

探讨计算机网络中的硬件安全与维护策略

王晨旭

联勤保障部队第九六八医院, 辽宁 锦州 121000

DOI: 10.61369/TACS.2025010006

摘 要 : 在互联网时代背景下, 科学技术的快速发展, 使得网络技术被广泛应用于各个领域, 其强大的信息传输功能和智能交互为人们的生活、学习和工作带来了巨大的便利。因此, 为了更好地满足人们的多元化需求, 计算机设备的稳定性和安全性成为社会关注的重点, 其中硬件维护是维持网络技术安全性的关键措施, 对计算机网络可持续发展产生重要影响。

关 键 词 : 防火墙; 硬件安全; 计算机; 设备; 网络安全

Exploring Hardware Security and Maintenance Strategies in Computer Networks

Wang Chenxu

NO.968 Hospital Of CPLA, Jinzhou, Liaoning 121000

Abstract : In the context of the Internet era, the rapid development of science and technology, making the network technology is widely used in various fields, its powerful information transmission function and intelligent interaction for people's life, study and work has brought great convenience. Therefore, in order to better meet people's diversified needs, the stability and security of computer equipment has become the focus of social attention, and hardware maintenance is the key measure to maintain the security of network technology, which has an important impact on the sustainable development of computer network.

Keywords : firewall; hardware security; computer; equipment; network security

引言

随着社会的发展和科技的不断进步, 人们的生活水平不断提高, 计算机网络技术凭借着其高效的信息传播、可靠的资源利用和灵活的交互性可以满足用户的不同需求。在此基础下, 计算机网络技术已经深入人们的生活和工作中。然而, 计算机网络技术在便捷生活和提高工作灵活性的同时, 也面临着巨大的网络安全问题。计算机网络具有较强的开放性, 信息泄露、数据丢失、病毒侵入等问题为人们的生活和工作带来风险。计算机安全问题需要建立在硬件的安全和维护上。因此, 探讨硬件安全与维护策略, 对于促进计算机网络安全运行具有重要的作用。

一、计算机网络中的硬件安全与维护的重要性

(一) 可以更好地服务计算机系统

硬件是计算机网络技术正常运行的重要组成部分, 是计算机的核心设施, 为网络提供物理层面的安全防护, 在计算机网络安全中起着至关重要的作用^[1]。对于计算机网络安全来说, 硬件设备是计算机保障计算机安全运行的基础, 只有硬件安全才能保障计算机得到稳定运行。在计算机硬件中, 网络连接的各种设备对网络安全的影响力最大, 如交换机、路由器以及防火墙等, 通过维护这些硬件设备, 可以帮助计算机硬件更好地服务计算机网络安全控制系统。保障计算机的稳定运行。比如, 防火墙是网络安全的第一道防线, 通过设置规则来监控和过滤进出网络的数据包, 阻止恶意软件和未经授权的访问。硬件防火墙通常具有更高的性

能和更强的安全保障, 可以通过物理层面对数据包进行检测和过滤, 减少运行的负担, 确保网络的稳定性^[2]。

(二) 可以减少信号不稳定情况

网卡和电缆作为网络连接的关键组件, 在硬件维护过程中发挥着重要的作用。比如, 在安装网卡的过程中, 当工作人员操作不当时, 可能导致网卡与主板接触不良, 进而引发网络信号不稳定、时常中断等问题。这些问题的出现会对用户的信息和数据产生影响, 出现信息泄露、数据丢失等情况, 从而对用户带来不便^[3]。电缆的质量直接关系到其信息承载能力。当电缆不能承载大量的信息时, 信息流通就会受到影响, 尤其是在网络使用高峰期, 可能出现卡顿和死机的情况。合理的线路规划可以优化网络布局, 减少信号干扰和损耗。因此, 技术人员需要根据用户需求选择合适的网卡与电缆, 避免网络安全问题出现。

（三）可以有效避免出现静电问题

根据计算机硬件部分的安全运行情况来说，静电问题是计算机安全中最容易出现的问题，可以造成极其严重的后果^[4]。计算机硬件通常需要在温度、湿度适宜的环境中运行，而干燥的环境往往容易引发静电问题，对计算机硬件造成多重损害。在当前的使用环境下，大部分用户将计算机设备放置于干燥的环境中，忽视了干燥环境产生静电的问题，从而导致计算机安全风险变大。一方面，当静电电压超过一定阈值时，它可能对计算机的芯片、硬盘等关键部件造成不可逆的损伤。比如，用户用手接触计算机显示屏一段时间后，会明显感觉到静电，这是因为人手指中带有的电荷与显示屏电荷中和，发生静电反应^[5]。这种长期的静电积累会对计算机造成损伤。

二、硬件设备网络安全的影响分析

（一）环境因素

作为计算机系统中必备的核心部件，硬件在推动计算机高效运行中体现着不可忽视的作用。其中包括交换机、路由器和保障网络环境安全的防火墙等。大部分计算机网络中的硬件设备都具有安全屏障，这些安全屏障可以确保硬件设备在网络安全运行中发挥作用^[6]。

环境因素对硬件设备的正常运行具有重要影响，其中主要包括空气湿度、温度、风力以及电磁波等。高温环境会导致硬件设备的技术参数出现误差，对设备的运行稳定性和准确性产生影响。同时，高温环境在一定程度上会加快设备内部的电子元件老化速度，缩短设备的使用寿命；而低温环境则可能出现水汽凝结等问题，导致硬件设备内部生锈和短路，影响设备的正常运行^[7]。同时，高湿度环境容易引起设备内部电路短路、腐蚀金属部件；低湿度环境可能产生静电，对电子元件造成损害。

（二）安全意识不足因素

目前，在计算机网络技术的应用过程中，存在很多影响计算机网络安全和稳定运行的因素。其中，用户安全意识欠缺是导致计算机网络安全问题的主要原因之一^[8]。在当前的形势下，虽然计算机网络为人们的生活和工作带来了极大的便利，但也存在很多不稳定的因素。这需要人们了解计算机网络安全的相关知识、掌握计算机硬件的功能和作用，以帮助他们更好地维护计算机。然而，由于对计算机硬件的安全和维护的重要性宣传不到位，使得计算机用户缺乏计算机安全意识和硬件维护意识，从而加大了计算机网络安全风险。

（三）维护不到位

部分用户没有意识到计算机硬件维护的重要性，常常将计算机设备置于较为恶劣的环境下进行使用，长此以往，硬件设备会因为环境的不耐受出现各种故障，这对计算机网络技术的正常运行产生影响。硬件设备维护周期较长，一旦计算机硬件出现损坏的情况，将会对用户甚至企业的正常使用和发展产生影响。具体来说，硬件设备往往集成了多种功能和技术，结构复杂，维修难度大。一旦出现故障，需要花费大量时间进行排查和修复^[9]。许多

企业忽视了设备的清洁、检查和维护，导致设备损耗加剧，需要长时间停机进行维修。这不仅增加了维修成本，还延长了维修周期。同时，部分用户对硬件维护不全面，使得一些硬件设备出现老化的状态。而老化硬件设备往往伴随着性能下降和功能缺失，这可能导致计算机网络运行不稳定，易受攻击。此外，维护的方法对于硬件设备的正常运行也极其重要。不当的维护方式可能无法有效清除硬件上的灰尘和污垢，导致硬件散热不良，性能下降^[10]。比如，一些用户使用潮湿的棉布擦拭计算机设备可能导致电路短路，损坏硬件。

三、计算机网络中的硬件安全与维护策略

（一）培养用户信息素养，提高安全意识

随着社会的发展和网络技术的不断更新，计算机网络应用系统逐渐多样化。为了更好地维护计算机硬件，保障计算机硬件的安全，相关部门应当加强对计算机用户的网络安全培训力度，为计算机网络技术的稳定运行和安全使用提供坚实的基础。从实际情况来看，用户不仅是计算机硬件的知识和维护计算机安全的知识了解不多，这是造成计算机硬件损坏的主要原因之一^[11]。随着网络技术的不断发展和更新，用户的信息素养培养成为当前社会重点关注的问题。用户的信息素质的提高和硬件维护知识的普及，可以在一定程度上增强用户的使用效果、保障计算机网络技术的稳定运行。在此基础上，可以从以下几方面入手。

首先，随着社会的不断发展和信息技术的应用，企业迎来快速转型期和成长期。而企业的发展依赖于计算机网络技术。计算机是推动企业发展的关键工具。加强员工的信息素养培育有利于维持企业正常运行，实现稳定发展。因此，企业管理部门应加强员工的信息素质培养，建立健全的培训体系。具体来说，企业需要制定出一套有针对性的职业规划和培训计划，以提高员工的信息技术应用能力和安全意识。其次，计算机设备的使用者大多数都是个人用户。因此，在购买计算机时，销售人员应向用户介绍一些常见的硬件设备故障的原因和解决办法，帮助他们掌握基本的故障排查和维修技能^[12]。

最后，操作人员在维护计算机硬件时，操作人员需要严格按照说明书上的操作步骤进行规范操作，同时操作人员需要严格遵守用户保密协议，避免出现维护过程中信息泄露的情况^[12]。

（二）建立完善的维护机制，实现高效维护

建立完善的维护机制，有利于实现计算机网络硬件的高效维护。具体来说，由于计算机硬件结构与运行技术较为复杂，错误地维护方法可能造成硬件损坏或性能下降，从而对整个计算机系统的稳定性和安全性产生影响^[14]。因此，计算机硬件维护需要选择更科学、合理的方法。当前的硬件维护工作主要集中在简单的升级和除尘等方面。然而，要想实现更高水平的维护，技术人员需要具备专业的技术和能力，以及丰富的计算机维护知识。CPU是计算机的核心硬件，有效地维护可以帮助其保持稳定的工作状态。在维护CPU过程中，技术人员需要采取专业的维护方法和技术。比如，技术人员可以选择更换质量好的散热片、扩展散热功

能、增加测速能力等方式，提高 CPU 的散热效果。

（三）加强防火墙应用，降低网络风险性

网络连接设备、计算机主体以及附属的网卡和网络连接等是计算机硬件设备的主要组成部分，也是影响设备安全的主要因素。一旦它们出现故障或被攻击，将对整个网络的安全构成严重威胁^[15]。为了更好地维护计算机硬件安全，相关人员需要从多方面努力。首先，防火墙是阻断各种恶意软件进入计算机系统的有效屏障。科学设置防火墙规则，可以在一定程度上限制计算机信息的传输范围，防止外部人员未经授权访问计算机内部系统资源，减少信息泄露的情况发生。同时，防火墙还可以对外部网络

系统的访问进行安全认证，当外部人员想要访问计算机内部系统时，需要完成相应的安全认证，防止外部网络系统侵入。其次，防火墙不仅可以抵御外来人员的侵入，还可以在在一定程度上保护计算机系统内部的各种操作过程，为用户传输各种信息和数据保驾护航。最后，防火墙可以实时监控网络运行状态，对网络中的信息数据进行安全监测，提高网络访问符合系统规定和标准，保证信息的完整性。防入侵技术是防火墙的进阶版技术。它可以实时监控和分析计算机网络系统和硬件设备中的信息资源。当检测到非法入侵或潜在的安全威胁时，防入侵技术能够立即发出警报，并记录入侵行为的相关信息。

参考文献

[1] 罗兴华. 基于深度学习的微机室计算机硬件故障检测及维护方法 [J]. 信息记录材料, 2024, 25 (12): 224-226.

[2] 隆昆. 新技术背景下计算机硬件维护的原则与方法 [J]. 信息与电脑 (理论版), 2024, 36 (12): 36-38+42.

[3] 黄智军, 吴泞君. 新技术背景下计算机硬件维护原则与方法 [J]. 科技创新与应用, 2023, 13 (24): 141-144.

[4] 刘仪. 计算机硬件维护技术及故障解决分析 [J]. 电子元器件与信息技术, 2022, 6 (06): 200-203.

[5] 肖霞. 计算机网络数据库的安全管理技术研究 [J]. 电子元器件与信息技术, 2022, 6 (01): 240-241+244.

[6] 王亚丽. 计算机网络安全问题及其防范措施研究 [J]. 无线互联科技, 2021, 18 (24): 23-24.

[7] 胡五音, 李程. 大数据时代计算机硬件维护和故障处理策略 [J]. 无线互联科技, 2021, 18 (21): 97-98.

[8] 尹大伟. 网络环境下计算机硬件安全保障及维护对策研究 [J]. 信息记录材料, 2021, 22 (10): 56-57.

[9] 李洪涛. 浅谈新技术背景下计算机硬件维护的原则与方法 [J]. 电脑知识与技术, 2021, 17 (24): 155-156. DOI:10.14004/j.cnki.ckt.2021.2318.

[10] 崔丽娟. 浅析硬件维护在计算机网络安全中的重要性——评《计算机硬件基础与维护技术》[J]. 现代雷达, 2021, 43 (06): 107.

[11] 黄家永. 大数据中心计算机硬件安全运行的维护措施研究 [J]. 电子元器件与信息技术, 2021, 5 (02): 215-216.

[12] 孟丹. 计算机硬件维护与数据恢复公司市场营销策略研究 [J]. 中国产经, 2020, (23): 77-78.

[13] 栾天. 计算机硬件维护与故障处理分析 [J]. 无线互联科技, 2020, 17 (22): 68-69.

[14] 吕红梅. 如何做好局域网网络安全与硬件维护工作 [J]. 内蒙古煤炭经济, 2020, (13): 126-127.

[15] 程燕. 计算机网络硬件建设的若干问题及解决方法 [J]. 电子技术与软件工程, 2020, (14): 13-14.