高等院校计算机应用系列教材

计算机网络故障诊断与排除

(第 4 版)

黎连业　罗　昶　王　萍　黎长骏　潘朝阳　编著

清华大学出版社
北　京

内 容 简 介

本书详细介绍了计算机网络故障诊断与排除方面的知识。全书由 11 章组成，内容包括网络故障和网络诊断测试工具、物理层故障诊断与排除、数据链路层故障诊断与排除、网络层故障诊断与排除、以太网络故障诊断与排除、广域网络故障诊断与排除、TCP/IP 故障诊断与排除、服务器故障诊断与排除、其他业务故障诊断与排除、网络故障管理和数据备份以及无线网络故障诊断与排除。

本书取材新颖，内容丰富，叙述由浅入深，重点突出，概念清晰易懂，是一本实用性很强的图书。

本书原为中科院计算所培训中心计算机网络故障诊断与故障排除课程指定教材，可作为高等学校计算机网络相关课程的教材，也可作为网络管理人员、信息系统管理人员、工程技术人员的参考书。

图书在版编目(CIP)数据

计算机网络故障诊断与排除 / 黎连业等编著. 4 版. -- 北京 : 清华大学出版社, 2025. 4. -- (高等院校计算机应用系列教材). -- ISBN 978-7-302-68251-6

Ⅰ. TP393.07

中国国家版本馆 CIP 数据核字第 2025C5Z247 号

责任编辑：刘金喜
封面设计：高娟妮
版式设计：思创景点
责任校对：成凤进
责任印制：丛怀宇

出版发行：清华大学出版社

网　　址：https://www.tup.com.cn，https://www.wqxuetang.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-83470000　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62794504

印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**24.75　　**字　　数：**682 千字
版　　次：2007 年 4 月第 1 版　　2025 年 4 月第 4 版　　**印　　次：**2025 年 4 月第 1 次印刷
定　　价：79.00 元

产品编号：087041-01

前　言

本书基于计算机网络故障诊断与排除，围绕着“故障”展开知识介绍，以网络故障的诊断与测试为主线，对物理层故障、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、网络故障管理和数据备份、无线网络故障等进行了详细的讨论。本书取材新颖，内容丰富，反映了网络故障诊断与故障排除所涉及的知识，是作者多年来积累的网络管理经验和教学经验的总结。

全书由11章组成，它们是：

第1章——网络故障和网络诊断测试工具；第2章——物理层故障诊断与排除；第3章——数据链路层故障诊断与排除；第4章——网络层故障诊断与排除；第5章——以太网络故障诊断与排除；第6章——广域网络故障诊断与排除；第7章——TCP/IP故障诊断与排除；第8章——服务器故障诊断与排除；第9章——其他业务故障诊断与排除；第10章——网络故障管理和数据备份；第11章——无线网络故障诊断与排除。

本书是在第3版的基础上编写的，本版改动较大，改动重点放在新技术上，新技术部分除了介绍基本知识，还融入了对实际应用中所产生的问题的一些实践和体会。对第3版中还在使用的传统的知识作了保留或修改，对数据存储内容进行了重写。本书取消的内容在PPT中予以保留，原因是许多单位以前是用磁带作为存储介质的，现在逐步改用磁盘阵列，在这一转换过程中，还需要这方面的知识；服务器部分增加了新内容，目的是国内的中小型网络将会转向国内产品。对即将淘汰的技术只做简要介绍。

本版修订工作由黎连业、王萍执笔。书中增加了许多新知识，需要读者跟上新知识、新技术迭代的步伐。

本书各章均有配套习题，以供读者巩固、复习所学知识。本书PPT教学课件可通过扫描右侧二维码下载。

教学资源

本书可作为高等学校计算机相关专业的教材，也可以作为计算机相关培训教材。本书也适合网络管理人员、信息系统管理人员、工程技术人员阅读和参考。

由于水平有限，书中难免有不当之处，敬请读者批评指正。

服务邮箱：476371891@qq.com。

作　者

2024年7月

目　录

第 1 章

网络故障和网络诊断测试工具

本章重点介绍以下内容：

- 网络故障概述；
- 网络管理系统基础知识；
- 常用的网络故障测试命令；
- 网络故障管理系统；
- 网络故障诊断；
- 网络故障管理；
- 网络故障的定位；
- 网络诊断工具；
- 网络测试工具。

1.1 网络故障概述

在信息化社会里，各企事业单位对网络的依赖程度越来越高，网络随时都可能发生故障，影响正常工作。所以，必须掌握相应的技术及时排除故障。有些单位如电信、电子商务公司、游戏运营商等使用的网络一旦发生故障，若不能及时排除，会产生很大的损失。这些单位一般会安装网络故障管理软件，通过软件来管理和排除网络的故障。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；
- 无线网络故障等。

那么，网络发生故障的原因是什么呢？根据有关资料的统计，网络发生故障的具体分布为：

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

引起网络故障的原因还有以下几种：

(1) 逻辑故障

逻辑故障中最常见的情况有两类：一类是配置错误，指由于网络设备的配置错误而导致的网络异常或故障。配置错误可能是路由器端口参数设定有误，或路由器的路由配置错误，以至于路由循环找不到远端地址，或者是路由掩码设置错误等。另一类是一些重要进程或端口被关闭，主要是系统或路由器的负载过高。

(2) 配置故障

配置错误也是导致故障发生的重要原因之一。配置故障主要表现在不能实现网络所提供的各种服务，如不能接入 Internet，不能访问某种代理服务器等。配置故障通常表现为以下几种情况：

- 网络链路测试正常，却无法连接到网络；
- 只能与某些计算机通信，而不能与全部计算机通信；
- 计算机只能访问内部网络中的服务器，但无法接入 Internet，这可能是路由器配置错误，也可能是交换机配置错误；
- 计算机无法登录至域控制器；
- 计算机无法访问任何其他设备。

(3) 网络故障

网络故障的原因是多方面的，一般分为物理故障和逻辑故障。物理故障又称硬件故障，包括线路、线缆、连接器件、端口、网卡、网桥、集线器、交换机或路由器的模块出现的故障。

(4) 协议故障

计算机和网络设备之间的通信是靠协议来实现的，协议在网络中扮演着非常重要的角色。协议故障通常表现为以下几种情况：

- 计算机无法登录至服务器；
- 计算机在网上邻居中既看不到自己，也看不到其他计算机或查找不到其他计算机；
- 计算机在网上邻居中能看到自己和其他计算机，但无法在局域网络中浏览 Web、收发 E-mail；
- 计算机无法通过局域网接入 Internet；
- 与网络中其他计算机的名称重复，或者与其他计算机使用的 IP 地址相同。

(5) DDoS 攻击

DDoS 即分布式阻断服务(Distributed Denial of Service)，黑客可以利用 DDoS 使很多计算机在

同一时间遭受攻击，引起网络故障，导致很多大型网站出现无法操作的情况。

(6) 网络管理员差错

网络管理员差错占整个网络故障的5%以上，主要发生在网络层和传输层，是由于安装设置没有完全遵守操作指南，或者网络管理员对某个处理过程没有给予足够的重视造成的。

(7) 海量存储问题

数据处理故障的最主要原因是硬盘问题。据有关报道，大约有超过 26%的系统失效都归结到海量存储的介质故障上。

(8) 计算机硬件故障

大约有 25%的故障是由计算机硬件引起的，如显示器、键盘、鼠标、CPU、RAM、硬盘驱动器、网卡、交换机和路由器等。

(9) 软件问题

软件引起的故障也不少见，表现为：

- 软件有缺陷，造成系统故障；
- 网络操作系统缺陷，造成系统失效。

(10) 网络使用者发生的差错

网络使用者没有遵守网络赋予的权限。例如：

- 越权访问系统和服务；
- 侵入其他系统；
- 操作其他用户的数据资料；
- 共享账号；
- 非法复制。

既然有网络故障产生，就有网络管理。

网络故障管理一般包括 5 项：

- 对网络进行监测，提前预知故障；
- 发生故障后，找到故障发生的位置；
- 解决故障；
- 记录故障产生的原因，找到解决方法；
- 故障分析预测。

1.2　网络管理系统基础知识

网络管理人员是通过网络管理系统来对网络故障进行监测，进而排除故障的，因此了解网络管理系统就显得非常重要。

1.2.1　网络管理系统的分类

随着技术的不断进步，网络管理系统的发展经历了四代。

- 第一代网络管理系统是最常用的命令行方式，它结合一些简单的网络监测工具，要求管理人员精通网络的原理，了解不同厂商的网络设备的配置方法和管理命令。
- 第二代网络管理系统有了图形化界面，管理人员无须过多了解设备的配置方法，就能图形

化地对多台设备同时进行配置和监控，提高了工作效率。

- 第三代网络管理系统采用 B/S 架构，将网络和管理进行有机结合，具有“自动配置”和“自动调整”功能，可实现远程管理，实现起来也非常容易。对网管人员来说，只要把用户情况、设备情况以及用户与网络资源之间的分配关系输入网络管理系统，系统就能自动建立图形化的人员与网络的配置关系，并自动鉴别用户身份，分配用户所需的资源。
- 第四代网络管理系统通过网络管理组件系统集成平台实现对全网络所有设备进行有效管理；对远程的网络设备或设施进行具体的操作、查询和分析，进行实时的网络运行监测；使用统一的方法在一个异构网络中管理多个厂商生产的计算机硬件和软件资源。第四代网络管理系统是目前各厂商研究的重点。

网络管理系统没有完全统一的分类标准，总的来说可以从三个角度来分类。

1. 根据管理对象分类

根据网络管理对象可将网络管理系统分为两大类，即网元(网络设备)管理系统和通用网络管理系统。

网元管理系统只管理单独的网元(如交换机、路由器、服务器等)，通用网络管理软件的管理目标则是整个网络。

(1) 网元管理系统

网元管理系统一般由设备厂商提供，各厂商采用专有的 MIB 管理库，以实现对厂商设备本身的管理，包括可以显示厂商设备图形化管理界面的面板，如华为网络公司的 Quidview、安奈特公司的 AT—View Plus、思科公司的 Cisco View 等。

(2) 通用网络管理系统

通用网络管理系统主要用于掌握全网的状况，如国内游龙科技的 SiteView、网强信息技术公司的网强网管、惠普公司的 HP Open View、CA 公司的 Unicenter、IBM 公司的 Tivoli NetView、安奈特公司的 AT-SNMPc 等。这些第三方网管平台支持对所有 SNMP 设备的发现和监控，可集成厂商设备的私有 MIB 库，实现对全网设备的统一识别和管理，从而打破了需要采用多台网管工作站分别安装不同的系统进行分别管理的局限性，有利于简化管理和降低成本。

2. 根据管理范畴分类

根据网络管理的范畴，网络管理系统可分为对交换机、路由器等主干网络进行管理；对接入设备的内部 PC、服务器进行管理；对用户的使用进行管理；对网络系统软硬件信息进行管理等。

3. 根据管理功能分类

国际标准化组织将网络管理系统定义为五大功能：故障管理、配置管理、性能管理、安全管理、计费管理。根据功能的不同，网络管理软件产品又可细分为五类：网络故障管理软件、网络配置管理软件、网络性能管理软件、网络服务/安全管理软件及网络计费管理软件。

(1) 故障管理

故障管理是在网络出现故障时，网络运行管理系统能够迅速查找并及时排除故障，从而保障网络的安全运行。故障管理主要是为了发现和排除故障，通过对设备、软硬件和节点的监控、分析，来实现对故障的诊断、定位和处理。

故障管理包括故障检测、故障隔离和故障纠正三方面的内容。其中，故障检测可以通过主动探测或被动接收获取网络上的各种事件信息，对发生故障的事件进行记录、跟踪，同时故障检测负责对故障日志进行维护和检查；故障隔离是指通过检测所获取的信息，分析发生故障的原因，

执行诊断测试，定位故障发生的位置；故障纠正指通过之前的分析、定位结果，结合故障发生的原因，对故障进行纠正和修复。

(2) 配置管理

配置管理指通过配置网络提供网络服务，其主要负责建立网络、展开业务和维护配置数据。配置管理集成了一个通信网络所必需的相关功能，包括辨别、定义、控制和监视等，并通过相关配置来实现网络性能的最优化。

配置管理主要包括自动获取配置信息、配置一致性检查和用户操作记录等功能。其中，自动获取配置信息支持网络管理人员通过相关技术手段来实现网络配置信息的自动获取功能。而网络的配置信息可以分为三类：

- 网络管理协议标准的 MIB 中定义的配置信息，包括 SNMP 和 CMIP 协议；
- 维护设备运行的重要配置信息，但这些信息不在网络管理协议标准中定义；
- 辅助信息，这些信息主要用于对网络进行管理。

配置一致性检查是为了防止由不同人员对网络进行配置所出现的不一致问题，而在网络配置中，对网络运行影响最大的主要是路由器端口配置和路由信息配置，因此，配置一致性检查也主要是对路由器端口配置和路由信息配置的检查。

用户操作记录能够对用户进行的每一步配置操作进行记录，并生成记录文件，以供网络管理人员随时查看，从而保证网络运行的安全性。

(3) 性能管理

性能管理通过对系统资源的运行状况以及通信效率等系统性能进行评估，以维护良好的网络服务质量和较高的网络运行效率。性能管理的功能主要包括性能监控、阈值控制、性能分析和性能管理。

- 性能监控。性能监控可以由用户定义监控对象及其属性。监控对象包括网络线路和路由器；监控对象的属性则包括网络流量、网络延迟、丢包率、内存余量、CPU利用率以及温度。对于每个监控对象需要定时采集性能数据，并且自动生成性能报告。
- 阈值控制。阈值控制可以对监控对象的每一条属性分别设置阈值，同时也可以根据不同的时间段和各自的性能指标来进行阈值设置。阈值控制就是通过对阈值进行设置实现相应的阈值管理和报警机制。
- 性能分析。性能分析是对所记录的历史记录进行统计、分析和整理，计算出性能指标，并对相应的性能状况作出判断，为网络规划提供建议和参考。而性能分析的结果则可能会触发某个诊断测试过程或重新配置网络，以维持网络的性能。
- 性能管理。性能管理通过对实时数据进行采集，对流量、负载等性能进行实时分析，实现对当前网络状况信息进行收集和分析。

(4) 安全管理

网络的安全性是网络管理中最为重要的部分。安全管理的任务是：

- 控制对网络资源的访问；
- 防止网络信息遭到恶意攻击和修改；
- 保护敏感信息不被泄漏；
- 防止非法获取。

安全管理主要包括授权机制、访问控制、加密管理和系统日志分析等功能。其中，授权机制通过身份验证等方式保护网络资源不被未授权的用户访问，避免入侵者非法获取。访问控制通过用户分组管理可以限定不同用户组中用户的权限，对用户的操作和访问进行控制，保证用户不能

越权访问网络资源。加密管理用于数据的存储和传输时的加密与完整性，通过在 Web 浏览器和网络管理服务器之间采用安全套接层(SSL)传输协议，对管理信息加密传输并保证其完整性；同时，网络内部所存储的数据等信息也都是经过加密的，从而保证数据的安全性。系统日志分析可以记录用户的所有操作，使用户对网络访问的操作以及网络管理人员对网络的修改均有据可查，从而有助于故障的跟踪和恢复，保障网络的安全运行。

(5) 计费管理

计费管理对公共商业网络是极为重要的一项功能，它通过对网络的使用情况进行统计和记录，来实现对网络资源的控制和操作代价的估算，并根据各用户对网络资源的使用情况进行计费。网络管理人员还可以对用户可以使用的最大资源和费用进行限定，从而避免用户占用过多的网络资源，以保证网络的性能，提高网络效率。

计费管理主要包括计费数据采集、数据管理与维护、数据分析与费用计算和数据查询等功能。数据分析与费用计算是通过采集到的用户对资源的使用信息，对用户的网络使用状况进行分析，并结合用户的相关信息进行费用计算。数据查询可以向网络管理人员和用户提供数据查询功能，网络管理人员可以查询出所有用户对网络资源的使用情况和费用记录，用户可以查询自己的网络使用记录以及账单，核对费用。

现在大多数网络管理软件都是以上功能的集合，单一功能的网络管理软件已不存在。

1.2.2 新兴技术和新行业对网络管理系统的新要求

现在的新兴技术和新行业与过去相比有很大不同，出现的新兴技术和新行业有云计算、大数据、移动通信网络、智能移动支付技术、物联网、智能电网、社交平台、电商等。这些新技术提高了网络管理流程的复杂性，网络管理人员需要全面、深入了解网络性能，提高对网络混合环境的认知能力，更科学地进行网络管理；需要使用更新的综合管理系统，能够支持智能化的操作模式、灵活匹配复杂的业务需要和资源监控，实现全方位立体化监控和排除网络故障。

网络故障的检测、发现和纠正不是容易的事情，大型数据中心和云网络让网络故障管理更具挑战性。

1. 云计算网络管理和排除网络故障的新要求

为加强云计算服务网络安全管理，维护国家网络安全，国家就党政部门云计算服务网络安全管理提出了相关管理意见，要求提供云计算服务的服务商遵守以下要求：安全管理责任不变；数据归属关系不变；安全管理标准不变；敏感信息不出境；合理确定采用云计算服务的数据和业务范围；对数据的敏感程度、业务的重要性进行分类；对于涉及国家秘密、工作秘密的业务，不得采用社会化云计算服务。对于包含大量敏感信息和公民隐私信息、直接影响党政机关运转和公众生活工作的关键业务，应在确保安全的前提下再考虑向云计算平台迁移；对于保护等级四级以上的信息系统，以及一旦出现问题可能造成重大经济损失，甚至危害国家安全的业务不宜采用社会化云计算服务。

当前的云计算技术与过去相比有很大不同，网络技术人员比较感兴趣或比较在意的地方有：

(1) 广域网线路和设置问题，不仅仅是指网络带宽。

(2) 与位置无关的计算。

(3) 规模和可靠性预期要增强。

(4) 故障点增多。

(5) 灾难恢复计划和风险评估需要重新制定。

(6) 云服务提供同步的重要性。

(7) 配置管理服务升级和迁移要有一致性，避免新服务对于业务产生冲击。

(8) 云服务带来的监测方面的挑战。随着云服务的普及，它对网络的影响仍然是 IT 决策者重点关注的领域。外部公共云流量最为普遍，约占网络流量总量的 45%，对网络性能的监测和管理将会是一项挑战，不能仅使用现有解决方案来监督云网络，需要为云服务获取一些新的监控和故障排除工具。依赖大量解决方案的网络团队不太可能检测到网络问题，而且更有可能每年遭受更多的网络服务中断。

(9) 最新的研究趋势和工具。

(10) 网络性能。网络性能取决于连接用户到应用的网络的类型和容量。很多拓扑结构和设计(其中包括虚拟化服务器、多个虚拟局域网和覆盖网络)让云故障检测和网络故障管理变得更加复杂，一个租户的应用出现性能问题可能会影响另一个租户的问题，虽然看起来没有什么关联，但它们可能是同一来源。每个租户的应用可能在相同超载或配置错误的服务器上执行，或者两个租户的覆盖网络通过相同超载或故障链接来路由。

(11) 海量的服务器、网络组件和链接出现故障。尽管硬件极为可靠，每个组件有多年平均无故障时间，但对于数千个独立的设备来说，依旧会有硬件故障发生。

(12) 配置错误。该问题可由网络故障管理系统进行跟踪。大型云计算系统通常包括来自不同供应商的组件，甚至来自同一供应商的相同组件也可能运行着不同的软件版本，服务器和网络设备不断添加、升级或取代。在这种环境中，任何变更都可能导致错误的出现，同时，对一个组件的改变还可能影响到其他组件。

(13) 链路故障。该故障会在链路两端的交换机上生成硬件故障提示，并且每次故障产生和恢复时都会发出新报告。第 2 层和第 3 层网络协议路由会改变，在备用路由流量水平接近最大数值时链路流量监控也会变化。同时，性能监控器会报告相应问题。

(14) 从云计算安全方面来考虑网络管理工作，如攻击保护、固件管理、备份、数据安全、性能优化等项目，防止外来入侵者对云计算中心发起恶意攻击，进入到云计算中心内部窃取或者破坏重要的数据。

(15) 网络操作系统平台。网络管理系统的运行都要求相应的网络操作系统平台的支持，目前用于网络管理的网络操作系统平台有三个：UNIX、Windows 和 Linux。通常大型网络中采用 UNIX 操作系统，而在一般的中小型网络系统中，采用的大都是 Windows 网络操作系统平台或 Linux，如 Windows Server 2022 系列。

(16) 云计算作为未来网络经济社会重要的基础设施，能否自主可控？它涉及国家安全，这就决定了凡是涉及国家安全的重要领域的云计算服务，比如金融、电信、能源、交通等重点领域都需要迅速查找到故障并能够及时排除故障，从而保障网络的安全运行。

2. 大数据中心网络管理和排除网络故障的新要求

(1) 大数据概述

大数据近几年来蓬勃发展，其应用已经十分广泛，尤其以企业为主，企业成为大数据应用的主体。它不仅是企业趋势，也是一个改变了人类生活的技术创新。

大数据对行业用户的重要性也日益突出。掌握数据资产，进行智能化决策，已成为企业脱颖而出的关键。

大数据是建设智慧城市的内核，智慧城市是大数据的源头。从市场角度看，大数据改变经济社会管理方式，可以提高企业经营决策水平和效率，推动创新，给企业、行业领域带来价值，促进行业融合发展。在技术和业务的促进下，跨领域、跨系统、跨地域的数据共享成为可能，大数

据支持着机构业务决策和管理决策的精准性与科学性，社会整体层面的业务协同效率提高。推动产业转型升级。

① 大数据特征

- 容量：指数据的大小决定所考虑的数据的价值和潜在的信息。
- 种类：指数据类型的多样性。
- 速度：指获得数据的速度。
- 可变性：妨碍了处理和有效管理数据的过程。
- 真实性：指数据的质量。
- 复杂性：数据量巨大，来源多渠道。
- 价值：合理运用大数据，以低成本创造高价值。

② 大数据的数据结构

大数据的数据结构分为结构化、半结构化和非结构化数据。非结构化数据越来越成为数据的主要部分。IDC 的调查报告显示，企业中 80%的数据都是非结构化数据，这些数据每年都按指数增长 60%。大数据在以云计算为代表的技术支持下，把原本很难收集和使用的数据利用起来了。通过各行各业的不断创新，大数据会逐步为人类创造更多的价值。

③ 大数据的层面

大数据的第一层面是理论。理论是认知的必经途径，也是被广泛认同和传播的基线。我们可以根据大数据的定义理解行业对大数据的整体描绘和定性；根据大数据价值来深入解析大数据的意义所在，洞悉大数据的发展趋势；从大数据隐私的视角审视人和数据之间的长久博弈。

大数据的第二层面是技术。技术是大数据价值体现的手段和前进的基石。云计算、分布式处理技术、存储技术和感知技术是大数据从采集、处理、存储到形成结果的整个过程。

大数据的第三层面是实践。实践是大数据的最终价值体现。我们可以根据互联网大数据、政府大数据、企业大数据和个人大数据四个方面来展望大数据的美好前景。

④ 大数据的核心点

大数据的核心点是：采集各行业的大数据，然后进行数据处理，最终作出决策并提出解决方案。

⑤ 大数据给我们带来了什么

大数据已经存在于我们生活中的方方面面。我们的消费记录，每天经过的路线，和亲朋好友们说过的话，我们看过的东西，生活中几乎所有的东西都记录在案。生活在网络时代我们已经没有秘密。

比如，我们刚刚在网上查找了一些东西，网页广告上就会弹出相关方面的广告，接着“抖音”就为我们推荐相关的视频。更有甚者，我们可能只是在和朋友的交流中提到想买什么东西，之后打开“淘宝”就突然发现淘宝的首页推荐里就出现了我们之前提到过的东西。这些都是大数据的功劳。

大数据为我们的生活带来了便利，同样也带来了诸如隐私泄露之类的弊端，如何利用好大数据，是我们当前面临的问题。

⑥ 数据中心

云计算、互联网、物联网、大数据等现代信息技术已成为国民经济的重要支柱。数据中心是一切信息化的基础，可以说，没有数据中心就没有信息化的发展。

随着数据中心的建设规模不断扩大，新技术层出不穷，数据中心变得越来越复杂。数据中心往往是由很多规模庞大的集群系统组成的，规模非常大，面临的挑战和问题非常多，所以要做好大型数据中心网络管理和网络故障排除工作。只有对这个数据中心整体非常了解，才能有针对性

地制定网络管理和故障排除方案，提升整个数据中心的运行效率，减少故障的发生。

(2) 大数据安全面临的挑战

① 大数据安全标准

大数据安全标准共分为五类：基础标准、平台和技术、数据安全、服务安全、行业标准。

② 大数据的安全体系

大数据的安全体系分为五个层次：周边安全(传统意义上提到的网络安全技术，如防火墙等)、数据安全(对数据的加密和解密，又可细分为存储加密和传输加密；还包括对数据的脱敏)、访问安全(认证和授权)、访问行为可见、错误处理和异常管理。

③ 大数据安全相比传统数据安全的特殊性

大数据安全虽仍继承传统数据安全保密性、完整性和可用性三个特性及云计算网络管理和排除网络故障的新要求，但也有其特殊性，主要表现在以下两方面。

- 个人隐私保护

以前数据是企业的资产，是在企业内部、局部的环境里使用，流动性不强，所以数据的个人隐私表现不突出。但是到了“互联网+”时代，数据无处不在，各种数据积累起来后形成了多元数据关联，不法分子和别有用心的人可通过多元数据关联分析导致个人隐私信息泄露。怎样有效保护个人隐私是大数据安全面临的一个重要问题。

- 跨境数据流动

当前，数据的流动很重要，数据的跨境流动是大数据的一个特殊属性。在法律制度、数据服务外包、打击网络犯罪方面，保护跨境数据的安全是很重要的。

④ 传统安全措施难以适配

大数据海量、多源、异构、动态的特征导致大数据系统存储结构复杂，需要提供开放性、分布式计算和高效精准的服务，这些特殊需求传统安全措施解决不了。

- 数据安全保护难度加大

大数据的应用环境不同，是开放的网络；系统的部署方式不同，是分布式的；数据的复杂度和用户访问方式也不同，这些都是面临的新问题。在数据应用的平台上数据安全保护的难度加大。

- 个人信息泄露风险加重

大数据关联分析易挖掘出更多的个人信息，易发生数据滥用、内部偷窃、网络攻击等安全事件，应从数据中心安全方面来考虑网络管理工作：攻击保护、固件管理、备份、数据安全、性能优化等，防止异常入侵者对数据中心发起恶意攻击。

大数据时代有的数据是假的，有的数据是真的，一定要去伪存真，从里面找到真正需要的数据。

- 数据所有者权益难以保障

现在大数据和“互联网+”经常会产生数据交换，在数据交换过程中怎样保证数据所有者的权益和数据所有者的隐私，是我们现在面临的挑战。在数据应用里所有者权益的保证，是数据治理中很关键的问题。

(3) 大数据应用面临的挑战

① 大数据网络管理系统是综合的网络管理系统，应能够支持智能化的操作模式、灵活匹配复杂的业务需要和资源监控，实现全方位立体化监控。

② 大数据计算速度快，采用非关系型数据库技术(NoSQL)和数据库集群技术(MPP NewSQL)快速处理非结构化以及半结构化的数据，以获取高价值信息，这与传统数据处理技术有着本质的区别。

③ 大数据技术要存储巨量数据，可用结构化数据存储、半结构化数据存储、非结构化数据存储。

④ 大数据项目所获取的数据往往携带大量的隐私信息，这些信息既有个人信息，也有政府机构、组织、公司的信息。当前业界各方隐私保护的意识都在增强，甚至很多国家把隐私保护提高到法律的高度加以规范。在这样的大背景下，大数据项目必须对数据安全和隐私保护给予足够重视，并通过技术手段和管理措施两方面加以保障。

大数据已渗透到各行各业，对经济发展、社会治理、国家管理、人民生活都产生着重大影响。如何有效解决大数据技术在发展和应用中存在的问题，使其发挥更大的价值，成为网络管理面临的关键问题。

大型数据中心的管理维护是通过托管、外包方式向企业提供大型主机的管理维护，以达到专业化管理和降低运行成本的目的。

⑤ 大数据领域涌现出大量新的技术。

- 大数据接入：包括实时数据接入、文件数据接入、消息记录数据接入、文字数据接入、图片数据接入、视频数据接入。
- 大数据存储：包括结构化数据存储、半结构化数据存储、非结构化数据存储。
- 大数据分析与挖掘：包括离线分析、准实时分析、实时分析、图片识别、语音识别、机器学习。
- 大数据共享：包括数据接入、数据清洗、转换、脱敏、脱密、数据资产管理、数据导出。

3. 移动通信网络的基础知识

2019 年 6 月，工信部正式向中国电信、中国移动、中国联通、中国广电发放 5G(第五代移动通信网络)商用牌照，中国正式进入 5G 商用元年。

(1) 5G 发展的动力

5G 发展的动力来自于人们对移动数据日益增长的需求。当前移动数据的需求呈爆炸式增长，原有移动通信网络(4G，第四代移动通信网络)难以满足未来需求。随着移动互联网的发展，越来越多的设备接入到移动网络中，新的服务和应用层出不穷。移动数据流量的暴涨将给网络带来严峻的挑战，第四代移动通信网络的容量难以支持千倍流量的增长。要提升网络容量，必须高效利用网络资源，针对业务和用户的个性化应用进行智能优化。为了解决上述问题，满足日益增长的移动流量需求，需要发展新一代 5G 移动通信网络。

(2) 5G 基本概念

5G 是数字蜂窝网络，在这种网络中：

① 供应商覆盖的服务区域被划分为许多称为蜂窝的小地理区域。

② 表示声音和图像的模拟信号在手机中被数字化，由模数转换器转换，以比特流传输。

③ 蜂窝中的所有无线设备通过无线电波与蜂窝中的本地天线和低功率自动收发器(发射机和接收机)进行通信。

④ 收发器从公共频率池分配频道，这些频道在地理上分离的蜂窝中可以重复使用。

⑤ 本地天线通过高带宽光纤或无线回程连接与电话网络和互联网连接。与现有的手机一样，当用户从一个蜂窝穿越到另一个蜂窝时，他们的移动设备将自动切换到新蜂窝中的天线。

(3) 5G 主要优势

① 数据传输速率远远高于以前的蜂窝网络，峰值速率达到 Gb/s 的标准，最高可达 10Gb/s，比当前的有线互联网要快，比先前的 4G LTE蜂窝网络快 100 倍，能够满足高清视频、虚拟现实等大数据量传输。

② 较低的网络延迟(更快的响应时间)，空中接口时延水平在 1ms(毫秒)左右，而 4G 为 30~70ms。由于数据传输更快，能够满足自动驾驶、远程医疗等实时应用。

③ 5G 网络不仅仅为手机提供服务，而且还将成为一般性的家庭和办公网络提供商，极大地改善人们的日常生活和工作方式，流量密度和连接数密度大幅度提高。超大网络容量，提供千亿设备的连接能力，满足物联网通信。

④ 系统协同化、智能化水平提升，可进行多用户、多点、多天线，协同组网，以及网络间灵活地自动调整。

(4) 5G 的关键技术

① 超密集异构网络

5G 网络正朝着网络多元化、宽带化、综合化、智能化的方向发展，超密集异构网络减小了小区半径，增加了低功率节点数量。密集部署的网络拉近了终端与节点间的距离，使得网络的功率和频谱效率大幅度提高，同时也扩大了网络覆盖范围，扩展了系统容量，并且增强了业务在不同接入技术和各覆盖层次间的灵活性。

② 自组织网络

传统移动通信网络中，主要依靠人工方式完成网络部署及运维，既耗费大量人力资源又增加了运行成本，而且网络优化也不理想。在 5G 网络中自组织网络具有以下功能：

- 网络部署阶段的自规划和自配合。
- 网络维护阶段的自优化和自愈合。

③ 内容分发网络

在 5G 中具有面向大规模用户的音频、视频、图像等业务，5G 分发业务内容降低了用户获取信息的时延。

④ D2D 通信

D2D(device to device，设备到设备)通信是一种基于蜂窝系统的近距离数据直接传输技术，能够提升系统性能、增强用户体验、减轻基站压力、提高频谱利用率。D2D 会话的数据直接在终端之间进行传输，不需要通过基站转发；而相关的控制信令，如会话的建立、维持、无线资源分配以及计费、鉴权、识别、移动性管理等仍由蜂窝网络负责。

⑤ M2M 通信

M2M(machine to machine，机器到机器)作为物联网最常见的应用形式，在智能电网、安全监测、城市信息化、环境监测等领域实现了商业化应用。M2M 主要是指机器与机器、人与机器以及移动网络与机器之间的通信，它涵盖了所有实现人、机器、系统之间通信的技术；从狭义上说，M2M 仅仅指机器与机器之间的通信。

⑥ 信息中心网络

在5G 中信息中心网络是实时媒体流、网页服务、多媒体通信等片段信息的总集合。信息中心网络的功能主要是信息的分发、查找和传递，不再是维护目标主机的可连通性。信息中心网络的信息传递流程是一种基于发布订阅方式的流程。

(5) 5G 的应用领域

5G 网络具有高速率和稳定性，其应用领域主要有：物联网、车联网、自动驾驶、智慧城市、智慧教育、无人机网络、医疗诊断和外科手术、智能电网等。

4. 智能移动支付基础知识

移动支付是指使用普通手机完成支付或者确认支付，而不是用现金、银行卡或者支票支付。移动支付将互联网、终端设备、金融机构有效地联合起来，形成了一种新型的支付体系。移动支付不仅能够进行货币支付，还可以缴纳电话费、燃气费、水电费等生活费用。移动支付把人们带

进无现金时代，它不仅是一种趋势，更将成为一种方式。

(1) 移动支付的方式

移动支付的方式有短信支付、扫码支付、指纹支付、声波支付等。

(2) 移动支付的特征

移动支付属于电子支付方式的一种，因而具有电子支付的特征，但因其与移动通信技术、无线射频技术、互联网技术相互融合，故又具有自己的特征。

① 时空限制小

移动支付打破了传统支付时空的限制，使用户可以随时随地进行支付活动。移动支付以手机支付为主，用户可以不受时间和空间的限制随时随地进行支付活动。

② 及时性

不受时间和地点的限制，信息获取更为及时，用户可随时对账户进行查询、转账或进行购物消费。

③ 定制化

基于先进的移动通信技术和简易的手机操作界面，用户可定制自己的消费方，付费方式可通过多种途径实现，如直接转入银行、用户电话账单或者实时在专用预付账户上借记，交易更加简单方便。

④ 集成性

以手机为载体，通过与终端读写器近距离识别进行的信息交互，运营商可以将移动通信卡、公交卡、地铁卡、银行卡等各类信息整合到以手机为平台的载体中进行集成管理，搭建与之配套的网络体系，从而为用户提供十分方便的支付以及身份认证渠道。

⑤ 方便管理

用户可以随时随地通过手机进行各种支付活动，并对个人账户进行查询、转账、缴费、充值等功能的管理，也可随时了解自己的消费信息。这对用户的生活提供了极大的便利，也更方便用户对个人账户的管理。

⑥ 综合度较高

移动支付有较高的综合度，其为用户提供了多种不同类型服务。例如：用户可以通过手机缴纳家里的水费、电费、燃气费；可以通过手机进行个人账户管理；还可以通过手机进行网上购物等各类支付活动。这体现了移动支付有较高的综合度。

(3) 移动支付的优点

对于消费者来说，可以在实体店直接扫描二维码，轻松付款；无需携带现金，无需找零，无需刷卡签字，很大程度上节约了时间，并且可以避免假币问题带来的麻烦。加之这些第三方支付平台经常会在网上做一些“满减”“抢红包”的活动，不仅给予我们优惠，更给我们带来了很多乐趣；移动支付可以轻松实现生活缴费、购买车票、手机充值等，真正做到足不出户也能办理各种业务。

(4) 移动支付存在的问题

① 移动支付在应用过程中存在的隐患

由于移动支付发展较快，安全保障体系还未健全，支付交易的收付款双方都存在一定的风险，移动支付更易被不法分子利用。在应用过程中，如果收款二维码被恶意掉包，付款二维码被恶意读取，就会造成他人财产损失。不良商家盗刷、重复刷，也会导致资金损失。

② 手机被盗风险

由于移动支付是在手机上完成的，手机丢失或被窃，会对手机上的资金造成风险。

③ 手机本身未加密

手机本身未采用加密等安全措施，不法分子通过钓鱼网站或木马程序窃取用户信息，并对移动支付功能进行非法复制，从而造成用户重要信息的泄露。

④ 手机电池续航能力

由于手机的电池续航能力有限，所以如果一个消费者手机突然没电，就没办法进行消费。

⑤ 移动支付的技术风险

在移动支付的发展过程中，有些支付创新为了实现用户的友好性及支付交易的快捷性，而忽略了交易验证的严谨性，特别是支付交易中的身份确认往往存在支付风险。是否严格执行有关规则，是否对每一个过程都进行严格的测试和反复验证，都事关重要。消费者应每扫码一次均与商家确认，以降低风险。

⑥ 网络安全问题

网络安全问题尚未妥善解决，易受到木马、黑客的攻击，手机支付类病毒、手机系统漏洞等均给手机用户支付安全造成威胁。

⑦ 资金寄存风险

移动支付中第三方支付平台是非金融机构，与银行、证券、保险等金融机构相比资金寄存能力存在差距，资金寄存具有一定的风险。如果有一家平台经营不善，会导致用户的资金不能保全，资金寄存风险升高。

1.3　常用的网络故障测试命令

常用的网络故障测试命令有 ipconfig、ping、tracert、netstat 和 nslookup 等。下面简要说明它们的基本用法。

1. ipconfig 命令

使用 ipconfig 命令可以查看 IP 配置，或配合使用/all 参数查看网络配置情况。ipconfig 命令采用 Windows 窗口的形式来显示 IP 协议的具体配置信息。如果 ipconfig 命令后面不跟任何参数直接运行，程序将会在窗口中显示网络适配器的物理地址、主机的 IP 地址、子网掩码以及默认网关等。还可以通过此程序查看主机的相关信息，如主机名、DNS 服务器、节点类型等。其中网络适配器的物理地址在检测网络错误时非常有用。在命令提示符下输入 ipconfig/？可获得 ipconfig 的使用帮助，输入 ipconfig/all 可获得 IP 配置的所有属性。

ipconfig 命令语法格式：

```
    ipconfig [- " "] [ ? ] [all] [release] [renew] [flushdns] [displaydns] [registerdns]
[showclassid] setclassid]
```

命令参数介绍：

- -" "：不带任何参数选项，则为每个已经配置的接口显示 IP 地址、子网掩码和默认网关值；
- ?：进行参数查询；
- all：显示本机 TCP/IP 配置的详细信息；
- release：DHCP 客户端手工释放 IP 地址；
- renew：DHCP 客户端向服务器进行手工刷新请求；
- flushdns：清除本地 DNS 缓存内容；
- displaydns：显示本地 DNS 内容；

- registerdns：DNS 客户端向服务器进行手工注册；
- showclassid：显示网络适配器的 DHCP 类别信息；
- setclassid：设置网络适配器的 DHCP 类别。

在“开始”菜单中单击“程序”→“运行”命令，输入 CMD 进入 DOS 命令行窗口。在 DOS 命令行窗口中输入 ipconfig /all，会显示出如图 1-1 所示画面。

```
C:\Documents and Settings\Administrator>ipconfig/all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : zhangjj
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : Yes
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter internet连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : CNC Enternet P.P.P.o.E
        Physical Address. . . . . . . . . : 44-45-53-54-77-77
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 221.219.16.50
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 221.219.16.50
        DHCP Server . . . . . . . . . . . : 1.1.1.1
        DNS Servers . . . . . . . . . . . : 202.106.46.151
                                            202.106.0.20
        Lease Obtained. . . . . . . . . . : 2005年12月5日 9:47:59
        Lease Expires . . . . . . . . . . : 2038年1月19日 11:14:07
```

图 1-1　输入 ipconfig/all 命令弹出的画面

在图 1-1 中显示出了本机 TCP/IP 配置情况。如果显示出的 IP 地址不在网络的网段中，本机则无法与其他计算机通信；如果网关、DNS 配置有误，则本机不能访问外网计算机，也不能上网。

可以使用/release 和/renew 参数重新从 DHCP 服务器上获取 IP 地址。

2. ping 命令

ping 命令主要是用来检查路由是否能够到达某站点。由于该命令的包长较小，所以在网上传递的速度非常快，可以快速检测要连接的站点是否可达。如果执行 ping 不成功，则可以预测故障出现在以下几个方面：

- 网线未连通；
- 网络适配器配置不正确；
- IP 地址不可用等。

如果执行 ping 命令成功而网络仍无法使用，问题很可能出在网络系统的软件配置方面。ping 成功只能保证当前主机与目的主机间存在一条连通的物理路径。

在 DOS 命令窗口中输入 ping/?，可以看到 ping 的各个参数如下：

```
C:\Documents and Settings\Administrator>ping/?
Usage: ping  [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
             [-r count] [-s count] [[-j host-list] | [-k host-list]]
             [-w timeout] destination-list
Options:
     -t                  Ping the specified host until stopped
                         To see statistics and continue - type Control-Br
                         To stop - type Control-C
     -a                  Resolve addresses to hostnames
     -n count            Number of echo requests to send
     -l size             Send buffer size
```

```
        -f                  Set Don't Fragment flag in packet
        -i TTL              Time To Live
        -v TOS              Type Of Service
        -r count            Record route for count hops
        -s count            Timestamp for count hops
        -j host-list        Loose source route along host-list
        -k host-list        Strict source route along host-list
        -w timeout          Timeout in milliseconds to wait for each reply
```

1) ping 命令参数介绍

- -t

ping 指定的主机，直到中断。

- -a

以 IP 地址格式来显示目标主机的网络地址，将地址解析为计算机名。

```
C:\Documents and Settings\Administrator>ping -a 159.254.188.86
Pinging lily [159.254.188.86] with 32 bytes of data:
```

通过运行 ping -a 159.254.188.86 可以知道 IP 为 159.254.188.86 的计算机名是 lily。

- -n count

发送 count 指定的 echo 数据包数，默认值为 4。

- -l size

发送包含有size 指定的数据量的 echo 数据包。默认值为 32 字节，最大值是 65 527 字节。

- -f

在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。

- -i TTL

将“生存时间”字段设置为 TTL 指定的值。

- -v TOS

将“服务类型”字段设置为 TOS 指定的值。

- -r count

在“记录路由”字段中记录传出和返回数据包的路由。count 可以指定最少 1 台，最多 9 台计算机。

- -s count

记录 count 所指定的跃点数的时间戳。

- -j host-list

利用 host-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔(路由稀疏源)，IP 允许的最大数量为 9。

- -k host-list

利用 host-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔(路由严格源)，IP 允许的最大数量为 9。

- -w timeout

指定超时间隔，单位为毫秒。

2) 使用 ping 命令测试故障的步骤

现在有一台计算机不能访问 Internet 上的 Web 服务器，可以使用 ping 命令找出故障的位置。操作步骤如下：

- ping 159.0.0.1

如果 ping 不通，则说明本机 TCP/IP 协议没有安装好。

- ping 本机的 IP 地址

如果 ping 不通，则说明网卡没有装好，或网卡驱动有问题。

- ping 本网段的其他设备 IP 地址

如果 ping 不通，则说明连接本机的线路有问题，或者交换机的端口有问题，也有可能是交换机本身出了问题。

- ping 本网段的网关

如果 ping 不通，则无法上网，因为没有设备能把数据包转发出去。原因可能是路由器没有配置好或代理服务器出了问题。

- ping DNS 服务器

如果 ping 不通，则说明 DNS 服务器出了问题，或本机的 DNS 服务器设置不正确。

3. tracert 命令

tracert 命令用来检验数据包是通过什么路径到达目的地的。通过执行 tracert 命令，可以清楚地看到数据传送的路径，判定数据包到达目的主机所经过的路径，显示数据包经过的中继节点清单和到达时间。当 ping 一个较远的主机出现错误时，用 tracert 命令可以方便地查出数据包是在哪里出错的。如果信息包连一个路由器也不能穿越，则有可能是计算机的网关设置错了。那么，可以用 ipconfig 命令来查看。

tracert 命令语法格式：

```
tracert [-d] [-h maximum_hops] [-j host_list] [-w timeout]
```

其中主要参数有：

- -d　不解析目标主机的名称；
- -h maximum_hops　指定搜索到目标地址的最大跳跃数；
- -j host_list　按照主机列表中的地址释放源路由；
- -w timeout　指定超时时间间隔，程序默认的时间单位是毫秒。

4. winipcfg 命令

winipcfg 命令的功能与 ipconfig 基本相同，只是 winipcfg 在操作上更加方便，同时能够以 Windows 的图形界面方式显示。当需要查看任何一台机器上 TCP/IP 协议的配置情况时，选择“开始”→“运行”，在出现的对话框中输入 winipcfg，即可出现测试结果。

winipcfg 命令语法格式：

```
winipcfg [/?] [/all]…
```

其中主要参数有：

- /?　显示该命令的帮助信息；
- /all　显示所有的有关 IP 地址的配置信息；
- /batch [file]　将命令结果写入指定文件；
- /renew_ all　重试所有网络适配器；
- /release_all　释放所有网络适配器；
- /renew N　复位网络适配器 N；
- /release N　释放网络适配器 N。

5. netstat 命令

利用 netstat 命令可以显示有关统计信息和当前 TCP/IP 网络连接的情况，用户或网络管理人员可以得到非常详尽的统计结果。当网络中没有安装特殊的网管软件，但要详细地了解网络的整个使用状况时，netstat 命令是非常有用的。

netstat 命令的语法格式：

```
netstat [-e] [-s] [-n] [-a]
```

其中主要参数有：

- -a　显示所有与该主机建立连接的端口信息。
- -n　以数字格式显示地址和端口信息。
- -e　显示以太网的统计信息，该参数一般与 s 参数共同使用。显示的内容中，Discards 表示不能处理被废弃的信息包数，Errors 表示坏掉的信息包数。这些数值较大时，很可能是集线器、电缆和网卡等硬件发生了故障。另外，网络太拥挤也可能导致这些数值增大。
- -s　显示每个协议的统计情况。如果想要统计当前局域网中的详细信息，可通过输入 netstat-e-s 查看。

6. nslookup 命令

nslookup 命令一般是用来确认 DNS 服务器动作的。nslookup 有多个选择功能，在命令行输入“nslookup <主机名>”并执行，即可显示出目标服务器的主机名和对应的 IP 地址，称为正向解析。若失败了，可能是执行 nslookup 命令的计算机的 DNS 设置错了，也有可能是所查询的 DNS 服务器停止或工作异常。还有一种情况，虽然返回了应答，但在和该服务器通信时就失败。这多数是目标服务器停止工作，但也有可能是 DNS 服务器保存了错误的信息。在 DNS 服务器出现问题时，有时可能只能进行正向解析，无法进行逆向解析。此时，只需执行 nslookup 命令，看是否输出目标主机名即可。

nslookup 命令语法格式：

```
nslookup [-SubCommand ...] [{ComputerToFind| [-Server]}]
```

使用方法：

在 DOS 命令行下输入 nslookup，按 Enter 键，此时标识符变为“>”，然后输入指定网站的域名，再按 Enter 键就可以显示该域名相对应的 IP 地址。

7. arp 命令

arp 命令可以显示和设置 Internet 到以太网的地址转换表内容。这个表一般由 ARP 维护。当仅使用一个主机名作为参数时，arp 命令显示这个主机的当前 ARP 表条目内容。如果这个主机不在当前 ARP 表中，那么 arp 就会显示一条说明信息。

arp 命令语法格式：

```
arp [-a] [-d host]  [-s host address] [-f file]
```

其中主要参数有：

- -a　列出当前 ARP 表中的所有条目。
- -d host　从 ARP 表中删除某个主机的对应条目。
- -s host address　使用以太网地址在 ARP 表中为指定的[temp][pub][trail]主机创建一个条目。如果包含关键字[temp]，创建的条目就是临时的；否则这个条目就是永久的。使用[pub]关键字表示这个 ARP 条目将被公布。使用[trail]关键字表示将使用报尾封装。
- -f file　读一个给定名字的文件，根据文件中的主机名创建 ARP 表的条目。

1.4 网络故障管理系统

使用 ping 的方法只能针对小型网络，在一些大型网络中一般使用网络故障管理软件。一个网络的故障管理系统不但能反映网络平常运行时的故障情况，更应该能在发生重大网络故障时，快速准确地报告、定位和排除故障。

网络故障管理系统包括：

- Navis NFM 故障管理系统；
- Netcool 故障管理系统。

Navis NFM(Network Fault Management)网络故障管理系统是朗讯科技网络运行系列软件中最著名的产品，其功能强大，能够提供实时故障监测和相关处理，快速定位故障，关联故障，并可提供多厂家、多技术和多业务区的集中管理。另外，“现成的方案”可以快速进行工程实施，并提供本地化的客户和技术支持。

Navis NFM 核心功能包括：

- 告警信息采集、浏览、过滤、分类等；
- 支持信息压缩，可根据信息发生的次数、数值、时间和分组进行压缩；
- 告警门限设置和级别升级(Critical、Major、Minor、Other、Cleared)；
- 自动的告警通知和告警处理功能(寻呼、发送电子邮件、生成工单、网元重新启动等)；
- 多种颜色的故障信息显示和图形化的网络地图显示；
- 支持开放的接口和 API(ASCII、SNMP v1～v3、CORBA、X.25、TL1)；
- 远端登录到网元和网元管理系统。

NFM 可以根据用户的级别，实现分权和分级管理。系统管理员可以为不同的用户设置不同的权限，只定义该用户关心的网元的故障信息的浏览、查找、操作和远程登录等功能。每个用户用自己的账户登录系统后, 只能看到权限之内的信息，以及执行被允许的各种操作。同时，NFM 还备有用户使用记录，从而实现对人员使用情况的管理，加强对整个系统的安全保障。

NFM 提供强大的告警抑制功能，可以对非告警类报告提供过滤；根据各种门限进行告警抑制；告警恢复后，NFM 可以自动清除原告警，并将其转入已清除告警中；对告警进行域内、域间的相关性处理等，从而大幅度地减少告警的数量，并有效减少分析故障根源所花费的时间。

用户还可以将客户信息和服务相关数据集成到 Navis NFM 数据库，NFM 可实时地显示与故障相关的客户和服务数据信息，产生针对特定客户和服务的故障报告，并在故障影响客户之前对其进行评估。

1.5 网络故障诊断

为了更好地发挥计算机网络的作用，更好地利用已有的网络资源，就必须做好网络故障修复工作。一般的网络故障修复对网络管理员来说相当简单，但是专业的、深层次的网络故障只有经过专业训练，并借助专业软件和工具才能诊断，并最终排除。

网络故障诊断是从故障现象出发，以网络诊断工具为手段获取诊断信息，确定网络故障点，查找问题的根源，排除故障，恢复网络的正常运行。

网络故障通常有以下几种可能：

- 物理层中的物理设备相互连接失败或者硬件和线路本身问题；
- 数据链路层的网络设备的接口配置问题；
- 网络层网络协议配置或操作错误；
- 传输层的设备性能或通信拥塞问题；
- 网络应用程序错误。

诊断网络故障的过程应该沿着 OSI 七层模型从物理层开始向上进行。首先检查物理层，然后检查数据链路层，以此类推，确定故障点。

1.5.1　故障诊断步骤

故障诊断应该实现三方面的目的：

- 确定网络的故障点，排除故障，恢复网络的正常运行；
- 发现网络中故障点的原因，改善优化网络的性能；
- 观察网络的运行状况，及时预测网络通信质量。

故障诊断的步骤如下：

(1) 确定故障的具体现象，分析造成这种故障现象的原因。例如，主机不响应客户请求服务。可能的故障原因是主机配置问题、接口卡故障或路由器配置命令丢失等。

(2) 收集需要的用于帮助分析故障原因的信息。从网络管理系统、协议分析跟踪、路由器诊断命令的输出报告或软件说明书中收集有用的信息。

(3) 根据收集到的信息分析可能的故障原因，排除其他故障原因。例如，根据某些资料可以排除硬件故障，把注意力放在软件原因上。

(4) 根据最后的可能故障原因，建立一个诊断计划。开始仅用一个最可能的故障原因进行诊断活动，这样容易恢复到故障的原始状态。如果一次同时考虑多个故障原因，返回故障原始状态就困难多了。

(5) 执行诊断计划，认真做好每一步的测试和观察，每改变一个参数都要确认其结果。分析结果，确定问题是否解决，如果没有解决，继续下去，直到故障现象消失。

1.5.2　故障排除过程

在动手排除故障之前，在记事本上将故障现象认真仔细地记录下来，观察和记录时一定要注意细节，因为有时正是一些特别小的细节使整个问题变得明朗化。

1. 识别收集故障现象

作为管理员，在排除故障之前，必须确切地知道网络上到底出了什么问题。知道出了什么问题并能够及时识别，是成功排除故障最重要的步骤。为了与故障现象进行对比，必须知道系统在正常情况下是怎样工作的，反之，则不易对问题和故障进行定位。

识别收集故障现象时，应该向操作者询问以下几个问题：

- 当被记录的故障现象发生时，正在运行什么进程(即操作者正在对计算机进行什么操作)？
- 这个进程以前运行过吗？
- 以前这个进程的运行是否成功？
- 这个进程最后一次成功运行是什么时候？从那时起哪些发生了改变？

带着这些疑问了解并分析问题才能对症下药来排除故障。

2. 对故障现象详细描述

当处理由操作员报告的问题时，对故障现象的详细描述显得尤为重要。如果仅凭他们的一面之词，有时很难下结论，这时就需要网络管理员亲自操作出错的程序，并注意出错信息。例如，在使用 Web 浏览时，无论输入哪个网址都返回“该页无法显示”之类的信息。使用 ping 命令时，无论 ping 哪个 IP 地址都显示超时连接信息等。诸如此类的出错信息会为缩小问题范围提供许多有价值的信息。因此在排除故障前，可按以下步骤执行：

(1) 收集有关故障现象的信息。

(2) 对问题和故障现象进行详细的描述。

(3) 注意细节。

(4) 把所有的问题都记录下来。

(5) 不要匆忙下结论。

3. 对计算机设备本身的运行状况进行检查

作为网络管理员，应对计算机设备本身的运行状况进行检查。

(1) 检查操作系统的运行、网络协议、网络地址的设置、网络接口设备驱动程序和设备收发网络数据包的情况。

(2) 检查网络接口设备与网络接入设备的连接情况。

(3) 检查服务器到网络接口设备的连接状况。

(4) 检查网络连接设备运行状况。

(5) 检查网络主干设备流量状况。

(6) 检查端口数据流量的大小，检查重发包、错包和丢包的比例，检查设备上数据包发生碰撞的比例，检查流量情况的日志文件内容，注意拥塞控制的报警阈值设置。

4. 列举可能导致错误的原因

作为网络管理员，则应考虑导致无法查看信息的原因有哪些，如网卡硬件故障、网络连接故障、网络设备(Hub)故障、TCP/IP 协议设置不当等。这里需要注意的是：不要急于下结论，可以根据出错的可能性把这些原因按优先级别进行排序，一个个先后排除。

5. 缩小搜索范围

对所有列出的可能导致错误的原因逐一进行测试，而且不要根据一次测试就断定某一区域的网络运行正常或不正常。另外，也不要在自己认为已经确定了的第一个错误上停下来，应直到测试完为止。

除了测试之外，网络管理员还要注意，千万不要忘记去查看网卡、Hub、Modem、路由器面板上的 LED 指示灯，通常情况下：

- 绿灯表示连接正常；
- 红灯表示连接故障；
- 不亮表示无连接或线路不通；
- 长亮表示广播风暴；
- 指示灯有规律地闪烁才是网络正常运行的标志。

同时不要忘记记录所有观察、测试的手段和结果。

6. 隔离错误

经过一番检查后，基本知道了故障的部位。对于计算机的错误，可以开始检查：

- 网卡是否安装好；
- TCP/IP 协议是否安装并设置正确；
- Web 浏览器的连接设置是否得当等一切与已知故障现象有关的内容。

处理完问题后，作为网络管理员，还必须搞清楚故障是如何发生的，是什么原因导致了故障的发生，以后如何避免类似故障的发生，并拟定相应的对策，采取必要的措施，制定严格的规章制度。

1.5.3　故障原因

虽然故障原因多种多样，但总的来讲不外乎硬件问题和软件问题。说得再确切一些，这些问题就是网络连通性问题、配置文件和选项问题和网络协议问题。

1. 网络连通性

网络连通性是故障发生后首先应当考虑的原因。连通性的问题通常涉及网卡、跳线、信息插座、网线、Hub、交换机、Modem 等设备和通信介质。其中，任何一个设备的损坏，都会导致网络连接的中断。连通性通常可以采用软件和硬件工具进行测试验证。如某一台计算机不能浏览网页时，网络管理员应当考虑以下情况：

- 网络连通吗？
- 看得到网上邻居吗？
- 可以收发电子邮件吗？
- ping 得到网络内的其他计算机吗？

只要其中一项回答为“是”，就可以断定本机到 Hub 的连通性没有问题。当然，即使都回答“否”，也不能表明连通性肯定有问题，也可能是其他问题，如计算机的网络协议的配置出现问题也会导致上述现象的发生。当然，还要查看网卡和 Hub、交换机接口上的指示灯是否正常。

如果排除了由于计算机网络协议配置不当而导致故障的可能，接下来要做的事情就复杂了。查看网卡、Hub 和交换机的指示灯是否正常，测试网线是否畅通。

2. 配置文件和选项

服务器、计算机都有配置选项，配置文件和配置选项设置不当，同样会导致网络故障。如服务器权限的设置不当，会导致资源无法共享；计算机网卡配置不当，会导致无法连接。当网络内所有的服务都无法实现时，应当检查 Hub、交换机。

3. 使用诊断工具

ping 无疑是网络中使用最频繁的小工具，它主要用于确定网络的连通性问题。ping 程序使用 ICMP(网际消息控制协议)简单地发送一个网络数据包并请求应答，接收到请求的目的主机再次使用 ICMP 发回相同的数据，于是 ping 便可对每个包的发送和接收时间进行报告，并报告无影响包的百分比。这在确定网络是否正确连接，以及网络连接的状况(包丢失率)时十分有用。ping 是 Windows 操作系统集成的 TCP/IP 应用程序之一，可以在“开始”→“运行”中直接执行。

- ping 主机名；
- ping IP 地址；
- ping 本地计算机名(即执行操作的计算机)。
  - ◇ 如 ping lily 或 ping 本地 IP 地址；
  - ◇ 如 ping 172.0.0.1(任何一台计算机都会将 172.0.0.1 视为自己的 IP 地址)。

使用 ping 命令后常见的出错信息通常分为以下 4 种。

(1) Unknown host(不知名主机)

这种出错信息的意思是，该远程主机的名字不能被命名服务器转换成 IP 地址。故障原因可能是命名服务器有故障，或者其名字不正确，或者网络管理员的系统与远程主机之间的通信线路故障。这种情况下屏幕将会提示：

```
C:\windows>ping www.163.net
Unknown host www.163.net
C:\windows>
```

(2) Network unreachable(网络不能到达)

这是本地系统没有到达远程系统的路由，可检查路由器的配置，如果没有路由，可添加。

(3) No answer(无响应)

即远程系统没有响应。这种故障说明本地系统有一条到达中心主机的路由，但却接收不到它发给该中心主机的任何分组报文。故障原因可能是中心主机没有工作，本地或中心主机网络配置不正确，本地或中心的路由器没有工作，通信线路有故障或中心主机存在路由选择问题。

(4) Timed out(超时)

即台站与中心的连接超时，数据包全丢。故障原因可能是到路由器的连接问题或路由器不能通过，也可能是中心主机已经关机或死机。此时，屏幕提示：

```
C:\windows>ping 10.11.1.1
Ping 10.11.1.1with 32 bytes of data:
Request timed out.
Request timed out
Request timed out
Request timed out
Ping statistics for 10.11.1.1:
Packets: sent=4,received=0,lost=4(100% lost),
Approximate round trip in milli-seconds:
Minimum=0ms,Maximum=0ms,Average=0ms
C:\windows
```

4. 使用硬件工具网络测试仪

使用网络测试仪测试网线。

1.5.4 网络故障的内容和故障排除的步骤

网络故障的内容如图 1-2 所示。

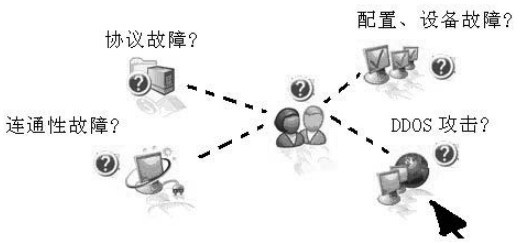

图 1-2 网络故障的内容

网络故障的排除是计算机专业人员面临的最困难的任务之一。问题往往出现在工作过程中，或者在工作任务有期限要求的时候，要快速修复出现的问题，困难就会很大。

网络发生故障后，首先要诊断是协议故障，连通性故障，配置、设备故障，还是 DDOS 攻击。找到问题的来源，然后进行故障排除。

网络故障排除的过程大致可分为 5 个步骤。

(1) 定义问题

这一步非常重要，却经常被人们忽视。如果对整个问题没有进行全面的了解，就有可能将大量的时间花在对症状的研究上，而不是对问题的原因进行探讨。这个阶段所需的工具仅仅是纸、笔和良好的接受能力。

听取客户或者网络用户的意见是最好的信息来源。记住，尽管您可能知道网络是如何工作的，并且可以发现故障的技术原因，但那些每天都使用网络的人在问题出现之前或者之后都在网络上工作，并且可能会回想起导致故障的事件。通过从他们的意见中提取信息，可以从纷繁复杂的各种可能的故障原因中理出头绪。列出故障发生的时间顺序将有助于了解问题。您可以建立一张表格系统地向用户提出以下问题(具体问题由具体情况而定)：

- 您是在何时注意到问题或者错误的？
- 计算机最近是否进行了移动？
- 最近是否在软件或者硬件上有所更改？
- 工作是否发生了变化？是否有某些东西砸在计算机上面？咖啡或者苏打水是否曾经洒在键盘上？
- 问题发生的确切时间是什么时候？是在启动的过程中还是午餐后？仅仅在星期一的商务活动中还是在发送电子邮件之后？
- 您可以使问题或者错误再现吗？如果可以，怎样产生错误？
- 问题或者错误的症状怎样？
- 描述计算机的任何变化(如噪声、屏幕更改和磁盘工作情况等)。

用户(甚至那些没有技术背景的人)在收集信息的过程中都非常有帮助，只要您有效地对他们提出一些问题。例如，可以问他们当网络出现何种表现时让他们感觉到出现了问题。用户的观察可能会构成解决网络问题的基础。这些问题包括：

- “网络真慢”；
- “我不能连接到服务器”；
- “我曾经连到服务器，但是后来又掉线了”；
- “我的一个应用程序不能运行”；
- “我不能打印”。

继续提问，就可以逐步缩小范围。

(2) 找出原因

这一步是隔离问题。首先排除明显的问题，然后再排除复杂的、隐晦的问题，目标是将重点缩小在一个或者两个分类之内。

要确保您亲眼见到故障。如果可能的话，让某些人演示发生错误的情况。如果是操作人员引起的问题，那么很重要的一点是观察问题是如何发生的，以及问题造成的后果。

最难以隔离的问题是间歇性发生的问题，并且，它们似乎从来不在您在场的时候发生。解决这类问题的唯一办法是重新创建产生问题的环境。有时，使用排除法是最好的方式，这个过程需要时间和耐心，用户也应该对问题出现之前和期间的所作所为进行记录。同时告知用户在计算机出现问题的时候不要对它进行任何操作，并且及时通知您，这种方式可以保证“现场”不被破坏。

尽管收集的信息为隔离问题提供了基础，但管理员也应该参考记录的基准信息，并与当前的网络操作进行比较。在与创建基准条件相同的环境下重新进行测试，然后比较两个结果，两者之间的任何变化都可能指示出问题的原因。

信息的收集包括对网络进行扫描，以及寻找问题的明显原因。快速扫描包括对网络的历史记录进行查询，以确定问题以前是否发生过，如果发生过，则查找是否存在记录在案的解决办法。

(3) 计划修复

在缩小研究范围之后，就可以开始下一过程：排除。

根据目前已经掌握的情况制订隔离问题的方法。首先尝试使用最显而易见的或者最简单的方

法来排除，然后再采用更复杂和麻烦的方法。必须对过程中的每个步骤，以及每个操作和该操作的结果都进行记录。

在制订好计划后，必须严格遵循计划的步骤。如果第一个计划没有成功(非常有可能)，则应在先前计划的基础上重新制订一个计划。一定要对前一个计划中所做的任何假设进行参考、重新检查和重新评估。

确定问题后，修复缺陷，或者替换有缺陷的部件。如果问题与软件有关，则一定要对前后的变化进行记录。

(4) 证实结果

在修复之后，如果没有证实结果如何，就不能说已经成功完成了任务。应该确保问题不复存在，请用户对问题的解决进行测试和验证。同时应确保修复没有带来新的问题。

(5) 对输出进行记录

最后，对问题和修复进行记录。记录故障排除过程非常有益。没有任何东西可以取代您排除故障的经验，并且每个新问题都为您提供了一个丰富经验的机会。在您的技术资料库中保留了一个修复过程的备份。这样，当问题(或类似的问题)再次出现的时候就非常有用了。对排除故障的过程进行记录是建立、保持和共享经验的一种方式。

要记住，您所做的任何更改都可能会影响基准条件，这时最好对网络的基准进行更新，以备未来出现问题时使用。

如果对网络统计数字和症状进行初步了解之后，还不能找出问题所在，则排除故障的下一步就是把整个网络分为较小的部分，以帮助隔离问题所在。

1.6 网络故障管理

故障管理是网络管理中最基本的内容之一，网络故障管理的目的在于防止类似故障的再次发生，确保网络系统的高稳定性。网络故障管理是相当重要的。

在网络出现故障时，一般情况下，网络管理员应报警。网络管理员应执行一些诊断测试来辨别故障原因，及时发现故障部位，做好对所有节点动作状态的监控、故障记录的追踪与检查，对网络系统进行测试。

网络发生故障可能会对社会或生产带来很大的影响。但在发生故障时，往往不能具体确定故障所在的准确位置，而需要相关技术的支持。因此，需要有一个故障管理系统，科学地管理网络发生的所有故障，并记录每个故障的相关信息，最后确定并排除故障，保证网络能提供连续可靠的服务。网络故障管理包括故障检测、隔离、纠正、分析故障原因、网络故障报告和设置优先顺序。

1. 故障检测

故障检测时按照顺序列出可能的原因，第一条是最有可能的原因，最后一条是最不可能的原因。然后逐条测试，看看是哪条原因造成的问题。例如，如果怀疑计算机中的网卡是造成问题的原因，就用一个能够正常工作的网卡来替换它进行测试。故障检测要做到：

- 收集故障检测报告并做出响应；
- 分析故障发生的情况，制订排错方案；
- 使用各种故障诊断工具，执行诊断测试；
- 确认故障的类型及性质。

2. 隔离

启用备用线路或设备，进行故障隔离。

3. 纠正

- 跟踪、辨认故障；
- 进行故障追踪定位；
- 根据故障分析结果，制定并实施解决方案。

4. 分析故障原因

根据网络系统故障的类型及发作频度，分析故障产生的原因和故障性质，预测将来网络故障的发作趋势，建立故障报警数据库，通过对历史故障报警资料的统计分析，寻找网络故障发生的规律，建立故障预防体系，制定并实施解决方案。

5. 网络故障报告

- 通过各种途径报告网络故障；
- 网络故障自动报警，使用自动通知的手段，包括寻呼机、手机、电子邮件等方法；
- 根据网络故障的危害程度将报警指示分级管理，系统根据故障级别做出不同反应。

6. 设置优先顺序

解决网络故障问题的一个基本要素是设置优先顺序。每个人都希望自己的计算机被最早修好，所以设置优先顺序并不容易。尽管最简单的方法是根据先到先服务的原则，但这并不总是可行的，因为某些问题与其他问题相比可能更重要。所以，第一步是根据问题的重要性设置优先顺序。

1.7　网络故障的定位

网络是一个动态系统，若干离散的部件在一起工作就形成一个功能整体。其功能图如图 1-3 所示。

故障定位是在部件基础上进行的 3 个步骤，如图 1-4 所示。

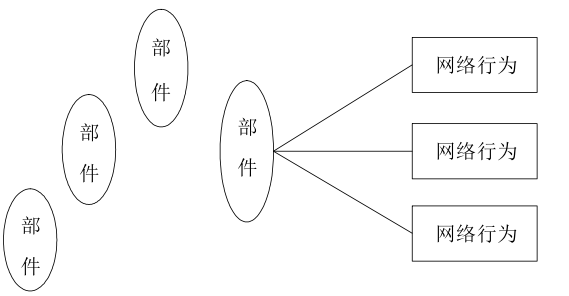

图 1-3　网络功能图

图 1-4　故障定位的 3 个步骤

1. 确定该问题的实际性质

主要考虑以下几个方面。

- 应用程序引起的故障问题；
- 服务器和客户机之间不能通信引起的问题；
- 服务器自身崩溃产生的问题；
- 服务器屏幕上的黑屏或一条信息。

确定问题性质的过程如图 1-5 所示。

针对图 1-5，做出如下考虑：

- 服务器或某客户机可能只是简单挂起，或者没有留下任何问题线索而不能运行。
- 如果还有客户机在运行，对这些客户机做记录。
- 如果该问题仅限于一台客户机或与相同硬件相连的一组客户机，首先怀疑这个硬件。

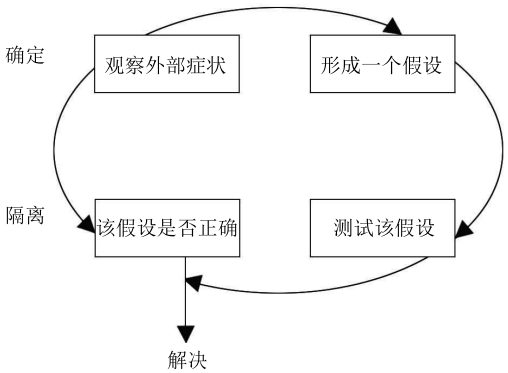

图 1-5　确定问题性质的过程

- 如果该问题影响所有的运行某个程序的客户机，那么该程序可能是引起问题的原因。
- 如果没有一个客户机能够访问该服务器，则可能是该服务器中的 LAN 信道(网络操作系统、LAN 驱动程序、网络接口卡、电缆系统、路由器等)出了问题。
- 自该网络上次正常工作以来，是否发生了什么改变。
- 如果服务器不能再运行，重新启动并且看问题是否再次出现。
- 以相同方式重复出现的问题更容易确定问题所在。
- 试图用另一个应用程序或不运行任何应用程序时重现该问题，能够帮助确定该问题是否与一个特定的应用程序有关。

一旦已经注意到能够观察到的一切现象，就可以对观察到的症状凭借经验进行猜测。

2. 隔离引起该问题的原因

服务器或某客户机可能简单挂起，或者没有留下任何问题线索而不能运行。考虑的问题如图 1-6 所示。

遵循图 1-6 所述确定可能的问题根源后，执行涉及这种可能的原因的各种测试。这样做，应当能够总结出其假设是否正确。

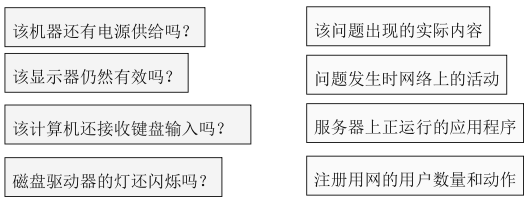

图 1-6　服务器或客户机挂起时考虑的问题

3. 解决该问题

解决问题的主要手段是找出问题、得出结论、排除故障。

(1) 找出问题

用能够正常工作的类似部件来替代怀疑有问题的部件。在熟悉每个部件的性能，了解它们可能会引起的问题后，使用这个方法比较有效。

- 如果怀疑是硬件问题，去除这个值得怀疑的硬件并用一个相同的硬件来代替，看看是否有所改变。
- 如果只是增加了新的硬件，则先替换该硬件。局域网络的一个优点是通常在 LAN 上的另一台客户机中有可供使用的类似网络硬件。许多有经验的人都会有备用设备，这样就不必从运行的机器上拆卸了。

(2) 得出结论

- 进行每个试验，必须确定该假定是否正确。如果正确地执行了其他步骤，这个步骤通常最为直接。
- 如果问题依然如故，则可判断该假定是不正确的。
- 如果该问题已经消除，则表明已经找到了问题的根源。
- 一种最为麻烦的情况是，当改变某一部件后，该问题依然存在但外在表现形式却不同。
- 对可能不熟悉其测试结果的问题，必须扩展或修订关于该问题的方法，这样能够更好地将观察到的结果与其症状联系在一起。
- 如果测试的结果没有得出结论，必须更为详细地关注该症状并且形成另一个假设。在大多数情况下需要在重新检查该症状之前，改变该问题的环境。例如，可能要从网络上去除一个节点，然后再次查看此症状。

图 1-7　网络故障定位涉及的内容

网络故障定位就是在给定的系统中检测、隔离和修理故障的过程。网络故障定位是一项综合性的技术，涉及网络的方方面面，如图 1-7 所示。

1.8　网络诊断工具

排除网络故障通常需要硬件和软件的辅助。为了更有效地排除故障，应该知道有哪些工具有助于解决网络问题。

1.8.1　硬件工具

以前硬件工具非常昂贵，而且难以操作。但现在的硬件工具比较便宜，而且也更加容易使用。这些工具对于了解性能趋势和问题是非常有帮助的。

1. 数字电压表

数字电压表(电压欧姆表)是多用途的电子测量工具。它被认为是计算机或电子专业人员的标准设备，它所能揭示的信息远远超出电阻两端的电压。使用电压表可以确定：

- 电缆是否连接(是否有断路)；
- 电缆是否可以运载网络通信量；
- 同一电缆的两个部分是否暴露和接触(因而造成短路)；
- 电缆的暴露部分是否触及了另一个导体，如金属表面。

网络管理员要检查网络设备的电源。大多数电子设备使用120V的交流电工作，但并不是所有的电源输出都满足这个要求。在较早的设备安装中，尤其是在大型的工业环境中，系统负荷会导致电压降低，有时电压会降为 102V。长时间在低电压下工作可能会导致电子设备出现问题，低电压通常会导致间断性的错误。可能出现的另一个极端是，过高的电压导致设备遭到破坏。在新建

筑物中，不正确的电路走线有可能造成实际的电压输出高达 220V。

因此，在新的地点或新的建筑物中，必须在连接电子设备之前对输出电压进行检查，以确保它们在可以接受的范围内。

2. 网络测试仪

网络测试仪具有如下优点：

- 测量速度快；
- 测量精度高；
- 故障定位准；
- 节省用户查找故障的时间。

3. 时域反射计(TDR)

TDR 沿着电缆发送类似于声纳的脉冲，以确定电缆中是否存在断点、短路或者缺陷。当电缆出现问题时，将影响到网络的性能。如果 TDR 发现了问题，就会对问题进行分析，并显示出分析的结果。TDR 沿着电缆长度方向的有效作用距离通常有数英尺。TDR 在安装网络时使用得比较频繁，在对现有网络进行检查和维护时，也经常用到该工具。

使用 TDR 需要经过专门的训练，因此并不是每个维护部门都有这种设备。但是，网络管理员应该知道 TDR 的功能，在网络出现介质问题时，可以用它来发现缺陷。

4. 高级电缆检测器

高级电缆检测器在数据链路层、网络层，甚至在物理层工作，这已经超越了 OSI 参考模型的物理层次。它也可以显示有关物理电缆的状态信息。

5. 其他硬件工具

(1) 交叉电缆：绕过网络，直接对计算机的通信能力进行隔离和测试。

(2) 硬件回送设备：这是一个串口连接器，利用它，您不必将计算机的串口连接到另一台计算机或外设，就可以对计算机的通信能力进行测试。在利用回送的情况下，数据被传送到一条线路，然后再作为接收数据返回。如果传送的数据没有返回，那么硬件回送就会检测出硬件中存在的问题。

(3) 音调发生器和音调定位器：音调发生器是所有领域中技术人员使用的标准设备，它用来将直流的或者连续的音调信号施加到电缆导体上。音调发生器被加到有疑问的电缆一端，匹配的音调定位器放置在电缆的另一端来测试电缆是否正常。

这些工具可以用来测试导线的连续性和线的极性，也可以用来跟踪双绞线、单个导体和铜轴电缆。

(4) 示波器：示波器是一种以时间为单位测量信号电压值的电子装置，它在一个显示器上显示结果。当与 TDR 一起使用的时候，示波器可以显示：

- 短路；
- 电缆中突然的弯曲和卷曲；
- 开路(电缆中的断路)；
- 衰减(信号的损失)等。

1.8.2　软件工具

软件工具用来监视趋势和确定网络性能问题。

1. 网络监视器

网络监视器是一种软件工具，其作用是对部分或者整个网络的通信量进行跟踪。它检查数据包并收集有关数据包类型、错误以及每台计算机传入和传出的数据包通信量等信息。

网络监视器对于建立部分网络基准非常有用。在建立了基准之后，用户将可以排除通信量故障和监视网络的使用情况，进而确定是否需要对其进行升级。例如，假定在安装新网络之后，用户了解到网络通信量使用了其全部能力的 40%，在一年后再次检查数据通信量时，用户注意到现在使用了全部能力的 80%。如果能一直监视，就可以对通信量的增加情况进行预测，并估计应该在何时升级网络，以避免出现故障。

2. 协议分析器

协议分析器也称为网络分析器，它通过采用数据包捕获、解码和传输数据的方法实时地分析网络通信量。管理大型网络的网络管理员在很大程度上依赖于协议分析器。

协议分析器通过查看数据包的内部来确定问题。它也可以根据网络通信量生成数据统计，从而帮助我们了解网络的总体情况。其中包括：

- 软件；
- 文件服务器；
- 工作站；
- 网卡。

协议分析器有内置的 TDR。

协议分析器可以分析和检测网络问题，其中包括：

- 有故障的网络部件；
- 配置或连接错误；
- LAN 瓶颈；
- 通信量的波动；
- 协议问题；
- 可能引起冲突的应用程序；
- 异常的服务器通信量。

协议分析器可以识别范围广泛的网络行为。它可以：

- 确定活动频繁的计算机。
- 确定发送错误数据包的计算机。如果某台计算机大量的通信量使得网络的速率降低，那么该计算机应该能够被移到网络中的其他网段。如果计算机正在产生错误的数据包，则应该将该计算机从网络中除去，并对它进行修复。
- 查看和筛选某些数据包类型。这对于通信量的路由非常有帮助。协议分析器可以确定何种类型的通信量可以通过网络中一个给定的网络分段。
- 跟踪网络性能以了解其趋势。了解这些趋势将帮助管理员更好地规划和配置网络。
- 通过生成测试数据包并对结果进行跟踪来检查部件、连接和线缆。
- 通过设置产生警告的参数来确定问题发生的条件。

下面是用来对网络交互活动进行监视的最常用工具。

(1) 网络通用 Sniffer

Sniffer 是 Network General 分析器家族产品的一部分，它可以对来自 14 种协议的帧进行解码和截取，这些协议包括 AppleTalk、Windows NT、Netware、SNA、TCP/IP、VINES 和 X.25。Sniffer 可以用 3 种方式测量网络的通信量，相应的单位分别为每秒千字节、每秒帧和可用带宽的百分比。Sniffer 可以收集 LAN 通信量的统计数字，测试一些诸如信标的错误，并将这些信息在 LAN 的配置文件中给出，还可以通过捕获计算机间的帧来确定是否存在瓶颈，并将结果显示出来。

(2) Novell 的 LANalyzer

LANalyzer 软件的功能和 Sniffer 的功能十分类似，但它只能在 Netware LAN 上使用。

1.9 网络测试工具

1.9.1 网络管理和监控工具

网络管理和监控工具主要包括以下几个。

(1) 性能监视器

目前大多数的网络操作系统都包括一个监视实用程序，这个监视实用程序可以帮助管理员对网络的服务器性能进行监视，可以查看实时或记录的操作。其对象包括：

- 处理器；
- 硬盘；
- 内存；
- 网络利用状况；
- 整个网络。

这些监视器可以完成以下操作：

- 记录性能数据；
- 向网络管理员发出警告；
- 启动另一个程序，将系统性能调整到可接受的范围内。

当监视网络时，重要的是必须建立一个基准。只要改变了网络，记录的网络正常运行参数值就应该定期更新。基准信息可以帮助我们对网络性能的巨大变化和微小变化进行监视。

(2) 网络监视器

网络监视器是一个截取和分析网络通信信息的软件，它通过图像来形象地描述每条信息来自哪里，发往何处，在传输过程中经过了哪些节点等。

(3) 协议分析仪

协议分析仪用于检测新设计的网络，帮助我们分析通信行为、差错、利用率、效率以及广播和多播分组。

(4) HP OpenView

HP OpenView 能够在网络测试运行过程中提示某些问题的网络事件出现。

1.9.2　网络诊断工具

常用的网络诊断工具有 360 系统诊断工具、Windows 网络诊断工具、无线网络检测工具。

1. 360 系统诊断工具

360系统诊断工具是完全免费的、安全类上网辅助软件工具，它提供系统诊断功能，能够对系统的 190 多个可疑位置进行诊断，并生成诊断报告。

360 系统诊断工具在 360 安全卫士的“功能大全”里。打开 360 安全卫士，在左下角的功能大全中找到两个相关的功能，分别是宽带测速器、断网急救箱，单击想用的工具，运行就可以了。它可以测试长途网络速度，网页打开速度；还可以进行网络诊断，发现不能上网的问题出在哪里。

2. Windows 网络诊断工具

Windows 网络诊断工具可以测试网络连接并确定与网络相关的程序和服务当前是否工作正常。Windows 网络诊断工具有 WinMTR、Windows IE 浏览器诊断工具等。

(1) WinMTR

WinMTR 运行环境为 Windows XP/2003/Vista/7/10。

它需要结合 traceroute 进行网络诊断，内有 32 位与 64 位版本，请注意区分。

(2) Windows IE

Windows IE 浏览器自带的网络诊断工具附带在 IE 浏览器中，单击 IE 浏览器右上角的“工具”→“诊断连接问题”，即可启动该工具。

Windows IE 功能有：

- 检测操作系统，抓取正在运行的进程，监视注册表内容、随机启动项和网络连接状况等细节。
- 创建系统快照，划分危险级别。创建系统快照的同时，ESET SysInspector 扫描被记录的对象，划分危险级别。
- 用户可以从海量数据中，利用滚动条找到特殊颜色标记的危险对象以做进一步的检查。

3. 无线网络诊断工具

无线网络诊断有 5 个免费工具。

(1) CommView for WiFi

CommView for WiFi 是一个专门为 WiFi 网络设计的数据包嗅探器。此工具能够抓取数据包，然后在其中搜索特定的字符串、数据包类型等。每当探测到某种事先设定的流量时，CommView for WiFi 就会发出报警。

(2) 无线信号扫描工具 inSSIDer

inSSIDer 类似于以前的 Net Stumbler 应用软件，只是它更适用于现在的环境，并且它支持 Windows 操作系统。此工具被用来检测无线网络并报告它们的类型、最大传输速率和信道利用率。甚至还能以图形方式显示每个无线网络的幅值和信道利用率情况。

(3) 无线向导 Wireless Wizard

Wireless Wizard 是一款免费工具，用来帮助用户在无线网络连接中获得可能达到的最好性能。除了能提供无线网络相关的所有常用统计信息外，它还能进行一系列诊断测试，检查用户的无线网络运行情况如何。

(4) 无线密钥生成器 Wireless Key Generator

Wireless Key Generator 是一个比较简单的应用软件，用来帮助用户提高无线网络的安全性。它会提示用户指定无线网络中使用的安全类型和密钥强度，然后为用户生成一个随机的加密密码。

(5) 无线热点 WeFi

WeFi 能帮助用户在全球范围内查找无线热点。此工具的初始屏幕显示当前无线连接相关的统计信息。它还能显示一个可用热点的过滤视图，用户可以选择显示最想查看的热点或任何可用的 WiFi。WeFi 最好的功能就是 WiFi 地图，此功能可向用户显示公共 WiFi 热点的位置。

1.9.3 网络诊断工具使用讲解

在 Windows 网络环境的实施和日常管理中，会经常使用一些诊断工具和实用程序来帮助解决网络常见的一些问题。掌握和了解这些常用的工具对网络技术人员十分重要。下面以 Windows 2000 网络操作系统为例进行讲解。

1. Windows 报告工具

选择“开始”→“运行”，输入“Winrep.exe”，启动 Windows 报告工具。它搜集计算机的有关信息，用户可以根据这些信息诊断和排除各种计算机故障。

2. 文件检查器

文件检查器在 Windows 2000 中只能应用于命令解释模式下。可以通过在命令行模式下输入“SFC”启动文件检查器，其作用是扫描所有受保护的系统文件并用正确的文件进行替换。

3. 脚本调试器

上网浏览网页时，经常会遇到一些脚本运行错误的提示，为了防止产生错误，一般是停止执行脚本。有了脚本调试器，就可以对错误进行调试和排除。脚本调试器可以测试一个脚本文件的运行情况，调试脚本文件中的错误。脚本调试器并非 Windows 2000 默认安装的。选择“控制面板”→“添加/删除程序”→“添加/删除 Windows 组件”→“脚本调试器”，然后单击“下一步”按钮就可以安装脚本调试器。选择“开始”→“程序”→“附件”→Microsoft script debugger 可以打开脚本调试器。

4. DirectX 诊断工具

选择“开始”→“运行”，输入“Dxdiag.exe”可以打开 DirectX 诊断工具。此工具用于向用户提供系统中 DirectX 应用程序编程接口(API)组件和驱动程序的信息，也能够测试声音和图形输出、Microsoft DirectPlay 组件，还可以禁用某些硬件加速功能，使系统运行得更加稳定。利用此工具可以诊断硬件存在的问题，提供解决的办法，并可以更改系统设置，使硬件运行在最佳的状态。

5. Windows 2000 故障恢复控制台

Windows 2000 故障恢复控制台是命令行控制台，可以从 Windows 2000 安装程序启动。使用故障恢复控制台，无须从硬盘启动 Windows 2000 就可以执行许多任务，可以启动和停止服务，格式化驱动器，在本地驱动器上读写数据(包括被格式化为 NTFS 的驱动器)，执行许多其他管理任务。如果需要通过从软盘或 CD-ROM 复制一个文件到硬盘来修复系统，或者需要对一个阻止计算机正常启动的服务进行重新配置，故障恢复控制台特别有用。

1.9.4 网络仿真和仿真工具

网络仿真也称为网络模拟，是一种网络研究工具，既可以取代真实的应用环境得出可靠的运行结果和数据，也可以模仿一个系统过程中的某些行为和特征。它以随机过程和统计、优化为基

础，通过对不同环境和工作负荷的分析比较，来优化系统的性能。

网络仿真就是在不建立实际网络的情况下使用数学模型分析网络行为的过程，从而获取特定的网络特性参数的技术。

随着网络的应用、网络新技术的不断出现和数据网络的日趋复杂，网络仿真的应用也越来越广泛，网络仿真已成为研究、规划、设计网络不可缺少的工具，无论是构建新网络，还是升级改造现有网络，都需要对网络的可靠性和有效性进行客观的评估，从而降低网络建设的投资风险，提高网络的性能。

目前在计算机网络仿真软件中，主流网络仿真软件有 OPNET、NS2、NS3、Matlab、CASSAP、SPW 等，这为网络研究人员提供了很好的网络仿真平台。

1. OPNET 网络仿真工具

OPNET 网络仿真工具主要面向网络设计专业人士，帮助客户进行网络结构、设备和应用的设计、建设、分析和管理。能够满足大型复杂网络的仿真需要。

(1) OPNET 网络仿真工具的特点

OPNET 网络仿真工具有如下特点：

① 提供三层建模机制，最底层为 Process 模型，以状态机来描述协议；中层为 Node 模型，由相应的协议模型构成，反映设备特性；上层为网络模型。三层模型和实际的网络、设备、协议层次完全对应，全面反映了网络的相关特性。

② 提供一个基本模型库，包括路由器、交换机、服务器、客户机、ATM 设备、DSL 设备、ISDN 设备等。OPNET 对不同的企业用户提供附加的专用模型库，附加的专用模型库需另外付费。

③ 采用离散事件驱动的模拟机理。

④ 采用混合建模机制，把基于包的分析方法和基于统计的数学建模方法结合起来，可得到非常详细的模拟结果。

⑤ 具有丰富的统计量收集和分析功能。它可以直接收集常用的各个网络层次的性能统计参数，能够方便地编制和输出仿真报告。

⑥ 提供了和网管系统、流量监测系统的接口，能够方便地利用现有的拓扑和流量数据建立仿真模型，同时还可对仿真结果进行验证。

⑦ 在软件功能方面，做得比较完备，可以对分组的到达时间分布、分组长度分布、网络节点类型和链路类型等进行很详细的设置，而且可以通过不同厂家提供的网络设备和应用场景来设计自己的仿真环境，用户也可以方便地选择库中已有的网络拓扑结构。

⑧ 易操作易用，使用比较少的操作就可以得到比较详尽和真实的仿真结果。

⑨ OPNET 是商业软件，界面非常好。

(2) OPNET 的缺点

① 价格高。

② 学习的门槛很高，通过专门培训而达到较为熟练的程度至少需一个多月的时间。

③ 仿真网络规模和流量很大时，仿真的效率会降低。

④ 提供的模型库有限，专用模型库需另外付费。

2. NS2 网络仿真工具

NS2 是一种面向对象的网络仿真器，可以用于仿真各种不同的 IP 网。NS2 网络仿真工具是一种针对网络技术的源代码公开的、免费的工具，最初是针对基于 UNIX 系统下的网络设计和仿真而进行的，它所包含的模块非常丰富，几乎涉及了网络技术的所有方面，成为学术界广泛使用的

网络模拟软件。NS2 作为辅助教学的工具，也被广泛应用在了网络技术的教学方面。

(1) NS2 网络仿真工具的特点

① 源代码公开。

② 可扩展性强。

③ 速度和效率优势明显。

④ NS2 是自由软件，免费，这是与 OPNET 相比最大的优势，因此它的普及度较高。

(2) NS2 的缺点

① NS2 界面不如 OPNET。

② NS2 内容庞杂，不容易上手。

③ 由于不是同一公司开发的，格式上不是很统一。

3. NS3 网络仿真工具

NS3 是一款面向网络系统的离散事件网络仿真软件，主要用于研究与教学。NS3 作为源代码公开的免费软件，经 GNU GPLv2 认证许可，可被大众研究、改进与使用，它将逐步取代目前广泛应用的 NS2 网络模拟软件。

NS3 是用 C++和 Python 语言编写的，可作为源代码发布并适用于以下系统：Linux、UNIX variants、OSX，以及 Windows 平台上运行的 Cygwin 或 MinGW 等。

NS3 并不是 NS2 的扩展，而是一个全新的模拟器。虽然两者都是用 C++编写的，但是 NS3 并不支持 NS2 的 API，而是一个全新的模拟器。NS2 的一些模块已经被移植到了 NS3 上。在 NS3 的开发过程时，NS3 项目组会继续维护 NS2，同时也会研究从 NS2 到 NS3 的过渡和整合机制。

(1) NS3 模型

NS3 的基本模型共分为五层：应用层(application layer)、传输层(transport layer)、网络层(network layer)、链路层(link layer)、物理层(physical layer)。

(2) NS3 中的构件模型

① 节点(node)

NS3 节点是一个网络模拟器，而非一个专门的因特网模拟器。NS3 中的基本计算设备被抽象为节点，节点由用 C++编写的 Node 类来描述，Node 类提供了用于管理计算设备的各种方法。可以将节点设想为一台可以添加各种功能的计算机。

② 信道(channel)

通常我们把网络中数据流流过的媒介称为信道。在 NS3 中用 C++编写的 Channel 类来描述。

③ 网络设备

在 NS3 中网络设备这一抽象概念相当于硬件设备和软件驱动的总和。在 NS3 仿真环境中，网络设备安装在节点上，使得节点通过信道和其他节点通信。网络设备由用 C++编写的 NetDevice 类来描述。

④ 应用程序

在 NS3 中没有真正的操作系统的概念，更没有特权级别或者系统调用的概念，需要被仿真的用户程序被抽象为应用，用 Application 类来描述。

(3) 有关 NS3 详细资料的获取

用户可以从以下几个网站获取：

① http://www.nsnam.org，提供 NS3 系统的基本信息。

② http://www.nsnam.org/ns-3-dev/documentation/，该页面主要包括以下主要资料。

- 初步介绍 NS3 的相关知识，以及下载及安装方法，简单用法。
- 更深一步讲解 NS3 的相关知识以及 NS3 的编码风格。
- 主要介绍 NS3 的相关模块。用户可以选择自己实际需要的模块进行学习，不需要全部阅读。

③ http://www.nsnam.org/doxygen/index.html，该页面上提供了 NS3 系统架构的更为详细的信息。在编写自己的模块时，查询类的成员函数、类的属性等，要经常用到这个链接。

④ http://www.nsnam.org/wiki，可以作为 NS3 主站点的补充。

⑤ NS3 的源码可以在 http://code.nsnam.org 找到。读者也可以在名为 ns3-dev 的源码仓库中找到当前的 NS3 开发树，以及 NS3 的之前发行版本和最新测试版本的代码。

4. MATLAB 网络仿真工具

MATLAB 网络仿真工具用于数值计算和图形处理的科学计算系统环境。MATLAB 是英文 Matrix Laboratory(矩阵实验室)的缩写。在 MATLAB 环境下，用户可以集成地进行程序设计、数值计算、图形绘制、输入输出、文件管理等各项操作。

MATLAB 提供了一个人机交互的数学系统环境，该系统的基本数据结构是矩阵，在生成矩阵对象时，不要求作明确的维数说明。与利用 C 语言或 FORTRAN 语言做数值计算的程序设计相比，利用 MATLAB 可以节省大量的编程时间。

(1) MTALAB 的五个主要组成部分

① MATALB 语言体系

MATLAB 是高层次的矩阵/数组语言，具有条件控制、函数调用、数据结构、输入输出、面向对象等程序语言特性。利用它既可以进行小规模编程，完成算法设计和算法实验的基本任务，也可以进行大规模编程，开发复杂的应用程序。

② MATLAB 工作环境

这是对 MATLAB 提供给用户使用的管理功能的总称，包括管理工作空间中的变量输入输出的方式和方法，以及开发、调试、管理文件的各种工具。

③ 图形图像系统

这是 MATLAB 图形系统的基础，包括完成 2D 和 3D 数据图示、图像处理、动画生成、图形显示等功能的高级 MATLAB 命令，也包括用户对图形图像等对象进行特性控制的低级 MATLAB 命令，以及开发 GUI 应用程序的各种工具。

④ MATLAB 数学函数库

这是对 MATLAB 使用的各种数学算法的总称，包括各种初等函数的算法，也包括矩阵运算、矩阵分析等高层次数学算法。

⑤ MATLAB 应用程序接口(API)

这是 MATLAB 为用户提供的一个函数库，使得用户能够在 MATLAB 环境中使用 C 程序或 FORTRAN 程序，包括从 MATLAB 中调用程序(动态链接)，读写 MAT 文件的功能。

在国际学术界，MATLAB 已经被确认为准确、可靠的科学计算标准软件。

(2) MATLAB 的缺点

① MATLAB 和其他高级程序相比，程序的执行速度较慢。由于 MATLAB 的程序不用编译等预处理，也不生成可执行文件，程序为解释执行，所以速度较慢。

② MATLAB 不能实现端口操作和实时控制，但结合 C++ Builder 的运用，实现优势互补就可以克服这一缺点。

5. CASSAP 网络仿真工具

CASSAP 网络仿真工具主要应用于数字信号处理和网络通信领域，它可以在概念、体系结构、算法三个层次上实现仿真。CASSAP 采用了数据流驱动仿真器，它比基于时钟周期的仿真器速度提高了 8～16 倍。CASSAP 提供了 1000 多个高层模块，并可对其中所需模块自动生成行为级或 RTL 级 VHDL，也可生成各种风格的 DSP 代码，供 DSP 处理器做软件实现。CASSAP 可广泛应用于数字传输系统，如通信、图像、多媒体等，并提供了针对 GSM、CDMA、DECT 等标准的专用开发平台。

6. SPW 网络仿真工具

SPW 网络仿真工具提供面向电子系统的模块化设计、仿真及实施环境，是进行算法开发、滤波器设计、C 代码生成、硬/软件结构联合设计和硬件综合的理想环境。SPW 的一个显著特点是它提供了 HDS 接口和 MATLAB 接口。SPW 通常应用于无线和有线载波通信、多媒体和网络设计与分析等领域。

习题

1. 从网络故障本身来说，经常会遇到的故障有哪些？
2. 简述网络发生故障的具体分布。
3. 网络发生故障的原因有哪几种？
4. 网络故障管理一般包括哪五项？
5. 根据网络管理系统的发展历史简述网络管理系统的分代。
6. 简述网络管理系统的分类方法。
7. 简述新兴技术、新行业对网络管理系统的新要求。
8. 简述第五代无线移动通信网络的基本概念。
9. 常用的网络故障测试命令有哪些？
10. 网络故障诊断应该实现哪三方面的目的？
11. 简述故障诊断的步骤。
12. 简述故障排除过程。
13. 网络故障排除的过程大致可分为哪 5 个步骤？
14. 故障检测要做到哪些？
15. 简述网络故障报告的内容。
16. 简述在部件基础上进行故障定位的 3 个步骤。
17. 网络诊断硬件工具有哪些？
18. 网络诊断软件工具有哪些？
19. 网络管理和监控工具主要包括哪几个？