文章编号：1005-8451（2004）10-0035-03

802.1x协议在铁路无线局域网中的应用

杨伟青
（上海铁路局 电子计算技术中心，上海 200071）

摘 要：介绍无线局域网存在的主要安全问题和当今比较主流的无线局域网安全解决技术，其中阐述了最新的802.1x协议，解释其基本原理及该协议在铁路无线局域网中的应用。

关键词：无线局域网；802.1x协议；安全；应用
中图分类号：TP393 文献标识码：B

Application of 802.1x protocol to railway wireless LAN

YANG Wei-qing
(Electronic & Computing Technical Centre of Shanghai Railway Administration, Shanghai 200071, China)

Abstract: It was introduced main security problems and the popular technique security solution for wireless LAN, explained the 802.1x protocol, including its definition and basic principle. It was also discussed the application of this protocol to railway wireless LAN.

Key words: wireless LAN; 802.1x protoco; security; application

上海铁路局电子调度楼智能信息化工程于2003年上半年完工，AP无线信号已经覆盖整个电子调度楼，它已成为铁路局新的决策和指挥中枢，配有视频会议及网上教育等多项应用，但同时也面临着网络安全的问题。

1 无线局域网的安全

1.1 无线局域网安全存在的主要问题及安全技术

无线网络面临着安全风险和安全问题的困扰，其中主要包括：（1）来自网络用户的进攻；（2）未认证的用户获得存取权；（3）来自公司的窃听、泄密等。

针对以上威胁问题，常规的无线网络安全技术有以下几种：

（1）服务集标识符（SSID，Service Set ID）；（2）物理地址（MAC，Media Access Controller）过滤；（3）连线对等保密（WEP，Wired Equivalent Protection）；（4）虚拟专用网络（VPN，Virtual Private Network）；（5）端口访问控制技术（802.1x）。

2 802.1x无线网络

2.1 IEEE 802.1x协议

收稿日期：2004-09-02
作者简介：杨伟青，助理工程师。

IEEE 802.1x称为基于端口的访问控制协议（Port based network access control protocol）。IEEE 802.1x协议的体系结构包括3个重要的部分：Supplicant System客户端、Authenticator System认证系统和Authentication Server System认证服务器。

（1）客户端系统

一般为一个用户终端系统，该终端系统通常要安装一个客户端软件，用户通过启动这个客户端软件发起IEEE 802.1x协议的认证过程。

（2）认证系统

通常为支持IEEE 802.1x协议的网络设备。该设备对应于不同用户的端口（可以是物理端口，也可以是用户设备的MAC地址、VLAN和IP等），有两个逻辑端口：受控（controlled Port）端口和不受控端口（uncontrolled Port）。不受控端口始终处于双向连通状态，可保证客户端始终可以发出或接受认证。受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。

（3）认证服务器

通常为RADIUS服务器，该服务器可以存储有关用户的信息，比如用户所属的VLAN、CAR参数、优先级和用户的访问控制列表等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量就将接受上述参数的监管。

2.2 802.1x身份验证

2.2.1 基于端口的网络访问控制的标准草案

在基于端口的网络访问控制交互期间，LAN 端口采用两个角色之一：验证者或恳请者。如果是验证者角色，LAN 端口在其允许用户访问可以通过那个端口访问的服务之前执行验证。如果是恳请者角色，LAN 端口请求访问可以通过验证者的端口访问的服务。身份验证服务器可以是单独实体或与验证者共存的代表验证者检查恳请者的凭证。验证服务器然后响应验证者，表明恳请者是否具有访问验证者的服务的授权。

IEEE 802.1x 身份验证提供对 802.11 无线网络和对有线以太网网络的身份验证的访问权限。IEEE 802.1x 通过提供用户和计算机标识、集中的身份验证以及动态密钥管理，可将无线网络安全风险（例如，对网络资源的非授权访问以及偷听）减小到最低程度。

通过802.1x，当一个设别要接入中心设备，中心设备就要求一组证书。用户提供的证书被中心设备提交给服务器进行认证。这台服务器称为RADIUS，也就是Remote Authentication Dial-In User Service.这整个过程被包含在802.1x的标准EAP（扩展认证协议）中。EAP是一种认证方式集合，可以让开发者以各种方式生成他们自己的证书发放方式，EAP也是802.1x中最主要的安全功能。2.2.2EAP方式主要有4种。

（1） EAP-MD5

通过MD5对传向RADIUS服务器的用户名和密码加密。EAP-MD5不需要密钥管理和动态密钥生成，而需要使用静态WEP密钥。但攻击者仍然可以监听无线通信，解密WEP密钥。一旦密钥被破解，他们就可以轻松地查看整个网络上的数据。

（2）EAP-Cisco Wireless（LEAP）

这是Cisco公司配合802.1x标准推出的，是其他EAP方式的基础。LEAP从客户端接受用户名和密码，并将这些数据传到RADIUS服务器上进行认证。和MD5不同之处就在于，LEAP集成在了802.1x/EAP规范中。LEAP一旦认可了该用户，WEP密钥就动态生成一个。这就是说每个用户使用的WEP密钥都是不一样的，彼此之间互相也不了解。而且，RADIUS服务器还让用户每隔一段时间就重新登陆，并重新生成一个WEP密钥。这样就使侵入者没有足够的时间来破解某个密钥。LEAP还提供客户和中心设备之间的双向认证。这也就解决了非法中心设备的问题。

LEAP也不是没有弱点。首先，传递认证数据的机制都是MS-CHAPv1，这个协议弱点很多，手法得当可以很快破解。其次就是LEAP只能在Cisco设备上使用，因为只有Cisco设备可以在无线客户机上加入LEAP功能。

（3）EAP-TLS

EAP-TLS没有采用用户名加密码的认证方式，而是使用X.509认证方式。与LEAP类似，与EAP-LTS动态生成的WEP密钥只会使用一次，并且会对中心设备和接入客户两方都进行认证。

（4）EAP-TTLS

中心设备要使用服务器证书向客户机证明自己的合法性，客户机才会向其发出相应的认证资料。EAP-TTLS接着将这些信息传给管理员制定的回应机制中（PAP、CHAP、MS-CHAPv1、MS-CHAPv2、PAP/Token Card、EAP等）。这种方式的唯一问题就在于比EAP-TLS的双重认证要显得单薄一些。而PEAP（Protected EAP）方式也与之类似。

3 802.1x的实际应用

3.1 选择进行证书服务器和RADIUS服务器

我们选择了CiscoACS 3.2和微软的证书服务器（CA）系统以及活动目录（Active Directory）。所有的客户都接入这样的中心设备中，而对用户的认证也在中心设备中进行。

3.2 准备可以发送认证信息的中心设备

EAP协议一诞生，中心设备就可以使用802.1x认证。我们选择了CiscoAironet 1100系列产品，完美支持802.1x协议，兼容性好。

3.3 客户端软件

Windows XP 有内建的EAP-TLS和EAP-MD5客户端，正好配合微软证书系统。EAP-TLS的认证过程：

（1）客户端发送EAP开始信息到AP；（2）AP返回一个EAP请求识别信息；（3）客户端通过EAP回应信息，向AP发送它的Network Access Identifier（NAI），即它的用户名；（4）AP通过RADIUS访问请求信息向RADIUS服务器发送NAI；（5）RADIUS服务器向客户端回应它的数字证书；（6）客户端确认服务器端的数字证书；（7）客户端向RADIUS服务器发送它的数字证书；（8）RADIUS服务器通过客户端的证书确认客户端的合法性；（9）客户端和服务器获得加

文章编号：1005-8451（2004）10-0037-03

加快推行上海铁路局无纸化办公

杨 骅
（上海铁路局 办公室文书科，上海 200071）

摘 要：通过对办公自动化和无纸化办公的分析，结合上海铁路局试点实行电子公文管理系统现状，由浅入深地揭示了其自身优势和存在的不足之处，并提出了新的设想和展望，以此来取长补短，查缺补漏，推动上海铁路局办公信息化建设深入发展。

关键词：办公自动化；无纸化办公；电子公文；观点
中图分类号：U29-39 文献标识码：B

Opinion on accelerating office automation in Shanghai Railway Administration

YANG Hua
(Amanuensis Office of Shanghai Railway Administration, Shanghai 200071, China)

Abstract: Combined with the current situation in the application of Electronic Documents Management System, it was pointed out the advantage and disadvantage through analyzing on office automation, put forward the new idea and expectation by doing so to remove the weak points and push forward the establishment of further development of office informatization in Shanghai Railway Administration.

Key words: office automation; handling documents by computer; electronic documents; opinion

上海铁路局实现办公自动化经历了 3 个阶段：

第 1 个阶段的主要标志是办公过程中普遍使用现代办公设备；

第 2 个阶段主要标志是办公过程中普遍使用电脑和打印机，通过电脑和打印机进行文字处理、表格处理、文件排版输出和进行人事财务等信息的管理等；

第 3 个阶段主要的标志是办公过程中网络技术的

收稿日期：2004-09-02
作者简介：杨 骅，干事。

密密钥；（10）RADIUS 服务器向 AP 发送 RADIUS ACCEPT 信息，包括客户端的 WEP 密钥，表明成功的认证；（11）AP 发送给客户端一个 EAP 成功信息；（12）AP 向客户端发送用客户端 WEP 密钥加密的广播密钥和密钥长度。

在此项目中，为无线网络专门设立一个 vlan，其网络地址实行动态分配，没有经过认证的客户端不会得到 IP 地址；用户若需使用无线网时先提出申请开通无线网认证，由电子中心开通，客户端必须先在可靠的网络连接下（如有线网络）下载和安装根证书（由 CA 服务器生成），并需启动 802.1x 认证服务（需要经过一定配置），完成后系统会提示输入用户名和密码（此用户名密码可以通过 Cisco ACS 软件映射 Active Directory 里的用户数据库，通过专门的页面用户可以自行修改密码），认证通过，客户端得到 IP 地址，便可得到方便、快捷、安全的网络服务。

4 结束语

当前，网络安全的形势相当严峻，网络攻击和病毒侵害等事件不断发生，而无线网络又是近年来新涌现的科技产物，其安全方面的技术和设备不多。但我们又不能拒绝其方便快捷和灵活的使用方式，在实施这套方案后，可以有效加强网络的安全性和可靠性，此外，802.1x 同样也适合有线网络，保证铁路信息安全稳定高效地传输。

参考文献：

[1] （美）Dr. Cyrus Peikari, Seth Fogie. 无线网络安全[M]. 北京：电子工业出版社，2004.
[2] （美）Jim Aspinwall. 无线网络-安装、调试与维护[M]. 北京：电子工业出版社，2004.