基于RADIUS的校园网认证管理系统的研究与实现

梁 根
(茂名学院 信息与网络中心,广东 茂名 525000)

摘 要:介绍了RADIUS协议的结构,讨论了其认证的工作过程。以校园网实际应用为例,建立了RADIUS认证计费服务器的网络架构和功能模型。根据PPPoE接入认证计费的特点,对开发中的数据库关键问题进行了详细分析,解决了校园网拨号认证和计费的问题。

关键词:RADIUS;网络接入服务器;认证;授权;数据库
中图分类号:TP393.09 **文献标识码**:A **文章编号**:1673-629X(2006)06-0043-02

Research and Implementation of Campus Network Certification Management System Based on RADIUS

LIANG Gen
(Information and Network Center, Maoming College, Maoming 525000, China)

Abstract: The structure and process of RADIUS are introduced. The network framework and functions of RADIUS server are given based on campus network application. The key problems of RADIUS database are also discussed based on the characteristic of PPPoE NAS. The problems of campus network authorization and accounting are solved.

Key words: RADIUS; NAS; certification; authorization; database

0 引 言

远程认证拨号接入用户服务(Remote Authentication Dial In User Service,RADIUS)协议是用户通过公用交换电话网、综合业务数字网、PPPoE或者其他线路访问Internet的认证、授权与计费的一种协议。

文中在校园网的RADIUS服务器的设计实现当中,成功地将RADIUS协议应用于校园网PPPoE接入服务器(PPPoE Networks Access Server,PPPoE NAS)。该方法具有通用性,可广泛应用于各种加密通信当中,特别是在网络用户数比较多和网络架构比较复杂的情况下,将敏感数据进行加密传输,实现用户身份的认证和计费,为网络数据提供了一定程度的安全保证,提高了用户认证的效率,并且具有良好的性价比。

1 RADIUS协议简介

RADIUS是一种C/S结构的协议[1],它的客户端通常是NAS(Net Access Server)服务器。RADIUS协议认证机制具有多样性,可以采用多种认证方式,如:PAP,CHAP。RADIUS进行的全部工作都是基于Attribute-Length-Value向量进行的,因此它的可扩展性非常好,可以满足多种应用需求。标准RADIUS认证端口号是1812,计费端口是1813。一个完整的RADIUS数据包是被封装在UDP的数据域中。RADIUS协议包的格式[2]如图1所示。

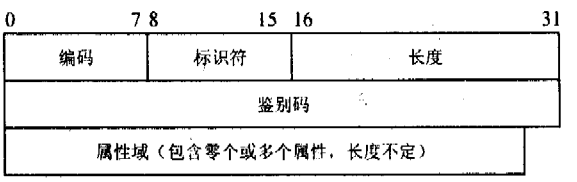

图1 RADIUS协议包格式

1)编码域是一位字节,确定RADIUS数据包的类型。RADIUS协议中指定了9种类型的编码,有接入请求(Access-Request)、接入允许(Access-Accept)、接入拒绝(Access-Reject)、记账请求(Accounting-Request)、记账回应(Accounting-Response)、接入询问(Access-Challenge)、服务器状态(Status-Server)、客户机状态(Status-Client)、保留(Reserved)9种类型。其中接入请求、接入允许、接入拒绝3种类型用于认证;记账请求、记账回应用于计费;服务器状态、客户机状态常作为保留。

2)标识符域是一个字节,用于比较请求与回复。如果在一个很短的时间片段里,一个请求有相同的客户源IP地址、源UDP端口号和标识符,RADIUS服务器会认为这是上一个重复的请求。

收稿日期:2005-09-29
基金项目:广东省自然科学基金资助项目(05011896)
作者简介:梁 根(1979-),男,广东高州人,硕士研究生,助工,主要研究方向为网络协议及应用。

3)长度域是两个字节。它指明了包括编码、标识符、长度、鉴别码和属性域在内的整个数据包的长度。在数据包长度以外的字节位在接收时可以忽略它。如果包的长度比指定的短,则此包会被直接丢弃。数据包的最小长度是20,最大长度是4096。

4)鉴别码域是十六个字节。鉴别码是被用于验证数据包的正确性,在请求和回复中都要用到。对于鉴别码不正确的报文,通常在接收时会直接丢弃。

5)属性域包含了零个或多个属性。每个属性,即Attribute-Length-Value向量,在请求和回复中携带详细的认证、授权、信息和配置细节。

2 系统设计与实现

2.1 校园网接入和认证的网络架构

基于RADIUS认证的校园网络架构如图2所示。

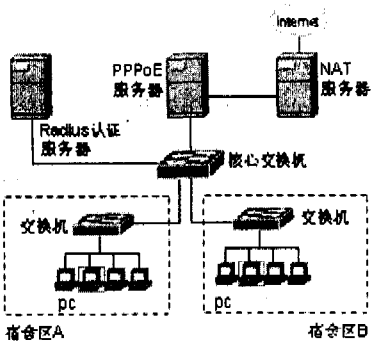

图2 RADIUS认证的网络架构

基于RADIUS认证的校园网主要由PPPoE服务器(NAS)和RADIUS服务器组成[3],以下为校园网用户上网认证的基本工作流程:

(1)用户上网接入NAS,NAS向RADIUS服务器发送认证请求(Access-Require)数据包提交用户信息,包括用户名、密码等认证信息,其中用户密码是经过MD5加密的,双方使用约定的共享密钥;

(2)RADIUS服务器对用户名和密码的合法性进行检验,如果服务器采用挑战式握手方式验证,会提出一个Challenge,要求对用户认证,也可以对NAS进行类似的认证,否则直接进行验证;

(3)如果验证合法,给NAS返回认证通过(Access-Accept)数据包,允许用户进行下一步工作,如果验证不通过返回认证拒绝(Access-Reject)数据包,拒绝用户访问;

(4)在验证合法情况下,NAS向RADIUS服务器提出计费请求(Account-Require),RADIUS服务器做出计费响应(Account-Accept),对用户的计费开始,同时用户可以进行自己的相关操作。

2.2 系统功能模块

本系统主要由3大功能模块组成,如图3所示:

(1)认证。认证部分是核心部分[4],NAS服务器向RADIUS服务器提交账号和密码,RADIUS服务器在后台MySQL数据库中查找,如果用户名和密码正确,就向客户端返回IP、掩码、DNS、NAS服务器IP地址等信息,然后客户端才能上网。

(2)用户管理。该部分主要是对上网用户各种信息进行存储,并且提供一个Web界面给上网用户修改密码和查询费用,系统管理员在该部分有最高的权限,可以对用户进行管理和查看系统操作日志。

(3)计费。目前茂名学院实行的是包月计费,上网用户交款后,管理员可以通过Web界面直接操作交费,大大地减轻了工作的负担。

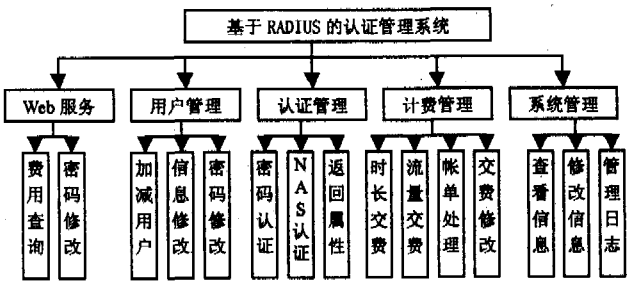

图3 校园网认证计费管理系统的主要功能模块

2.3 数据库设计

在本系统中,后台数据库使用MySQL,MySQL作为一个开源的软件,可以运行在各种平台中。下面设计了创建RADIUS后台数据库表[5]的程序:

```
CREATE TABLE radacct ( //创建账号登录信息表
    RadAcctId bigint(21) NOT NULL auto_increment,
    UserName varchar(64) NOT NULL default '', //账号名称
    NASIPAddress varchar(15) NOT NULL default '', //NAS的IP地址
    AcctStartTime datetime NOT NULL default '0000-00-00 00:00:00',//账号生效时间
    AcctStopTime datetime NOT NULL default '0000-00-00 00:00:00',//账号失效时间
    AcctAuthentic varchar(32) default NULL, //RADIUS
    ServiceType varchar(32) default NULL, //Framed-User
    FramedProtocol varchar(32) default NULL, //PPP
    FramedIPAddress varchar(15) NOT NULL default '', //客户端的IP地址
    PRIMARY KEY (RadAcctId),
    KEY UserName (UserName),
    KEY FramedIPAddress (FramedIPAddress),
    KEY AcctStartTime (AcctStartTime),
    KEY AcctStopTime (AcctStopTime),
    KEY NASIPAddress (NASIPAddress) );
CREATE TABLE radcheck ( //创建账号检查表
    id int(11) unsigned NOT NULL auto_increment,
    UserName varchar(64) NOT NULL default '', //账号名称
    Attribute varchar(32) NOT NULL default '', //属性值,包括密码、账号生效和失效时间
    op char(2) NOT NULL DEFAULT '==',
    Value varchar(253) NOT NULL default '',
```

(下转第47页)

查找到系统SPI程序的WSPStartup函数的指针,通过这个指针就可以将自己服务提供者的WSPStartup函数和系统SPI程序的WSPStartup函数相关联,进而调用系统的各个服务提供者函数。在插入的这一层传输服务提供者中,实现对特定数据包的过滤与封装[5]。

应用程序在调用WINSOCK API函数时,WSPStartup通过一个被当作参数投送的函数派遣表打开另外的30个SPI函数,传输服务提供者便由这30个函数组成。每个API函数都映射到对应的SPI函数。而我们只关注建立TCP连接,发送UDP包所调用的几个重要的API函数,如Connect,sendto等,在插入的SOCKS5传输服务提供者的相应SPI函数中做特殊处理。而其他WINSOCK API函数所对应的SPI函数不需要重新编写。

客户端运行时,首先将设置好的特定目标服务器IP表读入共享内存,所有目的IP在此表中的数据包即是需要代理转发的数据包。在Connect函数对应的SPI函数WPSConnect中,首先进行这样的判断,如果目的IP在表中,说明该连接的数据包需要代理转发,则发起到指定SOCKS5服务器的连接,进行身份认证,启动SOCKS5协议的Connect模式,从而实现TCP包的代理转发。对于不需要转发的数据包,则直接调用下一层基础服务者SPI接口,由系统服务提供者完成默认的功能。在sendto函数对应的WSPSendTo函数中,也要进行类似的对UDP包的判断和处理,对于需要代理转发的数据包,依照SOCKS5协议执行身份认证,启动UDP ASSOCIATE模式,对每一个UDP数据包加上特定的头信息。而值得注意的是,SOCKS5协议必须通过TCP方式进行通信。要发送穿透SOCKS5代理服务器的UDP数据包,其实首先需要建立客户端到代理服务器的TCP连接,通过一系列的交互,获得代理服务器的许可才能够发送出去(同时代理服务器也记录下客户端IP和端口),也确保从远端发回的数据能够通过代理服务器发回给某个UDP客户端(因为它登记了一个关于SOCKET UDP的通路映射)。所以为了发送UDP数据,必须建立和保持这个TCP连接。不能在取得代理服务器的通道后就关闭TCP连接。

本方案已经成功应用于一种商用的网络游戏集中计费系统中,即在客户机上运行该客户端,将所有发往需要计费的网络游戏服务器IP的数据包截取并转发到指定SOCKS5服务器上,SOCKS5服务器通过监控记录SOCKS5认证用户名,客户机IP,建立连接的时间、时长,目标服务器IP,端口等信息,完成分析和计费。而对客户完全透明。该方案为类似的基于有选择的代理服务器透明转发的相关应用提供了一种思路。

参考文献:

[1] 朱雁辉.Windows防火墙与网络封包截获技术[M].北京:电子工业出版社,2002.

[2] Jones A,Ohlund J.Network Programming for Microsoft Windows[M].US:Microsoft Press,2000.

[3] 汪国洋,王景中.基于SPI的访问控制技术[J].计算机应用,2003,23(6):267-269.

[4] Microsoft Corp.MSDN[Z].2001.

[5] 胡　滨.Windows下使用SPI过滤网络数据包[J].华中科技大学学报(自然科学版),2003,31(增刊):169-170.

(上接第44页)

```
    PRIMARY KEY (id),
    KEY UserName (UserName(32)) );
  CREATE TABLE radgroupcheck ( //创建组检查表
    id int(11) unsigned NOT NULL auto_increment,
    GroupName varchar(64) NOT NULL default '', //可以按照楼层来划分组
    Attribute varchar(32) NOT NULL default '', //属性值,包括组号、NAS标识
    op char(2) NOT NULL DEFAULT '==',
    Value varchar(253) NOT NULL default '',
    PRIMARY KEY (id),
    KEY GroupName (GroupName(32)) );
  CREATE TABLE radreply ( //创建由RADIUS返回给客户端的属性表
    id int(11) unsigned NOT NULL auto_increment,
    UserName varchar(64) NOT NULL default '', //认证账号
    Attribute varchar(32) NOT NULL default '', //返回属性,包括给客户端返回的IP
    op char(2) NOT NULL DEFAULT '=',
    Value varchar(253) NOT NULL default '',
    PRIMARY KEY (id),
    KEY UserName (UserName(32)) );
```

3　结束语

文中设计了一种基于RADIUS协议的校园网认证计费管理系统的方法,经过茂名学院校园网的长期测试表明,本系统长时间运行稳定、可靠,处理能力达到每秒250个接入认证。同时由于采用了后台数据库技术,增加了系统的可靠性、可用性和可伸缩性,能够实现在FreeBSD,Linux等各种平台上运行。

参考文献:

[1] Rigney C.RFC 2866,Radius Accounting[S].2000.

[2] RFC 2865,Remote Authentication Dial In User Service(RADIUS)[S].2000.

[3] 陶智勇.综合宽带接入技术[M].北京:北京邮电大学出版社,2002.75-83.

[4] 唐　磊,金连埔.大型拨号认证计费服务器的设计与实现[J].计算机工程与设计,2004(7):160-161.

[5] 赵　宇,刘　刚,杨宗凯.一种基于Linux的Radius客户端的设计与实现[J].计算机工程,2003(9):113-114.