**接入控制实验系统方案设计与实现**

**、**

陈静

ccjing93@gmail.com

目录

[一、PPPoE协议运行原理 3](#_Toc450684073)

[二、RADIUS协议与RSA模型的运行 4](#_Toc450684074)

[三、网络拓扑设计 5](#_Toc450684075)

[PPPoE+RADIUS远程接入控制环境搭建 6](#_Toc450684076)

[四、配置流程 7](#_Toc450684077)

[1. pppoe服务器配置流程： 7](#_Toc450684078)

[2. radius服务器具体配置流程： 7](#_Toc450684079)

[3. radius客户机的配置流程： 8](#_Toc450684080)

# 一、PPPoE协议运行原理

用户 PC 上必须运行 PPPoE 虚拟拨号程序。在用户 PC 和 PPPoE 服务器之间运行 PPPoE 协议，PPPoE 服务器对接入用户进行接入控制。PPPoE 服务器和 RADIUS 服务器之间运行 RADIUS 协议，由 RADIUS 服务器实现对用户的集中仲裁管理。

基于 PPPoE 协议的接入控制实质上是通过在以太网上运行 PPP 协议，在每个以太网站点与 PPPoE 服务器之间建立一条 PPPoE 虚拟连接，每个虚拟连接具有唯一标识，通过虚拟连接实现以太网单个用户到 PPPoE 服务器之间的端到端通信。PPPoE 服务器通过虚拟连接就可以实现对以太接入的单个用户进行接入认证、授权和记账。

PPPoE 协议操作分为两个阶段：PPPoE 发现阶段和 PPP 会话阶段。PPPoE 发现阶段完成以太网中 PPPoE 的会话建立，PPP 会话阶段则是在已建立的 PPPoE 会话中传送 PPP 帧。

 PPPoE 发现阶段

在 PPPoE 发现阶段，主机可能发现多个 PPPoE 服务器，但只在发现的所有 PPPoE 服务器中选择一个来建立 PPPoE 会话。发现阶段的操作如图 所示。

Figure

**单播PADO**

主机

PPPOE

接入服

务器

1

.

广播

**广播PADI**

2

.

单播

PADO

3

.

* 播

PADR

4

.

单播

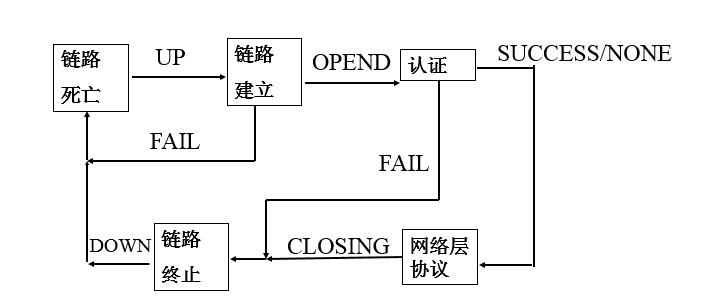
PADS

**单播PADR**

**单播PADS**

* 主机广播一个 PADI(有效发现启动)分组，寻找合适的 PPPoE 服务器。
* PPPoE 接入服务器收到其服务范围内的 PADI 后，如果可以向发送请求的主机提供服务时就会回应一个 PADO(有效分组发现提供)，否则不做任何回应。
* 主机收到 PADO 分组后，根据分组中的信息选择一个合适的接入服务器，然后向所选择的 PPPoE 服务器发送 PADR(有效发现请求)分组。
* PPPoE 服务器收到 PADR 分组后准备开始 PPPoE 会话，为该会话产生一个唯一的会话标识，并在 PADS(有效发现会话证实)分组中将该会话标识交给主机。

 **PPP** 会话阶段

PPPoE 发现阶段结束后，主机和 PPPoE 接入服务器之间建立点到点隧道，进入会话阶段。在会话阶段，PPP 帧封装在 PPPoE 帧中，而 PPPoE 帧封装在 Ethernet 帧中，通过以太接入网承载、运送。

Figure

* 链路建立阶段

客户机与PPPoE/S间：由LCP完成

建立请求、协商MRU、认证协议、链路质量监测协议，从而建立数据链路。

* 认证阶段

客户机与PPPoE/S间：由LCP和CHAP类认证协议协作完成

PPPoE/S与Radius/S间：由Radius协议完成

对用户身份的鉴别，若认证通过，则证明是合法的用户。

* 网络层协议阶段

客户机与PPPoE/S间：由NCP（IPCP）完成

对网络层协议进行配置，进行网络层地址（IP地址）分配

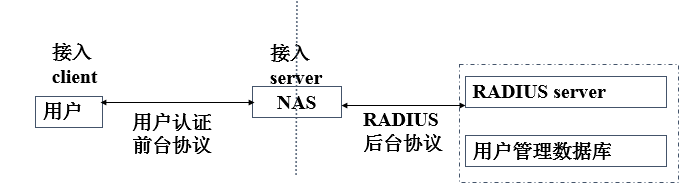
* 链路终止阶段

客户机与PPPoE/S间：由LCP完成

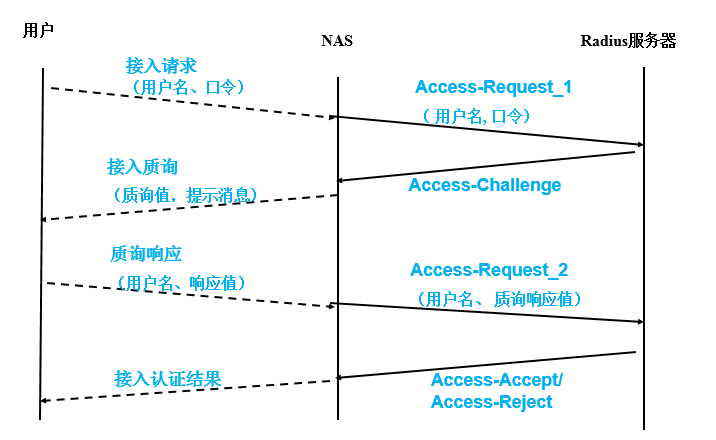
可以在任何时候终止链路，链路的正常终止由LCP分组完成，一个NCP的关闭不一定引起链路的关闭。

# 二、RADIUS协议与RSA模型的运行

RADIUS (Remote Authentication Dial In User Service) 拨号用户远程认证服务，是一种通用的、广泛使用的实现AAA功能的协议，对接入用户提供认证授权和记账功能，且支持对漫游用户的接入控制，作用于NAS与RADIUS服务器之间，但并不直接定义用户与NAS之间的前台认证协议，可以与多种前台协议协同工作。此处NAS为pppoe服务器



Figure

RADIUS服务器有请求/响应方式和质询/响应方式两种工作方式，由于本实验采用CHAP认证协议，故只介绍质询/响应方式

Figure

交互过程：

* 用户：将用户名和口令信息发到NAS
* NAS：将用户认证信息转发给RADIUS服务器
* RADIUS服务器：发送质询值Challenge
* NAS：将质询值Challenge转发给用户
* 用户：将用户名和由计算得到的质询响应值发给NAS
* NAS： 将用户名和质询响应值转发给RADIUS服务器
* RADIUS服务器：验证用户的合法性并予以适当授权，发送Access-Accept或Access-Reject
* NAS：接受后台授权，控制用户接入

# 三、网络拓扑设计

## PPPoE+RADIUS远程接入控制环境搭建

#### 1）拓扑如下：



图2 pppoe+radius 远程接入控制环境拓扑

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 虚拟机编号 | 操作系统 | 网卡数 | 网卡 | 配置模式 | 地址 | 功能 |
| 1 | xp | 1 | Eth0 | Host only | 192.168.2.11/24 | pppoe客户端 |
| 2 | xp | 1 | Eth0 | Host only | 192.168.2.22/24 | pppoe客户端 |
| 3 | ubuntu | 3 | Eth0 | Host only | 192.168.2.2/24 | Pppoe服务器 |
| Eth1 | Host only | 192.168.3.3/24 | Radius客户端 |
| Eth2 | briadge | 192.168.1.108/24 | 连接internet |
| 4 | ubuntu | 1 | Eth1 | Host only | 192.168.3.2/24 | Radius服务器 |

#### 2）通信实现过程：

1. 客户机在进行PPPoE拨号的发现阶段，发出广播帧PADI以发现PPPoE服务器， PPPoE服务器能从有线网卡0接口收到该广播帧并回复PADO。然后客户机又单播PADR，PPPoE单播回复PADS，至此，完成发现阶段，建立了虚拟隧道连接。
2. 后续会话阶段PPPoE服务器接收到客户提供的账号密码信息，从有线网卡1接口转交给RADIUS服务器认证 RADIUS服务器接收并处理，具体过程如Figure 4。
3. 在拨号成功的情况下，用户访问外网服务器，发送请求报文，该请求报文到达PPPoE服务器时，PPPoE服务器进行NAT从网卡2接口发送。外网服务器接收到PPPoE服务器转发的报文后发送响应报文PPPoE服务器接收到响应报文后，再经过NAT转换从有线网络接口发送，最终发送请求的客户端收到该响应报文。

# 四、配置流程

这里只放配置流程图，具体配置命令见文档《pppoe服务器的配置》、《Radius服务器的安装》、《PPPoE添加对Radius的支持》

## 1. pppoe服务器配置流程：



## 2. radius服务器具体配置流程：

## 3. radius客户机的配置流程：