文章编号:1001-5132（2008）01-0080-04

中小型校园网交换机 ARP 的检测配置研究

李　杰

（宁波市鄞州职业教育中心学校，浙江 宁波 315100）

摘要：主要探讨了 Cisco 中小型校园网如何防止 ARP 欺骗网络管理以及网络安全的相关问题，同时对动态主机配置协议 DHCP、DHCP 和 ARP 检测及访问控制列表等相关技术进行了分析研究，并提供了一些实用的相关配置.

关键词：动态主机配置协议；ARP 检测；访问控制列表

中图分类号：TP393.08　　文献标识码：A

随着办公信息化和设备数字化的不断普及，学校网络的建设也越来越重要，而局域网是学校信息化和数字化建设的前提.

虽然中小型校园网的网络结构相对比较简单，但就其本质来说，也是 Intranet 中的一种. 一般的高职院校由于没有相应的专业网管人员，以及具体实施者水平的参差不齐，在运行中也往往会出现广播风暴、地址冲突、ARP 攻击和滥用互联网等问题，使普通院校的计算机老师疲于应付，严重地影响了网络应用的效率和效果. 本文针对高职院校网络管理和应用的现状，从几个方面提出了一套配置学校校园网络的方法，有效地解决上述的相关问题，并基本上做到零维护.

1　拓扑结构

在中小型校园网的设计中，通常会采用的拓扑结构如图 1 所示.

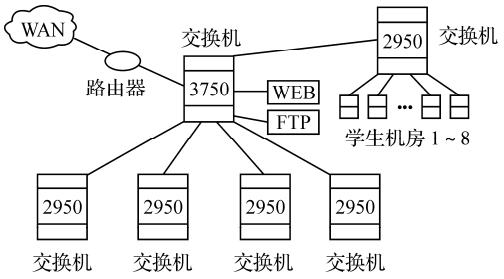

图 1　某国家级重点职业中学网络拓扑图

图 1 中Cisco catalyst 3750 三层交换机为校园网的核心交换机，它通过 1 台路由器和外网相连，并和各幢大楼内的Cisco catalyst 2950 二层交换机通过千兆光纤相连，同时还连接了WEB服务器和FTP服务器. 与路由器相连的端口为gi1/0/1，IP地址为 10.60.10.214，内网的IP地址分配从 10.63.144.0/24～10.63.150.0/24，其中 10.63.144.0/24、10.63.147.0/24 和 10.63.148.0/24 这 3 个网段分配给教师使用，分别为VLAN10、VLAN11 和VLAN12；学生机房共有 8 个，与所在大楼内的 2950 的 8 个端口(fa0/1～fa0/8)相连，占用 10.63.145.0/24 和 10.63.146.0/24 2 个网段，从VLAN101 到VLAN108. 服务器和网管机所在的网段为 10.63.150.0/24(VLAN

收稿日期：2007-10-17.　　宁波大学学报（理工版）网址：http://3xb.nbu.edu.cn
作者简介：李　杰（1972－），男，浙江宁波人，中教一级，主要研究方向：网络管理. E-mail: leejay@nbyzzj.cn

315)，其中服务器的IP地址采用静态地址 10.63.150.100～10.63.150.120 中的 1 个，需手工指定，DNS 指向本地教科网的DNS服务器 10.60.12.11. 因为只分配到 1 个公网IP地址，因此需要在路由器上作NAT地址转换，并且设置静态NAT以便在外网访问WEB服务器[1,2].

2　交换机配置

2.1　DHCP 配置

在校园网中，计算机分配地址的方法有静态和动态 2 种，静态分配地址的方法在排查故障等方面有优势，但是工作量大，而且容易造成地址冲突，也不利于笔记本等外来计算机的接入. 因此本文采用DHCP动态分配地址的方法，在这种情况下，也可以用计算机实名制这样的行政手段来辅助快速定位计算机. 用DHCP有 2 种方法：(1)交换机作为DHCP Server；(2)交换机作为DHCP Relay. 本文采用前一种方法[3]，以下介绍其详细的配置过程.

(1) 进入全局配置模式：

Core3750(config)#no ip dhcp conflict logging //不启用记录冲突日志，

Core3550(config)#ip dhcp excluded-address 10.63.150.100 10.63.150.120 //不分配从 10.63.150.100 到 10.63.150.120 的地址，以手动指定给各类服务器等使用.

(2) 在全局配置模式下指定 DHCP 地址池：

ip dhcp pool Teacher1　　//指定地址池名称为 Teacher1，

network 10.63.144.0 255.255.255.0　　//指定 teacher 的第 1 个网段，

default-router 10.63.144.1　　//默认路由地址，即 VLAN 接口地址，

netbios-node-type h-node　　//客户节点类型，

netbios-name-server 10.63.150.101　　//Wins 服务器地址，

dns-server 10.60.12.11　　//DNS 服务器地址，

domain-name nbyzzj.cn　　//域名称，

lease 7　　//租约期为 7 d.

重复上述步骤即可指定多个地址池以满足实际需要.

2.2　DHCP Snooping 和 Dynamic ARP Inspection

目前在局域网中 ARP 欺骗比较常见，较好的解决方法将 IP 和 MAC 地址的双向绑定，Cisco 的解决方案为 DHCP Snooping 和 Dynamic ARP Inspection(DAI)，而该解决方案只在 3550 型号以上的交换机中才能得到支持.

在 Cisco 网络环境下，boot request 在经过了启用 DHCP Snooping 特性的设备上时，会在 DHCP 数据包中插入 option 82 的选项. 此时，boot request 中数据包中的网关 IP 地址为全 0，所以一旦 DHCP relay 设备检测到这样的数据包，就会丢弃.

虽然 dhcp snooping 用来防止非法 dhcp server 接入，但是它的一个重要作用是使客户端获得 1 个合法的 dhcp offer. 启用 dhcp snooping 设备会在相应的接口下面记录所获得 IP 地址和客户端的 mac 地址. 这是另外一个技术 ARP inspection 检测的依据. ARP 将 1 个 IP 地址与物理地址关联起来，任何时候当主机或路由器需要找出另 1 个主机或路由器在此网络上的物理地址时，它就发送 1 个 ARP 查询分组，每个在网络上的主机或路由器都接收和处理这个 ARP 分组查询. 而这种处理机制为 ARP 欺骗提供了可能，但 ARP Inspection 即可用来检测 ARP 请求的，防止非法的 ARP 请求. 判断是否合法的方法是对照 DHCP Snooping 时建立的原先列表，因为该列表是 DHCP Server 正常回应时建立起来的，里面包含正确的 IP 地址与物理地址信息. 如果此时有 ARP 攻击信息，利用 ARP Inspection 技术即可以拦截到这个非法的 ARP 数据包. 其实利用这个方法，还可以防止用户任意修改 IP 地址，造成地址冲突的问题.

在全局配置模式下作如下配置：

S1 打开 dhcp snooping 功能：

Core3750(config)#ip dhcp snooping.

S2 定义 snooping 作用的 vlan：

Core3750(config)#ip dhcp snooping vlan 10-12,101-108, 315.

S3 将绑定表保存在 flash 中，避免重启设备后，重新绑定：

Core3750(config)#ip dhcp snooping database flash:dhcp-snooping.db.

S4 定义 arp inspection 作用的 vlan，它可根据 dhcp snooping binding 表做判断的：

Core3750(config)#ip arp inspection vlan 10-12, 101-108, 315.

S5 检测有效客户端，使其必须满足 src-mac dst-mac ip 均无错：

Core3750(config)#ip arp inspection validate src-mac dst-mac ip.

S6 定义 inspection 日志大小：

Core3550(config)#ip arp inspection log-buffer entries 1024.

S7 定义 inspection 日志刷新时间，interval 太小会占用大量 cpu 时间：

Core3750(config)#ip arp inspection log-buffer logs 1024 interval 300.

S8 在开始应用 Dynamic ARP Inspection 时，交换机会记录大量的数据包，当端口通过的数据包过多时，交换机会认为遭受 DoS 攻击，从而将端口自动 errdisable，造成通信中断. 为解决此问题，要在全局配置模式下加入以下命令：

Core3750(config)#errdisable recovery cause arp-inspection.

S9 3750 交换机的处理能力不强，因此还需要作一些额外的配置：

Core3750(config)#logging on //当 logging 关闭时会占用大量 CPU 资源，很容易死机，

Core3750(config)#no spanning-tree loopguard default //最好不要打开，

经过上述配置以后，此时客户机如果手工指定 IP，但因其不包含在 Snooping 表中，即会被交换机认为是非法地址，因此需手工指定如 WEB 服务器的地址，还要增加如下配置：

Core3750(config)#ip source binding 0004.76f6. e3e9 vlan315 10.63.150.100 interface Gi1/0/9 //手动增加静态地址的条目.

S10 设置连接各幢楼内 2950 的 gi1/0/2～8 端口：

Core3750(config)#interface range GigabitEther-net1/0/2 – 8 //定义端口组，

Core3750(config-if)#switchport trunk encapsu-lation dot1q，

Core3750(config-if)#switchport mode trunk，

Core3750(config-if)#ip arp inspection limit none，

Core3750(config-if)#arp timeout 2，

Core3750(config-if)#ip dhcp snooping limit rate 100.

由于下连设备，为避免检测让端口崩溃，所以对 arp 的侦测不做限制；若直接为接入设备，可使用 ip arp inspection limit rate 100. 以下为几个相关命令：

show logging //查看 Dymatic Arp Inspection 是否生效.

show ip dhcp snooping binding //查看 snooping 是否生效.

show ip dhcp binding //查看 dhcp server 是否生效.

show arp //查看 arp 信息是否与 dhcp snooping binding 表一致.

接着即可逐个配置各楼内的 2950 交换机，将和 3750 交换机相连的端口(如 gi0/1 定义为信任端口)来的 dhcp server 数据都为有效，其他端口为非信任端口，这样可阻止校园网内私自建立的 DHCP 服务器发送 DHCP 包，其具体配置如下：

S2950(config)#ip dhcp snooping　//打开 dhcp snooping 功能.

S2950(config-if)#int g0/1　//和 3750 交换机连接的上行端口.

S2950(config-if)#switchport mode trunk　//指定为 trunk 口.

S2950(config-if)#ip dhcp snooping trust //设为信任端口.

实验表明：对于已存在于绑定表中的 mac 和 ip 地址关系的主机，不管是通过 dhcp 获得，还是静态指定，只要符合该列表即可. 如果表中没有就阻塞其相应流量.

如果使用了 dhcp 中继服务，则还需要在网关交换机上键入如下命令：

方法一：

Switch(config-if)#inter vlan10，

Switch (config-if)#ip dhcp relay information trusted.

方法二：

Switch(config)# ip dhcp relay information trust-all.

3　小结

本文提供了一套解决校园网配置中的安全管理上可行的较为完善的方案，笔者所在学校的校园网共有 800 多台计算机，应用上述配置后，在实际运行几年中，系统稳定可靠、扩展性良好，在平时的运行中基本上不需要作大的维护.

当然网络技术的发展日新月异，新的安全问题和管理问题始终层出不穷，怎样合理解决资金和需求的矛盾，建设和管理好信息化建设的“高速公路”，使之能成为各类应用的坚实和稳固的平台，仍是值得我们不断探索与研究的课题.

参考文献：

[1] David Hucaby. Cisco 现场手册: Catalyst 交换机配置[M]. 北京: 人民邮电出版社, 2004.

[2] Behrouz A Forouzan. TCP/IP 协议族[M]. 北京: 清华大学出版社, 2001.

[3] 刘晓辉, 杨兴明. 中小企业网络管理员实用教程[M]. 北京: 科学出版社, 2005.

Probing ARP Switch Configuration for Campus Networks

LI Jie

(Ningbo Yinzhou Vocational School, Ningbo 315100, China)

Abstract: This paper explores the issues of preventing Cisco SMEs ARP spoofing for campus networks. Other issues regarding network management and security are also discussed and analyzed including Dynamic Host Configuration Protocol DHCP, DHCP and ARP detection, access control lists, etc. Some practical configuration methods are introduced.

Key words: DHCP Snooping; ARP Inspection; ACL

CLC number: TP393.08　　**Document code:** A

（责任编辑　章践立）