 局域网中的计算机往往都是连接到交换机设备上，并通过该设备进行相互交换、处理数据的，可以这样说，交换机工作状态的好坏会对局域网网络的整体运行性能产生直接的影响。 一般来说，新投入使用的交换机设备工作性能往往比较稳定，很少会发生故障.可是，随着工作时间的延长，以及网络应用的不断变化，交换机出现故障的机率也在逐渐增大。 为了提高交换故障的解决效率，保证局域网网络能够始终高效运行，本文现在就从实战角度出发，来对常见的三种交换故障进行还原解读，希望大家能够从中得到一些启发! 1.应对缓存溢出故障 某单位局域网共有两台普通交换机，每台交换机都通过百兆双绞线连接到单位的CISCO路由器设备上，并通过该设备访问Internet网络。平时每台交换机都连接有大约10台计算机，每台计算机都能通过交换机顺利地上网访问.最近不知道怎么回事，单位局域网中有的计算机可以正常上网，有的计算机却不能上网。 起初的时候，网络管理员还以为是计算机自身的因素，可是，在对计算机系统的上网设置以及网络病毒进行检查后，发现都没有问题，使用ping命令测试本地IP地址也是正常的，但是在ping局域网的网关地址时，发现不正常，看来故障计算机到交换机之间的这段线路存在问题。 会不会是物理线路的连通性存在问题呢? 想到这一点，网络管理员立即使用网络测试仪，对连接计算机与交换机的双绞线连通性进行测试，结果发现它们的连通状态很正常。 在排除了网络

线路以及计算机自身因素后，网络管理员准备检查一下交换机的工作状态是否正常.当他来到交换机设备现场时，他发现其中一台交换机的所有端口信号灯状态都处于点亮但不闪烁状态.按理来说，交换机如果能够正常处理数据信息的话，那么对应交换端口的数据信号灯也应该处于闪烁状态，很明显现在交换端口点亮但不闪烁，这说明了该交换机的工作状态不正常。而反观另外一台交换机设备，网络管理员发现它们的交换端口只要被点亮，基本上都能处于闪烁状态，这说明这台交换机能够正常交换数据。经过进一步检查，网络管理员看到那些不能上网的计算机，基本上都是连接到那台工作状态不正常的交换机上的，看来局域网中部分计算机不能上网的故障现象是由交换机引起的。 那么究竟是什么因素造成故障交换机的端口信号灯显示不正常呢? 一般来说，造成这种端口信号灯状态显示不正常现象的原因主要有两方面，一方面就是交换机系统存在问题，例如受到网络病毒的攻击，或者工作时间长了之后出现了系统缓存溢出错误等，另外一方面就是交换机设备存在硬件问题，例如交换机服役时间比较长之后，它内部的性能元件容易发生老化现象，这些老化的元件也容易造成交换机工作状态不正常。 通常，交换机的设置不发生变化，出现的一些“ 软 ”故障往往都能通过重新启动的方法来解决，依照这样的思路，网络管理员立即重新启动了一下故障交换机系统，没有多长时间，网络管理员观察到该故障的交换机端口工作状态已经恢复了正常.再次从故障计算机系统中尝试进行上网访问时，以前不能上网的故障现象立即消失了，这说明故障交换机的确存在类似缓存溢出这样的“ 软 ”故障，这样的故障造成了交换机的工作状态无法

正常。 如果每重新启动一段时间后，交换机又出现相同的故障现象时，那问题很可能是由局域网中的网络病毒引起的，因为有的网络病毒可能在一定时间内，会对交换机系统的内存或其他系统资源进行不停占用，最终导致交换机系统的资源全部被消耗殆尽，从而会引发局域网中的计算机不能上网的故障现象.为了避免网络病毒对交换机系统的冲击，我们应该在组建网络之前，认真选用质量可靠、性能稳定、缓存较大的设备，同时注意对局域网网络定期执行病毒清除操作。
2.应对ARP病毒故障 某一天，笔者接到一个故障申请电话，说618房间的计算机突然不能上网，并且系统托盘区域处的网络连接图标上有红色叉号标记出现.起初笔者以为肯定是网络线缆出现了松动，要求该用户自行将网线拔下来重新插一下，确保网络线缆与墙上的上网插口以及网卡接口之间连接牢靠，可是该用户按照笔者要求重新插拔了网络线缆后，还是出现相同的故障现象。 笔者不放心，立即登录到618房间所使用的交换机系统上，查看了对应交换端口的工作状态，发现目标端口处于“ up ”状态，这说明交换端口的工作状态也是正常的。后来，笔者怀疑618房间的计算机使用的IP地址可能与其他计算机的IP地址发生了冲突，于是建议那位上网用户换一个IP地址试试，果然在重新更换IP地址后，618房间的计算机又能正常上网了。 然后，没有多长时间，618隔壁房间的计算机又打来电话向笔者求援说，他们的计算机也不能正常上网了.笔者经过查阅档案资料，发现出现故障的计算机基本都处于相同的虚拟工作子网中，看来这种故障现象并不简单是由人工修改IP地址造成冲突引起的，很可能是对应虚拟工作子网中出现了ARP病毒。 我们知道，现在ARP病毒非常疯

狂，局域网中的计算机很容易感染该病毒，而该病毒往往会欺骗局域网中所有计算机以及网络设备，并强制目标计算机通过特定的病毒主机进行上网访问。很多计算机被感染了ARP病毒后，之所以不能上网或者访问网络的速度会下降，主要是由于在正常状态下目标计算机的网卡IP地址与物理地址是一一对应的，当目标计算机的网卡设备从DHCP服务器那里申请得到IP地址后，该地址就会被临时与网卡设备的物理地址“ 捆绑 ”在一起，并且还会被自动记忆存储到本地系统的ARP映射表中.当局域网中有计算机被意外感染了ARP病毒后，ARP病毒就会强行把病毒计算机的网卡物理地址映射到局域网的交换机或路由器设备上，并且还会自动向网络中发送大量的ARP广播信息，局域网中的其他计算机收到广播信息后，往往会错误地认为病毒计算机就是局域网的网关地址，这样一来其他计算机就会自动把上网请求转发到病毒计算机上，而病毒计算机实际上并不是真正的网关地址，所以其他计算机自然也就不能正常上网，即使能够上网速度也不会很快了。 为了查清楚究竟是哪台计算机感染了ARP病毒，笔者立即以系统管理员身份登录进入到目标交换机系统，进入该系统的全局配置状态，利用“ display dia ”命令，查看目标交换机各个交换端口的工作状态，结果发现网卡物理地址为0016-173d-43eb的计算机与对应虚拟工作子网的网关地址存在冲突现象.为了追查出网卡物理地址为0016-173d-43eb的计算机究竟位于哪个房间，笔者立即在交换机的全局配置命令行状态下，执行字符串命令“ display mac ”，从其后出现的结果界面中，笔者看到网卡物理地址为0016-173d-43eb的计算机使用了43交换端口。 100Test 下载频道开通，各类考试题目