

技 术 报 告

DSL 论 坛

TR - 069

CPE WAN 管 理 协 议

2004 年 5 月

作者:

DSLHOME-Technical Working Group

编辑:

**Jeff Bernstein, 2Wire
Time Spets, Westell**

工作组召集人

**Greg Bathrick, Texas Instruments
George Pitsoulakis, Westell**

内容摘要:

适用于 CPE 与自动配置服务器(ACS: Auto-Configuration Server)之间的通信协议，包括安全地自动配置及其它在公用框架下的 CPE 管理功能。

声明:

The DSL Forum is a non-profit corporation organized to create guidelines for DSL network system development and deployment. This Technical Report has been approved by members of the Forum. This document is not binding on the DSL Forum, any of its members, or any developer or service provider involved in DSL. The document is subject to change, but only with approval of members of the Forum.

©2001 Digital Subscriber Line Forum. All Rights Reserved.

DSL Forum technical reports may be copied, downloaded, stored on a server or otherwise re-distributed in their entirety only.

Notwithstanding anything to the contrary, the DSL Forum makes no representation or warranty, expressed or implied, concerning this publication, its contents or the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind shall be assumed by the DSL Forum as a result of reliance upon any information contained in this publication. The DSL Forum does not assume any responsibility to update or correct any information in this publication.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise any express or implied license or right to or under any patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein.

NOTE: The user's attention is called to the possibility that compliance with this report may require use of an invention covered by patent rights.

By publication of this report, no position is taken with respect to the validity of the claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the publisher.

目 录

1	序言	7
1.1	功能组件.....	7
1.1.1	自动配置和动态服务供给	7
1.1.2	软件/固件的映像管理.....	7
1.1.3	状态和性能监视.....	7
1.1.4	诊断.....	8
1.1.5	WEB应用的身份管理.....	8
1.2	在自动配置架构中的定位.....	8
1.3	安全目标.....	9
1.4	架构目标.....	9
1.5	假定.....	10
1.6	术语.....	10
1.7	文档约定.....	11
2	架构	11
2.1	协议组成.....	11
2.2	安全机制.....	12
2.2.1	安全初始化模型.....	12
2.3	架构组成.....	13
2.3.1	参数.....	13
2.3.2	文件传输.....	14
2.3.3	CPE发起通知	14
2.3.4	异步ACS发起通知.....	14
3	过程与要求.....	15
3.1	ACS发现	15
3.2	连接的建立.....	16
3.2.1	CPE连接的发起	16
3.2.2	ACS连接的发起.....	17
3.3	使用SSL/TLS和TCP.....	17
3.4	使用HTTP.....	18
3.4.1	SOAP Over HTTP编码.....	18
3.4.2	事务会话.....	19
3.4.3	文件传输.....	19
3.4.4	认证.....	19
3.5	使用SOAP.....	20

3.6	PRC支持需求.....	23
3.7	事务会话过程.....	24
3.7.1	CPE操作	25
3.7.2	ACS操作	26
3.7.3	事务示例.....	27
	参考规范	29
	附录A RPC方法.....	30
A.1	简介.....	30
A.2	RPC方法的使用	30
A.2.1	数据类型.....	30
A.2.2	其它要求.....	31
A.3	标准的RPC报文	31
A.3.1	通用方法.....	31
A.3.1.1	GetRPCMethods	31
A.3.2	CPE方法.....	32
A.3.2.1	SetParameterValues.....	32
A.3.2.2	GetParameterValues	33
A.3.2.3	GetParameterNames.....	33
A.3.2.4	SetParameterAttributes	34
A.3.2.5	GetParameterAttributes.....	36
A.3.2.6	AddObject.....	37
A.3.2.7	DeleteObject.....	38
A.3.2.8	Download	38
A.3.2.9	Reboot	40
A.3.3	服务器方法.....	40
A.3.3.1	Inform.....	40
A.3.3.2	TransferComplete.....	43
A.4	可选的RPC报文	44
A.4.1	CPE方法.....	44
A.4.1.1	GetQueuedTransfers.....	44
A.4.1.2	ScheduleInform	44
A.4.1.3	SetVouchers.....	45
A.4.1.4	GetOptions	45
A.4.1.5	Upload.....	46
A.4.1.6	FactoryReset.....	47
A.4.2	服务器方法.....	47
A.4.2.1	Kicked	47

A.4.2.2 RequestDownload	48
A.5 错误处理.....	49
A.5.1 CPE错误代码.....	49
A.5.2 服务器错误代码.....	49
A.5.3 服务器方法的重试行为.....	49
附录B. CPE参数.....	51
B.1 简介.....	51
B.2 CPE参数.....	51
B.2.1 数据类型.....	51
B.2.2 厂商自定义参数.....	52
B.2.3 参数列表.....	53
附录C. 签名凭据.....	84
C.1 概述.....	84
C.2 使用凭据控制选项.....	84
C.3 凭据定义.....	84
附录D. Web身份管理	89
D.1 概述.....	89
D.2 使用Kicked PRC方法	89
D.3 Web身份管理过程.....	89
D.4 LAN端接口	90
附录E. 签名包格式.....	92
E.1 简介.....	92
E.2 签名包格式结构.....	92
E.2.1 编码约定.....	92
E.3 头格式.....	93
E.4 命令列格式.....	93
E.4.1 命令类型.....	93

E.4.2	End 命令.....	94
E.4.3	Extract 和 Add 命令	95
E.4.4	Remove 命令.....	96
E.4.5	Move 命令.....	96
E.4.6	Version 和 Description 命令.....	97
E.4.7	Timeout 命令.....	97
E.4.8	Reboot 命令.....	98
E.4.9	Format File System	99
E.4.10	Minimum 和 Maximum Version 命令.....	99
E.4.11	Role 命令.....	100
E.4.12	Minimum Storage 命令.....	100
E.4.13	Required Attributes 命令.....	100
E.5	签名.....	101
翻译词汇对照表		102

1 序言

本文档描述 CPE WAN 管理协议，适用于 CPE 与自动配置服务器（ACS）间的通信。CPE WAN 管理协议定义包括安全地自动配置 CPE 以及在公用框架下的其它 CPE 管理功能。

1.1 功能组件

CPE WAN 管理协议支持管理 CPE 的一组功能，主要包括：

- 自动配置和动态服务供给
- 软件/固件的映像管理
- 状态与性能监控
- 诊断

1.1.1 自动配置和动态服务供给

CPE WAN 管理协议允许 ACS 通过多种准则来实现对一台或一组 CPE 的供给。供给机制包括规定供给参数和为支持厂商自定制供给能力而提供的通用机制。

供给机制允许 CPE 在连接到宽带网络的初始化阶段实现供给，并且允许以后重新供给，包括支持异步 ACS 发起的 CPE 重新供给。

本协议包含的认证机制允许基于一台 CPE 需要，或基于一些组合准则，比如 CPE 厂商，型号，软件版本等进行 CPE 供给。

协议同时提供可选工具，管理 CPE 相关的对安全有更高层次要求的可选应用或服务组件，比如与收费相关的应用或服务。附录 C 中定义如何通过数字签名凭据来控制这些选项的机制。

供给机制还允许对未来的尚未包含在本版本规范中的服务及性能进行直接扩展。

1.1.2 软件/固件的映像管理

CPE WAN 管理协议提供管理 CPE 软件/固件映像下载的工具。协议提供版本鉴别，文件下载的发起（ACS 发起或者可选的 CPE 发起），以起文件下载成功或失败后对 ACS 的通知。

CPE WAN 管理协议还定义一种数字签名的文件格式，可选地用来下载单个文件或者文件包，并且提供给 CPE 如何安装的明确指令。这种签名包格式保证下载的文件以及后续安装指令的完整性，同时对文件来源的身份进行认证，以避免来自除 ACS 以外的其它数据源的更新。

1.1.3 状态和性能监视

CPE WAN 管理协议支持 CPE 向 ACS 提供可能用于状态和性能统计数据。协议定义其公用参数集，并提供厂商在定义 ACS 能够监视的其它非标准参数时使用标准语法。它还定义 CPE 主动通知 ACS 自身变动的条件集合。

1.1.4 诊断

CPE WAN 管理协议支持 CPE 向 ACS 提供可用于诊断连接性和服务的信息。本协议定义一组公用参数集合，以及厂商添加自定义诊断能力的通用机制。

1.1.5 WEB 应用的身份管理

为了支持在 CPE 的本地网络中用浏览器来访问的基于 WEB 的应用，CPE WAN 管理协议定义一个可选机制，允许这样的 WEB 站点用相关的 CPE 的明确信息来自定制网页内容。该机制在附录 D 中描述。

1.2 在自动配置架构中的定位

TR-046[2]描述了 B-NT 自动配置的总体构架。这一过程包括三个连续的阶段，每个阶段集中描述总体 B-NT 自动配置过程的一个特定方面。

B-NT 自动配置前两个阶段的过程分别在 TR-062[3]和 TR-044[4]中定义。这两个规范分别定义了 ATM 层和 IP 层用来发起基本宽带连接的自动配置过程。

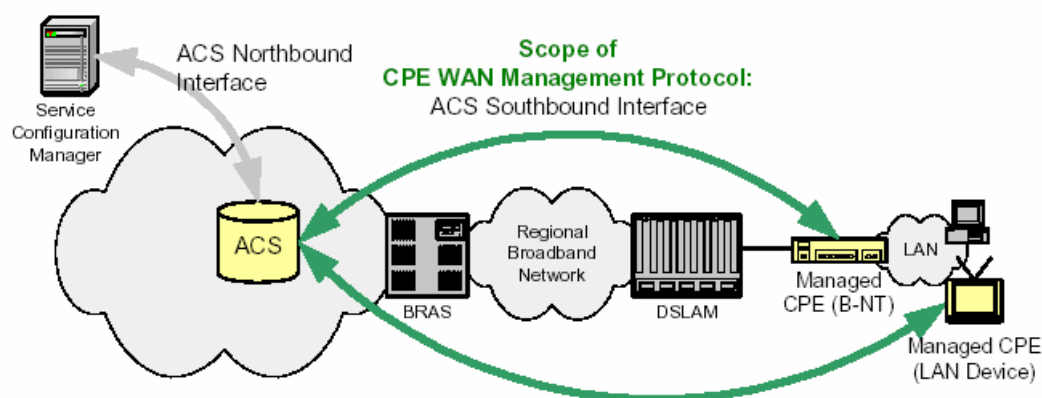
第三阶段的自动配置由 TR-046 定义，涵盖“自动配置复杂服务”。在 B-NT 情况下，CPE WAN 管理协议主要与该第三阶段有关。特别地，CPE WAN 管理协议被提议用于自动配置服务器（ACS）与 B-NT 之间的 ACS-Southbound 接口协议，如图 1 所示。

说明：在 B-NT 的情况下，与 TR-046 的嵌套模型相反，本协议还允许在未使用另一自动配置协议的情况下，对 ATM 层参数进行配置，如 TR-062 的定义。然而，如果另一个可选协议已经使用，那么本协议中对 ATM 层参数的配置就不能启用。

除了配置，本协议还提供从 ATM 层和 DSL Modem 中提取诊断和性能监视数据的途径。同样，这是与 TR-046 描述的嵌套模型相背的，但提供了一种可选方式来存取通过已有管理协议如 ILMI 和 DSL 链路的 EOC 而获取信息。通过本协议来提供更多高级诊断和性能监视功能是需要更深入研究的课题。

尽管 CPE WAN 管理协议致力于管理 B-NT，然而本协议也可以用来管理其它类型的 CPE，包括独立路由器和 LAN 端的客户端设备，如图 1 所示。除非另加说明，本规范定义的 CPE WAN 管理协议适用于任何这些被管理的设备。本规范中仅适用于 B-NT 的部分会作明确说明。本规范包括 B-NT 适用的 CPE 参数模型的完整定义。其它设备类型的相应参数模型超出了本规范的范围。

图 1 - 在自动配置架构中的定位



1.3 安全目标

CPE WAN 管理协议设计提供高安全级别。安全模型亦设计为能够扩展，允许在不太健壮的 CPE 部署下使用基本安全级别，而对能支持更高级安全机制的部署则允许使用更高安全级别。通常来讲，CPE WAN 管理协议的安全目标如下：

- 防止篡改 CPE 或者 ACS 的管理功能，或者两者之间的事务。
- 加密发生在 CPE 和 ACS 之间的事务。
- 允许每种类型的事务有恰当的身份确认。
- 防止服务被盗用。

1.4 架构目标

本协议的目的是对各种分发和管理 CPE 的商业模型提供灵活的支持，包括：

- 网络提供商来提供和管理 CPE。
- 以零售方式售出 CPE，预先将之注册，即与服务提供商和用户帐户（是一个与移动电话类似的模型）关联。
- 以零售方式售出 CPE，在安装后与服务提供商进行用户注册。

本协议的目的是在连接模型中提供灵活性。协议提供：

- 允许 CPE 和 ACS 发起建立连接，避免维持 CPE 和 ACS 之间的永久连接。
- ACS 和 CPE 之间的功能性交互作用应当与哪端先发起连接独立。特别地，即使在 ACS 发起连接不被支持的情况下，所有 ACS 发起的事务应当能够在 CPE 发起的连接上进行。
- 允许一个或多个 ACS 服务器为全部 CPE 提供服务，即使 CPE 是由一个或多个服务提供商提供。
- 优化已建立连接的使用，允许多条双向事务在同一个连接上进行，以最小化连接的负荷。

本协议用于支持 ACS 和 CPE 的发现和关联：

- 提供 CPE 在指定服务提供商时自动发现合适的 ACS 的机制。
- 提供允许 ACS 安全地鉴别 CPE 并将之与用户/客户关联起来的机制。支持这类关联的程序应当支持用户交互式及全自动式两种模型。

本协议模型允许通过访问 ACS 来控制 and 监视与 CPE 关联的各种参数。提供访问这些参数的机制基于以下假设而设计：

- 不同的 CPE 能够拥有不同性能级别，部署不同可选功能子集。因此，ACS 必须能够发现特定一台 CPE 的性能参数。
- ACS 必须能控制和监视 CPE 当前的配置。
- 除 ACS 外的其它控制实体能够控制 CPE 配置的某些参数（如，通过 LAN 端的自动配置）。因此，协议必须允许 ACS 能够解释对 CPE 配置的外源性改变。ACS 应当也能够控制哪些配置参数可由除 ACS 外的其它手段控制。
- 协议应当允许定义和访问厂商自定义参数。

本协议用于简化实施的复杂性，并提供在功能与复杂性之间折衷的灵活度。协议拥有一些可选的组件，只有在需要特定功能时才启用。协议同时结合适当的已有标准，允许利用已有实施。

本协议设计提供可扩展性。它包括支持未来对该标准的扩展机制，及基于厂商扩展的明确机制。

1.5 假定

在定义 CPE WAN 管理协议时所作的假定列示如下：

- 在 B-NT 情况下，在使用 CPE WAN 管理协议之前，在 TR-062[3]和 TR-044[4]中定义的 B-NT 初始自动配置已经完成，与 WAN 的连接已经建立，并且该 ACS 通过 WAN 可以访问到。
- 所有类型的CPE（网桥¹，路由器等）在与ACS通信之前要获得IP地址。
- 在某一个时刻，一台 CPE 只能与一台 ACS 交互作用。在任何时刻，一台 CPE 只知道它能连接的一台 ACS。只有明确地改变与 ACS 的联系方式和身份鉴别方式，ACS 才能将一台 CPE 转移给另一 ACS。（注意：在本文档中，在负载均衡设备后面的一组 ACS 服务器被认作为一台 ACS。）

1.6 术语

定义 CPE WAN 管理协议的一系列文档使用以下术语。

ACS	自动配置服务器(Auto-Configuration Server)。这是在宽带网络中负责 CPE 设备自动配置，以实现高级服务的组成要素。
B-NT	宽带访问 CPE 设备，能够被 ACS 所管理。
CPE	客户端设备（Customer Premise Equipment）。DSL B-NT 就是一类宽带 CPE。

¹ 在网桥（Bridge）的情况下，CPE必须建立专门用于管理通信的IP层连接。这一用于建立该连接的机制依赖于特定的网络结构。比如，一台网桥可能通过IPoE及DHCP来获得地址，或可能通过PPPoE来连接。

Internet Gateway Device/Internet 网关设备

CPE 设备，B-NT 或者是宽带路由器。

- Option/选项**可选的 CPE 功能，只能用数字签名凭据（digital signed Voucher）来启用或禁用。
- RPC**远程过程调用（Remote procedure call）。
- Parameter/参数**“名称-值”对，代表可管理的 CPE 参数，并可由 ACS 进行读和/或写。
- Session/会话**发生在 CPE 与 ACS 之间的事务序列。
- Voucher/凭据**数字签名的数据结构，指示某台 CPE 启用或禁用**选项**，以及用来决定在何种条件下，**选项**能够继续的属性。

1.7 文档约定

本文档中所用的关键词 “必须”（MUST），“不得”（MUST NOT），“要求”（REQUIRED），“会”（SHALL），“不会”（SHALL NOT），“应当”（SHOULD），“不应当”（SHOULD NOT），“建议”（RECOMMENDED），“可以”（MAY），和“可选的”（OPTIONAL）在[1]的描述中进行限定。

2 架构

2.1 协议组成

CPE WAN 管理协议包括几项本协议特有的组件，也使用几项标准协议。CPE WAN 管理协议定义的协议栈如图 2 所示。表 1 对协议各层进行了简单描述。

图 2 – 协议栈

CPE/ACS Management Application
RPC Methods
SOAP
HTTP
SSL/TLS
TCP/IP

表 1 – 协议各层概要

层	描述
CPE/ACS Application (CPE/ACS 应用)	分别在 CPE 和 ACS 运行的 CPE WAN 管理协议应用。应用由本地定义，并且不作为 CPE WAN 管理协议的一部分进行说明。
PRC Methods (RPC 方法)	CPE WAN 管理协议定义的特定 RPC 方法。这些方法在附录 A 中说明。 RPC 方法 包括定义 CPE 参数 。这些 参数 可由 ACS 通过与该 参数 相关的 PRC 方法 访问。专门为 Internet 网关设备 定义的参数在附录 B 中说明。
SOAP	基于 XML 的标准语法，用于编码远程过程调用。特别地，SOAP 1.1，由[8]定义。
HTTP	HTTP 1.1，由[5]定义。
SSL/TLS	标准的 Internet 传输层安全协议。特别的，SSL 3.0 (Secure Socket Layer)，由[10]定义，TLS 1.0 (Transport Layer Security) 由[11]定义。使用 SSL/TLS 是 建议 而非要求。
TCP/IP	标准 TCP/IP。

2.2 安全机制

CPE WAN 管理协议的设计允许基于该协议的交互作用具有高度安全性。CPE WAN 管理协议的设计防止 CPE 和 ACS 之间的事务被篡改，提供事务机密性，及允许多层次认证。

本协议使用下述安全机制：

- 协议支持 CPE 和 ACS 间的通信传输使用 SSL/TLS，提供事务机密性，数据完整性，以 CPE 和 ACS 间基于证书的认证。
- HTTP 层提供另一种基于共享密钥的 CPE 认证方法。

协议包括其它与可选签名凭据机制和签名包格式（Signed Package Format）相关的安全机制，分别在附录 C 和附录 E 中描述。

2.2.1 安全初始化模型

安全机制的初始化在不同的 CPE 分发商业模型背景下描述。考虑到三种商业模型：

- ACS 关联的服务提供商分发 CPE。
- CPE 的零售分发模型，CPE 与服务提供商和客户之间的关联在购买时刻确定。
- 零售分发，无任何 CPE 关联信息。

在前两种情况下，CPE 的身份在它第一次使用前，ACS 就能够了解。此时，下

述机制可以使用：

认证主体	使用的类型	描述
ACS	共享密钥	第一次使用 CPE 前，共享密钥必须事先在 CPE 中装载。
	证书	3.1 节描述的发现的 ACS URL 作为认证的证书，唯一地认证 ACS 身份。
CPE	共享密钥	在第一次使用 CPE 前，共享密钥必须先提供给 ACS。
	证书	CPE 可以使用与 ACS 相关的 CA 进行在线证书的登记。必须提供给 CPE 所需的信息以联系该 CA。

在最后一种 CPE 零售分发情形下，不可能将 CPE 与特定 ACS 预先关联。下表展示了适应这种情形的可能解决方法，但并没有试图指定一个特定解决方法。

认证主体	使用的类型	描述
ACS	共享密钥	不适合本情况。
	证书	由 3.1 节所描述的 ACS URL 发现作为证书的验证唯一地认证了 ACS 的身份。
CPE	共享密钥	可能的、但在本规范之外的方法： <ul style="list-style-type: none">● 在多个服务提供商间，建立 CPE 共享密钥安全分发的公用服务器。● 允许未经认证的未知 CPE 建立与 ACS 的初始化连接。ACS 在随后设置 CPE 共享密钥。在 ACS 的实现中需要注意防止 DOS（Denial of Service）攻击。
	证书	CPE 可以使用与 ACS 相关的 CA 进行在线证书的登记。必须提供给 CPE 所需的信息以联系该 CA，这可以通过发现过程获得。

2.3 架构组成

2.3.1 参数

RPC 方法说明（见附录 A）定义通用机制，通过该机制，ACS 可以向 CPE 读或写**参数**，以对 CPE 进行配置或监视 CPE 状态和统计数据。专为 **Internet 网关设备**所定义的**参数**列表在附录 B 中说明。

每个**参数**包含一个名称-值对。名称用于区分不同的**参数**，采用与目录文件相似的层次化结构，级与级间用“.”（点）隔开。**参数**值取值于定义的数据类型（见附录 B）。

参数可以定义为只读或读写。只读**参数**用于允许 ACS 获知特定的 CPE 特性，观

察 CPE 当前的状态，或者收集统计数据。可写**参数**允许 ACS 自定义 CPE 操作的不同方面。所有可写**参数**必须同时是可读的。一些可写**参数**可以独立地通过在本规范所定义的接口外的方式（比如，一些**参数**可以通过 LAN 端的自动配置协议）进行更改。

本协议支持发现机制，允许 ACS 获知一台特定 CPE 支持哪些**参数**，允许定义可选的参数，同时支持对未来标准**参数**的直接增加。

本协议还包括一个可扩展机制，允许使用除本规范定义之外的厂商定制**参数**。

2.3.2 文件传输

RPC 方法规范（见附录 A）定义为实现不同目标而进行文件下载或（可选的）上传的机制，比如对固件或厂商自定义配置文件的更新。

ACS 发起文件传输后，CPE 将获得传输文件的位置，使用 HTTP 协议、或者可选的使用 HTTPS、FTP 或者 TFTP 作为传输协议。CPE 接着执行传输，并向 ACS 通告成功或者失败。

可选地，可由 CPE 首先发起下载。在这种情况下，CPE 首先向 ACS 请求某一特定文件类型的下载。之后，作为对 CPE 请求的回应，ACS 可以通过与 ACS 自主发起下载相同的步骤开始文件下载。

CPE WAN 管理协议还定义数字签名文件格式，可选地用于下载。签名包格式在附录 E 中进行定义。

2.3.3 CPE 发起通知

RPC 方法规范（见附录 A）定义允许 CPE 通知相应 ACS 各种状态的机制，确保 CPE 到 ACS 的通信能够占用很少的频带。

这一机制包括在 CPE 初始化安装建立通信连接时，通过开机自陷方式（bootstrap）获得初始化定制**参数**；也包括在工作过程中与 ACS 建立定期通信，或者发生了必须向 ACS 报告的事件（比如当 CPE 的广播 IP 地址发生了改变）。ACS 必须能够获知这类事件，以建立与 CPE 之间的进向连接。

在每种情形下，当通信建立时，CPE 通过制造商及序列号信息唯一地标识自己，使 ACS 了解正在进行通信的是哪台 CPE，并以恰当的方式来回应。

2.3.4 异步 ACS 发起通知

服务自动配置的一个重要方面是 ACS 能够异步地通知 CPE 某一配置的改变。这使得自动配置机制可用于需要对 CPE 进行近于实时配置的服务。比如，这一特性可用来给最终用户立即提供预定服务/特性，而无需等待下一阶段通知的时延。

CPE WAN 管理协议内置在任何时刻 ACS 向 CPE 发出连接请求的机制，指示 CPE 建立与 ACS 之间的通信会话。

同时 CPE WAN 管理协议也允许 CPE 轮询而不是由 ACS 发起连接，而 CPE WAN 管理协议并不依赖于轮询或与 CPE 建立永久连接来提供异步通知。

3 过程与要求

3.1 ACS 发现

CPE WAN 管理协议定义如下可用于 CPE 发现它所关联的 ACS 地址的机制：

1. 可以在 CPE 本地配置 ACS 的 URL。例如，这可通过 LAN 端的自动配置协议来完成。CPE 可使用 DNS 来解析 URL 中 ACS 主机名部分所对应的 IP 地址。
2. 作为 IP 层的自动配置方式，在网络中的 DHCP 服务器可以将 ACS 的 URL 配置为其 DHCP 选项[12]之一。CPE 通过 DNS 将 URL 中 ACS 主机名部分解析为 ACS 的 IP 地址。这种情况下，可以用另一个 DHCP 选项设置供给编码（ProvisioningCode），向 ACS 提供其主服务提供商及其它配置信息。

CPE 通过将其厂商类型标志（Vendor Class Identifier，DHCP 选项 60）中包括“dslforum.org”（全部小写）来向 DHCP 服务器表明自己支持这一方法。

CPE 可以使用从 DHCP 服务器获得厂商相关信息（Vendor Specific Information, DHCP 选项 43）来设置相应的参数，见表 2。这一 DHCP 选项按一个或多个封装的厂商相关选项（Encapsulated Vendor-Specific Options）表进行编码，其格式在[12]中定义。该表可以包括其它未列示于此的厂商相关选项。

表 2 - 封装的厂商相关选项

封装的选项	封装的厂商相关选项号	参数 ²
ACS 的 URL	1	InternetGatewayDevice.ManagementServer.URL
供给编码	2	InternetGatewayDevice.DeviceInfo.ProvisioningCode

3. CPE 可以设置默认 ACS URL，当没有其它 URL 信息提供时，使用该默认值。

ACS URL 必须使用有效的 HTTP 或 HTTPS URL 形式[5]。使用 HTTPS URL 表明 ACS 支持 SSL。如果获得了 HTTPS URL，但 CPE 不支持 SSL，则它可以试图使用 HTTP，而保持后面的 URL 不变。

一旦建立了与 ACS 的连接，ACS 可以在任何时刻更改存储在 CPE 中（InternetGatewayDevice.ManagementServer.URL）的 ACS 的地址参数。一旦发生改变，CPE 必须使用更改后的地址进行与 ACS 的后续连接。

ACS URL 的“主机名”(host)部分在 CPE 通过基于证书的认证方式中验证 ACS 身份时使用。由于它依赖于 ACS URL 的精确度，该协议的安全性依赖于 ACS URL 的安全性。

² 针对Internet网关设备定义。

CPE 应当限制在本地配置 ACS URL 的能力以适应要求严格安全性的机制。CPE 可以进一步限制仅能在初始化安装时在本地设置 ACS URL，防止与 ACS 初始化连接建立起来以后再进行本地配置。这样，后续的对 URL 的更改只能由 ACS 来完成。

使用 DHCP 来配置 ACS URL 应当限于一定的条件，即 DHCP 服务器与 CPE 之间的链路是由服务提供商提供安全保障的。由于 DHCP 本身并没有提供安全机制，因此，必须提供其它安全性保证机制。

3.2 连接的建立

3.2.1 CPE 连接的发起

CPE 可以在任何时刻通过前面决定的 ACS 地址（见 3.1 节）发起与 ACS 的连接。在下述情况中，CPE 必须建立与 ACS 的连接，并启用 Inform RPC 方法（使用 3.7 节描述的过程）：

- 在初始化安装时，CPE 第一次建立与网络的连接
- 在加电或重置时
- 在每个 PeriodicInformInterval（比如，每 24 小时）
- 当可选的 ScheduleInform 方法被要求时
- 当 CPE 接收到来自 ACS 的有效连接请求时（见 3.2.2 节）
- 当 ACS 的 URL 变化时
- 当参数发生更改，而此参数要求在改变时发起 Inform 报文。对 **Internet 网关设备**，涉及改变的参数包括（见 A.3.3.1）：
 - 默认宽带连接的 IP 地址
 - 管理 IP 地址（与连接请求 URL 关联）
 - 供给代码
 - 软件版本
- 当由 ACS 通过 SetParameterAttributes 方法标定为“主动通告”（active notification）的参数值发生了外在原因导致的改变（该改变源非 ACS 自身）。由 ACS 自身通过 SetParameterValues 对参数的改变不得引发初始化新会话。如果在 CPE 初始化会话前，参数发生多次变化，只能进行一次通告。

如果外在原因引起参数变化需要建立新的会话，而原来尚有会话在进行中，则新会话必须在现有会话结束后再建立（新会话不得影响现有会话）。

为了避免 ACS 过多负荷，CPE 可以在本地定义一个发送参数更改通告的频率限值。这一限值应当予以定义，并且只能在异常情况下允许超过该值。如果超出该值，CPE 可根据本地定义会话初始值作延迟再通知 ACS。在延迟过后，CPE 必须发起与 ACS 的会话，以说明所有自上次通告以来所有的相关参数的变化（在通告中标明的那些参数）。

当 CPE 与 ACS 间不存在未传输报文时，CPE 不应当保持与 ACS 的活动连接。

3.2.2 ACS 连接的发起

ACS 可在任何时刻要求 CPE 使用连接请求（Connection Request）通告机制发起与 ACS 的连接。CPE **要求**支持这一机制，而 ACS 则**建议**支持该机制。

该机制的依赖条件是 CPE 拥有 ACS 通过路由可达到的 IP 地址。如果 ACS 与 CPE 之间存在防火墙或 NAT 设备，CPE 在该设备之后，则 ACS 根本不能访问 CPE。在这种情况下，只有 CPE 发起连接的可能性存在。

连接请求通告机制定义如下：

- 连接请求通告是 CPE 指定的特定 URL 的 HTTP Get。该 URL 值是 CPE 的只读**参数**。URL 值的路径**应当**由 CPE 随机产生，以使每台 CPE 的值不同。
- 连接请求通告**必须**使用 HTTP，而不是 HTTPS。相关的 URL **必须**是一个“http” URL。
- 在连接请求 HTTP Get 通告中不会承载数据。任何可能的数据都**应当**由 CPE 忽略。
- CPE **应当**在处理该报文之前，使用摘要认证（digest-authentication）来认证 ACS——如果认证失败，CPE **不应当**向 ACS 发起连接。认证 ACS 使用的共享密钥是 CPE 的可更改**参数**。
- CPE **应当**限制在指定时间段接收连接请求通告的次数以进一步减少可能发生的拒绝服务（DOS）攻击。
- 对指定端口和 URL 的 HTTP Get 成功认证后，CPE 会执行一个固定的动作：它与预先已确定的 ACS 地址（见 3.1 节）建立会话，并在成功建立会话连接后发送一条 Inform 报文。
- 如果 CPE 接收到一条连接请求通告时，已经与 ACS 建立了一个会话，则 CPE **不得**因此而过早地结束该会话。

本机制的前提是 ACS 在此前至少有一次由 CPE 发起的通信。在该通信中，如果 ACS 希望允许将来进行 ACS 发起的通信，则会读取 InternetGatewayDevice.ManagementServer.ConnectionRequestURL 参数的值。如果该管理用 URL 值改变，CPE 必须发出一条 Inform 报文通知 ACS 说明新的管理 IP 地址（如表 33 的描述），以维护 ACS 信息的及时更新。

3.3 使用 SSL/TLS 和 TCP

尽管 CPE WAN 管理协议可以直接使用 TCP 连接来实现，但**建议**使用 SSL/TLS 来传输。如果没有使用 SSL/TLS，则会牺牲某些方面的安全性。特别地，SSL/TLS 提供机密性和数据完整性，允许基于证书认证而不是共享密钥认证。

使用 SSL/TLS 和 TCP 的部分约束如下：

- 如果支持 SSL/TLS，则**要求**使用的版本为 SSL 3.0[10]或 TLS 1.0[11]。
- 如果支持 SSL/TLS，则**应当**支持密钥长度大于或等于 128 位的加密算法。
- CPE 必须能够发起与 ACS 的外向连接。
- ACS **必须**能够接受 CPE 发起的连接。
- 如果使用 SSL/TLS，CPE **必须**使用 ACS 提供的证书认证 ACS。

- 如果使用 SSL/TLS，ACS 可以接受 CPE 提供的有效证书来认证 CPE，但如果 CPE 没有提供证书，ACS 也必须允许 SSL/TLS 连接的建立。

3.4 使用 HTTP

CPE 和 ACS 间的 SOAP 报文使用 HTTP 1.1[5]来承载。此时，CPE 是 HTTP 的客户端，ACS 是 HTTP 的服务器。

3.4.1 SOAP Over HTTP 编码

SOAP Over HTTP 编码，扩展下列 SOAP 定义的基本 HTTP 特性（在[8]中描述）：

- ACS 发送给 CPE 的 SOAP 请求基于 HTTP response，而 CPE 返回给 ACS 的 SOAP 应答则基于后续的 HTTP post。
- 每个 HTTP post/response 可包含多于一个 SOAP 信包（在已协商的限度内）。每个信包可以与其它信包独立地包含一个 SOAP 请求或回应。
- 当一个 HTTP request 包含多于一个信包时，HTTP request 中的 SOAP Action 包头必须不包含值（即无引用），以说明该包头不提供信息，这也是该条报文的目的是。也就是说，它应当显示为：

SOAPAction:

Inform 报文中含有一个称作 MaxEnvelopes 的参数，向 ACS 指明可在一个 HTTP response 中最多可包含的 SOAP 信包的最大数目。该值可为 1 或者更高。一旦已经接收了 Inform 报文，任何从 ACS 发出的 HTTP response 可以包括至少该数目的 SOAP 信包（requests 或 responses。）

Inform 回复也包含一个称为 MaxEnvelopes 的参数，向 CPE 指定在一个 HTTP post 中可以包含的最大数据的 SOAP 信包。其值可以为 1 或更高。一旦接收了 Inform 应答，任何 CPE 发出的 HTTP post 可以包括至少这一值的 SOAP 信包（requests 或 responses）。

在每个方向上，SOAP 信包的次序与承载每个 HTTP post/response 对的信包数目独立。特别地，信包在一个 HTTP post/response 中从前到后排序，然后是后续的 post/response 对。也就是说，在一个 HTTP post/response 内的，和后续的 post 或 response 形成的一系列信包，可以被认作是一个单一排序的信包序列。

为保证对请求和应答的正确关联，请求者可以在 SOAP 包头中加入一个 ID 的标识。如果采用了这一标识，必须在应答中返回相同的值。这一信头的编码在 3.5 节中进行描述。

下面是一个 ACS 的 HTTP Response 的例子，例子中既包含对前面 SOAP 请求的应答，也包含一个未关联的 SOAP 请求。

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset="utf-8"
Content-Length: xyz

<soap:Envelope
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:cwmp="urn:dslforum-org:cwmp-1-0">
  <soap:Header>
    <cwmp:ID soap:mustUnderstand="1">1234</cwmp:ID>
  </soap:Header>
  <soap:Body>
```

```
<cwmp:Response1>
  <argument>value</argument>
</cwmp:Response1>
</soap:Body>
</soap:Envelope>

<soap:Envelope
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:cwmp="urn:dslforum-org:cwmp-1-0">
  <soap:Body>
    <cwmp:Request2>
      <argument>value</argument>
    </cwmp:Request2>
  </soap:Body>
</soap:Envelope>
```

3.4.2 事务会话

在构成一个会话的一系列事务中，CPE 应当在整个会话中维持不间断的 TCP 连接。

为适应不能维持持续 TCP 连接的情形（比如，通过 HTTP 1.0 代理的操作），ACS 应当使用会话 cookie 来维护会话的状态，见[7]中的描述。ACS 只应当使用一种标记为丢弃（Discard）的 cookie，而不应当认为在会话之后，CPE 还会维护 cookie。

为保护 ACS 可以使用会话 cookie，CPE 必须支持在[7]中定义的 cookie，在每一个后续的 HTTP post 中返回 cookie 值，并支持 CPE 在会话结束后不再支持 cookie 的存储。

当事务会话结束后，CPE 必须结束与 ACS 的相关 TCP 连接，并丢弃所有的标记为 Discard 的 cookie。

3.4.3 文件传输

如果 CPE 收到 ACS 的下载或上载请求，要求执行文件传输，并且标明该文件位置的 HTTP URL 中的主机名与 ACS 相同，则 CPE 可以选择以下的任一种方法来执行传输：

- CPE 可以在已经建立的连接上发送 HTTP get/post。一旦文件传输结束，CPE 可以继续发送其它信息给 ACS 并继续维持该连接。
- CPE 可以打开另一条连接，通过它来传输文件，并同时维持与 ACS 的会话，在该会话中，CPE 可以继续发送报文。
- CPE 可以结束与 ACS 的会话，然后执行传输。

如果文件位置不是 HTTP URL，或者文件不在 ACS 上，则只能使用后面的两种选项。

3.4.4 认证

如果 CPE 没有经 SSL/TLS 进行认证，ACS 必须通过 HTTP 对 CPE 进行认证。如果 SSL/TLS 用于加密，ACS 可以使用基本或摘要认证[6]。如果没有使用 SSL/TLS，则 ACS 必须使用摘要认证。

在首次 HTTP 事务中，ACS 可以进行一次认证，并且在整个 TCP 连接中不需再进行认证。

如果用任何形式的 HTTP 认证来认证 CPE，CPE 应当使用用户名/用户 ID，并且该值在所有 CPE 生产商中是唯一的。特别的，它应当是包含多个部分的字符串，包括厂商 ID 及在厂商内的唯一的序列号。该字符串的**推荐**格式如下：

OUI-SERIAL

其中 OUI 是 6 位十六进制字符，全部使用大写字母，并包含任何前缀零。OUI 的值**必须**是有效的由[9]中定义的 OUI。如果厂商有多种 CPE 产品，并且序列号范围重叠，SERIAL 字符串**必须**包括其它的区分字符，以保证该字符串的唯一性。

例如：“00D09E-0123456789”

在每种方式的 HTTP 认证中，所使用的密钥**应当**对每台 CPE 是唯一的。也就是说，多台 CPE **不应当**共享相同的密钥。该密钥是共享密钥，因此 CPE 和 ACS 都**必须**知晓。在 CPE 初始化安装时，让双方都知晓该密钥的方法不在本规范的讨论范围内（见 2.2.1 节）。CPE 和 ACS 都应当采取适当的步骤来防止对密钥（ACS 中为密钥表）的非授权访问。

3.5 使用 SOAP

CPE WAN 管理协议定义 SOAP 1.1[8]为编码语法，来传输 RPC 调用和应答方法（在附录 A 中定义）。

下面描述了 RPC 方法与对应的 SOAP 编码：

- 编码必须使用标准的 SOAP 1.1 信包和序列号名称空间：
 - 信包名称空间标识 “<http://schemas.xmlsoap.org/soap/envelope/>”
 - 序列号名称空间标识 “<http://schemas.xmlsoap.org/soap/encoding/>”
- 本版本的 CPE WAN 管理协议定义的所有元素和属性均与下列名称空间标识关联：
 - urn:dslforum-org:cwmp-1-0”
- 附录 A 中使用的数据类型，与 SOAP 1.1 的序列号名称空间一致。（通常情况下，在附录 A 中使用的类型限制为相应 SOAP 类型的子集。）
- 对参数数组，指定的参数名称与所有数组元素的名称一致。对每个单独的成员元素不再指定名称，而是用类型命名。例如，对名称为 ParameterList，类型为 ParameterValueStruct 结构的参数，可以如下编码：

```
<ParameterList soap:arrayType="cwmp:ParameterValueStruct [2]">
  <ParameterValueStruct>
    <name>Parameter1</name>
    <value xsi:type="someType">1234</value>
  </ParameterValueStruct>
  <ParameterValueStruct>
    <name>Parameter2</name>
    <value xsi:type="someType">5678</value>
  </ParameterValueStruct>
</ParameterList>
```

- 对 RPC 方法编码的 SOAP 规范（[8]的第 7 节），对附录 A 中定义的每种方法，每个方法调用的参数表示为[in]参数，而每个方法应答的参数表示为一个[out]参数。没有使用[in/out]参数。

- 使用标准的 SOAP 名称约定定义的 RPC 方法中，与指定方法对应的应答报文命令是在该方法名称上加前缀“Response”。
- 错误应答**必须**使用 SOAP 错误元素，使用下面约定：
 - SOAP 的 faultcode 元素**必须**指明该错误对应的源头是在客户方还是服务器方。在这里，客户方代表 SOAP request 的发起方，而服务方代表 SOAP 的应答方。
 - SOAP 的 faultstring 子元素**必须**包含字符串“CWMP fault”。
 - SOAP 的 detail 元素**必须**包含一个在“urn:dslforum-org:cwmp-1-0”名称空间中定义的错误结构。该结构包含以下元素：
 - FaultCode 元素，包含一个数字型的错误代码，在附录 A 中定义。
 - FaultString 元素，包含一个可人读的错误描述。
 - SetParameterValuesFault 元素，仅用于对 SetParameterValues 方法的错误应答。它包括一个或多个结构表，指明与每个错误参数关联的特定错误信息。该结构包括下列元素：
 - ParameterName 元素，包含错误参数的全路径名。
 - FaultCode 元素，包含一个数字型错误代码（在附录 A 中定义），指定错误参数相关的错误。
 - FaultString 元素，包含一个可人读的对错误参数发生的错误的描述。

下面的定义错误结构的 XML 模式（XML-schema）段：

```
<xs:element Name="Fault">
  <xs:complexType>
    <xs:sequence>
      <xs:element Name="FaultCode" Type="unsignedInt"/>
      <xs:element Name="FaultString" Type="string" minOccurs="0"/>
      <xs:element Name="SetParameterValuesFault" minOccurs="0" maxOccurs="unbounded">
        <xs:complexType>
          <xs:sequence>
            <xs:element Name="ParameterName" Type="string"/>
            <xs:element Name="FaultCode" Type="unsignedInt"/>
            <xs:element Name="FaultString" Type="string" minOccurs="0"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
    </xs:sequence>
  </xs:complexType>
</xs:element>
```

下面是一个包含错误应答的信包例子：

```
<soap:Envelope
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:cwmp="urn:dslforum-org:cwmp-1-0">
  <soap:Header>
    <cwmp:ID soap:mustUnderstand="1">1234</cwmp:ID>
  </soap:Header>
  <soap:Body>
    <soap:Fault>
      <faultcode>Client</faultcode>
      <faultstring>CWMP fault</faultstring>
      <detail>
        <cwmp:Fault>
          <FaultCode>9000</FaultCode>
        </cwmp:Fault>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

```
        <FaultString>Upload method not supported</FaultString>
      </cwmp:Fault>
    </detail>
  </soap:Fault>
</soap:Body>
</soap:Envelope>
```

下面是一个信包例子，包含一个 SetParameterValues 方法调用的错误应答：

```
<soap:Envelope
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:cwmp="urn:dslforum-org:cwmp-1-0">
  <soap:Header>
    <cwmp:ID soap:mustUnderstand="1">1234</cwmp:ID>
  </soap:Header>
  <soap:Body>
    <soap:Fault>
      <faultcode>Client</faultcode>
      <faultstring>CWMP fault</faultstring>
      <detail>
        <cwmp:Fault>
          <FaultCode>9003</FaultCode>
          <FaultString>Invalid arguments</FaultString>
          <SetParameterValuesFault>
            <ParameterName>
              InternetGatewayDevice.Time.LocalTimeZone
            </ParameterName>
            <FaultCode>9012</FaultCode>
            <FaultString>Not a valid time zone value</FaultString>
          </SetParameterValuesFault>
          <SetParameterValuesFault>
            <ParameterName>
              InternetGatewayDevice.Time.LocalTimeZoneName
            </ParameterName>
            <FaultCode>9012</FaultCode>
            <FaultString>String too long</FaultString>
          </SetParameterValuesFault>
        </cwmp:Fault>
      </detail>
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

- 为了将来扩展，在处理接收到的信包时，ACS和CPE都必须忽略：（a）所有未知的XMS元素³及其子元素和内容，（b）所有未知的XML属性及其值，（c）任何XML的注释和（d）任何XML处理指令。

CPE WAN 管理协议定义一系列 SOAP 头元素，见表 3。

表 3 – SOAP 头元素

标记名称	描述
ID	<p>该头元素可以用于将 SOAP 的请求和应答关联起来，方法是为每个请求使用唯一的 ID，而对应的应答中包含相同的 ID。ID 值为任何字符，由请求方决定。</p> <p>如果在 SOAP 请求中使用，该 ID 必须出现在对应的应答中（不管应答是成功还是失败）。</p> <p>由于该头元素是要求的，因此它的 mustUnderstand 属性必须设置为“1”</p>

³ 一种情况除外，当收到未知的SOAP动作，应当产生一个错误应答，指示Method Not Supported（见附录 A）。

标记名称	描述
	(true) 。
HoldRequests	<p>该头元素可以用于 ACS 发送给 CPE 的信包，用来规范来自 CPE 请求的传输。它不得出现在 CPE 发送给 ACS 的信包中。</p> <p>该标记值为布尔型“0”（false）或“1”（true）。如果标记不存在，可以解释为“0”（false）。</p> <p>CPE 接收到该头元素后的动作在 3.7.1.3 节中定义。CPE 要求支持该头元素。</p> <p>如果 ACS 必须更新流控制（flow-control）状态，但没有其它报文发送，它可以发送一个信包，含有该头和空包体。</p> <p>由于对该头的支持是要求的，因此它的 mustUnderstand 属性必须设置为“1”（true）。</p>
NoMoreRequests	<p>该头可以包含在 ACS 或 CPE 发送的信包中，用于明确向接受方指明是否它不得在后续会话中发送更多请求。</p> <p>该标记取值布尔型“0”（false）或“1”（true）。如果该标记不存在，则其值被解释为“0”（false）。可以在最后请求的信包或其后的信包中将该标记值设置为“1”。在会话中一旦设置为 true，该值应当在随后发送的所有信包中也设置为 true，并且在该会话中发送方不得再发送其它的请求报文。</p> <p>CPE 接收到该头后的动作在 3.7.1.4 节中定义。CPE 可选地支持该头的发送和接受。</p> <p>ACS 接收到该头后的动作在 3.7.2.4 节中定义。ACS 可选地支持该头的发送和接受。</p> <p>由于对该头的支持是可选的，因此，其 mustUnderstand 属性可以被设置为“0”，也可以不存在。</p>

下面是一个使用所有定义头元素的报文例子：

```
<soap:Envelope
  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:cwmp="urn:dslforum-org:cwmp-1-0">
  <soap:Header>
    <cwmp:ID soap:mustUnderstand="1">1234</cwmp:ID>
    <cwmp:HoldRequests soap:mustUnderstand="1">0</cwmp:HoldRequests>
    <cwmp:NoMoreRequests>1</cwmp:NoMoreRequests>
  </soap:Header>
  <soap:Body>
    <cwmp:Action>
      <argument>value</argument>
    </cwmp:Action>
  </soap:Body>
</soap:Envelope>
```

3.6 PRC 支持需求

表 4 提供所有方法的概要，说明在附录 A 中定义每个 RPC 方法的实现是要求还是可选，以及其条件。

RPC 报文需求

方法名称	CPE 需求	服务器需求
CPE 方法	应答	调用
GetPRCMethods	要求	可选
SetParameterValues	要求	要求
GetParameterValues	要求	要求
GetParameterNames	要求	要求
SetParameterAttributes	要求	可选
GetParameterAttributes	要求	可选
AddObject	要求	可选
DeleteObject	要求	可选
Reboot	要求	可选
Download	要求 ⁴	要求
Upload	可选	可选
FactoryReset	可选	可选
GetQueuedTransfers	可选	可选
ScheduleInform	可选	可选
SetVouchers	可选 ⁵	可选
GetOptions	可选	可选
服务器方法	调用	应答
GetRPCMethods	可选	要求
Inform	要求	要求
TransferComplete	要求 ⁶	要求 ⁷
RequestDownload	可选	可选
Kicked	可选	可选

3.7 事务会话过程

所有事务会话必须从 CPE 包含在初始 HTTP post 中的 Inform 报文开始。主要用于初始化事务集，并与 CPE 交换与报文编码有关的限制事项。

当 ACS 与 CPE 都没有更多请求需要传输，ACS 或者 CPE 上都没有尚未回复的应答时，会话将结束。此时，CPE 会关闭连接。

在同一时刻，CPE 与其关联的 ACS 之间不会存在超过一个事务会话。

注 – 只要有报文还需在任一方向上进行传输，事务会话才需要继续存在。会话与其相关的 TCP 连接在相关的信息交换结束后，不会保持打开状态。

⁴ 仅在支持任何类型的文件下载条件下需要。

⁵ 如果支持凭据机制，则 SetVouchers 和 GetVouchers 方法均需要。

⁶ 仅在支持任何类型的文件下载与上载时才需要。

⁷ 仅在 ACS 支持发起文件的下载或上载时才需要。

3.7.1 CPE 操作

3.7.1.1 会话的发起

CPE 在节 3.2.1 列示的条件下，将会向 ACS 发起一个事务会话。一旦与 ACS 的连接成功建立，CPE 发送一条初始 Inform 请求给 ACS，以开始一个会话。它向 ACS 说明 CPE 的当前状态，并且 CPE 已经准备好接收 ACS 的请求。

在承载 Inform 请求的该初始 HTTP post 中，只允许一个 SOAP 信包。Inform 应答中 MaxEnvelopes 参数指明后续 HTTP post 可承载信包的最大数目。

只有在 CPE 锁定本身该接口的参数，确保不会由其它机制更改后，CPE 才应当发起会话。CPE 应当维持该锁定状态，直到会话结束。

3.7.1.2 进向请求

从 ACS 接到 SOAP 请求后，CPE 必须以接收次序回复每一条请求。次序的定义见 3.4.1 节的描述。这一定义没有限制多个请求是在同一个 HTTP post 包中发送的（如果 ACS 能够接受超过一个信包）还是分布在多个 HTTP post 中

为防止死锁，CPE 不得推迟到一条对 ACS 请求的回复，以等待 ACS 对前一条 CPE 请求进行回复。

3.7.1.3 出向请求

当 CPE 有请求报文需要发送（在最初的 Inform 请求之后），该请求可以插入到 CPE 向 ACS 发送的应答序列的任何位置。也就是说，CPE 可以在它向 ACS 传输信包序列的任何位置插入一个或多个请求。没有指定 CPE 接收回复（未完成请求的数目）前可以发送多少个请求的限值。如果希望，CPE 可以在本地指定限值。

如果 CPE 从 ACS 接收到 HoldRequests 值为 True（见 3.5 节）的信包（无论请求或者应答），CPE 不得在随后的 HTTP post 中发送任何请求。只有再收到后续的 HoldRequest 值为 False 的信包（或者没有 HoldRequests 的信包）后，CPE 才能重新开始发送信包。为了决定它能否发送请求，CPE 必须检查收到的所有信包，包括所有收到的最近的 HTTP response。根据 3.4.1 节定义的信包顺序，只有 HTTP response 的最后一个信包决定是否在下一个 HTTP post 中允许发送请求，因此，如果 CPE 收到一条空的来自 ACS 的 HTTP response，就可以解释为 HoldRequests 的值为 false。

如果有来自 ACS 的一条或多条未处理完的请求，或者如果 CPE 有一条或多条未处理完的请求，并且 HoldRequests 的值为 false，则 CPE 必须在 HTTP post 中发送至少一条请求或应答给 ACS。如果 ACS 没有未发送完的请求或应答，必须发送一条空的 HTTP post。表 5 列示了在会话进行中 CPE 必须发送内容的完整约束集合。

表 5 – CPE 报文传送限制

有等待处理的 CPE 请求	HoldRequests	有等待的 ACS 请求	无等待的 ACS 请求
	False	一个或多个应答及/或请求	一个或多个请求
	True	一个或多个应答	空 HTTP post

无等待处理的 CPE 请求	-	一个或多个应答	空 HTTP post
---------------	---	---------	-------------

3.7.1.4. 会话的终止

CPE 必须结束事务会话，当以下条件全部满足时：

- 1) ACS 没有更多请求发送给 CPE。如果以下任一条件满足，CPE 会作该认定：
 - a) 从 ACS 收到的最近 HTTP response 没有信包。
 - b) 从 ACS 收到的最近信包（其顺序在 3.4.1 节定义）包括一个 NoMoreRequests 的信包头并且值为 true（见 3.5 节）。CPE 是否使用这一信包头是可选的。
- 2) CPE 没有更多的请求发送给 ACS。
- 3) CPE 已经从 ACS 接收到所有未处理完的应答报文。
- 4) CPE 已经把原有请求的所有应答报文发送给 ACS。

当 CPE 在本地定义的一个不短于 30 秒的时间段后，还没有从 ACS 收到 HTTP response，CPE 也必须中止会话。

如果上述条件没有满足，则 CPE 必须维持会话。

如果在会话中交换报文的结果需要 CPE 重新启动以完成所需的操作，则 CPE 必须等到会话根据以上标准判断已经完全结束后才能重新启动。

如果会话异常结束，CPE 应当试图建立新会话，从头开始建立会话过程。CPE 可以使用一个本地定义的限值，来限制在此情况下最多可以进行多少次重建会话的尝试。

3.7.2 ACS 操作

3.7.2.1. 会话的发起

在接收到 CPE 初始 Inform 请求后，ACS 必须用 Inform 应答回复。ACS 可以在此后向 CPE 发送一系列请求。

Inform 请求的 MaxEnvelopes 参数指定 ACS 发送给 CPE 的 HTTP response 中可以承载的最大信包数目。如果 CPE 可以接受多于一个信包，则初始承载 Inform 应答的 HTTP response 也可以包含额外的不超过 MaxEnvelopes 规定数目的请求。

3.7.2.2. 进向请求

从 CPE 接受到 SOAP 请求后，ACS 必须按照接收次序来回复每个请求。该次序在 3.4.1 节中定义。该次序的定义没有限制多个应答是以一个 HTTP response 承载发送（如果 CPE 可以接受多于一个信包）还是分散在多个 HTTP response 中。

为防止死锁，ACS 不得推迟到一条对 CPE 请求的应答，以等待 CPE 对前一条 ACS 请求进行应答。

如果 ACS 希望防止 CPE 在会话的某段时间内发送请求，它可以通过在每个传送给 CPE 的信包中，将 HoldRequests 信包头值设置为 true 来实现。当 ACS 再希望接受 CPE 请求时，将信包中 HoldRequests 值再设为 false。在结束会话前，ACS 必须允许 CPE 请求（可以通过明确的 HoldRequests 值或隐含地通过发送一个空

的 HTTP response 来实现。)

3.7.2.3. 出向请求

当 ACS 有请求报文发送时，它可以以任何次序发送请求，而不必管需要 ACS 发送给 CPE 的应答。也就是，ACS 可以在它向 CPE 传输的信包序列的任何位置插入一个或多个请求（在 Inform 应答之后）。没有指定的限制值，以限制 ACS 在接收回复（未完成请求的数目）前可以发送多少个请求。如果希望，ACS 可以在本地指定一个限额。

如果 ACS 仍有需要传送的一个或多个请求，及/或有一个或多个等待应答的 CPE 请求，ACS 必须在发回给 CPE 的 HTTP response 中包括至少一个请求或应答。只有在 ACS 没有请求和等待的应答时，才能发送一个空的 HTTP response。

3.7.2.4. 会话的终止

由于 CPE 是与 ACS 进行 HTTP 连接的驱动方，因此，只有 CPE 负责连接的初始和结束。

ACS 可以认为会话已经结束，当以下条件**全部**满足时：

- 1) CPE 没有更多的请求发送给 ACS。如果以下任一条件满足，ACS 会作上述认定：
 - a) 从 CPE 收到的最近 HTTP post 不包含信包。
 - b) 从 CPE 收到的最近信包（其顺序在 3.4.1 节中定义）包括一个 NoMoreRequests 信包头并且其值为 true（见 3.5 节）。ACS 是否使用这一信包头是**可选的**。
- 2) ACS 没有发送给 CPE 的更多请求。
- 3) CPE 已经发送给 ACS 以前所有请求的应答。
- 4) ACS 已经接收到 CPE 发送的所有应答报文。

如果上述标准没有完全满足，但 ACS 在本地定义的一个不短于 30S 的时间段后，还没有从指定的 CPE 收到 HTTP post，ACS 可以认为该会话已经终止。在这种情况下，ACS 可以试图执行**连接请求**（Connection Request）以重建连接（见 3.2.2 节）。

3.7.3 事务示例

在图 3 显示的例子中，ACS 首先读取一系列参数值，然后根据结果，来设置参数值。例子显示，CPE 和 ACS 定义的 MaxEnvelopes 均为 1，所以没有来自 ACS 的请求流水线，也没有来自 CPE 的一个 HTTP post 中的多个信包。

图 3 – CPE 及 ACS 的 MaxEnvelopes 的值均为 1 的例子

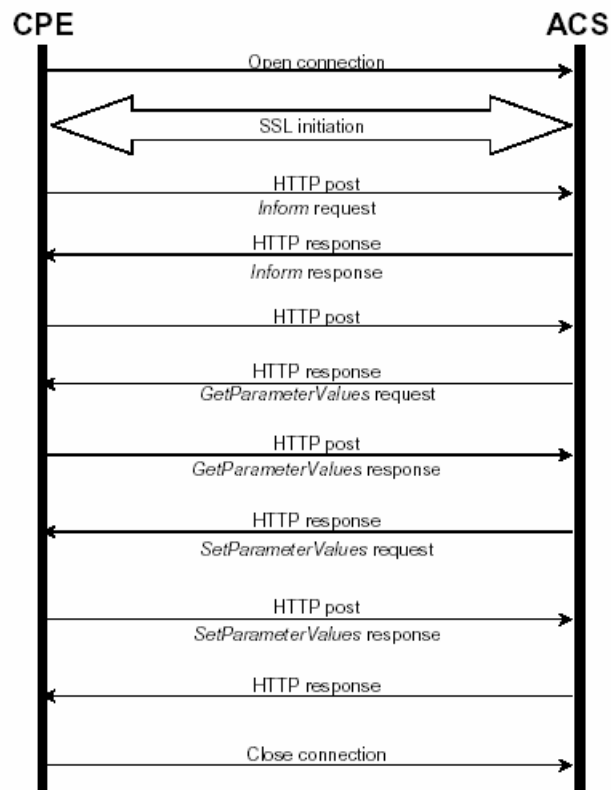
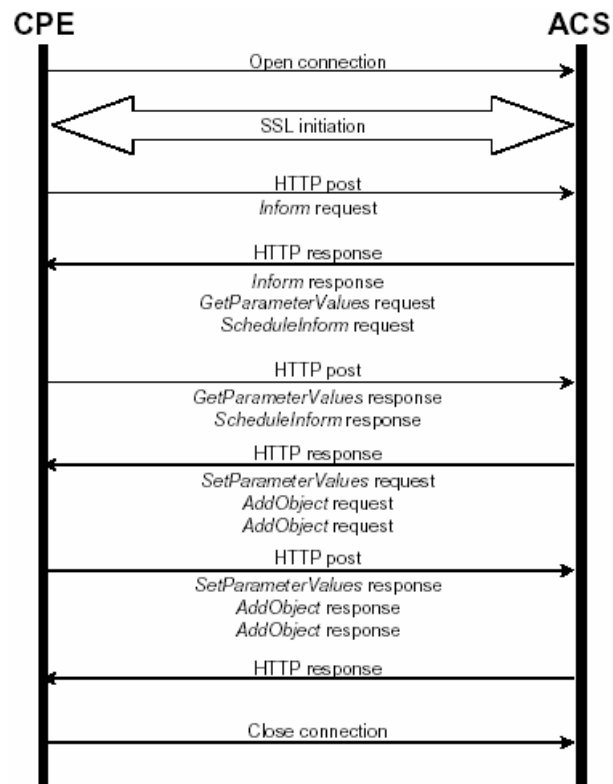


图 4 的例子显示 CPE 和 ACS 的 MaxEnvelopes 的值均为 3 的场景，允许在双向使用报文流水线。在此例子中，还显示一些源自 ACS 的其它请求。

图 4 - CPE 及 ACS 的 MaxEnvelopes 的值均为 3 的例子



参考规范

本规范参考以下文档。本规范所定义协议依赖于所参考的文档。除非特别声明，否则支持参考规范中的所有要求组件。

下列参考规范与本规范的文档约定或上下文相关，而不与 CPE WAN 管理协议本身的要求相关。

- [1] RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, <http://www.ietf.org/rfc/rfc2119.txt>
- [2] TR-046, *Auto-Configuration Architecture & Framework*, DSL Forum Technical Report
- [3] TR-062, *Auto-Configuration for the Connection Between the DSL Broadband Network Termination (B-NT) and the Network using ATM*, DSL Forum Technical Report
- [4] TR-044, *Auto-Configuration for Basic Internet (IP-based) Services*, DSL Forum Technical Report

下列参考规范与 CPE WAN 管理协议的要求的组件相关：

- [5] RFC 2616, *Hypertext Transfer Protocol -- HTTP/1.1*, <http://www.ietf.org/rfc/rfc2616.txt>
- [6] RFC 2617, *HTTP Authentication: Basic and Digest Access Authentication*, <http://www.ietf.org/rfc/rfc2617.txt>
- [7] RFC 2965, *HTTP State Management Mechanism*, <http://www.ietf.org/rfc/rfc2965.txt>
- [8] *Simple Object Access Protocol (SOAP) 1.1*, <http://www.w3.org/TR/2000/NOTE-SOAP-20000508>
- [9] *Organizationally Unique Identifiers (OUIs)*, <http://standards.ieee.org/faqs/OUI.html>

下列参考规范与 CPE WAN 管理协议的可选或建议组件相关：

- [10] *The SSL Protocol, Version 3.0*, <http://www.netscape.com/eng/ssl3/draft302.txt>
- [11] RFC 2246, *The TLS Protocol, Version 1.0*, <http://www.ietf.org/rfc/rfc2246.txt>
- [12] RFC 2132, *DHCP Options and BOOTP Vendor Extensions*, <http://www.ietf.org/rfc/rfc2132.txt>
- [13] *XML-Signature Syntax and Processing*, <http://www.w3.org/2000/09/xmldsig>
- [14] PKCS #7, *Cryptographic Message Syntax Standard*, <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html> 或 <http://www.ietf.org/rfc/rfc2315.txt>

附录 A RPC 方法

A.1 简介

在 CPE WAN 管理协议中，远程过程调用（RPC）机制被用于 CPE 设备和自动配置服务器（ACS）之间的双向通信。本附录说明过程调用（方法）的版本 1 的定义，包括由 ACS 发起并发送给 CPE 的方法，及由 CPE 发起并发送给 ACS 的方法。

本规范的目的是独立于定义 RPC 方法编码语法。在 CPE WAN 管理协议的上下文中所使用的编码语法在 3.5 节中定义。

这里假定传输 RPC 报文的低层协议提供大部分的安全性，包括 CPE 和 ACS 之间的双向认证，加密及数据完整性。

A.2 RPC 方法的使用

A.2.1 数据类型

本规范定义的 RPC 方法使用默认 SOAP 数据类型的有限子集[8]。本规范使用的完整类型集及其记法列示在表 6 中。

表 6 – 数据类型

类型	描述
string 字符串型	本规范列示的字符串，最大允许长度可以用格式字符串（N）表示，N 是以字符计的最大长度。 对所有字符串，其最大长度要么明确表明，要么隐含在构成该字符串的元素大小中。对内容是枚举类型的字符串，枚举的最大值决定了字符串的最大长度。如果没有明确指明最大长度或者不是枚举类型的字符串，默认最大长度为 16 个字符。如果字符串型动作参数超过了指定的最大值，会产生一个“无效参数（Invalid arguments）”的错误应答。
int 整数型	从 - 2147483648（含）到+2147483647（含）范围内的整数。 对列示的一些整数型，格式 int[Min:Max]表明取值范围，Min 和 Max 值包含在内。如果没有任一 Min 或 Max，表明没有限值。
unsignedInt 无符号整数型	无符号整数，取值范围为 0（含）到 4294967295（含）。 对列示的一些无符号整数型，格式 unsignedInt[Min:Max]表明取值范围，Min 和 Max 值包含在内。如果没有任一 Min 或 Max，表明没有限值。
boolean 布尔型	布尔型，1 = true（真），0 = false（假）。
dateTime 日期时间型	ISO 8601 data-time 类型的子集，由 SOAP 的 dateTime 型定义。 除非明确指明，所有的时间表示为 UTC（全球统一时间）。 如果 CPE 不知道绝对时间，它应当使用从启动后消逝的时间。比如，启动后的 2 天 3 小时 4 分 5 秒将表示为 0000-00-02T03:04:05。

类型	描述
base64	Base64 编码的二进制。 最大允许长度可以用格式 base64(N)来表示，N 是指在 Base64 编码后字符的最大长度。
any 任意	某元素包含该表中列示的任意类型。 根据[8]的 SOAP 规范，使用这一类型的元素 必须 包含一个类型属性，来表明该元素的真正类型。例如： <Parameter> <Name>InternetGatewayDevice.ProvisioningCode</Name> <Value xsi:type="xsd:string">code12345</Value> </Parameter> 上面使用的名称空间 xsi 和 xsd 在[8]中定义。

在本规范中定义的方法可能使用结构和数组（在某些情况下还可能使用复合类型）。数组元素用数据类型后加方框号表示。数组最大长度的说明表示在方框号中。如果最大长度没有说明，除非特别指明，接收方能接受的元素数目没有固定的要求。如果接收方收到的请求含超出其处理能力的过大数组的请求，应当产生“Resources exceeded”错误代码。

A.2.2 其它要求

所有方法调用应当使用与本文档规定完全相同的参数数目。如果调用缺少参数或参数过多的方法会产生一个错误应答。参数的顺序也必须与本文档的规定相同。

本规范将来版本不得重新定义在本附录中定义过的 RPC 方法。任何在将来版本的变动应当只定义新 RPC 方法，并且用不同名称来标识。

A.3 标准的 RPC 报文

A.3.1 通用方法

在本节中列示的方法需要 CPE 设备和 ACS 服务器均支持。CPE 或 ACS 均可调用这些方法。

A.3.1.1 GetRPCMethods

这一方法可用于 CPE 或 ACS 来发现另一方所支持的方法集。方法集列表可以包括标准方法（在本规范及后续版本中定义），也可以包括厂商自定义方法。接收该方法的应答方**必须**忽略掉任何不能解释的方法。

厂商定制方法**必须**采用 X_<VENDOR>_MethodName 的格式，其中<VENDOR>是唯一厂商标识符，可以是一个 OUI 或域名。OUI（organizationally unique identifier 组织的唯一标识）在[9]中定义，**必须**格式化为 6 个十六进制字符的 OUI，所有字母要大写，要包括所有前置 0。域名必须是大写，并且将每个点（“.”）替换为连字符或下划线。例如：X_00D09E_MyMethod，X_ACME_COM_MyMethod。

该方法的调用参数在表 7 中定义。应答参数在表 8 中定义。

表 7 – GetPRCMethods 参数

参数	类型	描述
-	Void	本方法没有调用参数。

表 8 – GetPRCMethodsResponse 参数

参数	类型	描述
MethodList	String(64)[]	字符串数组，包含接收方支持的每一个 PRC 方法名称。例如，CPE 仅实现了本规范本版本所定义的基本方法，则 CPE 会返回如下列表给 ACS： "GetRPCMethods" "SetParameterValues" "GetParameterValues" "GetParameterNames" "SetParameterAttributes" "GetParameterAttributes" "AddObject" "DeleteObject" "Reboot" "Download"

针对该方法定义的来自 CPE 应答的错误代码有：9001，9002。

针对该方法定义的来自 ACS 应答的错误代码有：8001，8002，8005。

A.3.2 CPE 方法

本节中列示的方法在 CPE 设备上支持。只有服务器能够调用这些方法。

A.3.2.1 SetParameterValues

服务器可用此方法来修改 CPE 的一个或多个参数。此方法的调用参数在表 9 中定义。应答参数在表 10 中定义。

表 9 – SetParameterValues 参数

参数	类型	描述
ParameterList	ParameterValueStruct[]	表 11 中所定义的 name-value 值对数组。对每个 name-value 值对，CPE 需要将指定名称的参数值设置为指定值。
ParameterKey	String(32)	设置 ParameterKey 参数值。该值可以用于服务器，来识别参数更新，或者让其为空。

表 10 – SetParameterValuesResponse 参数

参数	类型	描述
Status	int[0:1]	对该方法的成功应答返回一个整数型的枚举值定义如下： 0 = 参数的改动已经验证并应用。 1 = 参数的改动已经验证并提交，只是尚未应用（比如，在新的参数值应用前需要进行重新启动）。

在成功接受到 SetParameterValues PRC 后，CPE 必须立即和自动应用每个指定的

参数的变化值。参数表中参数的顺序无关紧——CPE 对改动值的应用**必须**与它们列示的顺序独立。只有当新的参数值已经成功应用后，才能给该 RPC 回复一个成功应答。如果 CPE 在应用新参数值前需要重新启动，**CPE 必须在**进行重新启动前应答，即在**参数值**应用之前应答。在这种情况下，应答时**必须**确认所有请求已经完成，并且新值已经正确地保存下来，一旦重新启动后，这些值一定会立即得到应用。

ParameterValueStruct 结构在表 11 中定义。

表 11 – ParameterValueStruct 定义

名称	类型	描述
Name	string(256)	这是参数的名称。
Value	Any	这是参数需要设置的值。

如果有一个或多个参数错误，对该方法的错误应答必须为每个错误的参数包括一个 SetParameterValuesFault 元素。在此情况下，整个错误应答的首要错误代码必须是无效参数（9003）。

本方法定义的错误代码有：9001，9002，9003，9004，9005，9006，9007，9008。

A.3.2.2 GetParameterValues

这一方法可用于服务器来获取一个或多个 CPE **参数**的值。该方法的调用参数在表 12 中定义，应答参数在表 13 中定义。

表 12 – GetParameterValues 参数

参数	类型	描述
ParameterName	string(256)[]	字符串数组，每个代表所请求的 参数 的名称。 如果 参数 名是以部分路径名的方式出现，则该请求需被解释为请求返回命名层次中共用相同前缀的该分支的所有 参数 。部分路径名 必须 在层次的最后一个节点名称后面以“.”（点）结尾。空字符串代表整个层次名称的顶部。 下面是完整 参数 名称的例子： InternetGatewayDevice.DeviceInfo.SerialNumber 下面是部分路径名称的例子： InternetGatewayDevice.DeviceInfo.

表 13 – GetParameterValuesResponse 参数

参数	类型	描述
ParameterList	ParameterValueStruct[]	Name-value 对的数组，在表 11 中定义。包括每个被请求参数的名称和值。

该方法定义了如下错误代码：9001,9002,9003,9004,9005。如果错误是由无效的**参数**名称引起，则**必须**使用 Invalid Parameter Name 错误代码（9005）而不是用更泛化的 Invalid Argument 错误代码（9003）。

A.3.2.3 GetParameterNames

本方法可以由服务器用来发现某一 CPE 上的可访问的**参数**。本方法的调用参数

列示在表 14 中，应答参数列示在表 15 中。

表 14 – GetParameterNames 参数

参数	类型	描述
ParameterPath	string(256)	<p>包括一个完整参数名或部分路径名的字符串，代表名称层次的一个子集。空字符串代表名称空间的顶层。部分路径名必须在层次中的最后一个节点名称后面以 “.”（点）结尾。</p> <p>下面是完整参数名的例子：</p> <p style="padding-left: 40px;">InternetGatewayDevice.DeviceInfo.SerialNumber</p> <p>下面是部分路径名的一个例子：</p> <p style="padding-left: 40px;">InternetGatewayDevice.DeviceInfo.</p>
NextLevel	boolean	<p>如果值为 false，则应答将列出所有以 ParameterPath 参数指定字符串开始的参数的完整路径名。</p> <p>如果值为 true，则应答只列出指定的 ParameterPath 下一层的部分路径名。例如，如果 ParameterPath 是</p> <p style="padding-left: 40px;">“InternetGatewayDevice.LANDevice.”， 应答可能列出</p> <p style="padding-left: 40px;">“InternetGatewayDevice.LANDevice.1. ” 和</p> <p style="padding-left: 40px;">“InternetGatewayDevice.LANDevice.2. ”， 而不会列出在该层次下面的所有参数。</p>

表 15 – GetParameterNamesResponse 参数

参数	类型	描述
ParameterList	ParameterInfoStruct[]	<p>结构数组，每个包含一个参数的名称和其它信息，见表 16 的定义。当 NextLevel 是 false 时，这一方法返回所有名称以 ParameterPath 参数指定的字符串开头的的所有可访问的参数及其信息。如果 ParameterPath 参数是一个空字符串，则将返回该 CPE 上所有可访问的参数名称。当 NextLevel 是 true 时，这一列表包括以 ParameterPath 指明路径的下一层的所有部分路径名。</p>

表 16 – ParameterInfoStruct 定义

名称	类型	描述
Name	string(256)	这是 参数 的名称或部分路径名。
Writable	boolean	<p>是否该参数值能够用 SetParameterValues 方法来覆盖。</p> <p>如果因 NextLevel 值为 true，该名称是一个部分路径名，则表明是否 AddObject 和 DeleteObject 可以被用于该层次来移除该实例或增加其它的实例。</p>

本方法定义的错误代码有：9001，9002，9003，9005。如果错误是由无效的**参数**名称引起，则**必须**使用 Invalid Parameter Name 错误代码（9005）而不是用更泛化的 Invalid Argument 错误代码（9003）。

A.3.2.4 SetParameterAttributes

本方法可以由服务器用来更改 CPE 上的一个或更多**参数**的属性。本方法的调用参数列示在表 17 中，应答参数列示在表 18 中。

表 17 – SetParameterAttributes 参数

参数	类型	描述
ParameterList	SetParameterAttributesStruct[]	列出用于更改一组 参数 的属性改动值。该数组中的每项条目是一个 SetParameterAttributesStruct 结构，在表 19 中定义。

表 18 – SetParameterAttributesResponse 参数

参数	类型	描述
-	void	该方法的应答没有参数。

表 19 – SetParameterAttributesStruct 定义

名称	类型	描述
Name	string(256)	<p>这是应用新属性的参数的名称。另一种方式是，该名称可以是一个部分路径名，表明新的属性应当应用于命名层次中该节点下的所有参数。部分路径名必须在层次中的最后一个节点名称后面以“.”（点）结尾。空字符串代表名称空间的顶层。</p> <p>下面是完整参数名的例子： InternetGatewayDevice.DeviceInfo.SerialNumber</p> <p>下面是部分路径名的一个例子： InternetGatewayDevice.DeviceInfo.</p>
NotificationChange	boolean	如果为 true，Notification 的值将替换该参数或参数组的当前 notification 的设置。如果是 false，则不作任何 notification 设置的改动。
Notification	int[0:2]	<p>指定是否 CPE 应当将指定的该（或多个）参数的变化值放到其 Inform 报文中，以及是否当指定参数的值发生变化时，CPE 应当发起一个到 ACS 的会话。值的定义如下：</p> <p>0 = Notification 关闭。CPE 不必通过 ACS 指定参数的变化。</p> <p>1 = 被动式 Notification。当指定的参数值变化时，CPE 必须在下一次建立与 ACS 的会话时，将这一新值包含在 Inform 报文的 ParameterList 中。</p> <p>2 = 主动式 Notification。一旦指定参数的值发生变化，CPE 必须发起与 ACS 的会话，将新值包含在相应的 Inform 报文的 ParameterList 中。</p> <p>因非零的 Notification 设置引起发送的 Inform 报文中参数发生变化，事件代码“4 VALUE CHANGE”必须包括在事件列表中。</p> <p>如果试图给一个不适合设置 notification 值的参数（比如一个持续变化的统计值）设置 notification 值，CPE 可以返回一个“notification request rejected”错误。</p>
AccessListChange	boolean	如果为 true，AccessList 的值会替换该参数或参数组的当前 access list 值。如果为 false，access list 不作改动。

AccessList	String(64)[]	<p>零个或多个实体的数组，该实体对指定的参数有写权限。如果数组中不包含条目，则只允许 ACS 有写权限。目前，只定义了一类实体可以包含在该列表中：</p> <p>“Subscriber” 指明由 LAN 上的 Subscriber 控制的设备拥有写权限。比如通过 LAN 端的 DSL CPE 配置协议或通过 UPnP。</p> <p>默认情况下，在 ACS 对 access list 作改动前，上述的所有实体应当被赋予写访问权。</p>
------------	--------------	---

本方法定义的错误代码有：9001，9002，9003，9004，9005，9009。如果错误是由无效的参数名称引起，则**必须**使用 Invalid Parameter Name 错误代码（9005）而不是用更泛化的 Invalid Argument 错误代码（9003）。

A.3.2.5 GetParameterAttributes

本方法可以由服务器用来读取 CPE 上的一个或更多**参数**的属性。本方法的调用参数在表 20 中定义，应答参数在表 21 中定义。

表 20 – GetParameterAttributes 参数

参数	类型	描述
ParameterNames	string(256)[]	<p>字符串数组，每一条对应所请求的参数的名称。</p> <p>如果参数名是以部分路径名的方式出现，则该请求需被解释为请求返回命名层次中共用相同前缀的该分支的所有参数。部分路径名必须在层次的最后一个节点名称后面以“.”（点）结尾。空字符串代表整个层次名称的顶部。</p> <p>下面是完整参数名称的例子：</p> <p>InternetGatewayDevice.DeviceInfo.SerialNumber</p> <p>下面是部分路径名称的例子：</p> <p>InternetGatewayDevice.DeviceInfo.</p>

表 21 – GetParameterAttributesResponse 参数

参数	类型	描述
ParameterList	ParameterAttributeStruct[]	列示指定的参数集的 access control 信息。该数组中的每一条目是一个 ParameterAccessStruct 结构，在表 22 中定义。

表 22 –ParameterAttributeStruct 定义

名称	类型	描述
Name	string(256)	这是给出属性值的 参数 名称。
Notification	int[0:2]	<p>指定是否 CPE 应当将指定的该（或多个）参数的变化值放到其 Inform 报文中，以及是否当指定参数的值发生变化时，CPE 应当发起一个到 ACS 的会话。值的定义如下：</p> <p>0 = Notification 关闭。CPE 不必通过 ACS 指定参数的变化。</p> <p>1 = 被动式 Notification。当指定的参数值变化时，CPE 必须在下次建立与 ACS 的会话时，将这一新值包含在 Inform 报文的 ParameterList 中。</p> <p>2 = 主动式 Notification。一旦指定参数的值发生变化，CPE 必须发起与 ACS 的会话，将新值包含在相应的 Inform 报文的 ParameterList 中。</p>

AccessList	string(64)[]	零个或多个实体的数组，该实体对指定的 参数 有写权限。如果数组中不包含条目，则只允许 ACS 有写权限。目前，只定义了一类实体可以包含在该列表中： “Subscriber” 指明由 LAN 上的 Subscriber 控制的设备拥有写权限。比如通过 LAN 端的 DSL CPE 配置协议或通过 UPnP。
------------	--------------	---

本方法定义的错误代码有：9001，9002，9003，9004，9005。如果错误是由无效的**参数名称**引起，则**必须**使用 Invalid Parameter Name 错误代码（9005）而不是用更泛化的 Invalid Argument 错误代码（9003）。

A.3.2.6 AddObject

这一方法可以由服务器使用来建立一个多实例对象（multi-instance object）的新实例。多实例对象是指**参数**集合及/或其它它定义了多个实例的对象。该方法调用的**参数**是需要建立新实例的一组对象的路径名，例如：

Top.Group.Object.

该路径名不包括要建立的对象的实例编号。实例编号由 CPE 指定，并在应答中返回。一旦指定，该对象的实例编号不得更改，并一直使用直到该对象被 DeleteObject 方法删除。在建立后，该对象的**参数**或其子对象用路径名及附加其后的实例编号来引用。例如，如果 AddObject 方法返回实例编号为 2，则该实例中的一个**参数**可以用这样的路径名来引用：

Top.Group.Object.2.Parameter

使用该方法建立了对象后，该对象包含的**参数**被设置为默认值，其相关属性值设置如下：

- Notification 设置为 0（Notification 关闭）
- AccessList 包括所有定义的实体

对 **Internet 网关设备**，可以使用该方法的特定对象集合列示在附录 B 中。本方法的调用**参数**在表 23 中定义，应答**参数**在表 24 中定义。

表 23 – AddObject 参数

参数	类型	描述
objectName	string(256)	要建立新实例的对象集合的路径名称。路径名 必须 在该对象的层次名称的最后节点后加上 “.”（点）结尾。
ParameterKey	string(32)	需要设置的 ParameterKey 参数的值。该参数由服务器决定，并可以为空。

表 24 – AddObjectResponse 参数

参数	类型	描述
InstanceNumber	unsignedInt[1:]	新建对象的实例号码。在对象建立后，可以在路径名中使用该实例号码来引用该对象的 参数 或子对象。由 CPE 指定的实例号码是任意的，并且与后续的 AddObject 调用分配的号码无需连续。 CPE 不应当 将曾经分配出去的现已删除的对象使用过的号码再分配给新的实例。CPE 应当在耗尽某指定对象的整个整数值空间后再重用实例号码。

Status	int[0:1]	对该方法的成功应答返回一个整数型的枚举值定义如下： 0 = 对象已经建立。 1 = 对象的建立已经验证并提交，只是尚未应用（比如，增加新对象前需要进行重新启动）。
--------	----------	---

该方法错误代码的定义有：9001,9002,9003,9004,9005。

A.3.2.7 DeleteObject

本方法用于删除一个对象的特定实例。该方法调用的参数值是包含实例号码的对象实例的路径名称。例如：

Top.Group.Object.2.

如果该方法的调用成功，则指定对象的实例无法再访问，CPE 可以丢弃与该实例包含的任意参数或子对象相关的状态。

当对象实例被删除后，与该实例号相关的同一对象集合的其它实例号码不变。这样，在同一个集合中，对象实例的实例号码可能是不连续的。

对 **Internet 网关设备**，可以使用该方法的特定的对象集合列示在附录 B 中。该方法的调用参数在表 25 中定义，应答参数表 26 中定义。

表 25 – DeleteObject 参数

参数	类型	描述
ObjectName	string(256)	欲删除的对象实例的路径名。路径名 必须 以对象的实例号码后加“.”（点）来结尾。
ParameterKey	string(32)	设置 ParameterKey 参数的值。该参数的值由服务器决定，并可以为空。

表 26 – DeleteObjectResponse 参数

参数	类型	描述
Status	int[0:1]	对该方法的成功应答返回一个整数型的枚举值定义如下： 0 = 对象已经删除。 1 = 对象的删除已经验证并提交，只是尚未应用（比如，将删除对象前需要进行重新启动）。

该方法错误代码的定义有：9001,9002,9003,9005。

A.3.2.8 Download

本方法可以由服务器使用来指示 CPE 在指定的位置下载特定的文件。该方法的调用参数在表 27 中定义，应答参数在表 28 中定义。

表 27 – Download 参数

参数	类型	描述
CommandKey	string(32)	CPE 用来指向特定下载的字符串。该参数在方法 TransferComplete 和 GetQueuedTransfers 中引用。

参数	类型	描述
FileType	string(64)	<p>一个整数，其后是一个空格，再其后是一个文件类型说明。目前 FileType 参数仅定义了以下值：</p> <p>"1 Firmware Upgrade Image"</p> <p>"2 Web Content"</p> <p>"3 Vendor Configuration File"</p> <p>下列格式用于定义唯一的厂商自定义文件类型：</p> <p>"X <OUI> <Vendor-specific identifier>"</p> <p>其中，<OUI>用 6 位十六进制数字的在[9]中定义的 OUI（组织唯一标识）代替，其中所有字母用大写，包括所有前置零。</p>
URL	string(256)	URL 说明源文件的位置。 必须 支持 HTTP 传输。 可以 支持其它可选的传输方式，如 2.3.2 节的定义。
Username	string(256)	CPE 用于认证文件服务器的用户名。如果不需要认证，则该字符串设置为空串。
Password	string(256)	CPE 用于认证文件服务器的密码。如果不需要认证，则该字符串设置为空串。
FileSize	unsignedInt	以字节为单位的要传输文件的大小。CPE 可以利用该值来判断它是否有足够的空间来下载该文件，或者它必须释放更多空间以为指定文件腾出空间。
TargetFileName	string(256)	在目标文件系统中应使用的文件名。如果目标文件名可以从下载的文件本身来提取，或可以从 URL 参数中提取，或不需要目标文件名，这一参数的值可以为空。如果说明了该值，但是目标文件名也由其它来源指明了（比如是从下载的文件中自动提取的），这一参数 应当 被忽略。如果目标文件名已经使用，下载的文件将替换任何已经使用的相同名称的文件（是否 CPE 将被替换的文件存档由 CPE 自主决定）。
DelaySeconds	unsignedInt	从本方法被调用到 CPE 被要求开始下载之间的时间间隔。如果值为零表明不需要延迟。如果是非零值，则下载 不应当 使用与该请求相同的事务会话。
SuccessURL	string(256)	<p>在能应用的情况下，本参数包含在下载成功完成后，CPE 应当将用户的浏览器重定向到哪一 URL。这一 URL 值可能包含服务器所需要的 CGI 参数（比如，来维护会话的状态）。</p> <p>只有当下载是由基于浏览器的用户交互式发起，并且 CPE 支持基于下载结果选择性重定向的能力时才能使用。</p> <p>在不需要这样的 URL 的情况下，这一参数应当为空。</p>
FailureURL	string(256)	<p>在能应用的情况下，本参数包含在下载未成功完成后，CPE 应当将用户的浏览器重定向到哪一 URL。这一 URL 值可能包含服务器所需要的 CGI 参数（比如，来维护会话的状态）。</p> <p>只有当下载是由基于浏览器的用户交互式发起，并且 CPE 支持基于下载结果选择性重定向的能力时才能使用。</p> <p>在不需要这样的 URL 的情况下，这一参数应当为空。</p>

表 28 – DownloadResponse 参数

参数	类型	描述
Staus	int[0:1]	<p>对该方法的成功应答返回一个整数型的枚举值定义如下：</p> <p>0 = 下载已结束并已应用。</p> <p>1 = 下载还没有结束（比如，CPE 需要重新启动后才能执行文件的下载）。</p> <p>如果该参数的值非零，则 CPE 必须在本会话的后续时间，或者在其后的会话中，调用 TransferComplete 方法来说明本次下载的完成状态（成功或者失败）。</p>

参数	类型	描述
Staus	int[0:1]	对该方法的成功应答返回一个整数型的枚举值定义如下： 0 = 下载已结束并已应用。 1 = 下载还没有结束（比如，CPE 需要重新启动后才能执行文件的下载）。 如果该参数的值非零，则 CPE 必须在本会话的后续时间，或者在其后的会话中，调用 TransferComplete 方法来说明本次下载的完成状态（成功或者失败）。
StartTime	dateTime	下载开始的日期和时间（UTC）。只有在下载结束后该值才需要填写。
CompleteTime	dateTime	下载完全结束并应用时的日期和时间（UTC）。只有在下载结束后该值才需要填写。

本方法的错误代码定义为：9000,9001,9002,9003,9010,9012,9013。

A.3.2.9 Reboot

这一方法令 CPE 重新启动。CPE 必须在启动前发送该方法的应答。在使用该方法时一定要万分小心。这一方法的调用参数在表 29 中定义，应答参数在表 30 中定义。

注 – 本方法主要用于诊断目的。本方法的目的不是让 ACS 在设置完 CPE 参数或初始化下载后进行重新启动而使用。如果在这些情况下，CPE 需要重新启动，它自主负责在会话结束后进行重新启动。因为一些 CPE 在此类条件下，可能不需要重新启动，因此 ACS 不应当在这类情况下调用该方法，以避免不必要的重新启动。

表 29 – Reboot 参数

参数	类型	描述
CommandKey	string(32)	当 CPE 重新启动并调用 Inform 方法时，将在 InfromStruct 的 CommandKey 元素中返回该元素值。

表 30 – RebootResponse 参数

参数	类型	描述
-	void	该应答方法无参数。

这方法定义的错误代码为：9001,9002,9003。

A.3.3 服务器方法

在本节中列示的方法只需在服务器的支持。只有 CPE 可以调用这些方法。

A.3.3.1 Inform

任何时刻要建立与 ACS 的连接，CPE 必须调用 Inform 方法，来初始化一个传输序列。该方法的调用参数在表 31 中定义，应答参数在表 32 中定义。

表 31 – Inform 参数

参数	类型	值
DeviceID	DeviceIdStruct	唯一标识 CPE 的结构，在表 34 中定义。
Event	EventStruct[16]	结构数组，在表 35 中定义，说明引发事务会话建立的一个或多个事件。如果存在多于一个原因，CPE 必须列出所有原因。
MaxEnvelopes	unsignedInt	CPE 能够从 ACS 接受的一个 HTTP 回复中的最大 SOAP 信包数目。零值表明在该信包数目上没有特别的限制。
CurrentTime	dateTime	CPE 的当前的日期与时间（UTC）。
RetryCount	unsignedInt	在成功完成对 Inform 方法的调用前，已进行了多少次调用尝试。特别地，该值在每次非成功的尝试后会增 1。非成功的尝试包括发送 Inform 报文以与 ACS 建立连接，或每次对 Inform 报文的不成功使用，比如收到错误应答或没有收到应答。在已经发送了 Inform 报文并且收到了成功应答后，该值重置为零。
ParameterList	ParameterValueStruct[]	表 11 中定义的 name-value 对的数组。对每种类型的 CPE，在 Inform 请求中包括参数信息表。表 33 列出了 Internet 网关设备 必须包括的参数。CPE 可以发送其它信息。

表 32 – InformResponse 参数

名称	类型	描述
MaxEnvelopes	unsignedInt	ACS 接受的来自 CPE 的每个 HTTP post 的 SOAP 信包的最大数目。零值表明没有对信包数目的限定。

表 33 列示了在 **Internet 网关设备**发出的 Inform 中需要包含的参数。CPE 也可以在 Inform 包中包括其它参数。

如果是一个或多个参数值变化引起的（不是由 ACS 自己要求设置而引起）Inform 调用，并且该参数值 ACS 通过 SetParameterAttributes 已经标记为 notification（包括主动与被动），所有这些改变了的参数也必须包括在 ParameterList 中。如果一个参数在最后一次这类 notification 后改变过多次，只需要包括其最后一次更动的值。

对表 33 中“更改通知”列中做了标记的项，相应参数值的任何变动**必须**产生一个 CPE 发起的与 ACS 的连接，以调用 Inform 方法，而不管 ACS 是否将这些参数设置为 notification。

因任何在表 33 中“更改通知”列标记过的参数变化而引起的 Inform 调用，或者 ACS 标记为 notification（包括主动与被动）的参数变化而引起的 Inform 调用，必须在 Inform 方法的事件列表中包括事件"4 VALUE CHANGE"。

表 33 – Internet 网关设备所需的 Inform 参数

参数	更改通知
InternetGatewayDevice.DeviceInfo.SpecVersion	
InternetGatewayDevice.DeviceInfo.HardwareVersion	
InternetGatewayDevice.DeviceInfo.SoftwareVersion	X
InternetGatewayDevice.DeviceInfo.ProvisioningCode	X
InternetGatewayDevice.ManagementServer.ConnectionRequestURL	X

参数	更改通知
InternetGatewayDevice.ManagementServer.ParameterKey	
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{j}.WAN{***}Connection.{k}.ExternalIPAddress ⁸	X ⁹

表 34 – DeviceIdStruct 定义

名称	类型	描述
Manufacturer	string(64)	设备的制造商（仅用于显示）。
OUI	string(6)	设备制造商的组织唯一标识。用 6 位十六进制值表示，均为大写，并且包括任何的前置零。该值 必须 是[9]中定义的有效 OUI 值。
ProductClass	string(64)	序列号所使用的产品类型标识。也就是说，对指定的制造商，该参数是用于标识产品或产品类型，在该类型下，SerialNumber 参数是唯一的。
SerialNumber	string(64)	对指定的产品类型和制造商，该标识可以唯一地确定该设备。

表 35 – EventStruct 定义

名称	类型	描述	
EventCode	string(64)	每个值包括一个标识字符随后是对应原因的文字描述。几项原因值列示在下面，同时也定义了厂商自定制原因的语法。	
		值	原因
		"0 BOOTSTRAP"	表明会话发起原因是 CPE 首次安装或 ACS 的 URL 发生变化。
		"1 BOOT"	表明会话发起原因是 CPE 加电或重置，包括系统首次启动，以及因任何原因而引起的重启，包括使用 Reboot 方法。
		"2 PERIODIC"	表明会话发起原因是定期的 Inform 引起。
		"3 SCHEDULED"	表明会话发起原因是调用了 ScheduleInform 方法。
		"4 VALUE CHANGE"	表明会话发起原因是一个或多个参数值的变化。该参数值包括在 Inform 方法的调用中。例如 CPE 分配了新的 IP 地址。
		"5 KICKED"	表明会话发起原因是为了 web 标识管理（见附录 D），及在本会话中将会调用 Kicked 方法（见 A.4.2.1 节）。
		"6 CONNECTION REQUEST"	表明会话发起原因是 3.2 节中定义的源自服务器的 Connection Request notification。
		"7 TRANSFER COMPLETE"	表明会话的发起是为了表明以前请求的下载或上载（不管是否成功）已经结束，在此会话中将要调用一次或多次 TransferComplete 方法。
		"8 DIAGNOSTICS COMPLETE"	当完成由 ACS 发起的诊断测试结束后，重新与 ACS 建立连接时使用。如 DSL 环路诊断（见附录 B）。
"M "<method name>	如果这是另一方法的结果，值“M”后紧接着一个空格和方法的名称。例如： “M Reboot”		
"X "<OUI>	厂商自定义事件。在“X”后的 OUI 和空格是		

⁸ 这里 {i}，{j}，和 {k} 是指默认的 WAN 连接，根据连接的类型，{***} 是“IP”或“PPP”。

⁹ 该参数值发生改变或默认的 WAN 连接更改成不同的连接，CPE 都必须调用 Inform。

名称	类型	描述
		<div><event></div> <div>组织唯一标识符，表示为 6 位十六进制值，均使用大写，并包括任何前置零。该值必须是在 [9] 中定义的有效 OUI。对 <event> 的值与解释是厂商自定义的。例如： “X 00D09E MyEvent”</div>
CommandKey	string(32)	<div>如果是因定义了一个 CommandKey 而产生了 Inform 结构，该元素必须 CommandKey 的值。在其它情况下，该元素的值为空字符串。</div> <div>对本规范的这一版本而言，对以下方法的调用会造成 CommandKey 值的改变：</div> <ul style="list-style-type: none"> ● ScheduledInform 方法 ● Reboot 方法 ● Download 方法 ● Upload 方法

为该方法定义的错误代码有：8001，8002，8003，8004，8005。

A.3.3.2 TransferComplete

本方法通知服务器由以前的 Download 或 Upload 方法调用而引起的文件传输已经结束（不管成功还是失败）。当相关的 Download 或 Upload 应答表明指定的文件传输在当时还没有完成（应答中 Status 参数非零）时，**必须**调用本方法。在这种情况下，本方法可以在发起文件传输的会话中调用，也可以在后续的会话中调用。如果使用该方法，则只有在文件传输已经结束（或者已经失败）后才能调用。CPE 用来判断何时传输可认作结束的标准由 CPE 的实现方法自行决定。该方法的调用参数在表 36 中定义，应答参数在表 37 中定义。

表 36 – TransferComplete 参数

参数	类型	值
CommandKey	string(32)	设置为 CommandKey 参数的值，该值是在发起文件传输的 Download 或 Upload 方法调用中传递给 CPE 的。
FaultStruct	FaultStruct	表 38 中定义的 FaultStruct 结构。如果文件传输成功，FaultCode 的值设置为 0。否则会指明非零的 FaultCode 值和说明失败原因的 FaultString。
StartTime	dateTime	文件传输开始的日期和时间（UTC）。
CompleteTime	dateTime	文件传输结束的日期和时间（UTC）。

表 37 – TransferCompleteResponse 参数

参数	类型	值
-	void	该方法应答无参数。

表 38 – FaultStruct 定义

名称	类型	值
FaultCode	unsignedInt	在 A.5.1 节中定义的数字型错误代码。在失败情况下，允许使用的代码是：9001，9002，9010，9011，9012。零值代表无错误。
FaultString	string(256)	错误的可人读文字描述。如果 FaultCode 的值为零，则该域应当为空。

本方法定义的错误代码为：8000，8001，8002，8003，8004，8005。

A.4 可选的 RPC 报文

A.4.1 CPE 方法

该节列示的所有方法是 CPE 设备可选支持的。只有服务器能够调用这些方法。

A.4.1.1 GetQueuedTransfers

服务器可以用本方法来确定前面的下载或上载请求的状态。该方法的调用参数在表 39 中定义，其应答参数在表 40 中定义。

表 39 – GetQueuedTransfers

参数	类型	描述
-	void	该方法没有调用参数。

表 40 – GetQueuedTransfersResponse 参数

参数	类型	描述
TransferList	QueuedTransferStruct[16]	结构数组，在表 41 中定义。每个结构描述了一个 CPE 已经指示去执行，但还没有完全结束的文件传输。

表 41 – QueuedTransferStruct 定义

名称	类型	描述
CommandKey	string(32)	其值设置为发起文件传输的 Download 或 Upload 方法传递给 CPE 的 CommandKey 参数值。
State	int[1:3]	传输的当前状态。定义的值有： 1 = 尚未开始 2 = 进行中 3 = 已结束，正完成清理 保留所有其它值。

为该方法定义的错误代码包括：9000，9001，9002。

A.4.1.2 ScheduleInform

服务器可以用本方法请求 CPE 来在未来某时刻计划（与 CPE 的定期调用 Inform 方法分离）一次性的 Inform 方法调用。方法的调用参数在表 42 中定义，应答参数在表 43 中定义。

表 42 – ScheduleInform 参数

参数	类型	描述
DelaySeconds	unsignedInt	从该方法被调用到 CPE 响应请求发起一次性的 Inform 方法调用之间的秒数。CPE 发送一个请求，然后 DelaySeconds 之后调用 Inform 方法。该值必须比零大。
CommandKey	string(32)	当 CPE 调用 Inform 方法时，InformStruct 的 CommandKey 元素应返回的值。

表 43 – ScheduleInformResponse 参数

参数	类型	描述
-	void	该应答方法没有参数。

A.4.1.3 SetVouchers

服务器调用该方法来设置 CPE 使用的一个或多个 Vouchers（凭据）选项。该方法的调用参数在表 44 中定义，应答选项在表 45 中定义。

表 44 – SetVouchers 参数

参数	类型	描述
VoucherList	base64[]	Vouchers 数组，其中每一个 Voucher 表示一个 Base64 编码的十进制字符串。Voucher 的具体结构在附录 C 中定义。

表 45 – SetVouchersResponse 参数

参数	类型	描述
-	void	该应答方法没有参数。

为本方法定义的错误代码有：9000，9001，9002，9003，9004。

A.4.1.4 GetOptions

服务器可以用此方法来获得 CPE 目前设置的选项表，及其它相关状态信息。该方法的调用参数在表 46 中定义，应答参数在表 47 中定义。

表 46 – GetOptions 参数

参数	类型	描述
OptionName	string(64)	表示一个特定选项的名称的字符串，或一个空串指出该方法应当返回 CPE 支持的所有选项的状态（而不管它们目前是否已经启用）。

表 47 – GetOptionsResponse 参数

参数	类型	描述
OptionList	OptionStruct[]	OptionStruct 数组，在表 48 中定义。包括或者一个 OptionStruct（当接收到对一个特定选项的信息请求）或一个 OptionStruct 表，每个结构包括 CPE 支持的一个选项。

表 48 – OptionStruct 定义

名称	类型	描述
OptionName	string(64)	标识特定选项的名称。
VoucherSN	unsignedInt	标识特定选项的数目。

名称	类型	描述
State	unsignedInt	由两位构成的数字，定义如下： Bit 0 (LSB): 0 = 选项目前被禁用 1 = 选项目前被启用 Bit 1: 0 = 选项已经被设置 1 = 选项未被设置 对每个选项的设置状态的解释是该选项所自定义的。但通常情况下解释为指定是否最终用户已经主动地执行了一些动作以使该选项完全发挥功能。
Mode	int[0:2]	这一元素说明指定选项启用还是禁用。如果已经启用，是否已经指定了过期。定义的值有： 0 = 禁用 1 = 启用，过期 2 = 启用，无过期
StartDate	dateTime	选项开始的日期时间（UTC）。如果是未来时间，是指要启用选项的时间。如果是过去时间，是选项启用时的时间。
ExpirationDate	dateTime	如果有，表明选项要过期的日期时间（UTC）。
IsTransferable	boolean	指定是否选项已被指定为能够传递或不能传递（见附录 C）。定义的值有： 0 = 不能传递 1 = 能够传递

为本方法定义的错误代码有：9000，9001，9002，9003。

A.4.1.5 Upload

服务器用本方法使 CPE 向指定的位置上载一个特定的文件。本方法的调用参数在表 49 中定义，应答方法在表 50 中定义。

表 49 – Upload 参数

参数	类型	描述
CommandKey	string(32)	CPE 用来指向特定上载的字符串。该参数在 TransferComplete 和 GetQueuedTransfers 方法中引用。
FileType	string(64)	一个整数，其后是一个空格，再其后是一个文件类型说明。目前 FileType 参数仅定义了以下值： "1 Firmware Upgrade Image" "2 Web Content" 下列格式用于定义唯一的厂商自定义文件类型： "X <OUI> <Vendor-specific identifier>" 其中，<OUI>用 6 位十六进制数字的在[9]中定义的 OUI（组织唯一标识）代替，其中所有字母用大写，包括所有前置零。
URL	string(256)	URL 说明目标文件位置。 必须 支持 HTTP 传输。 可以 支持其它可选的传输方式，如 2.3.2 节的定义。
Username	string(256)	CPE 用于认证文件服务器的用户名。如果不需要认证，则该字符串设置为空串。
Password	string(256)	CPE 用于认证文件服务器的密码。如果不需要认证，则该字符串设置为空串。
DelaySeconds	unsignedInt	从本方法被调用到 CPE 被要求开始上载之间的时间间隔。如果值为零表明不需要延迟。如果是非零值，则上载 不应当 使用与该请求相同的事务会话。

表 50 – UploadResponse 参数

参数	类型	描述
Staus	int[0:1]	对该方法的成功应答返回一个整数型的枚举值定义如下： 0 = 上载已完成。 1 = 上载尚未完成（比如，如果上载必须等等本会话终止）。 如果该参数的值非零，则 CPE 必须 在本会话的后续时间，或者在其后的会话中，调用 TransferComplete 方法来说明本次上载的完成状态（成功或者失败）。
StartTime	dateTime	上载开始的日期和时间（UTC）。只有在上载结束后该值才需要填写。
CompleteTime	dateTime	上载完全结束并应用时的日期和时间（UTC）。只有在上载结束后该值才需要填写。

为本方法定义的错误代码有：9000，9001，9002，9003，9011，9012，9013。

A.4.1.6 FactoryReset

这一方法将重置 CPE 到其出厂默认状态。该方法使用时需要万分小心。该方法的调用参数在表 51 中定义，应答参数在表 52 中定义。

表 51 – FactoryReset 参数

名称	类型	描述
-	void	该方法没有参数。

表 52 – FactoryResetResponse 参数

名称	类型	描述
-	void	该方法的应答没有参数。

为本方法定义的错误代码包括：9000，9001，9002，9003。

A.4.2 服务器方法

本节定义的方法为服务器可选支持，只有 CPE 才能调用这些方法。

A.4.2.1 Kicked

任何时刻 CPE 被“踢”（在附录 D 中描述）时，CPE 调用该方法。该方法的调用参数在表 53 中定义，应答参数在表 54 中定义。

表 53 – Kicked 参数

参数	类型	值
Command	string(32)	通用参数，服务器用它来作识别，或作其它目的。
Referer	string(64)	当被踢出时，发送给 CPE 的“Referer” HTTP 头的值。
Arg	string(256)	通用参数，服务器用它来作识别，或作其它目的。
Next	string(1024)	在正常情况下，服务器应当在本方法的应答中返回的 URL。

表 54 – KickedResponse 参数

参数	类型	值
NextURL	string(1024)	用户的浏览器应当重定向到的下一个 URL。该 URL 可以包括服务器所需的 CGI 参数（比如，为维持会话状态）。 如果服务器希望给用户的浏览器发送 CPE 设备本身的一个页面，则只返回 URL 的路径部分作为结果，（比如“/security/index.html”）。这使 CPE 在 HTTP 302 应答中能够使用自己的规范名称。注意这需要 ACS 通过其它机制（不在本规范中讨论）来对 CPE 设备上的可用 URL 有事先的了解。

如果本方法返回错误，CPE 应当将用户的浏览器重定向到 CPE 设备上的一个错误页面。

为本方法定义的错误代码有：8000，8001，8002，8003，8005。

A.4.2.2 RequestDownload

该方法允许 CPE 向服务器请示求一个文件下载。当接收到该请求时，服务器可以调用 Download 方法来启动下载。本方法的调用参数在表 55 中定义，应答参数在表 56 中定义。

表 55 – RequestDownload 参数

参数	类型	值								
FileType	string(64)	这是被要求的文件类型（见表 27 列示的允许的文件类型）。								
FileTypeArg	ArgStruct[16]	<p>零个或多个附加参数数组，每一个参数是一个表 57 所定义的 name-value 值对结构。对其它参数的使用依赖于指明的 FileType。</p> <p>对每个目前已定义的文件类型，定义了下列参数：</p> <table><tr><th>FileType</th><th>FileTypeArg 名称</th></tr><tr><td>1 Firmware Upgrade</td><td>（无）</td></tr><tr><td>2 Web Content</td><td>“版本”</td></tr><tr><td>3 Vendor Configuration File</td><td>（无）</td></tr></table> <p>如果服务器接收到它不能理解的参数，它必须忽略这些未知参数，但仍然用它能够理解的参数来处理请求。</p>	FileType	FileTypeArg 名称	1 Firmware Upgrade	（无）	2 Web Content	“版本”	3 Vendor Configuration File	（无）
FileType	FileTypeArg 名称									
1 Firmware Upgrade	（无）									
2 Web Content	“版本”									
3 Vendor Configuration File	（无）									

表 56 – RequestDownloadResponse 参数

名称	类型	描述
-	void	该方法应答无参数。

表 57 – ArgStruct 定义

名称	类型	描述
Name	string(64)	参数名称。
Value	string(256)	参数值。

A.5 错误处理

A.5.1 CPE 错误代码

表 51 列示了CPE能够返回的错误代码。注意这些错误代码的值以十进制表示。

表 58– 错误代码

错误代码	描述
9000	方法不支持
9001	拒绝请求（未说明原因）
9002	内部错误
9003	无效参数
9004	资源超限（当用于 SetParameterValues 的关联时，它 <u>不得</u> 用来指示参数错误）
9005	无效参数名（与 Set/GetParameterValues，GetParameterNames，Set/GetParameterAttributes 相关）
9006	无效参数类型（与 SetParameterValues 相关）
9007	无效参数值（与 SetParameterValues 相关）
9008	试图设置不可写的参数（与 SetParameterValues 相关）
9009	Notification 请求被拒（与 SetParameterAttributes 方法相关）
9010	下载失败（与 Download 或 TransferComplete 方法相关）
9011	上载失败（与 Upload 或 TransferComplete 方法相关）
9012	文件传输服务器认证失败（与 Upload，Download，或 TransferComplete 方法相关）
9013	文件传输的协议不支持（与 Upload 和 Download 方法相关）
9800 - 9899	厂商定义的错误代码

A.5.2 服务器错误代码

表 59 列出了服务器能够返回的错误代码。注意错误代码以十进制表示。

表 59 – 错误代码

错误代码	描述
8000	方法不支持
8001	拒绝请求（未指明原因）
8002	内部错误
8003	无效参数
8004	资源超限
8005	重试请求
8800 - 8899	厂商自定义错误代码

A.5.3 服务器方法的重试行为

如果 CPE 调用服务器方法不成功，它应当重试。在重试未成功的方法调用时，CPE 应当使用指数型的 back-off 算法来决定重试的间隔。

CPE 必须结束对方法调用的重试当它接收到一个“重试请求”（错误代码为

8005) 回复。

附录 B. CPE 参数

B.1 简介

本附录定义了 **Internet 网关设备** 的所有 CPE 参数，可以通过附录 A 定义的与 RPC 参数相关的方法来使用。本列表中的参数涵盖 CPE 的要求参数和可选参数。

B.2 CPE 参数

表 61 列出了通过 RPC 的 SetParameterValues, GetParameterValues 和 GetParameterNames 方法使用的 **Internet 网关设备** 的所有已定义的参数。

该表定义的参数的名称，数据类型，参数是否可写，参数是否需要（R-REQUIRED），可选（O-OPTIONAL）或者有条件（C-CONDITIONAL）地进行读或写，以及一个描述。除非特别说明，有条件是指当已经实现了包含它的对象时该参数是需要的。

参数名称使用了与目录树相似的层次形式。某个参数的名称由层次结构中的每个连续的节点连接在一起表示，中间用“.”（点）分隔，并按照从层次的树干到树中的次序。当说明部分路径，即层次中的一个中间节点，总是使用“.”（点）作为最后一个字符。

在某些可能出现一个对象的多个实例的情况下，将显示占位符节点名“{i}”。在实际使用时，该占位符要被实例编号替换，该编号必须是一个正整数（≥1）。

对使用 AddObject 方法对象的实例，该实例号码对应建立时该方法通过 InstanceNumber 参数返回的值。由于在一些情况下，对象实例也可能被删除，因此通常情况下，实例号码是不连接的。

由于本文档只是定义 **Internet 网关设备** 的参数列表，一些对象也可以用于其它类型的设备。在这种情况下，每个参数的路径名应当与表 61 中的定义配置，不同的是要在名称中用真正的设备类型来代替“InternetGatewayDevice”。下列对象可用于其它的大部分设备类型：

- DeviceInfo
- DeviceConfig
- ManagementServer
- Time

B.2.1 数据类型

该规范中定义的参数使用在[8]中定义的默认 SOAP 数据类型的有限子集。参数数据类型完整集合，以及用于表示这些类型的表示法列示在表 60 中。

表 60 – 数据类型

类型	描述
object 对象	参数及/或其它对象的容器。参数的完整路径名由其所属对象的完整路径名加参数名称构成。
string 字符串型	在本规范中列示的字符串，最大允许的长度可以用格式字符串（N）表示，N 是以字符计的最大长度。 对所有的字符串，其最大长度要么明确表明，要么隐含在构成该字符串的元素的大小中。对内容是枚举类型的字符串，枚举的最大值决定了最大长度。如果没有明确指明最大长度或者不是枚举类型的字符串，默认的最大长度为 16 个字符。
int 整数型	从 - 2147483648（含）到+2147483647（含）范围内的整数。 对列示的一些整数型，格式 int[Min:Max]表明取值范围，Min 和 Max 值包含在内。如果没有任一 Min 或 Max，表明没有限值。
unsignedInt 无符号整数型	无符号整数，取值范围为 0（含）到 4294967295（含）。 对列示的一些无符号整数型，格式 unsignedInt[Min:Max]表明取值范围，Min 和 Max 值包含在内。如果没有任一 Min 或 Max，表明没有限值。
boolean 布尔型	布尔型，1 = true（真），0 = false（假）。
dateTime 日期时间型	ISO 8601 data-time 类型的子集，由 SOAP 的 dateTime 型定义。 除非明确指明，所有的时间表示为 UTC（全球统一时间）。 如果 CPE 不知道绝对时间，它应当使用从启动后消逝的时间。比如，启动后的 2 天 3 小时 4 分 5 秒将表示为 0000-00-02T03:04:05。
base64	Base64 编码的二进制。 最大允许的长度可以用格式 base64(N)来表示，N 是指在 Base64 编码后字符的最大长度。

所有 IP 地址及子网掩码使用 IPV4 点分十进制表示法。注意在目前本附录中描述的参数列表不支持 IPv6。

所有 MAC 地址表示为 12 个十六进制数字的字符串（数字 0-9，字符 A-F 或 a-f），显示为用冒号分隔的六对数字。

B.2.2 厂商自定义参数

厂商可以用其自定义的参数和对象来扩展标准参数表。厂商自定义的参数和对象可以定义在不同的命名空间，或者定义在标准的命名空间。

厂商自定义的参数或对象的名称**必须**采用以下格式：

X_<VENDOR>_VendorSpecificName

在该定义中，<VENDOR>是唯一的厂商标识符，可以是一个 OUI 或域名。OUI（organizationally unique identifier 组织的唯一标识）在[9]中定义，**必须**格式化为 6 个十六进制字符的 OUI，所有字母要大写，要包括所有的前置 0。域名必须是大写，并且将每个点（“.”）替换为连字符或下划线。

VendorSpecificName **必须**是在 B.2.1 中定义的有效字符串，并**不得**包含“.”（小数点）或空格字符。

注 – 用字符串“X_”来表示厂商自定义的参数，也就暗示了不得有标准参数可以以“X_”开头

下面是一些厂商自定义的参数或对象名的例子：

InternetGatewayDevice.UserInterface.X_00D09E_AdBanner

InternetGatewayDevice.LANDevice.1.X_00D09E_LANInfraredInterfaceConfig.2.
Status

X_GAMECO-COM_GameDevice.Info.Type

在需要时，厂商也可以扩展枚举类型的值集。如果这样做，厂商自定义的值必须使用格式“X_<VENDOR>_VendorSpecificValue”。这样的字符的总长度不得超过 31 字节。

B.2.3 参数列表

表 61 – Internet 网关设备的 CPE 参数列表

名称 ¹⁰	类型	写 ¹¹	读 ¹³	描述
InternetGatewayDevice.	object	- ¹²	R	Internet 网关设备的顶级对象。
LANDeviceNumberOfEntries	unsignedInt	-	R	LANDevice 的实例数目。
WANDeviceNumberOfEntries	unsignedInt	-	R	WANDevice 的实例数目。
InternetGatewayDevice.DeviceInfo.	object	-	R	此对象包含通用的设备信息。
Manufacturer	string(64)	-	R	CPE 的制造商（可人读字符串）。
ManufacturerOUI	string(6)	-	R	设备制造商的组织唯一标识。表示为 6 位十六进制字符，全部使用大写字母，并包含任何前缀零。OUI 的值必须是有效的由[9]中定义的 OUI。
ModelName	string(64)	-	R	CPE 型号名称（可人读字符串）。
Description	string(256)	-	R	CPE 设备的完整描述（可人读字符串）。
ProductClass	string(64)	-	O	指定产品序列号所归属的产品类别。即，对指定制造商，该参数用于区分产品或产品类型，在该类型中，SerialNumber 参数是唯一的。
SerialNumber	string(64)	-	R	CPE 的序列号
HardwareVersion	string(64)	-	R	说明特定 CPE 的型号和版本的字符串。
SoftwareVersion	string(64)	-	R	说明安装在 CPE 上的软件的版本。 为允许版本比较，该元素应当采用点分整数格式，每个相对较后的整数代表一个更小的变化分类。比如，3.0.21 的各项成分代表：主版本号.子版本号.Build。
ModemFirmwareVersion	string(64)	-	O	说明安装在 CPE 上的 Modem firmware 的版本。只有在 Modem 的 firmware 与整体 CPE 软件可以分开时才会使用。
EnabledOptions	string(1024)	-	O	CPE 上当前已经启用的选项名称（OptionName）列表，以逗号分隔。每一 OptionName 与表 48 中描述的 OptionStruct 中的 OptionName 元素等同。只有其 State 状态表明已启用的选项才会列在这里。
AdditionalHardwareVersion	string(64)	-	O	逗号分隔的任何其它版本的列表。代表厂商希望提供的附加硬件版本信息。
AdditionalSoftwareVersion	string(64)	-	O	逗号分隔的任何其它版本的列表。代表厂商希望提供的附加软件版本信息。

¹⁰ 参数全名用黄色表头显示的参数名称与其后的参数名称拼接起来形成。

¹¹ “R” = Required需要, “O” = Optional可选, “C” = Conditional有条件, “-” = Not present无

¹² 对象的写访问是指该对象对AddObject和DeleteObject动作的支持是不允许(“-”), 可选地允许(“O”), 需要 (“R”), 或有条件允许(“C”)。

¹³ 对象的读访问是指该对象在CPE支持相应的功能或包含的对象存在的情况下, 该对象是否可选(“O”), 需要 (“R”)或者有条件地需要(“C”)。

名称 ¹⁰	类型	写 ¹¹	读	描述
SpecVersion	string(16)	-	R	代表该设备所实现的规范的版本。目前 1.0 是唯一可用的版本。
ProvisioningCode	string(64)	R	R	说明首要服务提供商或其它供给信息。服务器可以用该信息来决定与服务商相关的定制及其它供给参数。如果非空，该参数应当表示为含一个或多个节点的层次状描述。层次中的每个节点表示为 4 字符的子串，并包含数字或大写字母。如果有多于一个节点，则用 “.”（点）分隔。例子：“TLCO” 或 “TLCO.GRP2”。
UpTime	unsignedInt	-	R	CPE 上次重新启动以来的秒数。
FirstUseDate	dateTime	-	O	CPE 第一次成功建立网络连接的日期和时间（UTC）。
DeviceLog	string(32K)	-	R	厂商规定的日志。
VendorConfigFileNumberOfEntries	unsignedInt	-	O	VendorConfigFile 的实例数目。
InternetGatewayDevice.DeviceInfo.VendorConfigFile.{i}.	object	-	O	该对象的每一个实例是一个厂商配置文件，包括该厂商配置文件相关的参数。
Name	string(64)	-	C	厂商配置文件的名称。
Version	string(16)	-	C	字符串，说明 CPE 当前使用的配置文件版本。
Date	dateTime	-	C	CPE 首次应用该厂商配置文件当前配置内容的日期和时间。
Description	string(256)	-	O	厂商配置文件的说明（可人读字符串）。
InternetGatewayDevice.DeviceConfig.	object	-	O	该对象包括通用配置参数。
PersistentData	string(256)	O	O	CPE 重启后仍需存在的任意用户数据。
ConfigFile	string(32K)	O	O	CPE 当前正在运行的配置文件的转储。该参数提供备份和恢复最近的 CPE 正常运行状态的能力。该参数返回厂商规定的定义 CPE 状态的文档。在用 SetParameterValues 方法写回到 CPE 时，该文档必须能恢复 CPE 的状态。
InternetGatewayDevice.ManagementServer.	object	-	R	该对象包含 CPE 与 ACS 关联的参数。
URL	string(256)	R	R	CPE 使用 CPE WAN 管理协议连接 ACS 使用的 URL。该参数必须使用有效的 HTTP 或 HTTPS URL[5]格式。HTTPS URL 表明 ACS 支持 SSL。在基于证书的认证方法下，CPE 用该 URL 的 “host” 部分来验证 ACS 的证书。
Username	string(256)	R	-	当 CPE 使用 CPE WAN 管理协议来连接时 ACS 时，用于认证 CPE 的用户名。该用户名仅用于对 CPE 的基于 HTTP 的认证。
Password	string(256)	R	-	当 CPE 使用 CPE WAN 管理协议来连接时 ACS 时，用于认证 CPE 的密码。该密码仅用于对 CPE 的基于 HTTP 的认证。收到读请求时，该参数不管实际值如何，总返回一个空字符串。
PeriodicInformEnable	boolean	R	R	是否 CPE 必须定期向服务器通过 Inform 方法调用发送 CPE 信息。
PeriodicInformInterval	unsignedInt[1:]	R	R	在 PeriodicInformEnable 为真时，CPE 必须试图连接 ACS 并调用 Inform 方法的时间间隔（以秒计）。
PeriodicInformTime	dateTime	R	R	绝对时间值（UTC），决定 CPE 何时发起 Inform 方法调用。每个 Inform 方法必须在该值加上或减去 PeriodicInformInterval 的整数倍时调用。零 dateTime 值（0000-00-00T00:00:00）表示没有指定特定的时间。即，CPE 可以自主选时间，只要与指定的 PeriodicInformInterval 一致即可。

名称 ¹⁰	类型	写 ¹¹	读	描述
ParameterKey	string(32)	-	R	服务器最近调用 SetParameterValues, AddObject 或 DeleteObject 方法的 ParameterKey 参数的值。如果没有这样的调用, 该值为空。
ConnectionRequestURL	string(256)	-	R	ACS 向 CPE 发送连接请求 notification 时所用的 HTTP URL。格式为: http://host:port/path URL 的“host”部分可以用 CPE 管理接口的 IP 地址来代替主机名。
ConnectionRequestUsername	string(256)	R	R	ACS 向 CPE 发送连接请求时用于认证 ACS 的用户名。
ConnectionRequestPassword	string(256)	R	-	ACS 向 CPE 发送连接请求时用于认证 ACS 的密码。当接收到读请求时, 不管真实值如何, 参数都返回一个空字符串。
UpgradesManaged	boolean	R	R	说明 ACS 是否会管理 CPE 的升级。如果为真 (1), CPE 应当不使用除 ACS 以外的途径来搜索可用的升级。如果为假 (0), CPE 可以使用其它途径来升级。
KickURL	string(256)	-	O	仅在 CPE 支持 Kicked RPC 方法时才存在。 LAN 可访问的 URL, 从这里 CPE 能被“踢出”以发起 Kicked PRC 方法调用。 必须是绝对 URL , 包括主机名或 IP 地址, 并且用于 CPE 的 LAN 端。
DownloadProgressURL	string(256)	-	O	只在 CPE 提供 LAN 端的网页来显示文件下载进程时才使用。 在初始化文件下载时, ACS 的 web 服务器可以将用户的浏览器重定向到该 LAN 可访问的 URL 上, 向用户说明下载的状态。
InternetGatewayDevice.Time.	object	-	O	该对象包括与 CPE 中的 NTP 或 SNTP 时间客户端相关的参数。对该对象的支持是可选的。
NTPServer1	string(64)	C	C	第一个 NTP 时间服务器。可以是主机名或 IP 地址。
NTPServer2	string(64)	C	C	第二个 NTP 时间服务器。可以是主机名或 IP 地址。
NTPServer3	string(64)	O	O	第三个 NTP 时间服务器。可以是主机名或 IP 地址。
NTPServer4	string(64)	O	O	第四个 NTP 时间服务器。可以是主机名或 IP 地址。
NTPServer5	string(64)	O	O	第五个 NTP 时间服务器。可以是主机名或 IP 地址。
CurrentLocalTime	dateTime	-	C	在 CPE 当地时区当前的日期和时间。
LocalTimeZone	string(6)	C	C	当地时间与 UTC 的位移, 格式为: +hh:mm -hh:mm
LocalTimeZoneName	string(64)	C	C	当地时区的名称 (可人读字符串)
DaylightSavingsUsed	boolean	C	C	在 CPE 的当地时区中是否使用夏令时。
DaylightSavingsStart	dateTime	C	C	在当地标准时间中夏令时的开始时期与时间。如果夏令时未使用, 忽略该值。
DaylightSavingsEnd	dateTime	C	C	在当地标准时间中夏令时的结束时期与时间。如果夏令时未使用, 忽略该值。
InternetGatewayDevice.UserInterface.	object	-	O	本对象包含与 CPE 的用户界面相关的参数。对该对象的支持是可选的。
PasswordRequired	boolean	O	O	仅在 CPE 提供 LAN 端的密码保护的用户界面时存在。说明是否本地的用户界面必须提供一个用户选择的密码。如果为假, 是否选用密码由用户自己决定。

名称 ¹⁰	类型	写 ¹¹	读	描述
PasswordUserSelectable	boolean	O	O	仅在 CPE 提供 LAN 端的密码保护的用户界面并且支持 LAN 端的自动配置时存在。 说明是否保护 CPE 本地用户界面的密码是用户直接选择，还是必须与 LAN 端的自动配置协议使用的密码相同。
UpgradeAvailable	boolean	O	O	指示有可用的 CPE 升级，允许 CPE 将该信息显示给用户。
WarrantyDate	dateTime	O	O	指示 CPE 保单过期的日期与时间（UTC）。
ISPName	string(64)	O	O	客户 ISP 的名称。
ISPHelpDesk	string(32)	O	O	ISP 的客户服务电话。
ISPHomePage	string(256)	O	O	ISP 首页的 URL。
ISPHelpPage	string(256)	O	O	ISP 联机支持页面的 URL。
ISPLogo	base64 (5460)	O	O	Base64 编码的 GIF 或 JPEG 图像。该二进制图像限于 4905 字节或更小。
ISPLoSize	unsignedInt [0:4095]	O	O	以字节计的未编码的二进制图像大小。 如果 ISPLoSize 的输入值是 0 则 ISPLoSize 被清除。 ISPLoSize 也可以用来检验从 Base64 到图像是否经正确的传输和转换。
ISPMailServer	string(256)	O	O	ISP 邮件服务器的 URL。
ISPNewsServer	string(256)	O	O	ISP 新闻服务器的 URL。
TextColor	string(6)	O	O	GUI 屏幕的文字颜色，RGB 十六进制表示法（FF0088）。
BackgroundColor	string(6)	O	O	GUI 屏幕的背景颜色，RGB 十六进制表示法（FF0088）。
ButtonColor	string(6)	O	O	GUI 屏幕的按钮颜色，RGB 十六进制表示法（FF0088）。
ButtonTextColor	string(6)	O	O	GUI 屏幕的按钮上的文字颜色，RGB 十六进制表示法（FF0088）。
AutoUpdateServer	string(256)	O	O	CPE 用来检查是否有直接可以下载的升级信息的服务器。如果 InternetGatewayDevice.ManagementServer.UpgradeManaged 值为真，CPE 不得使用此参数。
UserUpdateServer	string(256)	O	O	用户通过 WEB 浏览器能够检查的是否有直接可以下载到 PC 的升级信息的服务器。如果 InternetGatewayDevice.ManagementServer.UpgradeManaged 值为真，CPE 不得使用此参数。
ExampleLogin	string(40)	O	O	根据 ISP 规定的规则，正确 login 的例子。
ExamplePassword	string(30)	O	O	根据 ISP 规定的规则，正确 password 的例子。
InternetGatewayDevice.Layer3Forwarding.	object	-	R	本对象允许管理设备上的路由和转发配置。
DefaultConnectionService	string(256)	R	R	说明默认的 WAN 接口。其内容是默认三层连接对象的完整层次参数名。例如，"InternetGatewayDevice.WANDevice.1.WANConnectionDevice.2.WANPPPOConnection.1"。
ForwardNumberOfEntries	unsignedInt	-	R	转发实例的数目。
InternetGatewayDevice.Layer3Forwarding.Forwarding.{i}.	object	R	R	3 层转发表。
Enable	boolean	R	R	启用或禁用转发条目。在建立时，默认情况下条目是禁用的。

名称 ¹⁰	类型	写 ¹¹	读	描述
Status	string	-	R	说明转发条目的状态。枚举值有： “Disabled” “Enabled” “Error”
Type	string	R	R	说明路由的类型。枚举值有： “Default” “Network” “Host”
DestIPAddress	string	R	R	目标地址。
DestSubnetMask	string	R	R	目标子网掩码。
SourceIPAddress	string	R	R	源地址。
SourceSubnetMask	string	R	R	源子网掩码。
GatewayIPAddress	string	R	R	网关的 IP 地址。
Interface	string	R	R	说明与该条目相关的 WAN 接口。其内容是 3 层连接对象的完整层次状参数名。例如： “InternetGatewayDevice.WANDevice.1.WANConnectionDevice.2.WANPPPPConnection.1”。
ForwardingMetric	int[-1:]	R	R	转发量度值。值为-1 说明不使用该量度值。
MTU	unsignedInt[1:1540]	O	O	最大传输单元，说明该路由可使用的 Ethernet 帧的最大允许长度。
InternetGatewayDevice.LANConfigSecurity.	object	-	R	该对象包含通用设备配置信息。
ConfigPassword	string(64)	R	-	对被保护的自动配置服务的 LAN 访问使用的密码。收到读取请求，该参数返回空字符串，而不管真实值如何。
InternetGatewayDevice.IPPingDiagnostics	object	-	O	该对象允许对 IP 层的 Ping 测试。
DiagnosticsState	string	C	C	说明测试数据的可用性。取下列值之一： “None” “Requested” “Complete” “Error_CannotResolveHostName” 把值设置为“Requested”来发起诊断测试。当写此参数时，只允许写“Requested”值。为了保证使用正确的测试参数（本对象的可写参数），测试参数 必须 在设置 DiagnosticState 值为 Requested 之前或同时设置（使用同一 SetParameterValues 方法）。 如果收到请求，CPE 应当 等与 ACS 之间的通信会话结束后再开始诊断过程。 当由 ACS 发起的诊断结束后（不管成功还是失败），CPE 必须 建立到 ACS 的新的连接，允许 ACS 查看结果，并在 Inform 报文中指明报文代码“8 DIAGNOSTICS COMPLETE”。
Interface	string(256)	C	C	说明测试执行的 WAN 或 LAN 的 IP 层接口。其内容是接口的完整层次状参数名称。 下面是一个 WAN 接口的例子： “InternetGatewayDevice.WANDevice.1.WANConnectionDevice.2.WANPPPPConnection.1” 下面是一个 LAN 接口的例子： “InternetGatewayDevice.LANDevice.1.LANHostConfigManagement.IPInterface.1”
Host	string(256)	C	C	要 ping 的主机的主机名或地址。

名称 ¹⁰	类型	写 ¹¹	读	描述
NumberOfRepetitions	unsignedInt[1:]	C	C	在报告结果前要重复多少次 ping 测试。
Timeout	unsignedInt[1:]	C	C	Ping 测试超时的微秒数。
DataBlockSize	unsignedInt[1:65535]	C	C	每个 Ping 要发送的数据块大小（以字节计）。
DSCP	unsignedInt[0:64]	C	C	测试分组要使用的 DiffServ codepoint。默认情况下 CPE 将该值设为 0。
SuccessCount	unsignedInt	-	C	结果参数，表明最近的 ping 测试中成功 ping 的次数（在超时前收到的成功的 ping 应答）。
FailureCount	unsignedInt	-	C	结果参数，表明在最近的 ping 测试中失败的 ping 次数。
AverageResponseTime	unsignedInt	-	C	结果参数，表明在最近的 ping 测试中，所有的成功 ping 应答所花费的平均应答时间（单位：毫秒）。如果没有成功应答，该值 必须 为零。
MinimumResponseTime	unsignedInt	-	C	结果参数，表明在最近的 ping 测试中，所有的成功 ping 应答所花费的最小应答时间（单位：毫秒）。如果没有成功应答，该值 必须 为零。
MaximumResponseTime	unsignedInt	-	C	结果参数，表明在最近的 ping 测试中，所有的成功 ping 应答所花费的最大应答时间（单位：毫秒）。如果没有成功应答，该值 必须 为零。
InternetGatewayDevice.LANDevice.{i}	object	-	R	每个实例包括给定桥接子网中所有 LAN 相关的对象。
LANEthernetInterfaceNumberOfEntries	unsignedInt	-	R	在该 LANDevice 中 LANEthernetInterfaceConfig 实例的数目。
LANUSBInterfaceNumberOfEntries	unsignedInt	-	R	在该 LANDevice 中 LANUSBInterfaceConfig 的实例数目。
LANWLANConfigurationNumberOfEntries	unsignedInt	-	R	在该 LANDevice 中 WANConfiguration 的实例数目。
InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.	object	-	R	本对象启用 LAN 相关设备信息的报告，设置和配置 LAN IP 地址。
DHCPServerConfigurable	boolean	R	R	在 LAN 接口上启用 DHCP 服务器配置。如果该变量设置为 false，则 CPE 应当恢复其默认的 DHCP 服务器设置。
DHCPServerEnable	boolean	R	R	启用或禁用 LAN 接口的 DHCP 服务。
DHCPRelay	boolean	-	R	说明在 LAN 接口上，DHCP 服务执行服务器（0）的角色还是中继（1）的角色。
MinAddress	string	R	R	说明在 LAN 接口上 DHCP 服务器可以分配的地址池中的第一个地址。
MaxAddress	string	R	R	说明在 LAN 接口上 DHCP 服务器可以分配的地址池中的最后一个地址。
ReservedAddresses	string	R	R	以逗号分隔的地址列表，在地址分配池中标记为保留。
SubnetMask	string	R	R	说明客户端的网络子网掩码。
DNSServers	string	R	R	逗号分隔的提供给 DHCP 客户端的 DNS 服务器列表。对三个以上 DNS 服务器的支持是可选的。
DomainName	string(64)	R	R	在 LAN 接口上提供给客户的域名。
IPRouters	string	R	R	在本子网上以逗号分隔的路由器的 IP 地址列表。也称为默认网关。对超过一个路由器地址的支持是可选的。
DHCPLeaseTime	int[-1:]	O	O	说明分配给客户端的 IP 地址的租约时间（以秒计）。值-1 表明无限期租约。

名称 ¹⁰	类型	写 ¹¹	读	描述
UseAllocatedWAN	string	O	O	枚举值： “Normal” “UseAllocatedSubnet” “Passthrough” 如果为 Normal，DHCP 地址从私有网络地址池中分配。 如果为 UseAllocatedSubnet，指示 CPE 从 AssociatedConnection 中标明的 WAN 连接的 WAN 子网块中分配 DHCP 地址。 如果为 Passthrough，由 Passthrough MAC 地址指定的 LAN 主机将获得 WAN IP 地址。
AssociatedConnection	string(256)	O	O	当 UseAllocatedWAN 设置为 UseAllocatedSubnet 或 Passthrough 时，本参数用来说明用做地址分配的连接实例。其内容是默认的 3 层连接对象的完整层次状参数名。例如： “InternetGatewayDevice.WANDevice.1.WANConnectionDevice.2.WANPPPConnection.1”。
PassthroughLease	unsignedInt	O	O	当 WAN IP 地址为 passed-through 时，分配给指定 LAN 主机的以秒计的 DHCP 租约时间。 注意：在获得 WAN IP 地址之前，可以先分配一个临时的私有的租约很短（如 1 分钟）的 IP 地址给要传递的 LAN 主机。
PassthroughMACAddress	string	O	O	如果 UseAllocatedWAN 的值为 “Passthrough”，该参数的值是要传递 WAN IP 地址的 LAN 主机的硬件地址。
AllowedMACAddresses	string	O	O	对给出的接口，如果其 MACAddressControlEnabled 值为 1，本参数值为允许连接到本连接的逗号分隔的硬件地址列表。
IPInterfaceNumberOfEntries	unsignedInt	-	R	CPE LAN 端的 IP 接口的数目。对不支持多宿主接口的 CPE，1 是一个典型值。对多于一个接口实例的支持是可选的。
InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.IPInterface.{i}.	object	O	R	IP 接口表。
Enable	boolean	R	R	启用或禁用本条目。在建立时，条目默认是禁用的。
IPInterfaceIPAddress	string	R	R	CPE LAN 端接口的 IP 地址。
IPInterfaceSubnetMask	string	R	R	IGD 的 LAN 端接口的子网掩码。
IPInterfaceAddressingType	string	R	R	代表 CPE 该接口的 LAN 端 IP 地址的寻址方式。为枚举值： “DHCP” “Static” “AutoIP”
InternetGatewayDevice.LANDevice.{i}.LANEthernetInterfaceConfig.{i}.	object	-	C	该对象是 CPE 设备上的 Ethernet LAN 连接的模型。如果 CPE 包含 LAN 端的以太网接口，就必须实现该对象。
Enable	boolean	C	C	启用或禁用该接口。
Status	string	-	C	表明接口状态。枚举值： “Up” “NoLink” “Error” “Disabled”
MACAddress	string	-	C	接口的物理地址。

名称 ¹⁰	类型	写 ¹¹	读	描述
MACAddressControlEnabled	boolean	C	C	说明本接口上 MAC 地址控制是否启用。MAC 地址控制限制客户端连接在 InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.AllowedMACAddresses 中说明的允许的 MAC 地址表中的主机。
MaxBitRate	string	C	C	该连接可用的最大上行和下行位速率。枚举值： “10” “100” “1000” “Auto”
DuplexMode	string	C	C	该连接可用的复用模式，为枚举值： “Half” “Full” “Auto”
InternetGatewayDevice.LANDevice.{i}.LANEthernetInterfaceConfig.{i}.Stats.	object	-	C	本对象包括 CPE 设备的以太网 LAN 接口的统计。
BytesSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上发送的总字节数。
BytesReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上接收的总字节数。
PacketsSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上发送的总分组数。
PacketsReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上接收的总分组数。
InternetGatewayDevice.LANDevice.{i}.LANUSBInterfaceConfig.{i}.	object	-	C	该对象是 CPE 设备上的 USB LAN 连接的模型。如果 CPE 包含 LAN 端的 USB 接口，就必须实现该对象。
Enable	boolean	C	C	启用或禁用该接口。
Status	string	-	C	表明接口状态。枚举值： “Up” “NoLink” “Error” “Disabled”
MACAddress	string	-	C	接口的物理地址。
MACAddressControlEnabled	boolean	C	C	说明本接口上 MAC 地址控制是否启用。MAC 地址控制限制客户端连接在 InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.AllowedMACAddresses 中说明的允许的 MAC 地址表中的主机。
Standard	string(6)	-	C	设备支持的 USB 版本。
Type	string	-	C	USB 接口类型，枚举值： “Host” “Hub” “Device”
Rate	string	-	C	USB 接口的速率。枚举值： “Low” “Full” “High” (USB 2.0)
Power	string	-	C	USB 接口的电源配置。枚举值： “Self” “Bus” “Unknow”
InternetGatewayDevice.LANDevice.{i}.LANUSBInterfaceConfig.{i}.Stats.	object	-	C	本对象包含 CPE 设备上 USB LAN 接口的统计。
BytesSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上发送的总字节数。
BytesReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上接收的总字节数。
CellsSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上发送的总信元数。

名称 ¹⁰	类型	写 ¹¹	读	描述
CellsReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上接收的总信元数。
InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.	object	-	C	本对象定义 CPE 设备的 802.11 LAN 的连接模型。如果 CPE 包含 LAN 端的 802.11 接口，就必须实现本对象。
Enable	boolean	C	C	启用或禁用本接口。
Status	string	-	C	说明本接口的状态。枚举值： “Up” “Error” “Disabled”
BSSID	string	-	C	接口的 MAC 地址。
MaxBitRate	string(4)	C	C	以 Mbps 为本连接可用的最大上行和下行位速率。或者是 “Auto” 或者是 OperationalData TransmitRates 的最大值。
Channel	unsignedInt[0:255]	C	C	连接使用的当前无线电频道。注意：目前没有请求自动选择频道的方法。
SSID	string(32)	C	C	连接使用的目前服务设置标识。SSID 是一个标识符，附加在通过无线 LAN 发送的分组中，为加入到特定的无线网络（BSS）起到“密码”的作用。注意：如果接入点（AP）希望提供多于一个 SSID，它必须为每个 SSID 提供一个 WLANConfiguration 实例。
BeaconType	string	C	C	该连接使用的信标类型。枚举值： “None” “Basic” “WPA” “11i”（可选） “BasicandWPA”（可选） “Basicand11i”（可选） “WPAand11i”（可选） “BasicandWPAand11i”（可选）
MACAddressControlEnabled	boolean	C	C	说明本接口上 MAC 地址控制是否启用。MAC 地址控制限制客户端连接在 InternetGatewayDevice.LANDevice.{i}.LANHostConfigManagement.AllowedMACAddresses 中说明的允许的 MAC 地址表中的主机。
Standard	string	-	C	说明设备当前运行在 IEEE 802.11 的哪个模式下。枚举值： “a” “b” “g”
WEPKeyIndex	unsignedInt[1:4]	C	C	默认 WEP 密钥的索引。

名称 ¹⁰	类型	写 ¹¹	读	描述
KeyPassphrase	string(63)	C	-	<p>产生 WEP 密钥的 passphrase。这一参数只是为了提供信息——CPE 不负责根据该值产生密钥。</p> <p>对 WLANConfiguration 的同一实例，该参数与 InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.PreSharedKey.1.KeyPassphrase 参数的值相同。当其中一个参数值变化，另一个值也相应变化。</p> <p>该值或者必须使用能被 8 整除的密钥长度，在这种情况下，每一字节为密钥贡献 8 位，或者必须由十六进制数字构成，长度必须能够被 4 整除，在这种情况下，每一字节为密钥贡献 4 位。</p> <p>注意：如果使用了 passphrase，所有 4 个 WEB 密钥应当相同。</p> <p>当收到读取请求时，不管真实值如何，该参数返回一个空串。</p>
WEPEncryptionLevel	string(64)	-	C	<p>所支持的密钥长度的逗号分隔的列表。列表中的每一项为枚举值：</p> <p>“Disabled”</p> <p>“40-bit”</p> <p>“104-bit”</p> <p>任何其它厂商自定义的值必须以位为单位的密钥的长度开头。</p>
BasicEncryptionModes	string(31)	C	C	<p>当启用了 basic 802.11 时可用的加密模式。</p> <p>“WEPEncryption” 暗指所有无线客户端可以使用 WEP 作数据加密。枚举值：</p> <p>“None”</p> <p>“WEPEncryption”</p>
BasicAuthenticationMode	string(31)	C	C	<p>当启用了 basic 802.11 时可使用的认证模式。枚举值：</p> <p>“None”</p> <p>“EAPAuthentication”（可选）</p>
WPAEncryptionModes	string(31)	C	C	<p>当启用 WPA 时可使用的加密模式。枚举值：</p> <p>“WEPEncryption”</p> <p>“TKIPEncryption”</p> <p>“WEPandTKIPEncryption”</p> <p>“AESEncryption”（可选）</p> <p>“WEPandAESEncryption”（可选）</p> <p>“TKIPandAESEncryption”（可选）</p> <p>“WEPandTKIPandAESEncryption”（可选）</p>
WPAAuthenticationMode	string(31)	C	C	<p>启用 WPA 后可使用的认证方法。为枚举值：</p> <p>“PSKAuthentication”</p> <p>“EAPAuthentication”（可选）</p>
IEEE11iEncryptionModes	string(31)	O	O	<p>启用 802.11i 后可使用的加密模式。枚举值：</p> <p>“WEPEncryption”</p> <p>“TKIPEncryption”</p> <p>“WEPandTKIPEncryption”</p> <p>“AESEncryption”（可选）</p> <p>“WEPandAESEncryption”（可选）</p> <p>“TKIPandAESEncryption”（可选）</p> <p>“WEPandTKIPandAESEncryption”（可选）</p>
IEEE11iAuthenticationMode	string(31)	O	O	<p>启用 802.11i 后可使用的认证模式。枚举值：</p> <p>“PSKAuthentication”</p> <p>“EAPAuthentication”（可选）</p> <p>“EAPandPSKAuthentication”（可选）</p>

名称 ¹⁰	类型	写 ¹¹	读	描述
PossibleChannels	string(1024)	-	C	无线标准（a, b 或 g）可能的无线电频道及规范的域。为逗号分隔的列表。允许范围格式“n-m”。例如，对 802.11b 及北美洲可以是“1-11”。
BasicDataTransmitRates	string(256)	C	C	逗号分隔的列表，其内容为接入点（AP）的单播，多播和广播帧的数据传播速率（单位为 Mbps）。比如，值“1,2”说明单播，多播和广播帧可以在 1Mbps 和 2Mbps 的速率上传播。
OperationalDataTransmitRates	string(256)	C	C	逗号分隔的列表，其内容为接入点（AP）的单播帧的数据传播速率（单位为 Mbps），该值为 BasicDataTransmitRates 的超集。按照上面例子 BasicDataTransmitRates 的值，OperationalDataTransmitRates 可以是“1,2,5.5,11”，说明单播帧还可以在 5.5Mbps 和 11Mbps 的速率上传播。
PossibleDataTransmitRates	string(256)	-	C	逗号分隔的列表，其内容为接入点（AP）允许一个站点连接的单播帧的数据传播速率（单位为 Mbps），该值为 OperationalDataTransmitRates 的子集。按照上面例子 BasicDataTransmitRates 和 OperationalDataTransmitRates 的值，PossibleDataTransmitRates 可以是“1,2,5.5”，说明 AP 将允许以 1Mbps, 2Mbps 和 5.5Mbps 的连接，即使理论上它可以接受 11Mbps 的连接。
InsecureOOBAccessEnabled	boolean	O	O	指示本对象的参数是否允许通过 CPE WAN 管理协议以外的机制进行非安全的写访问。
BeaconAdvertisementEnabled	boolean	O	O	指示接入点（AP）是否发送信标。
RadioEnabled	boolean	C	C	指示接入点（AP）是否启用无线。
AutoRateFallBackEnabled	boolean	C	C	指示接入点（AP）是否在噪音或争用情况下自动降低数据速度。
LocationDescription	string(4906)	C	C	XML 描述的信息，用于说明接入点（AP）的名称和物理位置。CPE 不解析该字符串，而只是把它看作一个不透明的字符串。空串表明没有设置位置信息。
RegulatoryDomain	string(3)	O	O	802.11d 规范的域串。前两个八位是 ISO/IEC 3166-1 的两个字符的国家代码。第三个八位或者是“”（所有环境），或“O”（外面）或“I”（里面）。
TotalPSKFailures	unsignedInt	-	O	共享密钥（PSK – Pre-Shared Key）认证失败的次数。只与 WPA 与 802.11i 相关。
TotalIntegrityFailures	UnsignedInt	-	O	MICHAEL 完整性检查失败的次数（只与 WPA 和 802.11i 相关）。
ChannelsInUse	string(1024)	-	O	接入点（AP）认为当前使用的频道（包括它自己使用的频道）。为逗号分隔的列表。允许范围格式“n-m”。
DeviceOperationMode	string(31)	O	O	当前接入点（AP）的操作模式。可选的模式允许 AP 配置为无线网桥（桥接两个有线网络），中继器（也可以为无线客户端服务的网桥），或无线站点。不支持 Ad hoc 站点。枚举值： “InfrastructureAccessPoint” “WirelessBridge”（可选） “WirelessRepeater”（可选） “WirelessStation”（可选）
DistanceFromRoot	unsignedInt	O	O	从根接入点（AP）到无线中继器或网桥的跳数。
PeerBSSID	string	O	O	在无线中继器或网桥模式中对等体的 MAC 地址。

名称 ¹⁰	类型	写 ¹¹	读	描述
AuthenticationServiceMode	string	O	O	说明是否在客户端认证中有相关的其它服务（LinkAuthentication 表明有 colocated 认证服务器，RadiusClient 表明有外置的 RADIUS 服务器）。枚举值： “None” “LinkAuthentication”（可选） “RadiusClient”（可选）
TotalBytesSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上发送的总字节数。
TotalBytesReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上接收的总字节数。
TotalPacketsSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上发送的总分组数。
TotalPacketsReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上接收的总分组数。
TotalAssociations	unsignedInt	-	C	与接入点（AP）关联设备的当前数目。对应 AssociatedDevice 表中的条目数。
InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.AssociatedDevice.{i}	object	-	C	当前与接入点（AP）关联的设备表。表的大小由 InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.TotalAssociations 给出。如果 CPE 设备在 LAN 端含有 802.11 接口，就必须实现此对象。
AssociatedDeviceMACAddress	string	-	C	关联设备的 MAC 地址。
AssociatedDeviceIPAddress	string(64)	-	C	关联设备的 IP 地址或 DNS 名称。
AssociatedDeviceAuthenticationState	boolean	-	C	是否关联设备已经认证。已认证(true)，未认证(false)。
LastRequestedUnicastCipher	string(256)	-	O	指定 MAC 地址的站点（仅适用 802.11i）最近使用的单播密码。
LastRequestedMulticastCipher	string(256)	-	O	指定 MAC 地址的站点（仅适用 802.11i）最近使用的多播密码。
LastPMKId	string(256)	-	O	指定 MAC 地址的站点（仅适用 802.11i）最近使用的 PMK（pairwise master key）。
InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.WEPKey.{i}	object	-	C	这是 WEB 密钥表。该表的大小是固定的，共 4 个条目（实例号码从 1 到 4）。如果 CPE 在 LAN 端有 802.11 接口，就必须实现该对象。
WEPKey	string(128)	C	-	用十六进制字符串表示的 WEP 密钥。WEP 加密的等级可从密钥的长度推断出，如 10 个字符表示 40 位加密，26 个字符表示 104 位加密。 当收到读请求时，该方法将返回一个空字符串，而不管真实值是什么。
InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.PreSharedKey.{i}	object	-	C	共享密钥表。该表的大小是固定的，共 10 个条目（实例号码从 1 到 10）。如果 CPE 在 LAN 端有 802.11 接口，就必须实现该对象。
PreSharedKey	string(64)	C	-	以十六进制字符串表示的 WPA PSK。 表的第一个条目包含默认的 PreSharedKey (InternetGatewayDevice.LANDevice.{i}.WLANConfiguration.{i}.PreSharedKey.1.PreSharedKey)。 当收到读请求时，该方法将返回一个空字符串，而不管真实值是什么。

名称 ¹⁰	类型	写 ¹¹	读	描述
KeyPassphrase	string(63)	C	-	<p>用于产生 WEP 或 PSK 密钥的 passphrase。该参数只是为了提供信息——CPE 并不负责基于 passphrase 来产生密钥。</p> <p>对 WEP 密钥，该值或者必须使用能被 8 整除的密钥长度，在这种情况下，每一字节为密钥贡献 8 位；或者必须由十六进制数字构成，长度必须能够被 4 整除，在这种情况下，每一字节为密钥贡献 4 位。</p> <p>对 WPA PSK，该值是用 WPA 定义的方法产生，使用 PKCS #5 规范的 PBKDF2（PKCS #5：基于密码加密规范 Password-based Cryptography Specification Version 2.0 (RFC2898)）。</p> <p>注：802.11i 标准定义了从 passphrase 产生 WEP 密钥的方法。</p> <p>当收到读请求时，该方法将返回一个空字符串，而不管真实值是什么。</p>
AssociatedDeviceMACAddress	string	O	O	与共享密钥关联的 MAC 地址，或空字符串（当没有 MAC 地址与密钥关联）。
InternetGatewayDevice.LANDevice.{i}.Hosts.	object	-	R	本对象提供 LAN 中的每一台主机的信息，包括那些使用 DHCP 从 CPE 获得地址的主机，以及静态指定 IP 地址的主机。
HostNumberOfEntries	unsignedInt	-	R	主机表中的条目的数目。
InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}.	object	-	R	主机表。
IPAddress	string	-	R	主机的当前 IP 地址。
AddressSource	string	-	R	<p>说明主机的 IP 地址是使用 DHCP 从 CPE 分配的，还是静态配置的，还是使用自动 IP 地址分配方法分配的。枚举值：</p> <p>“DHCP”</p> <p>“Static”</p> <p>“AutoIP”</p>
LeaseTimeRemaining	int[-1:]	-	R	<p>以秒计的剩余 DHCP 租约时间。值-1 表明无限期租约。如果 AddressSource 不是 DHCP，该值必须为 0（零）。</p>
MACAddress	string	-	R	主机的 MAC 地址。
HostName	string(64)	-	R	设备的主机名。如果未知则为空字符串。
InterfaceType	string	-	R	<p>主机连接到 CPE 使用的物理接口类型。枚举值：</p> <p>“Ethernet”</p> <p>“USB”</p> <p>“802.11”</p> <p>“HomePNA”</p> <p>“HomePlug”</p> <p>“Other”</p>
Active	boolean	-	R	<p>目前主机是否在 LAN 中。对存在状态的检测方法由 CPE 自己决定。</p> <p>列出不活动主机的能力是可选的。如果 CPE 在该包中包括不活动的主机，则不活动主机对应的本值必须设置为 0。不活动主机在本表中保留的时间由 CPE 自己决定。</p>
InternetGatewayDevice.WANDevice.{i}.	object	-	R	每个实例列出了与特定的物理 WAN 接口关联的所有对象。
WANConnectionNumberOfEntries	unsignedInt	-	R	在本 WANDevice 中 WANConnectionDevice 的数目。
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.	object	-	R	本对象是 WAN 接口所有连接实例共同属性的模型。
EnabledForInternet	boolean	R	R	在所有连接实例上启用或禁用 Internet 的双向访问。

名称 ¹⁰	类型	写 ¹¹	读	描述
WANAccessType	boolean	-	R	说明 WAN 访问 (modem) 类型。枚举值: “DSL” “Ethernet” “POTS”
Layer1UpstreamMaxBitRate	unsignedInt	-	R	说明 WAN 设备的最大上行位速率的理论值, 单位为 bps。
Layer1DownstreamMaxBitRate	unsignedInt	-	R	说明 WAN 设备的最大下行位速率的理论值, 单位为 bps。
PhysicalLinkStatus	string	-	R	说明从 WAN 设备到一个连接到的实体的物理连接 (链路) 状态。枚举值: “Up” “Down” “Initializing” “Unavailable”
WANAccessProvider	string(256)	-	O	在 WAN 上提供链路连接的服务提供商的名称。
TotalBytesSent	unsignedInt	-	R	在 WAN 设备上, 所有连接服务实例在上行方向所发送的字节总数。为累积计数器。
TotalBytesReceived	unsignedInt	-	R	在 WAN 设备上, 所有连接服务实例在下行方向所接收的字节总数。为累积计数器。
TotalPacketsSent	unsignedInt	-	R	在 WAN 设备上, 所有连接服务实例在上行方向所发送的分组 (IP 或 PPP) 总数。为累积计数器。
TotalPacketsReceived	unsignedInt	-	R	在 WAN 设备上, 所有连接服务实例在下行方向所接收的分组 (IP 或 PPP) 总数。为累积计数器。
MaximumActiveConnections	unsignedInt	-	O	说明 CPE 能够同时支持的活动连接的最大数目。
NumberOfActiveConnections	unsignedInt	-	O	在本 WAN 接口上目前活动的 WAN 连接服务实例的数目。
InternetGatewayDevice.WANDevice.{i}.WANCommonInterfaceConfig.Connection.{i}.	object	-	O	活动连接表。
ActiveConnectionDeviceContainer	string(256)	-	O	与本连接实例关联的 WAN 连接设备对象。内容是 WAN 连接设备的完整层次状参数名称。例如: “InternetGatewayDevice.WANDevice.1.WANConnectionDevice.2”。
ActiveConnectionServiceID	string(256)	-	O	说明与本连接实例关联的 WAN 连接对象。内容是三层连接对象的完整层次状参数名称, 例如: “InternetGatewayDevice.WANDevice.1.WANConnectionDevice.2.WANPPPPConnection.1”。
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.	object	-	C	本对象模型化针对 CPE 中使用 DSL modem 进行 Internet 访问的单个物理连接的物理层属性。这一对象对有 DSL modem WAN 接口的 CPE 是需要的。在一个给出的 WANDevice 实例中, 与其它 WAN*InterfaceConfig 对象互斥。
Enable	boolean	C	C	启用或禁用该链路。
Status	string	-	C	DSL 物理链路的状态。枚举值: “Up” “Initializing” “EstablishingLink” “NoSignal” “Error” “Disabled”

名称 ¹⁰	类型	写 ¹¹	读	描述
ModulationType	string	-	O	说明连接所用的调制类型。枚举值： “ADSL-G.dmt” “ADSL_Glite” “ADSL_G.dmt.bis” “ADSL_re-adsl” “ADSL_2plus” “ADSL_four” “ADSL_ANSI_T1.413” “G.shdsl” “IDSL” “HDSL” “SDSL” “VDSL”
LineEncoding	string	-	O	在 CPE 和 DSLAM 之间建立第一层的 DSL 连接时使用的线路编码方法。一般而言，该变量在供给后就不再更改。枚举值： “DMT” “CAP” “2B1Q” “43BT” “PAM” “QAM”
DataPath	string	-	O	说明数据路径是快速的（低延迟）不是隔行的（低错误率）。枚举值： “Interleaved” “Fast”
InterleaveDepth	unsignedInt	-	O	ADSL 隔行深度。该变量只有在 DataPath = Interleaved 时才使用。
LineNumber	int[1:]	-	O	表示 modem 用来连接的线路对。LineNumber = 1 表示最里面的线对。
UpstreamCurrRate	unsignedInt	-	C	上行 DSL 频道的当前有效负荷带宽（表示为 Kbps）。
DownstreamCurrRate	unsignedInt	-	C	下行 DSL 频道的当前有效负荷带宽（表示为 Kbps）。
UpstreamMaxRate	unsignedInt	-	C	上行 DSL 频道当前可达到的速率（表示为 Kbps）。
DownstreamMaxRate	unsignedInt	-	C	下行 DSL 频道当前可达到的速率（表示为 Kbps）。
UpstreamNoiseMargin	int	-	C	上行 DSL 连接的当前信噪比（表示为 0.1db）
DownstreamNoiseMargin	int	-	C	下行 DSL 连接的当前信噪比（表示为 0.1db）
UpstreamAttenuation	int	-	C	当前上行信号的衰减（表示为 0.1dB）
DownstreamAttenuation	int	-	C	当前下行信号的衰减（表示为 0.1dB）
UpstreamPower	int	-	C	当前 CPE 的 DSL 接口的输出功率（表示为 0.1 dBmV）
DownstreamPower	int	-	C	当前 CPE 的 DSL 接口的接收功率（表示为 0.1 dBmV）
ATURVendor	string(8)	-	C	在 G.994.1 和 T1.413 中定义的 ATU-R 厂商标识符。
ATURCountry	unsignedInt	-	C	在 G.994.1 中定义的 ATU-R 厂商的 T.35 国家代码。
ATURANSIStd	unsignedInt	-	O	在 T1.413 第二期中定义的 ATU-R 的 T1.413 的修订版本号。
ATURANSIRev	unsignedInt		-O	在 T1.413 第二期中定义的 ATU-R 的厂商修订版本号。
ATUCVendor	string(8)	-	C	在 G.994.1 和 T1.413 中定义的 ATU-C 厂商标识符。
ATUCCountry	unsignedInt	-	C	在 G.994.1 中定义的 ATU-C 厂商的 T.35 国家代码。
ATUCANSIStd	unsignedInt	-	O	在 T1.413 第二期中定义的 ATU-C 的 T1.413 的修订版本号。
ATUCANSIRev	unsignedInt		-O	在 T1.413 第二期中定义的 ATU-C 的厂商修订版本号。

名称 ¹⁰	类型	写 ¹¹	读	描述
TotalStart	unsignedInt	-	C	总体统计开始以来的秒数。 统计值在 CPE 重启后 应当 继续累积，即使这可能不总是可达到的。
ShowtimeStart	unsignedInt	-	C	最近DSL Showtime（用于统计Showtime ¹⁴ 值的开始时间）以来的秒数。
LastShowtimeStart	unsignedInt	-	O	最近的前一次 DSL Showtime（用于统计 LastShowtime 值的开始时间）以来的秒数。 如果 CPE 没有保留最近的前一次 Showtime，例如重启了，则 LastShowTime 的开始统计值 可以 暂时地与 Showtime 的开始统计值相同。
CurrentDayStart	unsignedInt	-	O	从开始统计 CurrentDay 值以来的秒数。 CPE 可以 按 UTC 时区的天来校正每个 CurrentDay 间距的开始，但这不是要求的。 统计值在 CPE 重启后 应当 继续累积，即使这可能不总是可达到的。
QuarterHourStart	unsignedInt	-	O	从开始统计 QuarterHour 值以来的秒数。 CPE 可以 按实时的十五分钟间隔来校正每个 QuarterHour 间距的开始，但这不是要求的。 统计值在 CPE 重启后 应当 继续累积，即使这可能不总是可达到的。
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.	object	-	C	本对象包括 WAN DSL 物接口的统计值。
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.Total.	object	-	C	本对象包括 DSL 的总统计值。
ReceiveBlocks	unsignedInt	-	C	成功接收块的总数目。
TransmitBlocks	unsignedInt	-	C	成功发送块的总数目。
CellDelin	unsignedInt	-	C	Cell-delineation 错误的总数（在 ITU-T Rec. G.997.1 中定义的 NCD 或 LCD 失效的总秒数）
LinkRetrain	unsignedInt	-	C	Link-retrain 错误的总数目（在 ITU-T Rec. G.997.1 中定义的完整初始化次数）。
InitErrors	unsignedInt	-	C	初始化错误的总数目（在 ITU-T Rec. G.997.1 中定义的 LINIT 失效）。
InitTimeouts	unsignedInt	-	C	初始化超时错误的总数目。
LossOfFraming	unsignedInt	-	C	Loss-of-framing 错误的总数目（在 ITU-T Rec. G.997.1 中定义的 LOF 失效）。
ErroredSecs	unsignedInt	-	C	错误的总秒数（在 ITU-T Rec. G.997.1 中定义的 ES-L）。
SeverelyErroredSecs	unsignedInt	-	C	严重错误的总秒数（在 ITU-T Rec. G.997.1 中定义的 SES-L）。
FECErrors	unsignedInt	-	C	检测到的 FEC 错误的总数目（在 ITU-T Rec. G.997.1 中定义的 FEC-C）。
ATUCFECErrors	unsignedInt	-	C	由 ATU-C 检测到的 FEC 错误的总数目（在 ITU-T Rec. G.997.1 中定义的 FEC-CFE）。
HECErrors	unsignedInt	-	C	检测到的 HEC 错误的总数（在 ITU-T Rec. G.997.1 中定义的 HEC-P）。
ATUCHECErrors	unsignedInt	-	C	由 ATU-C 检测到的 HEC 错误的总数（在 ITU-T Rec. G.997.1 中定义的 HEC-PFE）。

¹⁴ Showtime定义为DSL链路连接过程的成功结束。Showtime统计值是指自最近的DSL链路建立以来的所统计的值。

名称 ¹⁰	类型	写 ¹¹	读	描述
CRCErrors	unsignedInt	-	C	检测到的 CRC 错误的总数（在 ITU-T Rec. G.997.1 中定义的 CV-C）。
ATUCCRCErrors	unsignedInt	-	C	由 ATU-C 检测到的 CRC 错误的总数（在 ITU-T Rec. G.997.1 中定义的 CV-CFE）。
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.Showtime.	object	-	C	本对象包括自最近的 DSL Showtime 以来累积的 DSL 统计值。
ReceiveBlocks	unsignedInt	-	C	最近的 DSL Showtime 以来成功接收块的数目。
TransmitBlocks	unsignedInt	-	C	最近的 DSL Showtime 以来成功发送块的数目。
CellDelin	unsignedInt	-	C	最近的 DSL Showtime 以来 Cell-delineation 错误的数目（在 ITU-T Rec. G.997.1 中定义的 NCD 或 LCD 失效的秒数）。
LinkRetrain	unsignedInt	-	C	最近的 DSL Showtime 以来 Link-retrain 错误的数目（在 ITU-T Rec. G.997.1 中定义的完整初始化次数）。
InitErrors	unsignedInt	-	C	最近的 DSL Showtime 以来，初始化错误的数目（在 ITU-T Rec. G.997.1 中定义的 LINIT 失效）。
InitTimeouts	unsignedInt	-	C	最近的 DSL Showtime 以来，初始化超时错误的数目。
LossOfFraming	unsignedInt	-	C	最近的 DSL Showtime 以来，Loss-of-framing 错误的数目（在 ITU-T Rec. G.997.1 中定义的 LOF 失效）。
ErroredSecs	unsignedInt	-	C	最近的 DSL Showtime 以来，错误的秒数（在 ITU-T Rec. G.997.1 中定义的 ES-L）。
SeverelyErroredSecs	unsignedInt	-	C	最近的 DSL Showtime 以来，严重错误的秒数（在 ITU-T Rec. G.997.1 中定义的 SES-L）。
FECErrors	unsignedInt	-	C	最近的 DSL Showtime 以来，检测到的 FEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 FEC-C）。
ATUCFECErrors	unsignedInt	-	C	最近的 DSL Showtime 以来，由 ATU-C 检测到的 FEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 FEC-CFE）。
HECErrors	unsignedInt	-	C	最近的 DSL Showtime 以来，检测到的 HEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 HEC-P）。
ATUCHECErrors	unsignedInt	-	C	最近的 DSL Showtime 以来，由 ATU-C 检测到的 HEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 HEC-PFE）。
CRCErrors	unsignedInt	-	C	最近的 DSL Showtime 以来，检测到的 CRC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 CV-C）。
ATUCCRCErrors	unsignedInt	-	C	最近的 DSL Showtime 以来，由 ATU-C 检测到的 CRC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 CV-CFE）。
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.LastShowtime.	object	-	O	本对象包括自最近的第二次 DSL Showtime 以来，DSL 的累积统计值。
ReceiveBlocks	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，成功接收块的数目。
TransmitBlocks	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，成功发送块的数目。
CellDelin	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，Cell-delineation 错误的数目（在 ITU-T Rec. G.997.1 中定义的 NCD 或 LCD 失效的总秒数）。
LinkRetrain	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，Link-retrain 错误的数目（在 ITU-T Rec. G.997.1 中定义的完整初始化次数）。
InitErrors	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，初始化错误的数目（在 ITU-T Rec. G.997.1 中定义的 LINIT 失效）。

名称 ¹⁰	类型	写 ¹¹	读	描述
InitTimeouts	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，初始化超时错误的数目。
LossOfFraming	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，Loss-of-framing 错误的数目（在 ITU-T Rec. G.997.1 中定义的 LOF 失效）。
ErroredSecs	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，错误的秒数（在 ITU-T Rec. G.997.1 中定义的 ES-L）。
SeverelyErroredSecs	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，严重错误的秒数（在 ITU-T Rec. G.997.1 中定义的 SES-L）。
FECErrors	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，检测到的 FEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 FEC-C）。
ATUCFECErrors	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，由 ATU-C 检测到的 FEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 FEC-CFE）。
HECErrors	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，检测到的 HEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 HEC-P）。
ATUCHECErrors	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，由 ATU-C 检测到的 HEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 HEC-PFE）。
CRCErrors	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，检测到的 CRC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 CV-C）。
ATUCCRCErrors	unsignedInt	-	O	自最近的第二次 DSL Showtime 以来，由 ATU-C 检测到的 CRC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 CV-CFE）。
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.CurrentDay.	object	-	O	本对象包括在当天累积的 DSL 的统计值。
ReceiveBlocks	unsignedInt	-	O	在当天成功接收块的数目。
TransmitBlocks	unsignedInt	-	O	在当天成功发送块的数目。
CellDelin	unsignedInt	-	O	在当天 Cell-delineation 错误的数目（在 ITU-T Rec. G.997.1 中定义的 NCD 或 LCD 失效的秒数）。
LinkRetrain	unsignedInt	-	O	在当天 Link-retrain 错误的数目（在 ITU-T Rec. G.997.1 中定义的完整初始化次数）。
InitErrors	unsignedInt	-	O	在当天初始化错误的数目（在 ITU-T Rec. G.997.1 中定义的 LINIT 失效）。
InitTimeouts	unsignedInt	-	O	在当天初始化超时错误的数目。
LossOfFraming	unsignedInt	-	O	在当天 Loss-of-framing 错误的数目（在 ITU-T Rec. G.997.1 中定义的 LOF 失效）。
ErroredSecs	unsignedInt	-	O	在当天错误的秒数（在 ITU-T Rec. G.997.1 中定义的 ES-L）。
SeverelyErroredSecs	unsignedInt	-	O	在当天严重错误的秒数（在 ITU-T Rec. G.997.1 中定义的 SES-L）。
FECErrors	unsignedInt	-	O	在当天检测到的 FEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 FEC-C）。
ATUCFECErrors	unsignedInt	-	O	在当天由 ATU-C 检测到的 FEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 FEC-CFE）。
HECErrors	unsignedInt	-	O	在当天检测到的 HEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 HEC-P）。
ATUCHECErrors	unsignedInt	-	O	在当天由 ATU-C 检测到的 HEC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 HEC-PFE）。

名称 ¹⁰	类型	写 ¹¹	读	描述
CRCErrors	unsignedInt	-	O	在当天检测到的 CRC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 CV-C）。
ATUCCRCErrors	unsignedInt	-	O	在当天由 ATU-C 检测到的 CRC 错误的数目（在 ITU-T Rec. G.997.1 中定义的 CV-CFE）。
InternetGatewayDevice.WANDevice.{i}.WANDSLInterfaceConfig.Stats.QuarterHour.	object	-	O	本对象包括在当前 quarter hour 以来，累积的 DSL 的统计值。
ReceiveBlocks	unsignedInt	-	O	在当前 quarter hour 以来，成功接收块的总数目。
TransmitBlocks	unsignedInt	-	O	在当前 quarter hour 以来，成功发送块的总数目。
CellDelin	unsignedInt	-	O	在当前 quarter hour 以来，Cell-delineation 错误的总数（在 ITU-T Rec. G.997.1 中定义的 NCD 或 LCD 失效的总秒数）
LinkRetrain	unsignedInt	-	O	在当前 quarter hour 以来，Link-retrain 错误的总数目（在 ITU-T Rec. G.997.1 中定义的完整初始化次数）。
InitErrors	unsignedInt	-	O	在当前 quarter hour 以来，初始化错误的总数目（在 ITU-T Rec. G.997.1 中定义的 LINIT 失效）。
InitTimeouts	unsignedInt	-	O	在当前 quarter hour 以来，初始化超时错误的总数目。
LossOfFraming	unsignedInt	-	O	在当前 quarter hour 以来，Loss-of-framing 错误的总数目（在 ITU-T Rec. G.997.1 中定义的 LOF 失效）。
ErroredSecs	unsignedInt	-	O	在当前 quarter hour 以来，错误的总秒数（在 ITU-T Rec. G.997.1 中定义的 ES-L）。
SeverelyErroredSecs	unsignedInt	-	O	在当前 quarter hour 以来，严重错误的总秒数（在 ITU-T Rec. G.997.1 中定义的 SES-L）。
FECErrors	unsignedInt	-	O	在当前 quarter hour 以来，检测到的 FEC 错误的总数目（在 ITU-T Rec. G.997.1 中定义的 FEC-C）。
ATUCFECErrors	unsignedInt	-	O	在当前 quarter hour 以来，由 ATU-C 检测到的 FEC 错误的总数目（在 ITU-T Rec. G.997.1 中定义的 FEC-CFE）。
HECErrors	unsignedInt	-	O	在当前 quarter hour 以来，检测到的 HEC 错误的总数（在 ITU-T Rec. G.997.1 中定义的 HEC-P）。
ATUCHECErrors	unsignedInt	-	O	在当前 quarter hour 以来，由 ATU-C 检测到的 HEC 错误的总数（在 ITU-T Rec. G.997.1 中定义的 HEC-PFE）。
CRCErrors	unsignedInt	-	O	在当前 quarter hour 以来，检测到的 CRC 错误的总数（在 ITU-T Rec. G.997.1 中定义的 CV-C）。
ATUCCRCErrors	unsignedInt	-	O	在当前 quarter hour 以来，由 ATU-C 检测到的 CRC 错误的总数（在 ITU-T Rec. G.997.1 中定义的 CV-CFE）。
InternetGatewayDevice.WANDevice.{i}.WANEthernetInterfaceConfig.	object	-	C	CPE 用以太网物理连接来进行 Internet 访问时，本对象是该连接对应的物理层属性的模型。对有以太网 WAN 接口的 CPE 而言，该对象是要求实现的，并且对给定的 WANDevice 实例，该对象与其它 WAN*InterfaceConfig 对象互斥。注意，本对象与有时用到的 DSL 连接关联的以太网协议层 <u>无</u> 关系。
Enable	boolean	C	C	启用或禁用该接口。
Status	string	-	C	表明接口的状态。枚举值： “Up” “NoLink” “Error” “Disabled”
MACAddress	string	-	C	接口的物理地址。

名称 ¹⁰	类型	写 ¹¹	读	描述
MaxBitRate	string	C	C	该连接可用的最大上行和下行位速率。枚举值： “10” “100” “Auto”
DuplexMode	string	C	C	该连接使用的双工模式。枚举值： “Half” “Full” “Auto”
InternetGatewayDevice.WANDevice.{i}.WANEthernetInterfaceConfig.Stats.	object	-	C	本对象包含 CPE 设备上的以太网 WAN 接口的统计值。
BytesSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上发送的总字节数。
BytesReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上接收的总字节数。
PacketsSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上发送的总分组数。
PacketsReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，接口上接收的总分组数。
InternetGatewayDevice.WANDevice.{i}.WANDSLConnectionManagement.	object	-	C	具有 DSL modem WAN 接口的 CPE 要求有本对象。
ConnectionServiceNumberOfEntries	unsignedInt	-	R	ConnectionService 表中的条目数。
InternetGatewayDevice.WANDevice.{i}.WANDSLConnectionManagement.ConnectionService.{i}.	object	-	C	本表包含每个连接服务的一个条目。
WANConnectionDevice	string(256)	-	R	说明与该连接实例关联的 WAN 连接设备对象。其内容为 WAN 连接设备的完整层次状参数名。例如： “InternetGatewayDevice.WANDevice.1.WANConnectionDevice.2”。
WANConnectionService	string(256)	-	R	说明与该连接实例关联的 WAN 连接对象。其内容是三层连接对象的完整层次状参数名称。例如： “InternetGatewayDevice.WANDevice.1.WANConnectionDevice.2.WANPPPConnection.1”。
DestinationAddress	string(256)	-	R	WANConnectionDevice 条目的目标地址。下列值之一： PVC: VPI/VCI SVC: ATM 连接名称 SVC: ATM 地址
LinkType	string	-	R	WANConnectionDevice 条目的链路类型。取值为在 WANDSLLinkConfig 中描述的一个链路类型。
ConnectionType	string	-	R	WANPPPConnection 或 WANIPConnection 条目的连接类型。是在 WAN**Connection 服务中定义的一个 PossibleConnectionTypes。
Name	string(32)	-	-	用户可读的连接名称。
InternetGatewayDevice.WANDevice.{i}.WANDSL.Diagnostics.	object	-	C	对有 ADSL2 或 ADSL2+ modem WAN 接口的 CPE 设备，本对象是要求的。对其它 CPE 是可选的。
LoopDiagnosticsState	string	C	C	说明诊断数据的可用性。以下值之一： “None” “Requested” “Complete” 把值设置为 “Requested” 来发起诊断测试。在测试进行时，DSL 连接被断掉。当写此参数时，只允许写 “Requested” 值。 当由 ACS 发起的诊断结束后（不管成功还是失败），CPE 必须建立到 ACS 的新连接，允许 ACS 查看结果，并在 Inform 报文中指明相应的原因。
ACTPSDds	int	-	C	下行的实际功率频谱密度（PSD – Power spectral density）。对该值的解释见 ITU-T Rec. G.997.1 的定义。

名称 ¹⁰	类型	写 ¹¹	读	描述
ACTPSDs	int	-	C	上行的实际功率频谱密度（PSD – Power spectral density）。对该值的解释见 ITU-T Rec. G.997.1 的定义。
ACTATPds	int	-	C	下行的实际汇聚发射功率（ATP – Aggregate transmitter power）。对该值的解释见 ITU-T Rec. G.997.1 的定义。
ACTATPus	int	-	C	上行的实际汇聚发射功率（ATP – Aggregate transmitter power）。对该值的解释见 ITU-T Rec. G.997.1 的定义。
HLINSCds	int	-	C	下行线性表示量度（Linear representation scale）。对该值的解释见 ITU-T Rec. G.997.1 的定义。
HLINpsds	string	-	C	每一子载波的下行线性频道特性（Linear channel characteristics）。整数组成的，逗号分隔的列表。每一对后续整数代表每个复数的实数的虚数两部分。对 ADSL 和 ADSL2，复数偶的最大数字为 256，对 ADSL2+，则为 512。和下行线性对该值的解释见 ITU-T Rec. G.997.1 的定义。
QLNpsds	string	-	C	每一子载波的下行安静线路噪音（quiet line noise）。是整数组成的，逗号分隔的列表。对 ADSL 和 ADSL2，元素的最大数目为 256，而对 ADSL2+则为 512。对该值的解释见 ITU-T Rec. G.997.1 的定义。
BITSpds	string	-	C	每一子载波的下行位分配（bit allocation）。是整数组成的，逗号分隔的列表。对 ADSL 和 ADSL2，元素的最大数目为 256，而对 ADSL2+则为 512。对该值的解释见 ITU-T Rec. G.997.1 的定义。
GAINSpds	string	-	C	每一子载波的下行增益分配（gain allocation）。是整数组成的，逗号分隔的列表。对 ADSL 和 ADSL2，元素的最大数目为 256，而对 ADSL2+则为 512。对该值的解释见 ITU-T Rec. G.997.1 的定义。
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.	object	C	C	每一实例包含与给出的 WAN 链路关联的对象。在 DSL 情况下，每一实例对应单一一个 ATM VC。在建立 WANConnectionDevice 实例时，不包含初始的连接对象。
WANIPConnectionNumberOfEntries	unsignedInt	-	C	本 WANConnectionDevice 的 WANIPConnection 实例的数目。
WANPPPPConnectionNumberOfEntries	unsignedInt	-	C	本 WANConnectionDevice 的 WANPPPPConnection 实例的数目。
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANDSLLinkConfig.	object	-	C	CPE 进行 Internet 访问的 DSL modem 物理连接的 ATM 层特性模型。对有 DSL modem WAN 接口的 CPE，本对象是要求的，并且与给定的 WANConnectionDevice 实例的其它 WAN*LinkConfig 对象互斥。
Enable	boolean	C	C	启用或禁用链路。在建立 WANConnectionDevice 时，对象默认是禁用的。
LinkStatus	string	-	C	链路的状态。枚举值： “Up” “Down” “Initializing” “Unavailable”

名称 ¹⁰	类型	写 ¹¹	读	描述
LinkType	string	C	C	说明 DSL 连接的类型，指用于此连接的完成的协议栈。枚举值： “EoA”（RFC2684 bridged Ethernet over ATM） “IPoA”（RFC2684 routed IP over ATM） “PPPoA”（RFC2364 PPP over ATM） “PPPoE”（RFC2516 PPP over Ethernet on RFC2684 bridged Ethernet over ATM） “CIP”（RFC1577 Classical IP over ATM） “Unconfigured”
AutoConfig	boolean	-	C	说明 CPE 的该连接是否使用某些自动配置机制。如果该变量为 TRUE，该连接实例的所有可写变量变为只读。任何试图改变任何一个变量都应当失败，并返回一个错误。
ModulationType	string	-	O	指示这一连接关联的接口上使用的 DSL 调制类型（是 WANDSLInterfaceConfig 的副本）。枚举值： “ADSL_Gdmt” “ADSL_Glite” “ADSL_Gdmt.bis” “ADSL_re-adsl” “ADSL_2plus” “ADLS_four” “ADSL_ANSI_T1.413” “G.shdsl” “IDSL” “HDSL” “SDSL” “VDSL”
DestinationAddress	string(256)	C	C	该链路的目标地址。下列值之一： PVC: VPI/VCI SVC: ATM 连接名称 SVC: ATM 地址
ATMEncapsulation	string	O	O	说明要使用的连接封装。枚举值： “LLC” “VCMUX”
FCSPreserved	boolean	O	O	该标记说明是否在 ATM 的有效负荷中加入校验和。该值并不指一个 ATM 信元或 AALX 分组的校验和。在 LLC 和 VCMUX 封装下，该 ATM 校验和是指在 RFC1483 定义的 FCS 字段。仅适用于上行方向。
VCSearchList	string	O	O	当链路使用 DestinationAddress 不能建立时，要查找的 VPI/VCI 对的列表，以逗号分隔并有次序。格式： VPI1/VCI1,VPI2/VCI2,... 例： “0/35, 8/35, 1/35”
ATMAAL	string	-	O	描述目前 PVC 使用的 ATM 适应层（AAL）。枚举值： “AAL1” “AAL2” “AAL3” “AAL4” “AAL5”
ATMTransmittedBlocks	unsignedInt	-	C	当前成功传送的块数目。
ATMReceivedBlocks	unsignedInt	-	C	当前成功接收的块数目。

名称 ¹⁰	类型	写 ¹¹	读	描述
ATMQoS	string	O	O	描述了在虚电路（VC）上的 ATM 服务质量（QoS）。 枚举值： “UBR” “CBR” “GFR” “VBR-nrt” “VBR-rt” “UBR+” “ABR”
ATMPeakCellRate	unsignedInt	O	O	说明上行高峰信元速率，单位信元每秒。
ATMMaximumBurstSize	unsignedInt	O	O	说明上行最大突发信元大小。
ATMSustainableCellRate	unsignedInt	O	O	说明上行可维持的信元速率，单位信元每秒，用于流量的整形（traffic shaping）。
AAL5CRCErrors	unsignedInt	-	C	AAL5 层的循环冗余校验（CRC）错误的数目。
ATMCRCErrors	unsignedInt	-	C	ATM 层的循环冗余校验（CRC）错误的数目。
ATMHCEErrors	unsignedInt	-	O	ATM 层头错误校验（HEC）相关错误的数目。
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANATMF5LoopbackDiagnostics	object	-	O	该对象提供对 ATM 层的 F5 OAM 环回测试的访问。
DiagnosticsState	string	C	C	说明诊断数据的可用性。取下列值之一： “None” “Requested” “Complete” 把值设置为“Requested”来发起诊断测试。当写此参数时，只允许写“Requested”值。为了保证使用正确的测试参数（本对象的可写参数），测试参数必须在设置 DiagnosticState 值为 Requested 之前或同时设置（使用同一 SetParameterValues 方法）。 如果收到请求，CPE 应当等与 ACS 之间的通信会话结束后再开始诊断过程。 当由 ACS 发起的诊断结束后（不管成功还是失败），CPE 必须建立到 ACS 的新的连接，允许 ACS 查看结果，并在 Inform 报文中指明报文代码“8 DIAGNOSTICS COMPLETE”。
NumberOfRepetitions	unsignedInt[1:]	C	C	在报告结果前要重复多少次 ping 测试。
Timeout	unsignedInt[1:]	C	C	Ping 测试超时的微秒数。
SuccessCount	unsignedInt	-	C	结果参数，表明最近的 ping 测试中成功 ping 的次数（在超时前收到的成功的 ping 应答）。
FailureCount	unsignedInt	-	C	结果参数，表明在最近的 ping 测试中失败的 ping 次数。
AverageResponseTime	unsignedInt	-	C	结果参数，表明在最近的 ping 测试中，所有的成功 ping 应答所花费的平均应答时间（单位：毫秒）。如果没有成功应答，该值必须为零。
MinimumResponseTime	unsignedInt	-	C	结果参数，表明在最近的 ping 测试中，所有的成功 ping 应答所花费的最小应答时间（单位：毫秒）。如果没有成功应答，该值必须为零。
MaximumResponseTime	unsignedInt	-	C	结果参数，表明在最近的 ping 测试中，所有的成功 ping 应答所花费的最大应答时间（单位：毫秒）。如果没有成功应答，该值必须为零。

名称 ¹⁰	类型	写 ¹¹	读	描述
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANEthernetLinkConfig.	object	-	C	CPE进行Internet访问的物理连接的以太网链路层特性模型。对有以太网WAN接口的CPE，本对象是要求的，并且与给定的WANConnectionDevice实例的其它WAN*LinkConfig对象互斥。注意，该对象与DSL连接相关的有时使用的以太网协议层无关。
EthernetLinkStatus	string	-	C	以太网链路的状态。枚举值： “Up” “Down” “Unavailable”
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPOTSLinkConfig.	object	-	C	CPE 进行 Internet 访问的物理连接的 POTS 链路层特性模型。对有 POTS WAN 接口的 CPE，本对象是要求的，并且与给定的 WANConnectionDevice 实例的其它 WAN*LinkConfig 对象互斥。
Enable	boolean	C	C	启用或禁用链路。建立 WANConnectionDevice 时，该对象默认是禁用的。
LinkStatus	string	-	C	链路状态。枚举值： “Up” “Down” “Dialing” “Connecting” “Unavailable”
ISPPhoneNumber	string(64)	O	C	说明用分号(;)分隔的字符串列表。每个字符串代表连接到特定 ISP 的电话号码。电话号码的含义遵从 ITU-T E.164 规范。电话号码中数字之间的分隔符，如括号或连字符，会被 CPE 忽略。
ISPInfo	string(64)	O	C	标识 Internet 服务提供商 (ISP) 的信息。该字符串的格式由厂商自己定义。
LinkType	string	O	C	本变量说明用于拨号的 POTS 链路的类型，是枚举值： “PPP_Dialup”
NumberOfRetries	unsignedInt	O	C	在返回错误之前，CPE 应当尝试建立 Internet 连接的次数。
DelayBetweenRetries	unsignedInt	O	C	CPE 在建立新一次 Internet 连接尝试前应等待的秒数。
Fclass	string	-	O	说明 POTS modem 的能力，即它是否能处理数据 (0)，传真 (1, 2, 2.0)，语音 (8)，DSVD (80)。为下列枚举值的以逗号分隔的列表： “0” “1” “2” “2.0” “8” “80”
DataModulationSupported	string	-	O	数据目前使用的调制标准。枚举值： “V92” “V90” “V34” “V32bis” “V32”
DataProtocol	string	-	O	数据传输目前使用的协议标准。枚举值： “V42_LAPM” “V42_MNP4” “V14” “V80”

名称 ¹⁰	类型	写 ¹¹	读	描述
DataCompression	string	-	O	Modem 上使用的压缩技术。枚举值： “V42bis” “MNP5”
PlusVTRCommandSupported	boolean	-	O	数据和语音的全双工操作能力。
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}	object	R	R	该对象启用在 CPE 的 WAN 接口上 IP 连接的配置。对没有使用 PPP 寻址的 WANConnectionDevice，本对象是要求的。而且对象在使用 PPP 寻址的 WANConnectionDevice 上不得处于活动状态。
Enable	boolean	R	R	启用或禁用连接实例。在 WANIPConnection 实例建立时，它的初始值为禁用。
ConnectionStatus	string	-	R	目前连接的状态。枚举值： “Unconfigured” “Connecting” “Connected” “PendingDisconnect” “Disconnecting” “Disconnected”
PossibleConnectionTypes	string	-	R	逗号分隔的列表，表明本连接实例可能的连接类型。列表中的每一元素是下面枚举值之一： “Unconfigured” “IP_Routed” “IP_Bridged”
ConnectionType	string	R	R	说明连接实例的类型。枚举值： “Unconfigured” “IP_Routed” “IP_Bridged”
Name	string(256)	R	R	本连接的用户可读的名称。
Uptime	unsignedInt	-	R	本连接 up 的秒数。
LastConnectionError	string	-	R	最后一次建立连接尝试失败的原因。枚举值： “ERROR_NONE” “ERROR_COMMAND_ABORTED” “ERROR_NOT_ENABLED_FOR_INTERNET” “ERROR_USER_DISCONNECT” “ERROR_ISP_DISCONNECT” “ERROR_IDLE_DISCONNECT” “ERROR_FORCED_DISCONNECT” “ERROR_NO_CARRIER” “ERROR_IP_CONFIGURATION” “ERROR_UNKNOWN”
AutoDisconnectTime	unsignedInt	O	O	连接建立以来的秒数。到达该时间后，CPE 自动终止连接。该动作与连接是否在使用无关。零值（0）代表连接不会被自动终止。
IdleDisconnectTime	unsignedInt	O	O	空闲连接的时间（秒），如果到达该秒后，连接依旧空闲，则 CPE 会自动终止连接。零值（0）代表连接不会被自动终止。
WarnDisconnectDelay	unsignedInt	O	O	Status 保持在 PendingDisconnect 状态的时间（秒）。在该秒后，Status 会丢弃该连接，并转变为 Disconnecting。
RSIPAvailable	boolean	-	R	说明 Realm-specific IP (RSIP) 是 CPE 的可用特性。
NATEnabled	boolean	C	R	说明该连接是否启用了网络地址转换 (NAT)。如果 CPE 支持 NAT，该参数 必须 可写。

名称 ¹⁰	类型	写 ¹¹	读	描述
AddressingType	string	O	R	CPE 本连接的 WAN 端接口指定 IP 地址的方法。枚举值： “DHCP” “Static”
ExternalIPAddress	string	O	R	这是本连接 NAT 使用的外部 IP 地址。只有当 AddressingType 为 Static 时，该参数才可配置。
SubnetMask	string	O	R	WAN 接口的子网掩码。只有当 AddressingType 为 Static 时，该参数才可配置。
DefaultGateway	string	O	R	本连接默认网关的 IP 地址。只有当 AddressingType 为 Static 时，该参数才可配置。
DNSEnabled	boolean	O	R	是否设备应当通过该连接来试图查询一个 DNS 服务器。
DNSOverrideAllowed	boolean	O	R	是否手工设置的，非空的 DNS 地址，可以被从 WAN 获得的 DNS 条目覆盖。
DNSServers	string	O	R	本连接的 DNS 服务器的 IP 地址列表，用逗号分隔。对多于三个 DNS 服务器的支持是可选的。
MaxMTUSize	unsignedInt [1:1540]	O	O	来自 LAN 端设备的以太网帧的最大允许大小。
MACAddress	string	O	R	如果可应用，该值是 WANIPConnection 的物理地址。只有在 MACAddressOverride 存在并且值为 True 时才可配置。
MACAddressOverride	boolean	O	O	是否 MACAddress 参数的值可以被覆盖。如果为 false(0)，则使用 CPE 的默认值（或者恢复如果该值前面被覆盖过）。
ConnectionTrigger	string	R	R	建立 IP 连接的触发器。枚举值： “OnDemand” “AlwaysOn” “Manual”
RouteProtocolRx	string	R	R	定义使用的 Rx 协议。枚举值： “Off” “RIPv1”（可选） “RIPv2”（可选） “OSPF”（可选）
PortMappingNumberOfEntries	unsignedInt	-	R	端口映射条目的总数目。
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.PortMapping.{i}.	object	R	R	端口映射表。
PortMappingEnabled	boolean	R	R	启用或禁用端口映射实例。在建立时，默认是禁用的。
PortMappingLeaseDuration	unsignedInt	R	R	决定端口映射租约的以秒计的生存期。零值代表端口映射是静态的。静态端口映射并不一定意味着这些映射在设备重置或重启后还永久存在。
RemoteHost	string	R	R	本参数是内向（inbound）分组的源 IP 地址。空串表明“通配符”（在大多数情况下，该值都是一个通配符）。CPE 只要求支持通配符。 当 RemoteHost 是通配符时，所有发往网关 WAN 接口的 ExternalPort 的流量被转发给 InternalPort 的 InternalClient。 当 RemoteHost 是一个外网 IP 地址时，NAT 只转发从 RemoteHost 到 InternalClient 的内向分组，其它所有分组被丢弃。

名称 ¹⁰	类型	写 ¹¹	读	描述
ExternalPort	unsignedInt	R	R	NAT 网关侦听的连接请求的外部端口，对应 InternalPort。WAN 接口上连接该外部端口的内向分组应当转发给 InternalClient 的 InternalPort。 零（0）值代表通配符。如果值为通配符，则对所有外部端口（如果没有被其它条目映射）的连接请求将转发给 InternalClient。在通配符情况下，InternalClient 的 InternalPort 值将被忽略。
InternalPort	unsignedInt	R	R	InternalClient 上的端口号，网关应当将连接请求转发给它。零（0）值是不允许的。
PortMappingProtocol	string	R	R	端口映射的协议。枚举值： “TCP” “UDP”
InternalClient	string	R	R	LAN 上的内部客户端的 IP 地址或 DNS 主机名。 对 IP 地址的支持是必须的，对 DNS 主机名的支持是可选的。 该值不能是空串。 必须提供将 InternalClient 的值设置为广播 IP 地址 255.255.255.255 的可能，这将使多个 NAT 客户端同时使用同一个知名（well-known）端口。
PortMappingDescription	string(256)	R	R	用户可读的该端口映射的描述。
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANIPConnection.{i}.Stats.	object	-	C	本对象包含共享相同 MAC 地址的同一 WANConnectionDevice 的所有连接的统计。每个这样连接的本对象值应当等同。 对所有在接口上支持以太网层的（如 PPPoE, IPoE）WANConnectionDevice，本对象是要求的。
EthernetBytesSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，在共享相同 MAC 地址的同一 WANConnectionDevice 的所有连接上发送的总字节数。
EthernetBytesReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，在共享相同 MAC 地址的同一 WANConnectionDevice 的所有连接上接收的总字节数。
EthernetPacketsSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，在共享相同 MAC 地址的同一 WANConnectionDevice 的所有连接上发送的以太网分组总数。
EthernetPacketsReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，在共享相同 MAC 地址的同一 WANConnectionDevice 的所有连接上接收的以太网分组总数。
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPOConnection.{i}.	object			该对象启用在 CPE 的 WAN 接口上 PPP 连接的配置。对使用 PPP 寻址的所有 WANConnectionDevice，本对象是要求的。并且对象在不使用 PPP 寻址的 WANConnectionDevice 上不得处于活动状态。
Enable	boolean	R	R	启用或禁用连接实例。在 WANPPPOConnection 实例建立时，它的初始值为禁用。
ConnectionStatus	string	-	R	目前连接的状态。枚举值： “Unconfigured” “Connecting” “Authenticating” “Connected” “PendingDisconnect” “Disconnecting” “Disconnected”

名称 ¹⁰	类型	写 ¹¹	读	描述
PossibleConnectionTypes	string	-	R	逗号分隔的列表，表明本连接实例可能的连接类型。列表中的每一元素是下面枚举值之一： “Unconfigured” “IP_Routed” “DHCP_Spoofed” “PPPoE_Bridged” “PPPoE_Relay” “PPTP_Relay” “L2TP_Relay”
ConnectionType	string	R	R	说明连接实例的类型。枚举值： “Unconfigured” “IP_Routed” “DHCP_Spoofed” “PPPoE_Bridged” “PPPoE_Relay” “PPTP_Relay” “L2TP_Relay”
Name	string(256)	R	R	本连接的用户可读的名称。
Uptime	unsignedInt	-	R	本连接 up 的秒数。
LastConnectionError	string	-	R	最后一次建立连接尝试失败的原因。枚举值： “ERROR_NONE” “ERROR_ISP_TIME_OUT” “ERROR_COMMAND_ABORTED” “ERROR_NOT_ENABLED_FOR_INTERNET” “ERROR_BAD_PHONE_NUMBER” “ERROR_USER_DISCONNECT” “ERROR_ISP_DISCONNECT” “ERROR_IDLE_DISCONNECT” “ERROR_FORCED_DISCONNECT” “ERROR_SERVER_OUT_OF_RESOURCES” “ERROR_RESTRICTED_LOGON_HOURS” “ERROR_ACCOUNT_DISABLED” “ERROR_ACCOUNT_EXPIRED” “ERROR_PASSWORD_EXPIRED” “ERROR_AUTHENTICATION_FAILURE” “ERROR_NO_DIALTONE” “ERROR_NO_CARRIER” “ERROR_NO_ANSWER” “ERROR_LINE_BUSY” “ERROR_UNSUPPORTED_BITSPERSECOND” “ERROR_TOO_MANY_LINE_ERRORS” “ERROR_IP_CONFIGURATION” “ERROR_UNKNOWN”
AutoDisconnectTime	unsignedInt	O	O	连接建立以来的秒数。到达该时间后，CPE 自动终止连接。该动作与连接是否在使用无关。零值（0）代表连接不会被自动终止。
IdleDisconnectTime	unsignedInt	O	O	空闲连接的时间（秒），如果到达该秒后，连接依旧空闲，则 CPE 会自动终止连接。零值（0）代表连接不会被自动终止。
WarnDisconnectDelay	unsignedInt	O	O	Status 保持在 PendingDisconnect 状态的时间（秒）。在该秒后，会丢弃该连接，并转变 Status 为 Disconnecting。
RSIPAvailable	boolean	-	R	说明 Realm-specific IP (RSIP)是 CPE 的可用特性。

名称 ¹⁰	类型	写 ¹¹	读	描述
NATEnabled	boolean	C	R	说明该连接是否启用了网络地址转换（NAT）。如果 CPE 支持 NAT，该参数 必须 可写。
Username	string(64)	R	R	认证时使用的用户名。
Password	string(64)	R	-	认证时使用的密码。 当被读取时，不管实际值如何，该参数返回空字符串。
PPPEncryptionProtocol	string	-	O	描述在 WAN 设备和 ISP POP 之间使用的 PPP 加密协议。枚举值： “None” “MPPE”
PPPEncryptionProtocol	string	-	O	描述在 WAN 设备和 ISP POP 之间使用的 PPP 压缩协议。枚举值： “None” “Van Jacobsen” “STAC LZS”
PPPAuthenticationProtocol	string	-	O	描述在 WAN 设备和 ISP POP 之间使用的 PPP 认证协议。枚举值： “PAP” “CHAP” “MS-CHAP”
ExternalIPAddress	string	-	R	为该连接 NAT 所使用的外部 IP 地址。
RemoteIPAddress	string	-	O	这一连接的远端 IP 地址。
MaxMRUSize	unsignedInt [1:1540]	O	O	从远端对等体发过来帧的最大允许大小。
CurrentMRUSize	unsignedInt [1:1540]	-	O	在本连接上使用的当前 MRU。
DNSEnabled	boolean	O	R	是否设备应当通过该连接来试图查询一个 DNS 服务器。
DNSOverrideAllowed	boolean	O	R	是否手工设置的，非空的 DNS 地址，可以被从 WAN 获得的 DNS 条目覆盖。
DNSServers	string	O	R	本连接的 DNS 服务器的 IP 地址列表，用逗号分隔。对多于三个 DNS 服务器的支持是可选的。
MACAddress	string	O	R	如果可应用，该值是 WANIPConnection 的物理地址。只有在 MACAddressOverride 存在并且值为 True 时才可配置。
MACAddressOverride	boolean	O	O	是否 MACAddress 参数的值可以被覆盖。如果为 false(0)，则使用 CPE 的默认值（或者恢复如果该值前面被覆盖过）。
TransportType	string	-	R	连接的 PPP 传输类型。枚举值： “PPPoA” “PPPoE” “L2TP”（留作未来使用） “PPTP”（留作未来使用）
PPPoEACName	string(256)	R	R	PPPoE 的访问集中器（Access Concentrator）。
PPPoEServiceName	string(256)	R	R	PPPoE 的服务名。
ConnectionTrigger	string	R	R	建立 IP 连接的触发器。枚举值： “OnDemand” “AlwaysOn” “Manual”

名称 ¹⁰	类型	写 ¹¹	读	描述
RouteProtocolRx	string	R	R	定义使用的 Rx 协议。枚举值： “Off” “RIPv1”（可选） “RIPv2”（可选） “OSPF”（可选）
PPPLCP Echo	unsignedInt	-	O	PPP LCP Echo 的周期（秒）
PPPLCP EchoRetry	unsignedInt	-	O	在同一个 Echo 周期内重试 PPP LCP Echo 的次数。
PortMappingNumberOfEntries	unsignedInt	-	R	端口映射表的总条目数。
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPPConnection.{i}.PortMapping.{i}.	object	R	R	端口映射表。
PortMappingEnabled	boolean	R	R	启用或禁用端口映射实例。在建立时，默认是禁用的。
PortMappingLeaseDuration	unsignedInt	R	R	决定端口映射租约的以秒计的生存期。零值代表端口映射是静态的。静态端口映射并不一定意味着这些映射在设备重置或重启后还永久存在。
RemoteHost	string	R	R	本参数是内向（inbound）分组的源 IP 地址。空串表明“通配符”（在大多数情况下，该值都是一个通配符）。CPE 只要求支持通配符。 当 RemoteHost 是通配符时，所有发往网关 WAN 接口的 ExternalPort 的流量被转发给 InternalPort 的 InternalClient。 当 RemoteHost 是一个外网 IP 地址时，NAT 只转发从 RemoteHost 到 InternalClient 的内向分组，其它所有分组被丢弃。
ExternalPort	unsignedInt	R	R	NAT 网关侦听的连接请求的外部端口，对应到 InternalPort。WAN 接口上连接该外部端口的内向分组应当转发给 InternalClient 的 InternalPort。 零（0）值代表通配符。如果值为通配符，则对所有外部端口（如果没有被其它条目映射）的连接请求将转发给 InternalClient。在通配符情况下，InternalClient 的 InternalPort 值将被忽略。
InternalPort	unsignedInt	R	R	InternalClient 上的端口号，网关应当将连接请求转发给它。零（0）值是不允许的。
PortMappingProtocol	string	R	R	端口映射的协议。枚举值： “TCP” “UDP”
InternalClient	string	R	R	LAN 上的内部客户端的 IP 地址或 DNS 主机名。 对 IP 地址的支持是必须的，对 DNS 主机名的支持是可选的。 该值不能是空串。 必须提供将 InternalClient 的值设置为广播 IP 地址 255.255.255.255 的可能，这将使多个 NAT 客户端同时使用同一个知名（well-known）端口。
PortMappingDescription	string(256)	R	R	用户可读的该端口映射的描述。
InternetGatewayDevice.WANDevice.{i}.WANConnectionDevice.{i}.WANPPPPConnection.{i}.Stats.	object	-	C	本对象包含共享相同 MAC 地址的同一 WANConnectionDevice 的所有连接的统计。每个这样连接的本对象值应当等同。 对所有在接口上支持以太网层的（如 PPPoE, IPoE）WANConnectionDevice，本对象是要求的。
EthernetBytesSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，在共享相同 MAC 地址的同一 WANConnectionDevice 的所有连接上发送的总字节数。

名称 ¹⁰	类型	写 ¹¹	读	描述
EthernetBytesReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，在共享相同 MAC 地址的同一 WANConnectionDevice 的所有连接上接收的总字节数。
EthernetPacketsSent	unsignedInt	-	C	自 CPE 最后一次 reset 以来，在共享相同 MAC 地址的同一 WANConnectionDevice 的所有连接上发送的以太网分组总数。
EthernetPacketsReceived	unsignedInt	-	C	自 CPE 最后一次 reset 以来，在共享相同 MAC 地址的同一 WANConnectionDevice 的所有连接上接收的以太网分组总数。

附录 C. 签名凭据

C.1 概述

CPE WAN 管理协议定义了一个可选的机制，来安全地启用或禁用可选的 CPE 功能。与参数不同，凭据机制对需要安全追踪（比如与支持相关）的可选功能，提供更多一层的安全保护。

凭据是指一个数字签署的数据结构，可以指示 CPE 启用或禁用一个选项集。选项是指任何 CPE 可选的功能。当选项启用时，凭据可以说明一些特性，以决定在什么条件下选项可以存在。

C.2 使用凭据控制选项

选项可以被禁用、启用或者在限期内启用。对启用并没有规定期限的选项将一直为启用状态，直至服务器明确地禁用它。对启用且规定了期限的选项将仅在凭据指定的期间段内保持启用。过了指定的期限，CPE 必须自己禁用该选项。

选项可以定义为可传递或不可传递。除非特别指明，由凭据启用的选项是不可传递的。对不可传递的选项，当 CPE 与一个与该选项启用时不同的宽带服务提供商关联时，它会被自动禁用。可传递的选项是指不管服务提供商怎样变化，CPE 总是维护该选项。

每个凭据，可能包含启用或禁用一个或多个选项的指令，必须使用 [XML-Signature](#) 格式[13]来进行数字签署。在应用凭据的指令前，CPE 必须验证签名，并认证签署者。

凭据是针对特定 CPE，并且不能用于其它的非凭据中指定的 CPE。这就保证了用于分发凭据的机制，能够被用来确保只有那些已经正确指定选项的 CPE 才能启用该选项。

支持使用凭据的 CPE 必须支持网络时间的同步协议比如 NTP 或 SNTP，来确保精确使用时间和日期信息。只有在设置网络时间后，CPE 才能对接收到的凭据进行应用，或者将已存在的凭据与它的过期时间进行比较。

下面是与凭据相关的方法，在本规范的附录 A 中定义。

- **SetVouchers:** 允许服务器下载凭据列表给 CPE。每个凭据可以启用或禁用该凭据定义的选项。
- **GetOptions:** 允许服务器询问 CPE 支持的一个或所有选项的状态。

C.3 凭据定义

RPC 方法 SetVouchers 允许服务器启用，禁用或修改一个或多个选项的状态。SetVouchers 方法可以使用一个凭据数组作为参数。数组中的每个凭据都是单独用 Base64 编码的。

在使用Base64 编码前，每个**凭据**都是一个使用XML-Signature格式[13]签署过的XML结构。每个独立的签名**凭据**都可以包括一个或多个**选项说明**。每个**选项说明**是一个说明指定**选项**的预期状态的结构。

选项说明的元素在表 62 中定义。**选项**可以包含与该特定**选项**相关的其它 XML 元素。图 5 中显示了一个**选项说明**结构的例子。图 6 中显示了一个完整的签名**凭据**的例子。在该例子，在同一个**凭据**中启用了两个不同的**选项**。

表 62 – 选项说明定义

名称	类型	描述
VSerialNum	string(64)	标识特定 凭据 的唯一序列号。对给定的 ACS，创建的新 凭据 都必须指定一个单独的 凭据 序列号。该值在该 ACS 管理的所有 CPE 中必须唯一，并且对指定的 CPE，对不同时间的所有凭据也必须唯一。
DeviceId	DeviceIdStruct	用于唯一地标识一个需要应用 凭据 的特定 CPE 的结构。这一结构在表 63 中定义。 在接收到一个 凭据 后，CPE 必须确保在 DeviceId 中的信息与自己实际身份相符。如果不相符，CPE 必须忽略该 凭据 并应答一个请求被拒绝（Request Denied）的错误。
OptionIdent	string(64)	标识要启用或禁用的特定 选项 的名称。
OptionDesc	string(256)	选项 的文字描述。
StartDate	dateTime	可选元素。 选项 需要启用的日期和时间（UTC）。仅在 Mode = EnableWithExpiration 或者 Mode = EnableWithoutExpiration 时有用。如果该元素不存在，或所指定的时间已经过去，需要启用的 选项 被立即启用。
Duration	unsignedInt	在 Mode = EnableWithExpiration 时需要。对有期限的 选项 ，本元素指定 选项 以 DurationUnits 为单位的保持启用状态的期限。如果已经说明了 StartDate，则该期限相对于该起始日期。
DurationUnits	string	在 Mode = EnableWithExpiration 时需要。本元素指定 Duration 元素使用的单位。允许值为： “Days” “Months”
Mode	string	本元素说明指定的 选项 是要被启用还禁用，已经如果是启用，是否需要期限。允许值为： “Disable” “EnableWithExpiration” “EnableWithoutExpiration”
Transferable	boolean	可选元素。值 true(1)表示该 选项 是可传递的，即该选项在指定的期限日期到达前保持启用，而不管期间服务提供商做何变动。 如果该元素的值为 false(0)或不存在，表示 选项 是不可传递的。需要选项在服务提供商变化时（与附录 B 中定义的 ProvisioningCode 的任何变动相关）立即禁用。

表 63 – DeviceIdStruct 定义

名称	类型	描述
Manufacturer	string(64)	设备的制造商。本参数仅用于显示，不需要作为验证的一部分进行检查。

名称	类型	描述
OUI	string(6)	设备制造商的组织唯一标识。表示为六位十六进制的值，全部使用大写字母，并包含任何前置零。该值必须为[9]中定义的有效 OUI。
ProductClass	string(64)	产品序列号应用的产品类别标志。即，对给定的制造商，这一参数用标识产品或产品类别，在其中，产品序列号参数是唯一的。
SerialNumber	string(64)	特定设备的标识，在指定的产品类别和制造商条件下是唯一的。

图 5 – 选项说明的例子

```
<dsig:Object xmlns="" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
              Id="option0">
  <Option>
    <VSerialNum>987654321</VSerialNum>
    <DeviceId>
      <Manufacturer>2Wire</Manufacturer>
      <OUI>00D09E</OUI>
      <ProductClass>Gateway</ProductClass>
      <SerialNumber>123456789</SerialNumber>
    </DeviceId>
    <OptionIdent>Option Name</OptionIdent>
    <OptionDesc>Option Description</OptionDesc>
    <StartDate>20021025T12:06:34</StartDate>
    <Duration>280</Duration>
    <DurationUnits>Days</DurationUnits>
    <Mode>EnableWithExpiration</Mode>
  </Option>
</dsig:Object>
```

图 6 – 签名凭据的例子

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
      c14n-20010315"></CanonicalizationMethod>
    <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#
      dsasha1"></SignatureMethod>
    <Reference URI="#option0">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
          20010315"></Transform>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
        </DigestMethod>
      <DigestValue>TUuSqr2utLtQM5tY2DB1jL3nV00=</DigestValue>
    </Reference>
    <Reference URI="#option1">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
          20010315"></Transform>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
        </DigestMethod>
      <DigestValue>/YX1C/E6zNf0+w4lG66NeXGOQB0=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>
    KAMfQOSnmGH52qRVGLNFEEM4PPkRSmMUGr2D8E3vwwW280e1Bn5pwQ==
  </SignatureValue>
  <KeyInfo>
    <KeyValue>
      <DSAKeyValue>
        <P>
          /X9TgR11EilS30qcLuzk5/YRt1I870QAwX4/gLZRJmlFXUaiUftZPY1Y+r/F9
          bow9subVWzXgTuAHTRv8mZgt2uZUKWkn5/oBHsQIsJPu
          6nX/rfGG/g7V+fGqKYVDwT7g/bTxR7DAjVUE1oWkTL2d
          fOuK2HXKu/yIgMZndFIAcc=
        </P>
        <Q>l2BQjxUjC8yykrmCouuEC/BYHPU=</Q>
      </DSAKeyValue>
    </KeyValue>
  </KeyInfo>
</Signature>
```

```

9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCBg
LRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KouHiuzp
nWRbqN/C/ohNWLx+2J6ASQ7zKTxvqhRkImog9/hWuWfB
pKLZl6Ae1U1ZAFMO/7PSSo=

</G>
<Y>
TBASA/mjLI8bc2KM7u9X6nHHvjmgPgZtTBhr1/Fzs2AkDYCYMwy+v+OXU7u5e
18JuKG7/uolVhjXNSn6ZgObF+wuMoyP/OUmNbSkdN1aR
XXHPRsW2CcG3vjfV+Csg/LP3zfDxDkImSc8LuKXht/g4
+nksA/3icRQXWagQU9pUQ=

</Y>
</DSAKeyValue>
</KeyValue>
<X509Data>
  <X509IssuerSerial>
    <X509IssuerName>
      EMAILADDRESS=name@2wire.com, CN=2Wire, OU=CMS, O=2Wire, L=San\20
      Jose, ST=California, C=US
    </X509IssuerName>
    <X509SerialNumber>4</X509SerialNumber>
  </X509IssuerSerial>
  <X509SubjectName>
    CN=eng.bba.certs.2wire.com, OU=CMS, O=2Wire, L=San\20Jose, ST=CA,
    C=US
  </X509SubjectName>
  <X509Certificate>
MIIEUjCCA7uqAwIBAgIBBDANBgkqhkiG9w0BAQUFADCBhDELMakGA1UEBhMCVVMxEzARBgNVBAgT
CkNhbGlmb3JuaWEeXETAPBgNVBACtCFNhb1BKB3N1MQ4wDAYDVQQKEwUyV2lyZTEMMaGA1UECxDMD
Q01TMQ4wDAYDVQQDEwUyV2lyZTEfMB0GCSqGSIb3DQEJARYQZWJyb3duQDQ3aXJlLmNvbTAeFw0w
MjA5MDUyMDU4MTZaFw0xMjA5MDUyMDU4MTZaMG0xCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJQTER
MA8GA1UEBjMIU2FuIEpvcm2UxZjAMBgNVBAoTBtJXaXJlMQwwCgYDVQQLEwNDTVMxIDAeBgNVBAMT
F2VuZy5iYmEuY2VydHMuMndpcmUuY29tMIIIBtZCCASwGBYqGSM44BAEwggEfAoGBAP1/U4EddRIp
Ut9KnC7s5Of2EbdSP09EAMMeP4C2USZpRV1AILH7WT2NWPq/xfW6MPbLm1Vs14E7gB00b/JmYLdr
mVClpJ+f6AR7ECLCT7up1/63xhv401fnxqimFQ8E+4P208UewI1VBNAFpEy9nXzrithlyrv8iID
GZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC
+VdMCz0HgmdRWVeOutRZT+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KouHiuzpnWR
bqN/C/ohNWLx+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1U1ZAFMO/7PSSoDgYQAAoGATBAS
A/mjLI8bc2KM7u9X6nHHvjmgPgZtTBhr1/Fzs2AkDYCYMwy+v+OXU7u5e18JuKG7/uolVhjXNSn6
ZgObF+wuMoyP/OUmNbSkdN1aRXXHPRsW2CcG3vjfV+Csg/LP3zfDxDkImSc8LuKXht/g4+nksA/3
icRQXWagQU9pUSjgdAwgc0wHQYDVR0OBByEFMTl/ebdHLjaEoSS1PcLCAdFX32qMIGbBgNVHSME
gZMwgZChgYqkgYcwqYQxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwplDYWxpZm9ybmlhMREwDwYDVQ
HhEwTYW4gSm9zZTEOMAwGA1UEChMFMTdpdmUxDDAKBgNVBASTA0NNUzEOMAwGA1UEAxMFMTdpdmUx
HzAdBgkqhkiG9w0BCQEWEGvicm93bkAyd2lyZS5jb22CAQAwDgYDVR0PAQH/BAQDAgeAMA0GCSqG
SIb3DQEBBQUAA4GBAF1PGAByyvA0p+6o7nXfF3jzAdoHdaZh55C8sOQ9J62IF8D1j16JxR7pjcCp2
iYmWkqQMncGfq+X8xP7BIqntDmIlYXuDTlXbyxXsu6lnT7nCbjWmwlLOxFwN+Axy7BM3NkAFB5Mb
aaoJWtmD1QrvCAfFdhLeBT+tIRueK7Pq9LDS
  </X509Certificate>
  <X509Certificate>
MIICeTCAeICAQAwDQYJKoZIhvcNAQEEBQAwgYQxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwplDYWxp
Zm9ybmlhMREwDwYDVQHEwhtYW4gSm9zZTEOMAwGA1UEChMFMTdpdmUxDDAKBgNVBASTA0NNUzEOM
AwGA1UEAxMFMTdpdmUxHzAdBgkqhkiG9w0BCQEWEGvicm93bkAyd2lyZS5jb20wHhcNMDEwNzMx
MDMwNjQ5W5hcnMDcwMTIxMDMwNjQ5W5wCBhDELMakGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3Jua
WEeXETAPBgNVBACtCFNhb1BKB3N1MQ4wDAYDVQQKEwUyV2lyZTEMMaGA1UECxDMDQ01TMQ4wDAYD
VQQDEwUyV2lyZTEfMB0GCSqGSIb3DQEJARYQZWJyb3duQDQ3aXJlLmNvbTcBbnZANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA1ISJbL6i0J/6SBoet3aA8fki8s7pb/QUZueWj+0YKoDaQWh4MUCT0K06
N/0Z2cLMVg8JyezEpdnh3lVM/Ni5ow2Mst4dpdcccQEHOuqwnUWIBFU196/LPRyLj0m2NeIXSKMj
AdPwvcenxmgeVBr/ZUmr4JQpdSI2AZJuHvCIjUsCAWEAATANBgkqhkiG9w0BAQQFAAOBqQBa3CCX
ga9L0qrGWxpNj312Az+tYz8bpEp2e2pAvrJHdW/CJ0uRlE341oTkhfYFa5CuieF7Jcwf1B3+cGo
JrLWqeKqsNnrBmMFC/9hnrLlGZKEKi0POaGSFS/Pw9nodGWFZCiaQmeG+J6CWeASiFmdwgrGvESW
axfzzIKiXsXwKA==
  </X509Certificate>
</X509Data>
</KeyInfo>
<dsig:Object xmlns="" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
  Id="option0">
  <Option>
    <VSerialNum>987654321</VSerialNum>
    <DeviceId>
      <Manufacturer>2Wire</Manufacturer>
      <OUI>00D09E</OUI>
      <ProductClass>Gateway</ProductClass>
      <SerialNumber>123456789</SerialNumber>
    </DeviceId>
    <OptionIdent>First option name</OptionIdent>
    <OptionDesc>First option description</OptionDesc>
    <StartDate>20021025T12:06:34</StartDate>
    <Duration>280</Duration>
  </Option>

```

```
<DurationUnits>Days</DurationUnits>
<Mode>EnableWithExpiration</Mode>
</Option>
</dsig:Object>
<dsig:Object xmlns="" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
              Id="option1">
  <Option>
    <VSSerialNum>987654322</VSSerialNum>
    <DeviceId>
      <Manufacturer>2Wire</Manufacturer>
      <OUI>00D09E</OUI>
      <ProductClass>Gateway</ProductClass>
      <SerialNumber>123456789</SerialNumber>
    </DeviceId>
    <OptionIdent>Second option name</OptionIdent>
    <OptionDesc>Second option description</OptionDesc>
    <StartDate>20021025T12:06:34</StartDate>
    <Duration>280</Duration>
    <DurationUnits>Days</DurationUnits>
    <Mode>EnableWithExpiration</Mode>
  </Option>
</dsig:Object>
</Signature>
```


附录 D. Web 身份管理

D.1 概述

为了支持通过 CPE 本地网络的浏览器来访问局端 WEB 站点的基于 WEB 的应用程序，或其它与 CPE 相关的网页，CPE WAN 管理协议提供可选的机制，用来允许这类 WEB 站点根据与 CPE 关联的客户的确切信息来定制其网页内容。也就是说，在 CPE 所在 LAN 内进行浏览能够不需任何手动登录过程而自动完成认证。

协议定义了可选接口集合，允许 WEB 站点发起 CPE 和 ACS 之间的通信，使该 WEB 站点能够通过与 ACS 的通信，来识别用户在哪个 CPE 之后进行操作。这就允许 WEB 站点根据关联的宽带账号，CPE 的类型，以及 ACS 知道的其它特性来定制其网页内容。

注——这一识别机制不区分在一台 CPE 后面相同网络上的不同用户。在需要识别特定用户的情况下，需要使用其它不同的身份管理机制，如手动登录。

D.2 使用 Kicked PRC 方法

CPE WAN 管理协议在附录 A 中定义了可选的 Kicked RPC 方法，可以用于支持 WEB 身份认证功能。

CPE 对 Kicked 方法的调用源于 CPE 外部的激发源。这一外部激发源是基于 WEB 的，因此相关的方法提供了基于 WEB 事务的有用通信手段。D.4 节给出了对激发源接口的建议定义。

在 Kicked 方法调用中包含的信息包括需要唯一地识别该 CPE 的信息，也包括可以将该方法调用与特定 WEB 浏览会话关联的参数。

服务器通过对 Kicked 方法的应答将用户的浏览器重定向到一个指定的 URL。该 URL 可以包含 CGI 参数，允许服务器继续跟踪该浏览会话。

D.3 Web 身份管理过程

Web 身份管理机制基于 WEB 服务器与 ACS 关联并通信的模型。任何时候当 WEB 服务器希望识别用户的 CPE，或者为某种目的而让 CPE 建立与 ACS 的连接，会使用下列的事件序列（在正常情况下）：

1. 用户的浏览器访问一个 WEB 页面，要求获知用户 CPE 的信息，或者与之通信。
2. WEB 站点将浏览器重定向到一个指定的 URL，只有 CPE 的私网（LAN）接口才能访问这一 URL。通过浏览器“踢（kicks）”CPE，通过 CGI 参数提供给 CPE 在需要执行后续步骤时所需的信息（见 D.4 节）。
3. CPE 通过附录 A 中定义的 Kicked RPC 方法调用来通知 ACS 它被踢了。在该方法调用中，CPE 标识自己，并将唯一地标识该浏览器会话的信息传送给 ACS。
4. ACS 应答这一方法调用，并返回 CPE 应当将用户的浏览器重定向到的 URL。URL 通常包含 CGI 参数来说明会话状态。当连接打开时，ACS 可以

发起任何其它适合的 PRC 事务。

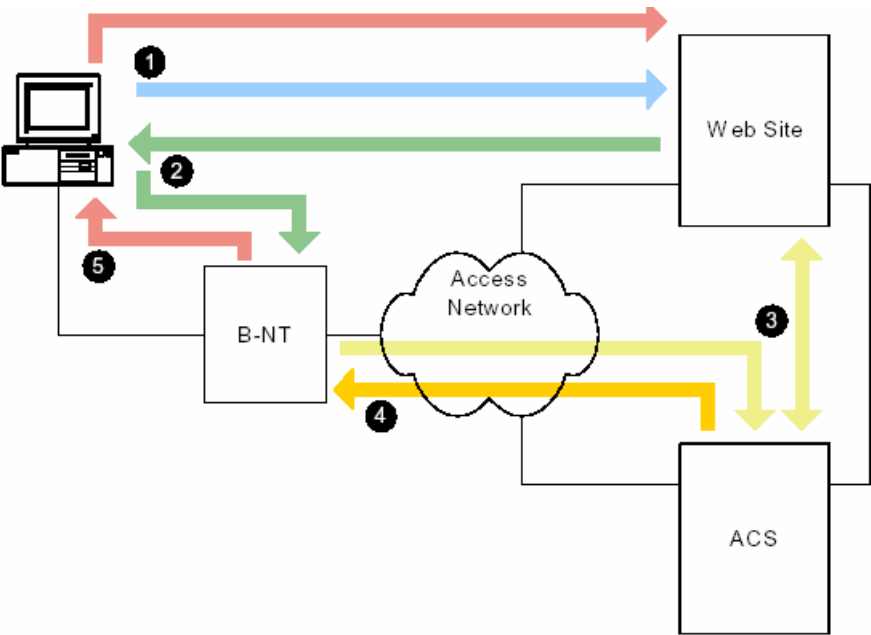
5. CPE 回复浏览器的 HTTP request，将浏览器导向 ACS 指定的 URL。

这一交换过程使 ACS 能唯一地区别该 CPE；能够根据获得的信息，包括特定用户，设备及相关的账号特权，来生成一个定制页面；然后将用户导向该定制的面。

ACS 也可以发起其它的与给定用户动作相适应的 RPC 事务。例如，如果用户在网页上请求对其 CPE 进行固件升级，ACS 应当指示 CPE 使用与 ACS 应答 Kicked 方法调用相同的连接开始下载文件。

图 7 显示了与本机制相关联的事件序列。其中显示的号码与上面的步骤号码相对应。

图 7 – “Kick”机制的事件序列



D.4 LAN 端接口

CPE 可以通过提供在本地网浏览器可以访问的 LAN 端 WEB URL 来支持 Web 身份管理。

CPE 中对应的 WEB 服务器应当支持 CGI 参数，并传递给在附录 A 中定义的 Kicked PRC 方法的对应参数。**推荐**参数在表 64 中列出。

表 64 – Kick URL 的推荐 CGI 参数

名称	类型	值
command	string(32)	传递给 Kicked 方法调用的 command 参数的值。这一 CGI 参数让 ACS 了解在 Kicked 方法调用后应当执行的命令。
arg	string(256)	传递给 Kicked 方法调用的 arg 参数的值。ACS 可以传递该 CGI 参数给相应的 command 命令。没有定义对该参数的特别使用。

名称	类型	值
next	string(1024)	传递给 Kicked 方法调用的 next 参数的值。包含在 Kicked 过程结束后发送给浏览器的希望它被重定向到的站点 URL。处理 Kicked 方法调用的 ACS 可以覆盖该请求，并在 Kicked 应答中返回一个不同的 URL。

为发起 kick 处理，浏览器被重定向到 CPE 的 URL，比如通过 HTTP 302 重定向，或通过正式的 post。这一访问应当提供在表 64 中定义的 CGI 参数。例如，浏览器可以被重定向到：

<http://cpe-host-name/kick.html?command=<#>&arg=<arg>&next=<url>>

在 CPE 接收到相应的 HTTP GET 请求后，CPE 应当发起一个 Kicked 方法调用，使用用 CGI 参数填写的附录 A 中定义的方法参数。

CPE 应当定义一个最大值来限制每小时调用 ACS Kicked 方法的最多次数。当接收到一个 Kick 请求，而执行该请求将超过定义的最大值，CPE 会认为这是对安全的侵犯，因此不应当调用 Kicked 方法。

附录 E. 签名包格式

E.1 简介

本文档说明可以用于安全地下载文件到接收设备的签名包格式。该格式允许在一个签名包中封装一个或多个文件。该包格式允许接收方验证源方，并包含针对接收方的解压和安装内容指令。

签名包格式用来通过 HTTP，HTTPS，或 FTP 文件传输方式从服务器下载文件，或者通过其它文件下载手段从远端或当本地源下载文件。

E.2 签名包格式结构

图 8 显示了基本的签名包文件的格式。

图 8 – 签名包格式

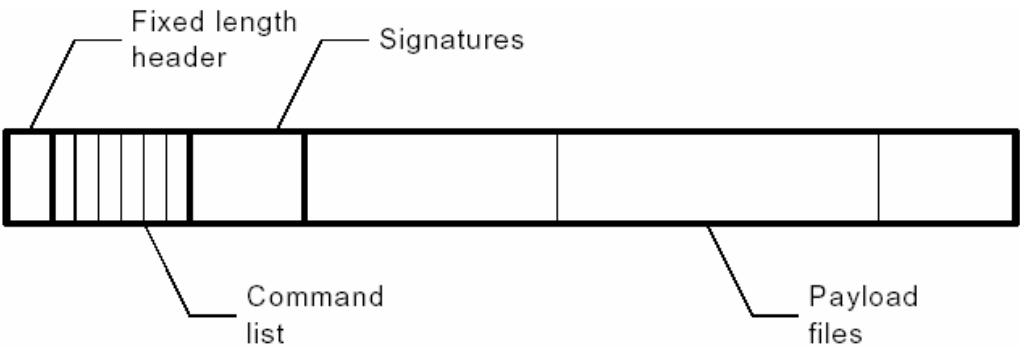


表 65 给出了对每个签名包格式成分的一般描述。

表 65 – 签名包成分简介

成分	描述
Header 头	头是固定长度的结构，包括报头，格式版本，以及命令列和有效负荷部分的长度。
Command list 命令列	命令列包含一系列指令，用来指示如果解压和安装包中所含的文件。每个命令列的格式为 TLV（type-length-value）。
Signatures 签名	本部分包括一个 PKCS #7 的数字签名块，其中是一个或多个在 E.5 节描述的数字签名集。
Payload files 有效负荷文件	本部分包含根据命令列指令来安装的一个或多个文件。

E.2.1 编码约定

除非特别说明，在本文档中使用下列编码约定：

- 多字节的数字值，以网络字节顺序（big endian format）编码。
- 文件或目录路径名以 UNIX 格式表示（例如，“/dir/dir/base.ext”）。

E.3 头格式

签名包的头是一个固定长度的 24 字节结构。其格式在表 66 中定义。

表 66 – 签名包头格式

名称	类型	描述
Preamble 报头	8 字节	固定序列的字节，包含下列十六进制值： 32 57 49 52 45 5F 53 50 解读签名包格式的程序 必须 确认报头包含了确切序列的值，才会认定它是有效的。
Major version 主版本号	32 位整数	指示包格式版本的主版本号。遵从本规范实现的主版本号为 1（壹）。 主版本号改变了，包格式就不再兼容。
Minor version 子版本号	32 位整数	指示包格式版本的子版本号。遵从本规范实现的子版本号为 0（零）。 子版本号的改变不会改变包格式的可兼容性。对本版本规范的实现应当能够解读使用不同子版本号值编码的包。
Command list length 命令行长度	32 位整数	命令列的以字节为单位的长度。其长度 必须 小于 2^{16} 。
Payload length 有效负荷长度	32 位整数	有效负荷的长度，包括其中的所有文件。

E.4 命令列格式

命令列中的每个命令的格式在表 67 中定义。

表 67 – 命令格式

字段	类型	描述
Type	32 位整数	说明特定的命令。
Length	32 位整数	说明 Value 列的以字节为单位的长度。该命令的总长度为 Length + 8 字节。
Value	（条件的）	与该命令类型关联的零个或多个字节的参数。

如果该文件格式的接收方发现有一个 Type 值它不认识，它**必须**忽略该命令，并继续解析包中的其它部分，如果下一条命令存在，则使用 Length 值来跳转到下一条命令。

E.4.1 命令类型

命令列包含两种类型的命令：包参数和需要采取的动作。包参数的例子包括软件镜像版本，或下载其它部分的超时值。动作的例子如增加，删除和移动。命令列的动作是有次序要求的，这些动作定义了需要解压和安装内含文件而对文件系统的修改。

文件相关命令有两个变种，一是用于操作普通文件，另一个用于操作版本文件。

版本文件的名称有两部分组成，固定的“基名”部分，不超过 8 个字符长度，“扩展名”部分，为 3 个字符长。每次版本文件在更新时，文件的扩展名改成新值，代表新的文件版本。由此，如果在升级中，如果需要替换版本文件，任何具有相同基名和不同扩展名的文件都必须删除。

表 68 中列出出本规范定义的命令。

表 68 – 命令类型简介

类型	命令名
0	End 结束
1	Extract File 解压文件
2	Extract Versioned File 解压版本文件
3	Add File 增加文件
4	Add Versioned File 增加版本文件
5	Remove File 删除文件
6	Remove Versioned File 删除版本文件
7	Remove Sub-Tree 删除子树
8	Move File 移动文件
9	Move Versioned File 移动版本文件
10	Version 版本
11	Description 描述
12	Recoverable Timeout 可恢复超时
13	Unrecoverable Timeout 不可恢复超时
14	Initial Timeout 初始超时
15	Initial Activity Timeout 初始动作超时
16	Reboot 重启
17	Format File System 格式化文件系统
18	Minimum Version 最低版本
19	Maximum Version 最高版本
20	Role 角色
21	Minimum Non-Volatile Storage 最小永久存储
22	Minimum Volatile Storage 最小临时存储
23	Reserved 保留
24	Reserved 保留
25	Required Attributes 需要的属性
1000-9999	厂商自定义命令

E.4.2 End 命令

该命令明确地结束命令列。在命令列中 End 命令不一定要存在，但如果接收方遇到了 End 命令，就必须停止对包中命令列部分其它命令的解析。

本命令的 Length 参数**必须**为 0（零），以表明随后没有 Value 字段。

E.4.3 Extract 和 Add 命令

Extract 和 Add 命令包括 Extract File, Extract Versioned File, Add File, 和 Add Versioned File。

Extract 命令指示接收者删除任何已经存在的同名文件, 并用有效负荷中的文件来替换。

增加命令指示接收者先检查是否存在同名文件, 并且只在没有同名文件存在时才安装新的文件。

针对版本文件的命令变种, 上述操作认定基名相同的文件为已存在。即 Extract Versioned File 命令在安装新文件前, 删除所有已经存在的基名相同, 扩展名任意的文件。相似地, Add Versioned File 命令检查是否存在与指定文件基名相同, 扩展名任意的文件, 如果没有才安装新文件。

当新文件需要建立在一个不存在的目录中时, 接收方**必须**自己创建需要的目录。

所有 extract 和 add 命令在它的 Value 选项中包括有信息。信息的格式在表 69 中定义。

表 69 – Extract 和 add 命令的 Value 格式

字段	类型	描述
Flags 标记	32 位整数	仅含一位的字段, 说明如下: Bit 0 (LSB): 不安全标记。如果该值为 1, 表明如果本命令成功结束, 但命令列表中的后续命令失败, 则接收方设备会处于一个非安全状态, 应当按照 恢复程序将它的文件系统恢复到一个已知的安全状态。 所有其它位保留, 必须 设置为 0 (零), 并且 必须 被接收方忽略。
Path Offset 路径偏移	32 位整数	从 Value 字段开始到该命令的 Path 字段, 以字节为长度的偏移量。
Path Length 路径长度	32 位整数	以八位为单位计量的 Path 字段的长度。
Hash Type Hash 类型	32 位整数	建立 Hash 字段时使用的 hash 算法的类型。目前定义了以下值: 1 = SHA-1。当设置为此值时, Hash 字段包含 20 字节的指定文件的 SHA-1 hash。在这种情况下, Hash Length 的值 必须 设置为 20 (十进制)。其它值被保留。
Hash Offset Hash 偏移	32 位整数	从 Value 字段开始到该命令的 Hash 字段, 以八位为计量单位的偏移。
Hash Length Hash 长度	32 位整数	Hash 字段的长度 (以字节计)。
File Offset 文件偏移	32 位整数	从包的有效负荷部分开始到指定文件开始, 以八位为计量单位的偏移。
File Length 文件长度	32 位整数	文件有效负荷的长度 (以字节计)。文件的真正内容存放在包的有效负荷部分。
Path 路径	Path Length 指定长度的字符串	指定文件的路径, 包括目录树和文件名。

字段	类型	描述
Hash	Hash Length 指定长度的八位串。	使用在 Hash Type 字段定义的 Hash 算法计算的有效负荷文件 Hash。将有效负荷文件 Hash 加到命令中，是因为签名仅仅验证包头和命令列。将文件 hash 加到命令中，签名也保证了文件内容的有效性。

E.4.4 Remove 命令

Remove 命令包括 Remove File, Remove Versioned File 和 Remove Sub-Tree。

Remove File 命令删除指定路径的指定文件，如果该文件存在。

Remove Versioned File 命令删除所有相同基名的文件，而不管其扩展名是什么。

Remove Sub-Tree 命令删除指定路径本身，以及其下的所有文件和子目录。

所有 Remove 命令在它的 Value 选项中包括有信息。信息的格式在表 70 中定义。

表 70 – Remove 命令的 Value 格式

字段	类型	描述
Flags 标记	32 位整数	仅含一位的字段，说明如下： Bit 0 (LSB): 不安全标记。如果该值为 1，表明如果本命令成功结束，但命令列表中的后续命令失败，则接收方设备会处于一个非安全状态， 应当按照恢复程序 将它的文件系统恢复到一个已知的安全状态。 所有其它位保留， 必须 设置为 0（零），并且 必须 被接收方忽略。
Path Offset 路径偏移	32 位整数	从 Value 字段开始到该命令的 Path 字段，以字节为长度的偏移量。
Path Length 路径长度	32 位整数	以八位为单位计量的 Path 字段的长度。
Path 路径	Path Length 指定长度的字符串	指定目录的路径。

E.4.5 Move 命令

Move 命令 Move File 和 Move Versioned File。

Move File 命令给该命令指定的文件重命名。如果指定的目标路径是个不同的目录，则文件被移动到指定的目标目录。

Move Versioned File 命令移动指定源路径中相同基名的文件，而不管其扩展名。如果指定的目录中存在多于一个这样的文件，只有一个文件被移走，其它的被删除。如果版本文件的扩展名字符地串是一个十进制数字，则只有编码最低的文件被移走，其它文件被删除。

在所有情况下，如果在指定的目标路径中已经存在相同的文件，移动命令将覆盖该文件。

如果在 move 命令中指定的源文件不存在，不做任何动作，接收方继续处理命令列中的其它命令。

所有 Move 命令在它的 Value 选项中包括有信息。信息的格式在表 71 中定义。

表 71 – Move 命令的 Value 格式

字段	类型	描述
Flags 标记	32 位整数	仅含一位的字段，说明如下： Bit 0 (LSB): 不安全标记。如果该值为 1，表明如果本命令成功结束，但命令列表中的后续命令失败，则接收方设备会处于一个非安全状态， 应当按照恢复程序 将它的文件系统恢复到一个已知的安全状态。 所有其它位保留， 必须 设置为 0（零），并且 必须 被接收方忽略。
Source Path Offset 源路径偏移	32 位整数	从 Value 字段开始到该命令的 Source Path 字段，以字节为长度的偏移量。
Source Path Length 源路径长度	32 位整数	以八位为单位计量的 Source Path 字段的长度。
Destination Path Offset 目标路径偏移	32 位整数	从 Value 字段开始到该命令的 Destination Path 字段，以字节为长度的偏移量。
Destination Path Length 目标路径长度	32 位整数	以八位为单位计量的 Destination Path 字段的长度。
Source Path 源路径	Source Path Length 指定长度的字符串	源文件路径。
Destination Path 目标路径	Destination Path Length 指定长度的字符串	源文件应当移往/重命令的目标文件路径。

E.4.6 Version 和 Description 命令

Version 和 Description 的 Value 字段的值均包含一个 UTF-8 的字符串，用于提供信息，显示或提供日志的目的。

Version 字段是为了说明与该包相关的整体版本号。例如，如果包中包含软件升级（可能包含很多文件），Version 字段可以用来指示与该升级关联的新软件版本号。

E.4.7 Timeout 命令

Timeout 命令包括 Initial Timeout, Initial Activity Timeout, Recoverable Timeout, 以及 Unrecoverable Timeout。

Timeout 命令说明在结束下载之前需要等待的包持续下载的超时值。该命令用于先下载和解析包的命令和签名部分，然后再下载包的其它部分的情况。此时，timeout 命令可以用来控制相应下载过程的超时参数。如果在解析包内容前，整个包已经下载并接收，则 timeout 命令可以忽略。

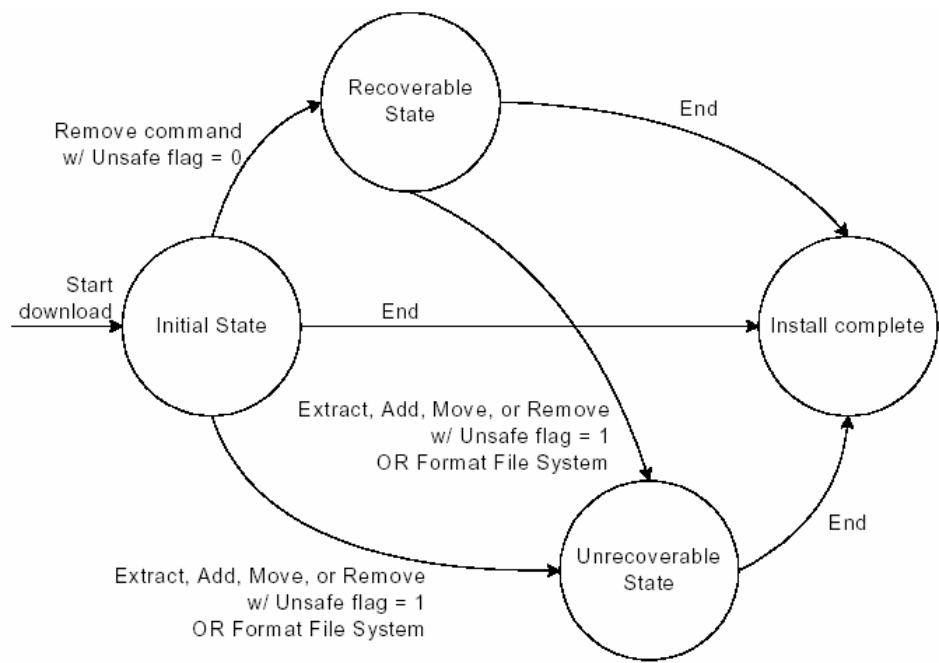
每个 Timeout 命令在它的 Value 选项中包括有信息。信息的格式在表 72 中定义。

表 72 – Timeout 命令的 Value 格式

字段	类型	描述
Timeout 超时	32 位整数	相对于包下载操作的超时值（以秒计）。值 0（零）表明无限超时。

每个 timeout 命令定义一个 timeout 值，Timeout 字段存储该期望的值。对超时值的使用基于接收方的状态。图 9 显示了接收方处理命令时的状态转换模型。图中显示了命令列中的每个命令在顺序执行时发生的状态转换。执行命令时并不会改变状态，除非状态转换箭头指示的情况发生。

图 9 – 用于超时模型的下载状态图



在下载时，接收方使用上述状态图来决定使用哪个超时值。表 73 中显示了 timeout 命令与类型的定义。

表 73 – Timeout 命令定义

命令	描述
Initial Timeout 初始超时	此命令设置在表 9 所示的初始化状态时使用的下载超时值。该值从整个包开始下载算起。
Initial Activity Timeout 初始动作超时	此命令设置 <u>仅在</u> 表 9 所示的初始化状态时使用的某个动作的超时值。该值从最近一次包数据发送给接收方算起。 注意在除初始化状态之外的其它状态，均无动作的超时设置（动作的超时设置是无限的）。
Recoverable Timeout 可恢复超时	此命令设置在表 9 所示的可恢复状态时使用的下载超时值。该值从整个包开始下载算起。
Unrecoverable Timeout 不可恢复超时	此命令设置在表 9 所示的不可恢复状态时使用的下载的超时值。该值从整个包开始下载算起。

E.4.8 Reboot 命令

该命令用来指示接收方重新启动，以完成安装过程。如果使用该命令，它 **必须**是命令列表中的最后一条命令（除了 End 命令，如果存在的话）。

这一命令的 Length 参数的长度必须为 0（零），说明没有后续的 Value 字段。

E.4.9 Format File System

这一命令指示接收方在安装过程中重新格式化其文件系统。该命令如果被使用，将暗含该文件系统中的现有文件（或与安装过程相关的部分文件）将被清除，并被包中的新文件覆盖。

这一命令的 Length 参数的长度必须为 0（零），说明没有后续的 Value 字段。

E.4.10 Minimum 和 Maximum Version 命令

Minimum Version 和 Maximum Version 命令用来说明本包应用的软件版本号的范围。

当在包中使用这些命令指定了最低和最高版本号，而且接收方的软件版本号未在指定的范围内，接收方**不得**安装文件或者执行命令列中的其它动作。

只有在与接收方相关的真实软件版本的格式为层次化格式，并能用下面列出的过程进行数字化比较时，该命令才能使用。

Minimum Version 和 Maximum Version 在命令的 Value 选项中包括有信息。信息的格式在表 74 中定义。

表 74 - Minimum Version 和 Maximum Version 命令的 Value 格式

字段	类型	描述
Version	32 位整数的数组	整数元素的数组，每个元素指示一个版本号。被认作是层次状的版本号码（例如，“1.0.20.3”），排在后面的整数代表版本号中更细微的部分。

下列过程用来判断版本是否在指定的范围内。

如果给出了 Minimum Version，则对 Version 数组中的每个元素，从第一个（最主要的）开始：

1. 如果接收方实际的版本号的该元素比 Minimum Version 的对应元素大，则接收方的版本满足要求，过程结束。
2. 如果接收方实际的版本号的该元素比 Minimum Version 的对应元素小，则接收方的版本不满足要求。在这种情况下，过程结束，但接收方**不得**安装包中的文件，或者执行后续的任何命令。
3. 否则（值相同），
 - a. 如果这是数组的最后一个元素，则接收方的版本号满足要求，过程结束。
 - b. 否则（还有更多的元素），过程应当从第 1 步开始使用数组中的下一个元素进行比较。

如果给出了 Maximum Version，则对 Version 数组中的每个元素，从第一个（最主要的）开始：

1. 如果接收方实际的版本号的该元素比 Maximum Version 的对应元素小，则接收方的版本满足要求，过程结束。
2. 如果接收方实际的版本号的该元素比 Maximum Version 的对应元素大，则接收方的版本不满足要求。在这种情况下，过程结束，但接收方**不得**安装包中

的文件，或者执行后续的任何命令。

3. 否则（值相同），
 - a. 如果这是数组的最后一个元素，则接收方的版本号满足要求，过程结束。
 - b. 否则（还有更多的元素），过程应当从第 1 步开始使用数组中的下一个元素进行比较。

E.4.11 Role 命令

Role 命令用来指示目标应用或包的目的。主要用来说明特定包可能需要的边际作用，或后续操作。

Role 命令在其 Value 选项中包括有信息。信息的格式在表 75 中定义。

表 75- Role 命令的 Value 格式

字段	类型	描述
Role	32 位整数	枚举值，说明包的目标应用，或者目的。定义了下列值： 1 = Software upgrade （软件升级） 2 = Software recovery （软件恢复） 3 = Web content （Web 内容） 4 = Vendor configuration （厂商配置） 以 0xFF 作为最高位的值，被解释为厂商定制的 Role。在这种情况下，后续的三个字节包含 OUI 值（组织唯一标识），标识在[9]中定义的对应该厂商。当使用该值时，厂商可以在此命令中定义后续附加参数，来明确标识该 Role。附加参数由厂商定制方式解读。 所有其它值保留。

E.4.12 Minimum Storage 命令

Minimum Storage 命令包括 Minimum Volatile Storage Size 及 Minimum Non-Volatile Storage Size。

Minimum Storage 命令说明接收端设备能安装包中文件的最低要求。如果存在，每个命令说明由名称决定的存储类型的最低要求。

如果接收端设备不满足指定的最低要求，接收方不得安装包中的任何文件，或者继续处理命令。

Minimum Storage 命令在其 Value 选项中包括有信息。信息的格式在表 76 中定义。

表 76 – Minimum Storage 命令的 Value 格式

字段	类型	描述
Storage Size	32 位整数	由命令名称指定的存储类型的最低要求（以字节为单位）。

E.4.13 Required Attributes 命令

Required Attributes 命令用来说明接收设备的其它属性。只有接收设备满足这些属

性时，安装包才认为是有效的。

一个包中可以有一个或多个 Required Attributes 命令，每个命令用来说明一个不同类别的属性。

Required Attributes 命令在其 Value 选项中包括有信息。信息的格式在表 77 中定义。

表 77 – Required Attributes 命令的 Value 格式

字段	类型	描述
Defining Entity 定义实体	32 位整数	用来说明本命令中使用的类别和属性的定义者的标识。定义值如下： 值 0（零）表明标准的类别和属性定义。标准定义是指由本规范的本版本或未来版本定义。 以 0xFF 做为最高位的值说明厂商定制类别和属性定义。在这种情况下，后续的 3 字节包含该厂商的 OUI（组织唯一标识），如[9]中定义。 如果接收方处理了包含一个它不认识实体值的 Required Attributes 命令，它应当忽略该命令，并继续处理后续的命令。
Class 类型	32 位整数	枚举值，用来指定接收方用来比较的准则，以决定是否该包适合该设备。对给定的准则，Attribute Array 字段的值指出该准则允许的特定值。 在本规范的本版本中，没有定义标准类型。对厂商定制的实体，对类型值的解释由厂商自己决定。 如果接收方处理了包含一个它不认识类型值的 Required Attributes 命令，它应当忽略该命令，并继续处理后续的命令。
Attribute Array 属性数组	32 位整数的数组	变长数组属性，每个属性是一个对应类型允许值的枚举。 如果接收方设备的真实值满足数组中列示的任何值，则接收方满足指定的要求。否则，接收方不满足要求，包不得安装。 在本规范的本版本中，没有定义标准的属性值。对厂商定制的实体，对属性值的解释由厂商自己决定。

E.5 签名

签名部分紧跟在包文件的命令列部分的后面。签名部分包含使用 PKCS #7 签名语法[14]定义的数字签名块。

特别地，签名块包含一个 PKCS #7 SignedData 对象，其中包含零个或更多个满足下列限制的签名：

- 签名为外部签名（external signatures），即签名报文不是封装在 SignedData 对象内的，而是包括由包的头和命令列部分组成的八位字符串。
- contentInfo 的 contentType 元素必须说明为类型 “data”。
- contentInfo 的 content 元素必须为空，原因是这是外部签名，报文数据存储在签名本身之外。
- 每个签名使用的 digestAlgorithm 必须为类型 SHA-1。
- 每个签名使用的 digestEncryptionAlgorithm 必须为类型 RSA。
- 整个 SignedData 对象的指示 Identifier 的 Tag 值必须小于或等于 30，即是对 Identifier 的只有八位的编码。
- 如果在签名块中没有签名，也就没有扩展的证书或证书废除列表。

SignerInfo 的值将为空，digestAlgorithms 集可以为空。SignedData 的所有其它字段必须正常存在。注意，空签名块的内容是与包内容独立的，因此可以当做固定序列的字节来预处理。

如果签名块包含一个或多个签名，接收方应当至少成功验证一个签名才能认为签名包是可以信任的。

如果接收到的包需要有一个或多个签名，接收方必须在处理命令列表中的命令前对签名进行验证。如果没有任何一个签名能通过验证，接收方**不得**处理命令列表中的任何命令，或安装包中的任何文件。

如果接收方的实施是在可以在从源下载整个包文件之前，进行命令列表的验证和处理，接收方**可以**认为头，命令列表和签名块的总长度不超过 150K 字节。

注意尽管签名报文数据只包含包头和命令列表，但签名仍能保证整个包的数据的一致性，因为所有引用有效负荷文件的命令均包含对应文件内容的 hash。

还要注意的，在已存在的签名包文件中加入附加的签名并不需要更改除签名块本身以外的文件其它部分。包格式的结构决定了在签名块的长度变化时，包文件的其它内容（头，命令列，有效负荷）不需要改变。

翻译词汇对照表

Access Point	接入点
ACS Discovery	ACS 发现
ACS/Auto-Configuration Server	自动配置服务器
ATP	实际汇聚发射功率（Aggregate transmitter power）
ATU-C	ADSL 终端单元-局端（ADSL Termination Unit – Central (Office)）
ATU-R	ADSL 终端单元-远端（ADSL Termination Unit – Remote）
Auto-configured complex services	自动配置的复杂服务
Beacon	信标
Bridge	网桥
Cell	信元
Cipher	密码
Common Framework	公用框架
Conditional	有条件的
Digest authentication	摘要认证
DSL loop diagnostics	DSL 环路诊断
Dynamic Service Provisioning	动态服务供应
End-user	最终用户
Envelop	信包
Firmware	固件

Image Management	映像管理
Incoming	进向
Instance	实例
Interaction	交互作用
Interleaved	隔行的
Message	报文
MRU	最大接收单元 (Maximum Receive Unit)
MTU	最大传输单元 (Maximum Transfer Unit)
multi-instance object	多实例对象
Object	对象
Organizational unique identifier	组织唯一标识
Outcoming	出向
Packet	分组
Package	包
Payload	有效负荷
Peer	对等体
Provisioning	供给
PSD	功率频谱密度 (Power spectral density)
Repeater	中继器
Require	要求
Signal-to-noise ratio	信噪比
Station	站点
Sub-object	子对象
SuperSet	超集
Transaction	事务
Transmit	传播
Vendor	厂商
Web identity management	web 标识管理
Wi-Fi Protected Access	WPA