实验 6：NAT 的配置实验报告

李伟

1711350 计算机科学与技术一班

更新：*November 27, 2019*

摘　　要

网络地址转换是 TCP 和 UDP 的典型应用之一，网络地址转换的目的就是利用较少和有限的 IP 地址资源将私有的互联网接入公共互联网，目前较多的路由器、无线 AP 等硬件设备都支持 NAT 功能，本实验将在真实环境和仿真环境下实现网络地址的转换功能。

关键词： NAT 配置，Web 服务器，仿真环境NAT配置，CISCO Packet Tracer

1　实验要求

本实验分为两个部分，分别要求在 4 台Windows Server 2003虚拟机上进行 NAT 的配置以及在Cisco Packet Tracer仿真环境下进行 NAT 的配置，配置实现的网络结构能够满足以下的检查条件：

- 在 Windows Server 2003 虚拟机上进行 NAT 的配置。共需配置三台机器，其中一台为主机、一台为 NAT 设备、一台为 WEB 服务器。
- 在 Cisco Packet Tracer 仿真环境下进行 NAT 的配置。
- 要求 WEB 服务器在内网，主机在外网，主机可以访问 WEB 服务器主页。

2　实验环境

2.1　虚拟机环境 NAT 配置

- 虚拟机系统环境 windows 2003 server
- 虚拟机运行环境 windows 7
- 虚拟机配置 1G 内存单核 CPU

2.2　仿真环境 NAT 配置

- 操作系统环境 windows 10
- 仿真环境 Cisco Packet Tracer 7.1

3 实验具体步骤

本次实验的实现分为两个大的部分，需要分别的三台windows 2003 server上以及Cisco Packet Tracer上实现 NAT 配置，同时对每一种环境均需要实现从外网访问内网中 web 服务器的功能（需要进行 NAT 穿透）。具体的实现步骤如下所述：

3.1 虚拟机 NAT 配置

3.1.1 IP 地址配置

首先，考虑虚拟机的 NAT 配置实现，通过windows 2003 server提供的路由和远程访问程序，可以便捷的设置每一台主机相应网卡的 IP 地址配置，在本次实验中三台虚拟机（一台作为 NAT 服务器，两台作为终端机器，分别为访问主机和 web 服务器）的 IP 地址配置如图 1所示：

图 1: 虚拟机互联网拓扑图结构

设置虚拟机的 IP 地址的步骤为：选择“路由与远程访问”的本地接口，选择“常规”，在界面中可以看到两个本地连接，分别对应虚拟机的两个网卡，在本次实验中，两台终端机器只需要使用一张网卡一个 IP 即可，NAT 服务器需要为两张网卡分别配置一个 IP，一个作为内网的网关，一个作为外网的网关。需要注意的是，作为终端机使用的主机 A 和主机 B 需要在设置 IP 地址的同时，设置好对应的默认路由（即为 NAT 服务器对应的网关 IP）。主机 A 与主机 B 的 IP 地址配置如图 2所示，NAT 服务器的两张网卡的 IP 设置如图 3所示。

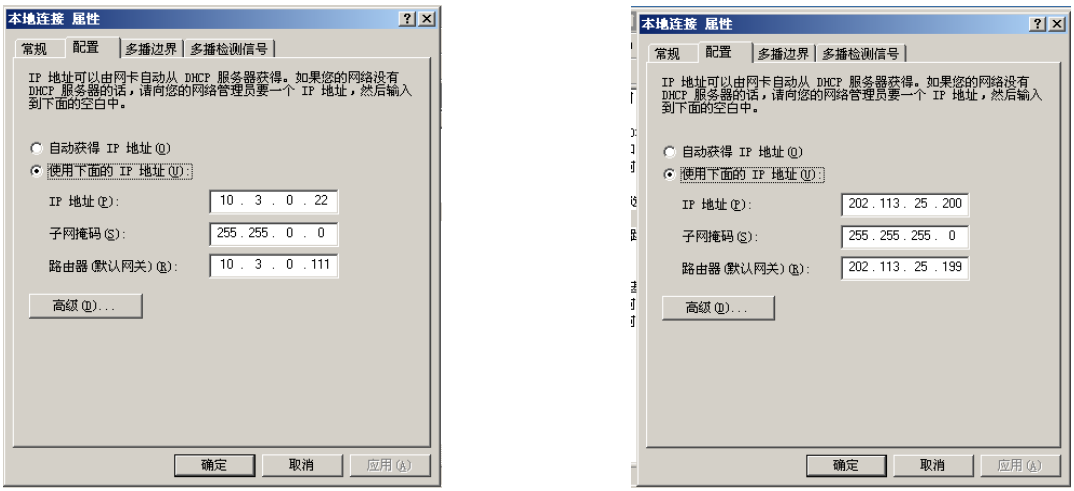

图 2: 主机 A 与主机 B 的 IP 地址及默认网关设置

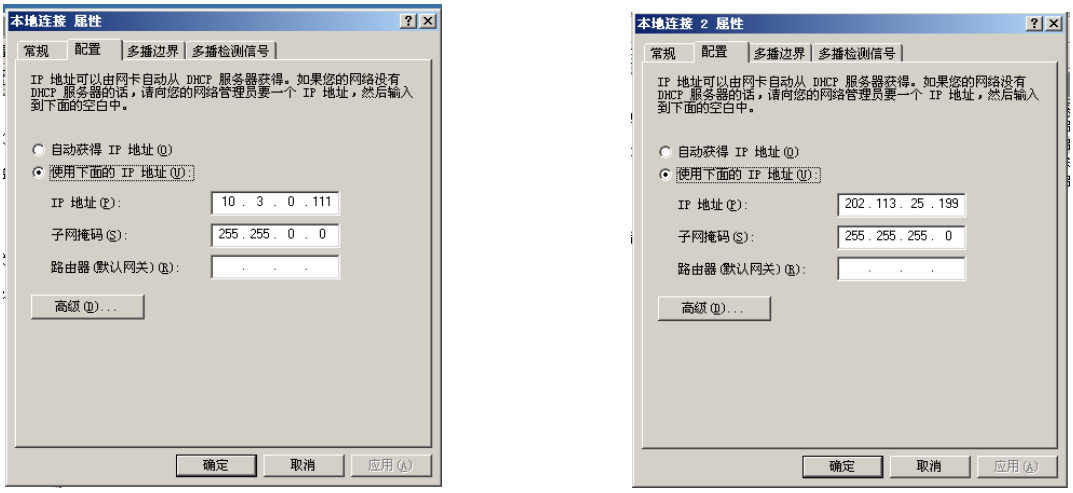

图 3: NAT 网卡的 IP 地址配置

3.1.2 NAT 转换配置

配置好虚拟主机的 IP 地址之后，开始配置 NAT 服务器的 NAT 接口，通过“路由与远程访问”程序实现，在这里以后一种方式说明，“程序与远程访问”界面如**图 4**所示：

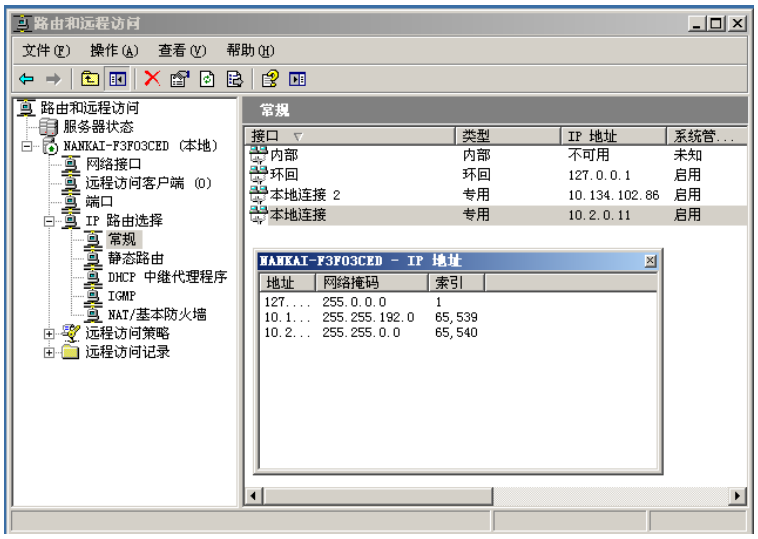

图 4: 程序与远程访问界面截图演示

从截图**图 4**可以看到 NAT/基本防火墙的选项，打开后在空白界面右键选择“新建接口”即可选择为相应的网卡连接添加 NAT 接口，新建接口的窗口界面如**图 5**所示，在建立内网的 NAT 接口时选择专有网络接口，在建立外网 NAT 转换时选择“公用网络到 Internet”以及“在此接口启用 NAT”。

为**图 1**中的 NAT 服务器的两张网卡分别添加 NAT 后的“程序与远程访问”界面**图 6**所示：

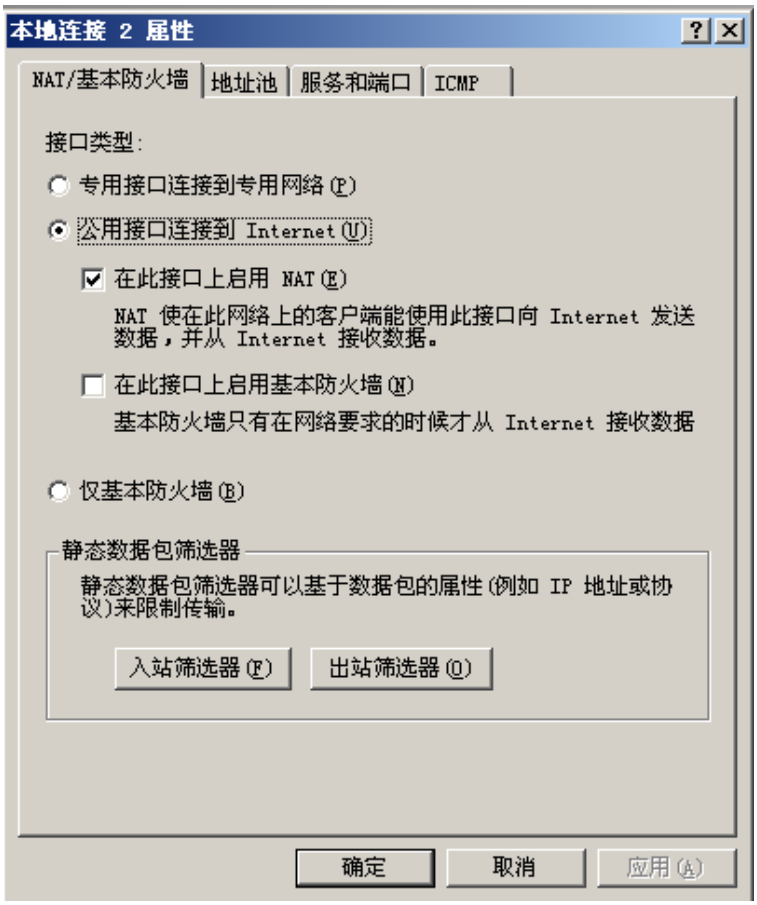

图 5: 建立 NAT 接口配置选项

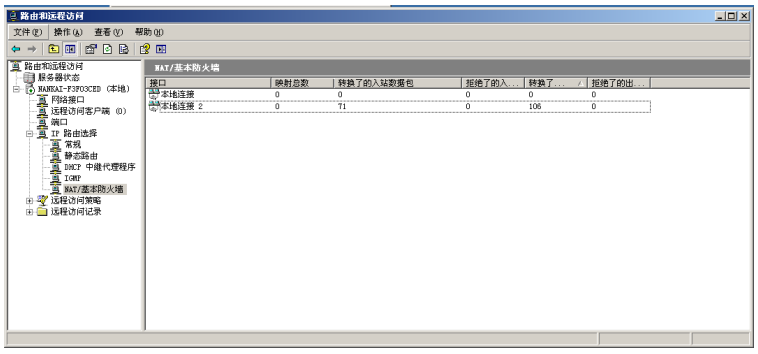

图 6: NAT 配置界面

3.1.3 NAT 穿透

由于本次实验要求从外网能够访问内网的 web 服务器，因此需要将内网中的主机 A 作为 web 服务器供外网进行访问，正常情况下外网是无法获取内网 IP 进行访问的，但是可以通过穿透 NAT 的方式将内网的 IP 和对外的公网 IP 地址做一个映射关系实现外网终端对内网 web 服务器的访问，实现方式为在对外公网 NAT 接口上添加 Web 服务接口，将内网的 web 服务器 IP 和公网 IP 进行端口映射，实现静态 NAT 的效果，如图 7、图 8所示，选择 web 服务器，并将专有地址设置为内网 web 服务器终端的 IP 地址如图 8所示。

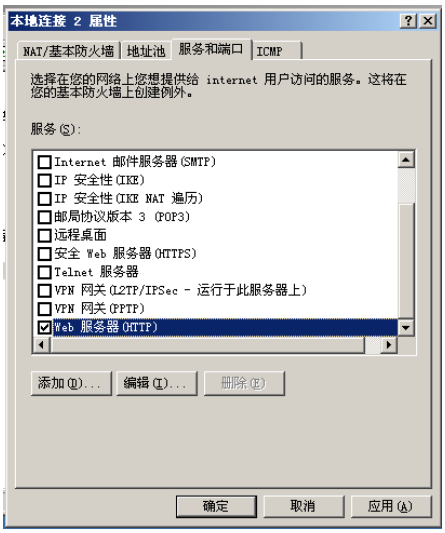

图 7: 服务与端口界面

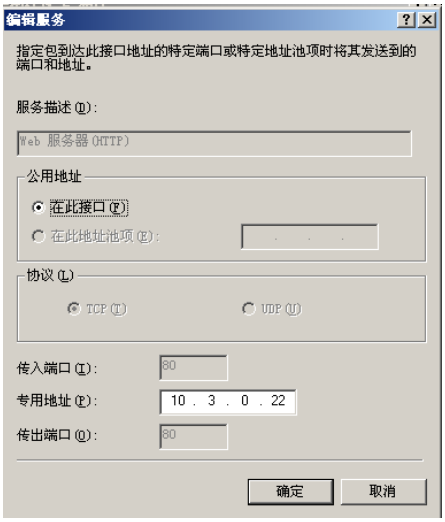

图 8: web 服务器服务设置

3.1.4 连通性测试

在配置好 NAT 服务器和 web 服务终端之后，需要进行连通性测试，在本实验中，内网的终端能够访问外网的机器，同时外网的机器也能够访问内网的特定 web 服务器终端，在下面主要展示主机 A、B 之间的连通性测试，连通性测试结果如图 9所示，web 服务器访问测试结果如图 10、图 11所示：

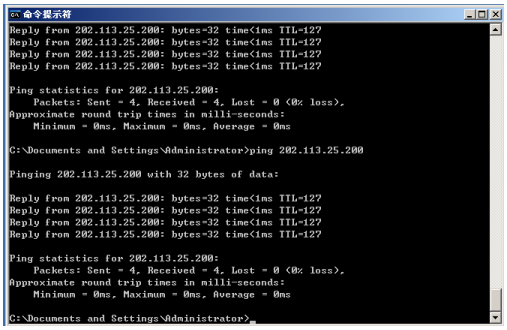

图 9: 主机 Aping 主机 B 的结果截图

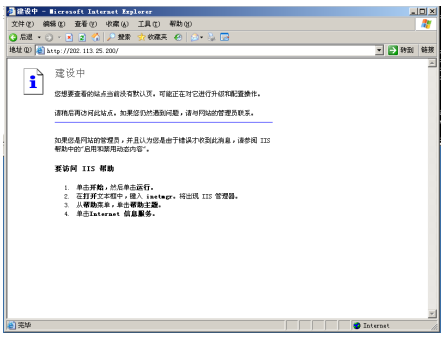

图 **10:** 主机 A 访问外网 web 服务器

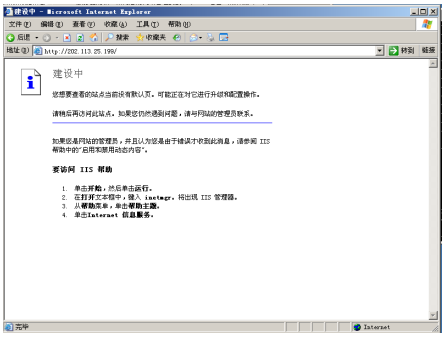

图 **11:** 主机 B 访问内网 web 服务器

3.2 仿真环境 NAT 配置

3.2.1 IP 地址和设备配置

与虚拟机环境类似，仿真环境下的配置步骤基本没有区别，都是先进行 IP 地址的配置，然后配置 NAT 议，图 **12**显示的是网络拓扑图以及相关接口的 IP 地址配置。

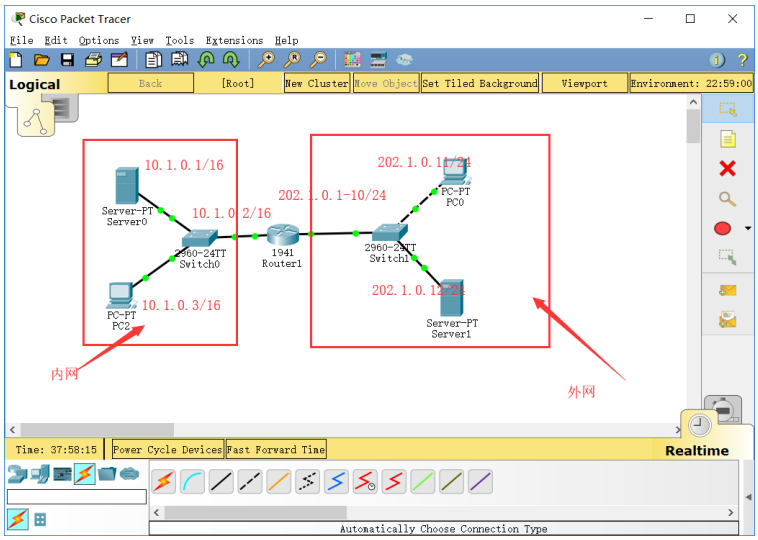

图 **12:** 仿真环境互联网拓扑图结构

按照网络拓扑图中的 IP 地址配置好了主机的 IP 地址之后，进一步可以配置 NAT，在仿真环境下的路由配置主要通过路由器的 CLI 中的命令进行 NAT 的配置。配置 NAT 的命令主要是 IP nat pool 、access-list 、ip nat inside list LabelID pool PoolName overload, 由于需要从外网访问内网 web 服务器，所以需要配置静态的 NAT，配置过程如下所示：

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static tcp 10.1.0.1 80 202.1.0.1 80
Router(config)#exit
Router#
```

```
%SYS-5-CONFIG_I: Configured from console by console

Router#exit
```

最终生成的 NAT 映射表如下所示，其中第二条为静态 NAT 映射。

```
Router>show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 202.1.0.1:1097     10.1.0.3:1097      202.1.0.12:80      202.1.0.12:80
tcp 202.1.0.1:80       10.1.0.1:80        ---                ---
tcp 202.1.0.1:80       10.1.0.1:80        202.1.0.11:1170    202.1.0.11:1170
```

3.2.2 测试结果截图

测试 web 服务器的访问截图如**图 13**、**图 14**所示，由于修改过 web 服务器的默认页面，所以可以通过查看页面内容判断访问的 web 服务器是哪一个。

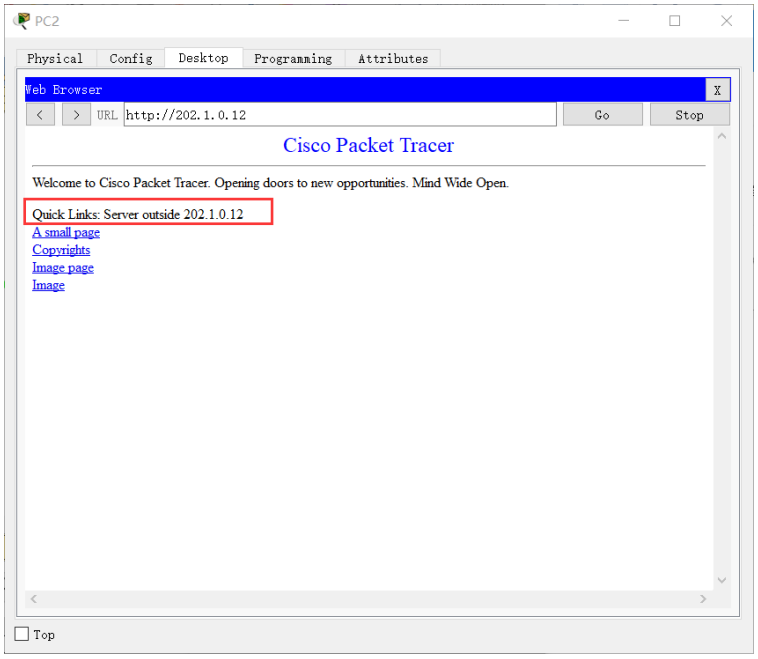

图 13: 内网访问外网 web 服务器

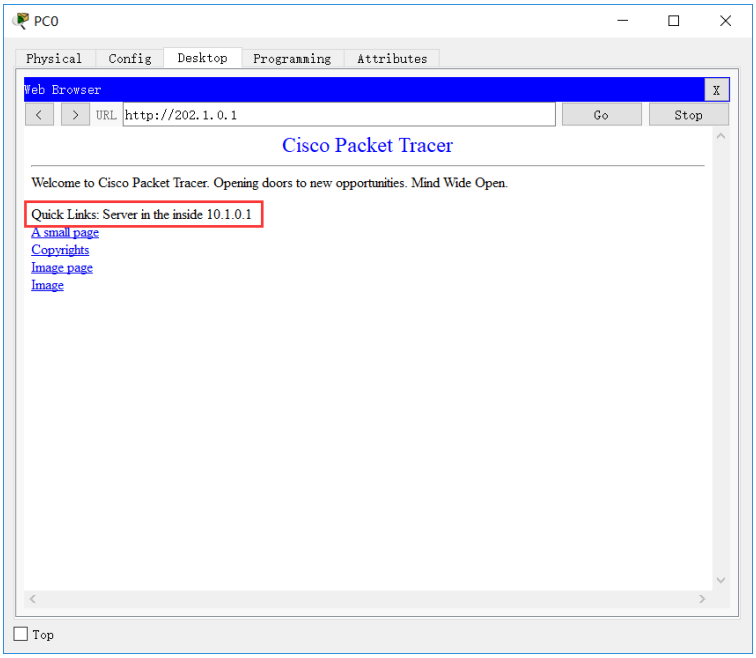

图 14: 外网访问内网 web 服务器

4 总结与思考

通过这次在三台虚拟机上进行 NAT 的配置以及在仿真环境下配置 NAT 并实现了从外网访问内网 web 服务器，进一步了解到了关于 NAT 的相关知识，深入理解了网络地址转换工作的基本原理和配置 NAT 的相关工作，能够理解网络地址映射形成的过程和网络地址转换在网络通信中的巨大作用。在这次实验的过程中发现，网络地址转换在很大程度上确实降低了对 IP 地址的数量上的要求，但是仍然让类似于服务器通信之类的网络服务变得不太方便，但是在另一方面 NAT 的存在对网络安全有一定的作用，起到的基本的网络防火墙功能。