基于以太网的工业控制远程访问的研究

侯 峥 张 伟 汪思源 赵永生 大连海事大学(116026)

Abstract

Network Address Translation (NAT) is a method of connecting multiple computers to the Internet (or any other IP network).It allows users to connect their industry control network to the Internet and access to other remote hosts.The implementation of using NAT technology to access to remote hosts that based on ethernet is discussed and an applied example is provided.

Keywords:NAT(Network Address Translator),remote access,indutry control

摘 要

NAT是一项专门用于网络互联的技术,可以用来解决工业控制网络的互联及远程访问的问题。探讨了利用NAT技术实现基于以太网的远程访问的实现,并给出了具体的实例。

关键词:网络地址转换,远程访问,工业控制

把工业以太网接入Internet，实现数据的共享和远程控制,可有效地提高企业的运作效率,但也引入了一系列网络安全问题。对此,一般可采用网络隔离(如网关隔离)将内部控制网络与外部网络分开。在设计内外网隔离的方案当中,NAT (Network Address Translator 网络地址转换）技术的应用是一种比较经济实用的办法。利用NAT技术不仅能够解决网络安全的问题,还能有效的避免申请过多的公用IP的问题。

1 NAT工作原理

工业以太网大多是基于TCP/IP协议。但是,IP地址空间紧张,公用IP地址还要逐年交纳费用,这就决定了不可能为现场的每个节点分配公用的IP地址,只有采用局域网的专用IP地址才能支持众多控制节点。但这些专用的IP是无法在Internet上路由的,也就是说它们无法直接访问Internet。传统的代理技术虽然可以解决控制节点接入Internet的问题，却严格禁止外部主机通过Internet对控制节点的访问。采用NAT技术既可以提供代理的功能，使内部的控制节点连接到外部,实现对互联网的访问,同时利用反向地址转换技术,还可以实现外部主机对任意的控制结点的访问,从而很好地解决了上面的问题。

NAT服务器实际上就是一台IP路由器。其作用就是将内部专用IP的数据包转换成为互联网可以直接访问的外部的公共IP地址。NAT的实质就是一个在数据包底层的Proxy代理，它为每一个TCP/IP数据包做代理,而不是单独为某一种互联网应用协议(例如Http,Ftp,Telnet)做代理工作。

NAT服务器可以对外部的网络隐藏内部的网络地址,这样可以有效地防止外界对应用网络的非法访问。当公司的网络安装了NAT服务器,NAT服务器上的公共IP地址是Internet用户唯一可以看到的IP地址。

NAT的实现包括两个方面,一方面企业内部局域网可以通过NAT访问Internet,另一方面外部网络也可以通过Internet访问局域网。企业内部局域网访问Internet时，局域网内部的计算机首先把要发送的数据包发给安装有NAT协议的Windows2000服务器,然后NAT会自动地把数据包中的内部IP地址。端口号和目的IP地址转换成自己的端口号和目的IP地址，并将转换后的数据包通过Internet发送给要访问的目的主机,同时将相关的信息记入地址映射表中,以便将返回的应答数据包准确无误地发送到客户端。相应的,外部网络通过Internet访问局域网时,首先外部网络的计算机发送数据包给装有NAT的服务器,然后NAT把数据包中的端口号和IP地址翻译成局域网内计算机的IP地址和端口号,并将数据包准确的发送给相应的内部计算机。

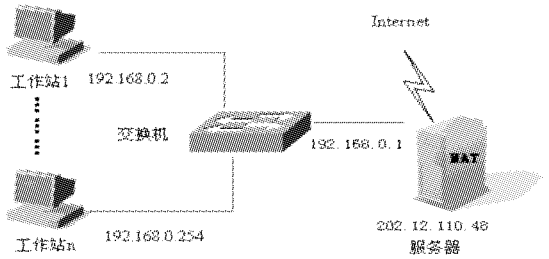

图1 NAT原理示意图

现以一实例来说明NAT的工作过程。如图1,设定有一IP为192.168.0.2的局域网用户使用Web浏览器欲连接到IP为210.77.145.66的一台公网Web服务器,则工作过程如下：

1)IP为192.168.0.2的局域网用户计算机创建带有下列信息的IP数据包,并将此IP包发送到NAT服务器：

目标IP地址:210.77.145.66

源 IP 地址:192.168.0.2
目标端口:80
源端口:1025

2)NAT 协议将此数据包地址转换成下面的形式,并在地址映射表中保留从 192.168.0.2:1025 到 202.127.129.188:5000 的映射:

目标 IP 地址:210.77.145.66
源 IP 地址:202.12.110.48
目标端口:80
源端口:5000

3)NAT 服务器将转发的 IP 数据包通过 Internet 发送到目的主机,如果目的主机的 IP 正确并能成功响应请求,则应答 IP 数据包通过 Internet 发回给 NAT 服务器。这时 NAT 服务器接收到的数据包包含下面的公用地址信息:

目标 IP 地址:202.12.110.48
源 IP 地址:210.77.145.66
目标端口:TCP 端口 5000
源端口:TCP 端口 80

4)NAT 协议检查地址映射表,将公用地址映射到专用地址,端口号也被重新映射回原先的端口号,并将数据包转发给位于 192.168.0.2 的计算机。转发的数据包包含以下地址信息:

目标 IP 地址:192.168.0.2
源 IP 地址:210.77.145.66
目标端口:TCP 端口 1025
源端口:TCP 端 80

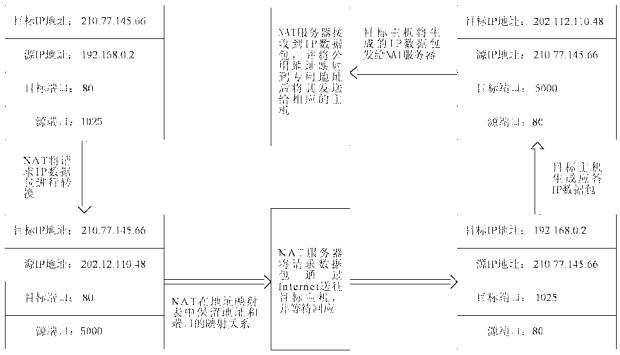

图 2 NAT 工作过程图

2 NAT 的实现

在 Windows2000 环境下实现 NAT 的功能并不复杂。涉及到 Windows2000 服务器的配置及其客户端的配置。如果要在局域网的内部部署 WWW 或 FTP 服务器,还要进行一些相关的工作。NAT 的具体实现步骤如下(仍以图 1 中的网络环境为例):

2.1 Windows2000 Server 服务器的配置

Windows2000 Server 服务器必须装有两块网卡。一块用于与内网相连接,另一块用于与 Internet 或其他企业内部网指定的接口地址相连。分别按照内外网的实际情况配置 TCP/IP 协议中的 IP 地址、网关及 DNS 等。然后安装和配置 NAT 协议。

在 Windows2000 Server 中,NAT 协议不是默认安装的,添加的步骤如下:

在【管理工具】中选择【路由和远程访问服务】,选择要启动 NAT 的服务器,单击鼠标右键,选择【配置并启用路由和远程访问】

选择【用于 Internet 连接服务器】,单击"下一步"

选择【网络地址转换 NAT】

NAT 协议的配置如下:

选择【网络地址转换 NAT】,单击右键,选择【属性】

在【常规】选项中,选择需要记录的事件日志

在【转换】选项中设置地址转换

在【地址分配】选项中,如果没有为局域网内的客户端分配固定的 IP 地址,就需要安装 DHCP 服务器。当然,也可以让 NAT 服务器兼做 DHCP 服务器,这时应当选择【使用 DHCP 自动分配地址】,并设置分配的地址范围。

2.2 客户端的配置

客户端的机器操作系统可以为 Windows95,98 或 2000,并且安装 TCP IP 协议,例如其网卡设定为:

IP:192.168.0.2.–192.168.0.255
子网掩码:255.255.255.0
网关:192.168.0.1
DNS:202.117.128.2(这里的 DNS 应当设置为校园网内的 DNS 服务器 IP,与用于做 NAT 转换的服务器所使用的 DNS 是相同的)

需要注意网络内部的主机可以使用 DHCP 服务器动态分配 IP 地址,但如果需要外部网络访问局域网内的计算机(例如提供对外服务的内部的 WWW 或 FTP 服务器)就必须将客户端 IP 地址设置为静态的。

通过以上的步骤,就可以在任意一台客户端访问局域网以外的主机了。如果需要的话还要部署可以接受外部访问的内部服务器。

2.3 配置内部主机作为 WWW 或 FTP 服务器

使用 NAT 的专用网络实际上对外的网络 IP 只有 NAT 服务器的 IP,其他内部主机的 IP 都被隐藏了。但我们可以配置静态端口来代表专用网络中的主机。例如可以配置一个特殊端口 80 将入站连接指引到一台 Web 服务器。这样,在公有网络上访问这个 IP 的 80 端口时,NAT 会根据这个特殊端口号找到相应的服务器,完成请求的功能。由此,局域网以外的计算机就可以直接访问内部的服务器。

3 应用实例

NAT 技术已经成功地被应用在了某高校锅炉房控制系统项目中。该项目的网络远程访问部分中我们要考虑的问题主要有以下三个方面:

1)锅炉系统在校园网内的安全性。这是由于锅炉房本身属于校园网的一部分,同时我们又要使其与其他网络系统相对独立;

(下转第 51 页)

```
Dim intBcc As Integer
intBcc = 0
For a = 2 To intC + DleCount
    intBcc = intBcc + CInt(byteSend(a))
    If byteSend(a) = DLE Then a = a + 1
Next
intBcc = intBcc Mod 256
If intBcc <> 0 Then byteBcc = &H100 - CByte (intBcc)
Else byteBcc = 0
byteSend(0) = byteSendTemp(0): byteSend(1) = byte-
SendTemp(1)
byteSend(intC + DleCount + 1)=byteSendTemp(intC + 1)
byteSend(intC + DleCount + 2)=byteSendTemp(intC + 2)
byteSend(intC + DleCount + 3) = byteBcc
comCom1.Output = byteSend
```

5 有关问题的说明

编制 PLC 与上位机的通信程序最关键一点是深刻理解 PLC 的数据包格式及通信过程,对串口数据的读写操作则相对较易。

在通信数据包校验连续失败的情况下,一般发送方只发送约定好的次数后就发送下一个有效包,作者的程序中未对失败的次数和请求响应的次数进行统计。对 PLC 的读命令的响应,作者未编制相应的程序,因为实际情况下 PLC 读上位机的数据极为少见。对上位机的读/写命令的程序清单,作者只是以一例代之,具体内容需根据工程中的数据在 PLC 内的实际地址来编制。串行口的初始化设置作者只作了初步的定义,并未提供串口的多种通信协议选择界面。个别变量的命名规则未遵循 VB 的代码约定规则,使用者可在实际使用中更改变量的命名,以利于阅读或测试。

目前情况下,人机界面程序由一个主窗体和一个名为 comCom1 的通信控件组成,主窗体未包含其它任何控件和代码,用户可将所有源代码拷贝至自己的工程下,将串口通信控件命名为 comCom1 即可。

限于文章篇幅,作者不能提供通信程序的全部代码,读者若在实际工程中需要请向作者索取,该程序目前在实际的工程应用中使用,暂未出现任何错误,使用者若在应用中发现错误请及时将意见提交 infor707@yahoo.com.cn,十分感谢。

参考文献

1 SLC500 系列 PLC 通信协议.美国 AB 公司编著

[收稿日期:2003.6.7]

(上接第 27 页)

2)实现远程访问,即在内部部署 WWW 或 FTP 服务器。这一方面有利于实现管控一体化的目标,使得管理人员可以通过网络及时准确的了解现场设备工作的情况;同时又可以使得我们工程技术人员即使不再现场也能够更迅速更快捷地解决控制现场所出现的问题,从而进一步提高我们的服务质量;

3)实施的费用不能太高。

NAT 技术恰好满足上述要求。由其工作原理可知,NAT 技术可以做到通过网关主机将内外网隔离,实现内网的安全性。这里的外网实际上包含两个层面。其一就是我们常说的 Internet,另外,这里的外网也可以是一个的局域网。也就是说,NAT 实际上是用于两个网络连接的,而并不一定要求这两个网路是专用网络还是公用网络。这一点对于该应用非常重要。因为锅炉房局域网是属于该校校园网的一部分,而且 WWW 或 FTP 服务器也主要是供 Intranet 用户使用。

4 NAT 与相关技术的比较

NAT 技术为内外网的隔离,实现工业控制网络的远程访问提供了一个经济实用的解决方案,但能够实现该功能的技术还有很多。下面将 NAT 与几种常见的相关技术进行简单的比较。

4.1 与 ICS 技术的比较

ICS 技术,实际上是 Microsoft 公司为解决小型网路共享上 Internet 地问题而提出的。作为提供共享服务的计算机必须要有静态的 IP 地址,并且只能使用一个公用 IP 地址。NAT 则适合于较大的网络,客户机也无需设定静态 IP 地址。ICS 无法在专用网络上部署 WWW、FTP、Email 服务器,而 NAT 可以。

4.2 与专用路由的比较

专用的路由设备(目前,某些较高档的交换机已经具有路有的功能,这里也包括这一类的设备)价格不菲,比较适用于大型网络。而 NAT 是 Windows2000 Server 自带的协议,不需另购设备,但比较而言工作效率没有硬件的路由器或高档交换机高。

4.3 与常见的代理服务器端软件的比较

常见的提供多用户共享访问 Internet 的代理服务器端软件有 WinGate、SyGate、WinProxy 等。它们与 NAT 实现的功能相当。但是这些软件是在应用层实现的网关,它们在 HTTP 或 FTP 等应用层协议以上实现数据包的转发,而 NAT 在网络层实现数据包转发,具有类似路由器的功能。而且 NAT 具有某些代理服务器所不具备的功能,如 NAT 可以作为简单的路由器及防火墙使用,允许用户在局域网内部布署各种服务器等。

另外,通常使用代理服务器时客户端要安装客户端的软件,而 NAT 没有这个要求,操作非常简单。

参考文献

1 李鹏飞.利用 NAT 实现局域网和 Internet 的互联.西安邮电学院学报,2002(7)

[收稿日期:2003.7.2]