

量体裁衣建网络记信息产业部电信研究院的网络建议 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/470/2021_2022__E9_87_8F_E4_BD_93_E8_A3_81_E8_c67_470489.htm

信息产业部电信研究院是我国重要的电讯科学研究机构、邮电行业的发展研究中心，担负着前沿技术开发、电信决策、标准制定的重任，因此利用最先进的手段更快地获取最新技术信息、密切跟踪国际发展动态就成了电信研究院工作中重要的组成部分，而Internet则提供了迅速更新、取之不尽的信息资源。但您能想象吗，在1998年新的电信研究院大楼建成以前，研究院甚至还没有一个成形的网络系统，研究人员只能在单个的计算机上用Modem拨号上网，大家交换文件也大多依靠软盘，信息收集和交流的瓶颈在一定程度上影响了科研工作的顺利进行。

系统特点 一方面是提供院内科研人员访问Internet上科技信息的顺畅通道，另一方面也要为院内科研项目的进程和数据管理建立先进、便捷的手段。常年积累的科研成果、报告也需要通过网络来沟通。

建网难点 研究院要处理大量敏感数据，其研究项目也都是热点课题。这些数据有着巨大的无形价值，所以安全性就成了电信研究院网络建设必须考虑的重要问题。电信研究院的网络，不仅要提供给科研人员一个通向Internet资源的通畅接口，而且如何利用这个网络系统建立科研辅助、内部信息交流、员工培训等众多应用也是网络建设开发的重头戏。

网络特点 这是一个快速以太网结构的网络，速率为服务器端100M、客户端10M。整个网络结构分为三段：外部的Internet、中间的FTP服务器、DNS服务器和WWW服务器以及内部的网管、数据库、VOD和其他应用

服务器。电信研究院信息网络始建于1997年。随着1998年电信研究院大楼竣工，以及网络系统开始运行，电信研究院的信息网络跨上了一个新的台阶。这个总投资约一千万元的网络系统以电信研究院大楼的布线系统为基础，采用了自己开发的应用系统。目前已有300台计算机接入该网络。不管是访问Internet，还是院内各种信息交流都可以做到畅通无阻，已经成为科研工作的重要支柱。特点鲜明看需求 电信研究院网络中心的庞中坚工程师告诉记者：研究院网络建设的目的就是为科研服务。最主要的应用是：一方面提供院内科研人员访问Internet上科技信息的顺畅通道，另一方面也要为院内科研项目的进程和数据管理建立先进、便捷的手段。常年积累的科研成果、报告也需要通过网络来沟通。同时，对外的信息服务现在还在筹备中。所以这个网络实际上也可以看成是一个庞大的Intranet系统。电信研究院自身的特点对网络建设提出了不少特殊的需求。作为中国电信产业的决策机构和研究中心，研究院要处理大量敏感数据，其研究项目也都是热点课题。这些数据有着巨大的无形价值，一旦网络被人攻击、重要数据丢失，就会造成无法估量的损失，所以安全性就成了电信研究院网络建设必须考虑的重要问题。防火墙技术是目前广泛采用的网络防护措施，在保障内部网络使用的同时，避免不友好的用户从未被授权的外部节点访问被保护的内部网络。当然，内部网络的安全同样重要，如何防止从接入Intranet的计算机上对其它计算机进行非法访问，或通过下属院所的远程接入攻击网络也是电信研究院网络建设需要面对的问题。电信研究院的网络，不仅要提供给科研人员一个通向Internet资源的通畅接口，而且如何利用这个网络系统建

立科研辅助、内部信息交流、员工培训等众多应用也是网络建设开发的重头戏。在研究院科研项目的立项、审批、结项、评奖等过程中，有大量繁琐的表格需要填写，有不少公章和签字等待科研人员一个一个地去跑，如果能将这个过程“数字化”，完全在网络上完成，将大大提高科研效率。此外，研究院每年要产生大量科研成果，同时也关注着每个电信方面的重要的会议。及时收集总结相关资料，如果这些最新的资料能让科研人员便捷地共享，将会成为一笔宝贵的财富……另外，按照庞中坚工程师的话说：“既然是电信研究院的网络，那么像VOD（视频点播）、视频会议等视频应用肯定必不可少。”为了适应视频数据流的自身特点，整个网络系统的带宽、服务上的相关应用程序、服务器的可扩展性等诸多要求都一下子浮出水面，成为系统选型时必须面对的问题。软硬兼施筑防火墙 高达12层的电信研究院大楼是按照智能大厦的标准设计的。在建设中已经基本完成了布线的工作。所以网络建设的主要工作是选择合适的硬件设备和开发相关的应用系统。这是一个快速以太网结构的网络，速率为服务器端100M、客户端10M。安全性是电信研究院网络建设首当其冲的要求，也确实让设计人员投入了很大的精力，进行过数次方案论证。所以在本次采访中，庞中坚工程师最常挂在嘴边的：“两层防火墙、三段式网络结构”，给记者留下了很深的印象。黑客软件的不断增加，给网络安全带来了不小的威胁。魔高一尺，道高一丈。网络安全技术的发展使得黑客们能钻的空子越来越少了。电信研究院的网络设置比较特殊，筑起了两道防火墙，最大限度地防止非法访问的发生。在紧邻Internet的路由器后是钢筋铁骨的硬件防火墙Cisco Pix

；在内部网络外还有一道以柔克刚的软件防火墙Gauntlet Firewall。这两堵“墙”将整个网络结构分为三段：外部的Internet、中间的FTP服务器、DNS服务器和WWW服务器以及内部的网管、数据库、VOD和其他应用服务器。而在网络设计的初期，两层防火墙是放在一起的。网络只分为内外两段，FTP、DNS和WWW服务器被置于保护之外，很容易受到攻击。实际上，对防火墙设置的这项改动，也是电信研究院网络从设计规划到实际建设中最大的改进。第一层Cisco Pix硬件防火墙主要是通过包过滤和地址转换来保障网络安全。其核心基于Adaptive Security Algorithm (ASA) 算法，对所有通过防火墙的信息包进行校验。能有效地阻止不速之客对内部网络的访问。同时Cisco Pix的NAT地址转换功能使得内部网络互相通讯采用内部IP地址，而对外连接时转换为外部地址。这样外部访问者只能看到假的IP地址，无法对服务器进行真正的攻击，而且屏蔽了很多端口。Cisco Pix实际上保护了对外公开的FTP服务器、DNS服务器和WWW服务器。与此同时，它还可以通过地址转换扩大和重新设置IP地址，缓解IP地址不足的情况。而第二层防火墙又为这些服务器增添了对内防护的功能，网络内部的人员对外访问也需要通过Gauntlet防火墙，所以它们也不会受到来自内部的攻击。“因此，这种攻击的可能性非常小。”庞中坚工程师笑着解释说。话虽这样说，内部网络自身的安全性也是不容忽视的。这个设计规模为600台接入客户的网络现在共有300多台计算机接入，其中绝大部分安装了微软的Win95或Win98操作系统。它们都采用广播包来进行通讯，如果不加抑制，任何一台接入网络的计算机都可以在“网上邻居”中看到所有接入的

计算机，成为安全的隐患。因此，电信研究院网络中的每个单位都按照VLAN虚拟局域网设计，用户只能在“网上邻居”中看到自己科室的计算机，进而防止广播风暴的产生，进一步保证了网络资源的安全。由于电信研究院并没有外地的分支机构，因此这个网络主要的覆盖范围，就是在新建的研究院大楼内。不过，大楼之外的北京几家下属院所已经建立了自己的网络系统，如何与它们进行信息交流又对整个网络的安全提出了挑战。通过Internet交换信息会使网络的安全系数大打折扣；直接通过专线连接投资较大，仿佛又没有必要。根据整个研究院都通过Lotus Notes应用来共享网络资源的特点，他们采用了两个服务器直接拨号相连的方式，主要进行内部邮件的通讯。因为Lotus Notes在连接时要进行非常严密的安全认证，让黑客毫无可乘之机。我们可以看到，经过精心的设计和配置，电信研究院的网络可谓是固若金汤，无论是妄图通过Internet入侵的黑客，还是来自内部网络的非法访问都会被拒之门外。信息产业部电信研究院Intranet结构图

着眼未来选硬件 谈到硬件设备的选型，电信研究院网络中心的庞中坚工程师表示：“我们选型的时候不仅考虑到设备自身的性能指标等几个因素，而且也非常重视设备日后的可扩展能力，力争让网络系统在一段时间内能够通过扩展来适应信息技术惊人的发展速度，最大限度地保护投资。”正是基于这种考虑，电信研究院选择了3台SGI Origin系列服务器，其中包括一台作为内部WWW服务器的Origin2000，两台作外部WWW服务器和内部Proxy服务器、DNS服务器和VOD服务器的Origin200。SGI的Origin系列服务器出色的运算性能、强大的I/O能力自然不必多说，它在视频数据流处理方面的特

殊优势加上WebFORCE MediaBase软件系统使它成为VOD系统的必然选择。而电信研究院在选型时更看重的是Origin系列服务器良好的可扩展性。O2000和O200都采用了SGI独特的CC - NUMA (Cache Coherent - Non Uniform Memory Access , 高速缓存一致性的非均匀内存访问) 结构 , 能够让用户通过增加CPU的数目来轻松地扩展系统 , 同时也能对投资加以保护。目前电信研究院的O2000服务器有4个CPU , 而SGI公司1998年已经可以实现256个CPU的扩展系统 , 这些CPU通过特有的Craylink光纤高速互连的系统 , 最高可以达到在1024个CPU , 以内保证性能与节点数目的线性增长关系。O200服务器也可以由单机扩展到双塔、“大立柜”甚至“大立柜组” , 成倍地提高处理能力 , 让用户在日后升级时也可以发挥目前的设备的作用。而且这些拥有多个节点的高速服务器并不需要用户在编程处理上作特殊处理 , 用户依然可以像面对单个的系统一样运行各种通用的应用程序、进行系统开发。在网络交换机的选择上 , 电信研究院采用了Cabletron模块化的5000系列交换机 , 它们支持媒体流的高带宽 , 可以满足VOD应用的大吞吐量要求 , 而且这些交换机模块可以通过简单的叠加来扩充处理能力。为了提高网络的可靠性 , 这个网络中使用了两台主交换机 , 如果其中一台发生故障 , 可以迅速地把一些重要客户转移到另一台正常运行的交换机上。在网管平台方面SUN具有公认的优势 , 电信研究院网络中的网管、VLAN虚拟网络管理服务器也采用了SUN Ultra系列服务器。量身定做巧应用 通过上面的描述 , 读者对电信研究院的网络建设可能已经有了一些了解 , 这是一个安全、高速、可靠、有着出色扩展能力的网络 , 那么在

这个完善的硬件平台上，又开发了哪些应用系统呢？电信研究院网络的应用主要在两个方面基于Lotus Notes的和基于Web方式的应用，利用Notes的内部邮件系统，大家可以很方便地协同工作，而网上交流都采用Web界面，研究院内部发布通知、进行讨论都变成了数码方式。由于Lotus Notes系统在群件、协同工作、内部邮件方面功能非常强大，而且具有与系统平台无关性，庞中坚工程师说他们几乎是毫不犹豫地选择了Notes作为应用平台，并在其上自主开发了科研项目管理系统，让繁琐的科研项目申报审批工作通过“纯数字”的方式变得高效便捷。科研人员再也不用为了签字和公章耗费大量时间了，这个科研项目管理系统完全接管了项目进行的全过程。按照项目管理的规范，立项过程中申请人把项目报到所科技处，所科技处再转到院科技处，其管理员把项目分配给具体的相关人员审阅并呈报给分管的院长，审批完毕后返回给立项人，项目就开始具体实施了；在科研项目的进行过程中，各种报告、调研资料不断写入网络上的数据库，管理系统会保持对项目进行跟踪；结题与立项过程类似，经过报批后项目完结；到年底时，管理系统还会整理科研项目进行报奖。现在电信研究院中，这套基于Lotus Notes群件的科研管理系统已经完成连接、开始运行，而下一步工作就是要连到信息产业部，让科研项目的全过程在网上畅通无阻地进行。基于Web界面的应用系统则是电信研究院员工进行信息交流的重要手段，而且今后还会进一步对外公布。其中有研究院历年来积累的科研成果；在科研辅助栏目中，存放了几十类科研项目的申请文档模版，科研人员可以从网络上直接下载模版，完成电子文档，大大方便了科研项目审批工作的进行。

；在资料情报栏目中，则收集有国内外各种电信相关会议资料，电信研究院规定，每个参会的研究人员回来后都要将资料整理完毕放在网络的数据库中，资源共享使得这些信息的价值得到了充分发挥。电信研究院网络应用的VOD视频点播系统也包含在Web界面中，主要基于SGI的WebFORCEMediaBase软件系统开发，界面简单直观。MediaBase系统可以为各种平台的客户机提供出色的视频服务，而且支持大量的视频流格式包括低传输速率的H.263和RealNetworks格式及要求高传输速率的MPEG1和MPEG2格式。此外，Web界面中还包括了内部的公告板、讨论系统，员工们的交流也进入了网络时代。采访后记谈起电信研究院的整体网络建设，虽然规模和投资都比较大，但还是一个典型的Intranet内部网，是以科研辅助功能为主要目的的。但它却又不很平凡，大量实用的选型设计使它确实确实发挥了自已应有的作用。在采访过程中，庞中坚工程师告诉记者，电信研究院的网络建设在立项时也有许多公司参加投标，并提供了不少各具特色的方案，但他们最终还是决定自己选型设计，并提出了别具一格的“两层防火墙、三段式网络”结构，使网络建设中最关键的安全问题得到了圆满的解决。在采访中，我们还谈到了网络打印的设置，庞中坚工程师说，由于他们的办公环境比较分散，采用专门的打印服务器加网络打印机的方案无形中会给科研人员增加许多“冤枉路”，所以采用了在每个科室共享一台普通个人激光打印机的方式，反而比较实用……正是这些从实用角度考虑的设计，让电信研究院的科研人员能用得舒心，让网络中心的管理人员能管得放心，同样让记者感受到实用是金。100Test 下载频道开

通，各类考试题目直接下载。详细请访问 www.100test.com