服务器知识手册（三）

狄登峰 主编

需要全本请访问 www.ertongbook.com

目　　录

路由器的应用 1

打造 Windows 2000 路由器 1

交换机及路由器如何更加安全 4

路由器和网络安全 7

Cisco 路由器的配置基础 9

Cisco 路由器存储器及 IOS 升级 26

WinRoute 拨号参数设置 28

WinRouteIP 地址设置 30

WinRouteDHCP 服务器设置 31

WinRoute 特性 33

网络路由技术基础 34

Windows NT 服务器用作路由器 44

校园网建设 49

构筑牢固的校园网络安全体系 49

校园网中 IP 盗用应如何解决 55

校园网运行管理与安全策略 62

搭建机房计费管理系统 68

校园网也用虚拟 Web 主机 75

校园网网络方案设计及分析 82

校园宽带网代理服务器的设置经验 97

中小学多媒体教育资源的存储及管理方案 99

Web 服务器 103

防火墙环境中 DNS 的配置 103

Apache+Tomcat 实现 Web 服务 114

政府 Web 网站的创建与管理 122

路由器的应用

打造 Windows 2000 路由器

路由器的一个作用是连通不同的网段，而另一个作用是选择信息传送的线路。选 择通畅快捷的线路，能够大大提高通信速度，减轻网络系统的通信负荷，节约网络系统资源，提高网络系统畅通率，从而让网络系统发挥出更大的效益。

假设现在有机房 1（网段为“192.168.1.XXX”，连接到 HUB1）和机房 2（网段为“192.168.2.XXX”，连接到 HUB2）两个网段，而这两个网段的 HUB 已相互连接。现在要求两个网段之间能够相互 Ping 通，并且可以通过“网上邻居”实现互访。

这时就需要路由器的帮助了，但由于路由器价格较高，限制了我们不能大范围使用。不过，这种普通的访问完全可以通过 Windows 2000 Server 自带的“路由和拨号连接”服务，利用两张网卡来实现网卡路由的功能。

一、TCP/IP 属性设置

1.首先，确保服务器·服务器系统采用 Windows 2000 Server·已安装好了两张网卡。然后，先用一条双绞线将 HUB1 和网卡 1 连接起来，再用另一条双绞线将 HUB2 和网卡 2 连接起来。

2.在 Windows 2000 Server 中，打开控制面板中的“网络和拨号连接”，如果两张网卡均已安装成功，则可以看

到其中有两个“本地连接”。接着，在网卡 1 上单击右键，选择“属性”以打开此本地连接的属性设置窗口。

3.选择本地连接属性设置窗口中的“常规”项，在它的组件列表中双击“Internet 协议（TCP/IP）”以进入 TCP/IP 属性设置窗口。

4.在 TCP/IP 属性设置窗口中点选“使用下面的 IP 地址”，再在“IP 地址”栏中输入“192.168.1.1”，“子网掩码”为“255.255.255.0”，其他项目不用再填，直接点击“确定”即可。

经过以上几个步骤的设置，就将网卡 1 绑定好 IP 地址“192.168.1.1”，它将是网段 1 中的客户端的网关地址。再用同样的方法，将网卡 2 绑定好 IP 地址“192.168.2.1”，它将是网段 2 中的客户端的网关地址。

服务器端设置完成后，再设置所有的客户机端，将它们的默认网关地址和默认 DNS 服务器地址均设置为本网段内的网关地址即可。

二、配置路由器

1.在 Windows 2000 Server 中，依次点击“程序·管理工具·路由和远程访问”，便可以进入路由器的配置主窗口。不过，此时的“服务器状态”是系统默认的“未配置”（图 1）。

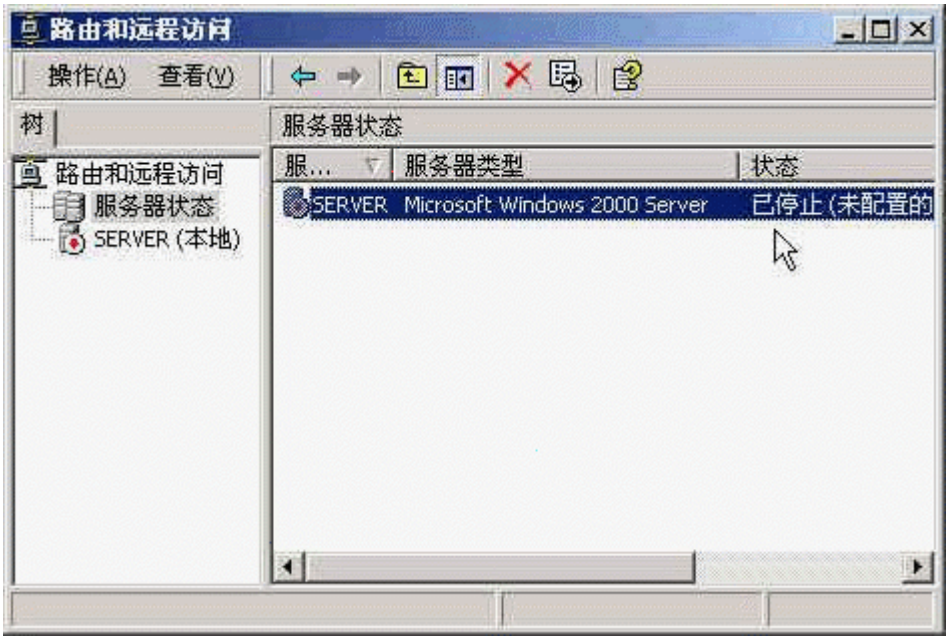


图 1

2.在主窗口左侧的“SERVER”（服务器名）处单击右键，选择“配置并启用路由和远程访问”，以打开此服务的安装向导。

3.在“路由和远程访问服务器安装向导”中，当出现“公共设置”时，选中“网络路由器”再单击“下一步”。

4.接下来会要求选择路由所需要的协议，此时在协议列表框中应该至少已有了“TCP/IP”一项，直接点击“是”，所有可用的协议都会出现在列表上，再点击“下一步”继续。

5.此时会显示系统提示信息“您想通过请求拨号来访问远程网络吗?”。由于不需要通过拨号访问远程网络，因此在此处点选“否”再点击“下一步”即可完成路由器的配置工作。此时，在“路由和远程访问”窗口中可以看到

需要全本请访问 www.ertongbook.com

已经完成了的相关操作（图 2）。

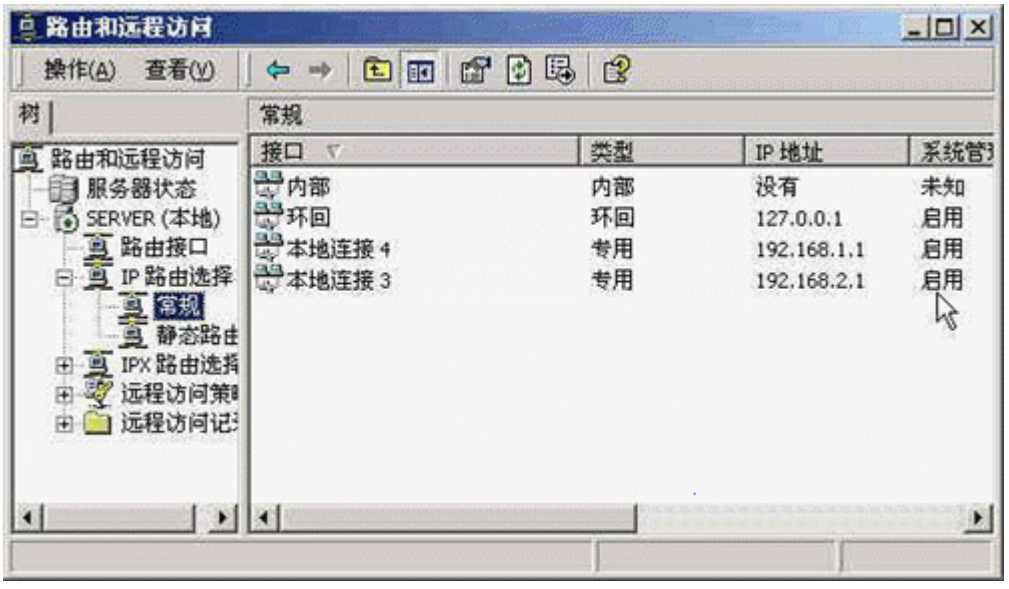


图 2

通过以上配置，一台路由器就架设完成了。现在我们来测试实际的连接效果：

1.在任何一个网段的任意一台计算机上，均可 Ping 通包括本网段、另一个网段以及服务器在内的所有计算机的 IP 地址。

2.此时打开任意一台计算机的“网上邻居”，都可以看到所有计算机的名字都已被加入到列表中了，双击任何一个计算机图标即可访问它所共享出来的资源。

交换机及路由器如何更加安全

传统的网络安全技术侧重于系统入侵检测，反病毒

软件或防火墙。内部安全如何？在网络安全构造中，交换机和路由器是非常重要的，在七层网络中每一层都必须是安全的。 很多交换机和路由器都有丰富的安全功能，要了解有些什么，如何工作，如何部署，一层有问题时不会影响整个网络。交换机和路由器被设计成缺省安全的，出厂时就处于安全设置的状态，特别操作的设置在用户要求时才会被激活,所有其他选项都是关闭的，以减少危险，网管员也无需了解哪些选项应该关闭。

在初始登录时会被强制要求更改密码，也有密码的期限选项及登录尝试的次数限制,而且以加密方式存储。限期的帐号（维护帐号或后门）是不会存在的。交换机及路由器在掉电，热启动、冷启动，升级 IOS、硬件或一个模块失败的情况下都必须是安全的，而且在这些事件发生后应该不会危及安全并恢复运作，因为日志的原因，网络设备应该通过网络时间协议保持安全精确的时间。通过 SNMP 协议连接管理的名称也应该被改变。

抵挡 DoS 攻击

从可用性出发，交换机和路由器需要能抵挡拒绝服务式 Dos 攻击，并在攻击期间保持可用性。理想状态是他们在受到攻击时应该能够做出反应，屏蔽攻击 IP 及端口。每件事件都会立即反应并记录在日志中，同时他们也能识别并对蠕虫攻击做出反应。

交换机及路由器中使用 FTP，HTTP，TELNET 或 SSH 都有可以有代码漏洞，在漏洞被发现报告后，厂商可以开发、创建、测试、发布升级包或补丁。

基于角色的管理给予管理员最低程序的许可来完成任务，允许分派任务，提供检查及平衡，只有受信任的连接才能管理倔们。管理权限可赋予设备或其他主机，

例如管理权限可授予一定 IP 地址及特定的 TCP/UDP 端口。

控制管理权限的最好办法是在授权进入前分权限，可以通过认证和帐户服务器，例如远程接入服务，终端服务，或 LDAP 服务。

远程连接的加密

很多情况下，管理员需要远程管理交换机及路由器，通常只能从公共网络上访问。为了保证管理传输的安全，需要加密协议，SSH 是所有远程命令行设置和文件传输的标准协，基于 WEB 的则用 SSL 或 TLS 协议，LDAP 通常是通讯的协议，而 SSL/TLS 则加密此通讯。

SNMP 用来发现、监控、配置网络设备，SNMP 3 是足够安全的版本，可以保证授权的通信。

建立登录控制可以减轻受攻击的可能性，设定尝试登录的次数，在遇到这种扫描时能做出反应。详细的日志在发现尝试破解密码及端口扫描时是非常有效的。

交换机及路由器的配置文件的安全也是不容忽视的，通常配置文件保存在安全的位置，在混乱的情况下，可以取出备份文件，安装并激活系统，恢复到已知状态。有些交换机结合了入侵检测的功能，一些通过端口映射支持，允许管理员选择监控端口。虚拟网络的角色虚拟的本地网络 VLAN 是第二层上的有限广播域，由一组计算机设备组成，通常位一多个 LAN 上，可能跨越一个或多个 LAN 交换机，而与它们的物理位置无关，设备之间好像在同一个网络间通信一样，允许管理员将网络分为多个可管理运行良好的小块，将啬、移动、更改设备、用户及权限的任务简化。

VLAN 可在各种形式上形成，如交换口，MAC 地址，

IP 地址，协议类型，DHCP，802.1Q 标志或用户自定义。这些可以单独或组合部署。

VLAN 认证技术在用户通过认证过程后授权给用户进入一个或多个 VLAN，该授权不是给予设备。

防火墙可以控制网络之间的访问，最广泛应用的是嵌在传统路由器和多层交换机上的，也称作 ACLs,防火墙的不同主要在于他们扫描包的深度，是端到端的直接通讯还是通过代理，是否有 session。

在网络之间的访问控制中，路由过滤措施可以基于源/目标交换槽或端口，源/目标 VLAN,源/目标 IP，或 TCP/UDP 端口，ICMP 类型，或 MAC 地址。对于某些交换机和路由器，动态 ACL 标准可以用户通过认证过程后被创建，就像是认证的 VLAN，不过是在第三层上。当未知的源地址要求连入已知的内部目标时是有用的。

现在的网络要求设计成各层次都是安全的，通过部署交换机和路由器的安全设置，企业可以传统的安全技术创建强壮、各层都安全的系统。

路由器和网络安全

路由器（Router）是因特网上最为重要的设备之一，正是遍布世界各地的数以万计的路由器构成了因特网这个在 我们的身边日夜不停地运转的巨型信息网络的“桥梁”。因特网的核心通讯机制是一种被称为“存储转发”的数据传输模型。在这种通讯机制下，所有在网络上流动的数据都是以数据包（Packet）的形式被发送、传输和接收处理的。接入因特网的任何一台电脑要与别的机器相互通讯并交换信息就必须拥有一个唯一的网络“地

址”。数据并不是从它的“出发点”直接就被传送到“目的地”的，相反，数据在传送之前按照特定的标准划分成长度一定的片断——数据包。每一个数据包中都加入了目的计算机的网络地址，这就好比套上了一个写好收件人地址的信封，这样的数据包在网上传输的时候才不会“迷路”。这些数据包在到达目的地之前必须经过因特网上为数众多的通信设备或者计算机的层层转发、接力传递。古代驿站的运作情形就是这个过程的一个形象比喻，在因特网上，路由器正是扮演着的转发数据包“驿站”角色。

流行的路由器大多是以硬件设备的形式存在的，但是在某些情况下也用程序来实现“软件路由器”，两者的唯一差别只是执行的效率不同而已。路由器一般至少和两个网络相联，并根据它对所连接网络的状态决定每个数据包的传输路径。路由器生成并维护一张称为“路由信息表”的表格，其中跟踪记录相邻其他路由器的地址和状态信息。路由器使用路由信息表并根据传输距离和通讯费用等优化算法来决定一个特定的数据包的最佳传输路径。正是这种特点决定了路由器的“智能性”，它能够根据相邻网络的实际运行状况自动选择和调整数据包的传输情况，尽最大的努力以最优的路线和最小的代价将数据包传递出去。路由器能否安全稳定地运行，直接影响着因特网的活动。不管因为什么原因出现路由器死机、拒绝服务或是运行效率急剧下降，其结果都将是灾难性的。

黑客攻击路由器的手段与袭击网上其它计算机的手法大同小异，因为从严格的意义上讲路由器本身就是一台具备特殊使命的电脑，虽然它可能没有人们通常熟识的 PC 那样的外观。一般来讲，黑客针对路由器的攻击

主要分为以下两种类型：一是通过某种手段或途径获取管理权限，直接侵入到系统的内部；一是采用远程攻击的办法造成路由器崩溃死机或是运行效率显著下降。相较而言，前者的难度要大一些。

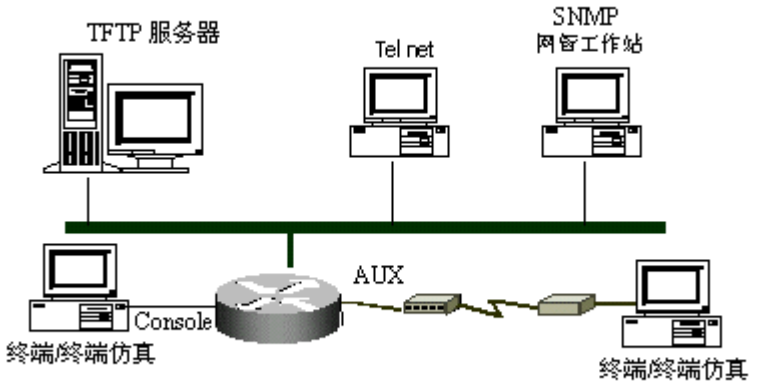
上面提及的第一种入侵方法中，黑客一般是利用系统用户的粗心或已知的系统缺陷（例如系统软件中的“臭虫”）获得进入系统的访问权限，并通过一系列进一步的行动最终获得超级管理员权限。黑客一般很难一开始就获得整个系统的控制权，在通常的情况下，这是一个逐渐升级的入侵过程。由于路由器不像一般的系统那样设有众多的用户账号，而且经常使用安全性相对较高的专用软件系统，所以黑客要想获取路由器系统的管理权相对于入侵一般的主机就要困难得多。因此，现有的针对路由器的黑客攻击大多数都可以归入第二类攻击手段的范畴。这种攻击的最终目的并非直接侵入系统内部，而是通过向系统发送攻击性数据包或在一定的时间间隔里，向系统发送数量巨大的“垃圾”数据包，以此大量耗费路由器的系统资源，使其不能正常工作，甚至彻底崩溃。此次的“桑达”路由器抗攻击性测试活动中，绝大多数的攻击行为就是属于此种类型。令人欣慰的是，用于测试的路由器顶住了来自国内外黑客近 72 小时的“轮番轰炸”，始终巍然挺立。

Cisco 路由器的配置基础

一、基本设置方式

一般来说，可以用 5 种方式来设置路由器：

需要全本请访问 www.ertongbook.com



1．Console 口接终端或运行终端仿真软件的微机；

2．AUX 口接 MODEM，通过电话线与远方的终端或运行终端仿真软件的微机相连；

3．通过 Ethernet 上的 TFTP 服务器；

4．通过 Ethernet 上的 TELNET 程序；

5．通过 Ethernet 上的 SNMP 网管工作站。

但路由器的第一次设置必须通过第一种方式进行，此时终端的硬件设置如下：

波特率 ： 9600

数据位 ： 8

停止位 ： 1

奇偶校验：无

二、命令状态

1. router>

路由器处于用户命令状态，这时用户可以看路由器的连接状态，访问其它网络和主机，但不能看到和更改路由器的设置内容。

2. router#

在 router>提示符下键入 enable,路由器进入特权命令状态 router#，这时不但可以执行所有的用户命令，还可以看到和更改路由器的设置内容。

3. router(config)#

在 router#提示符下键入 configure terminal,出现提示符 router(config)#，此时路由器处于全局设置状态，这时可以设置路由器的全局参数。

4. router(config-if)#; router(config-line)#; router(config-router)#;…

路由器处于局部设置状态，这时可以设置路由器某个局部的参数。

5. >

路由器处于 RXBOOT 状态，在开机后 60 秒内按 ctrl-break 可进入此状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导。

6. 设置对话状态

这是一台新路由器开机时自动进入的状态，在特权命令状态使用 SETUP 命令也可进入此状态，这时可通过对话方式对路由器进行设置。

三、设置对话过程

利用设置对话过程可以避免手工输入命令的烦琐，但它还不能完全代替手工设置，一些特殊的设置还必须通过手工输入的方式完成。

进入设置对话过程后，路由器首先会显示一些提示信息：

--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.

Use ctrl-c to abort configuration dialog at any prompt.

Default settings are in square brackets '[]'.

这是告诉你在设置对话过程中的任何地方都可以键入"？"**得到系统的帮助，按** ctrl-c **可以退出设置过程，缺省设置将显示在**'[]**中。然后路由器会问是否进入设置对话：**

Would you like to enter the initial configuration dialog? [yes]:

如果按 y **或回车，路由器就会进入设置对话过程。首先你可以看到各端口当前的状况：**

First, would you like to see the current interface summary? [yes]:

Any interface listed with OK? value "NO" does not have a valid configuration

Interface

IP-Address

OK?

Method

Status

Protocol

Ethernet0

unassigned

NO

unset

up

up

Serial0

unassigned

NO

unset

up

up

……

然后，路由器就开始全局参数的设置：

Configuring global parameters:

1．**设置路由器名：**

Enter host name [Router]:

2．**设置进入特权状态的密文**(secret)，**此密文在设置以后不会以明文方式显示：**

The enable secret is a one-way cryptographic secret used

instead of the enable password when it exists.

Enter enable secret: cisco

3．**设置进入特权状态的密码**(password)，**此密码只在没有密文时起作用，并且在设置以后会以明文方式显示：**

The enable password is used when there is no enable secret and when using older software and some boot images.

Enter enable password: pass

4．**设置虚拟终端访问时的密码：**

Enter virtual terminal password: cisco

5．**询问是否要设置路由器支持的各种网络协议：**

Configure SNMP Network Management? [yes]:

Configure DECnet? [no]:

Configure AppleTalk? [no]:

Configure IPX? [no]:

Configure IP? [yes]:

Configure IGRP routing? [yes]:

Configure RIP routing? [no]:

……

6．**如果配置的是拨号访问服务器，系统还会设置异步口的参数：**

Configure Async lines? [yes]:

1) **设置线路的最高速度：**

Async line speed [9600]:

2) **是否使用硬件流控：**

Configure for HW flow control? [yes]:

3) **是否设置** modem**：**

Configure for modems? [yes/no]: yes

4) **是否使用默认的** modem **命令：**

Configure for default chat script? [yes]:

5) **是否设置异步口的** PPP **参数：**

Configure for Dial-in IP SLIP/PPP access? [no]: yes

6) **是否使用动态** IP **地址：**

Configure for Dynamic IP addresses? [yes]:

7) **是否使用缺省** IP **地址：**

Configure Default IP addresses? [no]: yes

8) **是否使用** TCP **头压缩：**

Configure for TCP Header Compression? [yes]:

9) **是否在异步口上使用路由表更新：**

Configure for routing updates on async links? [no]: y

10) **是否设置异步口上的其它协议**。

接下来，系统会对每个接口进行参数的设置。

1．Configuring interface Ethernet0:

1) **是否使用此接口：**

Is this interface in use? [yes]:

2) **是否设置此接口的** IP **参数：**

Configure IP on this interface? [yes]:

3) **设置接口的** IP **地址：**

IP address for this interface: 192.168.162.2

4) **设置接口的** IP **子网掩码：**

Number of bits in subnet field [0]:

Class C network is 192.168.162.0, 0 subnet bits; mask is /24

在设置完所有接口的参数后，系统会把整个设置对话过程的结果显示出来：

The following configuration command script was created:

hostname Router

enable secret 5 1W5Oh$p6J7tIgRMBOIKVXVG53Uh1

enable password pass

……

请注意在 enable secret **后面显示的是乱码，而** enable password **后面显示的是设置的内容。**

显示结束后，系统会问是否使用这个设置：

Use this configuration? [yes/no]: yes

如果回答 yes，**系统就会把设置的结果存入路由器的** NVRAM **中，然后结束设置对话过程，使路由器开始正常的工作。**

需要全本请访问 www.ertongbook.com