局域网中 802.1x 认证方式研究与实现

Research and implementation of 802.1x authentication in LAN

白万建　刘 冰　（菏泽供电公司 山东 菏泽 274012）

摘要:802.1x 协议网络认证方式是一种具有发展潜力的认证方式。本文介绍了 802.1x 协议在局域网认证中的工作原理和认证过程,分析了与其他认证方式的差异,并对认证过程中可能存在的问题及解决方案进行了讨论,最后给出了 802.1x 认证客户端在 linux 下的实现。

关键词:802.1x 协议 认证方式 RADIUS PPPOE

1 802.1x 认证技术的起源

802.1x 协议起源于 802.11 协议,后者是标准的无线局域网协议,802.1x 协议的全称是基于端口的访问控制协议,主要目的是为了解决无线局域网用户的接入认证问题,它通过控制端口访问节点来提供无线局域网用户接入认证和安全性,现在已经开始被应用于一般的有线 LAN 的接入。

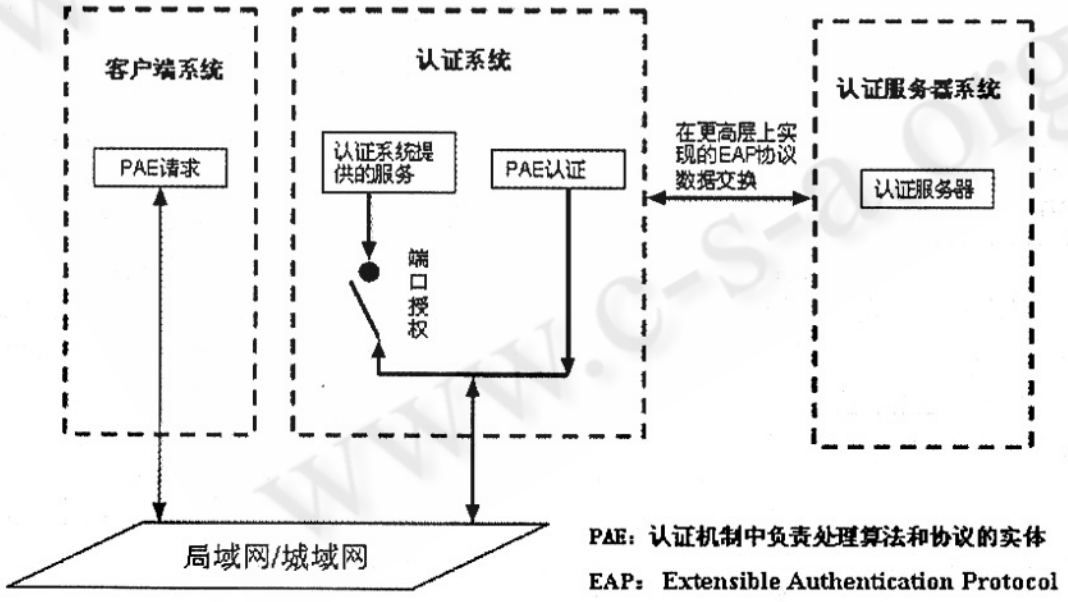

图 1

在 802.1x 出现之前,企业网上有线 LAN 应用都没有直接控制到端口的方法。也不需要控制到端口。但是随着无线 LAN 的应用以及 LAN 接入在电信网上大规模开展,有必要对端口加以控制,以实现用户级的接入控制。802.1x 就是 IEEE 为了解决基于端口的接入控制(Port – Based Access Control)而定义的一个标准。

2 802.1x 协议原理

802.1x 协议仅仅关注端口的打开与关闭,对于合法用户(根据帐号和密码)接入时,该端口打开,而对于非法用户接入或没有用户接入时,则该端口处于关闭状态。认证的结果在于端口状态的改变,而不涉及通常认证技术必须考虑的 IP 地址协商和分配问题,是各种认证技术中最简化的实现方案。802.1x 定义了基于端口的网络接入控制协议,并且仅定义了接入设备与接入端口间点到点这一种连接方式,即接入设备和认证服务器之间的认证方式没有规定,能够自

行实现，可以选择 Radius 或其它协议，也可以选择本地认证，即在交换机上设置用户数据库。其中端口既可以是物理端口，也可以是逻辑端口。

3　802.1x 认证过程

基于以太网端口的用户管理认证技术通过 3 个部分的功能实体来实现以太网端口用户管理认证的模式

（1）客户端软件（Supplicant System）

需要支持 EAPOL 协议，客户端必须运行 802.1X 客户端软件，如：802.1X – complain，Microsoft Windows XP，linux 下的 mdc – ssd，xsupplicant 等。

（2）认证系统（Authenticator System）

在以太网系统中指认证交换机，其主要作用是完成用户认证信息的上传、下达工作，并根据 RADIUS 服务器的认证结果，开放用户连接以太网业务端口的访问权限。

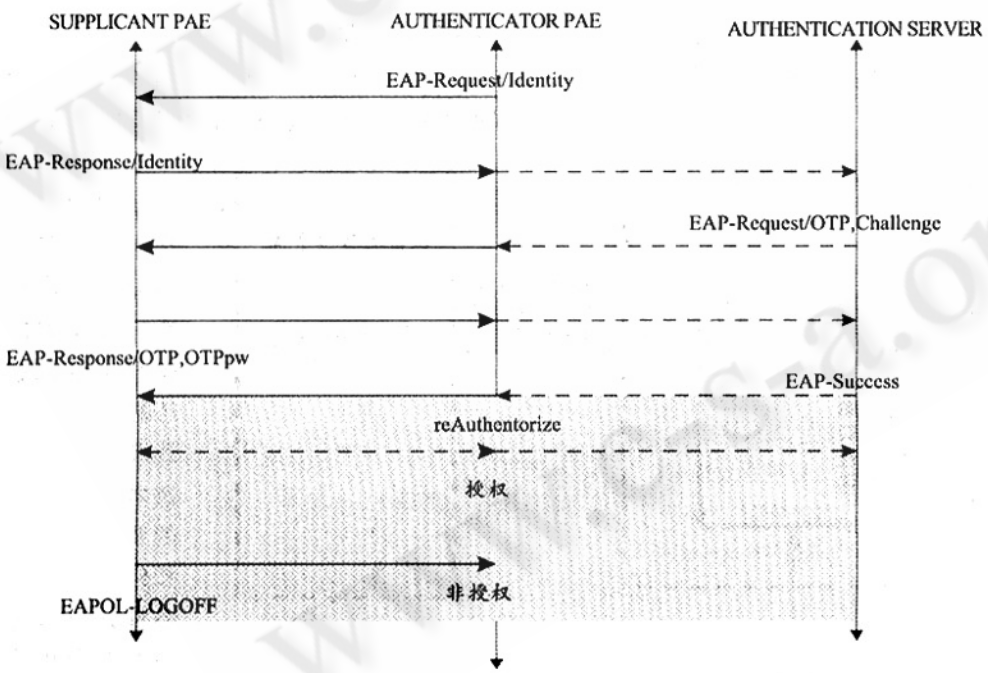

图 2

（3）认证服务器（Authentication server）

通过检验客户端发送来的身份标识（用户名和口令）来判别用户是否有权使用网络系统提供的网络服务，并根据认证结果向交换机发出打开或保持端口关闭的状态。

当用户有上网需求时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和口令，发起连接请求。此时，客户端程序将发出请求认证的报文给交换机，开始启动一次认证过程。

交换机收到请求认证的数据帧后，将发出一个请求帧要求用户的客户端程序将输入的用户名送上来。

客户端程序响应交换机发出的请求，将用户名信息通过数据帧送给交换机。交换机将客户端送上来的数据帧经过封包处理后送给认证服务器进行处理。

认证服务器收到交换机转发上来的用户名信息后，将该信息与数据库中的用户名表相比对，找到该用户名对应的口令信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字传送给交换机，由交换机传给客户端程序。

客户端程序收到由交换机传来的加密字后，用该加密字对口令部分进行加密处理（此种加密算法通常是不可逆的），并通过交换机传给认证服务器。

认证服务器将送上来的加密后的口令信息和其自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息，并向交换机发出打开端口的指令，允许用户的所有的报文通过。否则，反馈认证失败的消息，并保持交换机端口的关闭状态，此时只允许 802.1X 的认证报文 EAPOL（Extensible Authentication Protocol over LAN）通过。

在客户端与认证服务器交换口令信息的时候，没有将口令以明文直接送到网络上进行传输，而是对口令信息进行了不可逆的加密算法处理，使在网络上传输的敏感信息有了更高的安全保障，杜绝了由于下级接入设备所具有的广播特性而导致敏感信息泄漏

的问题。

4 与其他认证方式的比较

目前的主要技术有以下三种：PPPoE、Web + Portal、IEEE802.1x。

(1) WEB/Portal 认证过程可以简单描述如下：

① 用户通过 Web/Portal server 内置 DHCP 获得 IP 地址(也可以使用静态 IP 地址)。

② 用户通过 Explore 访问 WEB/Portal Server，输入用户名和密码。

③ WEB/Portal Server 获得用户 MAC/IP/VID 作为用户标识。

④ 通过 Server 给某个 MAC/IP/VID 以上网权限，并检验每个数据流是否满足权限要求。

⑤ 用户下线，需要在 WEB/PORTAL 的 Explore 界面上注销，通知系统停止计费。

⑥ 系统定期检测用户在线情况，发现用户下线，停止计费。

优点：不需要特殊的客户端软件，降低网络维护工作量，缺点：由于 Web/Portal 认证是基于 7 层的认证，为了达到网络 2 层的连接和认证而到 7 层认证，提高了网络响应消耗；用户连接性差，不容易检测用户离线，基于时间的计费较难实现；? IP 地址的分配在用户认证前，如果用户不是上网用户，则会造成地址的浪费，而且分配 IP 地址的 Web 认证服务器对用户而言是完全裸露的，容易造成被恶意攻击，并使得整网无法认证。

(2) PPPoE(Point – to – Point Protocol over Ethernet)

协议允许通过一个连接客户的简单以太网桥启动一个 PPP 对话。PPPoE 的建立需要两个阶段，分别是搜寻阶段(Discovery stage)和点对点对话阶段(PPP Session stage)。当一台主机希望启动一个 PPPoE 对话，它首先必须完成搜寻阶段以确定对端的以太网 MAC 地址，并建立一个 PPPoE 的对话号(SESSION_ID)。采用安装在端局 POP 节点的 BNAS，负责终结由用户 PC 机发起的 PPPoE 进程，并在 BNAS 后面连接运营商的 RADIUS(远程认证拨入用户服务)认证服务器和 RADIUS 计费服务器。当用户登录时，BNAS 将用户名和口令传送到认证服务器，验证通过后，BNAS 将允许用户接入网络，并启动计费服务器对用户进行计费。优点：是传统 PSTN 窄带拨号接入技术在以太网接入技术的延伸；和原有窄带网络用户接入认证体系一致；最终用户相对比较容易接收。缺点：PPP 协议和 Ethernet 技术本质上存在差异，PPP 协议需要被再次封装到以太帧中，所以封装效率很低；PPPoE 在发现阶段会产生大量的广播流量，对网络性能产生很大的影响；组播业务开展困难，而视频业务大部分是基于组播的；需要运营商提供客户终端软件，维护工作量过大；PPPoE 认证一般需要外置 BAS，认证完成后，业务数据流也必须经过 BAS 设备，容易造成单点瓶颈和故障，而且该设备通常非常昂贵。

(3) 802.1x 协议

优点：为二层协议，不需要到达三层，去除了冗余昂贵的多业务网关设备，对设备的整体性能要求不高，可以有效降低建网成本。通过组播实现，解决其他认证协议突出的广播问题，，对组播业务的支持性好。消除网络认证计费瓶颈和单点故障，由于 802.1x 实现了认证流与业务流的彻底分离，因而更易于开展多业务；有效的保证了企业内网的安全。缺点：需要特定客户端软件；由于 802.1x 是比较新的二层协议，要求客户端的交换机支持认证报文透传或完成认证过程，因此在全面采用该协议的过程中，存在对已经在网上的用户交换机的全部升级处理问题，加大了现有网络的改造难度；802.1x 认证技术的操作对象是端口，合法用户接入端口之后，端口处于打开状态，因此其它用户通过该端口时，不需认证即可接入网络。不能直接对流量进行统计，需要借助第三方系统开展基于流量的计费。

PPPoE 出现较早，产品支持最多，就目前而言，网络运营商多采用发展已经比较成熟的 pppoe 方案。；WEB 方式由于无标准，产品实现技术不统一；802.1x 为新认证方式，产品支持最少。

5 802.1x 认证可能存在的问题及解决方案

在 802.1X 解决方案中，接入认证通过之后，通常采用基于 MAC 地址的端口访问控制模式，IP 数据包在二层普通 MAC 帧上传送，认证后的数据流和没有认证的数据流完全一样，这是由于认证行为仅在用户接入的时刻进行，认证通过后不再进行合法性检查。采用此种模式将会带来降低用户建网成本、降低认证服务

器性能要求的优点。对于此种访问控制方式，应当采用相应的手段来防止由于 MAC、IP 地址假冒所发生的网络安全问题。

（1）假冒 MAC 地址的情况

当认证交换机的一个物理端口下面再级连一台接入级交换机，而该台接入交换机上的甲用户已经通过认证并正常使用网络资源，则此时在认证交换机的该物理端口中就已将甲用户终端设备的 MAC 地址设定为允许发送业务数据。假如同一台接入交换机下的乙用户将自己的 MAC 地址修改得与甲用户的 MAC 地址相同，则即使乙用户没有经过认证过程也能够使用网络资源了，这样就给网络安全带来了漏洞。解决方法是在认证交换机上通过 MAC 地址 + IP 地址的绑定功能来阻止假冒 MAC 地址的用户非法访问

（2）对于假冒 IP 地址的情况

由于 802.1X 采用了基于二层的认证方式，因此，当采用动态地址分配方案时，只有用户认证通过后，才能够分配到 IP 网络地址。

对于静态地址分配策略，如果假冒了 IP 地址，而没有能够通过认证，也不会与正在使用该地址的合法用户发生地址冲突。

如果用户能够通过认证，但假冒了其他用户的 IP 地址，则通过在认证交换机上采用 IP 地址 + MAC 地址绑定的方式来控制用户的访问接入。这使得假冒用户无法进行正常的业务通信，从而达到了防止 IP 地址被篡改、假冒的目的。

（3）掉线攻击

认证的整个过程都是在连路层完成的不涉及到 ip 层，tcp 层的东西，数据链路层通过的标识主机的数据为 MAC 地址，攻击者使用 arp 协议相关的工具能够得到被攻击者的 MAC 地址，如果使用 sniffer 等数据包构造工具构造一个包含被攻击者 MAC 地址的数据包，数据包的格式为注销（logoff）数据包，那么当这个数据包被发送到认证系统的时候，认证系统就会认为注销被攻击者的登录，对方就会掉线。对于这种攻击方式，由于数据包的构造不受网络中现有 MAC、IP 等影响，可以随意构造，设防上相对以上方式较难。

6 802.1 认证客户端在 Linux 下的实现

由于目前大多数认证系统的实现都建立在 windows 平台上，其中 windows XP 就自带认证客户端，相比较而言，对 linux/unix 下的认证客户端不予提供，本文以 redhat linux 为例，提供在 linux 下的登录客户端实现。

（1）下载免费的 mdc – ssd 802.1x 认证客户端软件。目前的版本是：mdc – ssd – 01.1.2 – 1.i386.rpm

（2）安装 mdc – ssd。由于 mdc – ssd 使用了 TLS 认证，所以需要一些 SSL 的库文件。如果您安装的时候提示需要安装 libssl 或 libcrypto 等软件包，请使用命令：

" rpm – Uvh – nodeps mdc – ssd – 01.1.2 – 1.i386.rpm" 安装。同时在/usr/lib 目录里，建立文件链接：

cd /us/lib

ln – s libssl.so libssl.so.1

ln – s libcrypto.so libcrypto.so.1

（3）配置 mdc – ssd。

cd /etc/mdc – ssd

修改文件 ifcfg，将 id 对应一栏的内容改成您的用户名。

cd /etc/mdc – ssd/eth0

修改 chap – secrets 文件，将系统自动添加的一栏改成您的用户名和密码，中间" * " 号保留。

可以只修改 ifcfg 文件，将 id 后面的默认口令设置为您的密码就可以了，chap – secrets 文件不需修改。

7 总结

802.1x 标准认证协议的出现，解决了传统 PPPoE 和 Web/Portal 认证过程中带来的问题，其优点就是实现简单、认证效率高、安全可靠，无需多业务管理设备，一次性投资低，支持组播等特性使其具有强大的生命力，为运营商建设可运营、可管理的电信级宽带以太网提供了很好的支持。

参考文献

1 陈晓涛，宽带接入的认证管理方式分析[J/OL]，通信世界网，2003.10。

2 孙丽丽，烽火网络宽带接入服务器用户认证浅析[J]，中国数据通信，2003.8。

3 李瀛寰、马云飞，802.1x：开创认证新时代[J]，中国计算机报，2003.6。