浅谈大型办公局域网的故障排查和优化措施

陈鹏程
南京南瑞信息通信科技有限公司　江苏南京　210037

摘　要：随着计算机的高速发展，计算机已经渗透到公司的日常办公，变成了公司提高产品效益所需要的技术手段。然而，在实际使用过程中，由于各用户的电脑操作系统技术参差不齐，或因使用者的误操作以及设施本身因素而导致的网络故障，为使用者日常工作造成了诸多不便。局域网是机关、企业、校园等单位常见的网络应用基础。企业已经进入资源优化、提高效益的新的发展阶段，各种数据和信息呈爆炸式的增长，信息系统成为提高企业生产经营管理效率的重要支撑。逐渐深入的信息化建设结果，是越来越多的业务应用系统投入使用，越来越多的用户终端接入网络。

关键词：网络运维；办公终端；网络安全；网络管理；故障处理

Discussion on troubleshooting and optimization measures of large office LAN

Chenpengcheng
Nanjing Nari information and Communication Technology Co., Ltd. Nanjing, Jiangsu 210037

Abstract: With the rapid development of computer, computer has penetrated into the company's daily office, has become the company to improve the product efficiency needed by the technical means.However, in the actual use process, due to the user's computer operating system technology is uneven, or due to the user's misoperation and the facilities itself factors caused by the network failure, caused a lot of inconvenience for the user's daily work.LAN is a common network application foundation in government organs, enterprises, campuses and other units.Enterprises have entered a new development stage of resource optimization and efficiency improvement, all kinds of data and information show explosive growth, and the information system has become an important support to improve the efficiency of production and operation and management of enterprises.As a result of the gradual deepening of information construction, more and more business application systems are put into use, and more and more user terminals are connected to the network.

Keywords: network operation and maintenance, office terminal, network security, network management, fault handling

1. 现状分析

以笔者目前所管辖的网络环境为例，网络拓扑以树形结构为主，从事的办公网络遍布大约有一千个节点，骨干网覆盖公司四个园区，接入网连通公司每一台用户终端。局域网中有近千台用途各异的计算机和服务器、数十台核心交换机、上百台终端设备以及若干防火墙、路由器等设备。然而在信息化办公过程中由于基础网络环境异常导致的生产力下降的情况时有发生，据统计，网络运维组平均每日接收50多起维修工单，组内6人几乎是连轴转，保证24小时有人员实时监控网络环境并及时处理网络故障。事实上，从事后原因分析来看，网络故障大致分为三类。第一类，超过七成的局域网报障都是由于用户终端本身软硬件出现故障或设置错误而形成的主要问题，如网卡驱动器工作不稳、服务器网卡硬件设备故障，或本地连接设置错误、被安全准入策略所影响、浏览器控件未能正常配置或安全站点设置错误等主要问题，造成网络不通、应用系统无法顺利启动或登陆后无法成功访问业务系统的各个模块。第二类，近二成故障都来自于网络线路故障，线路故障大多出现在经过综合布线接入的用户终端与路由器接口部位。第三类，尽管占比最少，却是危害最为严重的类型，通常来自于恶意病毒、木马、arp入侵，或者人为环路造成的广播风暴影响互联网正常工作，但也常常能造成更多用户的网络中断，使整个局域网片区网络完全崩溃，情况一旦出

现，影响将极为恶劣。这些网络故障大大损耗了用户与网络管理员的时间和精力。即便用户可以具体表述出完整的故障现象，但网络管理员却常常无法迅速精确地定位网络故障成因，从而做出针对性的排除，导致工作效率大打折扣，用户也会因网络故障而影响日常工作进度。

2. 故障排查分析

运维小组成员经过一段时间的摸索，形成了一套稳定有效的方法论，大致总结为故障初判、故障定位、故障确定、故障维修、故障解除五个步骤。在故障初判方面，需要先判断整体的网络状况，识别故障现象。在接到用户的网络故障报修来电时，网络管理员必须详细检查并记下上网的故障现象、发生故障机器TCP/IP（IP、DNS、网关、子网掩码）的设置、本地连接状态、故障发生的时间及提示的相关信息。在故障定位方面，需要根据描述的故障现象，判定故障范围。网络管理员会根据用户提供的相关信息和故障现象进行故障排查，确定故障发生的范围大小。然后进行测试，缩小故障范围。在故障确定方面，若是确定整个网段均发生故障，则需对机房交换机及光纤收发器进行检查和维修，找到并且隔离或排除个别机器网络故障。若是个别机器发生故障，在故障维修方面，需进行以下四部操作。第一，引导用户检测网络设备（网卡、HUB、HUB端口、网络路由器等）状态是否正常。如检测相关的网络设备电源指示灯能否正常工作，是否断电；双绞线接头是否接触良好。第二，检查TCP/IP（IP、DNS、网关、子网掩码）的配置是否正确、是否注册内网安全管理系统客户端或者是否因违规外联而导致网络中断。第三，若非上述原因，则考虑是否因更换新机器或更换新网卡而导致IP地址与MAC地址的绑定错误，造成网络故障。第四，检查防火墙设置的安全策略是否正确。若非上述网络原因，则检查是否机器网卡或其它硬件有问题，应当送维修室检查维修。故障解除方面，在网络故障维修完毕后，需再进行一次复查，若全局网络畅通，则证明故障已经解除。

笔者对所有发生过的网络故障进行了统计分析，发现引发网络故障的原因主要有以下几个方面：

（1）用户私自更改IP地址、网关、DNS等设置，并与电脑的MAC网址在交换机上实现了静态绑定，因为公司的每台电脑都有固定的IP地址，所以导致网络故障。

（2）用户在单位办公计算机私自使用无线网卡连接互联网，或者直接连接互联网，从而导致网络故障。

（3）用户在使用计算机时安全意识不强，对插入的U盘等存储设备不经过安全扫描，从而使计算机中毒，产生网络故障。

（4）由于光纤收发器、协议转换卡以及相关配件发生故障，包括其他部门工作时，造成光缆意外断开，通道出现问题，从而导致网络故障。

笔者根据处理公司网络故障的实践，按照故障种类归纳出如下解决方法：

（1）线路故障

无论是光纤还是双绞线，线路故障是常见的硬件故障之一。故障部位常常出现在线两端的RJ-45接头或接头插入设备的端口上。一般出现这种故障的原因有很多种，比如经常插拔水晶接头，双绞线质量较差，制作双绞线水晶接头不规范，网线被老鼠咬断等。针对线路故障问题，可以通过如下方法解决：

①检查网络设备（网卡、HUB、HUB端口、路由器等）指示灯是否正常；

②使用下列系统命令以完成初步检测：ping命令（检测是否连通）、Tracer命令（检测通讯路线）、netstat命令（检测网络及连线状态）、ipconfig命令或winipcfg命令（校验IP配置）；

③查看网卡驱动是否安装正确。

（2）网络协议故障

网络环路通常发生在办公区或者网络节点比较密集的环境中，因为网络跳线的两端的水晶头并没有区分是接Hub/switch或者是接PC，导致接入的随意性比较大。造成使用者可以随意将网络跳线同时接入到端口中，一旦发生这种问题就形成了环路，网络环路的危害非常大，会导致一个区域网络故障，如果上层设备不支持或未设置STP协议，则可能导致整个局域网网络瘫痪。对于网络协议故障可以通过以下方法解决：

①检查通信协议是否安装完全；

②检查TCP/IP（IP、DNS、网关、子网掩码）配置是否正确。

（3）通道故障

由于其他部门施工造成光缆意外断开，或者使设备电源掉电，产生通道不畅通，从而致使网络中断。可以通过使用网络管理软件，查看每台环网设备的运行状态，如果出现异常情况，应该立即联系相关部门，对断开光缆进行修复，对网络设备进行送电。

（4）安全故障

当网络链路通信正常，故障却依然存在时，则需重点考虑网络安全故障成因，其中很有可能是受到病毒感染、黑客侵入、存在安全漏洞或者是上文所提公司采用的安全策略出现了问题，可以通过使用内网安全管理软件，杀毒软件，防火墙，监控交换机端口流量，达到防治病毒的目的。

3. 优化措施

为了节省用户与网络管理员的时间和精力，加快日常工作进度，提高公司生产效率，笔者从绑定地址、设置安全管理系统、使用杀毒软件、增强网络健壮性四个方面对公司网络环境进行优化。

（1）IP地址与MAC地址绑定

局域网中防火墙的功能主要是进行信息的过滤和筛选，以及信息状态检测。通过信息过滤技术，能够实现对设备在网络环境中加载项的控制，比如，是否允许打开未知来源的安装文件，是否允许系统对浏览器中的插件进行调用等操作，对恶意的程序以及文件进行提示和拦截。同时，防火墙的状态检测功能能够详细地记录局域网的信息传递导向以及数据的传输对象，避免通过外网对数据调包替换以及损害等操作的进行。为更好地管理网络，笔者单位尝试对各个网段内已采取的IP地址在三层交换机上实行了静止ARP绑定，其余未采取的IP地址则用防火墙禁止，从而在有用户私用了其他用户的IP地址和被防火墙禁止的IP地址时，网络交换机根据静止ARP绑定的IP地址进行了转发，即IP相对应绑定的合法MAC地址，该用户就无法访问公司局域网，这样即可有效地防止用户私用IP地址而影响自己和其他用户正常使用网络。

有些情况下，有的非法访问者虽然没有目标计算机或者服务器的密码，但会用暴力破解软件来对密码进行破解解密，这种暴力破解密码的特点就是在极短的时间内利用计算机程序穷举所有可能的密码并进行登录实验。内网中的业务系统服务器如果一旦被暴力破解被攻击者得到了权限，就会造成数据泄露或篡改破坏等危害。针对这种情况业务系统服务器应设置最大密码尝试次数，服务器策略中有相关策略可以勾选，一旦登录失败次数超过设定值，计算机就将进入锁定状态，以终端暴力破解行为的继续进行。另外还应设定IP访问限制策略，重要的服务器只允许少数指定IP可以进行访问，这从根源上缩减了非法访问的范围。除此之外，对于一些易被攻击和利用的计算机端口，应提前在防火墙中设定限制策略。

（2）设置内网安全管理系统

内、外网间不应该混用U盘、移动硬盘等多次写入设备，如果有必要的文件传输，应使用一次性刻录光盘或是公安部认证的专用内外网文件传输设备。有条件的情况下，应关闭或封堵内网计算机的USB接口。内网与外网的隔离虽然保证了一定的安全性。但是在实际使用过程中，还是会存在着计算机病毒的感染以及针对系统、软件漏洞的安全事件。而内网中的杀毒软件和系统、办公软件不能连接外网，不能及时更新补丁修复漏洞无疑是办公内网的安全威胁之一。针对不能及时更新的问题，应建立内网统一的防病毒服务器以及系统补丁管理与分发服务器如天擎等等。由网络运维人员及时从安全防护网站上下载补丁和更新包并传输至内网系统中再进行分发，然后实现办公计算机终端通过天擎系统及管理系统的客户端进行自动的补丁安装及漏洞修复。

通过系统策略设置，可以统一控制各种硬件设备，启52A8或禁用红外设备、蓝牙无线通信设备、PCMCIA卡、PCI无线网卡、普通网卡等，并监控违规外联，监视网络连接（modem拨号、双网卡、代理等），防止违规接入互联网，并对违规行为予以消息提醒并进行处理，检测计算机的网络使用情况是否符合策略设置，并对不符合策略设置的计算机进行处理。

通过内网安全管理系统，管理移动存储设备。网络管理员可对公司所有移动存储设备进行标识认证，并对标识认证过的移动存储设备进行数据操作监控，这样有效地增强了公司内部数据的安全性，防止通过移动存储设备进行病毒传播。

（3）增强网络健壮性，保证网络通畅

通过网络管理软件进行实时监控每台网络设备的运行状态，并明确要求每日安排人员对告警设备进行逐一排查；构建环网，即使某一路链路意外断开，也不会影响正常的网络通信；加强装机修障管理，继续压缩大面积用户故障和长延时故障及重复故障的发生，不断提高故障修复及时率。这样大大增强了网络健壮性，保证了网络通畅，另外公司机房配有协议转换卡及相关网络设备，作为备用网络通道。通过加强对网络设备和网络管理软件所管理的设备的周期性检查，切实保证网络设备安全可靠的运行。

4. 总结

大型办公网络管理往往存在用户终端本身软硬件故障、用户操作不当、网络线路故障、遭受病毒或黑客攻击而产生的问题。但是只要将本文所提出的绑定地址、使用内网安全管理系统、使用杀毒软件和增强网络健壮性这四种有效可行的方法充分运用到日常工作中，即可切实保证网络的安全畅通。结合网络故障的一般解决办法与所得经验，并注重办公局域网的安全防护，积极采取相应的保护措施以减少因为网络安全风险而给企业所造成的经济损失，从而有效提升管理效率，促进信息化业务在生产工作中更好的发挥积极作用。

参考文献：

[1]李步宵.浅谈办公局域网的组建、维护及防护[J].网络安全技术与应用，2017（09）：40-41.

[2]凡荣.办公局域网组建维护和安全防护方法研究[J].网络安全技术与应用，2020（04）：26-27.

[3]毕雯婧.浅谈办公局域网网络安全防护与管理[J].电子世界，2020（07）：74-75.

[4]李红英，田苗，尹育红.局域网故障的快速诊断与排除[J].新疆农垦科技，2018，41（04）：48-50.

[5]陈东.企业局域网搭建及安全维护探讨[J].现代信息科技，2018，2（07）：166-167.

[6]徐广明.局域网故障处理[J].科技传播，2018，5（15）：216+209.