谈计算机网络的日常维护与实践

王 翔 新疆库尔勒解放军第九五一医院信息科 841000

【摘 要】 结合实际工作经验，总结计算机网络日常维护管理常见故障，对局域网容易出现的问题进行分类，针对不同类型的网络故障提出具体解决方法和技巧。

【关键词】：计算机网络；网络故障；日常维护

在信息高速发展的时代，网络已成为人们工作、生活、学习、娱乐等必不可少方式和手段，不仅提高了人们工作效率，提升了科学管理水平，还给单位带来了极大经济效益和社会效益。同时,也给网络安全带来前所未有风险和挑战，各单位对本级网络安全越来越重视。

1. 计算机网络中常见的故障

网络的安全稳定可靠运行是各种应用系统正常运行的前提，是主要数据信息安全的重要保证。计算机网络维护有诸多方面，具体包括硬件状态检测，线路检修，系统运维，软件升级，数据备份，病毒防护等。维护人员不仅要有扎实的理论功底，较强的实践经验，还要有慎密的思维判断。结合自身十几年局域网运维工作经验，总结常见故障分类。

1.1 人为故障 主要是指操作者有意或误操作引起的故障，据统计,其中因误操作引起的故障占整个网络故障的70%左右，主要表现为误删除系统或应用软件的重要文件，导致系统或程序无法正常启动和应用；误删除文件资料,造成文件资料的丢失; 误删除数据库数据，破坏数据的完整性和一致性;错误修改配置参数，导致无法上网或登录应用数据库等；在单位终端上使用不明来历带有病毒的U盘、光盘等移动存储介质，感染病毒；有些用户出于好奇或从某些报刊书籍杂志上学习到的“小技巧”，在办公计算机或网络终端上执行，造成的计算机网络故障；还有黑客通过远程登录单位内部计算机网络，植入木马、散播病毒、篡改数据、窃取信息，攻击服务器系统，造成网络变慢或瘫痪。

1.2 自然灾害 除各种恶劣的气象和自然灾害外，如地震海啸、暴风骤雨等。这里讲的是因设计不当造成的损害，严重影响计算机网络的安全稳定运行的因素，如突然断电、电涌过大、暖气漏水、机器坠落等不可预测的因素，导致计算机网络设备损坏，造成暂时或较长时间影响计算机网络正常运行。

1.3 硬件故障 硬件故障主要是有网卡、网线、交换机、路由器，服务器等通信传输和存储设备所引起故障[1]。是计算机网络故障中最为常见的，易于判断的故障，一般采用“替换法”进行排查。

1.3.1 线路故障 线路故障包括有楼宇间主干线路、楼内垂直主干线路、到桌面水平线路等，楼宇间和垂直主干线路主要以防腐蚀、防鼠咬、较硬、阻燃的单模或多模光纤，通过光纤接线端子链接核心与汇聚或汇聚与接入交换机。多采用地下管沟、竖井管槽、水平管槽埋线法，线路固定，走线隐蔽，故障发生率较小。墙上信息模块到水平接入交换机通常用超五类或六类双绞线链接，因经常拔插，挪动终端计算机，脚踢线路等原因，容易造成信息模块卡线松动或脱落，接触不良，通信时好时坏或线路不通。

1.3.2 设备故障 主要是交换机、路由器、服务器、存储器等硬件设备，主要表现为电源损坏、无法启动、硬盘损坏、主板烧坏、指示灯告警等。一般因为设备使用时间较长，维护不及时，操作不规范，多台设备同时加电造成电涌引起的设备损坏。

1.3.3 环境故障 计算机网络设备属于精密仪器，对工作环境的清洁度、干湿度、温度、电源电压电流质量都有较高要求，特别是计算机网络中心机房及每个楼宇设备机房应安装新风系统、温控系统、消防系统、除静电系统、干湿度调节设备和不间断电源（UPS）等，防止温度过高，服务存储设备、交换路由设备进行高温保护和烧坏。

1.4 软件故障 在日常工作中经常碰到是软件故障，也是最难排除的故障，绝大部分是因为误操作造成。常见是系统无法正常启动，参数配置不正确，相关服务没打开，服务器无法提供应用服务等。除本机系统和参数配置外，还有交换机、路由器、防火墙、服务器等中间设备配置参数不当，造成大面积网络故障。

2. 计算机网络日常维护技术

计算机网络日常维护是动态的，根据用户需求和安全稳定需要进行适时调节，日常维护中经常用到如下技术。

2.1 权限控制 权限控制是保证计算机网络安全、稳定、可靠、高效的基本保证。如果对用户权限设置不当，会造成商业秘密、涉密资料、主要数据、个人信息的泄露[2]，给单位和个人造成严重经济损失和恶劣影响。权限设置应遵循“按需分配，宁小勿大”原则，根据用户的应用需求分配权限，能够满足工作需要即可，切不可把系统管理员、系统操作员、DBA和DBO、创建导出对象等高级权限分配给应用用户。系统用户及应用程序用户要设置复杂的口令，经常更换口令，谨防口令泄露，防止他人窃取、篡改数据信息。

2.2 检查机制 维护人员要每天检查计算机网络设备运行状态，通过“看、听、查”等方法给设备“把脉”。“看”设备电源工作是否正常，有无“罢工”现象，“看”服务器、存储器等硬盘有无黄（红）灯“警告”。“ 听”设备内部及散热风扇有无异常声响。“查”设备表面温度是否过高。同时，详细填写检查日志记录，做好登记。除此外，还要检查操作系统的系统日志、事件日志、应用日志以及数据库运行和备份日志，警告日志有无异常报错，认真分析查看日志内容[5]，了解把握整个系统运行状况，争取“早发现，早治疗”。检查机制是保证计算机网络正常运行重要手段。

2.3 备份策略 备份目的是预防“不测”，任何系统设备都不能保证不出问题。系统无法启动，重要数据丢失，数据库无法开启等故障，都可能造成的数据损坏和丢失[3]，因此，做好整个系统得备份和还原就尤为重要。重要核心设备应做好冗余，一般选用厂家型号相同设备作冗余，这样性能一致，配置大致相同，一台出现故障，另一台立即进行接管，维护方便，效率较高。对重要文件资料要多种方式，不同方法，多路径备份。对操作系统要做好系统保护，创建系统驱动器的还原点，多份系统保障。应用数据库的控制文件、密钥文件、数据文件做好完全备份和增量备份，制定好备份策略，实时与定时备份相结合。此备份策略要通过模拟检验，确保备份数据真实有效、方法可用可行、方便快捷，一旦系统和数据库崩溃时，快速恢复到崩溃前某时间点的正常状态。

2.4 定期维护 定期维护是计算机网络维护最基本最重要的环节。包括日常维护和定期维护。日常维护是对软硬设备运行状况进行检修，根据应用需求，实时地对应用系统微调和变更，以及设备环境等日常工作，更主要是做好日常维护记录，对整个网络系统运行状况进行评估，为定期维护制定维护计划及策略。根据客户的硬件配置、拓扑结构、使用情况制订定期维护策略。包括软件更新升级改造，配置策略的优化调整，存储数据归档的等，使整个系统始终保持高效稳定安全可靠运行状态。

2.5 病毒防治 病毒可以说是当今信息网络最大的公害，具有隐蔽性强、危害性大、传播性快等特点，病毒防治防不胜防。对于我们网络用户来说，终端计算机经常更新系统补丁，堵塞系统漏洞；安装查杀病毒软件，更新病毒库，查杀病毒，保持终端计算机无感染病毒，具有较强的防御病毒的能力。如果发现某终端计算机感染病毒，立即采取措施，先断网隔离，再查杀病毒，重做系统等手段，切实切断传播途径，防止病毒传播蔓延。

2.6 硬件维护 在计算机网络维护过程中，因硬件设备相对固定，很少挪动，运行稳定，维护的工作量不是很大，维护起来相对简单。

2.6.1终端设备：终端设备故障一般用“替换法”进行排查。①线路，线路故障是计算机网络中常见故障。主要原因有：信息模块制作不规范；模块线卡金属刀片没有剥离双绞线塑胶皮；水晶头松动；线序排错，虽然四对线缆排序没做硬性要求，中间两对4、6线序交叉即可，但通常做法是:白橙，橙，白绿，蓝，白蓝，绿，白棕，棕。制作双绞线时，应使用六类或超五类双绞线与之对应的水晶头。如六类水晶头和超五类双绞线，很容易造成两根线缆插入水晶头同一线孔，造成环路。水晶头和双绞线要符合国家标准，信誉好品牌产品。②计算机终端，计算机终端是应用网络，处理业务的终端设备，一般安装有办公软件或应用系统客户端，日常应做好文件的备份和系统保护，如专用Ghost软件，Windows系统保护的驱动器创建还原点，做好系统备份，方便计算机快速恢复运行。另外，把重要文档资料和业务软件安装和备份到非系统盘，防止系统崩溃文档资料和备份数据的丢失。③网卡，网卡是计算机上网必须的设备。要选用品牌优质的网卡，优质网卡不仅提供自适应传输速率，更好控制数据包拥塞和丢失。正确安装网卡驱动并设置IP地址、子网掩码、网关、DNS服务等选项后，才能保证其正常运行。故障排除主要观察网卡指示灯颜色以及是否闪亮来判断运行状态：绿则通，灭则断，红则故障，闪烁则正常。若交换机及线路正常，网卡指示灯灭，可以判定网线断开、驱动安装有问题或网卡已坏，用替换法排除；绿灯闪烁，表示收发数据正常。维护人员对每台计算机网卡驱动、设置、型号等基本数据进行登记造册，备查[4]。

2.6.2网络设备：网络设备主要指交换机、路由器、防火墙等具有存储转发功能或包过滤功能的设备，其设备维护除保持内、外部清洁外，主要是对设备配置信息进行维护和优化，根据客户需求和业务流量需求，进行调整配置策略、安全策略，保持设备高效稳定运行状态。

2.6.3服务设备：服务器及存储设备是提供应用服务，存储数据重要设备，性能好坏直接影响着服务效能和工作效率。其维护不仅给其提供温湿度合适、电压稳定、动力连续、防静电、洁净的运行环境，更重要对服务器和存储设备做好冗余，主备互换，对存储陈列做好磁盘RAID方案，对数据做好可行备份恢复策略，最大限度地保护好数据，防止数据丢失和损坏[5]。

2.7 软件维护 软件维护是计算机网络维护的核心，具有维护复杂、工作量大、技术较高等特点，对软件维护人员工作态度，责任心、知识功底、操作技能及工作素养都有较高要求。软件包括系统软件和应用软件。软件研发、测试、应用过程中，必定存在一些未知的缺陷和安全漏洞，不法分子和黑客就会利用这些漏洞对网络进行攻击和破坏，传播病毒。软件维护人员应定期更新系统补丁，堵塞系统漏洞，关闭不必要的端口和服务，做好数据备份。经常与开发商联系，反映软件应用过程中的BUG和缺陷，及时查漏补缺，保持应用系统健康稳定的运行。

2.8 防火墙技术 防火墙（Firewall）是一款由软件和硬件组合而成，进行内外网互联，网闸隔离，确保内网信息安全的设备[6]。内外网互联使用的基本上都是TCP/IP协议，由于TCP/IP协议是为网络互联而设计的开放性协议，自身缺乏安全措施，黑客利用TCP/IP协议安全弱点进行网络攻击。防火墙技术是在防火墙上设置出入安全规则，对进出内部网络的数据包进行审计和控制，监视并记录进出系统中发生的事件，寻找受到攻击时留下的痕迹。对数据流进行扫描，过滤掉一些不安全的服务。防火墙可以对网络应用层协议进行检测和控制。经防火墙IP地址转换，使内网用户访问外网时，隐蔽内网IP地址，防止黑客直接攻击内网。

2.9 入侵检测技术 防火墙能有效防止外网的攻击，对于内网人员所做的攻击无能为力。入侵检测系统能在入侵攻击对系统发生危害前，按照一定的安全策略对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为[6]，利用报警与防护系统驱逐入侵攻击者；收集入侵攻击的相关信息，增加到防范系统知识库内，增强防范能力，避免系统再次入侵。入侵检测技术主要依赖用于信息收集的网络传感器，网络传感器需要在网络系统中若干不通网段的关键位置收集信息，存入入侵检测数据库中，系统对信息发生事件分析并作出反应。遇到可疑的数据包或通信模式时，系统就会根据事件类型触发不同类型触发器，发出不同警报消息。允许管理员添加自定义规则到攻击签名或行为数据库中。

3.总结

目前计算机网络仍是基于OSI开放系统互连模型，由于计算机网络开放性、互通性、异构性、复杂性，服务的多样，技术更新快，计算网络故障也必然复杂多样，网络安全问题越来越突出。如何有效地进行计算机网络进行维护，是国家、单位、企业所面临重要课题，也是每个计算机维护人员重要责任，本文对计算机故障分门别类，总结计算机网络日常维护经验和技巧，为他人提供借鉴，哪怕是一点点帮助，仅此而已。

【参考文献】

[1].张丽伟《网络维护的保养与故障维修》 中国管理信息化 2017年6月第20卷第12期。

[2].栾 灿《试论计算机网络维护与管理的方法和技术》计算机与软件 2017 年第 39 期。

[3].黄泽平《探讨如何提高计算机的网络维护效率》 计算机光盘软件与应用 10期。

[4].邵烨荣《探讨局域网网络维护及其管理措施》 网络安全技术与应用 2013年12期。

[5].隋宝石《浅谈医院计算机网络维护及常见故障排除的技巧》 医学信息 2013年1月第26卷第1期(下半月)。

[6].陈忠平 李旎 刘青风 等编著《网络安全》清华大学出版社。