关于数据通信网络维护与网络安全问题的探讨

刘树义
内蒙古平庄煤业（集团）有限责任公司　内蒙古　赤峰　024000

摘　要：数据通信网络在现代社会的重要性日益凸显，其维护与安全问题备受关注。当前，数据通信网络存在诸多问题，网络设备有故障隐患，如硬件老化、配置错误；安全漏洞与威胁不断，包括软件漏洞和多样的网络攻击；管理与运维短板明显，制度、流程等不完善；人员意识与技能也不足。为应对这些问题，需强化设备管理与维护，构建坚固安全防线，完善管理与运维体系，提升人员素养与能力，以保障数据通信网络稳定、安全运行。

关键词：数据通信；网络维护；网络安全；问题探讨

引言：在数字化时代，数据通信网络已成为社会运转的关键支撑。从日常社交到企业运营，从政府办公到科学研究，都高度依赖数据通信网络实现信息的高效传递与共享。其高速、便捷的特性极大地推动了经济发展和社会进步。与此同时，网络安全作为数据通信网络稳定运行的基石，关乎个人隐私、企业机密和国家信息安全。因此，深入探讨数据通信网络维护与网络安全问题，对于保障网络的可靠运行和信息安全具有重要的现实意义。

1 数据通信网络维护与网络安全概述

在数字化浪潮席卷的当下，数据通信网络已成为社会运转的关键支撑，其维护与网络安全的重要性愈发凸显。数据通信网络是基于一定协议，依托有线或无线通道，将各类计算机硬件连接起来的数据通信技术。依据覆盖范围，可分为国际网、广域网、城域网和局域网等。国际网即常见的互联网，广泛应用于日常生活；广域网覆盖范围大，资源共享丰富；城域网服务于城市区域；局域网则多用于单位内部，实现财务、人事等信息的高效处理与资源共享。其业务种类多样，如公用数据通信网中的分组交换、电路交换和租用电路形式的数据传输业务等。网络安全旨在保护网络中的软件和信息数据，确保信息安全和网络系统正常运行。在数据通信网络中，信息有公开和私密之分，私密信息在传递时需加密处理。内部网虽相对安全，但存在信息掌握者窃取信息的风险；公共网络环境下，网络攻击形式多样，严重威胁数据安全。数据通信网络维护与网络安全紧密相连[1]。有效的网络维护是保障网络安全的基础，通过对网络设备的定期检查、软件的更新升级等维护工作，可及时发现并排除潜在安全隐患。而网络安全则是数据通信网络正常运行的保障，只有确保网络安全，才能实现数据的高速、准确、安全传输，提升企业内部交流效率和决策水平。

2 数据通信网络维护与网络安全存在的主要问题

2.1 网络设备故障隐患

2.1.1 硬件老化与损坏

网络设备如路由器、交换机、服务器等，长时间处于运行状态，硬件会逐渐老化。例如，服务器的硬盘经过多年使用，磁头磨损、盘片老化，出现坏道的概率大大增加，可能导致数据丢失。路由器的主板电容在高温环境下，容易出现鼓包、漏液等问题，影响其正常工作。此外，设备在日常使用中还可能因意外碰撞、电源波动等原因造成物理损坏。如网络接口松动，会导致网络连接不稳定，频繁出现丢包现象，严重影响数据通信的质量和效率。

2.1.2 配置错误与冲突

网络设备的配置是一项复杂且精细的工作，稍有不慎就可能出现错误。管理员在设置路由器的访问控制列表时，规则配置错误，可能会导致合法用户无法正常访问网络资源，而非法用户却能绕过限制。不同设备之间的配置也可能存在冲突，如多台交换机的VLAN配置不一致，会造成网络拓扑混乱，数据无法正确转发。而且，随着网络规模的扩大和业务的变更，设备配置需要不断调整，如果没有及时更新和同步，也会引发各种网络故障。

2.1.3 散热与环境问题

网络设备在运行过程中会产生大量热量，如果散热不良，会导致设备温度过高。过高的温度会影响电子元件的性能，加速硬件老化，甚至引发设备死机。例如，服务器机房的空调制冷不足，服务器CPU温度持续升高，会出现降频现象，导致处理速度变慢。此外，环境的湿度、灰尘等因素也会对设备造成影响。湿度过高可能会使电路板短路，而过多的灰尘会堵塞设备的散热孔，进一步加剧散热问题，影响网络设备的正常运行和使用寿命。

2.2 安全漏洞与威胁

数据通信网络面临着诸多安全漏洞与威胁，严重影响其正常运行和数据安全。软件系统漏洞是常见的安全隐患，当前计算机运行着大量具有特殊功能的软件，部分软件存在设计缺陷或未及时更新补丁，黑客可利用这些漏洞入侵系统，窃取敏感数据、篡改信息或控制设备。例如，一些企业的办公软件存在漏洞，被黑客攻击后，商业机密可能泄露，造成巨大损失。网络攻击手段多样且不断演变，DDoS攻击通过大量虚假请求使目标服务器过载，导致服务中断，影响企业的正常运营。网络钓鱼则通过伪装成合法网站或邮件，诱使用户输入账号密码等信息，骗取个人隐私。此外，病毒和恶意软件的传播也十分猖獗，它们可通过网络感染设备，破坏数据、监控用户行为。内部人员的操作不当或违规行为也会带来安全风险，员工安全意识淡薄，如使用弱密码、随意共享账号等，容易被他人利用，增加了网络被攻击的可能性。同时，缺乏完善的内部管理机制，也难以有效防范内部人员的违规操作。

2.3 管理与运维短板

数据通信网络的管理与运维在保障网络安全稳定运行中起着关键作用，但目前存在诸多短板，严重影响了网络的性能和安全。（1）管理制度不完善。许多企业和机构缺乏健全的网络安全管理制度，对于网络设备的采购、使用、维护等环节没有明确的规范和流程，导致管理混乱，容易出现安全漏洞。（2）人员专业素养不足。网络维护和安全管理需要专业的技术人员，但部分从业人员的专业知识和技能水平有限，无法及时发现和解决复杂的网络问题，也难以应对日益复杂的网络安全威胁。（3）运维流程不规范。在网络运维过程中，缺乏标准化的流程和操作规范，导致故障处理不及时、不准确，影响网络的正常运行。例如，在设备故障时，没有明确的故障排查和修复流程，可能会导致故障扩大化。（4）监控与预警机制缺失。部分网络缺乏有效的监控和预警机制，无法及时发现网络中的异常流量、攻击行为等安全隐患，等到问题爆发时才采取措施，往往为时已晚。（5）应急响应能力薄弱。在面对网络安全事件时，一些企业和机构缺乏完善的应急响应预案和演练，无法迅速、有效地应对突发事件，导致损失扩大。

2.4 人员意识与技能不足

在数据通信网络维护与网络安全领域，人员意识与技能不足是较为突出的问题，给网络安全带来了诸多隐患。从意识层面来看，许多用户安全意识淡薄。部分员工在使用办公网络时，随意点击不明链接、下载来历不明的文件，容易导致病毒入侵和数据泄露。还有些人缺乏对网络安全重要性的认识，在设置密码时使用简单易猜的组合，且长期不更换，大大增加了账号被盗用的风险。技能方面的不足也十分明显，网络维护和安全管理需要专业的技术知识和操作技能，但一些从业人员的专业水平有限[2]。他们可能对新兴的网络安全技术和工具了解不够，在面对复杂的网络攻击时，难以准确判断和有效应对。例如，对于高级的加密算法、入侵检测系统等技术，部分人员无法熟练运用，导致在实际工作中无法充分发挥这些技术的作用，影响了网络的安全性和稳定性。

3 数据通信网络维护与网络安全应对策略

3.1 强化设备管理与维护

3.1.1 定期巡检与保养

定期对网络设备进行全面巡检是保障其稳定运行的基础。安排专业技术人员按照既定的巡检计划，对路由器、交换机、服务器等关键设备进行检查。查看设备的硬件状态，如是否有部件松动、过热等情况；检查设备的运行参数，如CPU使用率、内存占用率等是否正常。同时，对设备进行清洁保养，清除灰尘，防止因积尘影响设备散热和性能。通过定期巡检与保养，能够及时发现潜在问题并进行处理，避免设备故障的发生。

3.1.2 及时更新与升级

网络技术不断发展，设备的软件和硬件也需要及时更新与升级。及时为设备安装最新的操作系统补丁、驱动程序和安全软件，以修复已知的安全漏洞，增强设备的安全性和稳定性。对于硬件设备，根据业务需求和技术发展，适时进行升级换代，如增加服务器的内存、更换高速硬盘等，提高设备的性能和处理能力。这样可以使设备始终保持良好的运行状态，适应不断变化的网络环境。

3.1.3 建立备用设备与应急方案

为了应对突发的设备故障，应建立完善的备用设备体系。储备关键设备的备用件，如路由器的电源模块、交换机的接口板等，确保在设备出现故障时能够迅速更换，减少故障对网络运行的影响。同时，制定详细的应急方案，明确在设备故障时的处理流程和责任分工。定期对应急方案进行演练，提高相关人员的应急处理能力，确保在紧急情况下能够快速恢复网络正常运行。

3.2 构建坚固安全防线

构建坚固的安全防线是保障数据通信网络稳定运行、防范各类安全威胁的关键所在，可从以下几个方面着手。（1）部署防火墙。防火墙作为网络安全的基础屏障，能依据预设规则对网络流量进行严格过滤，阻止非

法访问和恶意攻击，有效保护内部网络免受外部威胁。（2）安装入侵检测与防御系统。实时监测网络中的异常活动，一旦发现入侵行为，能迅速发出警报并采取相应措施进行阻断，将安全风险扼杀在萌芽状态。（3）采用数据加密技术。对传输和存储的数据进行加密处理，即便数据被截获，攻击者也难以获取其中的敏感信息，确保数据的机密性和完整性。（4）设置访问控制。通过严格的身份认证和授权机制，对用户访问网络资源的权限进行精细管理，防止未经授权的访问，降低数据泄露风险。（5）定期更新安全策略。网络安全形势不断变化，及时调整和更新安全策略，才能使安全防线始终保持有效性，适应新的安全挑战。

3.3 完善管理与运维体系

完善管理与运维体系是保障数据通信网络稳定、安全运行的关键。在管理制度方面，要建立健全涵盖网络设备全生命周期的管理规范。从设备采购环节开始，严格把控质量，确保符合网络安全需求；使用过程中，明确操作流程和维护标准，规范员工行为；定期对设备进行评估和更新，淘汰老旧设备。同时，制定严格的安全管理制度，如用户权限管理、数据备份与恢复等制度，保障网络安全。运维流程上，需制定标准化的操作流程。故障发生时，能按照既定流程快速定位问题、解决故障，减少故障对网络的影响时间。建立7×24小时的监控体系，实时掌握网络运行状态，及时发现潜在问题。还要加强应急管理，制定完善的应急预案，定期进行演练，提高应对突发网络安全事件的能力。当遇到网络攻击或重大故障时，能够迅速响应，将损失降到最低。通过完善管理与运维体系，提升数据通信网络的可靠性和安全性。

3.4 提升人员素养与能力

提升人员素养与能力是保障数据通信网络维护与网络安全的重要环节。开展专业技能培训是关键，定期组织员工参加系统的网络安全和数据通信技术培训课程，邀请行业专家进行授课，内容涵盖最新的网络安全漏洞、防护技术以及数据通信协议等知识[3]。通过实际操作演练，让员工熟练掌握网络设备的配置、维护和故障排除技能，提高他们应对复杂网络问题的能力。加强安全意识教育也不容忽视，举办网络安全知识讲座和案例分析活动，向员工普及常见的网络安全威胁，如网络钓鱼、恶意软件攻击等，教导他们如何识别和防范这些风险。同时，制定严格的网络安全规章制度，要求员工遵守，如设置强密码、不随意点击不明链接等，培养员工良好的网络安全习惯。建立考核与激励机制，对在网络维护和安全工作中表现优秀的员工给予奖励，对违反安全规定的行为进行惩罚，激发员工提升自身素养和能力的积极性，为数据通信网络的稳定运行提供有力保障。

结语

未来，随着技术的不断发展，数据通信网络将面临更多新挑战。我们需持续关注并研究这些问题，不断优化维护与安全措施，以确保数据通信网络始终安全、稳定、高效地服务于社会。在数字化浪潮中，数据通信网络是支撑社会运转的基石，其安全与稳定关乎千家万户。面对层出不穷的技术难题，我们不能有丝毫懈怠。我们要以严谨的态度、创新的思维，积极应对挑战。通过不断探索和实践，提升网络性能，强化安全保障。只有这样，我们才能让数据通信网络在时代的进程中稳健前行，为社会的发展提供坚实支撑。

参考文献

[1]林庆锋.关于数据通信网络维护与网络安全问题的探讨[J].现代工业经济和信息化,2020,10(8):80-81.

[2]卢斌,郑建虎,张庭玉.网络通信中数据安全技术应用研究[J].通信电源技术,2025,42(1):147-149.

[3]程志国,寻之忠.数据通信网络维护与安全问题分析[J].微型计算机,2024(1):76-78.