一种网络设备账号管理授权的设计与实现①

李 睿, 周相兵, 李 丽

(阿坝师范高等专科学校 网管中心, 汶川 623002)

摘 要: 针对局域网内的设备账号管理和远程操作所出现的问题, 本文设计实现一种基于 Radius 协议的网络设备账号管理的授权策略, 其通过在 Freeradius 开源软件上实现整个局域网内的设备统一管理、授权、协调和修改, 以提高整个局域网内的设备管理授权效率.

关键词: Radius; 局域网; 密码管理授权; Freeradius; 网络设备

Design and Implementation of Network Device Account Management Authorization

LI Rui, ZHOU Xiang-Bing, LI Li

(Network Management Center of ABa Teacher's College, Wenchuan 623002, China)

Abstract: In response to problems associated with account management and remote operation of LAN devices, the paper implements a Radius based authorization strategies for account management of network facilities. Through unified management, authorization, coordination and modification of devices within the entire LAN using the open-source software of FreeRadius, the proposed schemes achieve improved authorization efficiency for management of all LAN devices.

Key words: Radius; LAN; account management; account authorization; Freeradius; network device

1 引言

当前局域网已广泛应用到各个领域中, 但采用什么技术来实现局域网多设备的账号授权管理一直都存在操作复杂、工作量大等问题, 当然所使用的技术也有多种[1,2]; 特别是当网络设备增加、管理员增多的情况下, 怎样实现快速、有效地对网络设备账号进行统一管理、授权、协调和修改, 以及提高整个网络的安全性和扩展性, 这就是本文所解决的问题, 其通过开源软件 Freeradius[3]来设计实现这些要求. 相关文献也对基于 Radius 协议技术进行了分析, 在文献[3]作者基于 Freeradius 实现了网络中的认证、访问控制和记录; 在文献[4]中作者通过采用 Radius 解决了校园网中对用户进行安全、高效的认证和访问控制的问题. 而本文所采用 Radius 协议不但能解决安全、认证和控制问题, 还可用来解决网络设备管理账号授权问题.

2 Radius协议及开源实现概述

Radius 协议是在 IETF 的 RFC 2865 中定义的, 主要分为认证、授权和计费三个部分[5]. Radius 是一种分布式的基于 UDP 的消息交互协议, 它定义了基于 UDP 的 RADIUS 帧格式及消息传输机制, 并规定 UDP 端口 1812 作为认证端口. RADIUS 最初仅是针对拨号用户的 AAA 协议, 后来随着用户接入方式的多样化发展, RADIUS 也适应多种用户接入方式, 如以太网接入、ADSL 接入. 而目前在网络管理技术上, RADIUS 基本属性可以用来为网络设备对管理员进行认证, 其扩展应用可以用于对网络管理员进行授权.

同时, 为了快速有效的应用 RADIUS, 一款基于 RADIUS 的开源软件 Freeradius 出现了[6], 它一般用来进行账户认证管理、记账管理、上网账户管理、鉴权记账等; 它包含一个 radius server 和 radius client 来对支持 radius 协议的网络设备进行鉴权记账. 通常, Freeradius 是一个模块化、高性能、功能丰富的一套 Radius 程序, 由服务器、客户端(radius client)、开发库和一些相关的 radius 工具组成, 具体表现就是由一个 Radius 服务器, 一个 BSD 协议授权的客户端库, 一个

① 基金项目:阿坝师专青年基金(ASC12-24)

收稿时间:2013-07-31;收到修改稿时间:2013-08-26

PAM 库和一个 Apache 的模块构成.

3 基于Radius的账号管理授权设计

基于 RADIUS 协议的账号管理授权设计如图 1 所示，它由四个实体：管理员(Admin)、管理终端(Terminal)、NAS、Radius 服务器(Server)组成[7]. 这就使得与账号的本地认证方式不同: 当网络设备收到用户 Telnet/SSH 登陆传出的账号时，不在本地进行认证，而是向 Radius 服务器发出认证、授权请求，服务器通过验证账号和密码的合法性来决定是否允许用户登入网络设备. 因此，只要在服务器上设置、更改、删除相应的账号、密码，就能更改全网网络设备的登入账号、密码.

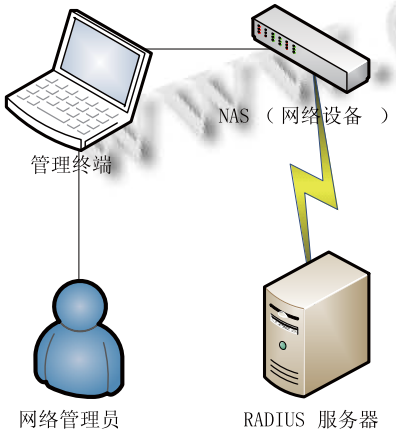

图 1 RADIUS 认证示意图

3.1 基于 RADIUS 协议的授权方案设计

当前 Radius 协议只能提供基于访问控制列表(ACL)的授权功能[8]，基于该功能实现对不同的网络管理员授权管理不同的网络设备. 如何实现对网络管理员操作命令授权的精细管理？目前业内有企业实现了该功能，比如思科的 Tacacs+能实现基于特定命令的壳式(Shell Command)授权，但是 Tacacs+是私有协议，只能在 CISCO 的设备上使用，不能被广泛使用. 基于 radius 的实现方案是利用该协议的 26 号属性进行扩展开发. 开发思想为: 在 RADIUS Authorization Server 的 Dictionary 数据库中创建 26 号属性表，该表有 3 个字段构成，分别是: 用户名(username)、CLI 命令和匹配方式. 用户字段用于存储管理员的账号, CLI 命令字段用于存储网络设备命令，匹配方式字段有 3 个值(精确匹配、匹配 CLI 命令首部、匹配 CLI 命令任一部分). 当 RADIUS Authorization Server 收到网络设备发过来的 Access-Request(Type=26)报文，将该报文拆包，取出用户名、将执行的 CLI 命令等信息，再将这些信息与 Dictionary 数据库中 26 号属性表进行匹配，判断属于那种匹配方式，若与匹配字段的匹配方式相同，那么向网络设备返回认证接受包(Access-Accept)，网络设备执行该命令；若不相同，则返回认证拒绝包(Access-Reject)，网络设备拒绝执行该命令.

3.2 基于 RADIUS 协议的认证、授权流程

基于 RADIUS 协议的认证、授权流程如图 2 所示，当网络管理员通过 TELNET/SSH 发起连接请求时向网络设备发送用户名和密码. 网络设备的 RADIUS client 截获用户名和密码，并向 RADIUS Authentication Server(主)发送认证请求包(Access-Request)，其中的密码在共享密钥的参与下由 MD5 算法进行加密处理. RADIUS Authentication Server(主)收到 Access-Request 包后对用户名和密码进行认证. 如果认证成功，RADIUS Authentication Server(主)向 RADIUS client 发送认证接受包(Access-Accept)，管理员输入 CLI 命令；如果认证失败，则返回认证拒绝包(Access-Reject)，用户登出；如果网络设备在等待一定时间后没收到 RADIUS Authentication Server(主)的响应包，则向 RADIUS Authentication Server(备)发送认证请求包(Access-Request). RADIUS Authentication Server(备)收到 Access-Request 包后对用户名和密码进行认证. 如果认证成功，RADIUS Authentication Server(备)向 RADIUS client 发送认证接受包(Access-Accept)，管理员输入 CLI 命令；如果认证失败，则返回认证拒绝包(Access-Reject)，用户登出；如果网络设备在等待一定时间后没收到 RADIUS Authentication Server(备)的响应包，则自行处理，进行本地认证.

网络管理员被网络设备通过认证后，可以在管理终端如 SecureCRT 中输入 CLI 命令，网络设备收到命令后，将命令封装到 Access-Request(Type=26)包中，发送给 RADIUS Authorization Server，RADIUS Authorization Server 将用户名和 CLI 命令在 Dictionary 数据库中进行匹配，如果允许该管理员执行该命令，则向网络设备返回认证接受包(Access-Accept)，网络设备执行该命令；如果不允许该管理员执行改命令，则返回认证拒绝包(Access-Reject)，管理员输入下一条命令；如果网络设备在等待一定时间后没收到响应包，

则在本地处理该命令.

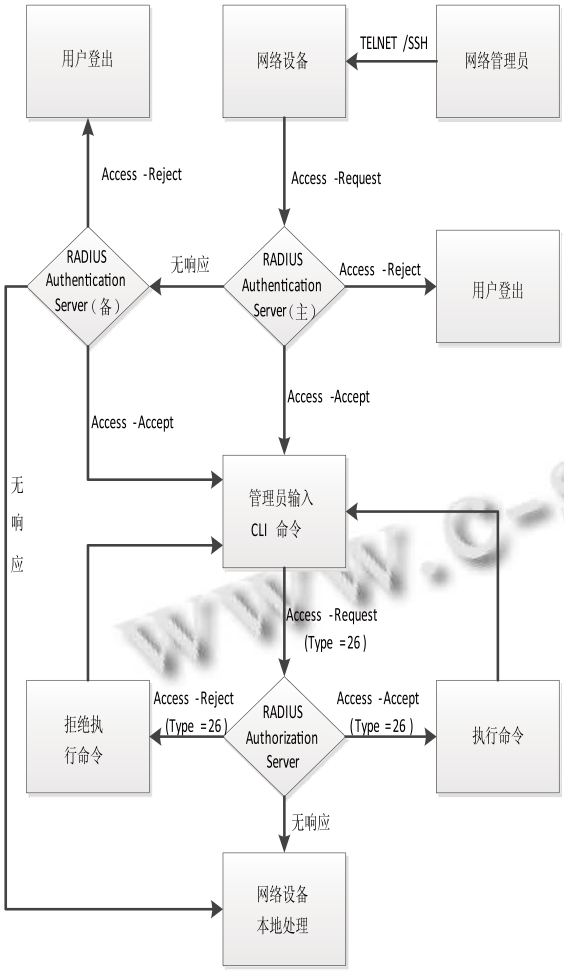

图 2　基于 RADIUS 协议的认证、授权流程结构

4　系统实现及验证

4.1　系统分析

本文采用 Freeradius 作为 RADIUS Authentication Server 和 RADIUS Authorization Server, 为实现上述认证、授权策略, 笔者在 Freeradius 开源代码的基础上做了相应的开发. Freeradius 有三个重要的组成部分, 分别是: Radius 守护进程、配置模块和管理接口. Radius 守护进程主要功能是实现 Radius 协议, 因此它是开发的重点. 配置模块和管理接口与本文关系不大, 在此不再阐述.

图 3 是 Freeradius 的工作流程图, 系统初始化工作主要是读取和解释系统配置文件, 对系统运行环境参数进行设置, 创建客户端和使用者列表, 创建 socket 等准备工作. 接着加载各个功能模块, 主要是认证和授权功能模块. 然后, 系统打开监听 socket(默认是 1812 和 1813 两端口), 随后开始监听, 当系统监听到 Access-Request 报文, 将其数据包的源地址在数据库中进行比较, 若该地址不存在于数据库中, 则丢弃 Access-Request 报文, 系统返回继续监听 socket; 若该地址存在于数据库中, 则认为是有效 client 发送的 Access-Request 报文, 随后系统开始处理 Access-Request 报文, 处理报文之前先检测 Access-Request 报文是否有效, 若报文无效, 则丢弃 Access-Request 报文, 系统返回继续监听 socket; 若报文有效, 系统处理报文后向客户端发送相应的响应报文.

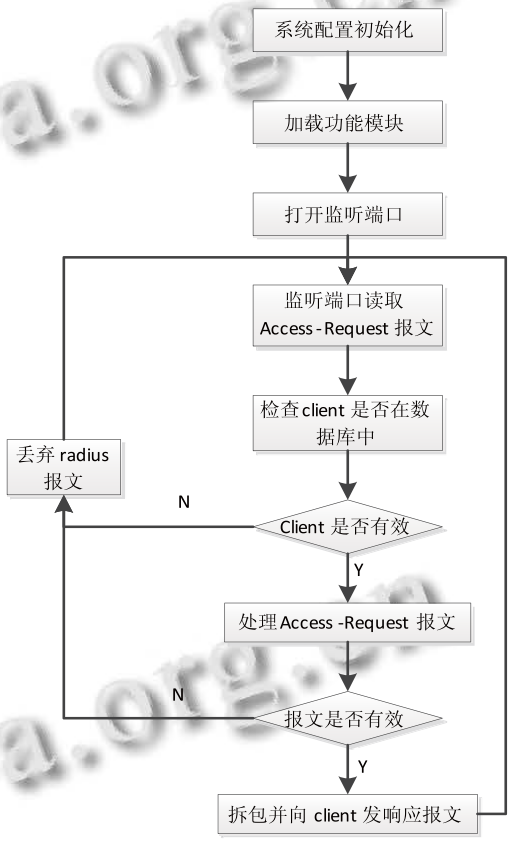

图 3　Freeradius 工作流程图

4.2　实验验证

4.2.1　实验目的

验证网络管理员登陆网络设备的统一认证、授权策略. 该实验通过在 Freeradius 上创建一个“aa”账号, 并授权该账号使用“show ip arp”命令, 然后验证:

ⓐ 账号 aa 能否成功登陆被管理的网络设备(本实验使用的是思科交换机);

ⓑ 网络设备本地账号以及除 aa 之外的其他账号能否成功登陆被管理的网络设备.

ⓒ 若账号 aa 能成功登陆, 该账号的权限有那些.

4.2.2 实验环境配置

硬件: 笔记本电脑; PC 电脑; 交换机;

软件: 操作系统(RedHat Linux 7.2)、数据库(mysql)、radius 服务端软件(经过编程修改后的 Freeradius).

4.2.3 实验拓扑

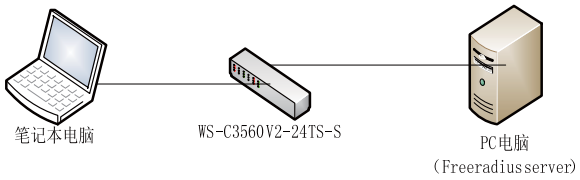

图 4 实验拓扑图

4.2.4 实验实现

Step1: 安装 RedHat Linux 7.2, 并在上面安装 MySQL, 部署经过编程修改后的 Freeraidus;

Step2: 设置 Freeradius, 如图 5 所示.

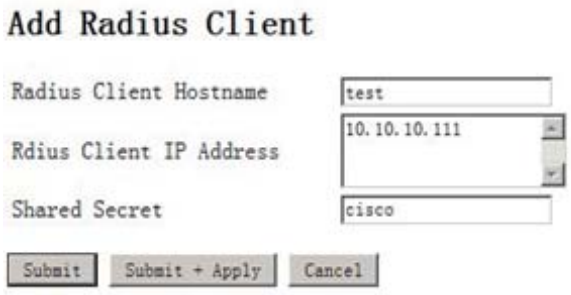

图 5 设置 Freeradius 之增加设置被管理网络设备

Step3: 配置 radius 服务器, 如图 6 所示.

Step4: 配置交换机, 命令如下:

aaa new-model

radius-server host 10.10.10.178 key cisco

aaa authentication login default group radius local

aaa authorization commands 15 default group tacacs+ local

Step5: 实验结果, 如图 7 表明账号 aa 已成功登陆, 并且该账号只能使用“show ip arp”命令, 当输入未被授权的“show run”命令是, 客户端提示“Command authorization failed. ”并拒绝执行该命令.

5 结语

本文设计了一种基于 radius 协议的认证、授权策略, 并在开源代码 Freeradius 的基础上开发. 该策略实现了对网络管理员进行认证和授权的精细化管理, 满足了大型局域网的管理需求, 提高了管理效率. 但在基于 radius 对网络管理员精细授权的安全方面考虑尚欠缺, 需要进一步改进, 也是后续需要设计内容.

图 6 radius 服务器配置

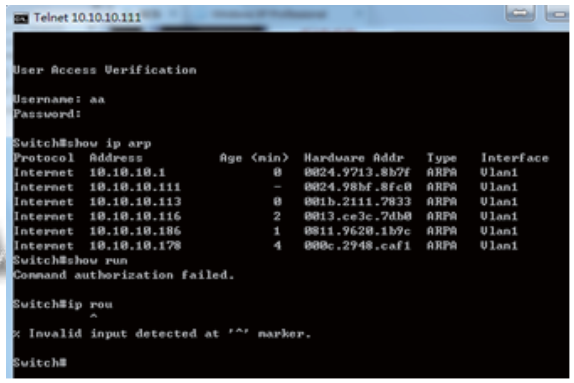

图 7 基于 RADIUS 协议的认证、授权的实验结果

参考文献

1 于周锋,蒋泽军,王丽芳.支持第三方认证的RADIUS系统设计.微电子学与计算机,2010,27(7):209–213.

2 陈沅涛,朱前飞,陈川.基于 Linux 的 RADIUS 服务器的设计与实现.计算机工程与设计, 2007,28(4):846–848.

3 白晓梅.一种网络认证计费的设计与实现.沈阳师范大学学报(自然科学版),2010,28(2):236–239.

4 陆金山,周健,靳春生.基于RADIUS协议的校园网络认证系

(下转第 136 页)

证明, 灰度图像的非线性变换是一种有效的图像增强方法, 利用量子遗传算法强大的搜索能力, 可以快速的获得非线性函数 BetaB(α, β)参数值, 实现灰度图像的自适应能力.

参考文献

1 韦芙芽,刘洪武,付春林.基于量子粒子群优化算法的光纤光栅参数重构.中国激光,2011,16(2):56−71.

2 黄力明,徐莹,于瑞琴.改进的量子遗传算法及应用.计算机工程与设计,2009,21(8):16−21.

3 朱筱蓉,张兴华.基于改进量子遗传算法的连续函数优化研究.计算机工程与设计,2007,8(21):147−152.

4 封安辉,苏宏升.一种改进的量子遗传算法及其应用.计算机工程,2011,13(5):212−218.

5 宣兆新,陆金桂,石云,吴慧.基于改进的遗传算法的图像恢复.计算机应用与软件,2010(3):32−36.

6 许少华,许辰,郝兴,王颖.一种改进的双链量子遗传算法及其应用.计算机应用研究,2010,7(6):44−49.

7 朱筱蓉,张兴华.基于改进量子遗传算法的连续函数优化研究.计算机工程与设计,2007,13(21):192−197.

8 黄沙日娜,赵国亮.模糊量子遗传算法及其应用.计算机工程与应用,2011,21(5):103−107.

9 Kouda N, Matsui N, Nishimura H. Image compression by layered quantum neural networks. Neural Processing Letters, 2002, 16(1): 213−219.

10 Yang J, Li B, Zhuang Z. Research of quantum genetic algorith and its application in blind source separation. Journal of Electronics(China), 2003, 20(1): 149−155.

11 Benioff P. Quantum mechanical hamiltonian models of turing machines. Journal of Statistical Physics, 1982, 29(3): 71−78.

12 Benioff PA. Quantum mechanical Hamiltonian models of discrete processes that erase their own histories. International Journal of Theoretical Physics, 1982, 21(3): 22−30.

13 Feynman RP. Simulating physics with computers. International Journal of Theoretical Physics, 1982, 21(6): 27−35.

14 Kačur J, Mikula K. Slow and fast diffusion effects in image processing. Computing and Visualization in Science, 2001, 3(4): 92−101.

15 Zhou J, Gan Q, Krzyżak A, Suen CY. Recognition of handwritten numerals by quantum neural network with fuzzy features. International Journal on Document Analysis and Recognition, 1999, 2(1): 137−142.

16 Han KH, Kim JH. Genetic quantum algorithm and its application to combinatorial optimization problems. Proc. of IEEE Conference on Evolutionary Computation, 2000, 9(14): 162−168.

17 Han KH, Park KH, Lee CH, et al. Parallel quantum- inspired genetic algorithm for combinatorial optimization problems. Proc. of IEEE International Conference on Evolutionary Computation, 2001, 14(7): 152−160.

18 Han KH, Kim JH. Genetic quantum algorithm and its application to combinatorial optimization problems. Proc. of IEEE Conference on Evolutionary Computation, 2000, 8(15): 133−140.

(上接第 247 页)

统的研究.合肥工业大学学报(自然科学版),2006,29(10):1231−1233.

5 单康康,张兴明.RADIUS 协议在 ACR 中的研究.广西大学学报:自然科学版,2011,S1:65−68.

6 杨凌凤.使用 USBKey 提高 FreeRadius 证书认证的安全性.计算机安全,2008,2:42−44.

7 于周锋,蒋泽军,王丽芳.支持第三方认证的RADIUS系统设计.微电子学与计算机,2010,7:210−213,217.

8 梁振方,盛焕烨.无线网状网的分布式 AAA 系统.微计算机信息,2009,33:90−91,134.