一个 INTERNET 拨号站点的建设

吕淑贤　（东北财经大学计算中心　大连 116023）

摘要：本文介绍了 INTERNET 拨号站的系统构成。以 WINDOWS NT 4.0 为例，介绍了系统的各主要部分。

关键词：DHCP　MAIL SERVER　PROXY SERVER　CISCOSECURE EASYACS

从 ISP 处得到一段 IP 地址，掩码是 255.255.255.248，即八个 IP 地址。在这段地址中可用的地址有六个，其中一个地址用于网关，实际可以使用的 IP 地址只有五个。这在实际应用中会感到紧张，针对这个问题，我们提出了一个 INTERNET 拨号站的建设设想，用很少的 IP 地址资源实现用户拨号访问。以实际 INTERNET 应用带动网络系统的发展和建设。建设一个 INTERNET 拨号站点虽然投资不大，却涉及了广域网，局域网及应用系统几乎所有的问题，可以说是一个完整的系统框架，站点的建设不但检验了系统的设计、所选的各种硬件、软件和集成商的真实情况，同时也大大地丰富了技术人员管理网络、开发应用的经验，为进一步的发展做好了技术、人员、应用等各方面的准备。

一、系统方案

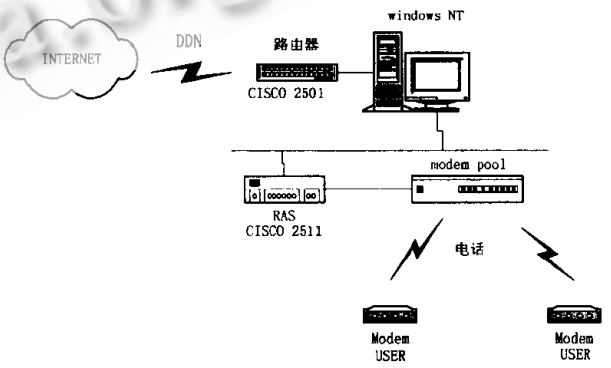
我们选择了 Netscape 和 Microsoft 的产品，理由主要是：MICROSOFT 提供了以网络操作系统 Windows NT 为基础并且相互高度集成的服务器软件系列。为应用系统提供了完整的解决方案。Netscape 的 PROXY SERVER 和 MAIL SERVER 相对于 Microsoft 产品而言主要是系统开销小、运行效率高。网络建设方案遵循易扩展、跨平台、充分利用现有资源的原则。局域网：采用普通以太网产品，使该网络具有较高的性能价格比和良好的可扩充性。远程拨号接入：通过 Cisco 2511 拨号服务器及 U.S. Robotics 调制解调器池实现远程的拨号接入，为社会提供信息服务。INTERNET 接入：通过 DDN，由 Cisco 路由器实现与 Internet 的专线接入。安全、计帐系统：通过 PROXY 和 CISCOSECURE EASYACS 实现远程拨号入网用户的确认及计帐管理，确保网络的安全。

主要的网络设备有：CISCO 2501 路由器、CISCO 2511 访问服务器、HUB、网卡、NT 服务器及调制解调器池。

二、网络应用系统设计

1. 系统构成

在应用系统的设计上，我们使用一台有 128MB RAM 的奔腾 166 建立了一个 WINDOWS NT SERVER。在 NT 服务器上加装了两块网卡 3c509 和 ne2000，安装了 NT 自身的 DHCP 服务器，netscape 的 MAIL SERVER 2.0 和 PROXY SERVER2.0 服务器，CISCO 公司的 CISCOSECURE EASYACS 等几个比较重要的应用软件。NT 服务器上的两块网卡，3C509 用与连接 INTERNET，设有合法的 IP 地址（203.93.53.4X）。NE2000 网卡设立内部 IP 地址（10.0.1.1）。两个网卡之间禁止路由转发，内部地址与外部的连接通过代理服务器。拨号服务器（RAS）连接在内部网络上，使用内部地址（10.0.1.2）。DHCP 分配的地址池为 10.0.2.1 到 10.0.2.254。代理服务器代理 10.0.1.X 和 10.0.2.X 的地址转发。邮件服务器对内部网络和外部网络都是透明的，保证拨号用户正常地使用 INTERNET 的 E-MAIL。



CISCO 2501 路由器的 WAN 口连接 INTERNET，以太网口连接本地子网，采用静态路由协议。NT 服务器的 3C509 网卡连接到这个子网上，使得 NT 服务器与 INTERNET 连通。NT 服务器的另一个网卡 NE 2000 连

到内部网上，CISCO 2511 访问服务器连接在内部网上，接受 NT 服务器提供的 DHCP 服务。如上图所示。

2.主要部分说明

(1)DHCP 服务器。对于使用 TCP/IP 协议的网络而言，每一台主机都必须有一个 IP 地址，并且通过此 IP 地址与网络上的其他主机通信。可是管理与分配客户端的 IP 地址及环境配置的工作，常常困扰着网络系统管理员，不过现在你可以通过 DHCP 所提供的功能，减轻这些网络管理的负担。Windows NT 计算机中安装 DHCP 服务器的软件，远程拨号入网的工作站也必须启用 DHCP 的功能。当 DHCP 工作站启动时，它就会自动与 DHCP 服务器通信，并由 DHCP 服务器给 DHCP 工作站提供 IP 地址。DHCP 服务也简化了远程拨号入网工作站的网络设置。

事实上，DHCP 服务器不但可以给 DHCP 工作站提供 IP 地址，它还可以提供给 DHCP 工作站一些其他的设置。如：默认网关(Default Gateway 或 Router)，其他的环境设置，WINS Server、DNS Server 等。

(2)Netscape 邮件服务器。Netscape 邮件服务器提供了基于 Internet 标准的 e－mail 方法。邮件服务器符合所有公用 e－mail 标准。如 SMTP、MIME、POP3 和 POP3 的新一代，Netscape 邮件服务器作为主邮件服务器。

让我们简单介绍 e－mail 的工作及使用的标准。

发送邮件：

①用户用 e－mail 客户程序构造信息和标识主送人与抄送人。

②E－mail 客户程序将信息发送到本地邮件服务器(网络管理员在配置 e－mail 客户程序时会标识本地服务器)。

③本地邮件服务器查询域名系统以找出相应的接收方邮件服务器。

④一旦找到接收方服务器，本地邮件服务器即用 SMTP 协议把信息发到该服务器。

⑤如果目标邮件服务器无法送达，发送邮件的服务器将信息放在队列中，以后在试。

接收邮件：

①e－mail 客户程序用 POP3 或 IMAP4 访问主邮件服务器。

②e－mail 客户程序输入 POP3 或 IMAP4 用户名和相应口令。

③所有新信息从邮件服务器下载到 e－mail 客户程序。

④阅读 e－mail 。

邮局协议 V3.0(POP3)是 e－mail 客户程序访问邮件服务器信息的传统方法。POP3 是个简单的协议，依靠用户名和口令表示每个用户。可以手工输入用户名或在启动邮件客户程序时自动登录，然后下载所有邮件服务器上等待该客户程序接收的信息。POP3 客户程序只能处理来自一个邮箱来自一个邮局的信息，所以用多个 e－mail 帐号很不方便，通常要求用户有不同配置文件指向各个邮箱，或要求用户手工输入第二个邮箱信息 。POP3 客户程序可以指定是否删除下载之后服务器上的信息或将信息留在服务器上。没有办法选择下载服务器上的具体某个信息。

使用支持 IMAP4 的邮件客户程序，用户依靠用户名和口令登录邮件服务器，在 IMAP4 中，服务器只发送头信息到 e－mail 客户程序，而且 e－mail 客户程序可以浏览多个邮箱中的信息头，然后只下载所要的信息。IMAP4 还允许用户搜索服务器上的信息文本之后再决定下载哪个信息。

邮件服务器(Mail Server)支持 POP3 和 IMAP4 邮件客户程序。Navigator 3.0 邮件客户程序属于 POP3 客户程序，Netscape Communicator 则使用 IMAP4 邮件客户程序，两者都可和邮件服务器通话。

配置 DNS

域名系统和邮件服务器之间有着密切的关系，当邮件服务器要将邮件信息发送到另一个它不提供服务的域时，它用 DNS 确定相应的目标邮件服务器，其他人要向你发送信息时，也要用 DNS 确定所用的邮件服务器。为此，要在 DNS 加进邮件服务器所负责的每个邮件域的 MX 记录。此外，还要确保操作系统配置成有效域名。

基本邮件服务器管理

Netscape 邮件服务器是最容易管理的邮件服务器。大多数时候，管理只是增加、修改和删除用户邮件帐号。但配置服务器时可能还要注意某些 SMTP 参数。邮件服务器的配置信息则大部分放在 Windows NT 注册表文件中，为了查阅这些设置，在 Windows NT 中使用注册表编辑器(运行 regedt32)，尽管在这里可以查阅信息，但改变应在服务器管理器或 e－mail 窗体中进行，注册表是

严肃的，小小的语法错误就会使邮件服务器无法工作。

用户帐号位于邮件服务器核心，这些帐号包含在服务器上有 e－mail 帐号的每个用户的信息。邮件服务器用户帐号包含用户全名之类的用户身份信息和 e－mail 地址别名之类的邮件特有信息。用户帐号包含下列信息：用户真名、邮件帐号口令、Finger 信息（Finger 查寻使发送者可以找到你的用户 e－mail 地址）、e－mail 地址信息、Internet 邮件地址（包括地址别名）、From 地址改写样式（邮件服务器发送的 from 地址消息格式）、局部传送信息：POP3/IMAP4 登录名和可选的邮件站目录、转发地址（帐号别名）、帐号安全参数：安全参数包括访问域和 Finger 访问域、自动答复信息：假期、答复、回显。

(3)代理服务器。WEB 缓存代理服务器（PROXY SERVER）可以为任何大小的网络实现更快、更经济、更安全地访问 WEB。它检查已被缓存起来的 WEB 页面及用户曾经访问过的 WEB 页面。如果页面已经被修改，那么代理服务器在本机上重新存储更新后的页面。代理服务器还可以根据一定的要求，自动访问和下载相关的页面。当用户重复访问那些常用的资源时，可以直接在代理服务器上获得，没必要访问 INTERNET 了，从而节省了时间。

代理服务器可以检查和存储大量的 WEB 页面。本地用户访问某个缓存页面时，代理服务器快速的发出缓存页面，同时代理服务器还可以有效地利用 INTERNET 连接，使多个用户共享单个连接，节约费用。代理服务器使内部网络有很好的安全性。代理服务器根据客户请求向目标服务器提申请，然后取得请求的 HTML 页面或其他信息并发送回浏览器，请求客户机不与目标服务器对话。在这个中间人角色中，代理服务器既有客户机过程也有服务器过程，它在接受客户机请求时是个 HTTP 或 FTP 服务器，而在向其他服务器发出请求时又是个客户机。通过过滤用户或 URL 资源提供了进一步的安全性。通过代理服务器上保存的日志跟踪最终用户活动。使用代理服务器还可以节省 IP 地址，只要一个 IP 地址即可实现群组拨号服务。

代理服务器的管理

管理员要对代理服务器做的主要工作是配置。这个配置包括建立用户组本和资源组。可以配置的代理服务器操作：打开或关闭代理功能、客户机请求选择路由、转发客户机 IP 地址、请求缓存命令缓存、限制访问、URL 地址过滤、映射和重定向 URL。在 Netscape Proxy Server 中，网络管理员可以基于多项内容来控制对 WEB 的访问，这里只有 IP 地址控制。

配置客户机使用代理服务器

管理员要建立代理服务器用户的使用规则，如果要用代理服务器登记所有 Internet 使用、统计用户访问 Internet 或限制特定 URL 的访问，则要确保用户使用代理服务器。为了确保至少在 Internet 连接中使用代理服务器，必须使用内部虚拟地址（10.0.＊.＊）防止用户不经代理服务器而访问 Internet。只要让代理服务器实现 IP 地址的代理即可。

在 Netscape Navigator 中，有两种方法使用代理服务器：手工引导浏览器到代理服务器或用代理自动配置。使用 APC（自动代理配置）更精彩，可以用相同配置配置每个 Navigator 客户机，然后管理位于中央的包含代理配置信息的脚本。这个：JavaScript 脚本必须由管理员手工生成。使用 APC 时，客户机启动时将脚本装入自己的自动配置中。这个脚本包含客户机如何使用代理服务器的信息。APC 通常用于有多个代理服务器和多个客户机。

三、用户拨入计帐服务

在 NT 服务器上安装了 CISCOSECURE EASYACS 1.0 软件，它与 CISCO 2511 拨号访问服务器配合使用，可以完成对用户的确认、授权和计帐。

CISCOSECURE EASYACS 1.0 是一个基于 WINDOWS NT 4.0 的访问控制服务器，它使用 TACACS＋协议，提供对用户的确认、授权和计帐，即 AAA。CISCOSECURE EASYACS 即可以使用 WINDOWS NT 的用户数据，也可以使用自己定义的用户数据。CISCOSECURE EASYACS 的授权不但可以是用户名，也可以是 IP 地址。同时 CISCOSECURE EASYACS 提供了用户完整的计帐信息。使用 CISCOSECURE EASYACS，必须调整 CISCO 2511 访问服务器的设置。在 CISCO 2511 的配置中加入 AAA 指令，确定用户数据库的类型。我们使用 CISCOSECURE EASYACS 的用户数据进行网络访问的确认。而不使用 WINDOWS NT 的用户。

（来稿时间：1998 年 3 月）