

深圳市罗湖区信息网络系统

深圳市罗湖区信息中心 谷瑞

深圳市罗湖区计算机信息网络(简称“罗湖信息网 LHNNet”)是建立在罗湖管理中心大厦综合布线系统之上的,运用世界先进计算机信息网络技术的,涵盖区委、区政府、区人大、区政协、区纪委等五套班子及各街道办事处和部、委、办、局在内的,面向全区的、致力于提高政府办公自动化水平,为政府实施宏观调控和管理职能提供依据和现代化手段,规范政府机关办事流程,并与深圳信息网联接配套的,面向二十一世纪的、高速的、开放的、分布的、大型多媒体 INTRANET 计算机综合信息系统。

总体设计原则和架构

1. 设计原则

(1) 高起点。广泛吸取国内外信息网建设方面的成功经验,最大限度地采用当今世界最先进、最成熟、最有发展前途的技术。由此实现的系统能随着未来科学技术的发展而不断地平滑升级。

(2) 实用性强。应充分体现罗湖区政府工作的特点,来构建罗湖信息网中的软硬件系统。各计算机应用系统,应做到功能完善、使用方便、符合实际、运作高效。

(3) 易维护。应提供完备的系统维护和检测手段,确保罗湖信息网安全、高效地运行。

(4) 易扩展。在对罗湖信息网进行设计和设备选型时,应充分考虑到信息技术的高速发展及政府工作可能发生的变化给罗湖信息网带来的影响,使罗湖信息网在技术和应用上均留下足够的发展空间。

2. 功能架构

(1) 架构内网/外网中心交换机及接入交换机,通过光缆把区府办接入交换机与中心交换机连接起来形成千兆网络骨干,并为网络提供远程接入访问能力。归划 IP 地址分配,建立网管系统。

(2) 建立 Internet/Intranet 各种服务(包括 WWW, FTP, 邮件服务, 目录服务等)能为未来罗湖区下属部门的多种接入提供各项服务,提出一套完整的解决内/外网安全问题的方案。

(3) 建立视频点播, 视频广播等服务。

(4) 建立数据库服务器。

(5) 完成区府办公自动化系统的开发和安装使用。

(6) 规划并制作内网/外网的 WEB 的主页,总结国内各政府部门主页的优点。形成具有罗湖特色的全方位,全角度面向社会的动态外网主页。

主干网实施

1. 主机数据库系统

主机系统是应用系统的核心,可靠性特别重要。在考虑到高可用性和经济性的基础上,采用双机构成互为备份高可用系统,以实现数据库和 OA 的应用服务。在综合比较各方产品的性能价格比后,选择 SUN 公司最成熟的企业级服务器 Enterprise 3500 双机共享 Sun StorEdge A5000 磁盘阵列,再加上 Rose HA 和相应的 Agent 软件构成该双机互备份高可用系统。

2. 网管工作站及网管平台软件

网管工作站选用 Sun Ultra 60 图形工作站。

网管平台的选择是基于操作系统和网络设备管理软件,操作系统在选择 SUN 的前提下,只能选择 Solaris。而网络设备选择 Cisco,网络设备管理软件也只能选择 Cisco Works,因此,网管平台必须考虑 Solaris,网管平台, Cisco works 三者之间的兼容,经比较,网管平台选择 SunNet Manager 较其他产品更好。

3. 局域网实施

选择千兆网作为主干网,采用局域网两级交换结构,两级交换结构把整个局域网分为主干和桌面两级,主干使用千兆以太网的连接方式。而桌面交换机的上连端口直接接入核心交换机上。

(1) 核心交换机选用一台 CISCO 公司的千兆位交换机 Catalyst 6509,为了实现核心交换机的高度可靠性,Catalyst 6509 配有双电源,双引擎冗余。配有路由交换模块(RSP),提供第三层路由。配有二十个千兆口提供桌面交换机的接入和应用服务器的接入,配有 24 个 100M 以太口。所有的服务器设备,直接连到核心交换机的千兆口上。百兆口提供信息中心的桌面连接。

(2) 桌面交换机选用 9 台 CISCO 公司的高密度 10M/

100M 自适应交换机 Catalyst 2948, Catalyst 2948 提供 48 个 10M/100M 自适应端口, 同时配有两个千兆位上连口, 提供了上连口的端口备份。对于高带宽的需求, 可同时使用两个千兆口上连 Catalyst 6509, 提供 4G 的全双工带宽。

(3) 每两个桌面交换机 2948 之间使用光纤相互连接, 形成九台楼层交换共四对互为备份系统, 实现主干交换线路的部分备份, 并打开 spanning tree 的功能, 防止物理环的形成。另一台 2948 放置楼层最底层。同时增加一台 1924 放置中心机房, 作为主干系统的硬备份。

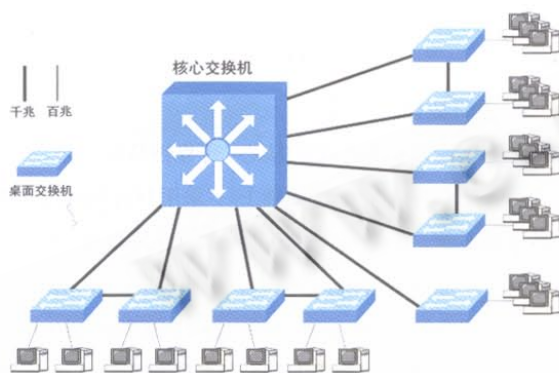


图 1 罗湖信息网局域网示意图

4. 广域网接入

(1) 中心接入访问服务器。访问服务器采用 CISCO 公司的 AS3640 模块路由器, 并配置有一块 8 口 ISDN 模块, 用于和 8 个街道办事处通过 ISDN 线路相连。同时配备一块 8 端口同步/异步模块, 考虑到原有的 CISCO2509 已具有 8 个异步端口, 在支持拨号用户时同时使用 3640 和 2509, 同时可支持 16 个用户拨号上网。3640 还配有一个 10M 以太网口, 用于和 Catalyst6509 相连。由于 7204 还有空余插槽, 可随时按需求增加模块, 提高网络拨号用户数或专线用户数。

(2) 街道办事处的接入。用于街道办事处的小型接入路由器选用配有一口 ISDN 模块的 CISCO 1603 模块化路由器, 在各街道办事处放置一台支持 ISDN 的路由器, 通过路由器将街道办事处的局域网接入罗湖信息网, 由于 ISDN 有两条 B 通道, 平时在传输量不大时只开启一条 B 通道, 传输速度为 64Kbps, 只有传输量到达设定的阈值时, 启用另一条 B 通道, 传输速度可达 128Kbps。

(3) 外部用户的拨号访问。为支持外部的访问, 拨号访问路由器在支持 8 路 ISDN 接入的同时还需要支持 16 条 PSTN 线路接入, 中心的访问服务器需要配置 16 个异步

口。由于拨号访问是一项开放的服务, 为保证安全, 在访问路由器的后面配置一台访问认证服务器, 并使用 RADIUS 认证协议。

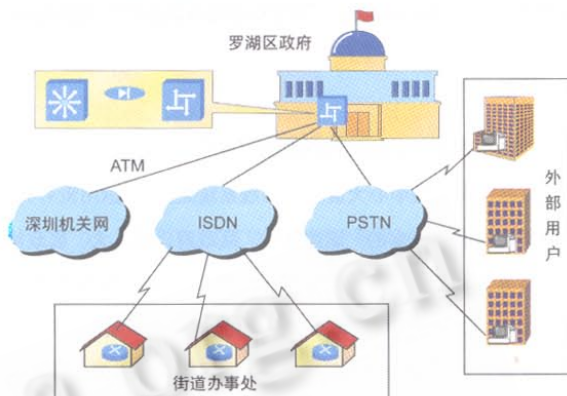


图 2 罗湖信息网广域网逻辑图

5. VLAN 子网划分及 IP 地址划分(略)

6. Internet 访问

罗湖信息网对 Internet 的访问分为两种方式

(1) 直接访问: 只通过 pix 的过滤, 与 Internet 相连, 罗湖信息网中的服务器一般使用这种方式

(2) 间接访问: 只能通过代理服务器实现对 Internet 的访问, 不能直接访问 Internet. 罗湖信息网中各部门一般使用这种方式。

7. 安全性设计

(1) 对于外部 罗湖信息网的接入点有提供拨号和 ISDN 访问的 AS3640 和 CISCO2509, 提供深圳机关网互连和 Internet 访问的 CISCO 7204, 其中来自 7204 的数据的不安全性是最大的。

为了达到对 7204 上来的数据的严格控制

· 通过在 7204 上使用 CISCO 的 IOS 实现对数据包的过滤

· 使用 CISCO 的硬件防火墙 PIX。通过 PIX 将网络分为内网和外网。外网主要放置与 Internet 有关的服务器和 workstation, 内网主要是罗湖区政府办公网。这样只有从内部发起的连接才能被 PIX 认可

· 对于拨号用户和 ISDN 拨号访问, 在 NT 服务器配置 CiscoSecure ACS v2.1 for Windows NT (ACS) 作为访问认证服务器, 认证到网卡一级, 通过 RADIUS 和 TACACS+ 认证协议, 访问路由器会把拨入的用户的用户名传给服务器, 服务器使用 CHAP 方式验证用户的口令, 并根据用户名分配用户不同的权限。

(2)对于内网 安全性主要体现在对数据或其他网络资源的访问控制上。罗湖信息网使用的6509和2948都支持VLAN, 可以划分VLAN来实现访问控制。

通过在6509和2948上的VLAN的划分, 将物理上的网络划分为逻辑上的不同子网, 不同子网之间不能直接相互通信, 确保不同子网内的数据安全。同时, 通过6509的RSP模块可以配置各子网之间的有条件的路由。实现各子网之间的安全访问。

- 原则上各部门为一独立子网

- 各部门子网之间原则上可以相互通信, 重要部门的子网可以单独隔离。

- 各部门子网可以有限制的访问服务器子网

- 拨号用户做为内部的一个子网

信息资源及应用系统

1. 数据库

Oracle8i 是一个面向 Internet 计算环境的数据库, 它改变了信息管理和访问的方式。Oracle8i将新的特性融入了传统的Oracle服务器之中, 从而成为一个面向Web信息管理数据库。Oracle8i支持Web高级应用所需要的多媒体数据, 支持Web繁忙站点不断增长的负载需求。从先进性, 可靠性, 长远性来看, 选择Oracle8i Enterprise Edition能满足罗湖区二期各种应用系统的开发。

2. 办公自动化O A系统

采用当今世界上最先进的群件产品 Lotus Domino/Notes, 针对罗湖的具体特点, 兼顾系统的标准性和通用性, 实现办公、办会、公共信息发布和个人信息处理的无纸化、自动化。力求功能全面细致、操作简单方便, 强调网络互联互通、信息资源共享等。办公自动化系统主要由十个功能模块构成: 领导查询系统、收发文、督查跟踪、会议管理、机要业务、信息刊物出版、机关业务、公共信息、个人信息、系统管理。

系统特点:

(1)使办公事务做到有据可查, 减少工作人员事后的推诿, 加强对工作人员的控制;

(2)可自定义流程, 采用组件化设计, 可实现收文、发文等各种审批流程;

(3)采用 Intranet/Internet 技术, 既丰富了网络的应用, 又充分利用了网络资源;

(4)跨平台特性, 由于采用了Lotus Notes、Java等编程技术, 使本系统在异构网络中亦可正常运转;

(5)用户只需打开邮箱, 或者进入你的待办事项今日

工作便一览无遗。所有需要成员间协同工作的事件, 都将通过电子邮件以工作流的方式进行, 形成真正快捷、安全、有效的办公模式。

(6)融合已有的业务系统, 采用文档数据库加关系数据库的信息管理模式, 充分利用现在信息资源, 帮助建立规范的管理体系;

(7)支持浏览器应用, 使移动办公成为可能;

(8)完善的安全体系, 充分利用防火墙、安全协议及权限管理来保证应用系统的安全性;

(9)构筑政府机关的信息仓库, 实现信息的查询、统计、检索。

3. 视频点播和视频广播

多媒体应用的视频服务器选择高性能, 高可靠性的IBM Netfinity5000服务器配合性能价格比很好的Microsoft Netshow Theatre 做视频点播, 同时配备了视频制作系统工程OptiBase MovieMaker 和视频广播设备FutureTel SuperPresto 实现了100个并发用户的高质量视频点播和多路视频广播。

4. 三层体系结构

内部WEB站点WWW服务器软件运行在两台SUN主机中之一上, 操作系统是Solaris。WEB服务器软件采用Apache Web Server for Solaris。整个内部WEB站点系统的应用开发和运行采用三层体系技术结构, 在WEB服务器和其他应用系统间放置一中间件应用服务器, 采用IBMWebSphere Application Server for Solaris, 通过此应用服务器系统, 内部WEB服务器和其他应用系统集成为一体。结构如图3所示。

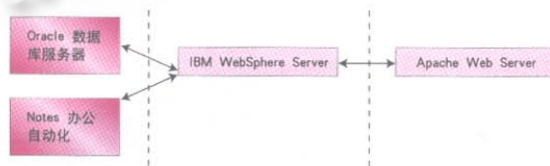


图 3

WEB应用开发涉及两个方面, 一是页面布局和外观设计, 使用Microsoft FrontPage页面设计工具, 二是动态页面的开发, 整个开发基于JSP、Java Servlet的动态页面技术, 通过Java进行编程开发, 使用工具有IBM WebSphere Studio和IBM Visual Age for Java, 进行基于Java的数据库应用组件开发和Notes的开发。开发工具都是运行在Window95或Window98客户端, 开发完后发布到WEB服务器上。■