

善用交换机DHCP中继增强网络稳定性思科认证 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/644/2021_2022__E5_96_84_E7_94_A8_E4_BA_A4_E6_c101_644197.htm 在局域网工作环境中

，遭遇网络病毒袭击总是不可避免的事情，一旦工作站意外感染了网络病毒，那么它就不能正常上网访问了；此外，用户要是随意改变IP地址时，局域网中就容易出现IP地址冲突故障现象，一旦发生这样的故障现象，工作站也将不能正常上网访问。为了控制上网访问稳定性，本文现在就从实战案例出发，巧妙利用单位局域网三层交换机中的DHCP中继代理功能，让普通工作站远离ARP病毒以及IP地址频繁冲突故障！案例要求某大楼局域网大约拥有1000个左右的网络节点，这些节点平均分布在25层楼上，每一个楼层的网络节点全部使用六类千兆双绞线线路连接到H3C型号的S3502系列二层交换机上，而所有二层交换机又通过千兆光线线路直接连接到单位局域网的H3C型号S8500系列的核心交换机上；为了方便大楼网络的管理维护，网络管理员为这些1000多个节点划分了若干个VLAN.由于大楼网络使用的核心交换机不支持DHCP地址分配功能，网络管理员特意安装架设了Windows 2003服务器，并在其中部署了DHCP服务器。刚开始的时候，大楼局域网一直能够正常地运行；可是没有多长时间，局域网中就频繁地出现由于ARP病毒攻击和IP地址冲突而无法上网的故障现象，每次出现这些现象，网络管理员都马不停蹄地在各个楼层中来回穿梭。很显然，频繁地遭遇ARP病毒攻击和IP地址冲突现象，不但会让网络管理员疲于应付，而且也会让大楼网络的运行稳定性大打折扣。有鉴于此，单位

领导要求网络管理员必须想办法对大楼网络的IP地址进行有效控制，确保大楼网络的稳定运行。初步方案为了能够实现领导提出的网络控制要求，大楼网络的几位网络管理员分头行动，咨询了多家单位的相关解决方案，也上网查询了不少内容资料，不过这些解决方案或内容资料都不怎么适合单位的大楼网络。后来，网络管理员们经过认真分析与讨论，决定在不增加任何投资的情况下，利用单位网络中核心交换机上的静态ARP表功能，来对局域网中的所有IP地址与网卡物理地址进行绑定操作，以便禁止任何上网用户随意更改工作站的IP地址；可是转念一想，对于一个包含1000多个节点的大型局域网，除了要手工统计所有工作站的网卡物理地址以及IP地址外，而且还要将它们的对应关系手工添加到核心交换机的静态ARP表中，更麻烦的是这些普通工作站可能还会处于不断更新、变化之中，所以这种应对方案实施起来相当麻烦。再说了，对于H3C型号S8500系列的核心交换机来说，其静态ARP表功能支持的记录也没有1000多条，最终这种方案不了了之。新的方案由于不能额外增加投资，网络管理员自然也不会指望专业工具或专业设备的帮忙，只能寄希望于大楼网络现有的网络设备了；于是，网络管理员开始查阅H3C型号S8500核心交换机的操作说明书，经过仔细查阅，网络管理员找到了该交换机支持DHCP中继代理功能的线索，从该线索的描述信息中，网络管理员得知当普通工作站通过核心交换机的DHCP中继代理功能，访问局域网的DHCP服务器并从中获得有效IP地址的过程中，该中继代理功能能够把普通工作站的IP地址与网卡物理地址的动态对应关系自动记录保存下来，同时自动生成动态用户地址记录表项。此外

，核心交换机的DHCP中继代理功能也允许用户手工输入IP地址与网卡物理地址对应关系记录，并生成静态用户地址记录表项。为了控制网络接入安全，网络管理员决定启用DHCP中继代理功能，并对支持DHCP中继代理的地址启用地址匹配检查功能，来限制非法用户或包含病毒的计算机随意配置一个IP地址就能自由接入网络的现象；日后，只要普通工作站的IP地址与网卡物理地址关系记录，没有出现在DHCP中继的动态地址或静态地址记录表项中，那么该工作站就不能通过DHCP服务器，自由接入到单位大楼网络中，如此一来就能控制大楼网络的运行稳定性了。方案实施 选好了合适方案后，实施起来自然也就不那么困难了。由于DHCP中继代理功能只对VLAN有效，我们必须对每一个VLAN进行相同的控制设置，才能让对应VLAN中的工作站始终稳定上网访问；为了方便叙述，本文就以控制VLAN 1的上网稳定性为操作蓝本，向各位朋友详细叙述一下具体的方案实施步骤：首先以系统管理员权限进入DHCP服务器所在的主机系统，打开对应系统的DHCP控制台窗口，再进入对应VLAN 1的作用域属性设置对话框，在其中根据每一个虚拟网络节点数的多少将VLAN 1的地址池以及其他参数设置好，这里就不重点叙述了；其次远程登录进核心交换机的后台管理界面，在该界面的命令行中执行“sys”命令，将后台系统切换到系统全局配置状态，在该配置状态下继续执行“inter vlan-interface 1”命令，将系统切换到VLAN 1接口模式状态；来源：考试大下面在VLAN 1接口模式状态下，我们输入字符串命令“dhcp relay address-check enable”，单击回车键后，VLAN 1接口就能正常使用DHCP中继的地址匹配检查功能了；一旦启用了该功能

后，普通工作站就不能随意配置IP地址进行自由上网了，那么网络运行的安全性与稳定性也就得到有效保证了。当然，局域网中有一些重要的计算机必需要使用静态的IP地址才能上网，为了保证该地址不被其他人随意抢用，我们可以采用手工方法将静态IP地址与重要主机的网卡物理地址绑定关系添加到DHCP中继功能的静态用户地址配置条目中，这样一来重要主机就能一直使用静态地址进行稳定地上网访问了；例如，要将 10.176.1.3地址与55-66-88-77-33-77地址的对应关系添加到DHCP中继功能的静态用户地址配置条目中时，可以在VLAN 1接口模式状态下，执行“`dhcp relay security static 10.176.1.3 55-66-88-77-33-77`”命令就可以了。编辑特别推荐：[关于思科认证考试的注意事项](#) [Cisco认证总结CCNA重难点](#) [各个方向CCIE认证投资回报分析](#) [思科证书的意义：技术经验的证明](#) [我是主考官：给一位应届毕业生的回信](#) [思科认证考试四个考点难点问题](#) [100Test 下载频道开通，各类考试题目直接下载](#)。详细请访问 www.100test.com