

网络运维管理系统优化建议

黄金东

江苏州维通信科技有限公司 江苏 扬州 225000

摘要：网络运维管理系统是企业网络稳定运行的核心保障，具备设备监测、性能分析、故障预警及安全防护等功能。当前部分系统存在技术架构陈旧、功能模块协同性差、运维流程不规范等问题，制约了网络管理效率。针对这些痛点，可通过升级技术架构（引入分布式、云计算等）、增强模块协同（建立数据共享平台等）、规范运维流程及强化安全管理等措施优化。优化后能提升系统实时性、扩展性与安全性，减少故障影响，保障企业业务持续运转。

关键词：网络运维；管理系统；优化建议

引言

在数字化时代，网络成为企业运营的关键支撑，网络运维管理系统的效能直接影响企业业务连续性。然而，随着网络规模扩大与技术迭代，现有系统在架构适应性、模块协作及流程规范等方面逐渐显现不足，难以应对复杂网络环境需求。本文基于系统现状，分析技术、功能及流程层面的问题，提出针对性优化建议，旨在为提升网络运维管理水平提供思路，助力企业构建更稳定、高效、安全的网络环境。

1 网络运维管理系统概述

在当今数字化浪潮中，网络已然成为企业运营的核心命脉，稳定、高效的运行对于企业发展的重要性不言而喻。网络运维管理系统作为保障网络顺畅运转的关键利器，应运而生并不断演进。网络运维管理系统犹如一位智慧的网络守护贤者，全面且精细地打理着企业网络基础设施的各项事务。它能实时监测网络设备，从核心的服务器、路由器，到分布各处的交换机等，将这些设备的运行状态尽收眼底，就像为运维人员配备了一个能透视网络的洞察神器。通过持续收集设备的各类运行数据，系统能对网络性能进行精准分析，比如敏锐洞察带宽利用率是否过高、丢包率是否异常，以及延迟是否在合理范围之内等。一旦发现网络存在异常，它会迅速拉响警报，及时通知运维人员，助力他们快速定位问题根源，并提供有效的解决方案，极大地减少网络故障对企业业务的影响时长。在安全管理方面，该系统更是筑起了一道坚固的网络防线。它具备强大的入侵检测能力，能够实时识别并抵御潜在的网络攻击，同时灵活支持防火墙的配置与管理，帮助企业依据自身需求制定并严格执行安全策略，全方位确保网络数据的机密性、完整性和可用性，有效保护企业的核心数据资产不被窃取或破坏。网络运维管理系统还能对网络设备的配置变更进行

详尽记录，形成清晰的配置变更历史档案，让运维人员对网络配置的每一次变动都了如指掌，确保网络配置的一致性与可追溯性。借助配置审计功能，管理员可轻松了解网络设备的配置详情，及时发现并纠正可能存在的配置错误，为网络的稳定运行夯实基础。

2 网络运维管理系统现状分析

2.1 技术架构相对陈旧

当下，部分网络运维管理系统仍依托早期构建的技术架构，这些架构在设计之初，主要面向当时相对简单的网络环境与业务需求。随着时间推移，网络规模呈几何倍数扩张，新的应用场景与业务类型不断涌现，旧有技术架构在应对这些变化时，逐渐力不从心。以数据处理能力为例，传统架构多采用集中式的数据存储与处理模式，所有数据汇聚于中心节点进行分析运算。在网络数据量有限时，这种模式尚可维持。然而，如今网络中每秒产生的数据量巨大，集中式架构下中心节点负载过重，数据处理速度严重滞后，导致对网络状态的实时监测与分析难以实现。比如在网络高峰时段，对网络流量的分析结果往往延迟数分钟甚至更长时间才得出，此时网络中的异常状况可能已造成较大影响，运维人员却无法及时察觉。在扩展性方面，传统架构犹如固定框架的建筑，难以灵活添加新的功能模块或适应新的网络设备接入。当企业引入新型网络技术，如5G边缘计算设备时，旧有系统架构无法快速适配，需要进行大规模的底层代码修改与架构调整，不仅耗时费力，还可能因兼容性问题引发新的故障^[1]。这种滞后性使得企业在享受新技术带来的优势时，面临重重阻碍，难以跟上数字化发展的步伐。

2.2 功能模块协同性差

网络运维管理系统通常涵盖多个功能模块，如设备监控、性能分析、故障诊断、安全管理等。理想状态

下, 这些模块应紧密协作, 如同交响乐团的各个声部, 共同奏响网络稳定运行的和谐乐章。实际情况是, 许多系统的功能模块之间协同性欠佳。设备监控模块主要负责实时采集网络设备的运行参数, 如CPU使用率、内存占用等。性能分析模块则侧重于对网络整体性能指标, 如带宽利用率、延迟等进行评估。然而, 在一些系统中, 这两个模块仿佛处于各自独立的孤岛。设备监控模块发现某台核心交换机CPU使用率持续过高, 但由于与性能分析模块缺乏有效联动, 无法及时结合当前网络性能状况, 分析该高CPU使用率是否已对网络整体性能造成影响, 以及影响的范围和程度。这就导致运维人员在面对设备异常时, 难以快速准确地判断其对网络全局的危害, 可能延误故障处理的最佳时机。再看故障诊断与安全管理模块。当安全管理模块检测到网络遭受疑似DDoS攻击时, 它未能及时将相关信息高效传递给故障诊断模块, 以便其结合网络故障现象进行综合分析。故障诊断模块依旧按照常规流程, 对网络中可能出现的硬件故障、配置错误等进行排查, 却忽略了正在发生的安全威胁, 使得故障排查方向出现偏差, 增加了故障定位与解决的难度, 延长了网络故障的持续时间, 给企业业务带来不必要的损失。

2.3 运维流程不够规范

在网络运维实践中, 缺乏规范的运维流程如同没有交通规则的城市街道, 极易引发混乱与低效。部分企业在网络运维过程中, 没有建立一套标准化、精细化的操作流程。当网络出现故障时, 不同运维人员的处理方式可能大相径庭^[2]。有的运维人员凭借个人经验, 从最可能出现问题的环节入手排查; 有的运维人员则缺乏系统的排查思路, 盲目尝试各种方法, 导致故障排查过程冗长且无序。例如, 在处理网络中断故障时, 有的运维人员可能直接检查网络线缆连接, 而忽略了对网络配置、路由状态等其他关键因素的排查, 使得故障根源迟迟无法找到。在故障处理流程中, 各环节之间的衔接也存在诸多问题。故障上报环节, 可能由于缺乏明确的上报标准与渠道, 导致故障信息传递不及时、不准确。例如, 一线运维人员发现网络故障后, 不知道该向哪个具体部门或负责人汇报, 或者在汇报时未能清晰描述故障现象与影响范围, 使得上级部门在接到故障报告后, 无法快速做出准确判断与决策。故障处理过程中的协作同样混乱, 不同专业领域的运维人员之间缺乏有效的沟通与协调机制, 各自为战, 无法形成高效的故障处理合力, 严重影响了故障处理的效率与质量, 给企业网络的稳定运行带来极大挑战。

3 网络运维管理系统优化建议

3.1 升级技术架构

(1) 引入分布式与云计算架构。利用分布式技术, 把数据存储与处理分散到多个节点, 防止中心节点负载超负荷。以网络流量监测数据处理为例, 采用分布式计算框架, 各节点并行作业, 大幅提升数据处理速度, 可实时精准掌握网络状态。融入云计算架构, 借助云平台弹性计算与存储资源, 能轻松应对网络规模扩张和业务高峰的资源需求。企业可依业务量灵活调配云资源, 增强系统扩展性与灵活性。(2) 应用大数据与人工智能技术。大数据技术可深度挖掘与分析海量网络运行数据, 通过收集网络设备多年性能、故障记录等资料, 运用大数据分析算法, 精准定位网络潜在问题与性能瓶颈, 为网络优化提供坚实依据。引入人工智能技术, 以机器学习算法开展网络故障预测, 让模型学习海量历史故障数据, 自动识别可能引发故障的异常模式并提前预警, 推动运维从被动应对转为主动预防, 降低网络故障风险^[3]。

(3) 采用微服务架构。将网络运维管理系统拆分为多个独立的微服务模块, 每个模块专注特定功能, 如设备监控微服务、性能分析微服务等。各微服务可独立开发、部署与升级, 互不干扰。当需要添加新功能或优化现有功能时, 只需对相应微服务进行操作, 无需改动整个系统架构, 极大提高开发效率与系统的可维护性, 还能根据业务需求灵活组合微服务, 满足多样化业务场景。

3.2 增强功能模块协同性

(1) 建立统一数据共享平台。将设备监控、性能分析、故障诊断、安全管理等各功能模块采集的数据汇总至统一平台。各模块从该平台获取所需数据, 保证数据一致性与实时性。例如, 性能分析模块可实时获取设备监控模块采集的设备运行参数, 结合网络性能指标进行综合分析, 准确判断设备状态对网络整体性能的影响, 为运维决策提供全面数据支持。(2) 设计模块间联动机制。当设备监控模块检测到设备异常, 如某路由器温度过高, 立即向故障诊断模块发送异常信息。故障诊断模块结合自身算法与其他相关数据, 快速定位故障原因。安全管理模块若发现网络攻击迹象, 及时将信息传递给设备监控与故障诊断模块, 协同排查攻击对设备与网络的影响, 实现各模块紧密协作, 提升故障处理效率与准确性。(3) 开发协同工作流程引擎。为各功能模块间的协同工作制定标准化流程。以网络故障处理为例, 从故障发现、上报、诊断、处理到验证, 每个环节涉及的模块与操作步骤都在流程引擎中明确规定。当故障发生时, 流程引擎自动触发相应模块按流程执行任务, 确保

各模块协同有序,避免混乱无序的操作,提高整体运维工作的流畅性与高效性。

3.3 规范运维流程

(1) 制定标准化故障排查流程。梳理常见网络故障类型,为每种故障制定详细排查步骤。如网络延迟过高故障,先检查网络链路状态,再查看路由器、交换机配置,接着分析网络流量分布等,按顺序逐步排查,避免运维人员盲目尝试。为每个排查步骤提供操作指南与参考数据,帮助运维人员快速判断问题所在,缩短故障排查时间。(2) 完善故障上报与处理流程。明确故障上报渠道与标准格式。一线运维人员发现故障后,通过专门故障上报系统,按规定格式填写故障现象、出现时间、影响范围等信息,系统自动将故障报告发送至相关负责人与处理团队。处理团队接到报告后,依据故障等级启动相应处理流程,规定各环节处理时间节点,确保故障得到及时、有序处理。(3) 加强运维人员培训与考核。定期组织运维人员参加标准化运维流程培训,使其熟悉并掌握各类运维操作流程与规范。建立考核机制,将运维人员对流程的执行情况纳入绩效考核。对严格按照流程操作且表现优秀的人员给予奖励,对违反流程或操作不规范的人员进行惩罚,督促运维人员自觉遵守流程,提高运维工作质量与效率。

3.4 加强安全管理

(1) 部署先进的入侵检测与防御系统。采用基于人工智能与机器学习技术的入侵检测系统,实时监测网络流量。通过学习正常网络行为模式,能精准识别异常流量与潜在攻击行为,如DDoS攻击、恶意软件传播等。一旦检测到攻击,入侵防御系统立即采取措施,如阻断攻击源IP、限制异常流量,有效保护网络免受外部侵害。(2) 定期进行安全漏洞扫描与修复。运用专业安全漏洞扫描工

具,定期对网络设备、服务器、应用程序等进行全面扫描。及时发现系统漏洞、弱密码、不安全配置等安全隐患。根据扫描结果,制定详细修复计划,优先处理高危漏洞。在修复过程中,做好数据备份与风险评估,确保修复操作不会对网络正常运行产生负面影响,保障网络系统安全稳定。(3) 强化员工安全意识培训。定期组织网络安全培训活动,向员工普及网络安全知识与防范技巧。培训内容包括常见网络攻击手段、如何识别钓鱼邮件、安全使用网络设备等。通过案例分析、模拟演练等方式,提高员工安全意识与应急处理能力^[4]。使员工在日常工作中养成良好安全习惯,如不随意点击不明链接、定期更换密码等,从人员层面降低网络安全风险。

结语

综上所述,网络运维管理系统的优化是应对数字化挑战的必然要求。通过升级技术架构以提升数据处理与扩展能力,增强功能模块协同性以提高故障处理效率,规范运维流程以保障操作有序性,同时强化安全管理筑牢防护屏障,可全面提升系统性能。这不仅能减少网络故障对业务的影响,还能为企业数字化转型提供坚实的网络支撑,助力企业在激烈的市场竞争中保持技术优势与运营稳定性。

参考文献

- [1]王欣.企业网络运维管理系统研究与实现[J].科学与财富,2021,13(11):149.
- [2]方欣欣.企业网络运维管理优化研究[J].信息系统工程,2020(5):155-156.
- [3]吕筱.基于Web的地震信息网络运维管理系统研究[J].科学技术创新,2025(5):18-21.
- [4]李宏,左延智,张宗鹏,等.一种有效的网络运维管理系统的设计与实现[J].数字通信世界,2020(4):20-22.