

一个中小型信息网站建设实例*

张 波, 鹿海涛, 邢仲景

(华南农业大学现代教育技术中心, 广州 510642)

摘 要: 介绍一个切实可行的网站建设方案, 该方案从应用需求出发, 结合当前的网络技术及网络产品, 对中小型网站的设计 (规模, 网络结构, 网络安全) 和实现 (综合布线, 路由器, 交换机, 服务器等设备选型) 做出详细介绍, 特别提出在当前 IPv4 技术中, 如何解决 IP 地址不足的问题, 可给予其他网站建设提供参考价值。

关键词: 网站; 建设; NAT 网络地址转换

中图分类号: TP393.18 **文献标识码:** A

随着 INTERNET 网络的迅猛发展, 网上资源和信息日益丰富, 各地、各部门为尽快与国际相接轨, 将本地的资源推向世界, 拟建立一个信息资源网站。华南农业大学网络中心与某地合作建立横向课题, 网络中心利用自身实力对一个中小型网站建设提供全面的技术支持服务, 分析用户需求, 选择网络技术, 提出建设方案, 并按期完成该工程。

1 总体需求 (用户需求及所需服务)

根据一个中小型上网工程任务需求书分析, 本工程将包括该网站, 覆盖该地多个部门的内部局域网, 供远地单位通过电话接入的拨号网, 供学校接入的光纤线路, Internet 接入五个主要部分; 工程完成后可提供完整的 Internet 应用 (包括 DNS 服务、电子邮件服务、WWW 服务、代理服务), 服务对象包括本地局域网用户、电话拨号接入用户、光纤专线用户及国内外 Internet 网上用户, 使该地区网成为真正 Internet 网中的一部分, 同时建成后的网络还可为各部门实现内部办公现代化提供服务 (如提供内部信息发布平台、公文流转、信息检索等)。

2 网络设计 (网络技术, 网络设备, 网络安全)

根据一个中小型网络规模及考虑今后发展, 本次工程建设全部采用成熟实用技术。

2.1 主干网技术的选择

目前, 流行的网络技术有 FDDI 技术、ATM 技术、高速以太网技术。

FDDI 是传统的高速局域网, 速率可达 100M, 其逻辑拓扑结构是一个逻辑环, 其物理拓扑结构是星型或环型。FDDI 网具有可靠, 容错的特性, 非常适用于作主干网, 尽管 FDDI 技术应用较多, 技术成熟, 但是有价格较高, 速率不会提高的缺点。

ATM 技术是应宽带、多媒体通信的需要而发展起来的, 基于时分多路复用和分组交

* 收稿日期: 2000-11-15; E-mail: bzhang@scau.edu.cn; lht@scau.edu.cn.

换的新技术，能提供多种服务和多种通信质量类型，目前速率可为 155M 和 622M。该技术允许声音、视频和数据在保证传输质量的前提下在同一物理信道上进行传输。ATM 有着众多的技术优势，但其价格偏高，管理也比较复杂。

高速以太网技术是在传统以太网技术基础上发展起来的，其速率可达到 100M，1000M。高速以太网以以太网交换机为中心，代替了传统的共享介质型的 HUB。利用交换机和路由器的结合，可以使用虚拟网技术来划分虚网，虚拟网络技术打破地理环境的制约，在不改动物理连接的情况下可以任意将工作站在工作组或子网之间移动，新增的工作站可以在最合理的物理连接点入网，因而可以实现按数据相关性原则将工作站组成逻辑工作组或虚拟子网，提高信息系统的运作性能，均衡网络数据流量，合理利用硬件及信息资源，对调整用户业务具有极大的灵活性。在逻辑网络或虚拟网络中的所有工作站彼此间可直接通信，不同虚拟网络间的站点不能直接通信，必经路由器（或第三层交换机），这极有利于网络安全；同时，利用虚拟网络技术，可大大减轻网络管理和维护工作的负担，降低网络维护费用。

千兆以太网和已充分建立的以太网与快速以太网的节点完全匹配。千兆以太网使用最初以太网规范定义的帧格式，支持 CSMD/CD 协议、全双工、流控制和有 IEEE802.3 标准定义的管理项目，并在网络链路层采用快速光纤连接方式，以适应日益增加的带宽的要求。它使电视会议、复杂图象和其它高数据密度的应用程序在 MAC（媒体访问控制）层的数据传递速率为快速以太网的十倍。千兆以太网可使网络自然、平滑地升级到 1000M 的带宽。

基于主干信道的选择及从建网初期应用内容和资金投入综合考虑，此次，选择高速以太网作为主干网。

2.2 网络安全

网络系统的安全性也是一个非常重要的问题。包括网络服务的安全和网络数据的安全，网络服务安全应能够防止网络黑客入侵后破坏系统的正常运行；网络数据安全应防止未经授权的数据访问。

本方案网络安全分为以下几个层次。

第一层次建立基于 MAC 地址和端口策略的 VLAN，限制内部不同组之间的非法访问，保证网络内部用户使用网络和数据的安全。

第二层次建立不同授权组的 IP 地址过滤列表，对内部或外部的不同 IP 地址段实行限制访问，甚至建立相应的第四层（TCP 层）各 TCP/UDP 协议，如 FTP-DATA、FTP、TELNET、SMTP、DNS、TFTP、HTTP、POP3、SNMP 等的过滤。

第三层次是授权认证机制及多级权限管理。

从建网初期应用内容和资金投入综合考虑，一期工程通过 CISCO 路由器和 3COM 的 3300 系列交换机及 PC 微机实现，待发展到一定规模（硬件和软件应用）后再使用专业防火墙及 IP 转换设备（比如，高档的第三层交换设备）。

方案中所选设备具有良好的兼容性，在未来的网络升级时，所有设备均可用于下一级使用，原投资可获完全保护。

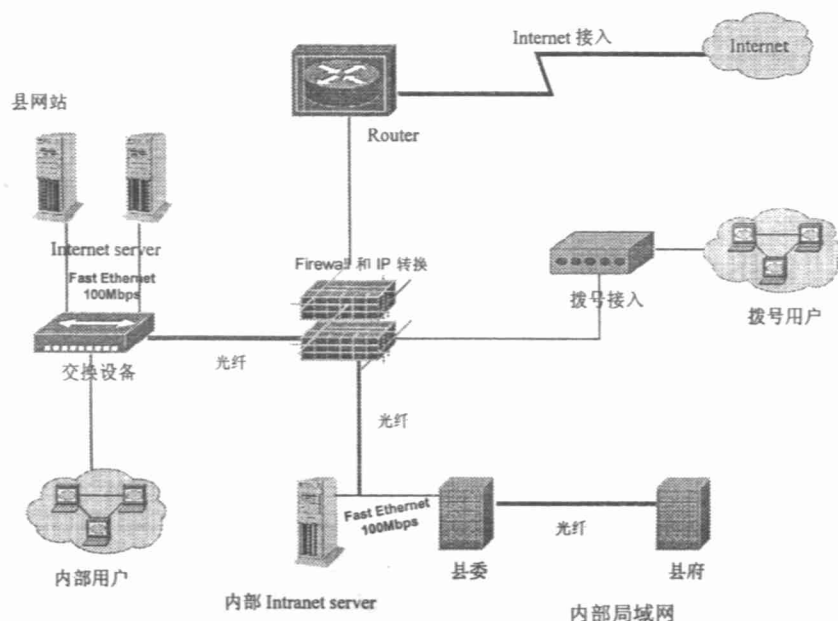


图 1 物理拓扑结构

3 网络技术方案

服务器主机采用两台部门级、一台工作组级 PC server, 分别作为 Internet 应用服务器和 Intranet 内部应用服务器, 使用 NT 操作系统作为网络操作系统, 可充分利用 NT 本身的安全管理机制和 IIS (Internet Information Server) 所提供的 WWW 服务和 FTP 服务, 灵活运用 ASP 编程实现用户与服务器的交互性, 配合 SQL 数据库的无缝连接, 能较大发挥服务器的功能, 均衡服务器的负载, 合理分配资源; 在当前网络需求及资源允许条件下, 网络设备采用 10M/100M 自适应交换机和集线器, 可满足用户的基本需求, 并能够随时升级网络设备; 县委、县府、县科委间通过光纤构成一个局域网络, 主干带宽为 100M, 能随时升级到 1000M; 网站部分服务器使用 Internet 合法 IP, 局域网及拨号部分采用保留 IP, 内部用户与局域网之间使用一台 PC 做代理服务 and NAT 转换, 拨号用户采用 CISCO2511 路由器实现 NAT 转换, 并提供安全保护; 拨号部分可同时支持 16 路电话接入, 使用 ACCESS SERVER 提供用户安全认证服务。

4 关键技术

在该网站建设中, 一个非常重要的技术问题是真实 IP 地址的严重不足, 该网站申请到的 IP 子网掩码为 255.255.255.248, 即总共只有 8 个 IP 地址, 其中除掉网络号和广播地址外, 路由器还占用一个 IP 地址, 即只有五个 IP 地址可被使用。

对于大量的局域网用户和拨号用户, 采用分配保留 IP 地址的方法, 在内部网关和路由器端提供 NAT (Network Address Translation) 服务来解决该问题。NAT 技术使得网络内部使用保留 IP 地址的计算机在与外部 Internet 网络进行通讯时, 由 NAT 转换设备负责将其所使用的保留 IP 地址转换成合法 IP 地址, 从而使局域网内部计算机可以享有与外部计算机

同样的 Internet 服务。

CISCO 系列路由器在 IOS11.3 以上的版本才支持 NAT 功能，因此，如路由器 IOS 版本太低，应在路由器的 FLASH MEMORY 允许的情况下对 IOS 进行升级，可使用 CISCO 的 TFTP 服务器来执行升级过程。

如，在 CISCO2511 路由器中有关 NAT 功能的配置如下：

```
!  
ip nat inside source list 8 interface Ethernet0 overload /* 动态 IP 转换 */  
!  
interface Ethernet0  
    ip address 202.104.199.65 255.255.255.248 /* 合法的 IP 地址 */  
    ip nat outside /* 允许外部地址 NAT 转换 */  
!  
interface Serial0  
    ip address 202.104.196.250 255.255.255.252  
    ip nat outside /* 允许外部地址 NAT 转换 */  
!  
interface Group - Async1  
    ip nat inside /* 允许内部地址 NAT 转换 */  
    member 1 peer default ip address 192.168.0.221 /* 对每根 LINE 分配一个内部 IP 地址 */  
    member 2 peer default ip address 192.168.0.222 /* 每个拨号上来的机器将分配一个 */  
    member 3 peer default ip address 192.168.0.223 /* 内部 IP 地址 */  
    .....  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 Serial0
```

使用 show ip nat translations 命令，可以即时看到动态翻译地址表的内容。

5 结束语

网站建设应遵循先进性、实用性、可扩充性、易管理和维护性以及较高的性能/价格比等原则，在有限的投资下建成技术比较先进、实用的网络。

An Example for the Construction of Middle-Small Scale Websites

ZHANG Bo^{*}, LU Hai-tao, XING Zhong-jing

Abstract: A solution, design and implementation of a middle-small scale website construction are introduced.

Keywords: website; design; NAT transition

^{*} Educational Technology Center, South China Agricultural University, Guangzhou 510642, China