ELECTRONIC ENGINEER
XIDIAN UNIVERSITY PRESS

Network Troubleshooting

网络故障诊断

王琨　马志欣　编著

西安电子科技大学出版社
XIDIAN UNIVERSITY PRESS

网络故障诊断

王　琨　马志欣　编著

西安电子科技大学出版社

内 容 简 介

本书首先从基础理论出发，简要讨论了网络可用性与差错管理以及网络故障诊断方法学，而后结合理论与实践经验，比较系统地介绍了计算机网络体系结构、网络管理、网络故障诊断与维护的理论和实践方法及技巧。

全书共分 11 章：网络可用性与差错管理、网络故障诊断方法学、常用网络故障诊断命令、网络故障诊断工具、物理层故障诊断、数据链路层故障诊断、网络层故障诊断、局域网故障诊断、无线局域网故障诊断、广域网故障诊断、常用网络服务故障诊断。

本书内容全面，实例丰富，语言简洁易懂，结构清晰合理。

本书可作为高校网络故障诊断课程的教材，亦可作为中小企业网络管理员学习网络故障诊断的入门参考书。

★本书配有电子教案，需要者可登录出版社网站，免费下载。

图书在版编目(CIP)数据

网络故障诊断/王琨，马志欣编著. —西安：西安电子科技大学出版社，2011.8

西安电子科技大学出版社，2011.8

ISBN 978 - 7 - 5606 - 2583 - 6

Ⅰ. ① 网… Ⅱ. ① 王… ② 马… Ⅲ. ① 计算机网络—故障诊断—基本知识 Ⅳ. ① TP393.07

中国版本图书馆 CIP 数据核字(2011)第 081311 号

策　　划　臧延新

责任编辑　臧延新　樊新玲

出版发行　西安电子科技大学出版社(西安市太白南路 2 号)

电　　话　(029)88242885　88201467　邮　　编　710071

网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com

经　　销　新华书店

印刷单位　陕西天意印务有限责任公司

版　　次　2011 年 8 月第 1 版　2011 年 8 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印　张　12.5

字　　数　292 千字

印　　数　1～3000 册

定　　价　21.00 元

ISBN 978 - 7 - 5606 - 2583 - 6/TP • 1279

XDUP 2875001-1

*** * * 如有印装问题可调换 * * ***

前　言

随着科技的发展，计算机网络已经深入社会的方方面面。与此同时，网络故障引起的系统业务运行不畅也越来越受到人们的关注。为满足社会对网络故障诊断人才的需求，国外一些大学在20世纪90年代就已经设立了网络故障诊断课程，培养相关专业人才。相较而言，直到近几年我国才有为数不多的大学设立了网络故障诊断课程。

目前，国内有关网络故障诊断的书籍或者是针对某些网络设备生产商的产品手册，或者是关于网络操作系统、软件配置使用方面的书籍，适合作为高校相关课程教学的教材还很少，而这正是我们编写本书的主要目的。

本书在讲述网络故障诊断知识的基础上，为读者提供了相应的故障案例和解决方法。力求使读者能感受到这些故障都是自己可能会遇到的，从而引起读者的阅读兴趣。在内容的安排上，通过理论结合实践，帮助读者学习掌握网络故障诊断的基础知识和方法。

本书第1至第7章由王琨编写，第8章至第11章由马志欣编写。具体内容安排如下：

第1章和第2章介绍了网络故障诊断的基础理论知识，是网络故障诊断的方法学，这部分内容是很多其他有关网络故障诊断的书籍所没有的。掌握故障诊断的方法学，有助于培养解决网络故障的能力，而不仅仅是针对已有故障案例给出相应的排除方法。编写这部分内容的目的在于“不仅仅授于鱼，而且授于渔”。

第3章和第4章介绍了一些常用的网络故障诊断命令和诊断工具。其中的一些诊断工具功能非常强大，但使用也非常复杂，本书不可能深入展开讨论，有兴趣的读者可以参考其他相关书籍和产品资料。

第5章到第10章涵盖网络从物理层到网络层，涉及从局域网到广域网的故障诊断基础知识、常见案例及其解决方法。随着无线设备费用的不断下降，无线局域网的应用也越来越广泛，因此，第9章专门介绍了无线局域网的故障诊断。

第11章简单介绍了一些常用网络服务器软件的故障诊断。网络故障不仅仅涉及硬件设备，还会涉及相关软件系统，软件配置错误同样会导致网络访问受阻。因此，本章着重介绍了几个常用服务器软件的故障诊断问题。

本书的主要目标读者是需要学习网络故障诊断基础理论知识，并在此基础上学习网络故障诊断技术的高校学生。本书可作为高校网络故障诊断课程的教材。为此，本书无论在介绍网络故障诊断命令、工具时，还是在介绍相关知识和案例分析时，都假设了一个前提，那就是读者能够接触到本书中使用到的命令、工具和网络设备，也会遇到书中提到的网络故障。这有助于在学习中将理论与实践相结合。

对于中小企业的网络管理员来说，书中列举的一些常见网络故障案例及其解决方法同样有助于他们应对一些常见网络故障。

当然，阅读本书，读者首先需要掌握计算机网络的基础知识。

本书的出版受到了西安电子科技大学教材建设基金资助项目和西安电子科技大学基本科研业务费资助项目(项目编号：JY10000903016)的资助，特此表示感谢！

编　者

2010 年 5 月

于西安电子科技大学

目　录

第 1 章　网络可用性与差错管理

1.1 OSI 参考模型

在谈到网络时，不能不提开放式系统互联(OSI，Open System Interconnect)，也叫 OSI 参考模型。它是 ISO(国际标准化组织)提出的网络互联模型。该体系结构标准定义了网络互联的七层框架，即 OSI 开放系统互联参考模型，如图 1-1 所示。在这一框架下详细规定了每一层的功能，以实现开放系统环境中的互联性、互操作性和应用的可移植性。

图 1-1　OSI 参考模型

下面对这七层的功能分别进行说明。

(1) 物理层。要传递信息就要利用一些物理媒体，如双绞线、同轴电缆等，但具体的物理媒体并不在 OSI 的 7 层之内，有人把物理媒体当作第 0 层。物理层的任务就是为其上一层提供一个物理连接，以及定义其机械、电气、功能和过程特性，如规定使用电缆和接头的类型，传送信号的电压等。在这一层，所传输的数据还没有被组织成任何格式，仅作为原始的位流或电气电压处理，数据的单位是比特。

(2) 数据链路层。数据链路层负责在两个相邻节点间的线路上无差错地传送以帧为单位的数据。每一帧包括一定数量的数据和一些必要的控制信息。与物理层相似，数据链路层要负责建立、维护和释放数据链路的连接。在传送数据时，如果接收点检测到所传数据中有差错，就要通知发送方重发这一帧。

(3) 网络层。在计算机网络中进行通信的两个计算机之间，可能会经过很多个数据链路，也可能还要经过很多通信子网。网络层的任务就是选择合适的网间路由和交换节点，确保数据及时传送。网络层将数据链路层提供的帧组成数据包，包中封装有网络层包头，其中

含有逻辑地址信息。

(4) 传输层。传输层的任务是根据通信子网的特性最佳地利用网络资源，并以可靠和经济的方式，为两个端系统(也就是源站和目的站)的会话层之间提供建立、维护和取消传输连接的功能，负责可靠地传输数据。在这一层，信息的传送单位是报文。

(5) 会话层。在会话层及以上的高层中，数据传送的单位为报文。会话层不参与具体的传输，具有访问验证和会话管理等功能，提供建立和维护应用之间通信的机制，如服务器验证用户登录便是由会话层完成的。

(6) 表示层。表示层主要解决用户信息的语法表示问题。它将欲交换的数据从适合于某一用户的抽象语法，转换为适合于 OSI 系统内部使用的传送语法，即提供格式化的表示和转换数据服务。数据的压缩与解压缩、加密与解密等工作都由表示层负责。

(7) 应用层。应用层确定进程之间通信的性质以满足用户需要，此外还提供网络与用户应用软件之间的接口服务。

OSI 参考模型定制过程中所采用的方法是将整个庞大而复杂的问题划分为若干个容易处理的小问题，这就是分层的体系结构方法，它作为一个框架来协调和组织各层协议的制定。OSI 参考模型定义了开放系统的层次结构、层次之间的相互关系及各层所包含的可能的服务。

OSI 的服务定义详细说明了各层所提供的服务。某一层的服务就是该层及其下各层的一种能力，它通过接口提供给更高一层。各层所提供的服务与这些服务的实现方式无关。同时，各种服务定义还定义了层与层之间的接口和各层所使用的原语，但不涉及接口的具体实现。

1.2 系统故障的原因

商业领域中日益激烈的竞争压力要求公司必须持续不断地优化各自的内部和外部结构，时常检查经营过程及日常工作的可行性和效率。虽然大多数经营过程都是物理活动与信息流程的结合体，但越来越多的关键性商业应用几乎完全由信息流程构成。现代的信息流程在很大程度上取决于信息技术(IT)，即便是持续几小时的网络失效也会给企业带来巨大损失，因此一个具有高性能、高可用性的信息技术系统就逐渐成为成功商业应用的先决条件。对计算机网络实行专业化的运行和管理已经成为几乎所有企业走向成功的决定性策略需求。

目前，网络技术越来越复杂，网络中所使用的软硬件数量也越来越多，使得网络操作和管理也变得越来越困难。现代通信网络要求通信介质、连接器、集线器、交换机、中继器、网卡、操作系统、数据协议、驱动程序以及应用软件在任何情况下都要保持稳定运行。即使网络系统有相对稳定的运行环境，其稳定性也仍然会受到许多不定因素的影响，如操作错误、管理错误、配置变动以及软硬故障等。总之，网络操作系统越复杂，影响其稳定性的因素就越多，也就越难预测其行为。

网络故障常常是由一系列差错引起的，一个事件触发另一个事件，一个差错引发另一个差错，反馈可能会放大也可能会缩小错误事件的影响，因此最终检测到的故障现象的位

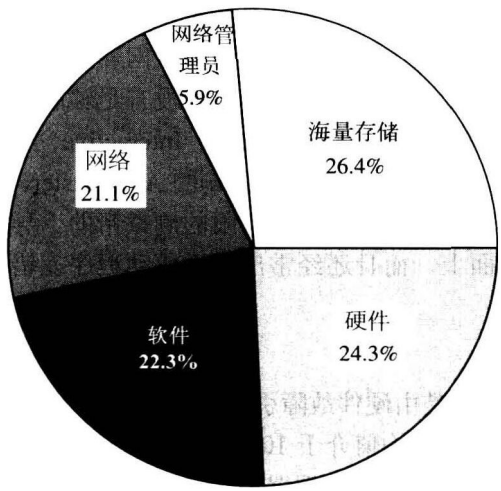
置可能早已远离最初的故障源，而且故障现象看起来也似乎是由其他差错事件引发的。

从网络故障本身来说，经常会遇到的故障有：物理层故障、数据链路层故障、网络层故障、以太网络故障、广域网络故障、TCP/IP 故障、服务器故障、其他业务故障等。

根据统计，网络故障的分布情况由高到低如下：

- 物理层占 35%；
- 数据链路层占 25%；
- 网络层占 12%；
- 传输层占 10%；
- 会话层占 8%；
- 表示层占 7%；
- 应用层占 3%。

引起系统故障的原因有多种，如图 1-2 所示。



数据来源：Find/SVP

图 1-2　系统故障的原因

1. 海量存储问题

数据处理故障的最主要原因是硬盘问题，大约 26%以上的系统失效都可以归结到海量存储的介质故障上。虽然高性能海量存储设备的平均无故障时间(MTBF, Mean Time Between Failures)可以达到 100 小时以上，但如果系统拥有大量硬盘驱动器，就意味着几乎每月都得更换硬盘。一般来说，实际能够达到的 MTBF 要远低于理论 MTBF 值。据统计，在理论 MTBF(1 000 000 小时，相当于 114 年)时间内，只有大约 30%的硬盘可以始终保持正常工作状态。为了计算给定系统在一定时段内需要更换的硬盘数量，可以用系统中的硬盘数量乘以系统服务时间(以小时为单位)，再除以理论 MTBF 值来得到。例如，如果系统中包含 1000 个硬盘，每个硬盘的理论 MTBF 值均为 100 小时，则在第一个 5 年(折合 43 800 小时)内出现故障的硬盘数 A 为

$$A=\frac{1000\times 43\,800\text{小时/硬盘}}{1\,000\,000\text{小时/硬盘}}=44$$

上面的计算方法是基于所有硬盘都具有相同的理论 MTBF，且工作条件也都相同的假设之上。但是，测试表明，工作在湿热环境下的海量存储单元的实际 MTBF 值要大大低于冷却条件良好的工作环境下的 MTBF 值。此外，频繁的磁盘搜索操作和经常性的磁盘位置变动都会降低海量存储介质的使用寿命。因此，某些硬盘厂商在提供了理论 MTBF 值和运行 MTBF 值之外，还提供了另外一个用来表征存储介质无差错运行时间的参数值——累积分布函数(CDF，Cumulative Distribution Function)。CDF 表示了特定时间段内海量存储介质出现故障的概率，如“5 年内的 CDF 值为 4%”表示的是“在第一个 5 年内海量存储介质出现故障的概率为 4%”。

2. 软件问题

软件问题引起的系统失效几乎与硬件问题引起的系统失效一样多。目前广泛应用于企业网中的客户/服务器架构和分布式平台使软件之间的关系变得极为复杂，根本不可能监视所有网络负载和运行状态下的系统行为。在企业内联网和互联网的发展过程中，应用软件的更新周期越来越短，使得软件在发布之前根本就没有足够时间来测试软件的可靠性，因此，只能借助于某些自动测试工具，如 Mercury Interactive 公司(www.loadrunner.com)的 LoadRunner、Auto Tester 公司(www.autotester.com)的 Auto Tester。虽然这些自动测试工具能够模拟不同的极限操作环境，但也只能提供有限的测试帮助。导致系统失效的新软件问题已不再仅仅局限在应用层面上，而且还经常出现于驱动程序差错、安装或备份程序差错以及操作系统差错上。

3. 硬件问题

大约有 1/4 的系统失效都是由硬件故障引起的。此处的计算机硬件包括计算机的所有组件。目前计算机系统的 MTBF 平均值介于 10 000～50 000 小时之间。系统越复杂，其平均 MTBF 就越低。例如，一个具有多个处理器和多条网络连接的计算机系统出故障的概率要高于相对较为简单的只有单个处理器的服务器。

相对于 MTBF，年故障率(AFR，Annual Failure Rate)可以更好地表征系统的可靠性，它等于 MTBF 除以系统一年运行的总时间(以小时计)。例如，一个服务器系统每年大概要出现 3 次故障。另一个表征计算机系统可用性的重要参数是平均修复时间(MTTR，Mean Time to Repair)，它表示了修复系统失效的平均时间。MTTR 等于修复系统失效的总时间除以失效次数。MTTR 的典型值介于 2～3 小时之间(此处的修复时间是指实际修复系统失效的工作时间)。

4. 网络问题

当我们把与网络操作直接相关的软硬件问题等都归到本类原因时，由网络自身引起的系统失效可以占到系统失效原因的 1/3 以上。可以按照 OSI 分层结构来划分这些网络差错。LAN 差错中大概有 30%都发生在 OSI 的第一层和第二层上，这类故障原因主要有：线缆、连接器或网卡损坏；集线器、网桥或路由器的模块出现故障；以太网中发生冲突；令牌环网重点环路严重告警进程；校验和出错；包大小不正确等。对这类故障只能靠开发和生产

出更高质量的硬件系统，并不断地提高线缆质量来减少故障出现的绝对次数。对发生于 OSI 高层上的差错只能靠严格控制高层软件的质量来减小出现故障的概率。网络操作系统、应用软件以及协议栈越稳定，网段中出现故障的次数就越少。总之，由网络自身问题引起的系统失效的原因在 OSI 所有 7 层上的分布大致相同。

在 WAN 中，由物理层差错引起的系统失效所占的比例更高。对永久 WAN 链路(租用线)来说，几乎 80%的差错都是由网络组件失效、调制解调器损坏以及线缆和连接器有问题引起的。对 ISDN 来说，这一比例更是高达 90%以上。

5. 网络管理员差错

据统计，网络管理员差错引起的网络失效占所有网络失效事件的 5%以上。网络管理员差错可以分为有意差错和无意差错。

有意差错并不是指网络管理员故意制造网络故障，而是指差错是由有意识的行为引起的，如执行某些快捷操作。因为有时候网络管理员认为可以简化某些特定的处理过程，或认为完全没必要遵守那些繁琐的安全操作指南，从而产生直接的或间接的网络差错。有意差错与带有不良企图的故意行为不一样。例如，某个员工为了报复管理人员或公司，或者有意给同事制造麻烦而故意破坏网络的行为就不是有意差错。

无意差错，主要起源于网络管理员对某些处理过程缺乏了解或没有给予足够重视。其他典型原因还包括软件和硬件差错以及安装和配置差错。此外，无意差错还可能由许多小差错引起，虽然这些小差错的单个影响都显得微不足道，但累加起来却足以导致网络失效。

1.3 系统故障的损失

估算系统失效引起的损失已变得越来越重要，因为这样可以从网络管理和网络维护角度出发确定网络的最佳规模，虽然这种估算很难准确化。知道了系统失效的代价之后，企业就可以据此来确定冗余设备以及网管系统和系统故障检测与修复的投资规模。

目前数据网络的可用性可达 98%～99%。对一个一周工作 5 天、一天工作 10 小时的系统来说，一年的网络中断时间为 52～104 小时。如果每次网络中断平均影响到 100 个人，则每次网络中断带来的产值损失就为 5200～10 400 小时。但是，这种计算方法过于简单，不能反映实际的损失情况，因此计算出来的损失要大于实际损失。

为了更准确地计算网络中断带来的损失，首先应区分立即损失和后效损失。每类损失又可以细分为直接损失和间接损失。其中，直接损失包括修复网络故障所需的各类直接开销，而间接损失指员工生产率下降或工程工期推延等引起的损失。

(1) 立即损失，指网络中断后 24 小时内造成的损失。

① 直接损失。例如：更换网络组件、增加新的网络组件、租用或购买诊断工具、网络专家的咨询费、软硬件厂商的咨询费、网络支持人员的加班工资等。

② 间接损失。例如：员工生产率下降、系统停工时间、客户或客户订单丢失以及客户信任度下降等。

像购买网络组件或咨询费等直接损失的计算较为简单，只要依据各类实际的单据、发票即可完成。对一个可用性为99%的中型网络(大约拥有500个节点)来说，每年的网络中断时间大概为52小时，网络或网络组件的故障次数为10～20次，每次网络中断1～5小时，如果每次解决网络故障的直接立即损失为1250美元，则10次网络中断将造成12 500美元的直接损失。

但是，定量计算网络中断造成的间接损失比计算直接损失要困难得多，一般只能计算员工生产率的累计损失，而这种损失与员工的生产率依赖于网络可用性的程度有关。在实际中，许多员工的生产活动可以推延几个小时至一天，因此不会造成生产率的下降。对中等规模的企业来说，网络中断造成员工生产率损失可以粗略地用网络中断时间的25%计算。例如，如果每次受网络中断影响的员工平均为100人，则每年52小时的网络中断造成的生产率损失为 $52 \times 0.25 \times 100 = 1300$ 小时。如果每小时的工资费用为40美元，则总的立即间接损失即为 $1300 \times 40 = 52\,000$ 美元。

(2) 后效损失，指网络中断24小时以后引起的损失。

① 直接损失。例如，新建或调整网络硬件配置，测试其他网段中相似差错，编制系统故障文档。

② 间接损失。例如，延误工期，耽搁业务处理，降低客户的忠诚度和满意度。

后效间接损失是所有网络失效造成的损失中最难计算的一种损失，这类损失一般也称为“公司损失”，因为这类损失无法归结到公司的任何部门或成本中心。该类损失的大小与公司对网络支撑处理系统的依赖程度成正比。例如，由于网络中断，导致无法打印标书，进而耽搁了公司的投标时间，到手的订单或支票也被耽搁了；由于无法打印收入传票而无法接收运到的货物；自动仓储系统无法运行等。如果货物采用特快方式运送，在网络出现故障时会增加运送成本；由于网络中断致使支付延时；由于无法使用基于Web的订单系统，因此销量下降；客户如果无法登录服务热线，将会产生不满情绪，因此可能会丧失今后的潜在订单。这些仅仅是网络中断给公司造成的部分后效损失。

1.4 系统的高可用性

对稳定的经营活动来说，高可用性是商业数据处理中最基本的要求。除了采用特别的方法来提高系统的可用性之外，目前IT系统的可用性普遍在98%～99%之间，相当于年中断时间为50～100小时。这样的可用性远远达不到要求，必须采用特别措施将系统的可用性提升到99.9%～99.999%(99.999%相当于每年的中断时间只有6.8分钟)，从而将中断时间减少到几小时甚至几分钟。

但是，系统可用性的提高是以增加大量的系统投入为代价的(几乎按指数关系递增)。因此在规划高可用性系统之前，要明确究竟需要提供什么级别的业务，从而决定系统可用性的指标。

评价系统的一个重要指标是系统失效引起的平均中断时间。在大多数场合下，持续几秒钟或几分钟的业务中断是可以接受的，但是那些持续几小时的业务中断则大多会造成严

重的后果。

构建高可用的网络需要使用高质量的网络组件，因为即使没有采用任何特殊的设备或配置措施，网络组件的质量也是决定系统软硬件可靠性的重要因素，而且网络组件的质量高低也决定了诊断工具、系统和网管应用的性能，以及能达到的系统维护和支撑级别。只要能保证所选网络组件的质量，系统的可用性就一定能大大高于平均值。如果希望进一步提高系统的可用性，就必须采用以下额外的网络组件和技术手段：

- 冗余组件；
- 软硬件交换技术；
- 详细规划每一次预定的网络中断；
- 减少系统管理任务；
- 开发自动差错反应系统；
- 在安装新的软硬件时进行全面检查；
- 提高网络管理员对系统故障的反应能力；
- 备份数据库和应用软件；
- 集群技术。

如果同时使用冗余组件和软硬件交换技术，则可以使冗余组件在几秒钟之内接管出故障的组件。此外，简化网络与网络管理员之间的交互级别也有助于建立不同差错环境下的确定反应。在理想情况下，某个给定的差错始终只会触发某个预定义的处理过程。图 1-3 中给出了建立高可用性系统的详细步骤。

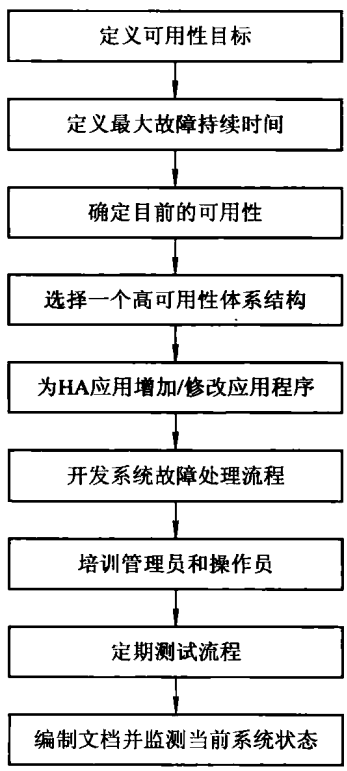


图 1-3　高可用性系统的建立步骤

1.5 企业的网络系统准则

不仔细规划网络管理系统或不严格遵守精确规定的操作规程，就不可能运营和维护规模越来越大且越来越复杂的数据网络。现代的网络管理大多基于服务等级协议(SLA，Service Level Agreement)。SLA 规定了具体的服务质量指标，因此网络管理员的首要任务就是确保 SLA 的实现，这代表了网络管理方式的重大变革。直到目前，网络运营的各个方面(如网络管理、差错管理、安装、配置和规划)基本上还是独立实施，但现在的服务管理已经要求将所有的任务都统一实现在 SLA 之下，以便更有效、更有针对性地使用网络资源。为了实现 SLA，还需要长期监视数据处理系统的运行情况并取得相关数据，从而有助于做出更切合实际的网络容量规划方案，并对整个数据处理系统实施更为精细的开销管理。

SLA 应针对企业准则中指定的主要服务类型进行逐项定义，精确描述所提供服务的质量等级、相应的价格、用户群体以及生效时间，并明确规定一天多少小时，一周(或一月)多少天提供规定等级的服务，其中包括必要的网络维护时间。SLA 还要具体规定用户的数量和位置，以及用户提供的硬件设施等内容。此外，SLA 还应描述用户的报障、服务变动请求等流程，以及满足这些用户要求的升级流程和网管响应时间。最后，SLA 还应详细定义以下服务质量参数所能达到的指标：

- 平均可用性；
- 最低可用性；
- 平均响应时间；
- 最大响应时间；
- 平均吞吐量。

不幸的是，客户常常拒绝参与 SLA 中规定的培训课程，或不愿遵守其中规定的操作流程。如果客户没有遵守这些约定，就应该为违反 SLA 生产的后果负责。在许多公司签订的 SLA 中都可能包括以下典型服务：用户支持、网络打印服务、电子邮件服务、Internet 接入服务、服务器存取以及一般的网络操作等。此外，对那些关键性的应用(如客户预订系统、数据库和产品控制系统等)也应该制定相应的 SLA。

差错管理属于网络管理的级别，但差错管理的许多方面都与其他的数据处理服务管理密切相关，因此服务管理的各个方面都在差错管理策略中扮演着重要的角色。例如，某个 SLA 中可能包含所提供服务的最大平均修复时间，为此就会对网络支撑部门的员工和网络设备提出相应的要求。因此，一个完整的差错管理策略至少应包括以下网络管理要素：

- 数据处理应用的企业准则；
- 网络提供的所有服务类型；
- 为所有服务定义详细的 SLA；
- 系统的网络规划；
- 所有网络组件的系统记录；
- 网管工具的使用；