基于 DHCP+的接入认证系统的技术浅析①

Technology of Access and Authentication System Based on DHCP+

徐润沁 (中国科学院研究生院 北京 100080)

刘军杰 (北京邮电大学 软件学院 北京 100876)

摘 要: 本文提出了一种基于 DHCP 协议通过控制终端用户的 IP 地址分配实现控制用户接入的认证鉴权技术，确保了以太接入的安全性、支持运营商对接入用户进行控制和管理的接入认证。首先从分析 PPPoE 的技术缺陷入手，提出了利用 DHCP 协议来实现接入认证，同时，通过扩展 DHCPoptions 属性在网络安全、网络监控以及用户控制和终端识别等方面的应用，使得运营商可以将这些属性与用户认证和地址分配策略结合起来，完成统一接入控制。最后，以中国网通某分公司的宽带用户的接入认证管理系统为例来介绍利用 DHCP+接入认证技术功能的实现。

关键词: DHCP PPPoE DHCP+ BRAS 接入认证

1 概述

随着互联网宽带业务的不断发展，IPTV、NGN、3G 业务的广泛应用，PPPoE 接入认证技术已逐渐暴露出其劣势。为了更好的开展业务，运营商迫切需要寻找一种适应多业务需求且灵活、可扩展的技术来支撑，这种技术同时能够确保以太接入的安全性、支持运营商对接入用户进行控制和管理的接入认证技术。DHCP+接入认证技术作为一种基于 DHCP 协议通过控制终端用户的 IP 地址分配实现控制用户接入的认证鉴权技术能够满足这种需求。DHCP+目前尚处于发展初期阶段，尚未推出正式的标准。目前，DHCP+在国内驻地网运营商的小区宽带或大客户接入中有小规模应用，海外地区的城域网建设中也有部分应用。

2 PPPoE技术的缺陷

PPPoE 协议(Point to Point Protocol over Ethernet，以太网上的点到点协议)基于 PPP 协议(Point to Point Protocol，点到点协议)演化而成，在宽带网络建设初期解决了 ADSL 技术在安全接入方面的很多问题而被运营商广泛使用。但随着网络的不断发展，宽带网络业务的不断增多，尤其是 IPTV、NGN、3G 等业务的开展，PPPoE 已难以支撑上述业务的开展。

(1) PPPoE 必须在网络的二、三层间部署一个网关型设备 BRAS，由于该设备只能采用集中部署方式，容易造成网络应用瓶颈，从而限制了网络和应用的平滑扩展，并且不能很好的支持组播。

(2) BRAS 设备无法进行统一的地址管理和设备管理，属于分散型单点应用。

(3) BRAS 设备不能支持冗余备份，负荷分担，容易造成单点故障。

(4) PPPoE 的协议扩展性较弱，难以支持未来新业务的开展。

(5) PPPoE 的认证和业务无法分离，造成处理效率低下，性价比较低。

3 利用DHCP技术实现接入认证

DHCP 真正意义上实现符合互联网未来发展趋势的 IPoE 网络承载技术。

DHCP 较其他接入认证技术具备以下优势:

(1) 部署与网络拓扑无关，应用灵活。

(2) 认证与业务流分离，处理效率高，能够实现 IPoE。

(3) 扩展属性丰富，终端和传输层设备均可通过对 DHCP OPTION 扩展属性的操作实现和服务端的交互。

① 收稿时间:2008-10-21

但是，由于 DHCP 协议原本为局域网所设计，不能进行认证、授权和 SESSION 控制，也不能精确采集用户的上网时长，不适合广域网；DHCP SERVER 由于设计简单，功能单一，不能满足电信级运营的需要。虽然设备厂家努力在改进这些缺点，并且在 DHCP 协议上进行了各种扩展，但是总体上仍然没有解决上述问题，最终 DHCP 协议还是无法被大规模采用。

4　DHCP+接入认证技术对DHCP的扩展

DHCP 协议是 DHCP+接入认证技术的基础，它是 RFC 组织定义的一种标准，采用客户机－服务器工作机制，实现客户机向服务器请求分配 IP 地址的流程。为了解决对用户进行有效的接入认证控制问题和提高接入网络的安全性，DHCP+接入认证技术在网络安全、网络监控以及用户控制和终端识别等方面对 DHCP 协议进行了扩展。

(1) 引入了多权限地址的概念，即在一个三层设备端口下，用户可以根据不同的权限情况得到不同的 IP 地址池中的地址。

(2) 引入了用户的业务使用流程，即打通了用户 AAA 流程和 DHCP 流程之间的关系，通过 MAC+物理端口来表示一个用户，在用户登录以后改变 MAC+物理端口的权限，为其变化对应的 IP 地址。

(3) 网络安全方面，在报文入接口通过对报文匹配 DHCP Snooping 绑定表项，防止了 IP 盗用、用户私接、DHCP Server 仿冒、IP/MAC Spoofing 攻击、DoS(Deny of Service)攻击，规避了 DHCP 协议的安全缺陷。

(4) 网络监控方面，通过对丢弃的非法报文分别计数，在网管系统的配合下，实现针对各种攻击的阀值告警分别输出，提高运维部门的故障定位和解决效率，以降低运营成本。同时，通过和用户之间定义采集时长信息的协议，完成了开始使用到终止使用的时长确认。

(5) 用户控制方面，DHCP PS(DHCP Policy Server)通过建立基于用户物理位置信息的本地数据库，对用户进行认证控制。所谓用户物理位置信息就是标识用户所在的设备、端口以及 QinQ 双层标签信息，当然，所谓用户是用一个或多个 MAC 地址来识别的。用这种方法限制了私拉盗接和用户串用等问题，从而减轻了运维压力，保护了合法用户的权益，为营运增收提供可能。

另外，由于扩展了 DHCP Option 属性的应用，满足不同场合的用户需求，使得运营商可以将这些属性与用户认证和地址分配策略结合起来，完成统一接入控制。

5　DHCP+接入认证技术功能实现介绍

目前，在接入认证领域占主流地位的是 PPPoE 技术，DHCP+认证技术在国内主要还是应用于部分驻地网运营商的小区或酒店接入。本文以中国网通某分公司的宽带用户的接入认证管理系统为例来介绍利用 DHCP+接入认证技术功能的实现

5.1　系统部署

图 1 显示了 DHCP+用于城域网接入认证的应用场景。在该城域网解决方案中，Internet 业务以原有 PPPoE 方式通过 BRAS 设备接入，VoIP、VoD、BTV 等业务以 DHCP+认证方式接入用户。

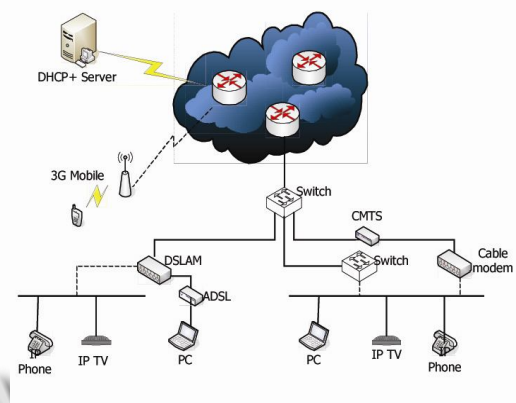

图 1　DHCP+认证接入技术城域网络模型

5.2 DHCP+系统模块架构

宽带网用户通过客户端软件和 DHCP 协议与宽带网接入认证管理系统进行交互，进而接入到宽带网络中，并使用某种特定的网络服务，如图 2 所示。

当该系统中在收到自客户终端的 DHCP Discover 报文后，将依据报文中 Option 描述的设备、所在端口、与开户时录入的用户物理位置数据库信息对照，根据结果进行下一动作，用户再次认证上线时，系统将根据用户 MAC 和录入的用户物理位置数据库信息唯一标识用户。系统用这种方法对用户做接入权限认证，防止用户私接盗用问题，增强用户控制。

此外，由于 DHCP 系统本身不具备用户 Session

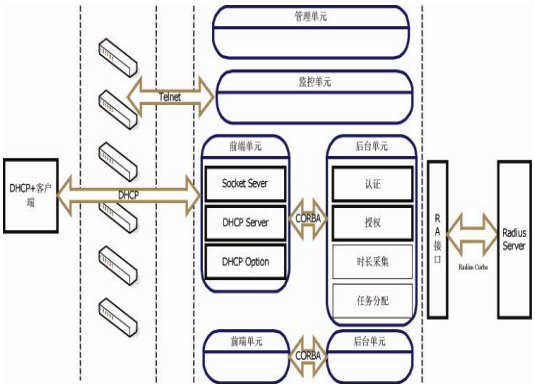

图 2 宽带网接入认证系统结构

管理的功能，而多数运营商采用的是宽带时长用户管理，因此需要系统能够控制和采集用户的时长。为此，系统专门设计了用于用户的身份认证和时长控制的模块能够准确的采集用户的时长。

6 结束语

DHCP+接入认证技术优势主要体现在其组播支持方面。众所周知，组播复制点越接近用户越能节省带宽，而组播复制点一般部署在二层和三层网络的分界线。这就意味着 DHCP+接入认证技术组播优势要充分体现，城域网络必须是三层路由到边缘的组网模式。倘若将来视频分发以 P2P 技术为主，其组播优势便无用武之地。

DHCP+接入认证技术尚处于其发展初期阶段，协议相关标准还没有最终制定，厂家之间的实现标准尚不统一，使其进一步发展完善受限。而且由于其开放性特点，其接入的安全性尚需接受更多的验证和考验。因而这种接入方式有很大局限性，但就目前的状况来看，DHCP+技术越来越被大多数运营商和设备厂家所接受并开始采用，支持 DHCP+规范的设备将越来越多。

参考文献

1 张志方.DHCP+技术分析及其在河南电信宽带 IP 网中的应用.科技创业月刊, 2004(15):151－153.
2 刘联海,周德新.安全 DHCP 系统的设计与实现.信息技术, 2004,(8):41－43.
3 任凤姣,王洪,贾卓生.DHCP 安全系统.计算机工程. 2004,(17):131－133.
4 孙力芾,李生红.DHCP 及 Option82 安全机制的原理与实现.信息技术, 2005,(8):36－39.
5 梁红军,何岩.DHCP 在宽带网络中的应用,光通信研究, 2005,(5):57－59.
6 但松健.校园以太宽带网用户接入认证技术的研究.重庆教育学院学报, 2006,19(3):41－43.
7 赵东升.利用改进的 DHCP+技术实现宽带 IP 网用户认证计费管理.电信科学, 2002,(7).