

文章编号:1001-9081(2005)07-1517-03

基于交换机的 802.1X 协议扩展及实现

曹华伟,尹治本

(西南交通大学 计算机与通信工程学院,四川 成都 610031)

(zbyin@home.swjtu.edu.cn)

摘 要:对 IEEE802.1X 协议的原理和认证流程进行了分析和介绍。根据交换机在以太网应用环境中对认证和端口控制的实际需求,结合端口控制和认证机制的选择,以及认证服务器的兼容性和安全性等问题,提出了一种 802.1X 协议的扩展方案。该方案在百兆交换机上予以实现,并在以太网环境中进行了认证测试。

关键词:802.1X 协议;交换机;以太网;安全;认证

中图分类号:TN915.04 **文献标识码:**A

Extension and implementation of 802.1X protocol for switch

CAO Hua-wei, YIN Zhi-ben

(School of Computer & Communications Engineering, Southwest Jiaotong University, Chengdu Sichuan 610031, China)

Abstract: The theory and authentication process of IEEE 802.1X protocol was analyzed and introduced. According to the requirements of authentication and port control of switch in Ethernet application environment, to solve the questions of port control, selection of authentication scheme, compatibility and security of authentication server, an extended scheme of 802.1X was given. It was implemented on a 100M switch, and tested in Ethernet environment.

Key words: 802.1X protocol; switch; Ethernet; security; authentication

近年来,随着以太网技术的发展,构建以太网的基础设备——交换机由局域网转接设备转变为广域网接入设备。对于网络服务提供商而言,网络必须是可运营的,对用户的管理是其中的一个重要的内容,只有合法的用户,才可以使用网络提供的服务。802.1X 协议提供了一套对接入到网络的设备进行认证、授权的机制,认证所使用的 EAPOL (EAP encapsulation over LANS)^[1] 帧承载于以太报文之上,很容易应用于以太网环境。因此将 802.1X 应用于交换机,通过交换机对广域网用户进行管理是一种常见的用户管理策略。同时,802.1X 也是交换机安全策略的一部分,可以有效防止非法用户访问没有授权的资源。

1 802.1X 协议的原理

802.1X 协议起源于 802.11 协议,是 IEEE 在 2001 年 6 月通过的基于端口的访问控制接入标准,它在局域网设备的物理接入级对接入设备进行认证和控制,用于交换式的以太网环境。

1.1 体系结构

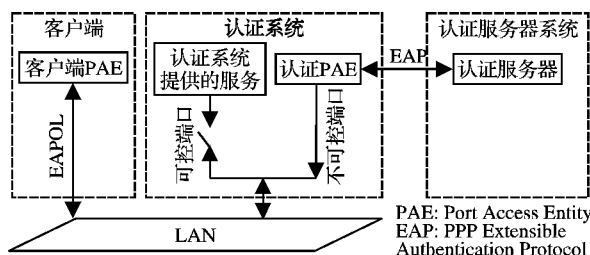


图 1 802.1X 协议的体系结构

802.1X 的体系结构由三部分组成:客户端、认证系统和

认证服务器,如图 1 所示。

客户端是指为了获取认证系统提供的服务而向认证系统提出认证申请的实体,它位于点对点连接的网络上的一端。客户端必须支持 802.1X 协议,可以收发 EAPOL 帧,这通常需安装 802.1X 的客户端软件。

认证系统是指对客户端进行认证的实体,它位于点对点连接网络上与客户端相对的一端。通常为支持 IEEE 802.1X 的网络设备。该设备对应于每个物理端口都有两个逻辑端口:可控端口和不可控端口。不可控端口始终处于双向连通状态,主要用来传递 EAPOL 帧,可保证客户端始终可以发出或者接收认证报文。可控端口只有在认证通过的状态下才打开,用于传递网络资源和服务。可控端口可配置为双向受控、仅输入受控两种方式,以适应不同的应用环境。如果用户端未通过认证,则可控端口处于未认证状态,客户端无法使用认证系统提供的服务。

认证服务器是对认证系统提供认证服务的实体,它通过由认证系统发送过来的认证信息,在认证数据库中进行查找,根据查找结果决定客户端认证是否成功。

1.2 认证过程

一个典型的 802.1X 认证流程如图 2 所示。

认证过程如下:

- 1) 客户端发送 EAPOL-Start^[1] 报文,启动认证过程;
- 2) 认证系统收到 EAPOL-Start 报文后,初始化一个会话 ID,作为一次认证过程的标识。整个认证过程中所有的 EAPOL 报文都带有该会话 ID,以便客户端和认证系统确认收到的 EAPOL 报文是否属于本次认证过程;
- 3) 认证系统向客户端发出一个 EAPOL-Request^[1] 报文,

收稿日期:2004-12-20;修订日期:2005-03-05

作者简介:曹华伟(1980-),男,山西大同人,硕士研究生,主要研究方向:软件工程;尹治本(1954-),男,云南腾冲人,教授,主要研究方向:软件工程、网络信息系统、算法设计。

要求客户端发送认证信息;

4) 客户端收到 EAPOL-Request 报文后, 发送 EAPOL-Response^[1] 报文, 将自己的认证信息(如用户名和密码)发送给认证系统;

5) 认证系统收到 EAPOL-Response 报文后, 向服务器转发承载于高级协议的 EAP 报文;

6) 认证服务器收到 EAP-Response 报文后, 根据认证信息在认证数据库中进行查找, 根据查找的结果, 向认证系统发送 EAP-Success^[2] 或 EAP-Failure^[2] 报文;

7) 如果认证系统收到 EAP-Success 报文, 说明认证成功, 认证系统将可控端口打开, 并向用户端发送 EAPOL-Success 报文; 否则说明认证失败, 认证系统的可控端口保持关闭状态, 向客户端发送 EAPOL-Failure 报文。

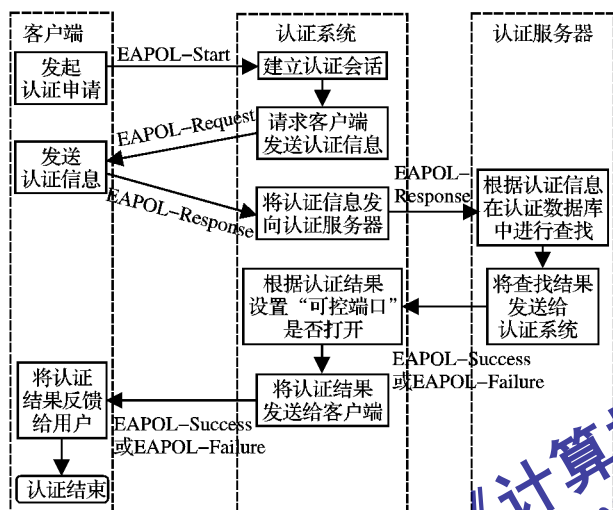


图2 一个典型的 802.1X 认证流程

2 802.1X 协议在以太网交换机中的扩展

在以太网环境中, 802.1X 体系结构中的客户端通常是运行于 PC 机上的客户端软件, 认证系统就是运行于交换机上的认证程序, 存有用户认证信息的计算机就是认证服务器, 用户通过认证后所能使用的服务主要是通过交换机进行对外连接, 如访问 Internet。作为一个标准, IEEE802.1X 并没有过多地考虑实际的应用环境和实现环境, 将它应用于交换机, 需要进行以下扩展。

2.1 将基于端口的控制变为基于用户的控制

802.1X 协议起源于 802.11 协议, 802.11 协议主要是为了解决无线局域网用户的接入认证问题。对于无线局域网而言, 认证之后建立起来的信道端口被独占, 不存在被其他用户再次使用的问题。但将 802.1X 应用于以太网, 需要认证的端口可能连接多个用户, 当某个用户认证成功, 端口打开, 就存在其他非法用户可以自由接入和无法控制的问题, 如图3所示。

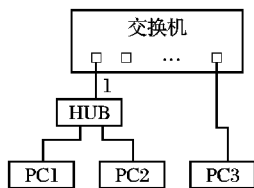


图3 端口控制存在问题的网络连接

PC1 和 PC2 通过 HUB 与交换机的端口 1 相连, PC3 直接与交换机相连, 为了限制任意用户对 PC3 的访问, 在交换机的端口 1 启动 802.1x 认证, 当 PC1 认证成功后, 端口 1 会被打开, 此时, PC2 虽然没有通过认证, 也仍然可以访问 PC3, 这显

然是不符合设计初衷的。

将 802.1X 应用于交换机, 受控的不应该是交换机的物理端口, 而是用户需要转发的数据包。我们可以在交换机上对用户需要转发的数据包进行过滤, 只有通过认证的用户, 交换机才转发其数据包。这样当 PC1 通过认证, 它发向 PC3 的数据包可以被交换机转发, 从而可以访问 PC3。而 PC2 没有通过认证, 它发向 PC3 的数据包不会被转发, 因此也就无法访问 PC3, 从而可以将连接于同一端口的 PC1 和 PC2 区别对待。

2.2 认证机制的选择

802.1X 只定义了认证过程的报文格式, 并没有定义具体的认证机制。从设计上而言, 这方便了扩展, 不同的环境下可以使用不同的认证机制, 但从实现上而言, 却增加了对兼容性的考虑。例如当连接到我方交换机的 PC 机上使用了第三方的客户端软件或运行我方客户端软件的 PC 机连接到了第三方的交换机上, 就可能会出现双方不识别对方的认证机制。对于认证机制的兼容性问题, 有两种解决办法: 一种是采用静态配置的方式, 在认证过程开始前指定客户端和认证系统所使用的认证机制; 另一种方法是通过对 EAP 报文的 Nak 应答报文的处理, 进行认证机制的动态协商, 如图4所示。

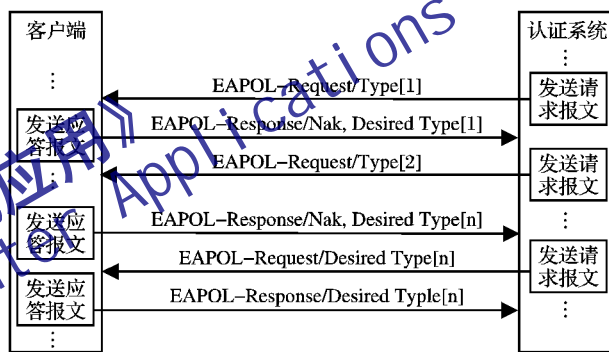


图4 认证机制的动态协商过程

协商过程如下:

1) 认证系统发送 EAPOL-Request 报文, 报文中的 Type 表示认证系统所使用的认证机制类型;

2) 如果客户端不支持 EAPOL-Request 报文中的 Type 认证机制, 返回 EAPOL-Response/Nak 报文, 表示不支持认证系统使用的认证机制, 报文中的 Desired Type 表明了客户端希望使用的认证机制类型, 继续 3); 如果客户端支持 EAPOL-Request 报文中的 Type 认证机制, 发送 EAPOL-Response 报文, 报文中的认证机制类型为 Type, 是双方都支持的认证机制, 协商成功;

3) 如果认证系统支持 Desired Type 认证机制, 将 Desired Type 赋值给 Type, 继续 1); 如果认证系统不支持 Desired Type 认证机制, 将 Type 取值为一种新的认证机制类型, 继续 1)。

由于标准的认证机制是任何一款产品都应该支持的, 因此最终至少可以协商到一种标准的认证机制, 如 MD5-Challenge^[2] 等。与静态配置相比, 自动协商不需要在认证开始前就指定采用何种认证机制, 提高了认证的灵活性, 简化了认证配置项。但协商过程要占用一定的时间, 降低了首次认证的效率, 同时要求客户端和认证系统必须支持对 EAP/Nak 报文的处理。支持自动协商的交换机与不支持自动协商的 PC 机相连或反之, 同样可以兼容运行, 不存在问题。

2.3 认证服务器的兼容性扩展

在 802.1X 协议中, 认证系统和认证服务器进行通信时, 将 EAP 报文承载于其他高级协议上, 如 EAP over RADIUS, 因

此要求认证服务器必须支持EAP协议,但目前市场上的认证服务器,很多都不支持EAP协议,对它们进行升级是一项庞大的工程。出于对已有认证服务器的兼容性考虑,在认证系统与认证服务器进行通信时,并不采用将EAP报文承载于其他高级协议报文之上的方式,而是直接采用认证服务器所支持的高级协议进行通信,如RADIUS协议。将需要由客户端经认证系统转发到认证服务器的EAP数据段,在认证系统中映射成为认证服务器支持的报文,同样,将需要由认证服务器经认证系统转发到客户端的高级协议报文,由认证系统映射成为EAP报文。这样,就可以在不改变现有认证服务器的前提下,使用802.1x认证,如图5所示。

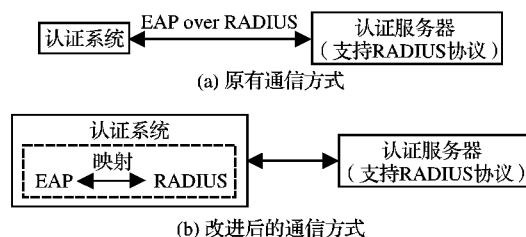


图5 认证系统与支持RADIUS协议的认证服务器进行通信的方式

2.4 802.1X的安全性问题

应用于交换机的802.1X面临两类安全问题:一是假冒认证服务器的中间人攻击;另一个是假冒用户的拒绝服务攻击。

所谓中间人攻击,就是攻击者通过假冒认证服务器,向交换机发送虚假的认证结果报文,这主要是由于802.1X协议的单向认证造成的,即只有认证服务器验证交换机发送的报文是否来自可信用户,而交换机总是假设发送认证结果报文的服务器是可信的。解决的方法就是当收到认证服务器发来的认证结果报文时,首先对服务器的身份进行验证,再处理认证结果。本文使用的一种处理方法如下:

- 1) 在交换机和认证服务器上保存同一个用于身份验证的密钥KEY,这个密钥不能通过网络传播;
- 2) 交换机向认证服务器发送认证报文时,附带一个串S1,并将S1在本地保存;
- 3) 认证服务器在发送认证结果时,也附带一个串S2,S2是由KEY通过算法F将S1加密所得的;
- 4) 交换机收到认证服务器发来的认证结果报文后,先将本地保存的S1使用同样的算法F用KEY加密,产生串S3,将S3与S2比较,若相同,则认证服务器可信,处理认证结果,否则不予认证。

由于EAP报文中表示认证结果的报文不带有任何附加信息,因此如果交换机与认证服务器之间通过承载于高级协议之上的EAP协议进行通信时,实现如上所示的身份验证比较复杂。但使用2.3的扩展方式后,交换机与认证服务器之间直接通过高级协议进行通信,协议本身允许报文携带任何信息,实现上述的身份验证相对比较容易。

拒绝服务主要是恶意用户假冒合法用户,向交换机发送EAPOL-LOGOFF^[1]报文,从而使交换机误认为用户下线,不再转发用户数据包。可以通过改进下线流程来解决这个问题,当交换机收到EAPOL-LOGOFF报文时,进行重认证,如果重认证失败,表明用户确实下线了,交换机作相应的下线处理;如果重认证成功,表明用户并没有下线,收到的EAPOL-LOGOFF是拒绝服务攻击,交换机不作任何处理。

3 802.1X协议的实现

结合上面的内容,选定如下具体方案,将802.1X协议在

百兆交换机上予以实现:

- 1) 通过控制端口对MAC地址的学习,来达到对用户数据包的过滤,从而形成对用户的控制;
- 2) 交换机上运行的认证系统支持认证机制的自协商和静态配置两种方式;
- 3) 认证服务器采用RADIUS协议,交换机与认证服务器之间通过RADIUS报文进行通信;
- 4) 交换机对认证服务器的身份验证采用静态配置身份验证密钥KEY和MD5加密算法,由认证服务器发送的RADIUS认证结果报文中携带串S2;
- 5) 对802.1X协议的状态机进行裁减,只实现了9个状态机中的3个(Authenticator PAE状态机、Backend Authentication状态机和Supplicant PAE状态机)^[1]。

4 测试结果

在一款24口的百兆交换机上,用户数量和全部通过认证的时间如表1所示。

表1 用户数量和全部通过认证的时间关系表

同时认证的 用户数	全部认证完毕 总耗时/s	单个用户平均 认证时间/s
1	0.38	0.380
10	0.37	0.037
100	1.80	0.018
1000	153.00	0.153

由于受到网络环境的影响,单个用户平均认证时间随用户数不同而有所不同(由于在具体的实现中,为了提高与认证服务器进行通信的效率,采用了并行机制,对认证结果采用定时轮询的方法,因此一定数量以内的用户,只要认证时间小于轮询时间,全部通过认证的时间是相同的,这也就解释了表中前两行的数据),1000个用户全部认证成功共耗时153s,平均每个用户的认证时间小于1s,还是可以接受的。

由于交换机的数据转发主要靠硬件来完成,所以软件层的用户认证过程不会影响数据包的转发,因此实现802.1X的交换机数据转发性能不会受太大的影响。

5 结语

结合对802.1X的扩展,我们已将802.1X协议成功地用于多款交换机,每个端口允许的最大用户数可达1200个,整台交换机最多可允许12000个用户通过认证,在具体的用户环境下运行良好,满足了用户需求,达到了设计要求。

参考文献:

- [1] IEEE 802.1X, Standards for Local and Metropolitan Area Networks: Prot-Based Access Control[S], 2001.
- [2] RFC2284, PPP Extensible Authentication Protocol[S], 1998.
- [3] RFC1994, PPP Challenge Handshake Authentication Protocol[S], 1996.
- [4] 赖炜, 钱骏. 关于在LAN环境中应用IEEE802.1X Standard的安全性分析[J]. 现代计算机, 2003, (4): 51-53, 87.
- [5] 张永德. 对IEEE 802.1x协议的安全性分析[J]. 东北电力学院学报, 2003, 23(2): 75-78.
- [6] 石琦文. 802.1x设计缺陷及其解决方案[J]. 电信网技术, 2003, 8(8): 45-48.
- [7] (美)BATES RJ, KIMMEL Jr Z. 北电网络第三层交换技术[M]. 卢泽新, 陶孜谨, 译. 北京: 机械工业出版社, 2001.