有备而来扼杀地址冲突于萌芽状态思科认证 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__E6_9C_89_E5_A4_87_E8_80_8C_E6_c101_644113.htm 我们知道，地址冲突现象在局域网工作环境中几乎无法避免，这种现象的频繁出现，不但会影响重要计算机的运行状态，而且也不利于网络管理员高效维护网络。为了提高网络管理效率，我们不能等到地址冲突现象出现时，才采取措施去解决这样的故障，而应该主动出击，想办法将地址冲突现象扼杀于萌芽状态.为此，本文从地址冲突现象产生的源头着手，采取以下几则措施，来将地址冲突现象扼杀于萌芽状态，从而达到治标更治本的效果! 1、合理设置DHCP地址池，扼杀地址冲突 为了方便管理、维护网络，不少单位的局域网都采用DHCP服务器来为普通计算机自动分配地址，这种网络环境看似很少会出现地址冲突现象，实际上网络管理员如果对DHCP服务器的参数配置不当，特别是对DHCP地址池设置不当的时候，也容易引发地址冲突现象的发生.此外，一些重要的网络设备也有可能自带有DHCP服务器，如果这些DHCP服务器同时启用运行的话，那么多个DHCP服务器同时为计算机分配动态IP地址时，也容易造成地址冲突现象。 一般来说，ADSL设备或宽带路由器只要启用了DHCP服务器，那么DHCP服务器往往就会把与目标设备默认使用的IP地址对应网段中的所有地址一次性加入到地址池中。例如，很多宽带路由器在默认状态下会使用192.168.0.1这个IP地址，如果此时我们将宽带路由器设备自带的DHCP服务器启用起来时，那么DHCP服务器地址池中会自动包含192.168.0.0192.168.0.254这个网段中的所有地址

，在这种情形下，地址冲突现象怎么会发生呢? 为了提高系统启动速度，不少朋友往往会自己动手，来为本地计算机分配一个与192.168.0.1地址同处相同网段中的静态IP地址，这样一来计算机在启动过程中就不需要从DHCP服务器那里申请IP地址了，那么系统启动成功所耗费的时间也就大大缩短了。比方说，如果某工作子网中有四台重要主机需要使用静态IP地址，假设分配给它们的四个静态IP地址为192.168.0.11～192.168.0.14。在一段时间内，倘若IP地址为 192.168.0.12的重要主机没有正常开启运行，而恰恰这个时候有一台使用了“ 自动获取地址 ”的普通计算机需要上网访问时，那么宽带路由器设备自带的DHCP服务器往往会自动判断出192.168.0.12地址处于空闲状态，于是就会将该空闲地址地址分配给那台普通计算机了，日后那台重要主机再次上线访问时，很自然地就会出现地址冲突现象了。 为了不让重要主机的IP地址被DHCP服务器抢用过去，我们必须对DHCP地址池参数进行合理设置，让地址池保留重要主机使用的那几个静态IP 地址.例如，在这里，我们只要将192.168.0.0192.168.0.10、192.168.0.15192.168.0.254这两段地址加入到DHCP地址池中，而将192.168.0.11～192.168.0.14这段地址保留下来，这样一来重要主机日后无论关闭多长时间，都不会有其他计算机会抢用它们的静态IP地址，那样的话局域网中就不会出现地址冲突现象了。 此外，如果有新的网络设备需要连接到局域网中时，我们应该在连接网络之前，先检查目标设备中是否存在默认的DHCP服务器，如果发现它们自带有DHCP服务器，应该及时将它们的启用状态停止掉，以确保这些DHCP服务器不会与局域网中已经存在的DHCP服务器发生地址冲突现

象.当然，如果一些重要的DHCP服务器的确需要启动运行时，我们必须设置好它们的运行优先级别，确保局域网中的主DHCP服务器能够正确地为普通计算机分配动态IP地址。 2、巧妙释放隐形地址，扼杀地址冲突 任何网络操作都有一定的操作流程，如果不按照流程进行操作，那么随时都有可能发生意想不到的网络故障。这不，要想卸载掉旧网卡设备，安装上新网卡设备时，如果操作流程不当的话，就很容易出现地址冲突现象，那么为什么会出现这种地址冲突现象呢?我们知道，在卸载旧网卡设备时，我们应该先打开系统的设备管理器窗口，从中找到旧网卡设备选项，用鼠标右键单击该选项，并执行快捷菜单中的“ 卸载 ”命令，将旧网卡设备的驱动程序从系统中彻底卸载干净，这样一来旧网卡设备先前占用的隐形IP地址才能被释放出来.相反，要是我们没有先卸载掉旧网卡设备的驱动程序，而是直接关闭计算机系统电源，拔出旧网卡设备时，先前占用的IP地址仍然保存在计算机系统中，当我们尝试再次将相同的IP地址分配给新网卡设备时，Windows系统就会弹出提示说存在地址冲突现象了。 很明显，我们必须正确安装、卸载网卡设备，才能有效地避免隐形网络地址引发地址冲突现象的发生。当出现由隐形地址引起的地址冲突现象时，我们可以右击Windows系统桌面上的“ 我的电脑 ”选项，点选右键菜单中的“ 属性 ”命令，在弹出的系统属性设置窗口中，点击“ 硬件 ”选项卡，再单击对应选项设置页面中的“ 设备管理器 ”按钮，切换进入系统设备管理器界面. 单击该设备管理器界面中的“ 查看 ”菜单项，再单击下拉菜单中的“ 显示隐藏的设备 ”选项，此时系统中的隐藏网卡设备就会显示出来，选中处于隐藏状态的网卡

设备，再右击该隐藏网卡设备选项，同时执行右键菜单中的“卸载”命令，如此一来我们就能成功将隐藏网卡设备从本地系统中删除掉了。之后，依次单击“开始”、“运行”命令，在弹出的系统运行对话框中，逐一执行“ipconfig /release”、“ipconfig /renew”字符串命令，那样的话隐形地址就被成功释放出来了。此时，我们再按照常规方法安装好新的网卡设备，再将先前释放出来的IP地址分配给新网卡，那样的话我们就能成功解决地址冲突现象了。 当然，为了将地址冲突现象扼杀于萌芽状态，我们必须在删除旧网卡时，先正确卸载对应设备的驱动程序，之后切断计算机电源，小心地拔出旧网卡，同时正确安装好新网卡设备。 3、集中捆绑上网地址，扼杀地址冲突 为了实现一些特殊的网络应用，网络管理员时常要为局域网中的重要计算机分配静态IP地址，不过在使用静态IP地址的过程中，地址冲突现象更容易发生，因为遇到计算机系统发生瘫痪而重装系统时cisco认证网，加入收藏，上网用户可能会随意设置IP地址参数，这样一来IP地址冲突故障在无意之中就发生了。此外，一些恶意攻击者为了达到破坏目的，也有可能会有意修改静态IP地址，以达到抢用局域网中重要主机IP地址的目的。 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 成本速度成关键解析 四种宽带接入技术 为了防止上网用户自行修改客户端IP地址，造成地址冲突现象，我们可以尝试将局域网中所有客户端IP地址与网卡MAC地址集中绑定在一起，以便限制指定IP地址只能在指定客户端系统上使用，其他人即使偷偷抢用了IP地址，也不能正常进行网络连接，那样的话就不容易造成地址冲突现象

了。在执行地址绑定操作时，我们可以先使用“ ipconfig /all ”字符串命令，查看出各个客户端系统使用的IP地址和网卡MAC地址，之后进入到单位局域网的核心交换机后台管理系统，设置好IP地址和网卡MAC地址的捆绑关系，确保所有合法上网计算机使用的IP地址与各自的网卡MAC地址互相绑定在一起。这么一来，局域网中的每一台计算机只能固定使用自己的IP地址，而不能随意使用其他地址进行上网访问。当然，我们也可以在客户端系统使用arp命令，来实现IP地址和网卡MAC地址的绑定操作.例如，要将192.168.1.12地址捆绑到0016-173d-43eb地址上时，我们可以在系统运行对话框中执行“ arp 192.168.1.12 0016.173d.43eb arpa ”字符串命令就可以了。 除了通过捆绑上网地址的方法来扼杀地址冲突外，我们也可以想办法限制用户随意修改上网参数。例如，我们可以依次单击“ 开始 ”、“ 运行 ”命令，在弹出的系统运行框中执行“ gpedit.msc ”命令，打开组策略编辑界面，逐一点选“ 用户配置 ”、“ 管理模板 ”、“ 网络 ”、“ 网络连接 ”分支，再打开目标分支下面的“ 禁止访问lan连接组件的属性 ”设置对话框，选中其中的“ 已启用 ”选项，最后单击“ 确定 ”按钮，那样一来任何上网用户也不能随意修改本地系统的TCP/IP属性参数了。 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