基于RADIUS协议的校园网AAA系统研究

孟 敏,周临震
(盐城工学院 优集学院,江苏 盐城 224051)

摘要:针对校园网现有的远程访问控制的网络安全问题,利用标准RADIUS协议属性的可扩展性,对RADIUS认证服务器进行扩展,实现了能够与802.1X客户端配合通告处理原因和处理结果的RADIUS服务器,同时根据所改进的RADIUS服务器,搭建了校园网的AAA认证系统,提高了校园网运行的性能和效率。

关键词:RADIUS;AAA服务器;通知消息
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1671-5322(2008)04-0018-04

目前,我国校园网的网络规模正急剧膨胀。网络用户的快速增长,关键性应用的普及和深入,校园网在学校的信息化建设中扮演着至关重要的角色,同时它的发展具有以下特点:(1)信息点多,网络规模大。校园网中往往要容纳七八千甚至数万个学生,因此需要对上万个节点进行管理;(2)网络流量峰值明显,应用丰富,网络负载重;(3)网络安全问题非常突出。由于学生对计算机的维护情况差别比较大,病毒和网络攻击比较猖獗;(4)传统的校园网没有提供相应的认证机制,任何用户能够不受控制的进入网络访问资源,并且对于IP地址盗用和MAC地址盗用的现象十分常见。

随着校园网络建设的发展,原有的网络管理和手段暴露出一系列的不足,严重地影响了网络的正常运行,成为网络安全的主要隐患。因此,必须采取相应的安全措施来接受合法校园网络接入用户,屏蔽非法校园网络接入用户,从而保护校园网络安全,为达到这些目标,就需要能够对连接到校园网中的用户进行身份认证和授权功能,即如何保证远程访问控制的网络安全。

远程访问控制的安全包含三方面的内容:认证、授权和计费[1]。本文主要在FreeRADIUS软件的基础上进行二次开发,根据标准的RADIUS协议的可扩展性,实现AAA系统的认证,提高系统的安全性。

1 AAA系统相关技术

1.1 AAA技术

AAA是Authentication(认证)、Authorization(授权)和Accounting(计费)的缩写,其应用在以太网上,通过对NAS接入网络的用户完成认证、授权功能,支持多种用户类型和业务属性,提供灵活的计费方式,设置用户的业务信息和资费信息,支持SNMP(Simple Network Management Protocol)后台数据库对AAA服务器程序保持透明。AAA技术具有以下3个功能:

(1)认证:对请求服务的用户进行身份认证。当作为AAA服务器客户端的NAS(Network Access Server)接收到包含有用户名和密码等认证信息的接入请求后,将其转换成特定协议的接入请求数据包发送给AAA服务器,服务器然后将该用户信息与自身服务区的数据库进行比较,确定用户的合法性,然后将结果通过NAS返回给用户。

(2)授权:对通过认证的用户根据相关协定分配网络资源,包括服务类型限制、宽带大小、IP地址等。该过程有时候与上述的认证过程整合,将授权结果作为认证结果的一部分返回给用户。

(3)计费:收集并记录用户对相关网络资源的使用状况,并根据收费策略对用户进行收费。不同的网络运营商有不同的收费策略,目前主要有两种,分别是资源占用时间和数据流量。

收稿日期:2008-09-07
作者简介:孟敏(1981-),女,江苏盐城人,助教,硕士,主要研究方向为网络与信息安全。

随着 Internet 新技术与新服务的出现,AAA 技术也在不断发展,出现了很多支持 AAA 服务的协议,目前比较流行的是 RADIUS 协议。

1.2 RADIUS

RADIUS(Remote Authentication Dial - In User Service)是远程用户拨号系统的简称,它是定义在网络接入服务器 NAS 和集中存放认证信息的 RADIUS 服务器之间传输认证、授权和配置信息的协议。RADIUS 协议采用 Client/Server 模式,是 TCP/IP 的应用层协议,在传输层每个 RADIUS 数据包都封装在 UDP 报文中,进而封装进 IP 包在网络上传输。

RADIUS 不仅指运行于服务器上的软件,还包括网络访问服务器与 RADIUS 服务器之间的交互操作协议。其中 RADIUS 协议是远程拨号接入用户服务的简称,是当前新兴的一种管理标准,主要用于对所处地域分散,数量大以及上网条件差别不一的串行线用户以及拨号接入的远程用户的认证、授权和计费的管理。

2 通知消息下发的设计

2.1 RADIUS 属性扩展

RADIUS 协议[2] 包主要由 Code、Identifier、Length、Authenticator 以及 Attributes 几个字段组成,以下是一个标准的 RADIUS 数据包的格式,如图 1 所示,各个域都按照从左到右的顺序在网络中传送。

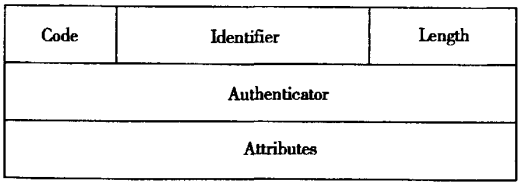

图 1　RADIUS 数据包格式

Fig. 1　Data format of RADIVS

(1)Code 域占一个八位字节,用来标识 RADIUS 包的类型,当收到的包的编码域无效时,该数据包将被自动丢弃。

(2)Identifier 域占一个八位字节,是用来匹配请求和响应包的标识符;每对请求包和应答包的 Identifier 应一致。如果服务器接收到的包具有相同的客户端源 IP 地址,源 UDP 端口号,且在很短的时间内出现了相同的标识符,服务器将认为这是一个重复的请求。

(3)Length 占两个八位字节,它是 Code、Identifier、Length、Authenticator 和 Attributes 的总长度即整个包数据的长度。包的最小长度是 20,最大长度是 4 095。如果包的实际长度小于 Length 域的数值,则直接丢弃该包;如果包的长度超过 Length 域给出的数值,则超出的部分忽略不考虑。

(4)Authenticator 占 16 个八位字节,用来鉴别客户端和 RADIUS 服务器端间的信息。认证码有两种:Request Authenticator 和 Response Authenticator。RADIUS 服务器和 NAS 的共享密钥与请求鉴别码和应答鉴别码一起支持发、收报文的完整性和认证。

(5)属性域(Attributes)不限定长度,它携带着用户的信息。RADIUS 数据包的长度域指示了属性列表的结束处。属性域可能包含多个实例,用于描述 RADIUS 协议的属性。在这种情况下,同种类型的各个属性的排列应当保持一定的顺序,而不同类型的各个属性的排列顺序可以是任意的。其中属性扩展的数据格式如图 2 所示:

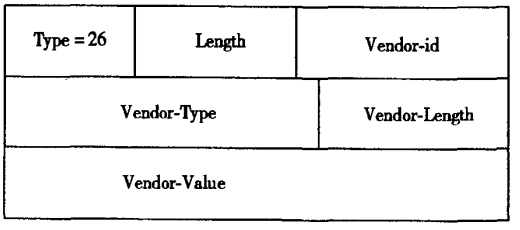

图 2　扩展属性的数据格式

Fig. 2　Data format of private attribute

其中 Vendor - id 在网络字节顺序中,高位的字节是 0,低 3 位字节是供应商的(SMI)网络个人管理器编码。Value 应按 Vendor - Type/Vendor - Length/Vendor - Value 顺序编码,Vendor - Value 域取决于厂商对这个属性的定义。

一个属性可能包含多个实例,在这种情况下同种类型的各个属性的排列应当保持一定的顺序。但是不同类型的各个属性排列顺序是任意的。同时并不是每个标准属性都可以被指定用来携带私有信息的,当前程序中设定允许用来携带私有信息的标准属性标号为:10 - 12、14 - 23、29 - 30、33 - 39、50 - 59、62 - 78、82 - 91。当使用 26 号属性携带私有信息时,Vendor - Type 的值范围是 1 ~ 255,只要不重复使用就可以了。

2.2 通知消息

通知消息主要是在用户发送认证计费请求时下发,AAA 服务器对每个到来的认证请求包进行分组处理,通常有两个分组处理方式:Authorization 和 Authentication[3]。

(1)Authorization:这一步是从外部数据源(如 file,database,LDAP 等)获得用户的信息,检查请求分组中的信息是否足够认证该用户。Authorization modules 是与数据源打交道的,所以 LDAP,SQL,files,passwd 等都是 Authorization modules。在 Authorization 阶段决定下一步 Authentication 所采用的认证方法,用 reply 属性列表来体现。

(2)Authentication:这一步就是简单的比较用户请求中的认证信息是否和服务器中存放的内容一致。通常认证要处理密码加解密,所以 PAP,CHAP,MS-CHAP 都是 Authentication modules。

在 Authorization 和 Authentication 处理过程中,FreeRADIUS 支持 3 个 RADIUS 属性:

(1)request items list:存放 FreeRADIUS 接收到的认证请求分组中的属性;

(2)config items list:存放用于 FreeRADIUS 服务器内部操作的属性,比如说 Authorization 模块向 Authentication 模块传送的 Auth-Type 等。这些类似于 Auth-Type 的属性不属于标准 RADIUS 协议,不能封装到 RADIUS 消息中。

(3)reply items list:存放用来应答 NAS 的属性,将被放入应答分组中。Authorization 和 Authentication 模块都可以向此列表增添属性值对。

在 FreeRADIUS 中,所有通知消息的下发都是依赖 Reply-Message 属性来实现。根据 Authentication 认证流程可知道 Reply-Message 所带的信息都保存在 reply items 中,因此在 reply items 中加入所需的信息即可实现通知消息的下发。

3 基于 RADIUS 的 AAA 系统实现

本文开发的 AAA 系统采用了面向对象、平台无关等设计方法,使系统具有很好的扩展性和可移植性。图 3 为本文的 AAA 系统应用架构图。

图 3 的 RADIUS 为 AAA 服务器,是通过对 FreeRADIUS 软件二次开发实现的。AAA 服务器的认证和计费接口各采用一个 UDP 端口号,通过监听来自这两个端口的 Client 请求,若有 RADIUS 请求消息到来,则把它们加入到请求队列的空闲位置中,等待服务器处理。

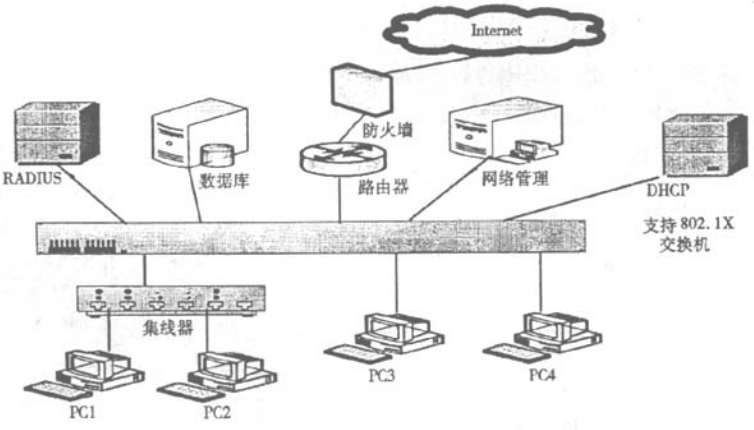

图 3 基于 RADIUS 的 AAA 系统应用架构图

Fig. 3 Application arohitecture of AAA system based on RADWS

网络接入服务器 NAS 是包含了 AAA 客户机程序的服务器,可以是交换机也可以是 PC 机。AAA 客户机程序可以将用户或系统管理员提交的消息封装成 RADIUS 包,并通过相应的端口转发给 AAA 服务器。当用户 PC 发出接入请求时,网络接入服务器 NAS 中的 AAA 客户机程序收集用户信息并提供给 AAA 服务器进行认证。若认证成功,则允许用户接入网络,同时客户机程序向 AAA 服务器发计费开始请求,启动计费进程。当用户停止接入时,再由客户机程序向 AAA 服务器发终止计费请求,停止计费。网络接入服务器可以处理多个用户的请求,且 AAA 服务器也可以同时处理多个接入请求。

AAA 系统的各个模块共享一个用户数据库。

数据库中存储系统配置数据、用户的认证、授权和计费信息数据等,所有系统模块都依赖于这个数据库。本文采用MySQL数据库作为用户数据库,MySQL是一个多用户、多线程SQL数据库服务器。它由一个服务器守护程序mysqld和很多不同的客户程序和库组成。

AAA服务器通过外置用户管理服务器来管理数据库中的用户。通常情况下是AAA服务器监听用户管理请求,这些请求可以是增加或添加用户,改变用户的用户类型、业务类型、计费方式等等,对恶意用户的黑名单管理也通过此服务进行。管理员也可以通过此服务器来查询各个用户的信息。

本文开发的用于校园网的AAA系统,通过NAS接入网络的用户完成认证、授权功能,支持多种用户类型和业务属性,提供灵活的计费方式,设置用户的业务信息和资费信息,支持SNMP;后台数据库对AAA服务器程序保持透明。

4　结束语

本文在研究AAA相关技术的基础上,开发了适用于校园网环境的基于RADIUS协议的AAA系统,系统中的RADIUS服务器实现了RADIUS协议的处理,完成认证信息和计费信息的采集,它是整个系统的核心处理模块,同时能与802.1x客户端配合通告处理原因和处理结果。该系统实现了对校园网进出外网,或外网进出Internet的用户进行认证、授权和访问控制。

参考文献:

[1] 刘涛.浅谈高校校园网络安全[J].工程论坛,2005(19):95-96.

[2] 吴伟斌.校园网AAA系统的设计与实现[J].中国教育网络,2007(2):27-29.

[3] Kim H,Afifi H. Improving mobile authentication with new AAA protocols[J]. IEEE International Confernce on Communications(ICC03),2003:497-501.

Research on Campus Network AAA System Based on RADIUS Protocol

MENG Min,ZHOU Lin-zhen

(UGS College of Yancheng Institute of Technology, Jiangsu Yancheng 224051, China)

Abstract: Aiming at solving the problems of remote access to the control of network security, which exist on campus network, this paper, using the extension of standard RADIUS attributes, improves the RADIUS authentication system, and implements the RADIUS server which can accord with the 802.1X client to handle reasons and results of operations. Meanwhile, this paper, based on the improved RADIUS server, constructs the campus network AAA authentication system, which can enhance the campus network performance and efficiency.

Keywords: RADIUS; AAA Server; Information Message

(责任编校:张英健;校对:沈建新)