fairfax, VA 22031-4648  
United States of America  
EMail: lidl@uu.net

Jeff Evarts  
UUNET Technologies, Inc.  
3060 Williams Drive  
Fairfax, VA 22031-4648  
United States of America  
EMail: jde@uu.net

David Carrel  
RedBack Networks, Inc.  
1389 Moffett Park Drive  
Sunnyvale, CA 94089-1134  
United States of America  
EMail: carrel@RedBack.net

Dan Simone  
RedBack Networks, Inc.  
1389 Moffett Park Drive  
Sunnyvale, CA 94089-1134  
United States of America  
EMail: dan@RedBack.net

Ross Wheeler  
RouterWare, Inc.  
3961 MacArthur Blvd., Suite 212  
Newport Beach, CA 92660  
United States of America  
EMail: ross@routerware.com



## 完整的版权通告

Copyright (C) The Internet Society (1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.