基于 DHCP 和 MAC 地址动态绑定的用户自助接入认证系统①

李 鹏[1,2], 李晓风[1], 谭海波[1]

[1](中国科学院 合肥物质科学研究院, 合肥 230031)
[2](中国科学院研究生院, 北京 100049)

摘 要: 通用的 DHCP 服务软件缺乏用户终端接入认证功能, 为了实现终端安全准入功能, 必须在 DHCP 系统之外额外部署一些商业软件. 但这些软件往往需要终端安装插件, 因此很难对于多样化的终端准入控制的异构网络提供完全的支持. 基于 MAC 地址动态绑定的 DHCP 认证系统就是为了满足多样化终端异构网络的 DHCP 安全接入需求而设计. 该系统实现了接入认证、用户自助 MAC 地址注册和上网记录查询、DHCP 服务器配置文件管理等功能, 系统灵活、易于配置、不需任何插件支持.

关键词: DHCP; 自助管理; 动态绑定; 接入认证; MAC 地址认证

Self-Management Access Authentication System Based on DHCP and Dynamic MAC Address Binding

LI Peng[1,2], LI Xiao-Feng[1], TAN Hai-Bo[1]

[1](Information Center, Hefei Institutes of Physical Science, Chinese Academy of Sciences, Hefei 230031, China)
[2](Graduate University, Chinese Academy of Sciences, Beijing 100049, China)

Abstract: Common service software implementing DHCP protocol lacks the network-access authentication, which makes DHCP network insecure, and to overcome this shortcoming and ensure the success of terminal and security of access, it has to deploy additional commercial software. However, these software need some plug-ins' support, and any one of these plug-ins is not qualified because of heterogeneity of network and terminal. To meet demands of diverse-terminal heterogeneous-network secure access, a self-management access system was designed which provides authentication function based on dynamic MAC address binding. Besides, this system provides a self-management module which has a vital function for registering and managing MAC address and querying network-access records, and a DHCP-configure file module which aims to dynamically generate and conveniently manage DHCP-Server configuration file. It is flexible and ease-configure without any plug-in.

Key words: DHCP; self-management; dynamic binding; access authentication; MAC address authentication

在 TCP/IP 网络中, 设备必须获取唯一的、独立的 IP 地址后, 才能和其他设备进行通信. 在大型网络中, 通常部署 DHCP 服务器用于动态分配 IP 地址, 然而 DHCP 协议不是安全的, 它没有在 DHCP 服务器分配地址的过程中提供任何认证机制. 为了保证网络的安全性, 通常在应用 DHCP 的网络中部署额外的商业软件, 由于网络的异构性和商用 DHCP 服务器软件需要插件支持, 导致这类软件很难完全满足的 DHCP 易用需求. 本文结合实际应用, 设计了基于 MAC 地址动态绑定的、无需插件支持的 DHCP 认证系统, 解决多终端网络的准入问题.

① 收稿时间:2012-02-27;收到修改稿时间:2012-03-31

1 研究现状

1.1 DHCP 的工作流程

DHCP[1,3]工作在 C/S 模式下, 并采用租赁的方式分配 IP 地址给接入网络的设备. 当终端设备接入网络时, 终端设备会广播一个 DHCP DISCOVER 消息, DHCP 服务器响应这个消息, 并发送一个 DHCP OFFER 消息给终端设备. 终端响应收到的第一个 DHCP OFFER 消息, 并向提供 DHCP OFFER 消息的 DHCP 服务器发送 DHCP REQUEST 消息. DHCP 服务器响应并发送 DHCP ACK 消息进行确认, 至此设备就获得了动态分配的 IP 地址.

由于 DHCP 协议缺乏接入认证机制[6], 为了弥补这个缺陷, 必须引入接入认证机制. 常用的认证机制有: 基于 MAC 的认证机制、基于证书的认证机制和基于用户的认证机制.

2 接入认证机制

2.1 静态绑定 MAC 和 IP 地址

静态绑定 MAC 和 IP 地址是在接入交换设备或网关上设置客户端的 MAC 和 IP 地址的一一对应关系, 因为必须对接入网络的终端设备进行 MAC 和 IP 地址的绑定设置, 所以这种方式只适用于小型局域网, 但是采用这种方式后, 所有用户终端将通过手动设置自己的静态 IP, 导致无法启用 DHCP, 使得网络的易用性大大降低, 目前基本已被废弃.

2.2 基于 MAC 的 DHCP 认证

MAC 认证是基于 DHCP 注册阶段的认证机制, DHCP 服务器在响应 DHCP DISCOVE 消息时, 先验证终端设备 MAC 地址是否合法, 如果不合法, 则丢弃该消息, 如果合法, 响应这个消息. 这种认证模式存在两个问题, 一是不安全, 非法用户完全可以通过手动设置静态 IP 绕过 DHCP 服务器实现网络接入, 二是不能自动管理和生成 DHCP 服务器配置文件, 导致基于 MAC 的认证机制的 DHCP 系统缺乏灵活性.

2.3 基于用户和基于证书的认证机制

基于用户认证机制有 pppoE 和基于 802.1x 协议认证机制, 这两种协议方式都需要结合 Radius 协议构建完整的认证系统. 由于 802.1x 和 pppoE 的客户端软件和网络配置的异构性, 使得基于用户的认证机制不能够完全适应异构的网络要求.

基于证书的认证机制需要第三方的认证服务器参与, 这类认证机制先通过证书对用户进行身份认证, 然后对合法用户分配 IP 地址. 这类认证需要额外的硬件服务器支持, 也缺乏灵活性.

3 系统设计

本文采用了基于 MAC 地址的 DHCP 认证机制, 并对 DHCP-MAC 认证方式进行了改进, 在实现认证功能的同时, 也增加了 MAC 地址注册的 GUI 管理功能、DHCP 服务器配置文件的自动生成和管理功能和接入网络设备的管理功能. 认证系统分为 3 个模块, 一是用户信息管理模块, 二是用户设备 MAC 地址自助管理系统模块(简称 MAC 自助管理模块), 三是实时监控模块, 用于管理 DHCP Server 的配置文件.

3.1 用户信息管理模块

用户信息管理模块实现用户的注册、删除、查询、禁用或者激活和用户信息的修改功能. 用户必须先注册到认证系统成为合法用户, 然后才有权限将终端设备的 MAC 地址注册到认证系统中, 此时用户设备才可以接入网络.

认证系统设置了全局变量 Update-Flag 标志用于及时刷新用户注册的 MAC, 使之在系统中生效. 添加用户、查询用户信息和修改用户都不会影响 Update-Flag 的值, 而删除用户和禁用/激活用户会改变 Update-Flag 的值, 并触发监控例程模块调用处理函数.

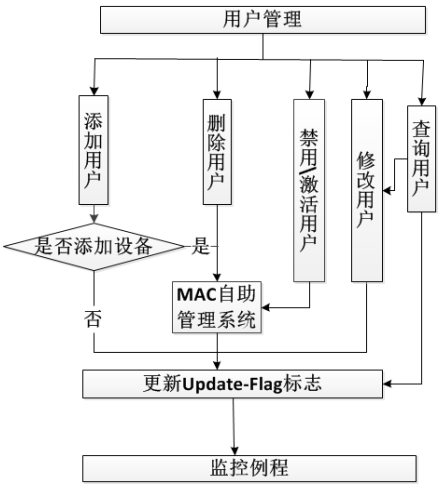

图 1　用户管理模块

认证系统允许用户注册多个 MAC 地址, 删除用户要求删除用户所注册的 MAC 地址, 而禁用用户则保留用户信息和用户注册的 MAC 地址信息以便用户

再次激活, 禁用状态的用户的终端设备不能够从 DHCP 服务器获取 IP 地址.

3.2 用户设备 MAC 地址自助管理系统模块

用户 MAC 地址自助管理系统模块实现用户 MAC 地址的注册、删除、修改和查找等功能, 每次对 MAC 地址的操作, 都会影响 Update-flag 的值, 由此触发监控例程模块调用处理函数.

认证系统认为注册的用户是合法的、可靠的, 系统赋予用户适当的权限管理注册的 MAC 地址. 如图 2 所示, 合法用户有添加、删除、修改、禁用/激活 MAC 的权限. 用户可以登录系统, 完成设备 MAC 的注册和管理, 也可以实时查看自己的网络接入信息, 例如分配的 IP 地址、分配时间、使用网络流量、在线时间等.

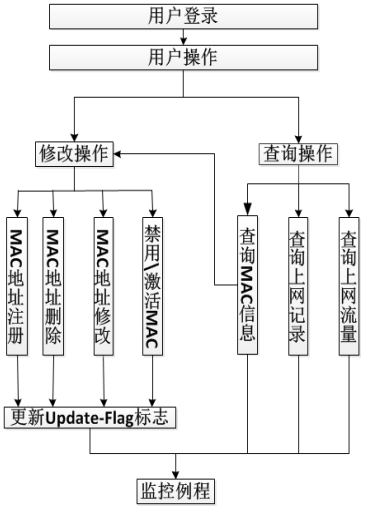

图 2 用户 MAC 自助管理系统模块

3.3 监控例程

监控例程的主要任务是动态更新 DHCP 服务的配置文件(dhcpd.conf). 监控例程轮询检测 Update-flag 标志的值, 如果 Update-flag 标志值为 true 时, 表明系统中注册的 MAC 地址发生了改变, 例如 MAC 地址的添加、修改和删除. 此时监控例程必须从数据库中读取当前系统的 MAC 地址信息, 并以此生成新 dhcpd.conf 文件, 如图 3 所示.

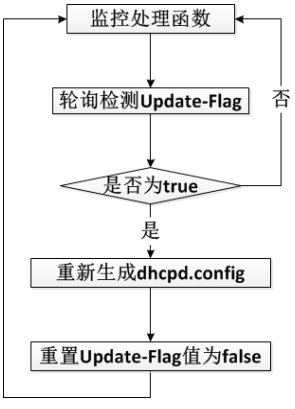

图 3 监控例程

3.4 网络硬件要求和设计

在整个网络中, 系统部署了 2 台 DHCP 服务器以构成 IRF(Intelligent Resilient Framework)网络系统, 其中一个 DHCP 服务器工作在 Master 模式作为主服务器, 另一个工作在 Slave 模式作为备份.

为了实现 MAC 地址在三层交换设备上的动态绑定, 在需要 MAC 地址匹配检测的 Vlan 接口配置 address-check 功能. 如果开启接口上的 address-check 功能, 三层交换设备就会通过学习来自 DHCP 服务器的 DHCP OFFER 封包, 并自动检查 IP 地址和 MAC 地址实现 MAC 在三层设备上的动态绑定. DHCP 协议工作在 UDP 协议基础上, 因此 DHCP IRF 系统必须工作在三层交换设备上.

4 系统运行和结果分析

4.1 MAC 注册

在 Centos 上安装 dhcp-3.0.1-58.EL4 和 dhcpstatus-0.60, 构成 DHCP 服务器. 在 DHCP 系统中注册 MAC 地址的格式为:

```
/*************************************/
host x { hardware ethernet MAC; }
host x { hardware ethernet MAC;
  fixed-address IPADDRESS;};
/*************************************/
```

认证系统将用户的 MAC 地址自动注册到 DHCP 服务器中, 并动态生成 DHCP 服务器配置文件, 代码如下所示:

```
/*************************************/
while ($MAC=mysql_fetch_array($queryresult))
{//实现动态 IP 地址分配的 MAC 注册
   $tempi++;
   $writestr="host    ".$tempi." { hardware
   ethernet ".$MAC['MAC']."; } \n ";
   $fileout=fwrite($dstfd, $writestr);
}
```

```
$fileout=fwrite($dstfd, "} \n");
                    ……
while($MAC=mysql_fetch_array($control_machines))
{//实现静态 IP 地址分配的 MAC 绑定
$tempi++;
$writestr="host control_machine_".$tempi." {\n hardware ethernet ".$MAC['MAC'].";\n
fixed-address ".$MAC['StaticIP'].";\n}\n";
$fileout=fwrite($dstfd, $writestr);}
/*********************************/
```

4.2 配置网络设备的 DHCP 中继功能

为了实现客户端从 DHCP Server 获得 IP 地址, 必须在网络设备中配置 DHCP 中继. 同时为了防止非法用户配置静态 IP 地址访问网络, 必须在支持 DHCP 中继的网络设备配置地址匹配检查[7].

DHCP 服务和设置地址匹配检查的配置:

```
/*********************************/
#定义的 DHCP Server
dhcp-server 0 ip
#不需要 MAC 地址匹配检查的 vlan 配置
interface Vlan-interface1
ip address 192.168.207.254 255.255.255.0
igmp enable
#需要 MAC 地址匹配检查的 vlan 配置
interface Vlan-interface2
ip address 192.168.206.254 255.255.255.0
dhcp-server 0
address-check enable
igmp enable
/*********************************/
```

从 Vlan2 接入的设备, DHCP 系统要求检查 MAC 地址的合法行, 对于没有注册的 MAC 地址, DHCP 服务器不会为其分配 IP 地址, 否则分配合适的 IP 地址, 而在 Vlan1 中设备不需要注册 MAC 地址就可以获得 IP 地址.

4.3 结果分析

由于多个局域网共享一个 DHCP 服务器, 为了防止非法 DHCP 服务器对网络的干扰, 需要在各层交互机上配置了 DHCP Snooping 功能.

本 DHCP 认证系统有效解决了 DHCP 网络接入认证问题. 对于注册 MAC 地址的设备, 能够在配置 address-check 和没有配置 address-check 的网段获取 IP 地址, 而非注册 MAC 的设备则只能在没有配置 address-check 的网段实现网络接入.

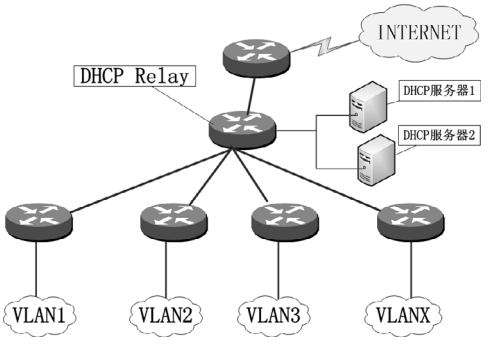

图 4　DHCP Server 工作网络拓扑

5　结语

DHCP 服务对于 Internet 的重要性不言而喻. 但是 DHCP 协议没有提供任何验证信息, 导致了应用 DHCP 的网络存在潜在的安全隐患. 因此在应用 DHCP 的网络中, 需要引入认证机制. 本文采用基于 MAC 认证模式, 并设计基于 DHCP 和 MAC 地址动态绑定的用户自助接入认证系统, 实现 DHCP 网络的安全接入. 同时使用开源 dhcpstatus 工具实时的监控 DHCP Server 状态和查看在线的用户 MAC, 能够很好的对其进行粗粒度的监控.

参考文献

1 Droms R, Bucknell University. Dynamic Host Configuration Protocol.RFC2131.IETF, 1997.
2 Kohl J, Corporation D.E, Neuman C. The Kerberos Network Authentication Service (V5). RFC1510.IETF,1993.
3 任凤姣,王洪,贾卓生.DHCP 安全系统.计算机工程,2004, 30 (17).
4 刘衍斌.基于 VLAN 动态规划的多子网反 DHCP 服务冒充技术.湖南理工学院学报,2006,19(1).
5 陈云,高静,邓亚平.Kerberos 认证协议的研究及其优化.重庆邮电学院学报(自然科学版),2006.
6 万春艳.DHCP 完全系统架构的研究.杭州:浙江大学,2007.
7 张晓丽,韩子韬.基于 8021x 协议的 Radius 服务器的应用.四川工业学院学报,2004.
8 张娜.基于 802.1x 协议的校园网络认证计费系统设计与实现.沈阳:东北大学,2009.