项目 9 广域网技术

主编：钟祥睿等

上海交通大学出版社

目录

单元学习目标

知识目标

1. 了解广域网的基本概念
2. 理解 PPP 的基本概念和工作原理
3. 理解 PAP 和 CHAP 的工作原理
4. 理解 PPPoE 协议的基本概念和报文格式

技能目标

1. 掌握 PPP 的配置方式
2. 掌握 PAP 验证的配置方法
3. 掌握 CHAP 验证的配置方法
4. 掌握 PPPoE 的基本配置方法

一 项目描述

静态路由协议、动态路由协议 OSPF 等只能解决相同自治系统内的网络 IP 数据包的通信，当网络终端处于不同的自治系统的的时候，甚至是像当今的主流使用的互联网的概念；怎么让终端接入到到广域网网络中，例如接入到互联网是计算机网络必须要解决的一个重大问题。这个工作需要定义一个新的网络协议来完成。在任何的网络中，接入广域网是最为核心的内容；当前广域网接入使用的协议主要是以 PPP （ Point to Point Protocol ）协议和专线接入。专线接入一般应用于较为大型的网络中，大多数普通互联网用户接入都是 PPP 协议，如何保障 PPP 协议安全验证及接入就是 ISP （ Internet Service Provider ）与用户之间的主要工作。

二 项目分析

PPP 协议早期主要应用于终端与终端之间的连接，它们使用串行电缆、电话铜线等传统的传输媒介进行通信。当计算终端之间连接之后，两端会发送配置请求， PPP 协议来处理链路控制、数据控制和数据封装。

现在 PPP 协议更多地应用于异步网络的连接，最为典型地就是大量应用到互联网接入。

PPP 协议解决了以下几大网络问题：

1. 具有动态分配地址的能力，解决了 IPV4 地址资源不足，但是部分闲置时间段终端占用地址的问题。

2. 可以支持多种不同的网络通信协议，解决使用不同网络通信协议终端之间的问题；例如 TCP/IP 与 NWLINK 之间的终端。

3. 网络开销小，速度快，且具有身份验证功能；非常适合普通用户接入互联网的业务。

二 项目分析

4. 支持不同传输媒介，从传统的串行电缆、铜线、双绞线到现在的光电和无线传输等。

应用于 PPP 协议安全验证模式有两种， PAP 和 CHAP 协议；网络管理员要理解不同安全验证的基础工作原理，安全验证适用的范围，以及配置的方法。对于常规网络接入用户来说，使用 PPPoE （基于以太网的 PPP 协议）更加广泛，如何熟练掌握 PPPoE 的配置方式以及相对应的安全验证模式、网络通信测试的方法是接下来项目的主要内容。

9.1 广域网

广域网（ Wide Area Network ）简称 WAN ，是指跨越很大地域范围的数据通信网络。广域网通常使用因特网服务提供商（ ISP ）提供的设备作为信息传输平台，对网络通信的要求较高。

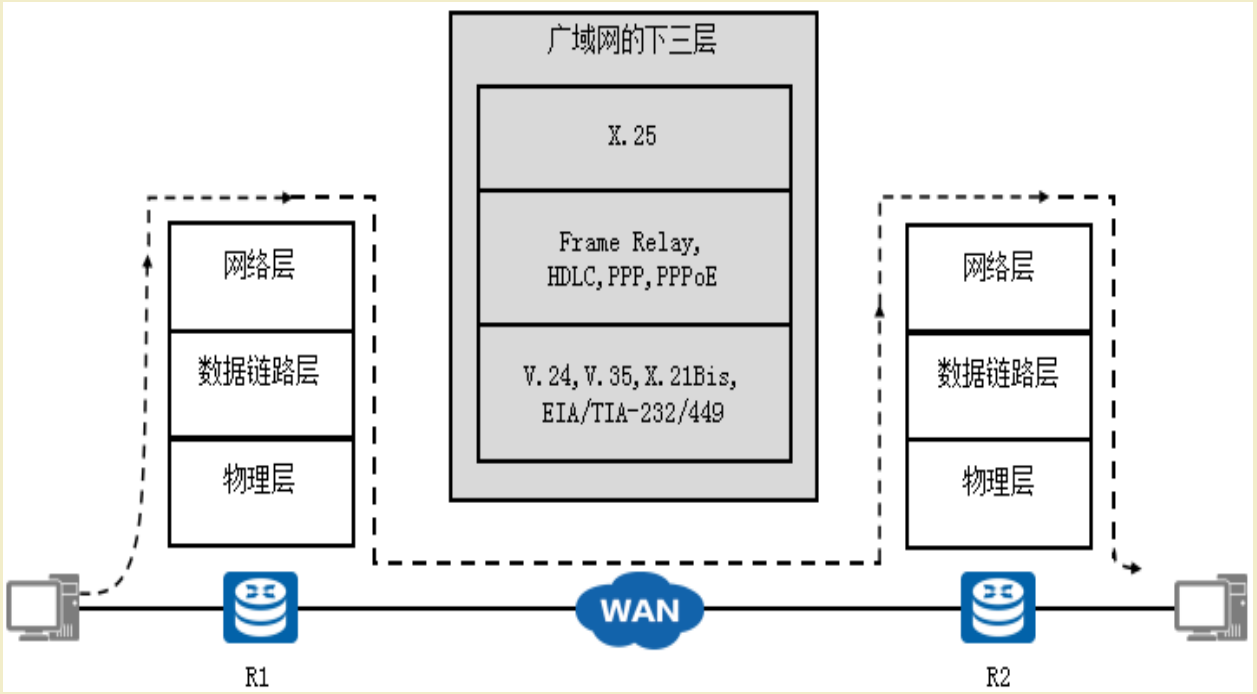


图 9-1 广域网对应的 OSI 三层模型

9.2 广域网接入方式

1.DDN 接入。 DDN 是数字数据网 (Digital Data Network) 的简称。它由光纤、数字微波或卫星等数字传输通道和数字交叉复用设备组成，为用户提供高质量的数据传输通道，传送各种数据业务；

电缆调制解调器远程接入：电缆调制解调器运行在有线电视（ CATV ）的铜轴电缆上，可以提供比传统电话线更高的传输速率；

2. PSTN 公共电话网接入。 PSTN 公共电话网的优点是覆盖区域广、易于使用、价格较低，缺点是网络线路质量较差，传输速率较低；

3. DSL 远程接入。 DSL 称为数字用户线路， DSL 远程接入方式是通过 DSL 调制解调器实现用户数据在传统电话线上的高速传输。 DSL 技术常见的类型包括

ADSL 、 VDSL 、 SDSL 、 HDSL 和 ISDN DSL 等。其中， ASDL

9.2 广域网接入方式

1.DDN 接入。 DDN 是数字数据网 (Digital Data Network) 的简称。它由光纤、数字微波或卫星等数字传输通道和数字交叉复用设备组成，为用户提供高质量的数据传输通道，传送各种数据业务；

电缆调制解调器远程接入：电缆调制解调器运行在有线电视（ CATV ）的铜轴电缆上，可以提供比传统电话线更高的传输速率；

2. PSTN 公共电话网接入。 PSTN 公共电话网的优点是覆盖区域广、易于使用、价格较低，缺点是网络线路质量较差，传输速率较低；

3. DSL 远程接入。 DSL 称为数字用户线路， DSL 远程接入方式是通过 DSL 调制解调器实现用户数据在传统电话线上的高速传输。 DSL 技术常见的类型包括

ADSL 、 VDSL 、 SDSL 、 HDSL 和 ISDN DSL 等。其中， ASDL

9.2 广域网接入方式

1.DDN 接入。 DDN 是数字数据网 (Digital Data Network) 的简称。它由光纤、数字微波或卫星等数字传输通道和数字交叉复用设备组成，为用户提供高质量的数据传输通道，传送各种数据业务；

电缆调制解调器远程接入：电缆调制解调器运行在有线电视（ CATV ）的铜轴电缆上，可以提供比传统电话线更高的传输速率；

2. PSTN 公共电话网接入。 PSTN 公共电话网的优点是覆盖区域广、易于使用、价格较低，缺点是网络线路质量较差，传输速率较低；

3. DSL 远程接入。 DSL 称为数字用户线路， DSL 远程接入方式是通过 DSL 调制解调器实现用户数据在传统电话线上的高速传输。 DSL 技术常见的类型包括

ADSL 、 VDSL 、 SDSL 、 HDSL 和 ISDN DSL 等。其中， ASDL

9.3PPP 协议

PPP 是 Point-to-Point Protocol 的简称，也叫做 P2P，目前是 TCP/IP 网络中最重要的点到点数据链路层协议。

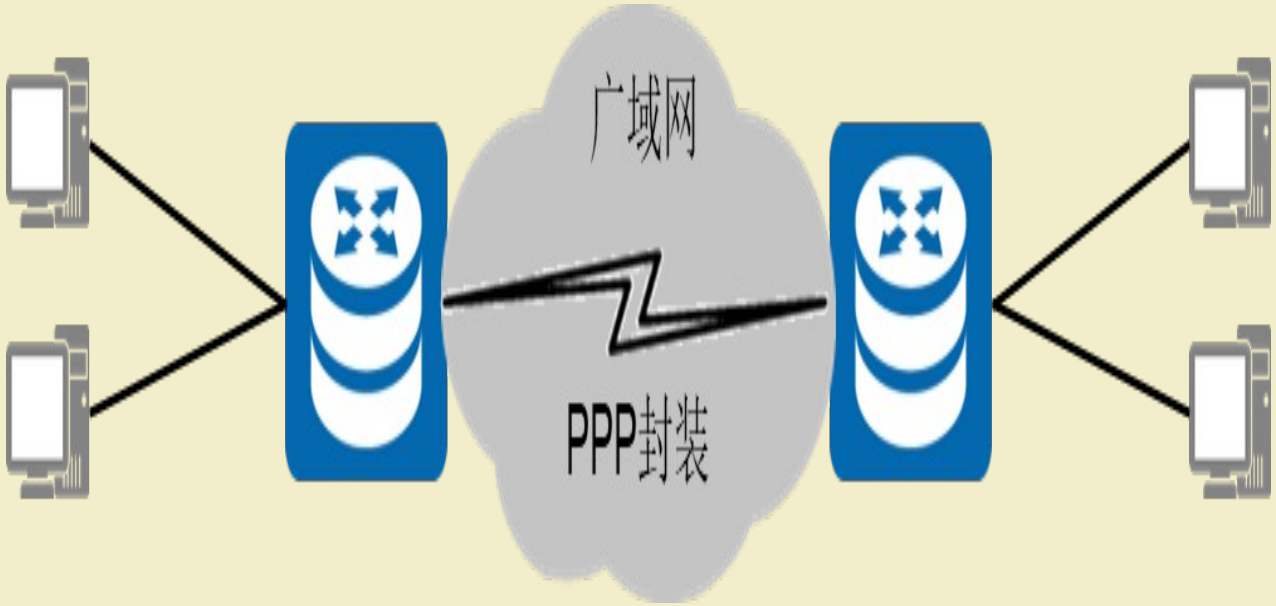


图 9-2PPP 连接

三 相关知识

一、 PPP 成员协议

1. LCP 。链路控制协议 (LCP， Link Control Protocol)，主要用于数据链路连接的建立、拆除和监控； LCP 主要完成 MTU （最大传输单元）、质量协议、验证协议、魔术字、协议域压缩、地址和控制域压缩协商等参数的协商；

2. NCP 。网络层控制协议族 (NCP， Network Control Protocol)，主要用于协商在该链路上所传输的数据包的格式与类型，建立和配置不同网络层协议。

二、 PPP 帧的结构

PPP 是面向字符的，帧的结构包含以下内容。

1. 标志字段，由二进制序列 01111110 组成， 16 进制为 0x7E，指示一个帧的开始或者结束。

2. 地址字段，由二进制序列 11111111 组成， 16 进制是 0xFF，标准的广播地址， PPP 不会指定单个设备的地址。

3. 控制字段，由二进制序列 00000011 组成， 16 进制是 0x03 ，用户数据采用无序帧方式传输。
4. 协议字段，长度为 1 至 2 字节，用于标识被封装于帧中的数据字段里的协议类型。
5. 信息字段，又称为数据字段，长度为 0 至多个字节，默认不超过 1500 字节，包含了符合协议字段中指定协议的数据。
6. 帧校验序列，通常为 2 字节，用于 PPP 帧差错控制。

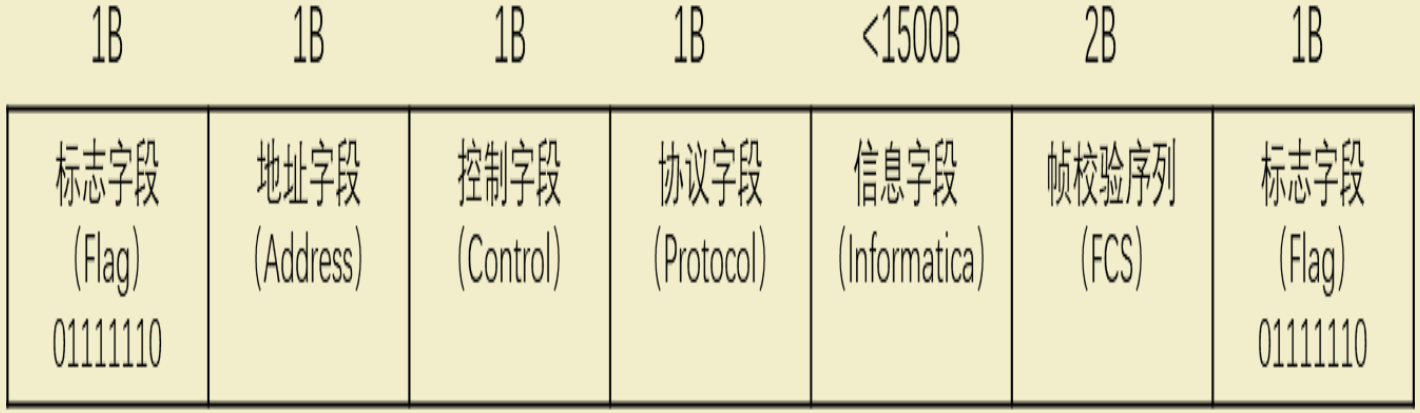


图 9-3PPP 帧的结构

三、 PPP 工作过程

PPP 工作过程分为以下几个阶段：

1. 链路不可用阶段。也称为物理层不可用阶段， PPP 链路都需从这个阶段开始和结束。当通信两端检测到物理链路处于激活状态之时，既会从当前切换到下一阶段（链路建立）。

2. 链路建立阶段。 PPP 协议中最复杂的阶段。这个阶段主要是发送配置报文来配置数据链路，该参数不包括网络层协议所需的参数。一旦完成了数据包的交换之后，就会继续下一阶段的状态，该阶段或许是验证阶段或许是网络层协议阶段。

三 相关知识

在次阶段中， LCP 的状态会发生两次改变；前面所说的当链路不可用时， LCP 的状态处于 initial 或者 starting ， 当检测到链路可用时，物理层会向链路层发送一个 UP 事件，链路收到该事件之后， LCP 的状态会从当前状态改变为 Request-Sent ， 根据此时的状态机 LCP 会进行相应的动作，也即是开始发送 Config-Request 报文来配置数据链路，无论哪一端接收到了 Config-Ack 报文时， LCP 的状态机又要发生改变，从当前状态改变为 opened 状态，进入 Opened 状态后收到 Config-Ack 报文的一方则完成了当前阶段，应该向下一个阶段跃迁。同理可知，另一端也是一样的，但须注意的一点是在链路配置阶段双方是链路配置操作过程是相互独立的。如果在该阶段收到了非 LCP 数据报文，则会的将这些报文丢弃。

3. 验证阶段。多数情况下的链路两端设备是需要经过认证后才进入到网络层协议阶段，缺省情况下链路两端的设备是不进行认证的。在该阶段支持 PAP 和 CHAP 两种认证方式，验证方式的选择是依据在链路建立阶段双方进行协商的结果。然而，链路质量的检测也会在这个阶段同时发生，但协议规定不会让链路质量的检测无限制的延迟验证过程。在这个阶段仅支持链路控制协议、验证协议和质量检测数据报文，其它的数据报文都会被丢弃。如果在这个阶段再次收到了 Config-Request 报文，则又会返回到链路建立阶段。

4. 网络层协议阶段。一旦 PPP 完成了前面几个阶段，每种网络层协议（ IP 、 IPX 和 AppleTalk ）会通过各自相应的网络控制协议进行配置，每个 NCP 协议可在任何时间打开和关闭。当一个 NCP 的状态机变成 Opened 状态时，则 PPP 就可以开始在链路上承载网络层的数据包报文了。如果在个阶段收到了 Config-Request 报文，则又会返回到链路建立阶段。

5. 网络终止阶段。 PPP 能在任何时候终止链路。当载波丢失、授权失败、链路质量检测失败和管理员人为关闭链路等情况均会导致链路终止。链路建立阶段可能通过交换 LCP 的链路终止报文来关闭链路，当链路关闭时，链路层会通知网络层做相应的操作，而且也会通过物理层强制关断链路。对于 NCP 协议，它是没有也没有必要去关闭 PPP 链路的。

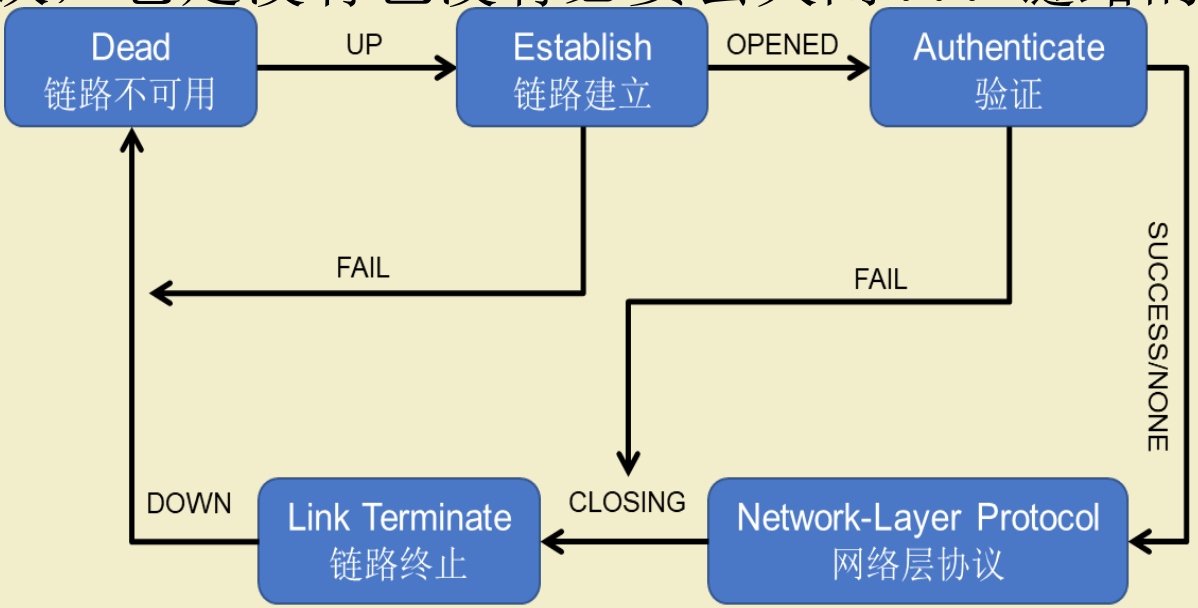


图 9-4PPP 协议过程状态图

9.4PAP 和 CHAP 认证

PPP 协议提供了可选的认证配置参数选项，默认情况下点对点通信的两端是不需要认证的；但是通常情况下都会设置认证模式，通常的设备都具备两种认证协议，分别是 PAP 和 CHAP 。

一、 PAP 认证

PAP （口令验证协议 Password Authentication Protocol ）是一种简单的明文验证方式。 NAS （网络接入服务器， Network Access Server ）要求用户提供用户名和口令， PAP 以明文方式返回用户信息。

PAP 认证是两次握手，链路建立阶段，如果设备配置了 PAP 认证，则验证方在发送配置请求报文会携带认证配置参数选项，对于被验证方则不需要，被验证方只需要收到配置请求报文后根据自身情况给对端返回报文。

。

三 相关知识

图 9-5PAP 协议过程状态图

PAP 这种明文验证方式的安全性较差，第三方可以很容易的获取被传送的用户名和口令，并利用这些信息与 NAS 建立连接获取 NAS 提供的所有资源。所以，一旦用户密码被第三方窃取， PAP 无法提供避免受到第三方攻击的保障措施。

三 相关知识

PAP 的认证过程的配置如下， HUAWEI-1 是验证方， HUAWEI-2 被验证方；配置过程以图 9-5 为例：

认证方建立本地用户数据库，验证被认证方设备是否可以建立连接。

[HUAWEI-1] aaa

[HUAWEI-1-aaa] local-user huawei password cipher huawei@123

[HUAWEI-1-aaa] local-user huawei service-type ppp

认证方启用 pap 认证。

[HUAWEI-1-Serial4/0/0]ppp authentication-mode pap

被认证方配置认证方提供的验证信息，包含用户名、密码、加密模式等信息。

[HUAWEI-2] interface Serial 4/0/0

[HUAWEI-2-Serial4/0/0] link-protocol ppp

[HUAWEI-2-Serial4/0/0] ppp pap local-user huawei password cipher huawei@123

二、 CHAP 认证

CHAP （挑战 - 握手验证协议 Challenge-Handshake Authentication Protocol ）是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。 NAS 向远程用户发送一个挑战口令（ challenge ），其中包括会话 ID 和一个任意生成的挑战字串（ arbitrary challengestring ）。远程客户必须使用 MD5 单向哈希算法（ one-way hashing algorithm ）返回用户名和加密的挑战口令，会话 ID 以及用户口令，其中用户名以非哈希方式发送。

三 相关知识

CHAP 的验证过程相较于 PAP 验证要安全许多。验证方在本地加密当前用户的密码成为密码散列，然后以明文的方式发送自己的账号给被验证方。被验证方收到验证方的验证请求，提取出验证方发送的主机名，然后根据该主机名在被验证方设备的后台数据库中查找相同的用户名记录，一旦找到该记录，则使用该用户名对应的密钥、报文 ID 和验证方发送的随机报文用 MD5 加密算法生成应答，并将应答和自己的主机名送回。当验证方收到被验证方发送回应后，提取被验证方的用户名，然后查找本地数据库，当找到与被验证方一致的用户名后，根据该用户名所对应的密钥、保留报文 ID 和随机报文使用 MD5 加密算法生成结果，与刚刚的验证方所返回的应答进行比较，如果相同返回确认 (Ack)，否则返回否认（ Nak ）。

三 相关知识

CHAP 的认证过程的配置如下， HUAWEI-1 是验证方， HUAWEI-2 被验证方；配置过程以图 9-6 为例：

三 相关知识

（1）认证方建立本地认证数据库

```
[HUAWEI-1] aaa
[HUAWEI-1-aaa] local-user huawei password cipher
huawei@123
[HUAWEI-1-aaa] local-user huawei service-type ppp
[HUAWEI-1-aaa] quit
```

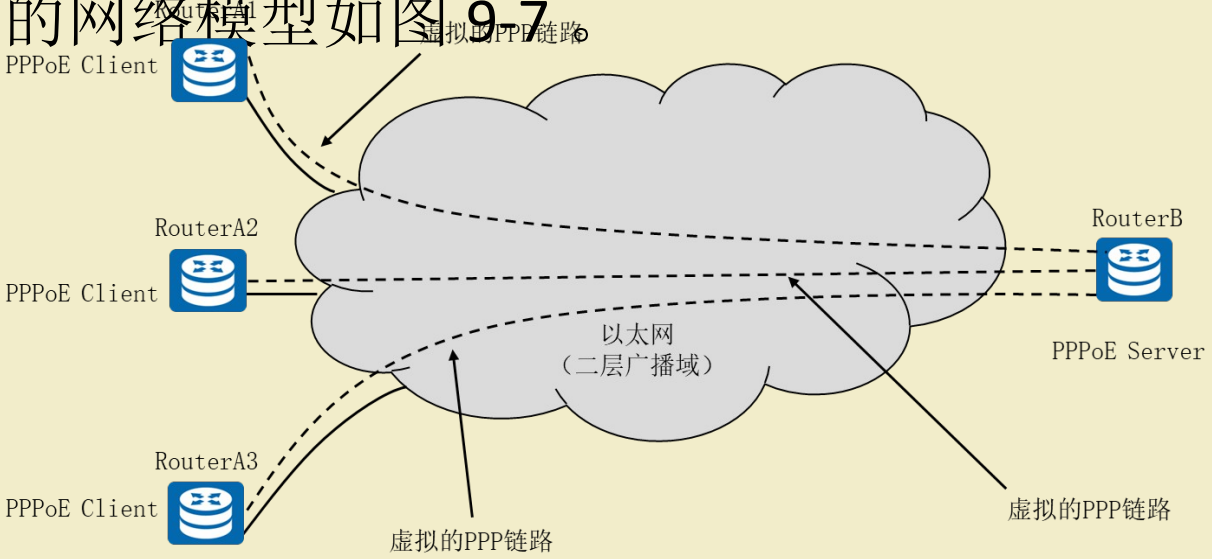
（2）被认证方要求进行 CHAP 认证

```
[HUAWEI-2] interface Serial 4/0/0
[HUAWEI-2-Serial4/0/0] link-protocol ppp
[HUAWEI-2-Serial4/0/0] ppp chap user huawei
[HUAWEI-2-Serial4/0/0] ppp chap password cipher huawei@123
```

三 相关知识

9.5PPPOE

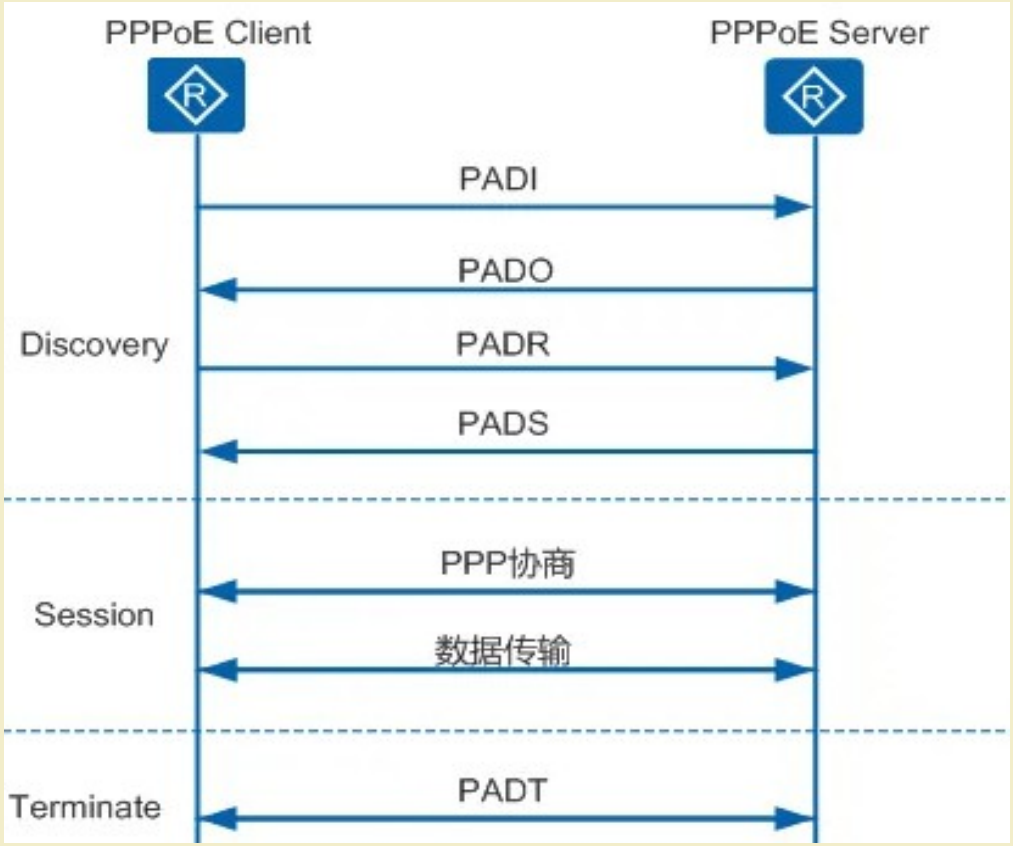
PPPoE （ Point-to-Point Protocol Over Ethernet ），以太网上的点对点协议，是将点对点协议（ PPP ）封装在以太网（ Ethernet ）框架中的一种网络隧道协议。由于协议中集成 PPP 协议，所以实现出传统以太网不能提供的身份验证、加密以及压缩等功能，也可用于缆线调制解调器（ cable modem ）和数字用户线路（ DSL ）等以以太网协议向用户提供接入服务的协议体系。 PPPoE 的网络模型如图 9-7。



三 相关知识

一、 PPPoE 的工作过程

PPPoE 的工作过程分为三个阶段：整个过程如图 9-8 所示。



三 相关知识

1. Discovery 阶段（发现阶段）

在这个阶段，由于客户端不知道服务端 MAC 地址，它将使用类似 ARP 解析过程的机制来获取服务端 MAC 地址，并建立连接，这个过程主要有 4 个步骤：

（1） PADI （PPPoE Active Discovery Initiation）报文：客户端拨号之前，在以太网内只能使用 MAC 地址进行通信，客户端这时会在以太网上广播一个 PADI 报文，这个报文包含有客户端的 MAC 地址。

（2） PADO （PPPoE Active Discovery Offer）报文：当客户端广播了 PADI 报文之后， PPPoE 服务端收到该报文后，会回复一个 PADO 报文，这个报文包含了服务端的 MAC 地址，名称等信息。

（3） PADR （PPPoE Active Discovery Request）报文：当客户端收到服务端的 PADO 报文后，就会发送一个 PADR 报文给服务端，用来确认接受服务端 PADO 报文提供的 PPPoE 连

（4） PADS （PPPoE Active Discovery Session Configuration）报文：客户端发送的 PADR 报文由服务端的 PADS 报文进行再确认，并会携带一个会话 ID；这时候就可以完成一个完整连接了。

2.Session 阶段（会话阶段）

一旦服务端和客户端都知道对端的 MAC 地址之后，这时候就进入了会话阶段。它可分为两部分： PPP 协商阶段和 PPP 报文传输阶段。 PPP 协商阶段和普通 PPP 协商方式一致，具体流程同 PPP 协商流程，如下图 9-9 所示。 PPPoE Session 的 PPP 协商成功后，就可以承载 PPP 数据报文。在这一阶段传输的数据包中必须包含在发现阶段确定的 Session ID，并保持不变。

3. 会话终结阶段

在 PPPoE 中定义了一个 PADT 报文用来结束会话， PPPoE 客户端或者 PPPoE 服务端可以在会话开始后的任何时候通过发送 PADT 报文来结束会话。

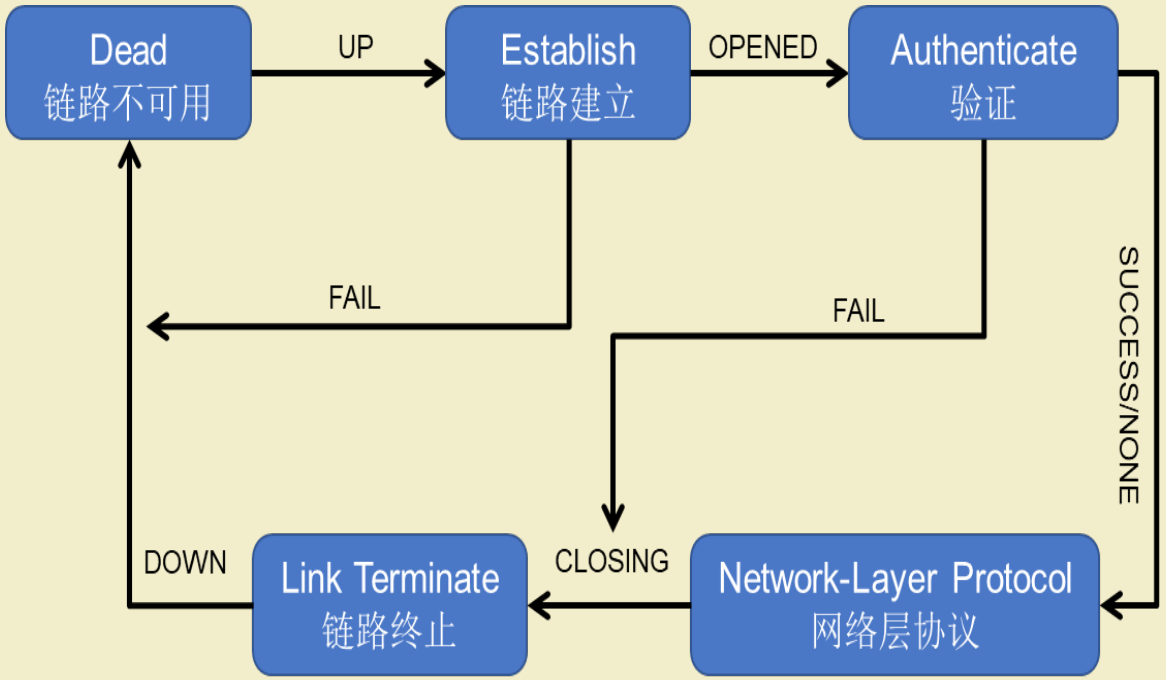


图 9-9 PPPoE 会话阶段过程

9.6 PPP 协议配置命令

一、 link-protocol ppp

link-protocol ppp　　# 用于配置接口封装的链路层协议为 PPP

undo link-protocol ppp　　# 用于删除接口封装的 PPP 协议

二、 ppp authentication-mode

ppp authentication-mode　　# 用于配置本端设备对对端设备的认证方式

undo ppp authentication-mode　　#用于恢复缺省情况

缺省情况下，本端设备对对端设备不进行认证。命令格式为：

ppp authentication-mode { chap | pap }

undo ppp authentication-mode

三、 ppp chap user

ppp chap user　　# 用于配置 CHAP 验证的用户名

undo ppp chap user　　# 用于删除 CHAP 验证的用户名

缺省情况下， CHAP 认证的用户名为空。命令格式为：

ppp chap user username

undo ppp chap user

四、 ppp chap password

ppp chap password　　# 用于配置 CHAP 验证的口令

undo ppp chap password　　# 用于删除配置的口令

缺省情况下，未配置 CHAP 验证的口令。命令格式为：

ppp chap password { cipher | simple } password

undo ppp chap password

四 项目实施及总结

具体实施过程参考实训报告

【项目总结】

本项目详细介绍了广域网常见协议的工作原理及应用，主要学习了以下知识内容。

1. PPP 协议广泛应用于广域网与局域网的链接，安全认证模式两种；分别是 PAP 协议和 CHAP 协议。

2. CHAP 协议的加密模式比 PAP 模式更加安全可靠，当前主流应用技术以 CHAP 为主。

3.PPPoE 协议应用广泛，大量应用于计费上网，用户认证等形式的网络。

4. PPPoE 协议具有可以防止 ARP 欺骗对网络的影响，可以提高网络的可靠性。

谢谢！