Web与无线
实用技术译丛

在Windows 2000上构建Cisco网络

许多人都在为Cisco和Windows 2000网络的规划和运行绞尽脑汁。本书将清晰地介绍Cisco针对Windows 2000活动目录的网络服务（CNS/AD）。从此这些问题将会迎刃而解了！

(美) Melissa Craft
Elliot Lewis 著

朱剑平 郭宁宁
李 季 张 静 译

科学出版社
www.sciencep.com

Web 与无线实用技术译丛

在 Windows 2000 上构建 Cisco 网络

（美） Melissa Craft
Elliot Lewis 著

朱剑平 郭宁宁
李 季 张 静 译

科学出版社

北 京

图字：01-2002-6694

内 容 简 介

本书系统介绍了在 Windows 2000 系统上构建 Cisco 网络的全过程。全书分为 12 章，按照案例实施的顺序分别介绍了 Windows 2000 的网络特性、Cisco 硬件及其 IOS 基本知识、网络协议和组网的概念、路由和远程访问、Windows 2000 网络体系的设计和调整、Cisco 路由器和交换机的应用以及 Windows 2000 服务器的实施。全书每章后都有内容小结和常见问题解答，供读者参考。

本书内容翔实丰富，权威性强，适合高级系统管理人员使用，也可供其他相关人员参考。

图书在版编目（CIP）数据

在 Windows 2000 上构建 Cisco 网络 / （美）克拉夫特（Melissa，C.）等著；朱剑平等译. —北京：科学出版社，2003
（Web 与无线实用技术译从）
ISBN 7-03-011554-6

Ⅰ.在… Ⅱ.①克… ②朱… ③汪… Ⅲ.计算机网络—操作系统（软件），Windows 2000 Ⅳ.TP316.86

中国版本图书馆 CIP 数据核字（2003）第 041489 号

责任编辑：袁永康 / 责任校对：都 岚
责任印制：吕春珉 / 封面制作：一克米工作室

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2003 年 6 月第 一 版 开本：787×1092 1/16
2003 年 6 月第 一次印刷 印张：23 1/2
印数：1—4 000 字数：534 000

定价：42.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

前　言

在风起云涌的网络时代，Microsoft 和 Cisco 以其领先的技术和辉煌的业绩成为业界两颗耀眼的明星。

Microsoft 作为软件供应商，提供的是操作系统和商用及个人应用程序。Cisco 是一家硬件方面的原始设备制造商，主要产品是互联网络设备和互联网络操作系统。互联网络主要是以企业为基础。然而，Internet 已经解除了对个人应用的限制，因此，每个用户都可通过互联网与企业进行各式各样的交易。

随着 Internet 的到来，在网络中移动数据的需求也急剧增加。企业和个人都希望能够连接到 Internet 上。Cisco 和 Microsoft 在各自的产品方面都十分注重 Internet 集成战略。他们的战略覆盖了 Internet 用户（包括企业和个人）所希望的大多数服务。Cisco 和 Microsoft 都支持网际协议（Internet Protocol，IP），并基于 IP 协议来连接 Internet。

用户出于个人娱乐的目的而访问 Internet 的次数也在急剧增加。已经有企业正在提供这样的娱乐服务和产品。Internet 娱乐列表还在不断增加中——您可以从 Internet 上找到下面这些或更多的服务：

- 电视节目转播
- 电影点播
- 音乐文件下载

由于娱乐节目中包含着多媒体成分，因此需要更高的带宽和流式的数据才能正常地播放。服务质量（Quality of Service，QoS）是用来保证更高的带宽和不间断数据流的技术之一。Cisco 的互联网络操作系统（Internetwork Operating System，IOS）和 Microsoft 的 Windows 2000 都提供了 QoS。本书将用几章的篇幅来讨论 QoS。

由于用户还要使用 Internet 进行语音通信，因此要用到个人网络电话（Net Phones）和用于企业的 PBX 及语音邮件应用程序。语音通信是 Internet 应用的高端领域，可以全部或部分地节省长途费用从而缩减成本。一般来说，个人或企业都能够因这项技术而节约成本，因为他们可以使用连接到 Internet 的本地连接来替代公共电话网上的长途电话。Cisco 的 IOS 和 Microsoft 的 Windows 2000 所包含的 Voice-over Internet Protocol（VoIP）和电话应用程序都可用在 Internet 上提供语音通信。本书将讨论这两种技术。

没有 World Wide Web 的 Internet 将会是什么样子？Internet 的主要使用方式是下载超文本标记语言（HyperText Markup Language，HTML）页面及其内容。在 HTML 出现之前，Internet 主要用于收发电子邮件、文件传输或网络新闻。Windows 2000 提供了所有这些服务，而使用 Cisco IOS 更可以高效地管理这些服务。您将会在本书中学习这些知识。

当个人用户面临着 Internet 带宽消耗和技术方面的限制时，企业也面临着一个新的问题——用户的管理。企业不仅要管理自己所服务的用户，更大的挑战是管理给网站用户所提供的数据。当访问者登录网站时，企业要意识到如果他们接收了私人的数据，那

么他们还会再次访问。为了跟踪此数据，需要一个目录服务来存储用户的信息、个人喜好和兴趣。Windows 2000 提供了一种名为活动目录（Active Directory）的 LDAP 兼容目录服务。该活动目录可从基于 TCP/IP 的网络上进行访问，包括 Internet。目录服务在将来可以进行扩展，包含关于网络系统、网络资源和信息的所有类型的信息。同样，本书将介绍活动目录的基础知识。

本书的独特之处在于介绍了 Cisco 和 Microsoft 各自的技术，以及对这两家公司的技术进行综合应用的知识。如果你面对着一个同时使用了 Cisco 设备和 Microsoft Windows 2000 的网络，那么可以从本书中得到很多有用的帮助。

本书是为高级系统管理员编写的。书中包含的一些概念需要读者具备网络、Windows NT 和数据路由的知识。本书在第一章提供了一些基础知识，如果您已经掌握了网络互联技术，那么请跳过第一章，或者快速浏览一下即可。

本书除了介绍技术本身、技术的优点和实现方式，还在每一章的最后安排了一个附加的小节，名为“案例分析”。这个小节将讨论两家不同的公司，以及他们的商业需求和现有的网络，然后会把本章所讨论的主要概念应用于每家公司。每章的案例分析都会使用相同的两个虚构公司。这些小节将提供 Cisco 和 Windows 2000 技术的实际应用情况。除了技术的实现，还讨论了每一家公司的互联网络的设计方法。

本书的最后是名为“内容速查”的一章。此章将把全书所介绍的主要概念汇总在一起。如果您想查阅前面的某个概念，可首先翻到这一章。如果您已经读完了全书，并且没有复习一遍，那么本章将是学习 Cisco 和 Microsoft 技术的最好的一章。

希望您能够从本书中找到一些有价值的东西，希望本书有助于您设计、实现和管理 Cisco/Microsoft 网络。

目　录

第 1 章　开发 Windows 2000 和 Cisco 互联网络

本章内容

- 目录驱动的网络（DEN）
- Windows 2000 概述
- Cisco IOS 概述
- 联网基础知识
- OSI 参考模型

1.1　概　　述

Microsoft 和 Cisco 是当今信息产业界两个最大的技术供应商。Windows 2000 是 Microsoft 的网络操作系统（network operating system，NOS），同时 Cisco 也正在向网上路由和交换语音、视频、数据等领域进军。此外，为了使用目录驱动的网络（directory enabled networking，DEN）将两者的系统进行集成，Microsoft 和 Cisco 还进行了合作。通过融合两者的技术，Microsoft 和 Cisco 都希望 DEN 能够成为未来全球化互联网络的主流。通过使用两者的目录软件产品，DEN 实现了 Microsoft/Cisco 互联网络的结合，现在任何机构都可以享受到 DEN 所带来的好处。

1.2　目录驱动的网络（DEN）

DEN 是 Cisco 和 Microsoft 合作的产物。他们开发出 DEN 规范的基本框架，并提交给分布式管理任务组（Distributed Management Task Force，DMTF）和 Internet 工程任务组（Internet Engineering Task Force，IETF）进行标准化。

为什么 Cisco 和 Microsoft 要提出 DEN 的概念呢？因为他们发现，尽管大多数网络操作系统和应用程序都支持目录服务，但是大多数目录服务都是专用的。以 Novell 的 NetWare 为例，先前的 NetWare 服务器自己有一个名为 bindery 的目录服务，而且每个服务器的目录服务都相互独立。用户必须将用户帐户信息输入到每一台要访问的服务器中。

要使多台服务器中用户帐户信息和密码（甚至仅仅用户帐户名本身）保持同步是很困难的。Novell 认识到该问题，并在 20 世纪 90 年代中期发布了 NDS（Novel Directory Services），当时的名称是 NetWare Directory Services（NetWare 目录服务）。NDS 是一个专用的目录服务，可供多个 NetWare 服务和 NetWare 应用程序访问。只需将用户帐户输入到 NDS 目录中一次，用户即可获得访问该 NDS 目录中任何服务器和资源的权限。

在一个公司中，要想目录服务能够良好地运行，该目录服务就必须是开放的，应该能由网络中的不同操作系统进行访问。如果一个目录服务是开放的（正如 DEN 标准所给出的那样），那么该目录服务就会包括用户帐户访问权限的相关规则。其结果就是网

络管理费用的大大降低。用户只需要记住一个用户 ID 和密码，管理员也只需在一个目录下维护信息。

互联网络正变得越来越复杂。由于网络操作系统提供的 Web 服务、不断更新的技术，以及数据库也被集成用以创建新的电子商务系统，互联网络也随之扩展，包括了新的介质类型、多种协议、很多不同的设备类型，以及大量的服务。在公司里，各业务部门的经理需要新的功能特性以提供电子商务服务，而 IT 部门的任务就是减少网络技术的整体成本，因此，他们之间必然会产生矛盾。IT 部门同时还将面临专用的管理程序和无法进行互操作的数据库系统，这两种情况会对增加新的网络服务造成困难，或者导致整体费用的上升。图 1-1 给出了这种分离系统的示例。

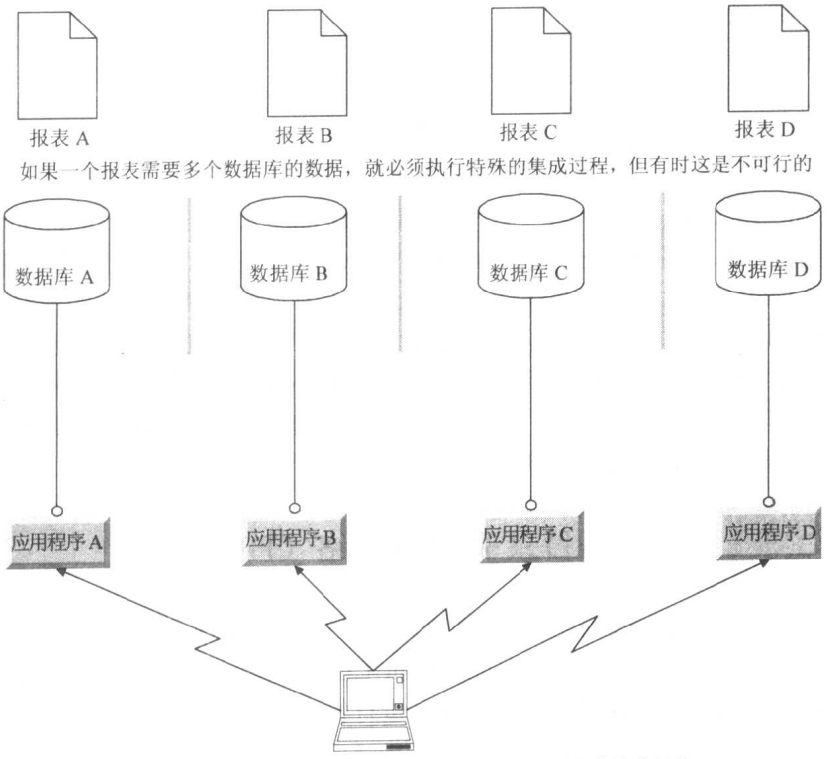

图 1-1 应用程序专用的独立数据库限制了互操作性

DEN 为企业管理者和软件商共同面临的问题提供了一种解决方案。下面是企业管理者和软件商所面临的问题：

- 如何集成新的电子商务系统？
- 如何针对特定用户加入服务级协议？
- 如何应用和管理各种策略？
- 如何集成管理“孤岛”（即独立的网络管理单元和网络管理系统）？
- 如何直接获得系统的互操作性？
- 如何获得可适用于整个网络的高级服务？

通过定义目录服务，DEN 可以解决这些问题，如图 1-2 所示。DEN 可以实现：

- 电子商务系统、介质、设备和协议的集成
- 服务级别与用户及应用程序管理的结合
- 策略的应用和管理
- 可扩展的管理应用程序与目录的集成，以实现网络管理的集中化
- 通用协议、通用应用程序编程接口（application programming interfaces，API），以及通用信息仓库的利用，以确保互操作性
- 配置、访问控制、安全性以及 QoS 措施等高级服务

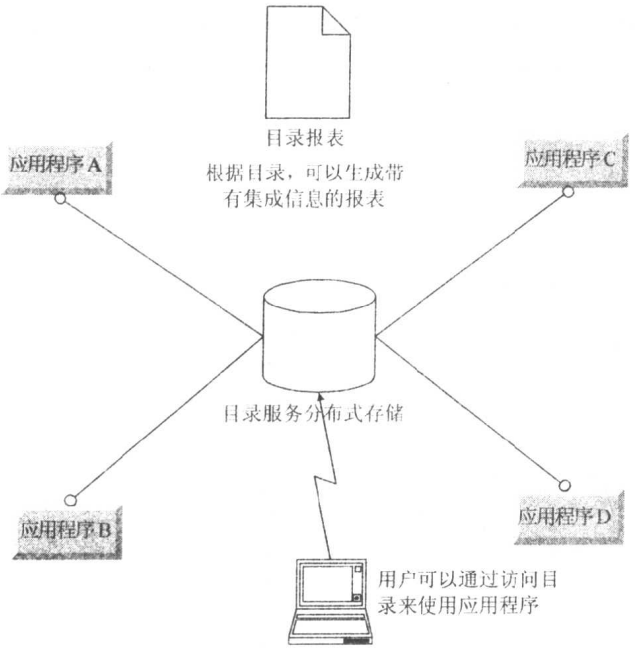

图 1-2　目录驱动网络的体系结构

DEN 利用数据库来集中管理网络系统和服务。它为网络单元和服务定义了一个通用的架构，并使得它们之间可以进行互操作。DEN 为网络单元定义了一个面向对象的信息模型，名为目录（directory）。在目录中，网络单元被定义为类（class）。网络单元（或者说类）并不仅仅局限于设备和用户帐户，它还包括网络中所有可能的应用程序和系统。类由具有相同属性特征的对象（object）组成。任何单独的网络要素（如用户帐号、服务器、策略等）都代表了网络中的独立实体（如用户 Joe、服务器 1、安全策略 A 等）。每个对象都包含了一组属性（attribute）用以描述自己的特性。例如，用户的电话号码就可以是用户帐户的一个属性。

DEN 并没有定义类似于简单网络管理协议（Simple Network Management Protocol，SNMP）那样的管理协议，尽管该协议使得网络管理达到了一个新的级别。DEN 也没有定义类似于轻量级目录访问协议（Lightweight Directory Access Protocol，LDAP）那样的网络协议，尽管新的目录服务很可能会集成 LDAP。而且 DEN 也没有为数据库定义新的架构类型。DEN 本身并不是一个产品。

DEN 是构建目录驱动的网络服务和应用程序所需的基本要素的定义。它为目录服务定义了一个标准层次结构，并通过定义可扩展性来减少限制。使用 DEN 后，多个供应商的架构之间就不会产生冲突，而且网络设备的配置和管理也可以通过目录服务来完成。

在 DEN 的策略服务器模型中，网络设备使用标准协议来访问网络，如域名系统（Domain Name System，DNS）、动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）。网络设备将访问服务器或主机以尝试一项网络事务，该事务将查看目录服务（不管它是存储在本地，还是存储在其他服务器上）来获得可用的策略。

如果一个策略确实适用于网络事务，那么就会应用该策略。根据该策略，事务被允许执行（事务还要进行策略所要求的任何更改）或者被拒绝，如图 1-3 所示。

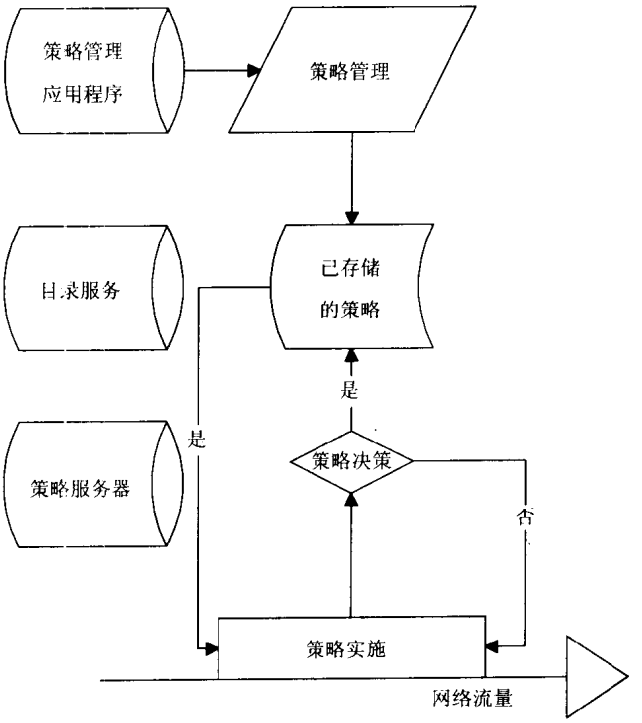

图 1-3 策略服务器模型

QoS 用于为特定类型的网络流量建立优先级别（或者取消优先级别），它取决于网络流量的发送时间、类型、源地址和目的地址。

下面来看一个例子：假设一位公司经理每个月都要通过互联网络召开一次视频会议直接听取报告，而他在各地巡视，在任何地方都可能召开视频会议。因此，在进行视频会议时，该经理不会使用相同的计算机和相同的 IP 地址。很多 QoS 产品都根据物理地址或 MAC 地址来标记流量类型的优先级。MAC 地址可以从 IP 地址或者利用地址解析协议（Address Resolution Protocol，ARP）解析计算机的主机名来获得。如果该经理希望视频会议获得比其他网络服务更高的优先级，那么网络管理员必须知道视频会议此时所用计算机的 IP 地址或主机名。而且，每次召开视频会议，管理员都要设法获得这些