目 录

PPP、MP

PPP 简介

PPP（Point to Point Protocol）协议是在点到点链路上承载网络层数据包的一种链路层协议，由于它能够提供用户验证、易于扩充，并且支持同/异步通信，因而获得广泛应用。

PPP 定义了一整套的协议，包括链路控制协议（LCP）、网络层控制协议（NCP）和验证协议（PAP 和 CHAP）。

- 链路控制协议（Link Control Protocol，LCP）：主要用来建立、拆除和监控数据链路。
- 网络控制协议（Network Control Protocol，NCP）：主要用来协商在该数据链路上所传输的数据包的格式与类型。
- 用于网络安全方面的验证协议族 PAP 和 CHAP。

PAP 验证

PAP（Password Authentication Protocol）验证为两次握手验证，密码为明文，PAP 验证的过程如下：

(1) 被验证方发送用户名和密码到验证方；

(2) 验证方根据本端用户表查看是否有此用户以及密码是否正确，然后返回不同的响应（Acknowledge or Not Acknowledge）。

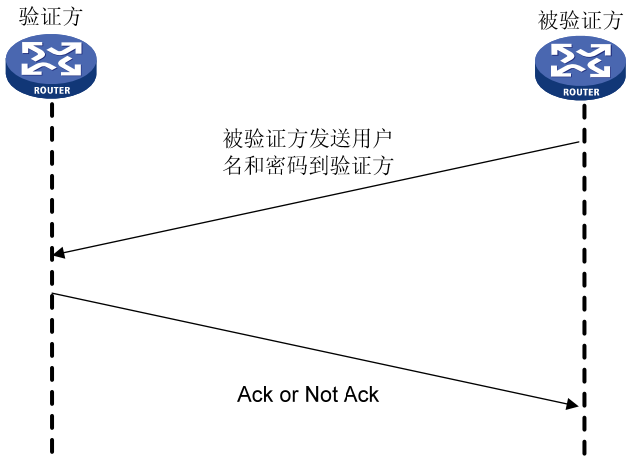

图1 PAP 验证示意图

PAP 不是一种安全的验证协议。当验证时，口令以明文方式在链路上发送，并且由于完成 PPP 链路建立后，被验证方会不停地在链路上反复发送用户名和口令，直到身份验证过程结束，所以不能防止攻击。

CHAP 验证

CHAP（Challenge-Handshake Authentication Protocol）验证为三次握手验证，密码为密文（密钥）。

CHAP 单向验证是指一端作为验证方，另一端作为被验证方。双向验证是单向验证的简单叠加，即两端都是既作为验证方又作为被验证方。在实际应用中一般只采用单向验证。

CHAP 验证过程如下：

(1) 验证方主动发起验证请求，验证方向被验证方发送一些随机产生的报文（Challenge），并同时将本端的用户名附带上一起发送给被验证方；

(2) 被验证方接到验证方的验证请求后，检查本端接口上是否配置了缺省的 CHAP 密码，如果配置了则被验证方利用报文 ID、该缺省密码和 MD5 算法对该随机报文进行加密，将生成的密文和自己的用户名发回验证方（Response）；

(3) 如果被验证方检查发现本端接口上没有配置缺省的 CHAP 密码，则被验证方根据此报文中验证方的用户名在本端的用户表查找该用户对应的密码，如果在用户表找到了与验证方用户名相同的用户，便利用报文 ID、此用户的密钥（密码）和 MD5 算法对该随机报文进行加密，将生成的密文和被验证方自己的用户名发回验证方（Response）；

(4) 验证方用自己保存的被验证方密码和 MD5 算法对原随机报文加密，比较二者的密文，根据比较结果返回不同的响应（Acknowledge or Not Acknowledge）。

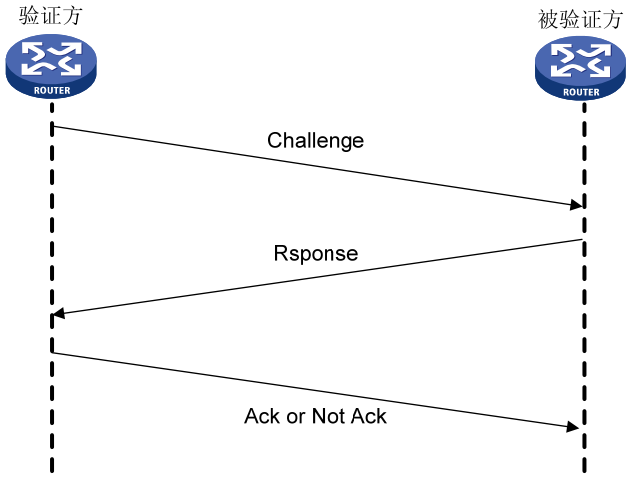

图2 CHAP 验证示意图

PPP 运行过程

PPP 运行过程（参见下图）如下：

(1) 在开始建立 PPP 链路时，先进入到 Establish 阶段。

(2) 在 Establish 阶段 PPP 链路进行 LCP 协商，协商内容包括工作方式（是 SP 还是 MP）、验证方式和最大传输单元等。LCP 协商成功后进入 Opened 状态，表示底层链路已经建立。

(3) 如果配置了验证（远端验证本地或者本地验证远端）则进入 Authenticate 阶段，开始 CHAP 或 PAP 验证。

(4) 如果验证失败进入 Terminate 阶段，拆除链路，LCP 状态转为 Down；如果验证成功就进入 Network 协商阶段（NCP），此时 LCP 状态仍为 Opened，而 IPCP 状态从 Initial 转到 Request。

(5) NCP 协商支持 IPCP 协商，IPCP 协商主要包括双方的 IP 地址。通过 NCP 协商来选择和配置一个网络层协议。只有相应的网络层协议协商成功后，该网络层协议才可以通过这条 PPP 链路发送报文。

(6) PPP 链路将一直保持通信，直至有明确的 LCP 或 NCP 帧关闭这条链路，或发生了某些外部事件（例如用户的干预）。

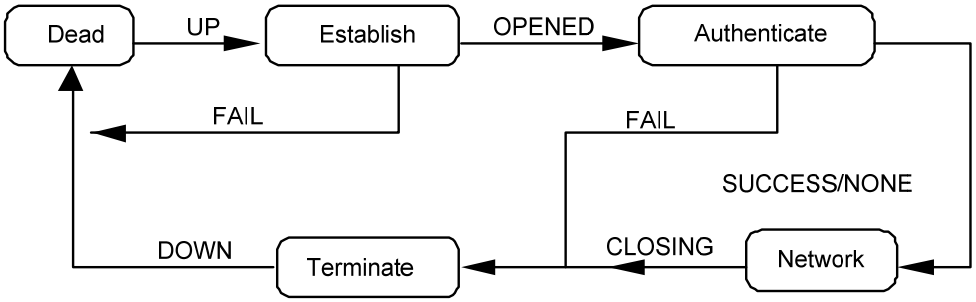

图3 PPP 运行流程图

有关 PPP 的详细说明，请参考 RFC1661。

MP 简介

为了增加带宽，可以将多个 PPP 链路捆绑使用，称为 MultiLink PPP，简称 MP。MP 会将报文分片（小于最小分片包长时不分片）后，从 MP 链路下的多个 PPP 通道发送到 PPP 对端，对端将这些分片组装起来递给网络层。

实现方式

MP 的配置主要有两种方式，一种是通过虚拟模板接口（Virtual-Template，VT），VT 是用于配置一个虚拟访问接口（Virtual Access，VA）的模板，将多个 PPP 链路捆绑成 MP 之后，需要创建一个 VA 与对端交换数据。此时，系统将选择一个 VT，以便动态地创建一个 VA；一种是利用 MP-group 接口。这两种配置方式的区别主要是：

- 虚拟模板接口方式可以与验证相结合，可以根据对端的用户名找到指定的虚拟模板接口，从而利用模板上的配置，创建相应的捆绑（Bundle，系统中用 VT 通道来表示），以对应一条 MP 链路。
- 由一个虚拟模板接口还可以派生出若干个捆绑，每个捆绑对应一条 MP 链路。那么这样一来，从网络层看来，这若干条 MP 链路会形成一个点对多点的网络拓扑。从这个意义上讲，虚拟模板接口比 MP-group 接口更加灵活。
- 为区分虚拟模板接口派生出的多个捆绑，需要指定捆绑方式，系统在虚拟模板接口视图下提供了命令 **ppp mp binding-mode** 来指定绑定方式，绑定方式有 **authentication**、**both**、**descriptor** 三种，缺省是 **both**。**authentication** 是根据验证用户名捆绑，**descriptor** 是根据终端描述符捆绑（LCP 协商时，会协商出这个选项值），**both** 是要同时参考这两个值捆绑。
- MP-group 接口与虚拟模板接口相比则单纯许多，它是 MP 的专用接口，不能支持其他应用，也不能利用对端的用户名来指定捆绑，同时也不能派生多个捆绑。但正因为它的简单，导致了它的快速高效、配置简单、容易理解。

协商过程

MP 的协商包括 LCP 协商和 NCP 协商两个过程：

- LCP 协商：两端首先进行 LCP 协商，除了协商一般的 LCP 参数外，还要验证对端接口是否也工作在 MP 方式下。如果两端工作方式不同，LCP 协商不成功。
- NCP 协商：在 LCP 协商成功后，根据 MP-group 接口或指定虚拟接口模板的各项 NCP 参数（如 IP 地址等）进行 NCP 协商，物理接口配置的 NCP 参数不起作用。

NCP 协商通过后，即可建立 MP 链路。

MP 作用

MP 的作用主要有：

- 增加带宽，结合 DCC（Dial Control Center，拨号控制中心）可以做到动态增加或减小带宽
- 负载分担
- 备份
- 利用分片降低时延

MP 能在任何支持 PPP 封装的接口下工作，如串口、ISDN 的 BRI/PRI 接口等，也包括 PPPoX（PPPoE、PPPoA、PPPoFR 等）这类虚拟接口，建议用户尽可能将同一类的接口捆绑使用，不要将不同类的接口捆绑使用。

PPPoE

PPPoE 简介

PPPoE 是 Point-to-Point Protocol over Ethernet 的简称，它可以通过一个远端接入设备为以太网上的主机提供因特网接入服务，并对接入的每个主机实现控制、计费功能。由于很好地结合了以太网的经济性及 PPP 良好的可扩展性与管理控制功能，PPPoE 在包括小区组网建设等一系列应用中被广泛采用。

PPPoE 协议采用 Client/Server 方式，它将 PPP 报文封装在以太网帧之内，在以太网上提供点对点的连接。

PPPoE 有两个阶段：Discovery 阶段和 PPP Session 阶段，具体如下：

- Discovery 阶段

当一个主机想开始 PPPoE 进程的时候，它必须先识别接入端的以太网 MAC 地址，建立 PPPoE 的 SESSION ID。这就是 Discovery 阶段的目的。

- PPP Session 阶段

当 PPPoE 进入 Session 阶段后 PPP 报文就可以作为 PPPoE 帧的净荷封装在以太网帧发到对端，SESSION ID 必须是 Discovery 阶段确定的 ID，MAC 地址必须是对端的 MAC 地址，PPP 报文从 Protocol ID 开始。在 Session 阶段，主机或服务器任何一方都可发 PADT（PPPoE Active Discovery Terminate）报文通知对方结束本 Session。

关于 PPPoE 的详细介绍，可以参考 RFC2516。

PPPoE Server

设备提供了 PPPoE Server 的功能，支持动态分配 IP 地址，提供本地认证、RADIUS/TACACS+等多种认证方式，配合访问包过滤防火墙及状态防火墙，可以对内部网络提供安全保障，适用于校园、智能小区等通过以太网接入 Internet 的组网应用。

这种组网方式需要在用户 Host 上安装 PPPoE 客户端拨号软件。

PPPoE Client

PPPoE 在 ADSL 宽带接入中被广泛使用。通常情况下，一台主机如果要通过 ADSL 接入Internet，必须在主机上安装PPPoE 客户端拨号软件。设备实现了 PPPoE Client 功能（即 PPPoE 的客户端拨号功能），用户可以不用在 Host 上安装 PPPoE 客户端软件即可接入 Internet，而且同一个局域网中的所有 Host 可以共享一个 ADSL 帐号。

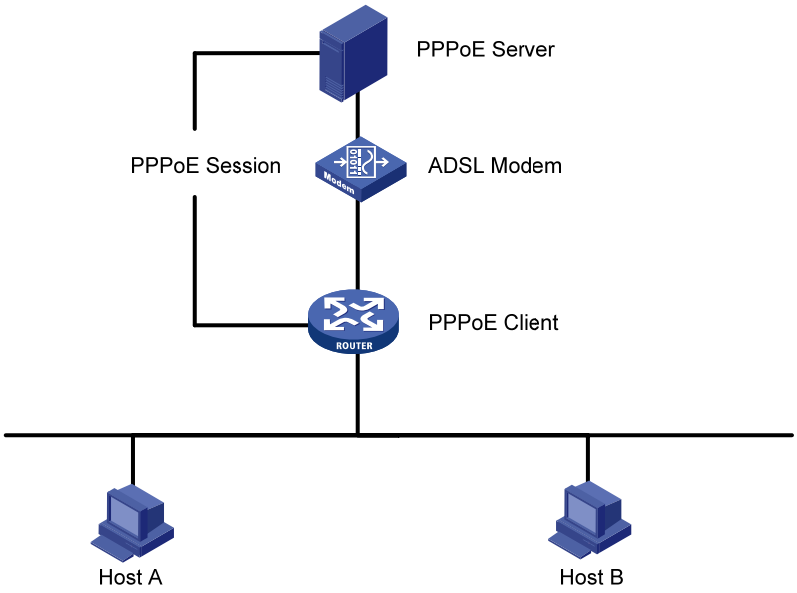

图1 PPPoE Client 典型组网图

从 图 1可以看到：以太网内的计算机连接到设备上，在设备上运行PPPoE Client。上网的数据首先到达设备，再通过PPPoE协议对数据进行封装，经由设备挂接的ADSL Modem到达ADSL接入服务器，最终进入Internet。整个上网过程，不需要用户另外在计算机上安装PPPoE客户端拨号软件就可以实现。