基于端口映射的网络资源互联设计与实现

罗祖川

（民航宁夏空管分局，宁夏 银川 750004）

摘 要 端口映射是 NAT 技术的一种，功能是把在公网的地址转翻译成私有地址。要实现两个独立的内网网络部分资源的互访，本文论述了可行的三种方案，并分析了三个方案在实际应用中的优缺点。综合考虑方案成本和实施难度后，通过在两个网络中间增加一普通无线路由器后实现了两个网络的互连，使用端口映射和 DMZ 主机的方式实现两个网络部分资源互访。通过 Netstat 命令查找不常见应用的通信端口，成功实现视频资源通过端口映射到其他网络。

关键词 虚拟服务器 端口映射 DMZ 主机 网络互联

中图分类号：TP393 **文献标识码**：A **文章编号**：1007-0745(2021)06-0013-02

1 网络情况

单位的内网是 10.25.1.X/24 网段（以下简称网络一），通过网关 10.25.1.254 访问上级单位的网络，上级单位在防火墙上做了策略，只有 10.25.1.X 的 IP 能够访问其网络。另一网络是一个内部视频监控网络，IP 段是 192.0.0.X/24（以下简称网络二），可以通过浏览器访问这些视频监控资源。这两个网络通过一台 Cisco 二层交换机连接起来，未做任何管理限制策略。在网络二中有一台控制电脑，这台电脑设置有网络一和网络二的双 IP，既可以实现通过网络二的 IP 对视频监控系统控制，又可以通过网络一的 IP 访问内网，网络一的任一电脑还可以访问这台控制电脑的共享文件夹。现在要增加一个功能，实现在网络一中任一电脑访问网络二的两个视频监控资源，同时还要满足之前的功能。

2 方案规划

因为之前是在控制电脑上通过设置网络一和网络二的双 IP 实现的同时访问两个网络的资源，除了这台控制电脑，两个网络的其他终端之间并不能直接通信，网络二中的视频监控终端也不支持双 IP，设计了多个方案来实现这些功能。方案一将网络二的 IP 段全部改为网络一的 IP 段，两个资源完全处于同一网络中，这个方案一方面网络改动多，网络二中的所有主机都需要更改 IP，视频配置也需要做相应更改，另一方面也不利于网络安全管理。方案二是增加一个三层设备，添加网络一和网络二之间的路由，网络二的终端添加网关，这两个网络通过三层路由实现互联，但是三层设备比较贵，也没有现成的三层设备，而且网络二中所有的终端都需要添加网关，改动比较多。方案三是在这两个网络中间增加路由器，网络二通过 NAT 转换访问网络一，并将网络二的控制电脑和两个视频资源通过端口映射出去，网络一中任一电脑都能访问这三个资源，正好单位有很多 TP-LINK 的无线路由器即可实现上述功能，而且这个方案改动不多，所以采用方案三来实现。

3 端口映射的定义

通过 TP-LINK 无线路由器的虚拟服务器功能可以将内部资源对外开放到指定端口，在保证内部资源安全的前提下实现外部网络对指定端口的内部资源的访问，其实质就是端口映射。

端口映射是 NAT 地址转换的一种，NAT 技术可以把公网的 IP 地址转翻译成私有 IP 地址，采用路由方式的 ADSL 宽带路由器拥有一个动态或固定的公网 IP[1]。实现 NAT 有三种方式，静态转换、动态转换和端口多路复用。端口多路复用是指改变外出数据包的源端口并进行端口转换，即端口地址转换（PAT，Port Address Translation)。目前网络中应用最多的就是端口多路复用方式[2]。

4 网络互联设计和实现

因为不需要无线网络功能，且需要连接内部网络，无线网络存在一定网络安全隐患，所以关闭无线路由器的无线功能，将无线路由器的 WAN 口接入网络一的交换机中，将 LAN 口接入网络二的交换机中，连接如图 1 所示。

对无线路由器和网络二的资源进行配置。将无线路由器的 LAN 口 IP 设置为网络二的 IP 192.0.0.1，此 IP 也是网络二中终端的网关 IP。WAN 口 IP 设置为网络一的 IP 10.25.1.28/24，网关是 10.25.1.254。网络二中的控制电脑的 IP 设置为 192.0.0.207/24，网关为无线路由器的 LAN 口 IP 192.0.0.1。这样可以实现控制电脑对网络二的控制和通过网关 IP 192.0.0.1 以 NAT 的方式访问网络一资源，也能访问上级单位的网络资源（源 IP 地址已经全部转换成合法的 IP 地址 10.25.1.28）。通过查询要实现 Windows 系统文件夹共享需要 4 个端口，UDP 的 137，138，TCP 的 139，445。在路由器的虚拟服务器设置页面添加一条规则，外部端口是 137，内部端口是 137，IP 地址是网络二的控制电脑 IP 192.0.0.207，协议是 UDP。138，139 和 445 的端口映射设置与 137 差不多。它们在路由器上的端口映射如表 2。修改两个视频监控的网络信息，增加网关 IP 192.0.0.1. 网络二的其中一个视频资源在配置的时候配置了其端口是 8000，所以其端口映射设置如表 1，而另一个视频监控不知道其端口，所以使用了 DMZ 功能，DMZ 主机 IP 地址设置为视频监控的 IP 地址 192.0.0.200，这样外部网络访问没有在虚拟服务

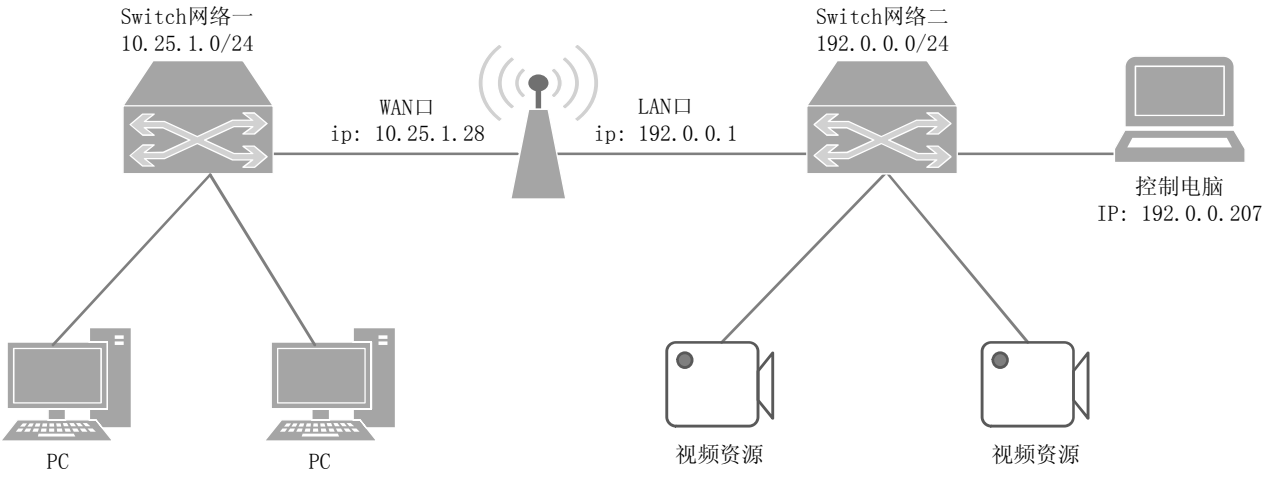

图 1 智能电网结构流程

表 1 端口映射设置

应用服务器				
常用服务器	外部端口	内部端口	IP 地址	协议类型
	554	554	192.0.0.150	ALL
	8000	8000	192.0.0.151	TCP
HTTP	80	80	192.0.0.150	TCP
HTTP	81	80	192.0.0.151	TCP
	445	445	192.0.0.207	ALL
	139	139	192.0.0.207	ALL
	138	138	192.0.0.207	ALL
	137	137	192.0.0.207	ALL
	136	136	192.0.0.207	ALL

器中设置的其他 10.25.1.28 的资源时，无线路由器会全部转发给 DMZ 主机 192.0.0.200，因为是通过浏览器以 HTTP 协议访问的视频监控资源，所以要将两个视频监控资源的 80 端口映射出去。

最后可以实现在网络二的控制电脑对网络二的视频监控的控制，也能访问网络一的资源。网络一的任一电脑能够通过访问无线路由器的 WAN 口 IP 加端口的方式访问网络二控制电脑的共享文件夹和两个视频监控资源。

但是后来在使用过程中发现两个视频监控一段时间后就出现无法访问的情况，通过重启无线路由器可以解决，但是过段时间又不能访问，有时重启无线路由器也无法访问。最后发现不能超过一台电脑同时通过 DMZ 方式访问网络二的视频监控资源。所以必须使用端口映射的方式，但是现在不知道视频监控所使用的端口。可以使用 Windows 系统的 Netstat 命令查看全部网络连接来找出视频监控使用的端口。在网络二中的控制电脑上通过浏览器访问视频监控，访问成功后，在 Cmd 中输入命令 netstat-a-n，可以列出此时这台电脑的所有网络连接，找到和视频监控的连接信息。其中有一条 TCP 192.0.0.207:65515 192.0.0.150:554 ESTABLISHED，其中 554 就是视频监控使用的端口。在无线路由器虚拟服务器中添加 554 的端口映射后解决了这个问题。

5 结语

两个网络的互连可以有很多种方法，但是针对本文实际情况，使用无线路由器来实现网络互联，通过虚拟服务器的方式实现业务的互访，成本极低，改动不大，施工难度也很低，基本不会影响两网络原来的业务，经济效率得解决这个网络互联问题。

参考文献：

[1] 李娟芳，陈瑞志 . 计算机网络技术与应用 [J]. 中国铁道出版社，2013(09):142.
[2] 郑洪霞 . 基于 NAT 的 IP 寻址方式在信息安全中的应用研究 [J]. 移动信息，2016(06):151.