

网络管理规划

全面管理网络是网络高效运行的前提和保障,管理的对象不仅指网络链路的畅通、服务器的正常运行等硬因素,更包括网络应用、数据流转等软因素。网络管理者必须时刻关注本企业网络的运行,关心企业对网络的应用,让网络能够随时满足企业的需求,或者说是引导企业的发展。

1.1 项目背景

某高新产品研发企业拥有员工 2000 余人,公司总部坐落在省会城市高新技术开发区,拥有 4 个生产车间和两栋职工宿舍楼,产品展示、技术开发与企业办公均在智能大厦中进行。该企业在外地另开设有两家分公司,由总公司进行统一管理和部署。目前,该企业网络的拓扑结构如图 1-1 所示,基本情况如下。

(1) 在当前网络中,所有的网络设备使用的均为 Cisco 的产品,接入层交换机为 Cisco Catalyst 2960,汇聚层交换机为 Cisco Catalyst 3750,核心层交换机为 Cisco Catalyst 4506,防火墙为 Cisco ASA 5540。

(2) 服务器所使用的操作系统平台为 Windows Server 2003 和 Windows Server 2008,其中以 Windows Server 2008 为主。

(3) 接入 Internet 方式采用 100M 光纤方式。现有接入用户数量为 500 个,客户端均使用私有 IP 地址,通过路由器地址转换接入 Internet。部分服务器 IP 地址为共有 IP 地址。

(4) 局域网覆盖整个厂区,中心机房位于智能大厦的第 3 层(共 15 层),职工宿舍楼和生产车间均有网络覆盖。

(5) 客户端操作系统采用 Windows XP Professional 和 Windows Vista,其中以 Windows XP Professional 操作系统为主。除部分客户端需要连接 Internet 外,其他客户端均只在局域网内通信使用。

(6) 会议室、产品展示大厅等公共场所部署无线接入点,实现随时随地无线漫游接入。

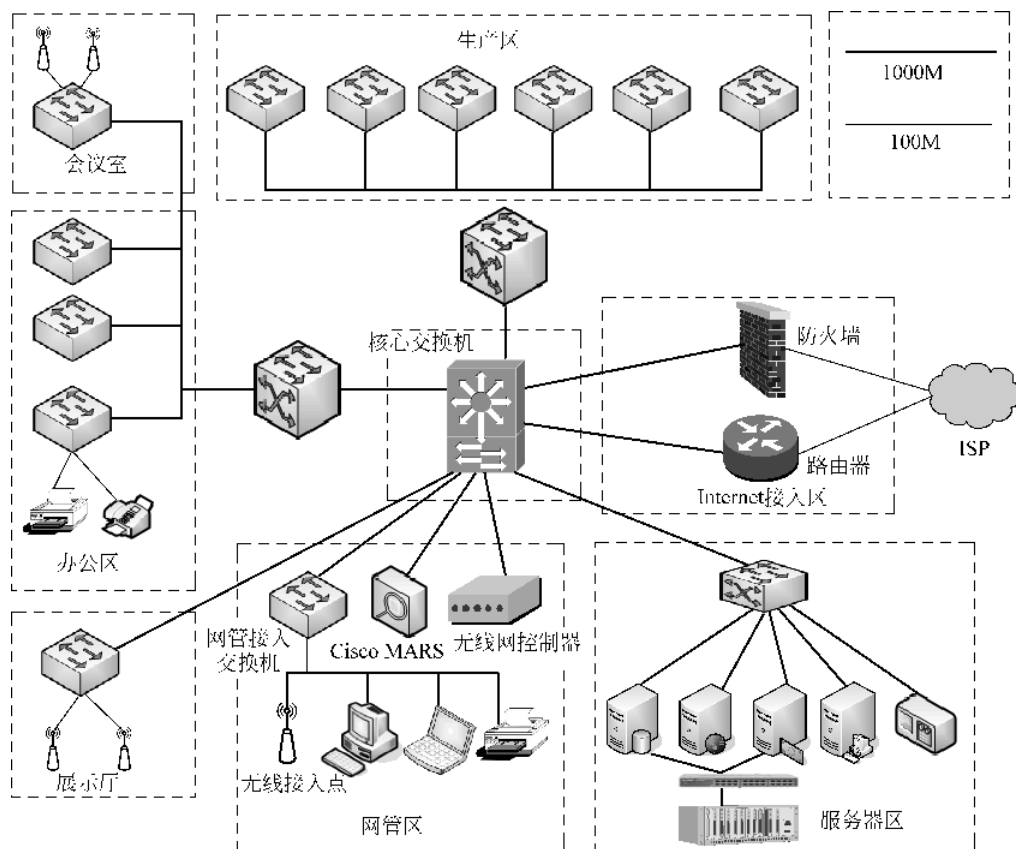


图 1-1 网络拓扑结构

1.2 项目需求

随着企业的日益发展,网络也在不断地发展,随之网络管理的难度也在提高。因为企业只有为数不多的几个管理员,并且各管理员之间的分工不同,即每个管理员分别管理网络的不同部分。因此,更加合理地、统一地管理网络也是管理任务所必需的。

针对当前网络的管理,具有如下需求。

(1) 服务器管理需求。因为服务器特殊性的原因,对服务器的管理必须由专人负责,从而保证其正常、安全地工作。作为管理任务之一,管理员还应时时关注服务器的运行状况。

(2) 网络设备管理需求。网络设备是网络通信的神经中枢,任何一个设备发生故障,对于与之相关的计算机而言都是致命的。

(3) 客户端管理需求。客户端计算机是网络的主要组成部分,用户所有的需求都需要通过客户端实现。另外,由于多数客户端计算机的使用者都无法像管理员般注重计算机的安全,所以客户端的安全性也是不容忽视的。

(4) 网络管理需求。只有将计算机接入网络,才能真正地发挥网络的作用,对于网络的管理包括网络链路、网络协议和资源等。

(5) 网络安全管理需求。网络安全是每个管理员所必须面对的问题,安全问题也是最

难管理的工作之一。

(6) 故障管理。无论是硬件还是软件都不可能保证永远不出问题,任何一种设备或网络的组成部分都有发生故障的可能。

1.3 项目分析

通过对各部分的管理分析,可以清楚地了解各部分所需要的管理内容。针对于当前网络的项目需求,具体分析如下。

(1) 服务器管理。因为服务器的管理所涉及的内容比较多,从而使服务器的管理难度比较大。通常情况下,服务器的管理包括如下几方面内容: Windows 系统管理、Windows 系统性能管理、Windows 系统安全管理和 Windows 网络服务管理等。

(2) 网络设备管理。网络设备的管理不单单是设备硬件的管理,软件的管理同样重要。通常情况下,网络设备软件是网络实现各种功能的基础,例如 VLAN 技术的使用。在设备购买后,均需根据网络的需要,进行相关的配置。对于已经可以正常使用的设备,则需要将其配置文件进行备份,在设备软件发生故障时,使用该备份文件进行恢复。

(3) 客户端管理。对于客户端的管理,如果需要通过实现统一管理的目的,则需要将客户端加入到企业域中,然后再进行相应的管理。

(4) 网络管理。网络管理包括网络链路的管理、网络流量及监控与分析两部分内容,只要网络中的计算机进行通信,就会在网络中产生流量,其中还可能会存在不允许的流量,因此,如果不对网络流量进行管理,其混乱程度是可想而知的。

(5) 网络安全管理。网络安全由多个部分组成,包括 Windows 系统安全管理、网络设备安全管理、网络安全管理、客户端安全管理等。

(6) 故障管理。正如 1.2 节所说,故障的发生是不可避免的,如何才能将因为故障而造成的损失降到最小,才是最为重要的。网络中的故障主要分为服务器故障和网络设备故障,其中服务器故障主要是系统故障。

1.4 项目规划

通过 1.3 节对网络项目的分析,可以对网络的不同组成部分进行相关的管理规划,使管理员的管理工作更加有秩序,使管理员的管理效率更高。

1.4.1 服务器管理规划

根据对本项目服务器管理的分析,服务器管理分为如下几部分内容。

1. Windows 系统管理

Windows 系统管理主要是管理与系统运行相关的内容,其中包括磁盘和分区管理、系统服务管理、网络服务管理、进程管理、任务管理、用户管理、网络配置与协议管理、远程管理等。

2. Windows 系统性能管理

Windows 系统性能管理的目的是保证服务器的性能或提高服务器的性能,使服务器可

以更好地提供服务。为了提高服务器的性能,首先应选择合适的操作系统软件,其中 Windows Server 2008 Server Core 操作系统是 Windows Server 2008 系列操作系统中占用资源相对较少的服务器操作系统。其次,对于安装图形界面的操作系统,应关闭不需要的图形化特效,以提高服务器的性能。最后,作为管理员还应随时关注服务器的运行情况,使用可靠性和性能监视器,可以随时监控服务器的性能和可靠性指数。

3. Windows 系统安全管理

Windows Server 2008 提供了一系列新的和改进的安全技术,这些技术增强了对操作系统的保护,为企业的运营和发展奠定了坚实的基础。使用安全配置向导,可以通过向导的方式增强系统的安全性。通过配置服务器的本地安全策略,从而提高本地计算机的安全级别。

另外,在 Windows Server 2008 系统中,日志系统是一个非常重要的功能组成部分。通过“事件查看器”中的事件日志,可以收集关于硬件、软件和系统问题的信息。

4. Windows 网络服务管理

服务器的作用是为网络提供所需的服务,该功能的实现需要在服务器上安装相应的角色服务,只有安装了相应的角色服务后,服务器才能够为网络提供相应的服务。在 Windows Server 2008 操作系统中,服务器角色及角色服务的安装都可以在“服务器管理器”窗口中实现。对于服务器角色的管理,则可以通过不同的服务器角色提供的独立管理单元,或在 MMC 控制台中统一管理。对网络服务稳定性要求较高的服务,则可以通过故障转移群集技术实现,例如文件服务器。网络访问量比较大的服务,则可以通过网络负载平衡技术实现,例如 Web 服务器。

另外,网络服务的日常监控也是不容忽视的工作之一,这部分工作可以在网络中部署网络服务监控软件,使其 7×24 小时监控服务器。

1.4.2 网络设备管理规划

网络设备主要是指交换机、路由器和防火墙,这些设备都是网络运行所必不可少的,缺少任何一部分都无法完成正常的网络要求。

1. 管理方式的选择

虽然网络设备拥有自己的操作系统,但却不像真正的计算机一样拥有输入/输出设备,即网络设备的管理需要借助计算机来实现。通常情况下,管理网络设备的方式包括如下几种:超级终端方式、Telnet 方式、Web 方式和网络管理软件方式。

2. 网络设备的初始化配置

任何网络设备在出厂前,生产商都已经对网络设备进行简单配置,这些配置是达不到用户的使用需求的,例如,无论使用的是何种级别的交换机,如果用户不进行任何配置都只能被用作二层交换机。

3. 配置文件的管理

通常情况下,在网络设备配置完成后,是不会发生改变的,根据管理员的日常工作原则,需要将所有的配置文件进行备份。另外,由于配置文件可以上传到其他设备运行,所以通过备份配置文件,还可以防止在设备发生故障时,使用该设备取代当前设备。需要注意的是,并不是所有的配置文件都是通用的,只能是相同厂商的设备才能实现该功能,这里所指的设

备均为 Cisco 厂商的网络设备。

4. 网络管理软件

使用网络管理软件,可以减少管理员的管理任务,因为管理软件所使用的都是图形化管理,与使用超级终端和 Telnet 方式相比要简单得多。最主要的原因是使用网络管理软件可以很直观地查看网络设备的监控结果。

1.4.3 网络流量管理规划

网络流量是网络必不可少的组成部分,但如果网络中存在大量的非法数据时,则会降低网络的稳定性,此时,则需要管理员了解网络中流量的具体情况,并采取相应的措施。

1. 网络带宽的监控与分析

网络带宽会在网络的使用过程中出现老化现象,当老化比较严重时,同样会影响网络的正常运行,即在网络使用中管理员非常有必要定期对网络带宽进行测试。同样,受外界环境影响较大的无线网络也应进行必要的监控和分析。

2. 网络流量的监控与分析

当网络中存在大量的流量时,会直接降低网络设备的性能,并导致整个网络的性能下降。例如网络中存在使用 P2P 软件的用户等。为了杜绝这种情况的发生,管理员需要实时监控网络流量情况,当网络性能突然下降时,则可以第一时间查看是否是由网络流量过大所引起的,并采取相应的应对措施。

3. 网络吞吐量分析

吞吐量是指在无帧丢失的情况下,设备能够接受的最大速率。在测试中以一定速率发送一定数量的帧,并计算待测设备传输的帧,如果发送的帧与接收的帧数量相等,那么就将发送速率提高并重新测试;如果接收帧少于发送帧则降低发送速率重新测试,直至得出最终结果。在实际操作中,这些操作均是由软件后台操作完成,管理员只需进行测试前的设置,以及查看测试结果。

1.4.4 网络链路管理规划

常用的网络链路包括双绞线、光纤和电磁波,在当前网络中,除布线困难的地域,其他链路均采用双绞线或光纤。当网络链路发生故障时,可以通过测试工具分别对物理链路和逻辑链路进行测试。

1. 网络物理链路测试

物理链路的测试,通常需要借助于物理链路测试工具,双绞线链路的测试可以使用 Fluke MircoScanner² 或简易网络测试仪等。而光纤链路的测试,则可以通过光纤链路测试工具。

2. 网络逻辑链路管理

网络逻辑链路的测试,则可以使用 Windows 自带的工具进行测试。Windows 自带的工具包括 IP 网络连通性测试工具(Ping)、路径信息提示工具(Pathping)和测试网络路由路径工具(Tracert)。

1.4.5 网络安全管理规划

当前计算机网络是充满恶意攻击者的网络,恶意软件使用与 E-mail、文件传输、Web 访问和实时合作之间的无缝通信相同的计算机网络技术,进而针对计算机弱点进行攻击。

1. 网络设备安全

正如 1.2 节所述,网络设备是网络的中枢神经,保证网络设备的安全也是保证网络安全的重要组成部分。通常情况下,网络设备的安全需要通过设备的配置完成,例如配置交换机的保护端口、流控制,在路由器上配置 IP 访问列表、MAC 访问列表等。

2. 网络安全设备

随着用户信息安全意识的逐渐加强,安全设备也越来越受到人们的重视,不过,简单的防火墙已难以满足基本安全防御需求。网络安全设备的目的并不是用来挽救或保护已经受到入侵的用户,而是防患于未然,最大限度地避免可能发生的安全侵害。常用的 Cisco 安全设备包括网络防火墙、入侵检测系统和入侵防御系统,这些设备分布在网络中的不同位置,可以为整个网络或重点对象提供更可靠的保护。

3. 客户端安全

对网络客户端进行必要的甚至是严格的安全控制和管理是保障网络正常、高效、安全运行的重要措施。在局域网环境中,普通客户端计算机的安全设置包括锁定计算机、设置高强度密码、配置 Windows 防火墙和启用系统更新等内容。

1.4.6 客户端管理规划

客户端是用户使用网络的基础,只有在保证客户端正常运行的前提下,用户才能更高效地完成日常工作。为了保证客户端的安全,可以从以下几方面内容进行操作。

1. 系统更新管理

Windows 系统漏洞可谓屡见不鲜、层出不穷,而且其危险性和危害性也是越来越大。因此,及时更新系统补丁、修补系统漏洞,保证 Windows 系统安全,就成为网络管理人员的当务之急。

2. 网络接入管理

接入网络的方式包括有线接入和无线接入,使用有线接入方式,即使用双绞线或光纤,直接将线缆的两端分别接入交换机和客户端的网卡即可。而对于无线网络接入方式,则因所用的无线网卡不同,配置方法也有所不同,通常可使用 Windows 配置程序和所使用无线网卡提供的配置程序进行配置。

3. 组策略管理

组策略(Group Policy,GP)是系统管理员为计算机和用户定义的,用来控制应用程序、系统设置和管理模板的一种机制。在当前网络中,首先,可以通过组策略定制客户端的用户环境,从而使所配置的用户使用相同的用户环境。其次,通过配置组策略,限制客户端计算机所使用的硬件。另外,使用组策略还可以在客户端计算机上部署软件,从而减少管理员为客户端安装软件的工作。

1.4.7 故障管理规划

发生故障的概率虽然可以通过管理员在日常工作中降低,却不能完全防止故障的发生。因此,如何在故障发生时及时发现故障并解决故障才是故障管理中的重点。

1. 系统故障诊断与排除

Windows Server Backup 是 Windows Server 2008 的备份与恢复组件。备份与恢复是保证信息系统安全可靠不可或缺的基础。对信息系统来说,可靠性和可用性是最基本的要求。另外,Windows Server Backup 支持图形模式和命令行模式,对于域控制器的备份而言,既可以支持域控制器完整备份,同时也可以支持组件备份。

2. 网络设备故障的诊断与排除

网络故障是一件令人头痛而又不得不面对的难题。对于局域网络而言,网络故障大致可以分为 4 类,即链路故障、配置故障、协议故障和服务器故障。链路故障通常是由于接插件松动或设备硬件损坏所致,而其他故障则往往由人为的设置所致。

Windows 系统管理

Windows Server 2008 是微软推出的强大、安全、易用的网络操作系统。不仅继承了 Windows Server 2003 的安全性、可管理性和可靠性,而且还融合了易用性、人性化、智能化,并在此基础上提供了更丰富的功能和更稳定的内核,非常适合于中小型网络中的各种网络服务,尤其适合那些没有经过专业培训的非专业管理人员使用。

2.1 Windows 系统管理规划

Windows 系统是实现所有功能的基础,无论是网络功能还是本地功能,这也是为什么必须保证 Windows 系统正常工作的原因。

2.1.1 项目背景

在当前网络中,几乎所有计算机使用的操作系统均为 Windows 操作系统,其中服务器主要使用两种操作系统,分别为 Windows Server 2003 和 Windows Server 2008。为使网络用户可以在服务器上存储某些数据,所有服务器均安装有多块硬盘及 RAID 卡。对于服务器操作系统,除拥有多个系统服务外,还包括多个网络服务,因此对服务器服务的管理不仅要管理系统服务还要管理网络服务。进程是服务器当前正在计算的内容,当进程过多时,会影响服务器的整体性能,因此需要关闭不必要的进程。

2.1.2 项目需求

对于 Windows 系统管理需要完成以下要求。

(1) 在网络中,除专用的存储设备外,服务器通常也会承担部分数据存储任务。对于这些数据,则同样需要保证其安全与稳定。

(2) 默认情况下安装的系统服务,可能并不适用于当前的网络。

(3) 对于网络服务的管理,在当前网络中要求实现统一管理的目的。

(4) 每一个服务器运行的程序都会创建一个或多个进程,并通过这些进程实现所需的功能,因此,对进程的管理在系统管理过程中也是不可或缺的。

(5) 对于某些特定的任务,需要在特定的时间自动完成。

(6) 用户和组管理是网络的重要组成部分,需要管理员严格管理网络中的用户和组。

(7) IP 地址和网络连接是服务器连接网络的基础,正确的配置是确保其正常接入网络

的基础。

(8) 对于服务器管理而言,通常会部署在网络中的特定位置。

2.1.3 解决方案

针对当前项目的 Windows 系统管理要求,可通过如下方式实现。

(1) 为了实现服务器存储的安全性和稳定性,可以在服务器安装 RAID 卡,使用 RAID 技术来实现。对于需要在服务器上存储数据的用户,为了防止用户无休止地使用硬盘空间,可以通过设置磁盘配额来实现。

(2) 对于不是系统所必需的服务,通常情况下需要停止其运行。对于系统服务的启动与停止可以通过命令行和 MMC 控制台这两种方法实现。

(3) 对于统一管理网络服务的要求,可以通过在加入域中的计算机上使用 MMC 控制台实现,在 MMC 控制台添加多个想要管理的网络服务管理组件即可。

(4) 对进程的管理主要包括查看进程并将无用的进程和所怀疑的非法进程结束,该工作可以通过 `tasklist` 和 `taskkill` 命令实现。

(5) 当在网络中需要在指定时间完成特定的任务时,可以通过 Windows 系统提供的任务计划功能实现。

(6) 用户和组的管理需要根据网络与企业的实际需求进行,通常情况下,为了便于管理需要将用户添加到不同的组中,并对组进行权限设置。

(7) 网络连接的管理主要是服务器的 IP 地址管理和接入网络的方式管理,通常情况下,服务器都会接入固定的网络中,并使用固定的 IP 地址信息。当服务器使用拨号方式连接网络时,则还应创建所需的网络连接。

(8) 对于服务器的管理不会每次均要实现与服务器的面对面管理,通常可采用远程管理的方式实现。

2.2 磁盘和分区管理

在 Windows 操作系统中,数据都保存在磁盘中,并以分区或卷的形式作为目录结构的顶级。另外,为了提高数据的读取速度和保证数据的安全,服务器磁盘通常还会使用 RAID 技术,针对于不同的环境要求所使用的 RAID 类型也有所不同。

2.2.1 RAID 卡管理

一般情况下借助 RAID 控制卡实现硬 RAID,而如果资金不足,则可借助操作系统来实现软 RAID。这里以 Dell PowerEdge 2650 为例介绍 RAID 卡的设置,不同 RAID 卡的设置方式有所区别,请注意查看 RAID 卡的使用手册。

(1) 打开计算机电源,当显示图 2-1 所示的信息时,按 `Ctrl+M` 键,进入 RAID 卡设置界面。

(2) 使用方向键,依次选择 `Configure`→`Easy Configuration` 选项,如图 2-2 所示,并按 `Enter` 键,实现 RAID 卡的快速配置。

注意: 如果该计算机以前配置有 RAID,那么,在配置新的 RAID 之前,应当先使用 `Clear Configuration` 命令删除。RAID 删除后,硬盘中保存的所有数据将全部丢失。

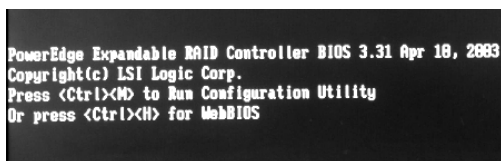


图 2-1 提示 RAID 卡设置组合键

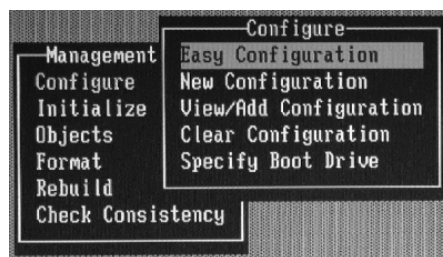


图 2-2 采用 Easy Configuration 方式

(3) RAID 卡搜索并显示该计算机中安装的所有硬盘驱动器,如图 2-3 所示。

(4) 使用方向键选择欲添加至 RAID 的磁盘,然后,按空格键选中,将该硬盘添加至 RAID 阵列,如图 2-4 所示。

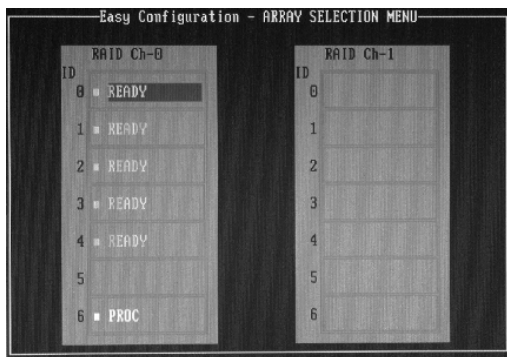


图 2-3 显示所有的硬盘驱动器

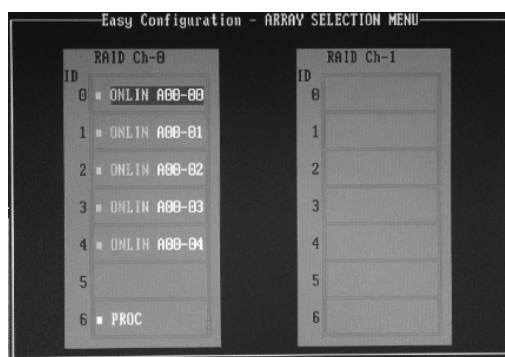


图 2-4 选择欲添加至 RAID 的磁盘

注意: 若欲设置 RAID 5,为了最大限度地提高磁盘空间利用率,应当将所有的磁盘都加入至 RAID。若欲设置 RAID 1,则需要添加两块硬盘。

(5) 按 Enter 键,显示图 2-5 所示的页面,使用方向键移动光标选择欲配置的阵列。如果只使用了一个通道,那么,应当选择 Span-1 选项。

(6) 按 F10 键,显示图 2-6 所示的页面,选择欲使用的 RAID 级别。当计算机安装有 3 块以上硬盘时,系统默认的级别为 RAID 5。

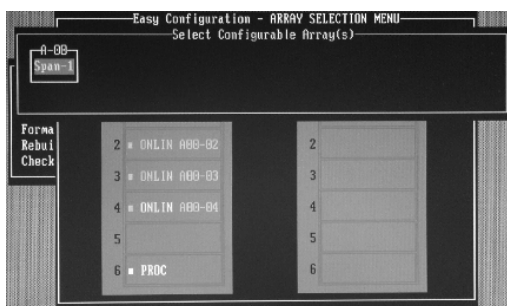


图 2-5 选择 RAID 卡通道

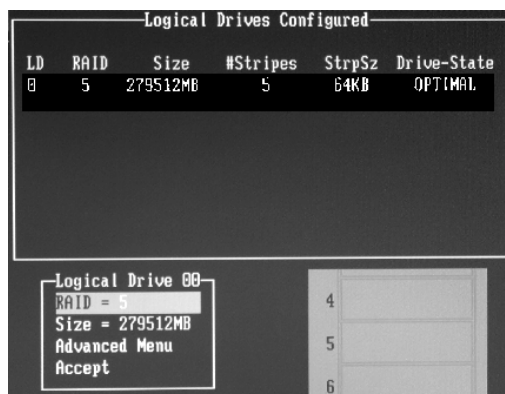


图 2-6 选择 RAID 5 级别