专家年终话网络系列：网络排故技巧及经验谈思科认证 PDF 转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/629/2021_2022__E4_B8_93_E5_AE_B6_E5_B9_B4_E7_c101_629012.htm 作为一名网络工程师，我的主要工作是实施网络工程并为客户提供相应的网络支持。干这行已经八年了，工作中遇到的网络案例不计其数，也接触了不少网络管理员。网管们平时工作就非常繁重，大家最怕网络发生故障。因为，网络排故不仅考验技术，更是体力和耐心的煎熬。如果不能很快地排除故障，领导的怀疑，同事的轻视更难以忍受。正是基于这样的考虑，我把自己在这方面的积累的一些技巧和经验写成文和大家分享。 1、区分硬故障和软故障 网络故障分硬故障和软故障，有时是软硬件相结合的故障，网络工程师要能够根据故障表现敏锐准确地判断是哪类故障。所谓硬故障就是由硬件引起的网络故障，比如接触不良，插口、元件损坏等。硬故障具有立竿见影的效果，如果发生硬故障其所在的这段网络马上崩溃。我特别提醒大家，所谓软故障并不仅仅是软件故障。这种故障时隐时现，可以由软件故障引起，也可以是硬件故障引起，是难度比较高的一类故障。这除了需要网络维护和管理人员具备一定的软硬件故障诊断知识外，对诊断经验的积累也有一定的要求。 通常情况下，借用适当的网络检测工具可以使我们的工作事半功倍。如何选择合适的检测工具对故障监测点进行测试是很有讲究的。许多故障需要进行多点测试才能定位，这时非常需要的是便携式的测试工具。网络故障的诊断发展方向是测试工具的网络化和故障诊断的网络化。一般的网络设备和网上设备只支持有限的网管功能，所以监测网

络性能和快速定位网络故障需要一些必要的固定测试工具(如固定探头、网管系统等)和移动测试工具(如网络测试仪、流量分析仪等)。对重要的网络设备要准备适当的备用设备，至少要留足备用通道。网络关键设备不一定要选用最昂贵和功能最齐全的设备，但一定要选用应用比较成熟，可靠性高、用户数量大的设备，这样技术支持的难度就会降低。如果将关键网络设备的维护工作交给集成商或厂商来做，那用户就得准备将网络的命运完全交给集成商或厂商来控制，而这是非常危险的。因此对人员进行适当的培训并配备合适的、易懂易用的工具是做好网络维护工作的必要条件之一。 2、掌握故障隔离技巧 网络故障不可避免，如何才能快速定位并排除故障呢?以我的经验，依据经验并借用第三方工具分析就可以逐渐缩小范围，直至定位到故障源。在这个过程中，需要借助网络隔离技术。这样不仅可以简化网络快速定位故障源，同时也可以减少网络故障给整个网络带来的损失。 其中，用交换机来隔离网段和网络故障有较好的作用。主服务器、网管机等重要网络设备应以独享交换机端口为佳，不宜再用共享式集线器连接上其它设备，这样可以迅速孤立出故障设备，减少因网络停运造成的损失。如果恰好遇到交换器故障，那么根据网络拓扑结构图就可以迅速定位交换机的问题，提高维护工作的时效性。另外，Mac地址是文档备案的最重要内容之一，除了用于排除网络设备故障有极大方便外，对于迅速查找我们称之为“ 恶意用户 ”的非合法上网成员也有很大帮助。 3、网络诊断中的社会工程学 社会工程学通俗地说就是使人们顺从你的意愿、满足你的欲望的一门艺术与学问，在黑客技术中比较常用。其中不少网络故障是有网络内

部的人员有意或者无意造成的，一个对公司不满的员工就可以在一定程度上损坏企业的网络，至少会让网络工程师忙得团团转。有的时候，进行网络故障的诊断，了解这方面的信息是非常有用的，很多时候会让我们的工作柳暗花明。 说一个简单的例子，某公司的网管辞职后，不到一天就出现了网络故障。具体症状为：公司外网基本上两小时自动掉一次线，然后过一分钟又自动连接上。这期间虽然耽误时间只有一分钟，但由于公司很多广告设计都是多人在线协作完成。另外，公司的视频点播系统对网络的连通性要求很高。因此，这一分钟的掉线对公司的影响还是比较大的。在网络故障的排查过程中，排除了硬件连接和病毒等因素，就是找不到原因，网络排故陷入困境。最后维护人员了解到，前网管因不满公司待遇愤然辞职的事实后，事情才柳暗花明，原来是前管理员离职前为泄愤修改了路由器的拨号设置才造成了如此蹊跷的网络故障。由上面的这个案例可以看到，社会工程学在网络排故中的作用。这个例子非常简单，大家在实战中可能遇到更复杂的情况，不管怎样掌握一定的社会工程学知识是必要的，它可是“ 技术之外的技术 ”。 基于长期的网络支持的经验和相关的案例，我发现网络管理的漏洞大多数来自于内部管理人员，因此建立严格的内部管理机制是非常必要的。比如将MAC地址的备份列入必备文档。另外，每日对网络进行状态自动搜寻会有助于很快发现并清除非法用户。健康的网络维护方案中必须要有定期测试(包括每日测试和每日循环测试)的项目，只要坚持每日必要的测试和检查，就可以保证99.9%的网络不会有超过2天而解决不了的严重网络问题的存在。 4、工程师的秘密武器 工欲善其事，必先利其器。

因为，通常情况下，网络管理系统只能发现约30%～40%的网络故障(这还取决于被管理设备支持网管的能力和分析、记录网络异常流量的能力)，当有故障报警后，多数情况下需要进一步迅速确定具体的故障位置和故障属性。所以，为大型网络的管理者配置一些备用网络设备是必要的。并且还需要按网络规模和使用级别、维护人员的技术等级配备相应的维护工具，并建立一整套测试维护的方案和规定，这样才能保证网络的可靠性，并保证能及时处理各种网络故障。 另外，人们往往有这样的错觉：只要具备网管功能，就能发现网络的一切故障。其实，进一步的性能测试需要专用工具，要求这类工具不光能识别各种正常的工作协议，还要能识别形形色色的“ 网上垃圾 ”。网络工程师除了配备相应的LAN测试工具外，由于WAN链路的测试维护由WAN链路运营商(比如电信公司)负责，但网络用户和系统集成商也需要配备一定数量的WAN测试工具以备性能评测、故障救急以及定期测试的需要。 5、黑客技术是高级工程师应备的技能 网络工程师掌握黑客技术并不是为了攻击，考试,大提示而是为了防御知己知彼积极主动有效地防御。我的理解，工程师不仅仅是网络的维护者(维护网络正常运行)，而且还应该是网络的保护者。不说WAN，就LAN也面临者来自外部和内部的攻击，可以说在夹缝中求生存。攻击者攻击一个企业的网络，其最终目标的取得企业服务器、核心网络设备(路由器/交换机)的控制权。从而进一步控制整个网络或者获取重要数据。作为网络工程师，应该特别对这些核心设备重点保护，那就需要有一定的黑客(安全)技术了。 一名高级工程师必须掌握以下安全技能： (1).入侵检测技术。对于安全要求比较的企业网络一般

都部署了IDS(入侵检测系统)，它能够监控并帮助检测网络系统是否发生了攻击行为，它扩展了管理员的安全管理能力。但是，设备部署万能的(往往被突破)，工程师自身掌握一定的入侵检测技术这样互相配合才能把安全做得更好。 (2).入侵测试技术。网络部署完成后，或者添加了新的服务器、网络设备后工程师最好自己进行入侵测试，看看是否足够安全。当然，工程师的入侵测试技术越高，网络安全就更有保障。 (3).入侵跟踪技术。如果网络屡遭攻击入侵，工程师除了能够分析找到安全漏洞进行修复外，还要能够进行入侵跟踪。入侵跟踪除了进行入侵习惯的分析，最终目标是定位入侵者。不管是内网还是外网的入侵者，如果领教了该网络后面的工程师的厉害后，也许它就会就此停止对该网络的入侵。入侵跟踪不仅是网络保护，更是对入侵者的震慑。 以上的技巧和经验来自笔者平时为客户做网络支持的实战经历。其实，只要大家善于总结，并掌握一定的技巧，善用相关的工具网络排故并不可怕。另外，平时要注重学习，自觉提高自己的实战和技术素养。希望我的经验能够帮助你。 