



中华人民共和国通信行业标准

YD/T 2813-2015

基于端口控制协议（PCP）扩展的 LAFT6 端口区间集扩展协议技术要求

Technical specification for port-set allocation for
LAFT6 using PCP extension

2015-04-30 发布

2015-07-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 缩略语	1
3 概述	1
4 报文要求	2
4.1 PCP 总体要求	2
4.2 PORT_SET Option 的报文格式	3
4.3 MAP 出错代码列表	3
5 PORT_SET Option 使用	4
5.1 PCP 客户端的处理过程	4
5.2 PCP 服务器的处理过程	4
5.3 端口集的更新和删除处理	5
5.4 多个端口集处理	5
6 PORT_SET Option 部署相关考虑	5
6.1 设备形态	5
6.2 故障场景	5
6.3 安全考虑	6
附录 A (资料性附录) LAFT6 应用背景	7
参考文献	8

前 言

本标准按照GB/T1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

标准起草单位：中国电信集团公司、华为技术有限公司、清华大学、工业和信息化部电信研究院、中兴通讯股份有限公司。

标准主要起草人：孙 琼、解冲锋、赵晶晶、张忠建、崔 勇、赵锋、史 凡、胡 捷、王 茜、李忠超、何 琪、陈运清、王作强、阎 璐。

基于端口控制协议（PCP）扩展的
LAFT6端口区间集扩展协议技术要求

1 范围

本标准规定了在IPv6过渡中LAFT6系统中隧道发起点设备获得外部地址和端口区间集的技术要求，包括报文格式及处理过程。

本标准适用于具有LAFT6隧道发起点设备、隧道终结点设备，同时也可应用于其他具有NAT功能的网络设备和用户驻地设备，如运营级NAT设备、DS-lite设备、NAT64设备、防火墙设备、NPTv6设备等。

2 缩略语

下列缩略语适用于本文件。

AAA	Authentication, Authorization and Accounting	认证、授权和计费
BRAS	Broadband Remote Access Server	宽带接入服务器
CGN	NATCarrier-Grade NAT	运营级
CPE	customer premises equipment	用户驻地设备
CR	Core Router	核心路由器
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHCPv4	Dynamic Host Configuration Protocol Version 4	动态主机配置协议版本4
DS-Lite	Dual-Stack Lite	轻型双栈方案
IANA	Internet Assigned Numbers Authority	Internet号码分配授权委员会
IETF	Internet Internet Engineering Task Force	互联网工程任务组
IP	Internet Protocol	互联网协议
LAFT6	Lightweight Address Family Transition for IPv6	轻量级IPv6过渡方案
NAT	Network Address Translator	网络地址翻译器
NAT64	Network Address Translator 64	从IPv6地址翻译IPv4地址
NPTv6	IPv6-to-IPv6 IPv6 Network Prefix Translation	IPv6到IPv6网络前缀转换
PCP	Port Control Protocol	端口控制协议
SR	Service Router	业务路由器

TC	Tunnel Concentrator	隧道终点
TI	Tunnel Initiator	隧道起点
UDP	User Datagram Protocol	用户数据报协议

3 概述

基于PCP扩展的LAFT6端口区间集扩展协议的应用场景如图1所示。

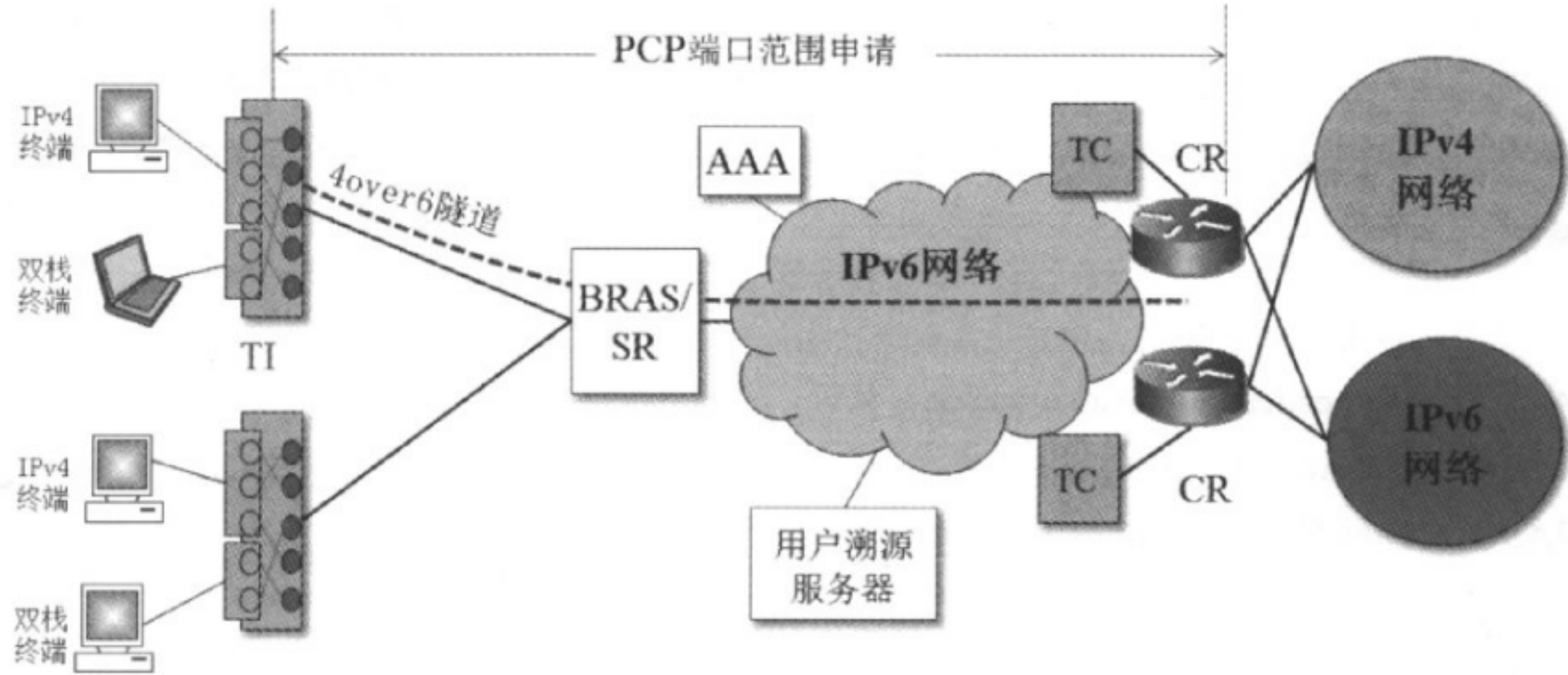


图 1 基于 PCP 扩展的 LAFT6 端口区间集扩展协议应用场景图示

基于PCP的端口区间扩展协议可应用于LAFT6系统中，该协议主要用于TI、TC之间的PCP端口范围申请。使用该协议的原因如下：

- 当运营商没有部署 DHCPv4 服务器时，无法通过 DHCP 获得外部地址和外部端口集；
- 基于 PPP 扩展的协议只能在 TC 部署在 BRAS 上时应用，对于 TC 和 BRAS 分离式部署的场景不适用；
- 对于已部署了 CGN 的运营商而言，可基于现有的 CGN 板卡进行扩展，使之成为 LAFT6 系统中的一部分，对端口区间值进行下发。

本标准中定义的端口集扩展协议是基于PCP MAP的一个扩展选项实现的，命名为PORT_SET Option。通过该选项可获取一个外部IP的端口集。

PORT_SET Option选项的主要过程为，首先在已获得IPv6地址的TI处配置TC的地址，然后发起PCP MAP请求（MAP request）。TC接到请求后，对请求进行相应的过滤后，根据请求内容，进行创建、更新、删除映射表项（包括IPv6地址、IPv4地址和端口区间）。同时，TC生成PCP MAP响应（MAP response），用于反馈信息。主要反馈映射表项和生命周期（lifetime）。最后，TI获取到端口区间集并对端口区间集进行管理。

注：本标准中MAP请求和响应的主报头具体格式和内容与draft-ietf-pcp-base定义的标准格式一致，PORT_SET Option的定义格式与draft-ietf-pcp-port-set中定义的一致。

4 报文要求

4.1 PCP 总体要求

PCP是采用UDP报文来进行发送，在与LAFT6等隧道类协议配合使用时，应采用与数据报文一致的IPv4-in-IPv6的报文发送，从而尽可能保证在传输过程中PCP报文和数据报文在传输路径上的一致性。每个PCP请求将会对应一个响应（response），PCP单播报文使用的UDP端口号为5351。

要求PCP能够处理多次PCP请求与响应，应支持客户端发送更新时间周期（lifetime）的更新报文。

PCP客户端中对于PCP服务器的地址配置应支持多种方式，其一可以采用动手配置的方式，其二可以采用与TC地址合一的方式，PCP客户端应支持采用TC的地址作为其PCP服务器的地址。

PCP客户端应支持MAP Request报文中PORT_SET Option的发送。PCP服务器应支持对PCP MAP请求中携带PORT_SET Option报文的解析和响应报文的生成。

4.2 PORT_SET Option 的报文格式

PORT_SET Option总体说明如下：

- Option 名：PORT_SET；
- 定义 Option 目的：分配一个端口集用于映射；
- 可以使用该 Option 的 Opcode:MAP；
- Option 可以出现在：请求报文和响应报文；
- 每个 MAP 请求或响应报文中 Option 最多出现的次数：1 次。

PORT_SET Option主要用于指示PCP客户端希望PCP服务器预留一段端口给客户端使用。客户端请求的端口数量是通过Option来指明的，客户端所获得的外部地址即为MAP Opcode中所得到的External IP Address。PORT_SET的格式如图2所示。

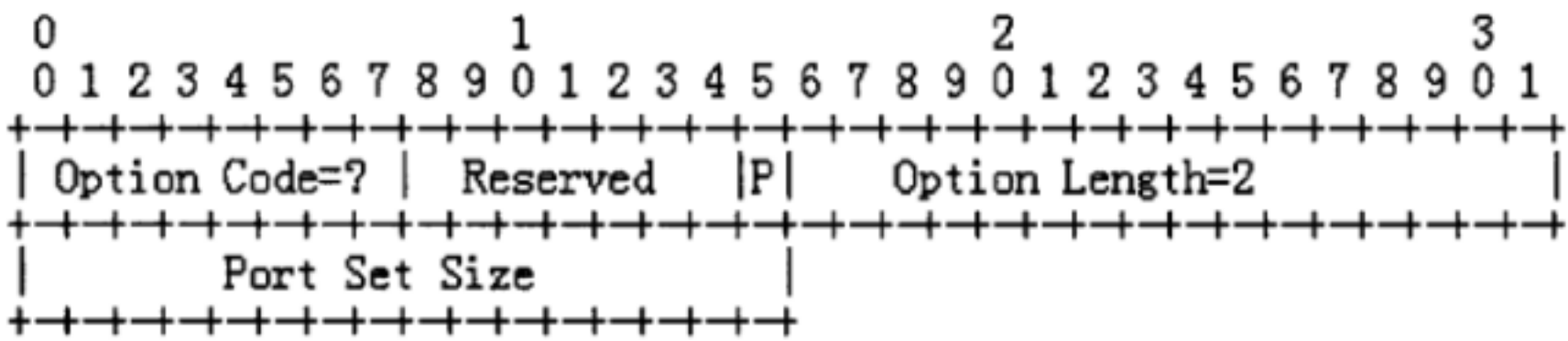


图 2 PORT_SET Option 报文格式

其中，每个标识位的设置方式如下：

- Option Code: 暂定为 XXX（后期与国际标准保持一致）。
- Reserved: 预留域。置 0。
- P: r 如果需要奇偶预留则置 1，否则置 0。
- Option Length: 2(字节)。
- Port Set Size: 请求的端口数，不能是 0 或 1。客户端获取的端口起始值为 MAP 主报头中的 External Port 值，实际用户可使用的端口区间即为[Assigned External Port, Assigned External Port + Port Set Size]。

注：目前该Option不支持分配不连续端口集。后继可能会根据国际标准的定义增加。

4.3 MAP 出错代码列表

表1中列出了结果码的值（代码值为暂定值，待国际标准发布之后，与国际标准一致）和具体含义。结果码是服务器返回的结果标示，其中只有错误代码0代表执行成功，其他所有的值都代表了有错误产生。如果服务器在处理过程中碰到多个错误，则会选择一个最明确的错误返回。每个错误码属于长期错误或

YD/T 2813-2015

者短期错误，主要是为开发者提供建议的错误生命周期值。这里推荐短期错误生命周期为30s，长期错误的生命周期为30min。

表 1 错误代码值以及含义列表

错误代码	含义	说明
0	SUCCESS: 成功	
1	UNSUPP_VERSION: 不支持的版本号	长期错误
2	NOT_AUTHORIZED: 该请求功能不支持	长期错误
3	MALFORMED_REQUEST: 该请求无法解析	长期错误

表 1 (续)

错误代码	含义	说明
4	UNSUPP_OPCODE: 该 Opcode 无法支持	长期错误
5	UNSUPP_OPTION: 该 Option 无法支持	长期错误
6	MALFORMED_OPTION: 选项形式不正确	长期错误
7	NETWORK_FAILURE: 网络不可达	短期错误
8	NO_RESOURCES: PCP 服务器端当前没有足够的计算资源来进行处理，该功能将来可能可以满足	短期错误
9	UNSUPP_PROTOCOL: 不支持的协议	长期错误
10	USER_EX_QUOTA: 当前没有可用的端口	短期错误
11	CANNOT_PROVIDE_EXTERNAL: 没有可用的外部端口或外部地址	短期错误
12	ADDRESS_MISMATCH: 报文的源 IP 地址与请求中的 IP 地址不一致	短期错误
13	EXCESSIVE_REMOTE_PEERS: 仅在 MAP 的 filter 中出现	长期错误

5 PORT_SET Option 使用

5.1 PCP 客户端的处理过程

为了获取一个端口集，PCP客户端需要在PCP MAP请求中增加一个PORT_SET Option。如果需要对端口奇偶性预留，PCP客户端应设置P值为1，来要求PCP服务器分配奇偶端口（也就是分配的外部端口和内部端口具有相同的奇偶性）。PCP客户端需要在PORT_SET Option中指明建议的端口集的大小。

一个MAP请求中只能包含一个PORT_SET Option。如果需要多个端口集，PCP客户端应发送多个携带PORT_SET Option的MAP请求给PCP服务器，而且每个MAP请求应包含不同的内部端口。

5.2 PCP 服务器的处理过程

PCP服务器接收到PCP MAP请求后，除了对PCP MAP请求进行常规的检查外，对生命期非零且包含PORT_SET Option的报文做如下的检查：

- 如果在一个 MAP 请求中包含了多个 PORT_SET Option，则 PCP server 应返回一个MALORMED_OPTION 错误；
- 如果 PORT Set Size 是 0 或者 1，返回 MALORMED_OPTION 错误。

如果在报文中包含了PREFER_FAILURE Option,并且服务器不能满足请求的端口集或者不能预留奇偶端口，则返回CANNOT_PROVIDED_EXTERNAT错误。

如果在报文中没有包含PREFER_FAILURE Option,服务器可以不满足请求的外部端口集大小的需要，而只提供给有限的外部端口。PCP服务器不要提供客户端超过客户端的需要需求的端口数量。

如果请求的端口集由于端口不可用而不能成功, PCP服务器则只分配一个外部端口(也就是PCP服务器会忽略掉PORT_SET Option)。无论何种原因导致只能分配一个外部端口, PORT_SET Option都不能包含到响应的报文中。

当报文中没有包含PREFER_FAILURE Option, 而且PORT_SET Option中设置了奇偶位(P bit=1), 服务器会预留端口的奇偶性。这种情况下, 设置的外部端口的值和内部端口的值具有相同的奇偶性。

如果请求的映射已经存在, PCP服务器根据PORT_SET Option更新映射的端口集信息, 并且发送一个代表正确处理的响应报文。

如果请求的映射端口成功, 则MAP响应中分配的外部端口值为分配的外部端口的第一个端口。PORT_SET Option的Port Set Size的值为分配的端口集的大小。

5.3 端口集的更新和删除处理

端口集的MAP映射的更新和删除是作为一个表项统一处理的, 也就是说端口集中的所有端口的生命周期都分配为相同的生命周期。

PORT_SET Option应包含到更新或删除的请求报文中。如果服务器接收到一个没有包含PORT_SET Option的请求, 并且请求的内部端口在端口集映射的内部端口范围内, 服务器应返回一个MALFORMED_REQUEST 错误。

5.4 多个端口集处理

为每个PCP客户端分配的端口数量是由PCP服务器决定的。如果PCP控制的设备支持对某个PCP客户端多次委派端口集, 则PCP客户端在耗尽一个请求的端口集后, 会重新发起一个PCP请求获取另外一个端口集。

如果PCP控制的设备支持对某个用户多次委派端口集, 则对该用户分配的多个端口集都使用相同的外部IP地址。

为了优化在PCP服务器维护的映射表项, 推荐服务器配置在一个响应中分配一个最大的端口集给客户端的策略。

6 PORT_SET Option 部署相关考虑

6.1 设备形态

PCP的客户端用两种设备形态, 硬终端和软终端。

软终端, 即TI以软件形式和host集成在一起, 在host上直接发起PCP请求, 向服务器端申请外部地址和外部端口集。此时, 外部地址和外部端口集由主机获得。

硬终端(例如CPE), 即TI和host分离, 硬终端发起PCP请求, 向服务器端申请外部地址和外部端口集。此时, 外部地址和外部端口集由硬终端获得。硬终端进行NAT, 将所获得的外部资源, 分配给接入它的host。

PCP服务器端, 可以是嵌入式的设备, 也可以是独立式的设备。

6.2 故障场景

针对于PCP服务器端和PCP客户端出现的各类问题, 提出相应的解决方法, 用于恢复映射关系表。

6.2.1 PCP 服务器端的 IP 地址改变

当PCP服务器端的IP地址改变时, PCP客户端应针对PCP服务器端新的IP地址重新创建所有映射关系。

6.2.2 PCP 客户端的 IP 地址改变

YD/T 2813-2015

当PCP客户端的IP地址改变时，PCP客户端向PCP服务器端重新发起请求，建立新的映射关系，并获得重新分配的端口段号，同时更新PCP客户端本身的映射关系。之前的映射关系，当生命周期到期会自动被PCP服务器端删除。

6.2.3 PCP 客户端崩溃重启

当PCP客户端由于致命错误崩溃重启时，需要恢复映射关系。此时，PCP服务器端不需要更新映射关系。如果PCP客户端存储了映射关系，则可以直接进行映射关系的恢复。如果没有存储映射关系，则需要重新发起携带PORT_SET Option的MAP请求。PCP客户端将内部IP地址和它所对应PCP服务器端的IP地址发送给PCP服务器端，PCP服务器端经过检查，将所对应的端口段地址返回给PCP客户端，完成PCP客户端的映射关系恢复。

6.2.4 PCP 服务器端的崩溃重启

当PCP客户端由于致命错误崩溃重启时，需要恢复映射关系。如果PCP服务器端进行了同步的冗余备份，则进行直接恢复。如果PCP服务器端没有进行同步的冗余备份，则将通过Epoch告知各个PCP客户端崩溃现状，并进行映射关系同步。

6.3 安全考虑

6.3.1 PCP 服务器端的端口区间控制

PCP服务器所持有的外部地址和外部端口集的数量是有限的。它可能会给几台PCP客户端甚至数十台PCP客户端分配地址并提供服务。当PCP服务器端下发外部端口集后，得到端口段的PCP客户端可以进行使用。如果其中存在恶意的PCP客户端，它可以恶意占用大量端口，致使其他PCP客户端无端口集可用，引发PCP服务器端对其他主机拒绝服务的问题。

因此，PCP服务器端在下发外部端口集时，应对下发的端口数量进行限制，防止恶意主机对端口段的恶意占用。

6.3.2 PCP 服务器端的地址过滤

当存在恶意报文攻击时，TC处会接收到大量的创建映射的请求，占用大量资源，严重时会导致PCP服务器端的崩溃。因此，在PCP服务器端之间应建立入口的TI过滤机制，以防止欺骗报文的攻击。

附 录 A
（资料性附录）
LAFT6 应用背景

随着全球IPv4地址的耗尽，IPv4向IPv6过渡已成为解决该问题的重要方案。其中，作为主流过渡技术的LAFT6系统，它的主要特点是轻量级地址管理和轻量级地址维护。LAFT6系统中将有状态方案中网关的集中式状态表处理分布到不同的TI中，在TC中仅维护少量的地址转换状态信息，将“每连接”的状态表减少为“每用户”的状态表。

LAFT6端口区间集扩展协议，支持LAFT6系统轻量级这一特点。它规定PCP服务器端可以一次性向PCP Client下发一块端口区间，在TC处仅维护内部地址、外部地址和外部端口区间集这一三元组映射。对比于TC对每一端口号的维护，大大降低了TC处的负担。另外，该协议还支持PCP Client对PCP服务器端进行多次端口区间集的请求。由PCP服务器端设置请求次数和每次下发端口区间集的大小。

参 考 文 献

- [1]Q. Sun et al, “Port Control Extension (PCP) Extension for Port Set Allocation”, IETF draft, January 17, 2013
- [2]Y. Cui et al., “Lightweight 4over6: An Extension to the DS-Lite”, IETF Softwire draft, October 2011.
- [3]D. Wing, Ed et al, ” Port Control Protocol (PCP)” , IETF draft, November 7, 2012.
-