第33卷 第17期 计 算 机 工 程 2008年9月
Vol.33 No.17 Computer Engineering September 2007
·网络与通信· 文章编号：1000—3428(2007)17—0117—03 文献标识码：A 中图分类号：TP393

基于802.1x协议的认证系统的研究与改进

于承斌，尚 年，杨慧慧，崔 萌
（泰山医学院信息网络中心，泰安 271016）

摘 要：在以太网接入控制技术中，基于IEEE802.1x协议的认证系统有较大的优势，但在网络接入管理的实际中存在缺陷与不足。该文对基于802.1x协议的认证管理系统进行研究，介绍802.1x协议的体系结构，分析802.1X协同RADIUS协议应用于认证计费系统的工作原理、认证机制与流程，针对存在的问题给出一个改进的方案，通过增加网络流量作为新的认证元素，达到主动认证、高效控制的效果。
关键词：认证；802.1x协议；RADIUS协议

Research and Amelioration of Authentication System Based on 802.1x Protocol

YU Cheng-bin, SHANG Nian, YANG Hui-hui, CUI Meng
(Information Network Center, Taishan Medical College, Taian 271016)

【Abstract】The authentication system based on IEEE802.1x protocol has more advantages in LAN access, but it still has some problems and flaws based on the practice of network management. This paper gives a brief introduction to authentication architecture of the 802.1x protocol, the whole work theory, authentication mechanism and process of the system based on 802.1x and RADIUS protocol is discussed. An amelioration of the authentication system is presented. As a new element, the network flux is added to participate in its authentication. The project has advantages of automatic authentication and high efficiency in control.
【Key words】authentication; 802.1x protocol; RADIUS protocol

随着网络信息技术的不断发展，基于端口的访问控制协议802.1x[1]与RADIUS[2]认证服务器结合，把认证与计费管理结合起来，成为一种有效的网络管理控制技术。然而在具体的网络管理中，仍然发现这个系统存在一些缺陷与问题[3]，如在认证交换机下串接HUB设备后，非法用户可以随同合法用户一起上网。再如基于802.1x协议的认证对客户端软件的依赖性非常大，尤其是扩展一些功能后，完全靠客户端上报一些检测的数据，从而依赖性更大。然而其客户端软件又十分脆弱，十分容易被破解与仿造。为此，进一步研究基于802.1x协议的认证系统并进行改进，才能更加有效地对网络接入进行控制与管理。

1 基于802.1x协议的认证系统

1.1 802.1x协议的体系结构

IEEE802.1x协议的体系结构包括3个重要的组成部分：

(1)客户端请求系统(supplicant system)：请求者通常是支持802.1x认证的用户终端设备，用户通过启动支持802.1x协议的客户端软件发起802.lx认证。

(2)认证系统(authentication system)：认证系统通常为支持802.lx协议的网络设备组成，简称NAS(Network Access Server)，如Cisco系列交换机、华为3com等公司的系列交换机。802.lx认证技术的操作粒度为端口，端口可以是一个物理端口，也可以是一个逻辑端口，这个端口在逻辑上又分为“可控端口”与“不可控端口”。“不可控端口”始终处于双向连通状态，主要用来传递EAP协议包，保证客户端始终可以向认证方发出或接收认证消息。“可控端口”只在客户端认证通过的情况下才打开，一旦认证成功，请求方就可以通过“可控端口”访问网络资源并获得相应的服务。

(3)认证服务器系统(authentication server system)：认证服务器是提供认证服务的实体，通常为RADIUS服务器，该服务器可以存储有关用户的信息从而实现认证和授权功能。3个部分的结构如图1所示。

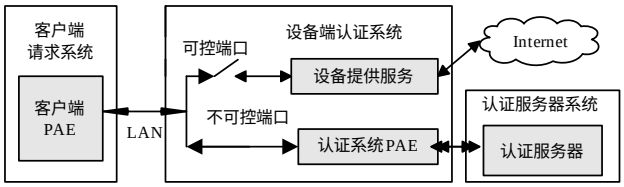

图1 802.1x协议的认证体系结构

1.2 802.1x协议的认证机制与流程

在802.1x协议的体系结构中，“不可控端口”始终处于双向连通状态，主要用来传递EAP[4]协议包，因802.lx本身没有定义具体的认证协议，它主要应用上层的EAP协议进行认证与通信，具体的封装实现应用了EAPOL(EAP over LAN)协议，可保证客户端始终可以向认证方发出或接收认证消息。而在认证者与认证服务器之间，EAP报文要承载在RADIUS协议之上，实现EAP报文的传输。通过使用EAP协议， RADIUS认证服务器可以支持多种认证机制，整个系统的具体认证工作机制与流程如图2所示。

作者简介：于承斌(1970－)，男，讲师、硕士，主研方向：计算机网络；尚 年，助理工程师；杨慧慧、崔 萌，助教
收稿日期：2008-05-10 **E-mail：**cbyu@tsmc.edu.cn

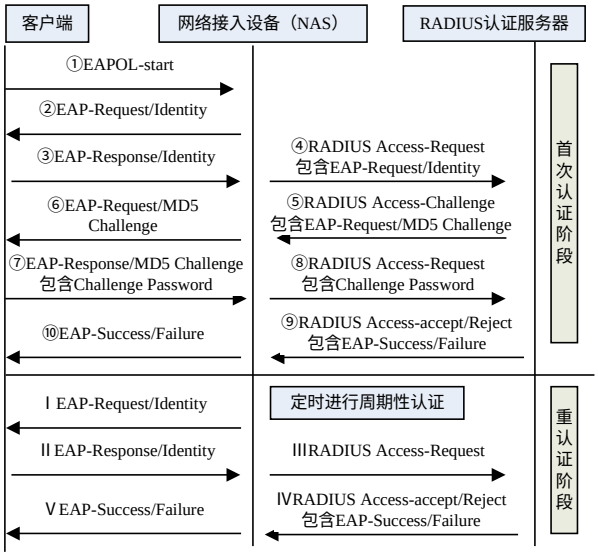

图 2　802.1x 协议的工作机制

1.3　802.1x 认证的优势与不足

1.3.1　802.1x 认证的优势

IEEE 802.1x协议为二层协议，不需要到达三层，对设备的整体性能要求不高，可以有效降低建网成本。采用“可控端口”和“不可控端口”的逻辑功能，从而可以实现业务流与认证流分离[5]。

1.3.2　802.1x 认证的不足

基于 802.1x 及 RADIUS 协议的认证计费管理系统采用的“可控端口”和“不可控端口”的逻辑功能实质是一把双刃剑，在它实现了业务流与认证流分离的同时，也带来了认证通过之后不可控制的问题与缺陷，即在认证通过之后，可控端口一直处于打开状态，使得同 VLAN 里面的非法用户与合法用户一起能够通过串接 HUB 接入并使用网络，即使在认证过程中加入了对 MAC、IP 乃至 VLAN ID 以及 NAS 端口号等属性的绑定，但仅对这些固化表示的认证也不能监管到认证通过后可控端口的状态。

2　认证计费系统的改进

2.1　改进思路

在改进系统的认证方面，充分利用系统的重认证功能设置成持续的周期性认证。最主要的认证控制方法是增加新的认证元素，使系统能判断出有非法的用户接入，从而切断可控端口的连接，这个重要的判别元素就是网络使用的流量。基于合法用户自己产生的网络流量与有非法用户接入一起产生的网络流量绝对不一样的事实，得到改进系统认证控制的重要思路。

由于目前的认证系统统计的流量是流经 NAS 设备的端口的流量，为此进一步通过客户端程序采集到合法用户本身的流量，显然有非法用户接入时这 2 个网络流量绝对不一样，这样通过系统的处理，就能判别是否有非法用户接入。

2.2　改进 802.1x 认证系统的方案及其实现

在此思路下，改进 802.1x 认证系统的具体方案与实现包括 3 个方面：

(1)改进客户端程序

增加客户端程序采集本机网络流量的功能，同时在客户端中扩展 EAP 报文的 Date 属性域，把上述采集到的网络流量作为新的属性增加封装进 EAP 报文，如用 PCIn 表示流入字节数，用 PCOut 表示流出字节数，扩展后封装的报文格式如图 3 所示。

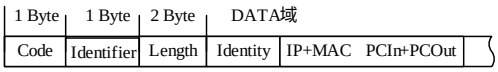

图 3　改进后的 EAP-Response 数据帧结构

(2)合理设置 NAS 设备的重认证功能

利用 NAS 的重认证的功能，根据管理需要合理设置 NAS 设备主动重认证的时间，系统缺省的配置时间为 15 s，一般可设为 3 min~5 min。

(3)扩展 RADIUS 认证服务器的功能

对 RADIUS 协议的属性扩展，在 RADIUS 协议的扩展属性列表中再增加定义 2 个属性 PCIn 与 PCOut，对应用户主机当前的流入与流出字节数。同时对数据库的信息表进行扩展，增加记录 PCIn0, PCOut0, PCIn, PCOut 的 4 个字段，最终得到(PCIn-PCIn0)+(PCOut-PCOut0)就是该用户这段时间内总的流量，记作 LIU1。改进的 RADIUS 的工作流程如图 4 所示。

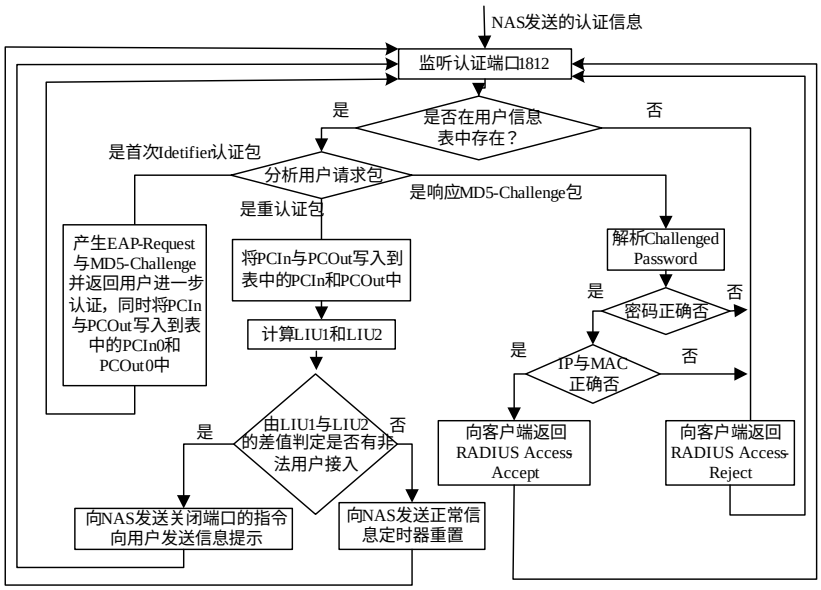

图 4　改进的 RADIUS 流程

具体改进的认证流程如下：

当 RADIUS 服务器收到 NAS 传递的数据包后，分析包的内容，如果发现是客户初始请求包，则在产生一个包含 EAP-Request/MD5-Challenge 的 RADIUS Access-Challenge 报文同时，也把扩展包中上传的 PCIn, PCOut 的值记录到相应数据库表的 PCIn0、PCOut0 字段中。

同理，当 RADIUS 服务器分析包的内容，发现是客户重认证发来的数据包，则把扩展包中上传的 PCIn、PCOut 的值记录到相应数据库表的 PCIn、PCOut 字段中；然后计算出用户在开始认证与开始后的重认证这段时间内实际的总流量 LIU1=(PCIn-PCIn0)+(PCOut-PCOut0)。

再从数据库相应表中读出 NAS 端口的流入流出字节数 Acct-Input-Octets 和 Acct-Ootput-Octets，计算出流经 NAS 端口的总流量，不妨记作 LIU2，则 LIU2=(Acct-Input-Octets)+(Acct-Ootput-Octets)。

把 LIU2 与 LIU1 作差，看其差是否不超过一个给定的数

值如 2 000 Byte，若 LIU2-LIU1≥2 000 Byte，则认为有非法用户接入；若 LIU2-LIU1≤2 000 Byte，则认为没有非法用户接入。

最后根据以上的判断认证，若认为有非法用户接入，则向 NAS 发送关闭端口强制用户下线的数据包指令，并将该情况记录到日志中以备查询；反之，只向 NAS 发送一个提示信息包，维持网络连通的状态。

2.3 改进后认证系统的整体工作机制

图 5 是改进后系统的认证机制与流程示意图，对比原来的 802.1x 的认证流程，系统改进后的认证机制与流程主要是：在认证中的第③步与第④步中，增加上报与传递 PCIn, PCOut 的数据，并把该数据写入数据库表的 PCIn0, PCOut0 字段中。

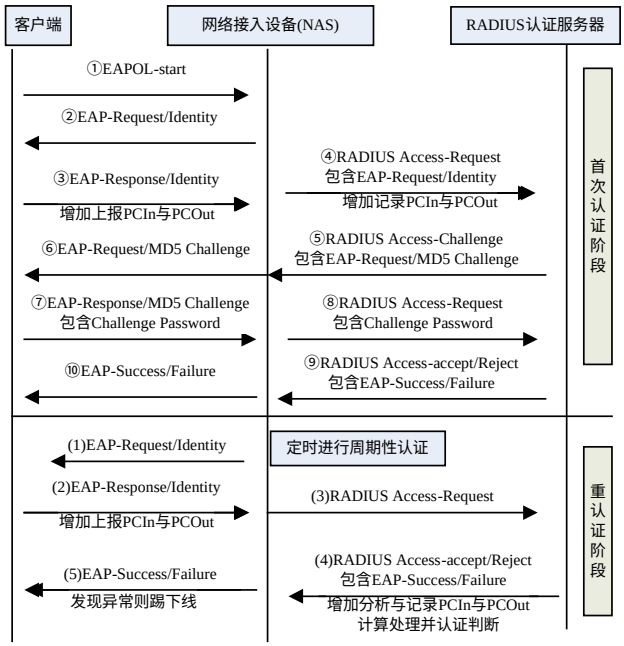

图 5 改进后系统的认证机制与流程

在重认证阶段中，第(2)步客户端响应 NAS 的请求，向 NAS 发送应答报文时，增加封装客户端采集到的 PCIn, PCOut。第(4)步中，RADIUS 认证服务器解析 NAS 发来的数据包，按如上提到的 RADIUS 的处理流程计算 LIU2-LIU1 的值后再和设定的数值比较，依此判断是否有非法用户接入，最终把判断认证成功/失败的结果封装成 RADIUS Access-Accept/Reject 报文发到 NAS。若是收到认证失败报文，即判断有非法用户接入，NAS 便把可控端口关闭，并向用户发出强制下线的提示信息，用户网络服务被断开，从而达到检测是否有非法用户随同上网的作用。

3 结束语

本文增加网络流量作为新的认证元素，从客户端程序、NAS 设备的重认证设置以及扩展 RADIUS 认证服务器的功能 3 方面入手，对基于 802.1X 与 RADIUS 协议的认证计费系统进行了研究与改进，改进后的认证系统能有效地阻止通过串接 HUB 的非法用户使用网络资源，减轻 RADIUS 服务器与 NAS 设备的负担与压力，其整体性能得到提升；客户端程序易被破解的缺陷将得以弥补，因为即使破解了客户端程序，使它丧失了上报用户机网络流量的能力，认证服务器因收不到这个属性的数据，在和 NAS 设备上报的流量比对时肯定会远远大于系统给定的数值，这样就会强制用户下线，因此破解变得没有意义。

将来的工作主要是针对不同厂商、不同类型的系统在程序设计上采取不同的具体方法与细节，将改进方案真正实施到实际的交换机产品与相应的网络接入管理系统软件中。

参考文献

[1] IEEE Std802.1D-1998 IEEE Standard for Local and Metropolitian Area Netwoks: Port-based Network Access Control[S]. 2001-06.

[2] Rigner C, Willens S, Rubens A, et al. Remote Authentication Dial in User Service (RADIUS)[S]. RFC 2865, 2000-06.

[3] 于承斌. 对基于 802.1x 协议的认证机制及缺陷的研究[J]. 信息技术, 2006, 13(11): 94-96.

[4] Blunk L, Vollbrecht J. PPP Extensible Authentication Protocol (EAP)[S]. RFC 2284, 1998-03.

[5] 宗 平, 占建峰. 802.1x 协议在宽带接入认证中的应用[J]. 计算机工程, 2004, 30(10): 119-121.

（上接第 116 页）

```
LONG _StunSendRequest(STUN_INSTANCE *pInst)；
/*发送 STUN 请求*/
LONG _StunInstanceGetPublicBinding
  (H_PROTOCOL_INSTANCE hStunInstance,DWORD
*pdwPublicIp,WORD *pwPublicPort)
/*确定映射 IP 和端口地址*/
```

5 结束语

本文设计并实现了一个基于端口探测且适用于大多数场合的 SIP 穿透 NAT 方案。基于 STUN 探测穿越 NAT 的优点是：无须对现有 NAT 设备做任何改动，即可在多个 NAT 串联的网络环境中使用，并且不需要对 SIP 协议进行任何扩展。测试表明，本方案能穿越大部分对称 NAT 和所有其他类型的 NAT。

进一步提高预测端口的命中率是下一步的重点。另外，STUN 协议方式的其他不足之处，如网络安全、QoS 保证以及与其他穿越机制相融合的问题也有待进一步研究。

参考文献

[1] Rosenberg J, Schulzrinne H, Camarillo G. SIP: Session Initiation Protocol[S]. IETF RFC 3261. 2002-06.

[2] 刘 刚, 吕玉琴, 张 毅, 等. SIP 协议穿透 NAT 网关的研究[J]. 中国电子科学研究院学报, 2006, 1(2): 195-196

[3] 张智江, 张云勇, 刘韵洁. SIP 协议及其应用[M]. 北京: 电子工业出版社, 2005.

[4] Rosenberg J, Weinberger J, Huitema C, et al. STUN-simple Traversal of User Datagram Protocal(UDP) Through Network Address Translators(NATs)[S]. IETF RFC 3489. 2003-03.

[5] Takeda Y. Symmetric NAT Traversal Using STUN[Z]. [2007-01-05]. http://www.cs.cornell.edu/projects/stunt/draft-takeda-symmetric-nat-traversal-00.txt.

[6] 张 波, 胡瑞敏, 边学工. 一种实现 SIP 穿越 NAT 的新方案[J]. 计算机工程, 2005, 31(2): 119-121.