DR

牛云 徐庆 辛阳 等编著

数据备份与灾难恢复

国家信息化安全教育认证(ISEC)系列教材

机械工业出版社
CHINA MACHINE PRESS

国家信息化安全教育认证(ISEC)系列教材

数据备份与灾难恢复

牛　云　徐　庆　辛　阳　等编著

机械工业出版社

本书主要介绍了数据存储技术、数据备份与灾难恢复的相关知识与实用技术，讨论了数据备份与灾难恢复策略、解决方案，数据库系统与网络数据的备份与恢复，对市场上的一些较成熟的技术和解决方案进行了分析比较。本书的特色是实用性强，使读者能够利用书中的方法和步骤去解决实际应用中的常见问题。

本书适用于大专院校信息安全专业的师生和从事数据备份与灾难恢复的专业技术人员。

图书在版编目（CIP）数据

数据备份与灾难恢复/牛云等编著. —北京：机械工业出版社，2004.3
（国家信息化安全教育认证（ISEC）系列教材）
ISBN 7-111-14164-4

Ⅰ. 数… Ⅱ. 牛… Ⅲ. 磁盘存储器－资格考核－教材
Ⅳ. TP333.3

中国版本图书馆 CIP 数据核字（2004）第 019308 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：时 静

北京蓝海印刷有限公司印刷·新华书店北京发行所发行

2004 年 6 月第 1 版·第 1 次印刷
787mm×1092mm 1/16·10.5 印张·248 千字
0001－5000 册
定价：19.00 元

国家信息化安全教育认证(ISEC)专家组

卿斯汉　中国科学院信息安全技术工程研究中心主任　研究员
曲成义　中国航天科技集团公司第710研究所总工　研究员
许榕生　中国科学院高能物理研究所计算中心研究员
贾颖禾　国务院信息化工作办公室网络与信息安全组研究员
曹元大　北京理工大学软件学院院长　博士生导师
杨义先　北京邮电大学信息安全中心主任　博士生导师
林　鹏　国家计算机网络应急技术处理协调中心广东分中心副主任
　　教授级高级工程师
祁　金　公安部公共网络信息安全监察局管理监察处副处长
景乾元　公安部公共网络信息安全监察局安全对策处副处长
万平国　国际信息战略研究中心理事　中网通讯网络有限公司董事长
刘宝旭　中国科学院高能物理研究所计算中心副研究员

教材编委会

主　任：宋　玲
副主任：赵小凡　张会生　欧阳满　蔡金荣　沈志工
成　员：洪京一　张宝泰　王　宏　孙论强　彭　澎　张晓伟
　　刘树安　刘　旸　马志谦　胡　铮　宁宇鹏　阎　慧
　　王　伟　薛静锋　辛　阳

出版说明

随着信息化在我国的不断深入和发展，信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力。人们在感受它所带来的新体验、享受它为我们带来高效率的同时，也面临着日益突出的信息安全问题。党和国家领导人多次强调，必须充分认识到做好信息安全保障工作的重要性，大力搞好技术开发和人才培养。

对信息安全专业人才的需求是多层次的。从信息安全基础理论研究到新技术的开发利用，再到各级网络信息系统信息安全保障体系的建设、运行，需要根据不同要求有针对性的进行人才培养。

国家信息化安全教育认证(ISEC)项目是由信息产业部信息化推进司推出的信息安全领域的国家级认证体系。该项目由中国电子商务协会监督，由 ISEC 国家信息化安全教育认证管理中心统一管理与实施。ISEC 国家信息化安全教育认证管理中心以行业为基础、以技术为核心制定了一套面向应用的教育方案。根据工作性质的不同，教育对象被划分为规划决策层、管理运营层和操作层三个层次。认证体系的设计，课程内容及相应的教学考试大纲的编写和指定是针对三个层次人员对信息安全知识和技能的不同需求和理解程度的不同而制定的。确保不同层次，不同需求的各类人员从各自的角度充分掌握和理解信息安全的知识和技能。

本系列教材是在国家信息化安全教育认证(ISEC)专家组的指导下，由国家信息化安全教育认证(ISEC)教材编委会组织编写的。始终以 ISEC 国家信息化安全教育认证管理中心制订的各级考试大纲为依据，坚持面向行业用户的需求和侧重技术应用两个基本原则，全面地介绍了信息安全各种主流技术和管理规范，以帮助读者深入了解信息安全本质，并熟练掌握相应的技能，从而建立完备的信息安全观念。本系列教材包括：《网络安全基础》、《防火墙原理与技术》、《入侵检测技术》、《VPN 技术》、《PKI 技术》、《数据备份与灾难恢复》、《网络隔离与网闸》、《信息安全法规与标准》、《信息安全策略与机制》、《信息安全团队构建与管理》，共计 10 本。

在写作过程中，北京正阳天马信息技术有限公司为本系列教材的编写提供了很多宝贵的建议和支持。

前　言

数据存储备份和存储管理技术源于20世纪70年代的终端/主机计算模式，当时数据主要集中在主机上；20世纪80年代以后，由于PC的发展，尤其是90年代应用最广的客户机/服务器模式的普及，网络上的文件服务器和数据库服务器成为要害数据集中的地方，而客户机上也积累了一定量的数据，数据的分布造成了数据存储管理的复杂化。当前，网络正在使存储、备份、恢复技术发生着革命性的变化：首先是存储容量的急剧膨胀；其次是数据存储时间和方式的延展；最后是数据存储的结构不同。在全球经济信息化的浪潮下，数据的存取更多地受到安全机制的管理，而不是受到地域空间的约束。

网络为数据信息的急剧膨胀提供了合理、有效的存储管理手段，同时也给数据引入了新的安全隐患。网络系统环境中数据被破坏的原因主要有以下几个方面：

(1) 自然灾害，如水灾、火灾、雷击、地震等造成计算机系统的破坏，导致存储数据被破坏或完全丢失。

(2) 系统管理员及维护人员的误操作。

(3) 计算机设备故障，其中包括存储介质的老化、失效。

(4) 病毒感染造成的数据破坏。

(5) Internet上“黑客”的侵入和来自内部网的蓄意破坏。

从国际上看，发达国家都非常重视数据存储备份和数据恢复技术，而且将其充分利用，而在国内，只有不到15%的服务器连有备份设备，这就意味着，85%以上的服务器中的数据面临着随时可能遭到全部破坏的危险。对于一个企业来说，网络数据的安全性是极为重要的，一旦重要的数据被破坏或丢失，就会对企业日常生产造成重大的影响，甚至是难以弥补的损失。

数据备份与灾难恢复是一种保护数据信息的安全技术，在实际应用中具有重要的地位和作用。本书概要介绍了数据存储技术、数据备份与灾难恢复的基础知识、基本理论，数据备份与恢复的策略和解决方案。读者可以利用书中的知识和方法去解决实际应用中的常见问题。通过阅读本书，能够较为全面地了解数据备份和灾难恢复技术，掌握常用的数据备份和灾难恢复策略与解决方案，熟悉市场上的一些比较成熟的技术和解决方案。

本书共分七章。第1章“数据存储技术概述”介绍实现数据备份与灾难恢复的基础知识和部分基本理论，阐述深入探讨数据备份和恢复技术的基本原理、策略、解决方案和其他预备知识。本章可使读者较为全面地了解存储技术的发展和现状。

第2章“数据备份技术概述”介绍数据备份的作用与意义，数据备份的定义，数据备份的类型，数据备份系统基本构成，最后介绍常用的数据备份工具。

第3章“灾难恢复技术概述”讲述灾难恢复的作用与意义、灾难恢复的定义、灾难恢复策略、灾前措施、灾难恢复计划、灾难恢复计划的测试和维护、如何应付紧急事件，以及常用灾难恢复工具的使用。

第4章“数据备份与灾难恢复策略”阐述备份策略的定义、备份策略的分类、备份策略的规

划，以及制订备份策略应考虑的问题；同时结合实际情况指出如何来制定符合安全需求的备份与灾难恢复策略。

第5章“数据库系统的数据备份与灾难恢复”以当前市场上通用的三种常用数据库：MS SQL Server2000数据库、Oracle数据库、Informix数据库为例，阐述如何进行数据库系统的备份与灾难恢复，以便能更紧密地结合实际。

第6章“网络数据备份与灾难恢复技术”指出由于网络的快速发展和网络安全的特殊性，给网络上的数据备份和灾难恢复带来了新的问题。本章在此基础上阐明网络备份系统的目标与意义、如何对网络数据备份的需求进行分析、网络数据备份的实现以及如何进行网络数据备份系统的实效测试。

第7章“数据备份与灾难恢复解决方案”阐述如何在制定备份与灾难恢复前进行正确的需求分析，选择合适的备份硬件、软件与数据备份方案加以实施；并以HP、VERITAS、CA、IBM等公司为例介绍典型的数据备份和灾害恢复解决方案。

本书主要由牛云和徐庆执笔编写，其中第1、5、6、7章由牛云编写，第2、3、4章由徐庆编写。在编写过程中，北京邮电大学的潘剑利为此书准备了写作提纲并且搜集了大量资料，辛阳博士对提纲提出了意见和建议，并审阅了全书，另外赵海洋博士、高新波老师、黄明硕士、徐勤、薛元星也参加了本书的部分编写工作。此外还得到了北邮信息安全中心杨义先教授，国家信息化安全教育认证管理中心的宁宇鹏博士、刘旸先生的热情帮助，在此表示感谢！

由于数据存储、备份与灾难恢复技术涉及的知识面广、发展迅速，加之作者的水平有限，书中的错误在所难免，若有不当之处，敬请指正。

希望本书能对读者有所裨益。

作　者

目　录

第1章　数据存储技术概述

本章导读：本章主要讲述了实现数据备份与灾难恢复的基础知识和部分基本理论，重点在于为将来深入地探讨数据备份和恢复技术的基本原理、策略和解决方案提供预备知识。通过阅读本章，可使读者较为全面地了解存储技术的发展和现状。

数据存储备份和存储管理技术源于20世纪70年代的终端——主机(Terminal——Server,T/S)计算模式，当时数据集中在主机上，因此磁带库作为易管理的海量存储设备，是当时通常使用的存储备份和存储管理设备。20世纪80年代后期个人计算机(Personal Computer,PC)的发展和20世纪90年代应用最广的客户机/服务器(Client——Server,C/S)模式的普及为网络数据地发展起到了推波助澜的作用。此后，网络文件服务器和数据库服务器逐步成为要害数据的集中地，同时，考虑到安全性能和分布状况，客户机的数据信息也有了一定程度的积累。随之出现了数据分布，数据分布造成了数据存储管理的复杂化。

Internet在快速发展的同时，也使存储、备份、恢复技术发生着翻天覆地的变化。这种变化主要表现在以下三个方面：

- 存储容量的急剧膨胀。
- 数据存储时间和方式的延展。今天，Internet使网络数据能够每天24小时、每周7天、每年365天始终处于就绪状态；同时可以通过多重渠道和方式实现数据的更新与修改。
- 数据存储结构的不同。在全球经济信息化的浪潮下，数据的存取更多地受到安全机制的管理，而不是受到地域空间的约束；在Internet时代，数据是面向全世界的，正常的使用者可以在世界任何可接入的地点实现数据的存储与管理。

存储是指根据不同的应用环境通过合理、安全的方式将数据保存在某种存储介质上，并能确保其有效的访问。人们对数据存储备份一词并不陌生，然而对备份的真正内涵并不完全了解。备份过程是预防介质、操作系统、软件和其他重要数据文件被损坏的重要防护措施。在一般人的脑海里，往往将备份和复制等同起来，其实不然。备份既不是简单地复制，也不属程式化的、单调的介质更换操作。除了复制外，数据存储还包括更重要的内容，这就是数据的备份管理。备份管理涉及备份的可计划性、磁带机的自动化操作、历史记录的保存以及日志记录等。事实上，备份管理是一个全面的概念，它不仅包含制度的制定和磁带的管理，而且还能决定引进备份技术，如备份技术的选择、备份设备的选择、介质的选择乃至软件技术的挑选等。

有不少人往往也把双机热备份、磁盘阵列备份以及磁盘镜像备份等硬件备份的内容和数据存储备份相提并论。事实上，所有的硬件备份都不能代替数据存储备份，硬件备份只是拿一个系统、一个设备等作牺牲来换取另一台系统或设备在短暂时间内的安全。若发生人为的错误、自然灾害、电源故障、病毒侵袭等，引起的后果就不堪设想，如造成所有系统瘫痪，所有设备无法运行，由此引起的数据丢失也就无法恢复了。事实证明，只有数据存储备份才能为人们提供万无一失的数据安全保护。

综上所述，理想的数据存储备份应该是使用一种容量大、具有先进自动管理功能、价格又

相对便宜的设备对整个系统(特别是对整个网络系统)的数据进行备份。

1.1 数据存储的作用与意义

1.1.1 网络数据安全的重要性

互联网络的快速发展,为信息资源的共享和传输提供了有利条件。无论是社会、企业还是个人,利用网络沟通联系、贸易买卖和传递大量文件数据已成为可能。互联网络在为全球提供方便快捷的同时,也伴随着大量的安全问题。面对网络中众多的黑客攻击和商业间谍,必须为网络数据、电子商务、电子政务和其他网络基础设施构筑强有力的安全屏障。

1. 互联网络与安全问题

随着 Internet 技术的日益成熟与普及,其功能也从信息共享演变为大众化信息传播的工具。公司在重新解释与用户沟通、产品销售和建立商务关系的方式,社会机构也在利用网络媒体的宣传优势。贸易活动和媒体活动进入网络世界,使 Internet 成为信息传播的源动力。由于 Internet 是开放性网络,费用低廉,而且基于 Internet 的传输可以不受特殊数据交换协议的限制,使用更灵活;同时所支持的功能更全面。

但是,商业间谍无处不在,网络黑客无孔不入。对企业而言,要通过 Internet 达到从异地取回重要数据,并且使异地员工和本地员工都能够安全地访问内部网络,并保护公司或是内部的机密信息不受黑客和商业间谍入侵所侵害,则必须解决互联网络的安全问题。由于 Internet 的开放性及安全性不足,针对网络存在众多的攻击手段,如病毒、陷门、隐通道、侦听、欺骗、口令攻击、路由攻击等,并且攻击手段日新月异、防不胜防,这对网络数据的存储与利用产生了巨大的挑战。

2. 网络数据的安全性

对于一个企业来说,数据的安全性是极为重要的,一旦重要的数据被破坏或丢失,就会对企业日常生产造成重大的影响,甚至是难以弥补的损失。

通过网络传输的数据就要考虑到数据在传输中的安全性。通常,在网络中的计算机数据的安全性涉及到以下几个方面:

1) 数据的机密性(Confidentiality)。防止合法或隐私数据为非法用户所获得,通常使用加密的手段实现,从而确保在只有通信或是数据的合法拥有者才能惟一知道数据信息的内容。对于敏感信息对加密还有更为严格的要求,即便入侵者非法进入系统也不能够获得信息的内容。

2) 完整性(Integrity)。确保数据信息在传输中,不为通信他方或非法拦截者对传输的数据内容进行修改;或是数据在存储的过程中,不会有对数据内容、属性等的不明修改。

3) 可用性(Availability)。是指计算机资源在系统合法用户需要使用时必须是可用的;对于正常的用户和授权者应该能随时且安全地使用信息和信息系统的服务,可用性是在大面积拒绝服务攻击发生后保障正常服务的一项安全行为。

4) 鉴别(Authentication)。数据在传输过程前,应该确认发送和接收信息的双方,即通信双方是可以信任的;确保提供信息和接收信息服务间的相互身份认证,才能防止欺诈行为和信

息泄漏的产生。

5) 授权的安全。保证是合法用户在通信和提供服务中对无线或是有线网络与计算资源的使用;既要避免非法用户的盗用,也要考虑合法用户的有效信任模式。

网络数据的安全性如果不能得到正常的保证,通常会产生严重的问题。根据 3M 公司的一项调查表明,对于市场营销部门来说,恢复数据至少需要 19 天,耗资 17000 美元;对于财务部门来说,这一过程至少需要 21 天,耗资 19000 美元;而对于工程部门来说,这一过程将延至 42 天,耗资达 98000 美元。而且在恢复过程中,整个部门实际上是处在瘫痪状态。在今天,长达 42 天的瘫痪足以导致任何一家公司破产,而惟一可以将损失降至最小且行之有效的办法莫过于数据的存储备份。

1.1.2　我国数据存储备份的现状

从国际上看,以美国为首的发达国家都非常重视数据存储备份技术,而且将其充分利用,服务器与磁带机的连接已经达到 60% 以上。而在国内,只有不到 15% 的服务器连有备份设备,这就意味着 85% 以上的服务器中的数据面临着随时可能遭到破坏的危险。因此,有必要加强对数据存储备份。数据存储备份目前应该成为保证信息安全可用的一项重要防护措施,并不断引进先进的数据存储备份设备来确保网络数据的安全和在紧急情况下的应急使用。

1.1.3　数据被破坏的原因

信息时代的来临,使得电子商务、电子政务,以及网络本身正在改变我们的生活,人类在进入信息化社会享受高度文明的同时,也面临着伴随信息科技发展而来的种种威胁。计算机系统与网络的广泛应用方便了商业和国家机密信息的传送和管理,但是对这些信息的保护以及在信息时代下的电子对抗、信息对抗的需求也有显著的增加。

同样,存储数据信息的系统也面临着极大的安全威胁。一方面,来自开放的网络、社会;另一方面,来自系统设计和自身的发展。

1. 信息系统面临的威胁

信息系统本身面临着各种各样的威胁,其中包括:

1) 潜在的网络、系统缺陷危及系统的安全。

2) 传统的安全保密技术的局限性不能够确保系统的安全。

3) 网络犯罪、黑客等入侵者对网络与系统的攻击。

4) 计算机病毒。

5) 木马等陷门。

6) 蠕虫。

7) 隐蔽通道。

8) 拒绝服务攻击。

9) 来自系统内部的入侵攻击或信息泄露等。

2. 网络自身和信息系统自身的发展存在一定程度的安全隐患

信息系统的安全问题:

1) 操作系统的脆弱性。操作系统的安全问题又包括:

- 模块层次结构、动态连接、打补丁、安全管理。
- 网络安装、传输程序。
- 创建进程、远端进程的创立、特权继承等的管理。
- RPC(远程过程调用)。
- NFS(网络文件系统)。
- DAEMON(守护进程)。
- Bug 的存在。
- 开放端口、隐蔽通道等的存在。
- 系统集成与开放和安全之间的矛盾。

2) 计算机网络的资源开放、信息共享以及网络复杂性增大了系统的不安全性。

3) 操作系统和网络系统的漏洞。

- 缓冲区溢出。
- 拒绝服务攻击漏洞。
- 代码泄漏、信息泄漏漏洞。
- 配置修改、系统修改漏洞。
- 脚本执行漏洞。
- 远程命令执行漏洞。
- 其他类型的漏洞。

4) 数据库管理系统等应用系统设计中存在的安全性缺陷。

5) 缺乏有效的安全管理。

Internet 起源于实现信息资源共享的研究项目,那么在开始构建的阶段,安全问题不是主要的考虑因素。Internet 的安全问题存在于以下几个环节:

1) 网络的设计适合于少量的用户,在初始时期的参与者多是研究人员,因此网络的角色定位在可信的用户群体,而对网络可能面临的安全威胁缺乏应有的考虑。

2) 可靠性、计费、性能、配置、安全等。

3) 网络协议的开放性与系统的通用性。

4) 目标可访问性,行为可知性。

5) 攻击工具易用性和入侵等行为实现的建议性。

6) Internet 缺乏集中的管理权威和统一的政策。

7) 在安全政策、计费政策、路由政策等方面。

在信息系统和网络建设快速发展的今天,系统漏洞和黑客攻击的情形有增无减,这种状况不能不令人担忧。

图 1-1 显示了在 1998 年到 2001 年间网络攻击行为,仅仅在四年内,就飙升了 13.1 倍。

正是由于上述原因,在当前情况下,针对网络系统环境,数据信息的安全性又有极为特殊的情况。分析网络系统环境中数据被破坏的原因,主要有以下几个方面:

1) 自然灾害,如水灾、火灾、雷击、地震等造成计算机系统的破坏,导致存储数据被破坏或完全丢失。

2) 系统管理员及维护人员的误操作。

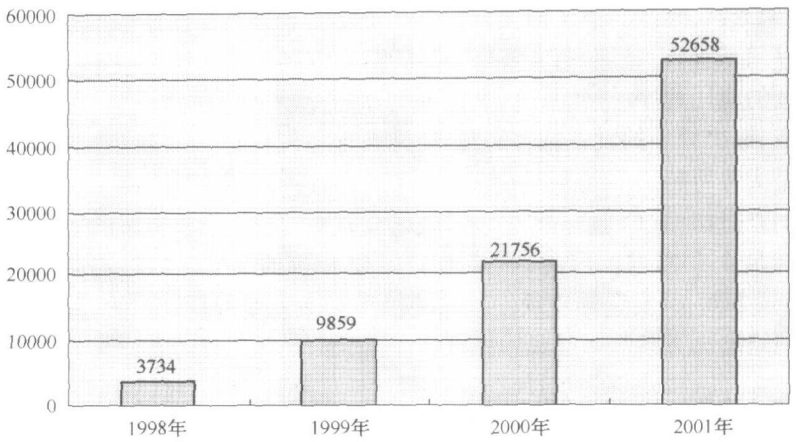

图 1-1　网络攻击行为的增长趋势

3）计算机设备故障，其中包括存储介质的老化、失效。

4）病毒感染造成的数据破坏。

5）Internet 上“黑客”的侵入和来自内部网的蓄意破坏。

1.1.4　数据存储的意义

近几年来，国内网络系统的规划和设计不断推陈出新，在众多网络方案中，通常对数据的存储和备份管理的重要性重视不够，至少在方案中提及不多，甚至忽略。当网络建成运行后，缺乏可靠的数据保护措施，等到出现事故后才来弥补。总之，无论是规划设计还是运行维护阶段，都缺乏对整个系统数据存储管理和备份应采取的专业而系统的考虑。

网络设计方案中如果没有相应的数据存储备份解决方案，不能称其为完整的网络系统方案。计算机系统不是永远可靠的。使用双机热备份、磁盘阵列、磁盘镜像、数据库软件的自动复制等功能均不能称为完整的数据存储备份系统，它们解决的只是系统可用性的问题，而计算机网络系统的可靠性问题需要完整的数据存储管理系统来解决。因此，对原网络增加数据存储备份管理系统和在新建网络方案中列入数据存储备份管理系统就显得相当重要了。

1.2　数据存储技术的现状

目前，SAN 是存储市场发展的主流。从 1999 年开始，EMC、IBM、Compaq、Sun、HP 等公司相继推出自己的 SAN 产品，使 SAN 成为存储领域的一个新的技术热点。SAN 的重要性和热度在最近一段时间以来一直有增无减。

1.2.1　SAN 的互操作性问题

SAN 是存储区域网络（Storage Area Network，SAN）的缩写，见 1.3 节。

存储的互操作性分为两个方面：一是存储设备支持不同的服务器系统。这个问题已经得到了很好的解决，存储供应商的存储设备都能够做到支持主流操作系统，或者是其中的某些版

本。目前,多服务器平台的SAN解决方案是一个发展趋势。互操作性的另一个方面是如何支持多厂商的存储系统,也是使SAN解决方案的核心应具有开放性(Open SAN)。Open SAN的目标是支持任何应用程序、操作系统、文件系统、服务器平台、存储系统、磁带库以及客户所要求的互连设备,解决棘手的设备兼容问题,使网络设备发挥最大的效率。在这个方面,采用开放式的标准是大势所趋。

据权威调查机构IT Centrix的存储网络调查表明:只有不到30%的用户会选择专有存储解决方案来满足企业需求。因此,企业迫切需要开放的SAN系统(Open SAN),在其后的Open SAN发展方面,开发存储软硬件产品的相互支持功能和开放式的存储系统,以促进开放式存储区域网络解决方案的兴起成为主流。

1.2.2 数据存储标准之争的问题

SAN采用的是专门的存储协议,而NAS使用的是IP协议,而目前,为了维持对现有的SAN的兼容性,出现了几大存储技术流派,使得整个存储技术市场形成了百花齐放的局面。

在这些方案中,比较有影响的是:

1) Internet工程任务组(IETF)提出的基于TCP的SCSI(iSCSI)方案。

2) IETF与ANSI(美国国家标准机构)共同提出的基于IP的光纤方案。

3) ANSI提出的光纤骨干网方案。

上述方案各有其利弊。一个存储网方案的出台,其标准的主体定义必须完整细致,不然将难以推广运用。

下面简要介绍一下SCSI(iSCSI)方案和基于IP的光纤方案:

(1) iSCSI(SCSI over TCP)

iSCSI方案是由Adaptec、Cisco、HP、IBM、Quantum等公司共同倡导,提供基于TCP传输、将数据驻留于SCSI设备的方法。

在千兆以太网出现以前,要传输这种类型的块数据,LAN的速度是无法胜任的;在10G以太网登台后,这种基于IP传输块数据的方案无疑更具吸引力。

iSCSI并不改变传统标准通信方案和网络基础架构的设置,但需要额外的千兆光纤以太网路由器及复杂的相关路由器软件来支撑,透过网络,以IP数据形式实现存储设备中SCSI数据的传输。

iSCSI是由IBM的研发机构——加利福尼亚Almaden和以色列Haifa研究中心共同开发的,是一个供硬件设备使用的可以在IP协议的上层运行的SCSI指令集。简单地说,iSCSI可以实现在IP网络上运行SCSI协议,使其能够在诸如高速千兆以太网上进行路由选择。

SAN架构需要高昂的建设成本,远非一般企业所能够承受。与之相对,NAS技术虽然成本低廉,但是却受到带宽消耗的限制,无法完成大容量存储的应用,而且系统难以满足开放性的要求。iSCSI的使用在以上两者之间架设了一道桥梁,基于IP协议,却拥有SAN大容量集中开放式存储的品质。

iSCSI基于IP协议的技术标准,实现了SCSI和TCP/IP协议的连接,对于以局域网为网络环境的用户,只需要不多的投资,就可以方便、快捷地对信息和数据进行交互式传输和管理。

iSCSI的产生解决了开放性、容量、传输速度、兼容性、安全性等问题。