基于802.1X的宽带认证技术在校园网中的应用

Campus Broadband Network's Authentication Based on 802.1X

肖志新 （湖南吉首大学网络中心 416000）
杨岳湘 （长沙国防科技大学网管中心 410073）
杨 霖 （湖南吉首大学网络中心 416000）

摘 要：本文介绍了当前几种宽带接入认证技术，在对其进行了比较的基础上详细讨论了802.1x技术的原理和实现过程，并给出了一个大学校园网应用的解决方案。

关键词：802.1x协议 认证 端口访问控制

1 IEEE 802.1X认证系统原理

1.1 802.1X简介

802.1X技术是基于端口（包括物理端口和逻辑端口如MAC地址、VLAN等）的认证技术，其认证阶段采用EAP（RFC2284）报文，EAP报文是PPP报文的扩展，其认证阶段与PPPoE方式类似。其认证过程为：用户通过802.1X客户端软件发起认证（EAPol报文）->交换机终结EAPoA报文并向认证服务器转发EAP报文->认证通过->DHCP服务器分配IP地址->受控端口打开->正常通信。由此可以看出，802.1X在认证阶段进行EAP封装，通信过程中采用TCP/IP协议。

IEEE802.1x认证有三个角色，分别为申请者（客户端）、认证系统、认证服务器。

申请者（Supplicant）：申请者即IEEE802.1x标准描述中的Supplicant，是最终用户所扮演的角色。它请求对网络服务的访问，并对认证系统的协议请求报文进行应答；

认证系统（Authenticator）：

认证系统控制申请者对网络服务的访问。它实际在认证过程中只是一个认证信息交换的途径，负责与申请者通信，将申请者的认证请求发往认证服务器，而后根据认证服务器的指示执行对申请者的授权；

认证服务器（Authentication Server）：认证服务器是最终用户的认证服务的实际提供者。它认证用户的身份并将认证结果通知认证系统。

1.2 原理

IEEE 802.1x协议的精华就是关于受控和非受控的访问（Controlled and uncontrolled access），以下将详细描述关于受控和非受控的访问。

如图1所示，认证系统的端口分成两个逻辑端口：受控端口和不受控端口。

不受控端口只能传送认证的协议报文，而不管此时受控端口的状态是已认证状态（Autherized）还是未认证状态（Unautherized）。受控端口传送业务报文。如果用户通过认证，则受控端口的状态为已认证状态，可以传送业务报文。如果用户未通过认证，则受控端口的状态为未认证状态，不能传送业务报文。

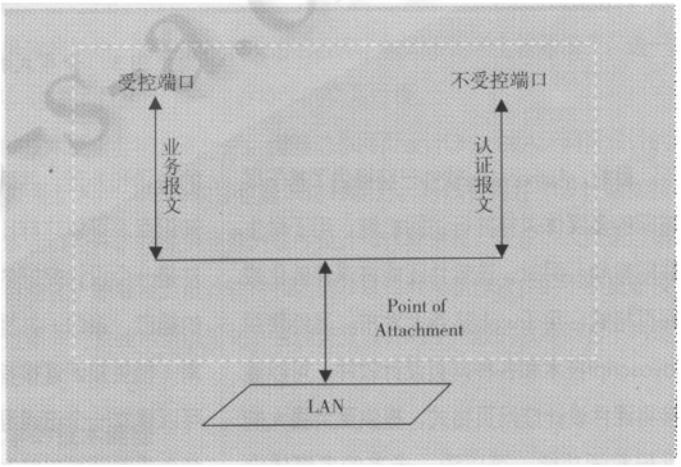

图1 受控制口和不受控制口

如图2所示，当用户未通过认证时，受控端口处于开路，端口状态为未认证状态，此时交换机的交换功能是关闭的，也就是说交换机无法像传统的通过查找目标MAC地址来进行交换，如果用户有业务报文是无法通过的。当用户通过认证后，受控端口闭合，端口状态为通过认证状态，此时交换机的交换功能打开，就和传统的交换方式一致

了，用户的业务报文就可以顺利通过。

对于端口的控制，可以有很多种方式。端口可以是物理的端口，

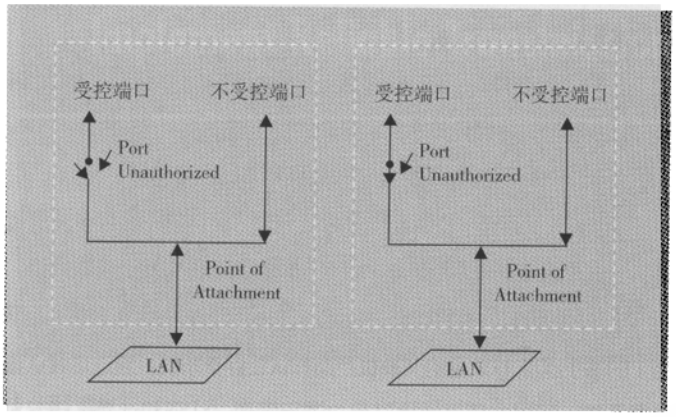

图 2　受控端口的状态变化

也可以是用户设备的MAC地址，如果设备支持全程的VLAN，也可以把VLAN ID看成是端口。

基于物理端口的控制方式，每个物理端口包含两个逻辑端口：受控端口和不受控端口。不受控端口传递认证的协议报文，受控端口传递业务报文。采用这种端口控制方式，则必须在与最终用户直接相连的交换机实现802.1x认证，在相应的端口进行控制。这样会导致低端交换机的成本上升，势必增加整个网络的建网成本。

另一种端口控制方式就是基于用户设备的MAC地址进行控制。把用户设备的MAC地址看成端口，每个MAC地址有两个逻辑端口：受控和不受控端口。

如果用户要访问LAN的资源，则首先其MAC地址必须处于激活状态，然后才能有协议报文通过不受控的端口传递，开始整个认证过程。如果其MAC地址未激活或者被管理性的禁止，则无法进行认证。

1.3 认证过程

认证的发起可以由用户主动发起，也可以由802.1X交换机发起。当802.1X交换机探测到未经过认证的用户使用网络，就会主动发起认证；用户端则可以通过客户端软件向802.1X交换机发送EAPOL-Start报文发起认证。

（1）由802.1X交换机发起的认证。当802.1X交换机检测到有未经认证的用户使用网络时，就会发起认证。在认证开始之前，端口的状态被强制为未认证状态。如果客户端的身份标识不可知，则802.1X交换机会发送EAP-Request/Identity报文，请求客户端发送身份标识。这样，就开始了典型的认证过程。客户端在收到来自802.1X交换机的EAP-Request报文后，将发送EAP-Response报文响应802.1X交换机请求。802.1X交换机支持定期的重新认证，可以随时对一个端口发起重新认证的过程。如果端口状态为已认证状态，则当802.1X交换机发起重新认证时，该端口通过认证，那么状态保持不便；如果未通过认证，则端口的状态改变为未认证状态。

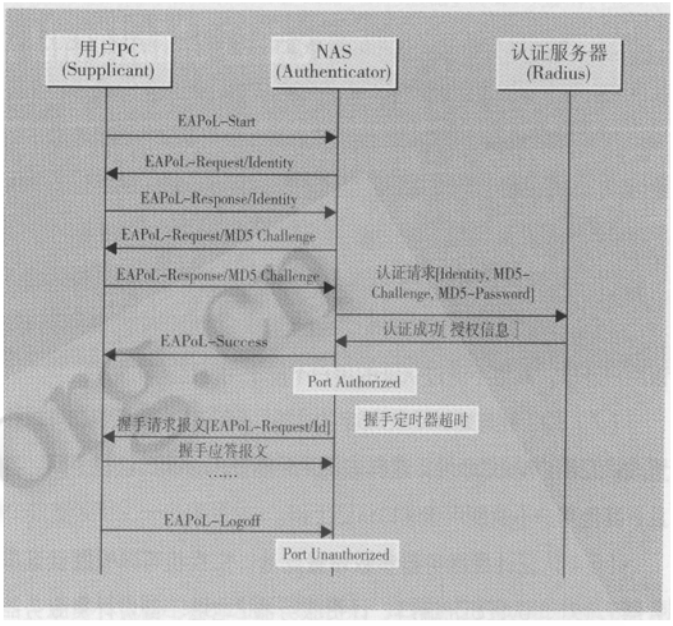

图 3　802.1X 基本业务流程图

（2）由客户端发起认证。如果用户要上网，则可以通过客户端软件主动发起认证。客户端软件会向802.1X交换机发送EAPOL-Start报文主动发起认证。802.1X交换机在收到客户端发送的EAPOL-Start报文后，会发送EAP-Request/Identity报文响应用户请求，要求用户发送身份标识，这样就启动了一个认证过程。

2 系统的实现和应用

2.1 客户端系统

IEEE 802.1X认证协议已经得到了很多软件厂商的重视，目前微软也在大力推广，并在WindowsXP操作系统中整合了IEEE 802.1X客户端软件。

2.2 认证系统

许多网络产品厂商推出了支持IEEE 802.1X认证协议的交换机产品。例如国内的华为、实达、神州数码、港湾等等。不管采用哪一款交换机，认证系统必须实现以下功能，才能算是一个比较完整的认证系统：

（1）用户接入控制功能。打开IEEE802.1x认证功能后，缺省情况下，所有用户都处在未认证状态。此时，用户对网络进行访问的所有信息都将被交换机禁止，当然不包括认证过程需要的报文。交换机将为认证需要的报文维护一个专门的通道，保证所有用户都可以进行正常的认证过程。用户认证通过后，交换机才允许该用户访问网络的所有信息通过。

（2）强制认证功能：强制已认证即管理员可以在交换机上设置一

些特定的用户，这些用户不需认证就可以正常访问网络。

（3）强制非认证功能。强制非认证即管理员限制某些特定用户不允许进行认证，即永远都无法使用网络。

（4）重认证功能。在设定的重认证时间后自动向用户（802.1X客户端软件）发出重认证请求，以验证再次验证用户身份的合法性。

（5）代理进程检测功能。当用户启动一个代理服务器软件后，交换机能自动检测到代理进程，并终止用户的接入。这可以防止多个用户通过代理接入。

（6）端口锁定用户功能：当一个用户在一个802.1X交换机端口通过认证后，该端口即立即锁定该用户的MAC地址，实现该端口只对该用户开放，其他不通过认证的用户不能使用网络的功能。

（7）802.1X与端口MAC绑定的功能：802.1X交换机端口可以设置成认证用户MAC地址，这样该用户只能使用该端口认证上网，并且，其他用户不能使用该端口认证上网。

（8）认证计费服务器参数设置灵活：交换机可以设置认证服务器IP地址、认证UDP端口、计费服务器IP地址、备份计费服务器IP地址、计费UDP端口、认证服务器与认证者（交换机）的验证字。特点是设置灵活方便，同时可靠性高。认证服务器通常使用Radius服务器。

3 结论

总结起来IEEE 802.1x有以下五大优点。

（1）简洁高效：纯以太网技术内核，保持IP网络无连接特性，去除冗余昂贵的多业务网关设备，消除网络认证计费瓶颈和单点故障，易于支持多业务。

（2）容易实现：可在普通L3、L2、IP DSLAM上实现，网络综合造价成本低。

（3）安全可靠：在二层网络上实现用户认证，结合MAC、端口、帐户和密码等绑定技术具有很高的安全性。

（4）行业标准：IEEE标准，微软操作系统内置支持。

（5）易于运营：控制流和业务流完全分离，易于实现多业务运营，少量改造传统包月制等单一收费制网络即可升级成运营级网络。

（6）在我们目前的校园网环境中，采用了锐捷网络（原实达网络）的基于802.1x认证的交换机产品和认证计费系统，通过这套认证计费系统，可以方便灵活地对用户进行管理、认证和计费。随着对802.1x认识的不断加强，必将成为大学校园网管理的主要手段之一。

参考文献

1 中国广电，宽带用户认证管理方式和技术实现探讨，http://www.cbtn.com/info/news.asp?new=1628

2 Stone. 新的宽带认证方式ББIEEE802.1x协议，http://www.yesky.com/20020530/1613717.shtml

3 Tony Jeffree, Neil Jarvis, Mick Seaman. IEEE standard for local and metropolitan area networks. Port-based network access control. IEEE Std 802.1x-2001。