利用RADIUS进行FTTH宽带网络认证

鄢野春[1],佘 堃[1],聂为清[2],周明天[1]
(1.电子科技大学 计算机学院,四川 成都 610054;
2.汇源光通信股份有限公司,四川 成都 611731)

摘 要:宽带接入已经逐渐成为很多家庭的必要设施之一,ADSL和小区宽带是当前主要的接入方式。而带宽需求的日益提高需要有更高速的接入网络,光纤到户(FTTH)是一种比较理想的方案。针对当前兴起的光纤到户宽带接入方式,介绍了城域FTTH宽带网络宽带接入认证方式,利用既有的RADIUS标准对用户做认证,以Web的方式,具有良好的通用性和扩展性,为改进现有的宽带用户认证提供了一条更为通用的解决方案。

关键词:远程认证接入用户服务;光纤到户;Web认证
中图分类号:TN915.63 **文献标识码**:A **文章编号**:1673-629X(2006)05-0112-03

Authentication for FTTH Broadband Network with RADIUS

YAN Ye-chun[1],SHE Kun[1],NIE Wei-qing[2],ZHOU Ming-tian[1]
(1.Computer Sch., University of Electronic Science and Technology,Chengdu 610054,China;
2.Huiyuan Optic Communication Co.Ltd, Chengdu 611731,China)

Abstract:Broadband network has become a necessary facility of many families. ADSL and FTTB take main part of current broadband market. Focusing on the booming FTTH broadband accessing,this paper introduces FTTH broadband for city networking, and gives a kind of authentication method, which is based on RADIUS protocol and through Web. It has strong expansibility and general availability, and provides a way for improving present authentication.

Key words:RADIUS;FTTH;Web authentication

0 引 言

FTTH(Fiber To The Home,光纤到户)是近年来网络建设不断追求的目标和技术方向,但是由于技术、成本、市场方面的障碍,至今还没有大规模的发展。然而,随着技术的提高和成本的降低,光纤网络的发展越来越快,也引起了业界的关注,相信未来几年内会有巨大的发展。认证模块是宽带运营系统中的重要部分,而认证方式的选择决定了用户接入的效率和质量[1]。

1 系统介绍

1.1 FTTH介绍

当前宽带接入领域大都使用ADSL(非对称数字用户线路)、Cable modem(电缆调制解调器)、FTTB(Fiber To The Building)技术提供接入网络服务,由于其无法提供长距离及高速宽带等系列服务,渐渐已无法适应固网运营商在原有带宽基础上推出更多更新的服务项目。所以基于无源光网络(PON)的可提供全业务、高速率的光纤到户(FTTH)光接入网无疑是宽带接入网的最有效的解决方案。

典型的城域网EPON系统的架构如图1所示。

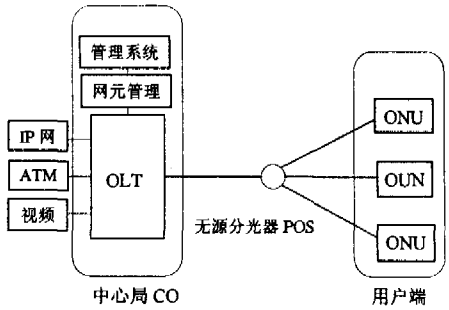

图1 EPON架构模型

EPON主要分成三部分,即OLT(Optical Line Termination),ODN(Optical Distribution Network)和ONU(Optical Network Unit)。其中OLT位于局端,一般放在中心机房(CO,Central Office);ONU位于用户端。

(1)OLT:在EPON系统中,OLT既是一个交换机或路由器,又是一个多业务提供平台(MSPP),它提供面向无源光纤网络的光纤接口。OLT到ONU间的距离最大可达20km,如果使用光纤放大器(有源中续器),距离还可

收稿日期:2005-09-09
基金项目:四川汇源光通信股份有限公司资助项目
作者简介:鄢野春(1981-),男,四川资中人,硕士研究生,研究方向为网络计算;周明天,博士生导师,教授,研究方向为网络计算、网络安全技术。

以扩展。高容量 EPON 能够提供上下行达到 1Gb/s 的带宽,在未来 10 年内能够满足用户需求。

(2)ODN:由无源分光器 POS 和光纤构成。

(3)ONU:用户端的 ONU 采用以太网协议,实现了成本低廉的以太网第二层和第三层交换功能。

1.2 RADIUS 协议基础

RADIUS 协议即远程认证接入用户服务(Remote Authentication Dial In User Service),最初是由 Lucent 公司开发,现在的最新版为 RFC2865、RFC2866,也是新一代 OSS(运营支撑系统)标准中指定的相关标准之一。作为一种电话接入 Internet 的认证/计费协议。RADIUS 具有很好的扩展性、安全性,易于管理,同时还有很好的记账功能,所以现在的大规模宽带认证计费,不管采用何种接入方式,多数仍然使用 RADIUS 协议,或者在 RADIUS 之上开发的非标准 RADIUS + 协议,几乎所有的 NAS(Network Access Server)设备都支持标准 RADIUS。RADIUS 使用 UDP 协议,RADIUS 服务分为客户端和服务器端,接入设备 NAS 通常是客户端。用户,NAS,RADIUS 服务器的关系如图 2 所示[2]。

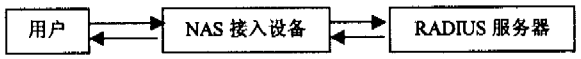

图 2　位置关系图

RADIUS 数据包格式[3]如图 3 所示。

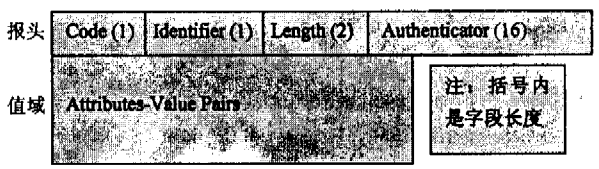

图 3　RADIUS 数据包格式

Code:报文类型代码,RADIUS 协议定义了 8 个类型代码和一个保留代码;

Identifier:用于请求和应答包的匹配;

Length:包长度,包括从 Code 到 Attributes 的字节数;

Authenticator:用于验证服务器端的应答,另外还用于用户口令的加密,也就是 CHAP 认证中的 Challenge;

Attributes:认证用到的属性对,以数字表示 Attribute(如 1 表示 User－Name),RFC 定义了 63 种(1～63),其中第 17,21 没有定义,40～59 被保留给计费可以根据 RADIUS 服务软件和 NAS 设备的种类自行决定其类型和作用,详见 RFC2865[4]。

RADIUS 支持多种认证方式,包括 PAP(Password Authentication Protocol RFC1334),CHAP(Challenge－Handshake Authentication Protocol RFC1471 RFC1812),或者其他认证协议,比如 Windows 的 Domain 属性,只要 NAS 和 RADIUS 服务软件都支持即可。

2　认证方案

认证方式目前主要有 3 种:PPPoE(Point to Point Protocol over Ethernet)、IEEE 802.1X、Web 认证[5,6]。PPPoE 是很成熟的技术并且有完善的标准,但是不适合电信多元业务的开展,并且可扩展性较差;IEEE 802.1X 方式是一种基于端口控制的认证方式,主要用于无限网络认证,简单的说,在通过认证之前用户只有管理和认证端口开放,其他业务端口关闭,通过认证之后打开相应业务端口。此标准最初是为无线认证授权指定的,也可以用于以太网,优点是可以通过直接升级现有交换机达到管理目的,成本低,效率高;缺点是标准有待成熟化,也需要客户端软件,而业务支持需要做大量的重新开发,现有的 RADIUS 软件业不支持,需要重新开发。

而 Web 认证不需要客户端软件,可扩展性强,适合开展各种业务,升级维护也比较方便,虽然现在没有正式的标准,但各大厂商的设备都已经支持。

2.1 Web 认证流程

Web 认证的流程如下:用户开机并通过 NAS 服务器获得 IP 地址,然后用户访问登录页面,用户输入用户帐号信息并发往认证服务器(RADIUS),认证服务器获得用户 MAC/IP/VLAN ID 作为用户标记,认证服务器反馈认证成功信息,局端设备(NAS)将用户 VLAN ID、用户端口、用户 IP 地址和 MAC 地址进行可选择性的绑定作为用户认证识别的标志并开放用户的上网功能。其时序图如图 4 所示。

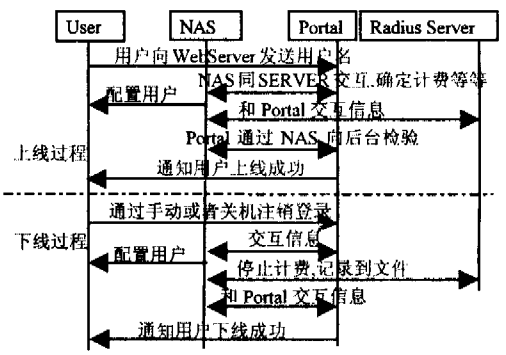

图 4　Web 认证方案时序图

Web 认证用到的各服务器在 FTTH 中的位置如图 5 所示。

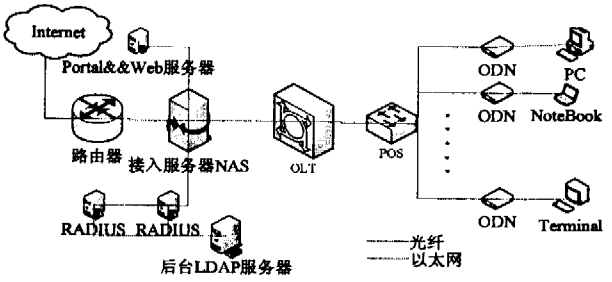

图 5　FTTH 网络架构

2.2 各服务器软件配置

测试服务器的配置环境如下文(第 3 节)所示。

·freeraduis:认证方式为 CHAP,后台目录服务为 OpenLDAP,注意填写 LDAP 的正确位置,打开日志功能;

·OpenLDAP 使用了 core 和 freeradius 提供的 RA-

DIUS－LDAPv3 两个 schema 文件，并且设置了相应的目录结构，通过 ldif 文件加入记录，每一条 user 记录中包括用户名和密码，以及认证类型 Auth－Type，内容的多少可以根据需求(如计费需求)增减。

2.3 Web 认证中的问题

·NAS 和 Portal 之间的通信协议不是标准协议，需要 NAS 设备提供商提供接口，否则不能交互；

·用户端浏览器第一次连接时 NAS 应将其定向于 Portal 的页面上，之后用户端通过 Web 执行 Java 小程序用以计时或者流量等；

·用户非正常下线的处理：可以通过 NAS 定时发送握手信息给用户主机，如果连续 3 次不响应，可以判断用户离线。

3 RADIUS 服务器的性能测试

RADIUS 服务器的性能关系到正式投入运行后用户的等待时间、网络稳定性，直接影响到服务质量的好坏，所以一个简单的性能测试是必需的：

测试环境为：

· 软件环境：

OS：REDHAT ENTERPRISE Linux AS 3.0

RADIUS：Freeradius－1.0.0－pre3

LDAP：OPENLDAP－2.2.13 + Berkeley. DB. 4.2.25

Database：MySQL－Standard－4.0.20－pc－Linux

WebServ：Apache－2.0

· 硬件环境：

4 台普通 PC + Dell Linux 服务器

· 网络环境：

Hub 式共享局域网内

测试结果如图 6 所示。

图中横轴表示使用的客户机的台数，纵轴表示 log 文件中平均每分钟服务器响应的个数。显然随着认证来源的增加，服务器响应速度有所减慢，但总体的负载能力基本满足电信负荷的要求，并且这里是在普通试验环境，若移植到分布式或者集群的环境中，负载能力会进一步提高。

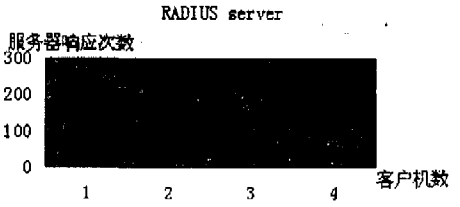

图 6 性能测试结果

4 结 论

描述了 FTTH 宽带网络中的用户 Web 认证技术，并且对其性能作了一定的测试，Web 认证有很明显的优点，当然也有一些缺点，如认证效率相对于 PPPoE 较低[7]，但现代 OSS 强调的是“以客户为中心”，对新业务的支持要非常灵活，而这正是 Web 认证的优点，也是未来发展的方向。可以预见，随着 FTTH 宽带业务的进步和发展，Web 认证技术会更有用武之地。

参考文献：

[1] 邹 洁. 宽带接入认证和计费方式分析[J]. 广东通信技术，2002(6)：15－20.

[2] 崔晓波. RADIUS 协议的原理(上)[J]. 中国数据通信，2001(2)：49－51.

[3] Hassell J. Radius[M]. America：O'Reilly，2002.

[4] RFC2865，RFC2866. Remote Authentication Dial In User Service，RADIUS Accounting[S]. 2000.

[5] 李有斌. 宽带城域网建设主要接入认证方式及其分析[J]. 江西通信科技，2003(3)：40－41.

[6] 邢小良. 宽带网接入认证的发展方向——WEB 认证[J]. 通信世界，2002(4)：23－26.

[7] Hill J. An Analysis of the RADIUS Authentication Protocol [EB/OL]. http://www. untruth. org/josh/security/radius/radius－auth. html，2001.

(上接第 111 页)

实现了 Kerberos 认证和授权功能的无缝集成。

参考文献：

[1] Bellovin S M，Merritt M. Limitations of the Kerberos Authentication System[J]. ACM SIGCOMM Computer Communication Review，1990，20(5)：119－132.

[2] Kehne A，Schonwalder J，Langendorfer H. A nonce－based protocol for multiple authentication[J]. Operating Systems Review，1992，26(4)：84－89.

[3] Itoi N，Honeyman P. Smartcard integration with kerberos v5 [J]. Lecture Notes in Computer Science，2001，2041：73－78.

[4] 蒙 杨，刘克龙，卿斯汉. 一种利用公钥体制改进 Kerberos 协议的方法[J]. 软件学报，2001，12(6)：872－877.

[5] 文铁华，谷士文. 增强 Kerberos 协议安全性的改进方案[J]. 通信学报，2004，25(6)：76－79.

[6] Steiner J G，Neuman B C，Schiller J I. Kerberos：An Authentication Service for Open Network Systems[A]. In Proceedings of the {USENIX} Technical Conference[C]. [s. l.]：USENIX Association，1988. 191－202.

[7] Neuman B C. Proxy－Based Authorization and Accounting for Distributed Systems [A]. International Conference on Distributed Computing Systems [C]. [s. l.]：The Washington Technology Center，1993. 283－291.

[8] Au R，Looi M，Ashley P. Cross－domain one－shot authorization using smart cards[A]. In Proceedings of the 7th ACM conference on Computer and communications security[C]. [s. l]：ACM Press，2000. 220－227.