计算机网络管理运维要点探究

刘 岩[1] 马 睿[2] 张 锋[1]
1. 新疆维吾尔自治区地震局和田地震监测中心站 新疆 和田 848000
2. 新疆维吾尔自治区地震局 新疆 乌鲁木齐 830011

摘 要：本文围绕计算机网络管理运维展开探究，分析了其重要性，包括保障系统稳定运行、充分发挥计算机功能及确保数据安全。同时指出当前运维存在工作繁重不受重视、网络环境复杂、员工操作能力参差不齐、技术滞后等问题。在此基础上，阐述了硬件设施维护、软件设施维护、人员管理与培训、网络结构优化、网络监管技术应用等要点，并提出建立完善制度、加强安全防护、引入自动化技术、开展服务外包等策略，为提升计算机网络管理运维水平提供参考。

关键词：计算机网络；管理运维；要点探究

引言：随着信息技术的飞速发展，计算机网络已成为社会生产生活中不可或缺的部分，其稳定高效运行直接影响企业、机构的运营效率与安全。计算机网络管理运维作为保障网络正常运转的核心环节，承担着维护硬件软件、监管网络状态、应对安全风险等重要职责。然而，当前网络规模扩大与技术升级，使运维面临诸多挑战。本文结合网络管理运维的重要性与现状，深入探讨关键要点及优化策略，旨在为解决运维难题、提升网络可靠性提供切实可行的思路。

1 计算机网络管理运维的重要性

1.1 保障系统稳定运行

计算机网络系统稳定是企业与机构运转的根基。网络故障会引发业务中断、工作停滞，带来严重损失。科学的管理运维能实时监测设备状态，及时发现硬件老化、线路松动、带宽拥堵等潜在问题并解决。对路由器、交换机等核心设备定期检查维护，可降低突发故障；动态调控网络流量，能避免系统因负载过高崩溃，为业务持续开展提供可靠支撑。

1.2 充分发挥计算机功能

计算机网络的价值在于互联互通实现资源共享与协同，管理运维是发挥其功能的关键。合理运维可释放硬件性能，如优化服务器配置提升数据处理速度，升级带宽满足高清会议、大文件传输等需求。同时，及时更新调试软件系统，保证应用程序兼容性与效率，让网络成为高效协同平台，服务业务发展。

1.3 确保数据安全

数字化时代，数据是重要战略资源，其安全关乎企业机密、用户隐私及机构生存。计算机网络管理运维构建多层次安全防护体系，通过安装防火墙、入侵检测系统抵御外部攻击，借助数据加密、权限管理规范内部操作，避免信息泄露。定期备份与灾难恢复演练，能在数据丢失或损坏时快速恢复，降低损失[1]。

2 计算机网络管理运维现状

2.1 运维工作繁重且不受重视

随着网络规模扩大，设备数量与日俱增，运维人员需处理日常巡检、故障排查、系统更新等大量事务，工作负荷持续攀升。但不少企业将重心放在业务拓展上，忽视运维部门的价值，认为其只是 “后勤保障”，在资源分配上优先满足业务部门，导致运维团队人员不足、设备老化问题难以解决，进一步加剧了工作压力。

2.2 网络环境日益复杂

移动互联网、物联网等技术普及，企业网络不再局限于固定局域网，而是融入无线设备、远程终端等多元节点，网络拓扑结构从简单星型、总线型向复杂混合型转变。同时，云计算的广泛应用使数据存储与处理分散在本地与云端，数据传输路径变长，网络协议种类增多，这让网络状态监控难度加大，单一故障可能引发连锁反应，增加了问题定位的复杂性。

2.3 内部员工计算机操作能力参差不齐

企业员工年龄、专业背景差异大，部分老员工对新型网络设备操作生疏，易因误操作导致网络拥堵或安全漏洞；年轻员工虽熟悉基础操作，但缺乏网络安全意识，存在随意连接外部设备、点击不明链接等行为。此外，跨部门协作中，不同岗位员工对网络资源的需求与使用习惯不同，缺乏统一规范，给运维工作带来诸多不确定性。

2.4 网络管理技术滞后

部分企业仍沿用传统的人工管理模式，依赖运维人

员手动记录设备状态、排查故障，效率低下且易出错。面对新型网络攻击手段，如勒索病毒、APT 攻击等，传统防火墙、杀毒软件防护能力不足，无法实时监测隐蔽的恶意行为。同时，缺乏智能化的网络管理平台，难以实现对全网设备的集中监控与数据汇总分析，导致潜在风险难以及时发现，无法适应现代网络的动态变化[2]。

3 计算机网络管理运维要点

3.1 硬件设施维护

3.1.1 硬件设备选择与采购

硬件设备选择需结合网络规模与业务需求，优先考虑兼容性、扩展性和稳定性。采购前要对供应商资质、产品口碑及售后服务进行调研，避免因设备型号不匹配导致的兼容问题。同时，需评估设备性能参数，如服务器处理速度、交换机端口容量等，确保满足当前及未来一段时间的网络负载。此外，建立采购审批流程，杜绝盲目采购，在保证质量的前提下控制成本，为网络稳定运行奠定硬件基础。

3.1.2 硬件设备运行环境维护

硬件设备运行环境直接影响其使用寿命，需保持机房或设备存放处通风良好、温度湿度适宜，避免高温、潮湿或粉尘过多导致设备老化加速。定期清洁设备表面及内部灰尘，检查散热风扇、空调等辅助设施是否正常运行。同时，做好电源管理，配备稳压电源和不间断电源（UPS），防止电压波动或突然断电对设备造成损害。另外，设置物理安全防护，限制非授权人员接触设备，降低人为损坏风险。

3.1.3 硬件设备定期巡检与维护

制定详细的巡检计划，定期检查路由器、交换机、服务器等设备的运行状态，记录指示灯显示、接口连接、线缆磨损等情况。对设备运行参数进行监测，如 CPU 占用率、内存使用率、端口流量等，及时发现异常并处理。针对老化部件，按损耗程度及时更换，避免故障扩大。建立设备维护档案，记录每次巡检结果、维修内容及更换部件信息，为后续维护提供数据支持，提升硬件设备的可靠性。

3.2 软件设施维护

3.2.1 系统补丁安装

系统补丁是修复软件漏洞的关键，需建立规范的安装流程。及时关注操作系统及应用软件厂商发布的补丁信息，区分紧急补丁与常规补丁，优先处理高危漏洞修复。安装前进行兼容性测试，避免补丁与现有系统冲突导致故障，可先在测试环境验证后再批量部署。同时，记录补丁安装时间、版本及设备信息，便于后续追溯，确保所有终端和服务器均完成补丁更新，减少因漏洞被利用的安全风险。

3.2.2 数据备份

数据备份需遵循 “多副本、异质化、异地存储” 原则，根据数据重要性分级制定备份策略。核心业务数据采用实时备份与定时备份结合的方式，非核心数据可按日或周定期备份。备份介质选择硬盘、磁带、云端等多种类型，避免单一介质失效导致数据丢失。定期对备份数据进行恢复演练，检查备份完整性与可用性，确保在数据损坏或丢失时能快速恢复，同时加密备份文件，防止数据泄露。

3.2.3 病毒防护

构建多层次病毒防护体系，在终端、服务器及网络边界部署杀毒软件和防火墙。定期更新病毒库，开启实时监控功能，对文件下载、邮件附件等进行自动扫描。限制移动存储设备接入权限，对必须使用的设备进行强制杀毒。加强员工安全意识教育，禁止访问不明网站或下载非官方软件。建立病毒应急响应机制，发现感染终端及时隔离，避免病毒扩散，最大限度降低病毒对系统的破坏。

3.3 人员管理与培训

3.3.1 优化运维岗位与排班

结合网络规模和业务需求，科学划分运维岗位，明确各岗位职责，如设备监控岗、故障处理岗、安全审计岗等，避免职责重叠或空白。根据网络运行峰值时段合理排班，实行 24 小时轮班制，确保突发故障能及时响应。同时，建立岗位轮换机制，让运维人员熟悉多环节工作，提升综合能力。通过动态调整人员配置，平衡工作负荷，减少因疲劳导致的失误，提高运维团队的协作效率和应急处置能力。

3.3.2 加强网络安全培训考核

定期组织网络安全培训，内容涵盖安全操作规范、病毒防范技巧、数据保密要求等，结合实际案例讲解违规操作的危害。针对不同岗位制定差异化培训方案，技术岗侧重漏洞检测与修复，行政岗强化基础安全意识。培训后通过理论测试和实操考核检验效果，将考核结果与绩效挂钩，督促员工掌握相关知识。

3.4 网络结构优化

3.4.1 网络拓扑结构优化

依据网络规模与业务需求，评估现有拓扑结构的合理性，对冗余节点、低效链路进行精简调整。小型网络可采用星型结构提升灵活性，大型网络则结合树形与网状结构增强可靠性，通过增加冗余链路避免单点故障。同时，将

核心业务与普通业务网络分区隔离，减少相互干扰。优化后需模拟测试不同负载下的网络性能，确保拓扑结构能适应业务增长，提升数据传输效率与网络稳定性。

3.4.2 合理配置网络资源

基于业务优先级分配带宽资源，保障核心业务如数据中心交互、关键系统运行的带宽需求，限制非必要应用的资源占用。通过负载均衡技术，将流量均匀分配至各服务器，避免单点过载。动态调整 IP 地址、端口等资源，定期清理闲置资源，提高利用率。结合网络监控数据，预判资源瓶颈并提前扩容，确保网络资源配置与业务发展相匹配。

3.5 网络监管技术应用

3.5.1 建立健全网络监管机制

明确网络监管责任分工，制定涵盖设备运行、数据传输、用户行为等多维度的监管标准，确保监管无死角。建立实时监测与预警流程，对网络流量异常、非法访问等风险及时响应，规定故障处理时限与升级路径。定期开展监管数据审计，分析网络运行趋势，优化监管策略。同时，结合行业法规与企业制度，完善违规处理机制，形成 “监测–预警–处置–复盘”的闭环管理，为网络监管提供制度保障。

3.5.2 采用先进的网络监管软件

引入具备全网可视化功能的监管软件，实现对路由器、服务器、终端等设备的集中监控，直观呈现网络拓扑与运行状态。选择支持实时流量分析、异常行为识别的工具，精准定位攻击源与故障点，提高问题排查效率。优先采用兼容云计算、物联网环境的监管系统，适应复杂网络架构。通过软件自动生成监管报表，辅助运维决策，减少人工干预，提升网络监管的智能化与精准度[3]。

4 计算机网络管理运维策略

4.1 建立完善的网络管理制度

构建覆盖设备管理、操作规范、安全防护等全流程的制度体系，明确各部门与岗位的网络管理职责，避免责任推诿。制度内容需包括设备采购审批流程、日常运维操作标准、故障应急处理预案等，确保每项工作有章可循。同时，结合网络技术发展与企业实际需求，定期修订制度条款，删除过时内容、补充新型网络环境下的管理要求。通过制度培训与执行监督，强化全员制度意识，将制度约束转化为实际操作规范，为网络管理运维提供刚性保障。

4.2 加强网络安全防护体系建设

构建多层次安全防护架构，在网络边界部署下一代防火墙、入侵防御系统，拦截外部恶意攻击；终端层面安装杀毒软件与主机防护工具，防范病毒入侵与数据泄露。建立安全漏洞定期扫描机制，及时发现并修复系统与应用程序的安全隐患。同时，制定网络安全事件应急响应预案，明确突发事件的处置流程与责任分工，定期开展应急演练，提升安全事件的快速处置能力，形成“预防－监测－处置－复盘” 的完整防护链条。

4.3 引入自动化运维技术

借助智能化运维平台实现设备状态监测、故障预警、补丁部署等工作的自动化，减少人工操作量与失误率。通过脚本编程与批量处理工具，完成服务器配置、网络参数调整等重复性任务，提升运维效率。构建运维数据中台，整合设备运行日志、网络流量数据等信息，利用大数据分析技术挖掘潜在风险，实现从被动运维向主动预防转变。此外，部署自动化备份与恢复系统，确保数据在突发故障时能快速恢复，降低业务中断损失，适应现代网络的高效运维需求。

4.4 开展网络运维服务外包

针对企业内部运维资源不足或技术短板，选择专业的第三方运维服务商承担部分运维工作，如高端设备维护、复杂网络架构优化等。明确外包服务范围与质量标准，签订详细服务协议，约定故障响应时间、问题解决率等关键指标。建立外包服务监督机制，定期评估服务商的服务质量，确保其提供的技术支持符合企业网络管理需求。通过服务外包，既能利用外部专业资源弥补内部能力不足，又能让内部运维团队聚焦核心业务管理，实现资源优化配置与运维效率提升[4]。

结束语

综上所述，计算机网络管理运维是保障网络稳定、安全、高效运行的核心环节，其要点涵盖硬件软件维护、人员管理、结构优化、监管技术应用等多方面。面对日益复杂的网络环境与技术挑战，需通过完善制度、加强防护、引入自动化技术、合理外包等策略持续优化。随着数字化进程加速，网络运维将向更智能、更精准的方向发展。

参考文献

[1]韩琳.计算机网络运维及安全管理设计[J].电子技术与软件工程,2019(23):198.

[2]蔡虎.高校计算机网络运维与发展趋势探析[J].计算机产品与流通,2019(10):210.

[3]张仁飞,李研.网络运维管理常见安全问题与防范对策[J].中国新通信,2019(19):168.

[4] 冯卫,刘恋,张景竹. 论计算机机房网络建设的安全与管理[J].中国高新区,2018(12):225.