大型局域网中 IP 地址非法使用解决方案探讨

Solution for solving IP address confliction in large LAN

陈平仲　（广东外语外贸大学教育技术中心 510420）

摘要：在传统的网络中，都不可避免地会出现 IP 地址非法使用问题。在小型网络中，大部分的网络管理员都是采用 IP 地址与网卡 MAC 地址绑定的方法来解决该问题，但是这种方法在中、大型网络中不太适用。因此，我们必须引入一种高效的 IP 地址管理方法，此文就针对用 DHCP 解决这一难题做一些探讨。

关键词：IP 地址冲突 DHCP DHCP Snooping MAC 地址

1　前言

随着 Internet 的迅猛发展及网络基础建设的全面实施，局域网络的规模也越来越大，特别在高等学校的校园网络中，接入用户数目突破万人的比比皆是。网络规模的扩大，网络管理员所面临的问题也就越多，比如：关键业务服务质量保证问题、信息点可控性问题、网络可靠稳定性问题等等。可靠稳定的网络平台，是应用业务系统得以实施和推广的基石，网络平台的必须从设备、网络拓扑结构、网络技术、用户管理等几个方面保证网络的可靠稳定性。针对用户的管理就包括了用户 IP 地址的管理，在大多数局域网的运行管理工作中，网络管理员负责管理用户 IP 地址的分配，用户通过正确地注册后才被认为是合法用户。在局域网上任何用户使用未经授权的 IP 地址都应视为 IP 非法使用。但在用户操作系统中，终端用户可以自由修改 IP 地址的设置，从而产生了 IP 地址非法使用的问题，改动后的 IP 地址在局域网中运行时可能出现的情况如下。

（1）非法的 IP 地址即 IP 地址不在规划的局域网范围内；

（2）重复的 IP 地址与已经分配且正在局域网运行的合法的 IP 地址发生资源冲突，使合法用户无法上网；

（3）冒用合法用户的 IP 地址，当合法用户不在线时冒用其 IP 地址联网，使合法用户的权益受到侵害。

在小型网络中，由于用户数目比较少，解决 IP 地址非法使用的最直接的方法是使用 IP－MAC 地址绑定技术。但是这种方法在中、大型网络中非常不适合实现，主要原因是收集用户的 MAC 地址的花费大量的人力和时间，并且维护工作量也非常巨大。本文就针对中、大型网络中使用 DHCP（Dynamic Host Configuration Protocol）、DHCP SNOOPING 功能的方法解决 IP 地址非法使用做一些探讨。

2　IP 地址非法使用的解决方法

DHCP 称为动态主机配置协议。DHCP 服务允许工作站连接到网络并且自动获取一个 IP 地址，配置 DHCP 服务的服务器可以为每一个网络客户提供一个 IP 地址、子网掩码、缺省网关、以及一个 DNS 服务器的 IP 地址。DHCP 服务的工作过程是这样的：

（1）发现阶段。即客户机寻找 DHCP 服务器的阶段；DHCP 客户机以广播方式发送 DHCP discover 发现信息来寻找 DHCP 服务器。网络上每一台安装了 TCP/IP 协议的主机都会接收到这种广播信息，但只有 DHCP 服务器才会做出响应。

（2）提供阶段。即 DHCP 服务器提供 IP 地址的阶段；在网络中接收到 DHCP discover 发现信息的 DHCP 服务器都会做出响应，它从尚未出租的 IP 地址中挑选一个分配给 DHCP 客户机，向 DHCP 客户机发送一个包含出租的 IP 地址和其他设置的 DHCP offer 提供信息。

（3）选择阶段。即 DHCP 客户机响应 DHCP 服务器提供的 IP 地址的阶段；DHCP 客户机接受第一个收到的 DHCP offer 提供信息后，它就以广播方式回答一个 DHCP request 请求信息，该信息中包含向它所选定

的 DHCP 服务器请求 IP 地址的内容。

(4) 确认阶段。即 DHCP 服务器确认所提供的 IP 地址的阶段;当 DHCP 服务器收到 DHCP 客户机回答的 DHCP request 请求信息之后,它便向 DHCP 客户机发送一个包含它所提供的 IP 地址和其他设置的 DHCP ack 确认信息,告诉 DHCP 客户机可以使用它所提供的 IP 地址。然后 DHCP 客户机便将其 TCP/IP 协议与网卡绑定。

(5) 重新登录。以后 DHCP 客户机每次重新登录网络时,就不需要再发送 DHCP discover 发现信息了,而是直接发送包含前一次所分配的 IP 地址的 DHCP request 请求信息。当 DHCP 服务器收到这一信息后,它会尝试让 DHCP 客户机继续使用原来的 IP 地址,并回答一个 DHCP ack 确认信息。

使用 DHCP 服务优点不少:网络管理员可以验证 IP 地址和其它配置参数,而不用去检查每个主机;DHCP 不会同时租借相同的 IP 地址给两台主机;可以为每个 DHCP 作用域设置很多选项;客户机在不同子网间移动时不需要重新设置 IP 地址。但同时也存在致命的缺点:DHCP 不能发现网络上非 DHCP 客户机已经在使用的 IP 地址。这样单纯使用 DHCP 的方式还不能解决局域网中 IP 地址非法使用的问题,原因是:用于还可以手工设定 IP,并且该手工设定的 IP 有可能被 DHCP 服务器分配给第二个用户,从而造成 IP 地址的冲突,如何控制用户不能设定静态 IP 地址是该解决方案的关键。

控制用户不能设定静态 IP 地址,可以通过在交换机上启用 DHCP snooping 功能,DHCP snooping 功能是 DHCP 的一项安全特性,启用该功能后,交换机会监听 DHCP 的 IP 地址分配过程,同时交换机会生成一个 IP 地址、MAC 地址、交换机端口的对应表。然后根据 DHCP Snooping 监听获得的 IP 地址、MAC 地址、交换机端口对应表,进行绑定,在开启 Dynamic ARP Inspection 后,交换机将监听所有的 ARP 数据包,一旦发现 ARP 数据包中源 IP 地址和 MAC 地址的对应关系和 DHCP Snooping 获得的对应关系不同,则丢弃数据包,这样就可以防止用户私自更改地址。以下就是 DHCP snooping 功能的配置过程:

```
C4506(config)#ip dhcp snooping // 启用 DHCP snooping
C4506(config)#ip dhcp snooping vlan 186 -187 // 监听的范围
C4506(config)#ip arp inspection vlan 186 -187
C4506(config)#ip arp inspection validate src -mac dst -mac ip
C4506(config)#interface GigabitEthernet2/1 // 具体端口进行配置
C4506(config-if)#ip arp inspection limit rate 100
C4506(config-if)#ip dhcp snooping limit rate 100
C4506#sh ip dhcp snooping binding // 查看交换机中的绑定表
```

MacAddress	IpAddress	Type	VLAN	Interface
00:03:0F:F7:7F:45	192.168.186.77	dhcp-snooping	186	GEthernet2/4
00:E0:4C:E6:93:CF	192.168.187.57	dhcp-snooping	187	GEthernet2/6
00:30:18:C0:6C:74	192.168.187.97	dhcp-snooping	186	GEthernet2/9

交换机经过上述的配置后,其接入的计算机只能通过 DHCP 的方式获取自动分配的 IP 地址,并且获取到的地址不能修改为其它地址(交换机上的绑定表决定了 IP 与 MAC 一一对应关系);设定的静态 IP 地址由于没有在交换机上形成绑定表而不能接入网络,从而可以解决 IP 地址非法使用的问题。我校从 2003 年 5 月份开始全面实施使用 DHCP snooping 来解决 IP 地址非法使用问题,在为 14000 多名学生、1000 多名教师提供接入的 400 多台交换机中都设置了该功能,到目前为止交换机运行一直非常稳定,实施效果良好,为繁杂的用户管理工作提供了极大的便利。

参考文献

1 思科网络技术学院教程(第一、二学期),【美】CISCO SYSTEM 公司著,人民邮电出版社,2003 年。

2 思科网络技术学院教程(第三、四学期),【美】CISCO SYSTEM 公司著,人民邮电出版社,2003 年。

3 CISCO TCP/IP 路由管理专业参考,【美】Chris Lewis 著,机械工业出版社,1999 年。