

白皮书：实施 IT 故障排除的最佳实践

随着网络技术的成熟，您可能希望减少故障单的数量和处理时间。遗憾的是，对于网络支持组织来说，可靠性和简易性的每一个进步都有一个抵消技术进步，这导致网络更为复杂并且容易出现的问题。如统一通信、BYOD、高速 Wi-Fi、云计算和 IPv6 技术。领先的网络支持组织正在开发新的故障排除方法，以便即使支持最新、最先进的技术时也能够减少问题和问题处理时间。

目录

- » 问题是否即将成为过去式？
- » 如今处理问题的方法
- » 更好的方法
- » 改进流程
- » 核对清单测试
- » 流程自动化
- » 协作最佳实践
- » 最佳实践故障排除总结



问题是否即将成为过去式？

最近对超过 300 个大中型组织网络专业人员的调查研究发现：

- 其中 48% 的组织解决故障单的时间平均超过半天。
- 46% 的组织需要减少故障单处理时间。
- 网络专业人员花费约 25% 的工作时间来解决问题。

既然所有 IT 技术的进步目的都是为了解决问题，为何还会出现这种现象？其中一种解释是，可靠性和简易性的每一个进步都有一个抵消技术进步，这导致事情变得更为复杂：统一通信、802.11n、云计算或 IPv6。不论原因是什么，提高解决问题的效率仍有许多益处。

如今处理问题的方法

IT 部门如何处理与故障排除有关的问题？过去所采取的方法（如投入更多员工，进行更多培训）在预算紧张的今天是行不通的。对网络进行大规模更换或升级也困难重重。许多 IT 部门可能希望争取到更好的用户，但这也仍是个梦想。

问题的关键在于大部分组织用于进行故障排除的应急方法。绝大多数（72%）组织并没有遵循标准流程。不仅组织内部的程序各式各样，并且这些组织用于排除问题的工具也大不相同。调查对象表示，解决某个问题需要多达八种不同的工具。47% 的情况需要两种或更多的工具。由于故障排除方法和工具各式各样，63% 的故障排除持续时间超过一小时也就不足为奇了。

因此，减少故障排除时间不在于投入更多的人员或进行更多培训，而在于采取更好的解决问题的流程。

更好的方法

可借鉴 IT 部门外部的故障排除最佳实践。通信服务提供商技术人员遵循详细的故障排除流程。医疗服务供应商按照医疗方案来检查和诊断病人。手术室的标准核对清单可减少并发症。标准化的测试项目可以降低操作过程中的复杂性。仔细想想，人们进行的大部分任务的组织性要强于网络故障排除的应急方法。

当前的流程

我们首先看看当前的实际流程。当人们提起故障排除，首先想到的是试错法。技术人员进行一些尝试，看能否解决问题。不断进行尝试，直至解决问题。该做法完全取决于技术人员的技能和经验。实际上，这根本不是一个真正的流程。

然而，故障排除还必须采取第二步。在许多情况下，技术人员无法独自解决问题。他们有时需要帮助才能解决某个难度特别大的问题。另一方面，由于问题不在技术人员职责范围内，他们必须与公司的某个独立小组（如服务器管理小组或应用程序开发人员）或外部小组（服务提供商或设备供应商）合作。这种情况并不少见——我们的调查表明，41% 的问题都需要此类协作。这部分流程会花很长时间，原因至少有两个：首先，负责方并不总是轻易就能发现出现的问题。其次，技术人员可能无法轻易捕获到解决问题通常所需的跟踪文件（19% 的时间）。

问题解决技巧研究

本白皮书涉及 Fluke Networks 在 2012 年 4 月对 315 位网络专业人员进行的调查研究。调查对象主要来自各行各业的大中型网络机构。他们大多是高水平的网络支持人员。

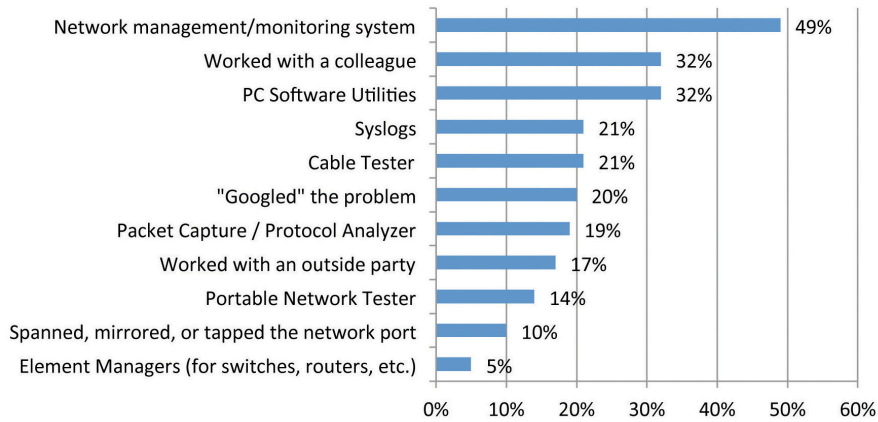


图 1：您曾经使用以下哪种工具对最近出现的用户问题进行故障排除？

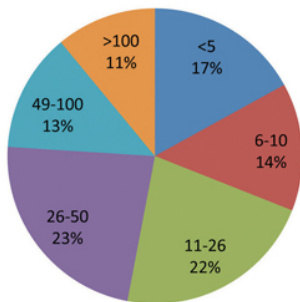


图 2：您平均每月处理多少故障单？

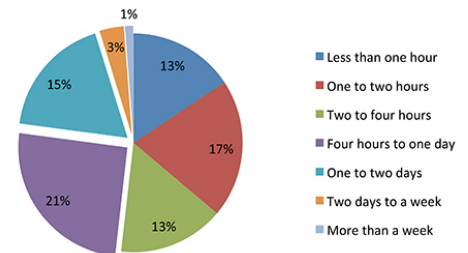


图 3：您的小组处理一个故障单平均需要多少时间？
注意，48% 的调查对象表示需要四个小时以上的时间。

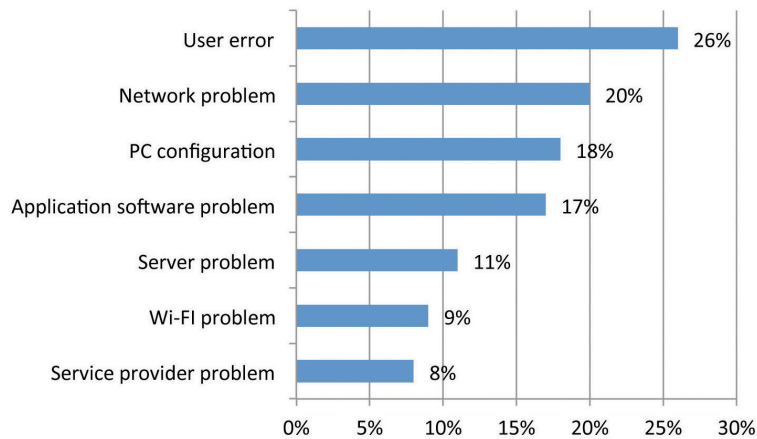


图 4：您上次解决的用户问题的根本原因是什么？（可提供多种回答。）

调查要求调查对象找出用户最近一次报告的问题的根本原因。（调查对象可以选择多个根本原因。）27%的调查对象指出，首要原因是网络问题（有线或 wi-fi 网络）。42%的调查对象表示，问题的根本原因是最终用户配置和操作问题。

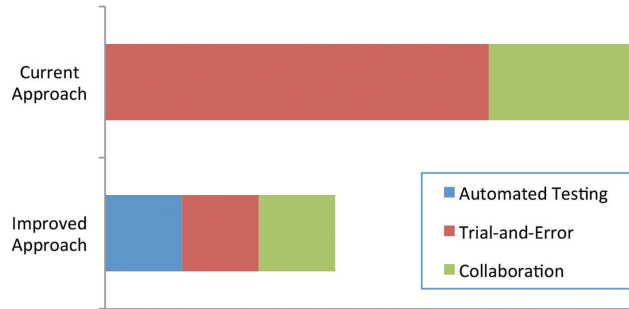


图 5：新方法可通过用自动化测试代替试错法测试，并减少协同故障排除时间，大大减少解决问题的时间。

改进流程

医学界有句老话说，“大病没有，小病不断”。这一简单的反复可为故障排除提供最佳实践方法。通过第一步快速确定常见问题，可节省大量时间。创建问题核对清单首先进行检查（按问题出现的可能性次序），可减少故障排除时间。我们稍后将介绍该流程的自动化如何节省更多时间。因此，实际上一个更好的流程应包含三步：

1. 常见问题自动化测试
2. 手动试错法故障排除
3. 与他人协同合作

增加一个步骤将减少时间可能看似违背常理。但如果自动化测试步骤可大量减少手动试错法故障排除的时间，则总的的时间就会减少。

自动化测试

可快速测试的常见问题有哪些？一个比较好的办法是从图 4 中显示的根本原因入手。让我们逐一看看这些根本原因，了解哪些问题可快速测试。

用户错误 / PC 配置 – 用户错误可通过许多不同的方式显示。错误的无线密码可使用户与网络完全断开连接。错误的 URL 快捷方式将阻止访问服务。更改网络控制面板设置会引起各种各样的问题。

确定用户是否操作错误的其中一个最快的方法是利用正确配置的设备进行同样操作。如果设备可以访问用户不能访问的资源，则用户的 PC 就是导致问题的罪魁祸首。如果不是这样的话，则表示网络或正在访问的设备的某处出现问题。

有线网络问题 – 网络会出现许多故障。布线故障、硬件故障、以及设备配置错误。许多故障都可通过相对简单的方式进行测试。一个最好的方法是从物理层开始，然后再逐步过渡到网络层：

- 布线（开路、短路、串绕线对）
- 以太网供电（等级、电压、使用的供电线对）
- 以太网设置（信号级别、速度、双工设置）
- 交换机配置（端口和 VLAN）
- DHCP（响应时间、数值）
- DNS（响应时间、数值）
- 网关路由器（响应时间、可用性）
- 整个网络健康状况（错误、丢弃的数据包）

还可以进行性能测试，测量吞吐量、丢包、延时和抖动，从而确定网络是否由于某种原因运行缓慢。

应用软件和服务器问题 – 在这方面投诉最多的是“运行缓慢”。检查该问题的快速方法是与出现问题的服务器或应用程序连接，检查响应时间。例如，从 HTTP 服务器加载页面时，我们可能希望了解：

- 查找时间
- 连接时间
- 数据启动时间
- 传送时间

我们可以从上述几项确定是否存在网络或服务器问题。此外，如果测试多个服务器和应用程序，我们可以将其迅速进行比较，看看是否只是某个服务器出现问题，还是所有服务器都有问题（说明网络问题）。其中许多问题都比较复杂，需要协作。下面我们将进一步讨论这点。

Wi-Fi 问题 – 与测试有线网络一样，测试 Wi-Fi 网络的有效方法是先从第 1 层开始，然后逐步过渡到第 3 层。

- Wi-Fi 环境（信号强度、使用率、信噪比）
- Wi-Fi 设置（SSID、安全性）
- DHCP（响应时间、数值）
- DNS（响应时间、数值）
- 网关路由器（响应时间、可用性）

验证 Wi-Fi 性能的一个快速方法是访问有线网络和 Wi-Fi 网络的若干服务器或服务，并比较响应时间。这么做可以迅速查明是否只有某个服务器或 Wi-Fi 网络出现问题，还是一切都运行缓慢。另一种方法是进行性能测试，测量整个 Wi-Fi 网络的吞吐量、丢包和延时。

服务提供商问题 – 这些问题可能不在技术人员的解决范围内，但确定问题的根源可加快其解决速度。其中一种方法是将现场和场外（云）应用性能进行比较，看看差别是否比预期的要大。更全面的方法是测量出现问题的服务提供商链路的性能（吞吐量、丢包、延时）。

流程自动化

流程一旦定义，可自动执行。自动化测试有几大优点。第一，速度远超过手动测试。第二，不会出现遗漏测试的人为错误。第三，任何人员（不论技术水平如何）均可进行这些测试，确定问题。

自动化可带来很大的节省。利用 Fluke Networks OneTouch™ AT 进行的测试表明，在一分钟（或更少时间）内可进行上述的一小时标准化测试——可能会节省大量的试错法故障排除时间。

协作最佳实践

如前所述，网络技术员需要定期与其他人合作解决问题。前面提到的许多常见问题（如服务器、应用程序和服务提供商问题）始终要求技术人员与其他人合作。然而，从相关人员获取正确信息的过程可能会花数小时，甚至几天时间。即使技术人员在这期间能够解决其他问题，但这对无法完成工作的最终用户或者无法实现故障单时间目标的 IT 经理还是没有帮助。下面介绍加快协作流程的一些最佳实践。

报告 – 技术人员进行的所有测试和观察的详细报告使技术人员能够向同事准确说明他们在观察问题时发生的情况。完整的自动化测试报告应包含缺乏经验的技术人员可能不会想到要考虑的内容，但这些内容是知识更渊博的团队成员所要评估的。

在线数据包捕获 – 跟踪文件对于难度极大的问题，或者作为应用程序开发商、服务提供商或设备供应商等外部团体的证据来说是必不可少的。收集此类信息一般需要对交换机进行重新配置。这可能需要 30 分钟或更长时间。更糟糕的是，很多技术人员可能并不具备进行交换机配置的访问权或知识。这意味着将问题转给其他人员时便会耽误更多时间。

若要减少捕获时间，每位技术人员可以掌握一种无需访问交换机也可以进行数据包捕获的在线捕获工具，以及数据包过滤和拼接，从而确保捕获相关数据包。

远程界面 – 技术人员的测试设备应安装能够让组织内部其他人员进行远程访问的软件（例如利用平板电脑或智能手机上的 VNC 客户端）。远程用户不仅能够看到技术人员所看到的内容，还可以远程控制测试设备并将跟踪文件或报告从测试仪导入到自己的本地设备中。远程访问可能会导致安全漏洞，必须进行正确安装和维护。

最佳实践故障排除总结

故障诊断阶段	问题	任务
发现常见问题	用户错误/ PC 配置	快速确定问题是否出在 PC，是什么问题。
	网络问题	发现网络连接的常见问题。
	服务器/应用程序问题	测试服务器和应用程序的响应时间。
	Wi-Fi 问题	检查 wi-fi 环境、连接性和性能。
	服务器提供商问题	测试整个 WAN 或云应用程序的响应时间；测量性能。
自动化	自动进行上述测试	可减少 90% 或更多的所需时间。
协作	报告	以上测试结果的完整报告使支持团队无需重复进行测试。
	远程控制/共享	可让远程支持人员了解结果，在出现问题时可随地进行测试。
	数据包捕获	为技术人员提供及时准确捕获问题流量的快速而简单的方法。

表 1.故障排除“最佳实践”方法的摘要。

采用上述方法无法隔离的特殊问题仍需要采取试错法故障排除。然而，通过建立支持团队采用定义流程来隔离大多数问题，并提供可减少协作时间的一整套工具，可大大减少故障排除的时间。这些“最佳实践”方法可减少故障单的处理时间，使员工能够腾出时间进行具有前瞻性的项目。