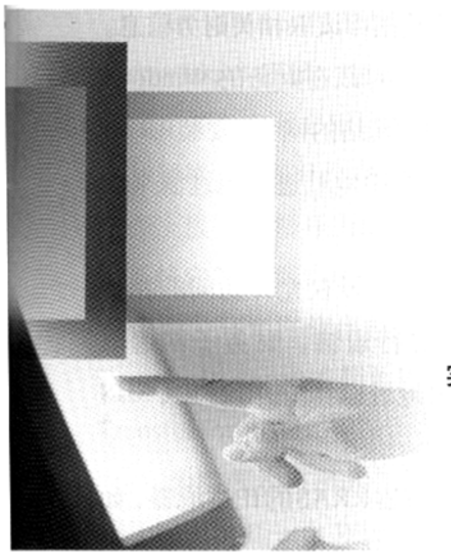
Microsoft 软件路由器及其典型应用



黄 文 东 （广东省佛山电力工业局计算机中心 528000）

摘要：本文通过对Windows服务器软件路由功能的深入分析，结合电力系统计算机网络的特殊实际，在此归纳Microsoft软件路由器的几种典型应用案例，其设置的注意事项与适用范围。

关键词：子网 路由 RRAS 包过滤

1 引言

路由器是用于连接物理上分离的网络并在不同网段之间转发数据，允许处在不同网段中的主机进行通信的网络设备。

然而，时至今日，路由器已经不单纯是一个专门的硬件设备，还可以是一台包含路由软件或操作系统功能的计算机。就Microsoft公司而言，它首先在Windows NT 3.51 引入了路由信息协议 RIP（Routing Information Protocol）与静态路由，为带有Windows NT服务器的小型网络提供低成本的路由方案；接着又推出路由和远程访问服务 RRAS（Routing and Remote Access Service）作为Windows NT 4.0的附加软件，使基于NT服务器的路由功能更为强大和灵活；现在还把更为强壮的RRAS增强版本集成到Windows 2000服务器中。

本文将主要针对Windows NT 4.0的路由和远程访问服务RRAS进行论述。

2 Windows 服务器的软件路由

Windows NT 3.51和Windows NT 4.0自身内置的路由是多协议路由器MPR（Multi-Protocol Router）1.0，能够支持RIPv1、RIPv2与静态路由，但是只提供有限的过滤功能，而且性能低下，静态路由只能在命令行界面用ROUTE ADD来完成，较难使用。

Microsoft 在 Windows NT 4.0 提供的附加软件：路由和远程访问服务RRAS，其研发和测试阶段被称作铁头（Steelhead），除继续支持MPR1.0所提供的路由功能外，允许其作为IP路由器灵活地按源或目的IP地址和源或目的端口号来进行包过滤，新增了对最流行和最标准化的域间路由协议 -- 开放最短路径优先 OSPF（Open Shortest Path First）的支持，另外还提供可以选用点到点通道协议PPTP（Point-to-Point Tunneling protocol）及按需拨号路由DDR（Dial-on-Demand Routing）的WAN路由。RRAS提供了可管理和控制路由软件各个方面的GUI图形用户界面，其管理比基于硬件的传统路由器简单。

3 以 Windows 路由实现电力系统计算机子网互联的安全性分析

在电力系统计算机网络中，存在财务子网、配电监控DA子网与电力调度SCADA子网等，为提高管理水平和工作效率，MIS子网需要与之实现互连以达至信息共享。但是，MIS子网与这些特殊子网互连，必须确保连接的安全性。

由于电力系统计算机网络一般是一个物理上与外界完全隔离的网络，或是通过专用路由器和专业防火墙与Internet等外界网络连接。因此，如果能够保证内部子网互连的安全性，就无须再花费大量资金购置专用路由器和专业防火墙来进行内部子网的互连。

使用路由和远程访问服务RRAS，Windows服务器就可以成为能够灵活地按源或目的IP地址和源或目的端口号来进行包过滤的IP路由器，在系统级上实现网络安全性。其中：

(1) 输入过滤器（input filters），过滤发给服务器的数据包，除减少网络通信量外，还可降低从子网外对服务器和子网内电脑的攻击。特殊地，若子网内的电脑数

目为零，输入过滤器可用于加强Windows服务器自身的主机级安全性。

(2) 输出过滤器（output filters），过滤子网内发出的数据包，防止从子网内激活对其他子网主机的攻击，从而显著提高网络的整体安全性。

4 典型应用案例

结合电力系统计算机网络的特殊实际，在此归纳Windows软件路由器的几种典型应用案例。

4.1 MIS子网间互联（进行网络分段或子网互连）

随着计算机应用的普及，计算机网络的规模也日益扩大，使用光纤可连接地理位置比较分散的局域网。为方便进行网络管理，充分利用现有带宽，有必要进行网络分段，使不同子网之间处于冲突域隔离状态，减少网络中信息包的碰撞概率以降低网络广播风暴发生的可能性。

本应用可利用网络中原有的Windows服务器加设一块或多块网卡并安装RRAS作为软件路由器对局域网进行分段并实现互连，典型网络结构如图1所示。

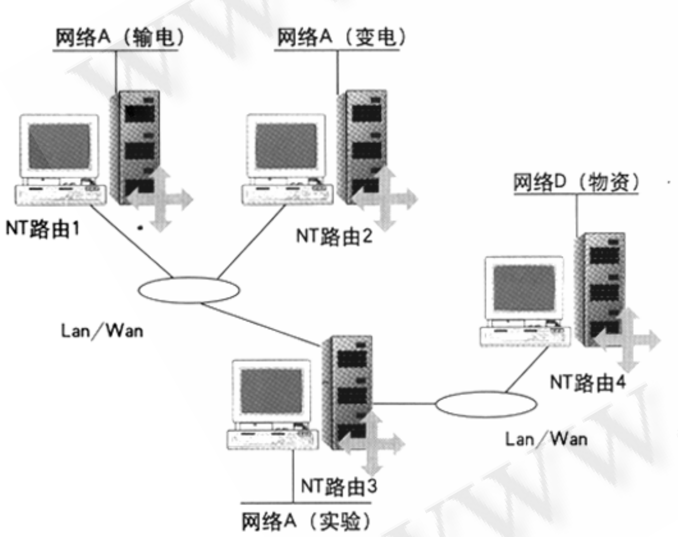


图 1

根据经验，一般可按MIS各功能子系统即用电营业、物资购销、输电、变电、试验等进行子网划分，也可按建筑物的地理分布即按不同地点的建筑物或按同一建筑物的不同楼层进行子网划分。

一般MIS网络均为多路径、动态IP的网际网络，其中对于小型到中型规模网络适宜选用RIP路由；对于较大型到特大型规模网络适宜选用OSPF路由。

4.2 MIS子网与财务子网互联（基于IP地址进行包过滤）

MIS子网与财务子网互联，其安全方面的具体需求为：MIS网络中只允许上级主管领导用机访问财务Windows服务器，财务子网内机器能够从MIS网络中的用电营业子网、物资购销子网的数据库读取相关财务信息。

为实现本应用的工程目标，可以在财务的Windows服务器上加设一块用以连接MIS网络的网卡，安装RRAS作为路由器，并使用RRAS基于IP地址进行包过滤来实现与MIS网络的安全互连。其中：

(1) 财务子网与MIS网络中被授权允许访问的相关机器必须使用TCP/IP协议进行通信，财务子网选取RFC1918指定的C类私用IP地址以独立网段接入MIS系统。

(2) 对于财务Windows服务器RRAS的IP过滤器，如果分配给MIS网络被授权允许访问财务子网的地址号为2的n次幂（2, 4, 8等等），则可以用单个IP地址和掩码表示范围。例如，如果给出四个私用IP地址，分别为192.168.22.102、192.168.22.103、192.168.22.104和192.168.22.105，那么可以把这四个地址表示成192.168.22.102，掩码为255.255.255.252。否则，可以通过指出起始和终结IP地址按范围或一连串范围输入。

(3) 财务Windows服务器的RRAS设定只能路由TCP/TP，只须使用适合小型、单路径、静态IP网际网络的静态路由机制，无须使用如RIP、OSPF等的动态路由协议，不与网络中已存在的其他路由器交换路由信息，使财务子网（包括作为软件路由器的财务Windows服务器）对未被授权者而言成为MIS网络的一个"黑洞"。

这样，MIS网络中由财务部门指定的特许IP地址的机器如领导用机和相关数据库服务器能与财务子网正常连接，而MIS系统中其他机器均不能PING通作为路由器的财务Windows服务器的IP地址，更不能连接财务子网，其网络结构如图2所示。

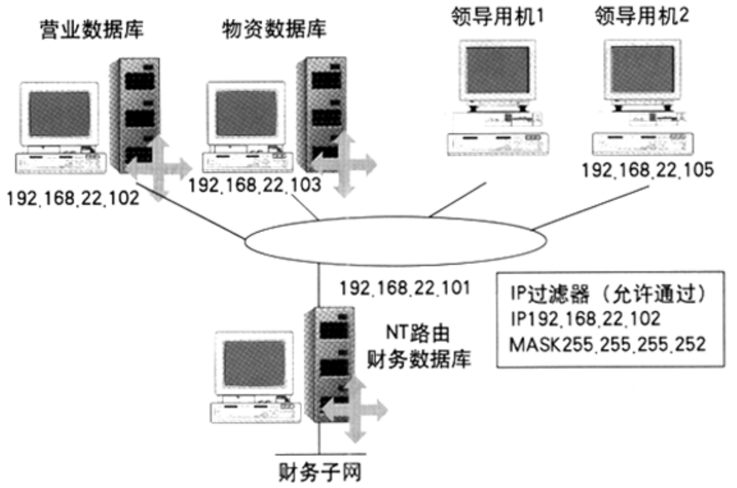


图 2

4.3 MIS子网与工控子网互联(基于IP地址和端口号进行包过滤)

对于MIS与配网自动化DA（Distribution Automation）系统、电力调度SCADA系统等工控子网的连接，安全方面必须比MIS子网与财务子网连接的要求更加严格。本应用的安全方面具体需求为：MIS网络中只允许上级主管领导用机以浏览器方式访问工控系统，工控系统向MIS网络中的应用服务器以定时或实时方式提供数据，只允许使用超文本传输协议HTTP(Hypertext Transfer Protocol)或简单邮件传输协议SMTP(Simple Mail Transfer Protocol)。

为实现本应用的工程目标，可以在MIS网络中或工控子网中选择一台Windows服务器，加设一块网卡，安装RRAS作为软件路由器，并使用RRAS基于IP地址和端口号进行包过滤来实现子网的安全互连。这要求除进行跟上例MIS子网与财务子网连接相类似的全部网络设置和路由配置外，特别的，还必须对作为软件路由器的Windows服务器RRAS的IP过滤器中分配给MIS网络被授权允许访问工控系统的IP地址的端口号作出必要的严格限制，其中：对用于领导查询用机的IP地址，只放开用于HTTP通信的TCP端口号80；对于MIS网络中的应用服务器的IP地址，只放开用于HTTP通信的TCP端口号80或用于SMTP通信的TCP端口号25。

这样，MIS系统中所有机器均不能PING通作为路由器的Windows服务器的IP地址，即使MIS网络中拥有特许IP地址的机器也只能以HTTP或SMTP与工控系统通信。

4.4 作为远程营业点或办公室的拨号路由（作为广域网路由）

远程营业点或办公室子网中的Windows服务器，可以装设调制解调器或ISDN适配器并安装RRAS成为按需拨号路由，以远程访问方式RAS(Remote Access Service)连接中心网络中相应的远程访问服务器，其网络结构如图3所示。

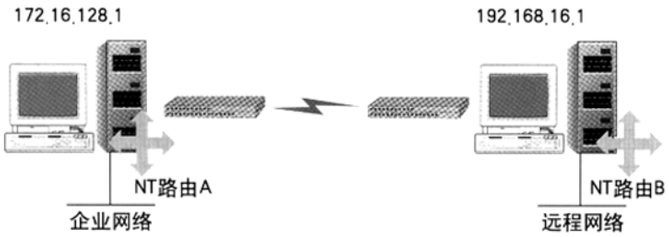


图 3

当然，如果广域网已经使用更佳的连接方式，也可以把这种方式建立的低成本广域网路由作为一种必要的通信备用方案。

5 路由设置的注意事项

投运前路由器的路由设置(包括传统的专用路由器)必须在试验环境下先行充分测试。

网络中的路由器之间会根据路由协议通过广播或多广播来互相交换路由信息。如果路由协议或路由表设置错误，错误的路由信息就会象病毒一样传播给在网络上的相关路由器（若路由的饱和时间太长,甚至会发生循环路由），由于存在广播时延，其后果可能在数小时后才会显示出来。同样，即使隔离和纠正上述错误，故障的消失也可能需要数小时，在这期间会出现子网通信中断、整个网络转发通信能力降低乃至瘫痪。

对于网络规模较大、子网较多、拓扑结构较为复杂的企事业单位，特别是电力系统企业，网络中如果已经设置多个路由器分别承担与广域网（连通省局和各县市局）、城域网（连通各营业网点）、调度和配电等工控系统的连接，错误地进行路由设置，将会对整个网络系统乃至企事业单位的日常生产和管理工作造成不可估量的影响。因此，即使已经通过试验环境下测试，在对实际运行环境的Windows服务器进行路由的安装、更改和调试时，最好有专业的系统工程师或网络工程师参与。

6 结束语

综上所述，只要根据业务需求对路由环境的可靠性和性能要求进行细致评估，在确定满足系统需求的前提下，对于大多数企事业单位的计算机系统，使用Windows软件路由器来替代传统的专用路由器进行网络分段并实现网间路由是一个最经济并易于管理的方案，而对于一些试验性、教学性、过渡性或急需投运的应用系统，RRAS更是一个首选方案。■

参考文献

1 *Craig Zacker，TCP/IP网络管理 [M]，王晓东、殷伯连、吴蓉、陈晓燕译，北京中国水利水电出版社，1998。*

2 *Sean K. Daily，优化Windows NT [M]，刘毅兵、吉全详、刘向军、宋江洪译，北京电子工业出版社，1999。*