基于RADIUS的拨号上网认证、计费和管理

军事医学科学院网络信息中心　赵东升　孙焕东

本文以某园区网拨号网络服务系统的建设为例，讨论如何基于RADIUS进行拨号网络用户的集中统一管理，介绍我们开发的用户自动计费和访问监控管理系统的实现。

随着Internet和Intranet应用的日益普及，越来越多的企业和机构已经有了局域网。出于安全或其他因素的考虑，很多企业不希望用户通过Internet出口访问自己的内部网络，需要建立自己的拨号服务器，为用户提供拨号网络服务。然而，管理大量分散的拨号设备和用户是一项复杂而费时的工作，如何统一集中地管理它们、确保网络安全运行，是网管部门的重要任务。

RADIUS（Remote Authentication Dial-In User Service-远程认证拨入用户服务）国际标准的推出，为拨号用户的统一管理提供了便利的途径。本文以某拨号网络服务系统的建设为例，讨论基于RADIUS的拨号网络的管理，介绍我们开发的用户自动计费和访问监控管理系统的实现。

RADIUS的基本原理

RADIUS是由朗讯公司提出的客户／服务器安全协议，现已成为Internet的正式协议标准（RFC 2138、2139和2200），为众多网络设备制造商所支持。安全信息集中存放在RADIUS服务器中，RADIUS客户（各种拨号网络服务器设备）与RADIUS 服务器通信，以认证用户、进行用户授权和保存计帐信息。RADIUS不仅是协议标准，更多的情况表示整个客户／服务器系统。

1.RADIUS认证

RADIUS 对拨入的远程访问用户进行认证。认证信息可以存放在本地文件中，也可以通过外部的认证机制如操作系统的口令文件得到。认证（authentication）和授权（authorization）过程的数据流向如图1所示。当用户bob试图登录到拨号访问服务器PortMaster（它在这里作为RADIUS客户端）上时，会发生下列的认证过程：

(1)PortMaster提示bob输入他的用户名和口令，bob输入用户名和口令后，PortMaster在自己的本地用户表中比较该“用户名－口令”对。

(2)如果①本地用户表中没有该用户名② bob登录的端口需要安全检查③ PortMaster被设置为使用RADIUS服务器，则PortMaster向RADIUS服务器发送一条“访问请求”消息，消息中包含RADIUS服务器用来认证该用户所需要的信息。

(3)RADIUS服务器查看它的数据库中是否存在用户bob。

(4)根据不同情况，用户bob可能被接受或拒绝：

如果bob的用户名和口令与RADIUS数据库中的项匹配，且“访问请求”中的其他附加属性（如访问类型）也与数据库中该项的附加属性匹配，则RADIUS服务器向PortMaster发送一条“访问－接受”消息，通知PortMaster 用户bob已被成功地认证。该消息中还包括bob能够访问的服务、bob的连接配置等用户授权信息。“授权”控制用户对特定网络服务的访问。一旦用户被认证，RADIUS服务器通知PortMaster该用户允许访问那些网络服务。例如，bob 可被授权使用PPP连接，使用动态分配的IP地址192.168.0.201。

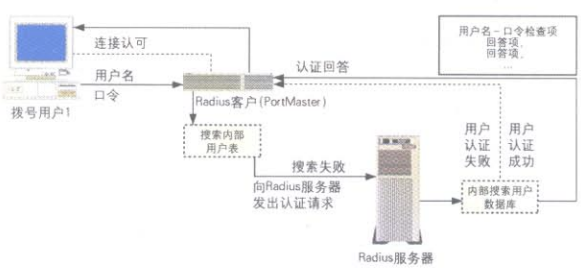

图 1　RADIUS认证过程

如果口令不对或附加的检查失败，则RADIUS服务器向PortMaster发送一条“访问－拒绝”报文以指示认

证过程失败。PortMaster收到该报文后，终止与bob的连接。为了防止用户口令等信息在传输中被非法窃取，RADIUS将需要传输的信息进行加密处理（使用MD5算法）。

2.RADIUS计帐

RADIUS的计帐功能记录拨入连接的各种信息，这些信息通常用于计费。RADIUS 计帐包括下面的过程:

(1)RADIUS客户向RADIUS服务器发送“计帐请求”报文，其中包含了与计帐有关的事件信息。

(2)RADIUS服务器在收到“计帐请求”报文后，向RADIUS客户发送“计帐响应”报文。

(3)如果RADIUS客户在给定的时间内没有收到“计帐响应”报文，则继续发送“计帐请求”报文，直到它收到RADIUS服务器的响应或请求的次数超过了事先定义的阈值。

(4)RADIUS客户使用一种回退算法决定重复请求的时间间隔。“计帐请求”报文中包含RADIUS客户发送该报文的时刻和对应事件发生时刻的时间差，称为“计帐延迟时间”（Acct-Delay-Time)。

(5)每当一个用户拨入RADIUS客户后，RADIUS客户就向RADIUS服务器发送一条“开始”报文，该报文通常包含“会话Id”、“用户名”、“服务类型”、“登录类型”、“登录客户IP地址”、“报文发送时间”、“计帐延迟时间”以及其他相关信息，RADIUS服务器将收到的每条记录写入一个文本文件或数据库表中。

(6)每当一个用户断开连接后，RADIUS客户就向服务器发送一条“结束”报文，该报文除了包含“开始”报文中的字段外，还包含“会话时间”字段（即该次连接持续的时间，按秒计算)。

某园区网拨号网络服务系统总体结构

1.网络结构

该拨号网络系统是一个大型园区网络的子系统，为用户通过电话拨号上网、访问因特网和园区网内的公共服务器提供支持。拨号上网方案采用“多号连一”方式，即若干条外线捆绑在一起，可用一个号码拨入。使用三台3Com公司的USR Netserver Plus/16拨号访问服务器作为网络接入设备，共有48条33.6Kbps的接入线路，可支持500个用户。使用一台运行Windows NT4.0的服务器作为RADIUS服务器，同时作为代理和电子邮件服务器。自主开发了访问监控和自动计费软件。

考虑到网络安全的问题，对拨号用户的访问权限进行了限制，而且用一个独立的子网将拨号网络和园区网的内部网络进行隔离。拨号用户的IP地址都是动态分配的临时内部IP地址，只能直接访问园区网络公共网段上的公共服务器，而对Internet的访问只能通过代理服务器完成。

2.软件系统结构

一般的RADIUS服务器软件对用户计费只是将访问记录写入文件中，没有用户费用的计算、查询功能，用户帐号的管理也不方便。为了实现用户和Internet访问的管理自动化，我们自主开发了集用户信息、Internet访问与机时统计、邮件记录等功能于一体的拨号用户访问监控系统。该系统的主要功能包括:

(1)管理拨号用户的一般信息。

(2)统计用户的访问机时、上网费用等。

(3)对用户访问资料自动记录并长期备份。

(4)对超时用户实行自动关闭／开启，并自动发送邮件通知。

(5)支持用户通过WWW修改口令、查询上网时间和剩余机时等自我管理功能为实现上述功能，该系统由多个子系统组成，它运行于多台服务器上。主要包括:

(6)客户端拨号上网信息管理子系统：用于管理拨号用户的一般信息

(7)服务器端拨号用户数据访问子系统：为前者提供数据库访问支持

(8)拨号用户计费和访问监控子系统：完成访问监控和自动计费

(9)服务器端Web服务子系统：为用户通过WWW修改口令，查看费用提供服务

系统实现

1.用户管理子系统的实现

用户的一般信息管理采用传统的C/S结构实现，以SQL Server6.5作为数据库服务器，由该服务器上的用户数据访问子系统提供客户对SQL6.5数据库请求访问。当客户端的信息管理子系统需要访问拨号用户数据库时，它做出请求，由服务器端的数据访问子系统形成响应数据集，返回给客户端，客户端的信息管理子系统最终完成用户的请求输出。在具体实现时做了以下工作:

(1)建立了运行于MS SQL Server6.5上的用户信息数据库，包括拨号用户资料库、用户交费收费库、用户拨号机时统计库及用户收发邮件信息库。

(2)用C++Builder实现用户信息系统的管理界面，具有用户信息的录入、修改、查询、打印、统计、邮件通知等功能，从而实现对用户信息库的有效管理。C++Builder不仅是优秀的C++语言开发平台，还提供了数据库访问接口。它的多层数据库应用构件MIDAS是实现网上远程数据库访问的有效手段。我们利用MIDAS构件实现客户端对数据库服务器的访问，用户仅需安装客户端管理程序，就可以访问数据库，不需要对客户端进行数据库配置。

(3)建立基于MIDAS的服务器端数据库访问子系统。

2.计费和访问监控子系统的实现

计费和访问监控子系统是一个运行于Windows NT上的服务器程序（后台程序），用C++ Builder编写，负责用户访问的计费和监控，把用户访问信息和邮件信息记录到数据库中，并对没有访问费的用户实行关闭（在交费后开启），从而完成自动计费。为了方便用户的使用，当一个用户的剩余机时（或费用）下降到一个给定的值后，系统自动向该用户发送电子邮件，提醒该用户补交网络费。实现要点如下：

(1)借助于RADIUS生成的计费和认证记录，完成对拨号用户的访问计费。RADIUS服务器把拨号用户访问的开始与结束时间写入文件或数据库中，然而它所写入的记录却不能直接用于用户计费。一般地，RADIUS遇到用户拨入时写入一条开始记录，用户断开时写入一条结束记录。但是，经常出现一些难以区分的情况：结束记录有多条、同一会话的结束记录时间不同、结束记录的会话时间不相同等等。我们使用了一些智能化的处理方法，使所有拨号认证的记录都保证得到正确的处理，保证拨号上网的合理计费。

(2)利用MS SDK for Windows NT实现用户的自动开启和停用。通过C++Builder可以使用MS SDK编程，我们用它设计了用户帐号的开启和停用、用户帐号认证、用户更改口令等功能。一旦出现用户超量超时，系统就会自动关闭用户，从而大大地减轻了网管人员的劳动强度。

(3)通过MS Proxy2.0代理服务器记录访问日志。用户的访问信息都记录到MS SQL数据库中，然后再由程序进行必要的自动处理。记录在数据库的访问信息是经过筛选的，仅保留用户所访问的有效资料。

(4)用MS Exchange5.5记录邮件访问日志。邮件服务信息记录在两类数据文件中：一类文件是每天一个，记录每天该服务器收发邮件的用户信息，包括邮件的发信地址、收信地址、信件字节数据等。另一类文件记录用户的信息内容，每封用户信件占一个文件，其文件名也记录在前一类日志文件中。我们用前一类日志文件来获得用户邮件的收发地址、信件字节数，并把它存入数据库中，这也可以用于计算邮件的数据量。

3.Web服务子系统的实现

Web服务子系统完成用户通过WWW浏览器对服务器及其数据库进行访问，使拨号用户可以经常检查自己的访问机时，以及修改用户密码。用户甚至还可以即时检查你到那些站点访问过，与那些用户进行了电子邮件联系。

通过C++Builder设计ActiveX构件，从而使用户通过浏览器实现更改口令和数据库查询。利用在ASP中编写脚本代码实现对数据库的查询。由于VB Script不支持直接调用SDK函数，我们用C++Builder设计实现了一个具有更改口令功能的ActiveX控件，嵌入在ASP页面中，在IIS服务器端执行。

结束语

随着用户对网络服务要求的进一步提高，网管也需要更加自动化、智能化。我们将进一步研究开发这方面的新技术、新举措，使对网络用户的管理更完善，使用户对Internet的访问更方便。■

参考文献

1 Remote Authentication Dial In User Service (RADIUS). RFC2138. 1997年4月

2 RADIUS Accounting. RFC2139. 1997年4月

3 孙焕东，赵东升，代炼忠. 一个企业级网的网络管理系统. 计算机系统应用. 1999. 2. 11-13