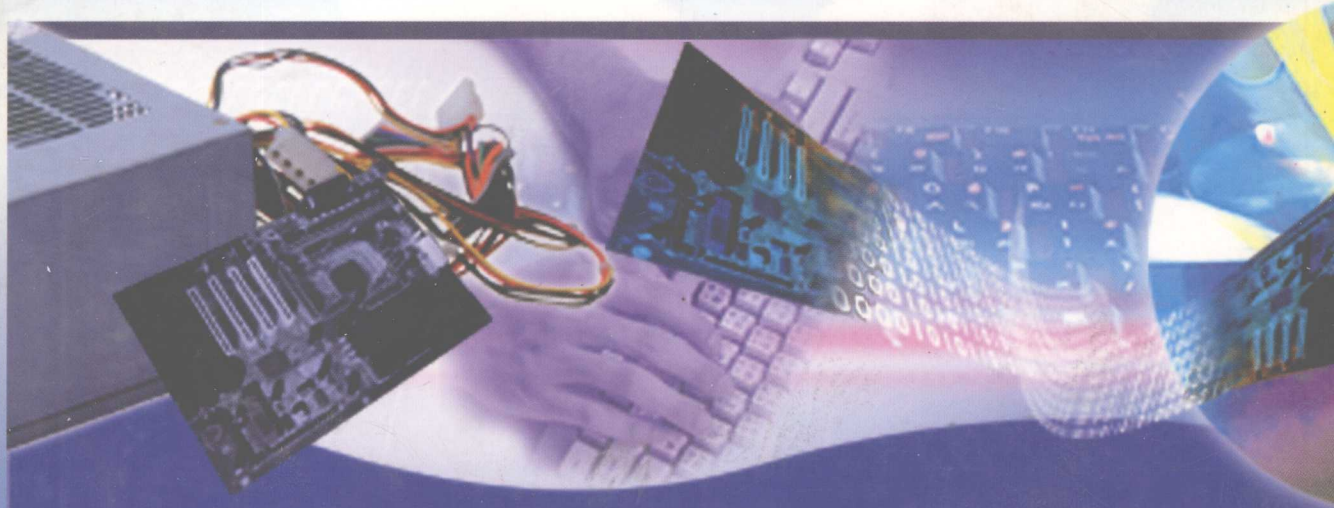
万水计算机组装与维护系列

Windows Server 2003

网络配置详解

陶英华　等编著



中国水利水电出版社
www.waterpub.com.cn

万水计算机组装与维护系列

Windows Server 2003 网络配置详解

陶英华　等编著

中国水利水电出版社

内 容 提 要

从 Windows Server 2003 开始，微软公司将操作系统的服务器版本和桌面版本分开，服务器版本统称 Server 系列，桌面版本统称为 XP 系列。这标志着 Windows Server 2003 在技术上是一次飞跃，在功能上较以前版本有着很大的提高。

本书从实用性的角度出发讲解了 Windows Server 2003 在实际工作过程中的网络配置方法，以丰富的截图演示了 Windows Server 2003 各项网络功能的详细配置方法。内容包括网络命令、DNS 服务器配置、活动目录服务配置、活动目录的管理、活动目录出错处理、组策略、文件服务器、DFS 服务器、Web 服务器、论坛聊天室的组建、FTP 服务器、邮件服务器、证书服务和 IPSEC 等等。通过本书的讲解，读者能够熟悉 Windows Server 2003 在企业内部网上的管理应用，在 Internet 网站组建上能够具备很强的技术水平。

本书适合 Windows Server 2003 的初学者、网络管理员、计算机教师以及 Windows Server 2003 的爱好者学习参考，在内容上兼顾初中级 Windows Server 2003 使用者。特别是对于网络管理员来说，它可以作为一本日常网络管理的参考书。

图书在版编目（CIP）数据

Windows Server 2003 网络配置详解 / 陶英华等编著. —北京：中国水利水电出版社，2004

（万水计算机组装与维护系列）

ISBN 7-5084-2335-6

Ⅰ. W… Ⅱ. 陶… Ⅲ. 服务器—操作系统（软件），Windows Server 2003 Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字（2004）第 087352 号

书　　名	Windows Server 2003 网络配置详解
作　　者	陶英华　等编著
出版　发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）　68331835（营销中心）　82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京市天竺颖华印刷厂
规　　格	787mm×1092mm　16 开本　27 印张　660 千字
版　　次	2004 年 9 月第 1 版　2004 年 9 月第 1 次印刷
印　　数	0001—5000 册
定　　价	45.00 元

前　言

Windows Server 2003 被微软称为有史以来最强大和最稳定的操作系统，虽然在发布以来也在不断发布补丁程序，但是用户在使用过程中确实感到了 Windows Server 2003 与 Windows 2000 有着很大的不同，包括新增了很多系统策略的应用，这些应用使管理员在网络管理过程中感到更加轻松。正因为如此，在 Windows Server 2003 中的网络配置有很多地方和 Windows 2000 不同了，所以采用以前的配置方法不一定能够成功。因为 Windows Server 2003 被设计用在广域网中，所以很多配置在一个广域网中才能讲解清楚。本书采用了笔者做过的系统方案来讲解 Windows Server 2003 中的网络配置，讲解时采用了四台路由器和一台中心交换机的网络硬件环境来模拟广域网环境。看过本书后，相信读者能够对 Windows Server 2003 有一个深刻的了解，能够在企业内部网管理上得心应手，在对外网站建设上具备一定的动手能力。

最后，要感谢我的妻子韩美琦，没有她的鼓励与帮助，笔者不可能完成本书。还要感谢翟宏颖，林小杰等同志在子网端为本书作截图。

目　录

第一章　网络和操作系统基础

1.1　Windows Server 2003 特点

Windows Server 2003 是微软公司的一系列产品。它们包括 Windows Server 2003 标准版、Windows Server 2003 企业版、Windows Server 2003 数据中心版和 Windows Server 2003 Web 版。

Windows Server 2003 系列产品继承了 Windows 2000 Server 的先进技术并且更易于部署、管理和使用。Windows Server 2003 系列产品包括有几个主要优点：

- 可靠性：据微软公司宣传，Windows Server 2003 是迄今为止速度最快、性能最可靠和使用最安全的 Windows 服务器操作系统，它用以下方式保证可靠性：
  - 提供集成结构，用于帮助您确保商业信息的安全性。
  - 提供可靠性、实用性和可伸缩性，可以建立用户需要的网络结构。
- 高效性：Windows Server 2003 提供了各种工具，帮助用户在部署、管理和使用网络结构的过程中获得最大效率。主要实现方式有：
  - 提供灵活易用的工具，使得用户的设计和部署与计算机的组织及网络要求相匹配。
  - 通过策略加强，任务自动化以及升级简化来帮助用户主动管理网络。
  - 让用户通过自行处理更多的任务来降低开销。
- 连接性：连接 Windows Server 2003 可以帮助用户创建业务处理方案的结构，方便用户与雇员、合作伙伴、系统以及客户更好地连接。主要实现方式有：
  - 提供集成的 Web 服务器和流媒体服务器，帮助用户快速、轻松和安全地创建动态 Intranet 和 Internet Web 站点。
  - 提供集成的应用程序服务器，帮助用户轻松地开发、部署和管理 XML Web 服务。（Extensible Markup Language，XML）
  - 提供多种工具，使用户得以将 XML Web 服务与内部应用程序、供应商以及合作伙伴连接起来。
- 经济性：与来自 Microsoft 的许多硬件、软件以及渠道合作伙伴的产品和服务相结合，Windows Server 2003 提供了有助于使用户的基础架构投资获得最大回报的选择。它通过以下方式来实现这一目的：
  - 为使用户得以快速将技术投入使用，对完整解决方案提供简单易用的说明性指南。
  - 利用最新的硬件、软件和方法来优化服务器部署，从而帮助用户合并各个服务器。
  - 降低用户的所属权总成本（TCO），使投资很快就能获得回报。

Windows Server 2003 标准版是为小型企业和部门使用而设计的，它提供的功能包括：智能文件和打印机共享、安全 Internet 连接、集中式的桌面应用程序部署、连接职员合作伙伴

和顾客的 Web 解决方案等。Windows Server 2003 标准版提供了较高的可靠性、可伸缩性和安全性，它充分利用了 Windows 2000 Server 技术，更易于部署、管理和使用。在较高级别上，Windows Server 2003 标准版提供以下支持：

- 高级联网功能，如 Internet 验证服务（IAS）、网桥和 Internet 连接共享（ICS）。
- 双向对称多处理方式（SMP）；
- 4GB 的 RAM。

针对大中型企业而设计的 Windows Server 2003 企业版，是运行某些应用程序的服务器推荐使用的操作系统；这些应用程序包括：联网、消息传递、清单和顾客服务系统、数据库、电子商务 Web 站点以及文件和打印服务器。Windows Server 2003 企业版提供高度的可靠性和优异的商业价值。它同时有 32 位版本和 64 位版本，从而保证了最佳的灵活性和可伸缩性。各组织可从优化了的高效结构中获益，这种优化是针对关系到业务的应用程序和服务而进行的。与 Windows Server 2003 标准版的主要差异是：支持高性能服务器以及将服务器群集在一起，以处理更大负载。这些功能提高了系统的可靠性，即确保无论是出现系统程序失败或是应用程序变得很大，其他系统程序仍然可用。在较高级别上，Windows Server 2003 企业版提供以下支持：

- 8 路对称多处理方式（SMP）；
- 8 节点群集；
- 32 位版本支持 64 GB RAM，64 位版本支持 64 GB RAM。

针对企业最高级别的可伸缩性、可用性和可靠性要求，设计的 Windows Server 2003 数据中心版为数据库、企业资源规划软件、大容量实时事务处理以及服务器合并提供关键的解决方案。它同时有 32 位版本和 64 位版本，从而保证了最佳的灵活性和可伸缩性。各机构可从优化了的高效结构中获益，这种优化是为了运行要求极为严格的应用程序和服务而进行的。与 Windows Server 2003 企业版的主要区别：支持更强大的多处理方式和更大的内存。另外，Windows Server 2003 数据中心版只通过 Windows Datacenter 项目提供，该项目提供了来自 Microsoft 和合格的服务器供应商（如原始仪器制造商（OEM））的硬件、软件和服务集成。在较高级别上，Windows Server 2003 数据中心版提供以下支持：

- 32 路对称多处理方式（SMP）；
- 8 节点群集；
- 32 位版本支持 64GB RAM，64 位版本支持 512 GB RAM。

Windows Server 2003 Web 版是单目的的 Web 服务器，专为需要以经济的方式建立及配置 Web 页、Web 站点及 Web 服务的机构设计。它为 Internet 服务提供商及致力于前端 Web 服务器的组织提供了一种经济且高效的 Web 服务器操作系统。Web 版是专门用于 Web 服务器而构建，它提供了 Windows 服务器操作系统的下一代 Web 结构功能。通过包含 Internet Information Services (IIS) 6.0、Microsoft ASP.NET 及 Microsoft .NET 框架提供了丰富的 Web 服务环境。Windows Server 2003 Web 版提供了以下优点：

- 为 Intranet 及 Internet 站点或网络集群主机提供了丰富的网络基本构架能力，以及 N-tier 应用配置——包括在 Internet Information Services (IIS) 6.0、Microsoft ASP.NET 和 Microsoft .NET 框架上的改善。
- 单任务的网络服务功能可支持对称多处理器（SMP）、2GB RAM、10 个会话消息块

（SMB）连接到网络。

- 迅速帮助用户建立并配置网页、网站及网络服务。

1.2　操作系统的作用

在进入 Windows Server 2003 网络的具体配置之前我们先熟悉一下计算机操作系统。

计算机由硬件系统和软件系统两大部分组成，它们构成了一个完整的计算机系统。计算机硬件是各种物理设备的总称，是完成工作任务的物质基础。计算机软件是指程序和与程序相关的文档的集合。通常，把未配置任何软件的计算机称为“裸机”。如果用户面对的是一台“裸机”，那么用户想要做的每一项任务都需要直接针对硬件进行，需要深入到计算机硬件里面去。比如针对磁盘的操作，用户就需要知道磁盘地址、内存地址、操作数和操作类型。这样一来，用户需要学会和必须记的东西就太多了，根本就无法把精力集中到要解决的问题上。所以，为了能够从繁重的硬件控制中脱身，合理有效地使用计算机，最好的办法就是开发一种软件，通过它来管理整个计算机，发挥计算机的潜在能力，达到扩展功能、方便用户使用。这就是“操作系统”产生的根本原因。由于操作系统隐蔽了硬件的具体细节，因此计算机在使用者眼中看来更简单和清晰，也可以说操作系统为用户和应用程序提供了一个使用平台。而在网络范围内，用于管理网络通讯和共享资源、协调计算机上任务的运行，并向用户提供统一、有效、方便的网络接口的程序集合，就称为网络操作系统。现今比较流行的操作系统大多数都是网络操作系统，如 Windows Server 2003、各种版本的 LINUX 系统以及 UNIX 系统等等。

整个操作系统的构成按照功能来划分可以分为四个部分。如图 1-1 所示。

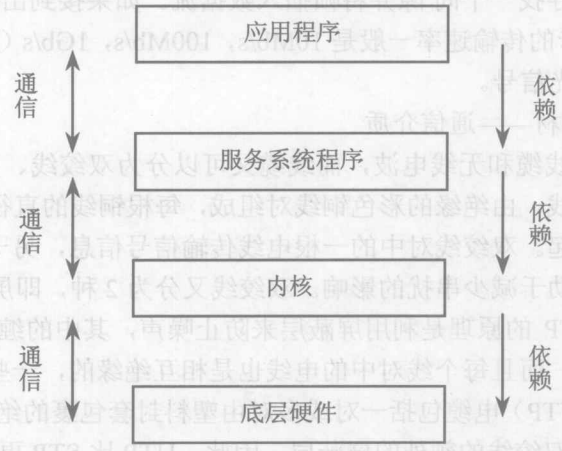


图 1-1　操作系统层次结构

（1）应用程序

在操作系统中，应用程序直接和用户进行交互，它包含各种不同的应用，比如图片浏览器、文本编辑器和邮件程序等。

（2）服务系统程序

服务系统程序其实也是应用程序的一种，但它们通常被看作是操作系统的一部分，如内存管理、设备管理和作业进程管理等。

（3）内核

内核的功能就是完成上述两种应用程序与硬件之间的联系和协调工作。

（4）底层硬件

底层硬件就是计算机系统的硬件设备。

操作系统的这四个部分是层层依赖的，并且只能和相邻层进行通信。

1.3 网络基础知识

（1）数据收发的门户——网卡

网络接口卡（NIC）是一种连接设备。简称网卡，它们能够使工作站、服务器、打印机或其他节点通过网络介质接收并发送数据。网卡也叫网络适配器，它是一种插在计算机主板上的提供网络接口的电路板，它们只传输信号而不分析高层数据，属于 OSI 模型（OSI 模型将在 1.8 节详细说明）的物理层。在有些情况下，网卡也可以对承载的数据做基本的解释。网卡有很多种，根据它所依赖的网络传输系统不同（如以太网与令牌环网）而不同，还与网络传输速率（如 10Mbps 与 100Mbps）、连接器接口（如 BNC 与 RJ-45）以及兼容的主板或设备的类型，制造商有关。不同类型的网络需要使用不同种类的网卡，不同速度的网络也需要使用不同的网卡。每一块网卡都有一个世界惟一的 ID 号，也叫 MAC 地址，这在网络中（包括局域网和广域网）用来标识计算机身份，从而实现不同计算机之间的通信。在计算机工作时，网卡负责监听所有正在网络上传输 的信息，并根据 ID 号来辨别应接收的信息。当需要发送信息时，网卡在数据流中寻找一个间 隙并将帧插入数据流。如果接到出错信息，它将把信息帧重发一遍。现阶段，网卡的传输速率一般是 10Mb/s，100Mb/s，1Gb/s（通常用在高端服务器），传输的信号有电信号和光信号。

（2）网络连接的器材——通信介质

通信介质可以分为线缆和无线电波，而线缆又可以分为双绞线、同轴电缆、光缆等。双绞线（TP）类似于电话线，由绝缘的彩色铜线对组成，每根铜线的直径为 0.4 毫米~ 0.8 毫米，两根铜线互相缠绕在一起。双绞线对中的一根电线传输信号信息，另一根被接地并吸收干扰。将两根线缠绕在一起有助于减少串扰的影响。双绞线又分为 2 种，即屏蔽双绞线（STP）和非屏蔽双绞线（UTP）。STP 的原理是利用屏蔽层来防止噪声，其中的缠绕电线对被一种金属如箔制成的屏蔽层所包围，而且每个线对中的电线也是相互绝缘的，一些 STP 使用网状金属屏蔽层。非屏蔽双绞线（UTP）电缆包括一对或多对由塑料封套包裹的绝缘电线对。正如名字所示，UTP 没有用来屏蔽双绞线的额外的屏蔽层。因此，UTP 比 STP 更便宜，抗噪性也相对较低。IEEE 已将 UTP 电缆命名为“10/100BaseT”，其中“10/100”代表最大数据传输速度为 10/100Mbps，“Base”代表采用基带传输方法传输信号，“T”代表 UTP。在数据中心通常使用非屏蔽双绞线。STP 和 UTP 具有许多共同的特性，在吞吐量上，STP 和 UTP 能以 10Mbps 的速度传输数据，5 类 UTP 以及在某些环境下的 3 类 UTP 数据的传输速度可达 100Mbps。高质量的 5 类 UTP 也能以每秒 1GB 的速度传输数据。在制造成本方面，STP 和 UTP 的成本区别在于所使用的铜态级别、缠绕率以及增强技术。一般来说，STP 比 UTP 更昂贵，但高级 UTP

也很昂贵。

大型数据中心交换机之间使用的是光缆连接，以提供高速链接。光缆就是光导纤维。在它的中心部分包括了一根或多根玻璃纤维，通过从激光器或发光二极管发出的光波穿过中心纤维来进行数据传输。在纤维的外面，是一层玻璃称之为包层，它如同一面镜子，将光反射回中心。反射的方式根据传输模式而不同，这种反射保证信号的完整性。在包层外面，是一层网状聚合纤维，以保护内部的光纤。最外一层塑料封套覆盖在网状屏蔽物上。光缆也存在许多不同的类型，分成两大类：单模式和多模式。单模光缆携带单个频率的光，将数据从光缆的一端传输到另一端，数据传输的速度更快，并且距离也更远。但是这种光缆开销太大，因此不被考虑用于一般的数据网络。相反，多模光缆可以在单根或多根光缆上同时携带几种频率的光波。这种类型的光缆通常用于数据网络。

在网络中，光缆目前主要用作主干线，以每秒 10GB 的速度可靠地传输数据。通常，光纤结合 UTP 连接各个工作站，以满足对网络传输容量要求。

（3）连接器

连接器是连接线缆与网络设备的硬件。网络设备包括文件服务器、工作站、交换机或打印机等等，每种通信介质都对应一种特定类型的连接器。使用的连接器的种类将影响网络安装和维护的成本，网络增加段和节点的容易度，以及维护网络所需的专业技术知识。通常，UTP 使用 RJ-45 连接器，也叫水晶头，它比电话线接头大一些。STP 使用 D 型连接器与网卡连接。与普通电缆不同，光纤容易在连接器处发生色散，所以光纤使用 SMA(螺纹安装适配器)和 ST（弹簧扭转器）进行连接。ST 连接器使用具有一定压力的弹簧夹紧光纤，而 SMA 靠螺纹进行端部连接。

（4）集线设备——交换机

早期以太网使用的集线设备是集线器，基于介质共享。随着网络中设备数量的增加，网络性能会逐渐下降。当网络中设备的数量达到一定程度时，由于冲突不断发生，网络传输速度就会令人难以忍受，有些网络甚至会迅速崩溃。这在宽带网络中是最大的瓶颈。现在，数据中心设备都使用线速交换机作为核心交换设备以处理庞大的数据交换率。交换机提供了桥接能力以及在现存网络上增加带宽的功能。用于 LAN 上的交换机与网桥相似，因为它们都运作在数据链路层（第 2 层）的 MAC 子层上，都检验着所有进入的网络流量的设备地址。与网桥还有一点相似，交换机保持一张有关地址的信息表，并用该信息来决定如何过滤并转发 LAN 流量。而与网桥不同，交换机采用交换技术来增加数据的输入输出总和和安装介质的带宽。

交换机是一种存储转发设备。交换机转发信息的方法有 3 种：直通方式、无碎片直通方式、存储转发方式。

交换机以直通方式转发信息时，不需要接收整个转发的帧，只需要收到帧最前面的源地址和目的地址部分即可。根据目的地址找到相应的交换机端口，然后直接引导帧至该端口。这种方式的优点：一是转发速度快；二是延时一致性很好，不论长帧还是短帧都具有相同的传输延时。缺点是不进行错误校验。直通方式不能对不同速率的端口进行转发，如从 100Mb/s 高速端口向 10Mb/s 低速端口转发信息帧时，必须对帧进行缓冲存储，如果低速端口来不及处理从高速端口送来的信息，将造成缓冲区溢出错误。

一个正常的以太网帧至少是 64 个字节，小于 64 个字节的帧（称为碎片）一定是错误的帧。如果让交换机不仅接收 MAC 地址，还必须满足收到一个帧的前 64 个字节以判断是否是

正确帧，这种转发方式就称为无碎片直通方式。

存储转发方式首先要把整个数据帧全部读入到内部缓冲区中，并对数据帧进行校验，一旦发现错误就通知源站重发该帧。利用存储转发机制，网管还可以定义过滤算法来控制通过该交换机的通信流量。存储转发方式可以在不同速率的端口之间进行转发操作。

（5）隔离子网——路由器

路由器的主要作用有两个，一是用于连接不同类型的网络，二是用于隔离广播域，避免广播风暴。城域网要想和 Internet 相连只能通过路由器来实现。为了防止广播风暴，路由器判断帧的目标地址，并于自己的路由表进行比较，如果是本网段就截留，非本网段就转发。路由器是一种多端口设备，它可以连接不同传输速率并运行于各种环境的局域网和广域网，也可以采用不同的协议。路由器属于 OSI 模型的第三层。网络层指导从一个网段到另一个网段的数据传输，也能指导从一种网络向另一种网络的数据传输。路由器的有些功能与网桥类似，如学习、过滤和转发等。但与网桥不同，路由器具有内置的智能来指导包流向特定的网络，可以研究网络流量并快速适应在网络中检测到的变化。路由器在 OSI 模型的网络层连接 LAN，从而与网桥相比，可以从包流量中解释更多的信息。

过去，由于过多地注意第三层或更高层的数据，如协议或逻辑地址，路由器曾经比交换机和网桥的速度慢。因此，不像网桥和第二层交换机，路由器是依赖于协议的。在它们使用某种协议转发数据前，它们必须要被设计或配置成能识别该协议。传统的独立式局域网路由器正慢慢地被支持路由功能的第三层交换机所替代。但路由器这个概念还是非常重要的。独立式路由器仍然是使用广域网技术连接远程用户的一种选择。路由器的稳固性在于它的智能性。路由器不仅能追踪网络的某一节点，还能和交换机一样，选择出两节点间的最近、最快的传输路径。基于这个原因，再加上它们可以连接不同类型的网络，使得它们成为大型局域网和广域网中功能强大且非常重要的设备。例如，因特网就是依靠遍布全世界的几百万台路由器连接起来的。

（6）与大型机相连——网关

网关能够完成比路由器更为复杂的任务。路由器只是查看分组信息，把分组从一台路由器传送到另一台路由器，并且不断修改源节点与目标节点的数据链路地址，它不会修改帧内的任何其他信息。网关则能够有效的把信息从一种协议标准转换成另一种协议标准。因为网关的应用程序范围极广，所以它可以在 OSI 模型的任一层上运行。最传统的网关是一种用来将一类协议转化为另一类具有截然不同的结构组成的协议的网络设备。这种网关在 OSI 模型的网络层上运作。关于这种网关的一个最好的例子就是将 IBM 开发的用于大型机的系统网络结构（Systems Network Architecture，SNA）转化为另一种协议，如 TCP/IP。这类网关的主要问题在于，与其他解决方案相比，速度较慢，因此传统的网关用得越来越少了。另外，网关一词常用于将一种格式的 E-mail 转变为另一种格式的软件。这类网关在 OSI 模型的应用层上运行。

（7）计算机通信规则——通信协议

通信协议用来协调不同的网络设备间的信息交换。通信协议能够建立起一套非常有效的机制，每个设备均可据此识别出来自其他设备的有意义的信息。通信协议就好象是语言，通信双方必须使用同一种语言才能彼此通信。在 Internet 中使用最广泛的是 TCP/IP 协议。因特网连接了许多网络，它们都使用 TCP/IP 协议。TCP 和 IP 大致分别对应于 OSI 模型的第 4、第 3 层，尽管它们不是 OSI 模型的一部分。它们是随 ARPA（ARPAnet，阿帕网）工程开发的，

并成为美国国际部 DoD 标准。TCP/IP 可能是世界上实行最广泛的协议了，它运行在从 PC 机到超级计算机的任何机器上。TCP/IP 不是一个简单的协议，而是一组小型、专业化协议，包括 TCP、IP、UDP、ARP、ICMP 以及其他一些被称为子协议的协议。大部分网络管理员将整组协议称为 TCP/IP，有时简称为 IP。TCP/IP 的前身是由美国国防部在 20 世纪 60 年代末期为其远景研究规划署网络（ARPAnet）而开发的。由于低成本以及在多个不同平台间通信的可靠性，TCP/IP 迅速发展并开始流行。它实际上是一个关于因特网的标准，迅速成为局域网的首选协议。一些最近发行的网络操作系统（NOS）（如 NetWare 5.0）使用 TCP/IP 为缺省协议。TCP/IP 最大的优势之一是其可路由性，也就意味着它可以携带被路由器解释的网络编址信息。TCP/IP 还具有灵活性，可在多个网络操作系统或网络介质的联合系统中运行。

然而由于它的灵活性，TCP/IP 需要更多的配置。TCP/IP 协议组可被大致分为四层，应用层大致对应于 OSI 模型的应用层和表示层，借助于协议如 Winsock API、FTP（文件传输协议）、TFTP（普通文件传输协议）、HTTP（超文本传输协议），SMTP（简单邮件传输协议）以及 DHCP（动态主机配置协议），应用程序通过该层利用网络。传输层大致对应于 OSI 模型的会话层和传输层，包括 TCP（传输控制协议）以及 UDP（用户数据报协议），这些协议负责提供流控制、错误校验和排序服务。所有的服务请求都使用这些协议。互连网层对应于 OSI 模型的网络层，包括 IP（网际协议）、ICMP（网际控制报文协议）、IGMP（网际组报文协议）以及 ARP（地址解析协议）。这些协议处理信息的路由以及主机地址解析。网络接口层大致对应于 OSI 模型的数据链路层和物理层。该层处理数据的格式化以及将数据传输到网络电缆。

1.4　系统集成方案

构建一个计算机网络，可以分为两个部分进行配置：一是硬件架构，二是软件配置。软件的配置是随着硬件结构进行的。一个物理拓扑不好的网络，即使网络服务器配置得再好，也可能出现问题，轻者网络速度不够，重者引起安全问题，甚至整个网络的崩溃。所以一个合格的网络管理员不只要做服务器方面的配置，首要前提是在物理上设计一个网络拓扑环境。为了讲清楚 Windows Server 2003 的网络应用，本书以一个自来水公司 IP 城域网为硬件基础结构来进行 Windows Server 2003 的配置，以后的大多数配置都是基于这一基本结构。这样做的好处是，在一个网络中涉及了路由器和交换机等网络设备，模拟出了一个小型的广域网环境。Windows Server 2003 的一些概念在基于交换的局域网这样的环境中是无法阐述清楚的。下面说明网络拓扑各个部分的作用以及子网划分的概念。

1.4.1　第一方案

整个网络中心采用港湾 FlexHammer 24 千兆三层交换机，通过瑞斯康达 RC101-FE 以太网光纤收发器和各个水厂相连。考虑到自来水公司要在网络中传输重要财务数据，各个水厂的出口采用华为的 2600 系列路由器作为硬件防火墙与光纤收发器相连，具体网络拓扑如图 1-2 所示。

从图中可以看出自来水公司下属的三个水厂要通过 FlexHammer 24 和公司通讯，并将财务信息，实时监控信息送回总公司；总公司通过 FlexHammer 24 去访问三个水厂的局域网；邮件服务器、FTP 服务器、WEB 服务器等都放在自来水公司监测中心。

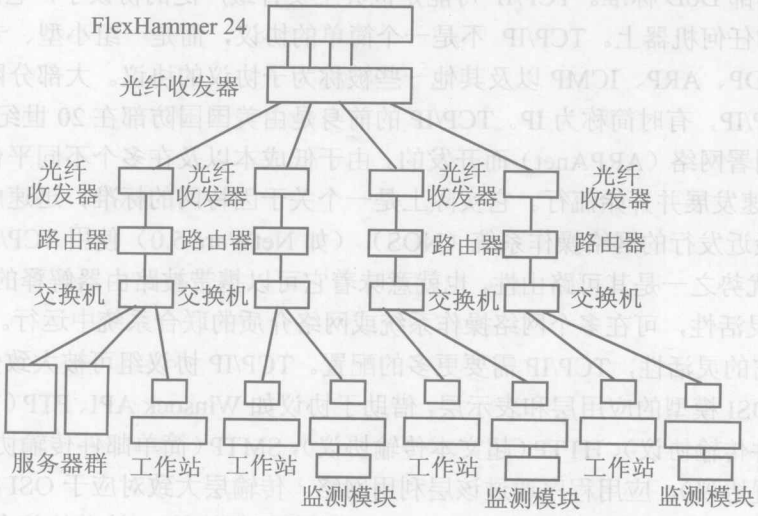


图 1-2 第一方案

用户端通过路由器和整个 IP 网域相连。路由器可以配置访问列表和硬件防火墙，以满足信息对安全性的需求。路由器后是自来水公司的四个分立的计算机局域网，三个水厂都配置了摄像设备和视频采集模块，采集到的视频信息都被打成 IP 数据包传输到自来水监测中心的局域网，可以在计算机上观看或分屏输出到电视墙上监视。每个水厂的设备都安装有数字输出接口和数据采集模块相连。从计算机上可以实时观看到设备的工作参数，采集到的参数每隔 8 小时向自来水监测中心的服务器传输一次。

IP 地址划分：从交换机到路由器的广域网接口采用 A 类私用地址 10.0.0.0，子网掩码为 255.255.255.248。采用 248 掩码的原因是为了不引起 IP 地址的浪费。这样一来，主机地址为 1-6，0 和 7 为网络地址和广播地址，整个网络留有 1 个空闲地址。这样的方案对于用户地址数量相对固定的情况来说比较有效。如果子网范围内的主机地址不够，一旦用户地址超量，则必须更改用户的 IP 或子网掩码。这样就不可避免的造成用户的数据传输中断，如果正在传输重要数据，就会造成数据丢失。所以对于不同的情况必须留有一定余量的主机地址，以备将来的需要。

配置方式：首先在物理网络上，光纤应铺设完毕。由网络公司到各个水厂及自来水公司应存在一收一发两条光纤，在用户端，尾纤应熔接完毕，在局端，尾纤的一端插入光纤收发器，活动接头一端用法兰和各个用户端溶好的尾纤相接。在逻辑网络上为各个端口分配好 IP 地址。在局端的 FlexHammer 24 交换机上建立一个 VLAN 并命名为 WATER。然后将 2-5 端口以无标签模式加入 VLAN。一端口没有加入是因为考虑到将来的扩容将使用一端口作中继使用。这样划分以后，在交换机上存在两个 VLAN，一个为 WATER，另一个为默认的 default VLAN。然后为 WATER 分配 IP 为 10.1.1.1，子网掩码为 255.255.255.248。因为各个路由器的 WAN 端口必须在同一个子网内，所以自来水公司和三个水厂的 IP 依次为 10.1.1.2，10.1.1.3，10.1.1.4 和 10.1.1.5。用户端内部 IP 地址依次为 192.168.0.0 网络地址，192.168.1.0 网络地址，192.168.2.0 网络地址和 192.168.3.0 网络地址。IP 地址规划完毕后，接下来就要进行光路的连接。首先保证机房的光纤收发器的供电正常，把光纤收发器的尾纤和用户端的各路尾纤通过法兰相接，然后就要连接各

个用户端。因为并不知道用户端的两根尾纤哪一根为接收，哪一根为发送，所以判断方法为把两根光纤依次插入光纤收发器的 RX 接收端。如果光纤收发器的 LNK 链接指示灯亮起，说明这根光纤是接收光纤；然后把另一根光纤插入 TX 发送端，如果局端相应的光纤收发器的 LNK 指示灯亮起，说明这一用户端的光链路连接正常；然后将光纤收发器的电端口通过 RJ-45 网线和华为 2621 路由器的 LAN 0 或 LAN 1 相连，连接方式为交叉线连接。连接正确后，光纤收发器的电端口的 LNK 指示灯将亮起。接下来配置路由器的 LAN 0 或 LAN 1 端口的 IP 为预先规划好的 WAN 地址。剩下来的 LAN 端口接用户端的局域网。配置完毕后存盘，用超级终端接入路由器的 CONSOLE 口。进入 CLI 命令模式后 ping 一下 VLAN WATER 的 IP 10.1.1.1。这时，光纤收发器的 RX，TX 指示灯将亮起并不断闪动，说明有数据进行传输。接下来再 ping 一下配置成功的各台服务器。它们都位于 192.168.0.0 子网内，ping 的方法为：先 ping 其网关地址，再 ping 服务器。ping 的结果，正常情况下回应应小于 2 毫秒。以同样方式配置好其他各个用户端。

测试：在各个局域网上设置好各自的网关，网关的 IP 地址为各自局域网的路由器的 LAN 端口地址，然后在一个用户端 ping 其他用户端。首先 ping 一下其他路由器的 WAN 端口地址。如果通过的话再 ping 一下这个用户端的局域网内的任意一台主机地址。如果通过的话，用 ping -S -C 命令发送指定数量和大小的数据包来测试一下网络的工作环境。从测得的情况看，发送 5000 个 1000BYTE 的数据包，回应小于 2 毫秒，丢包率为 0。

从现在的网络结构看，每个用户端都直接和前端的交换机通过光纤相连。笔者觉得这只适合用户较少的情况，将来如果网络进一步扩大，预留光纤将不够用。如果每个用户端都用单独的一根光纤，势必造成光纤的浪费，因此笔者考虑将 FlexHammer 24 交换机作为节点使用，中心采用 BigHammer 800 交换机提供高背板带宽。整个网络拓朴如图 1-3 所示。

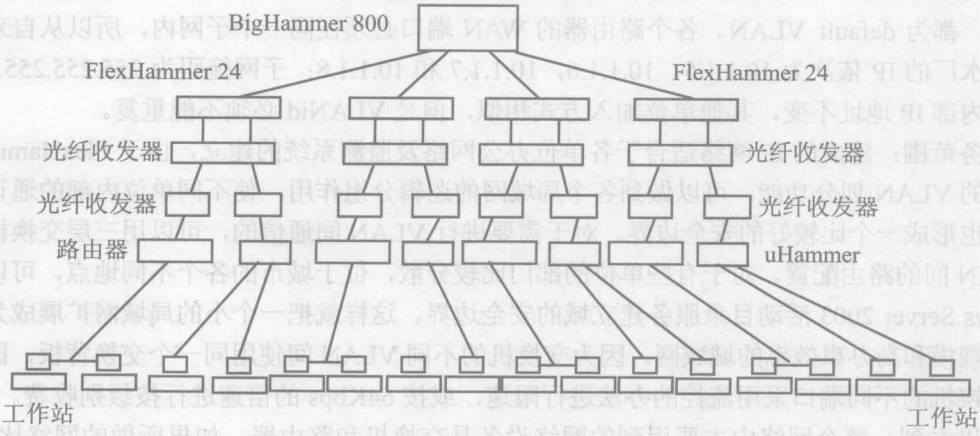


图 1-3　第二方案

1.4.2　第二方案

整个网络的中心交换采用了港湾公司的 BigHammer 800 骨干智能多层交换机。它的特点是包括 Gigabit 以太网光接口和 10/100Mbit/s 以太网电接口；提供备份电源，双电源同负载；可达到 224 个 10BASE-T/100BASE-TX 以太网端口，58 个千兆端口，30 个 G 位以太网端口。

支持基于 IP 的三层交换和虚拟局域网技术，支持通过串口的 CLI 连接；交换背板的带宽为 128G，支持 L2/L3 层线速包转发；市区各个节点采用 FlexHammer 24 可网管交换机；各个交换机和局端中心交换机通过千兆光接口相连，为业务扩展提供足够的带宽。用户端根据传输数据对安全性的不同需求采用交换机或者路由器，如自来水厂、财务部门以及公安交警部门都需要采用保密性好的路由器，对以达到资源共享为目的的政府和事业单位可以采用港湾的 uHammer 交换机作为办公网的中心交换设备。网络管理计算机连接在 BigHammer 800 中心交换机上，通过为各个节点配置 IP 地址的方式可以在局端对各个节点的设备进行配置和管理。

IP 地址划分：在前端的中心交换机上建立一个基于端口的 VLAN，默认状态下，所有的端口属于一个 default VLAN。接下来在各个节点的交换机上各建立一个 VLAN WATER，并且分配 IP 地址为：10.1.1.1/240，10.1.1.2/240，10.1.1.3/240，10.1.1.4/240。然后把各个节点的光纤接口以标签模式加入 WATER 中。接下来配置各个路由器的 IP 地址为：10.1.1.5/240，10.1.1.6/240，10.1.1.7/240，10.1.1.8/240。当网络掩码为 255.255.255.240 时，表示 IP 地址的前 28 位为网络地址，后 4 位为主机地址。这样一来，网络地址是 10.1.1.0，广播地址是 10.1.1.15。在子网划分中，这两个地址不能分配，所以，可用 IP 地址为 1-14，9-14 可以作为备份用，以备将来进行业务扩充使用。其他单位的子网以同样方式划分。只需建立不同的 VLAN。

配置方式：在逻辑网络上为各个设备分配好 IP 地址。在节点的 FlexHammer 24 交换机上建立一个 VLAN 并命名为 WATER，设定其 VLANid 为 1，然后将 1 端口以无标签模式加入 VLAN。光纤接口连接到中心交换机，光纤接口以标签模式加入此交换机的所有 VLAN。这样划分以后，在交换机上存在两个 VLAN，一个为 WATER，另一个为默认的 default VLAN。然后为 WATER 分配 IP 为 10.1.1.1，子网掩码为 255.255.255.240。其余连接自来水公司路由器的节点配置同上。名字也为 WATER，VLANid 必须为 1，这样，就跨交换机创建了 VLAN。各个节点的默认 VLAN 名相同，都为 default VLAN。各个路由器的 WAN 端口必须在同一个子网内，所以从自来水公司到三水厂的 IP 依次为 10.1.1.5，10.1.1.6，10.1.1.7 和 10.1.1.8；子网掩码为 255.255.255.240。用户端内部 IP 地址不变，其他单位加入方式相似，但是 VLANid 必须不能重复。

业务范围：建成的 IP 网络适合于各单位办公网络及监测系统的建立，由于 FlexHammer 24 交换机的 VLAN 划分功能，可以做到各个局域网的逻辑分组作用，使不同单位内部的通讯互不影响，也形成一个比较好的安全边界。对于需要进行 VLAN 间通信的，可以用三层交换模块进行 VLAN 间的路由配置。对于有些单位的部门比较分散，位于城市的各个不同地点，可以采用 Windows Server 2003 活动目录服务建立域的安全边界。这样就把一个小的局域网扩展成为一个有相当规模和高办事效率的城域网。因为交换机的不同 VLAN 间使用同一个交换背板，因此可以对交换机的不同端口采用流控的办法进行限速，或按 64Kbps 的倍速进行按级别收费。

可以看到，整个网络中主要用到的网络设备是交换机和路由器。如果所做的网络比较小，只想作为办公和 Internet 共享使用，那么只需使用交换机就行了。对于想进行隔离分组或者考虑到网络安全使用的，就需要使用到路由器了，但也视其网络链路速度的大小。

1.5 交换机的特点

交换机也被称为交换式集线器，为什么这么称呼呢？在 1996 年以前，局域网的中心设备是集线器，它的特点是共享带宽；如果是一个 10M 的集线器，那么这 10M 的带宽就被每个端

口共享；随着交换技术的发展，二层、三层、四层交换技术的出现，人们已经渐渐的用交换机代替了集线器；现在集线器的市场已经非常小了，但还是沿用了集线器这一名称。

二层交换机只依赖于数据链路层中的信息（MAC）地址完成不同端口之间信息的线速交换。三层交换机具有了路由器的功能，它使用 IP 地址进行路径选择而且能够实现 VLAN，因此现在的大中型网络都把三层交换机作为基本网络设备。

转发方式：转发方式是指交换机所采取的用于决定如何转发数据包的转发机制。一般，分为存储式转发和直通式转发。另外，还有一种碰撞逃避转发技术。各种转发技术各有优缺点。

1. 直通转发方式

交换机一旦解读到数据包目的地址，就开始向目的端口发送数据包。通常，交换机在接收到数据包的前 6 个字节时，就已经知道目的地址，从而可以决定向哪个端口转发这个数据包。直通转发技术的优点是转发速率快、减少延时和提高整体吞吐率。其缺点是交换机在没有完全接收并检查数据包的正确性之前就已经开始了数据转发，这样，在通讯质量不高的环境下，交换机会转发所有的完整数据包和错误数据包，这实际上是给整个交换网络带来了许多垃圾通讯包，交换机会被误解为发生了广播风暴。总之，直通转发技术适用于网络链路质量较好、错误数据包较少的网络环境，在选购时要根据自己的网络规模进行考虑。一般低端交换机只具有一种转发方式，高端交换机兼具两种转发方式，可以通过实时的网络状况进行自动切换，如果网络的传输速率较高，可以采用直通式转发，如果传输速率要求不太高，可以采用存储转发方式。

2. 存储转发方式

存储转发技术要求交换机在接收到全部数据包后再决定如何转发。这样一来，交换机可以在转发之前检查数据包完整性和正确性。其优点是：没有残缺数据包转发，减少了潜在的不必要数据转发。其缺点是：转发速率比直接转发技术慢。所以，存储转发技术比较适应于普通链路质量的网络环境。

3. 碰撞逃避转发技术

碰撞逃避转发技术通过减少网络错误繁殖，在高转发速率和高正确率之间选择了一条折衷的解决办法。某些厂商（如 3Com）的交换机还提供这种厂商特定的转发技术。

转发速率：在选购交换机时，转发速率是一个重要考虑的指标。但是现在的交换机一般都支持线速交换，也就是转发速率接近传输线上的传输速率。

背板带宽：在交换机进行不同端口之间的交换时，实际上都是通过背板完成的。交换背板带宽越大，提供给各个端口的可用带宽越大，交换速度就越快。

端口：在选购时还要注意交换机支持的端口数和端口类型以及是否有高速端口以支持将来的扩容。

延时：交换机延时是指从交换机接收到数据包到开始向目的端口复制数据包之间的时间间隔。有许多因素会影响延时大小，比如转发技术等。采用直通转发技术的交换机有固定的延时，因为直通式交换机不管数据包的整体大小，而只根据目的地址来决定转发方向，固定值取决于交换机解读数据包前 6 个字节中目的地址的解读速率。采用存储转发技术的交换机由于必须要接收完了完整的数据包才开始转发数据包，所以它的延时与数据包大小有关。数据包大，则延时大，数据包小，则延时小。

管理功能：交换机的管理功能是指交换机如何控制用户访问交换机，以及用户对交换机