中国科学技术大学计算机学院

《信息安全导论》实验报告

实验题目：用 Windows2003 实现网关-网关 VPN

学生姓名：郭耸霄

学生学号：PB20111712

完成日期：2022 年 5 月 3 日

计算机实验教学中心制

2020 年 09 月

实 验 报 告

11 系 20 级 3 班　　郭耸霄 PB20111712　　2022 年 5 月 3 日

1 实验题目

用 Windows2003 实现网关-网关 VPN。

2 实验目的

用 IPsec 隧道方式配置网关-网关 VPN，连接被 Internet 隔开的两个局域网 (VMnet1 和 VMnet3)，使之进行安全通信，实现信息的保密和完整。

3 实验设计

从链接:https://rec.ustc.edu.cn/share/5898f130-b7ac-11eb-9d5f-1f1cf7c9a9eb 下载 raServerA.ova，导入到虚拟机。然后复制 5 台 Windows2003SP2 虚拟机，分别用作 ServerA、ServerB、Router、ClientA 和 ClientB。用 VirtualBox Host-Only Ethernet Adapter 模拟两个局域网和一个广域网（用路由器模拟）。每个局域网含若干台客户机和一台 Windows server 2003 组成。具体设计和规划如下图:

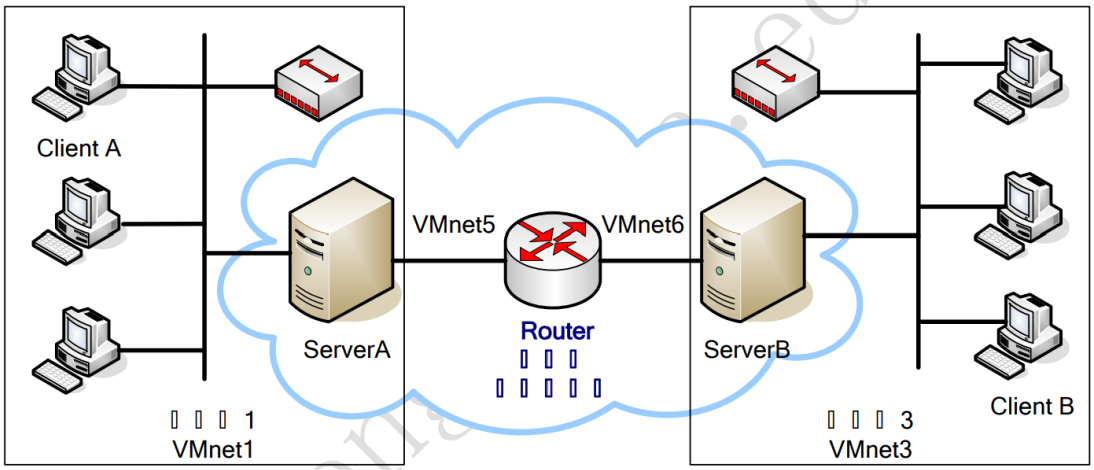

图 1: 实验具体设计

虚拟网卡 VMnet1 和 VMnet3 分别模拟两个局域网，VMnet5、VMnet6 和 Router 模拟因特网。ServerA 和 ServerB 模拟互联网上的边界路由器 (远程服务器)，建立 IPSec 隧道以连接两个局域网，用于保证通信安全。

4 实验步骤

4.1 创建 ServerA 的 IPSec 策略

1、管理工具中打开 “本地安全策略” –右击 “IP 安全策略, 在本地计算机” — “创建 IP 安全策略” –命名为 “AB” –取消选择 “激活默认响应规则” –. 编辑 “AB” 属性, 添加新规则（不使用添加向导)。

2、添加 “IP 筛选器列表”，命名为 “A to B” –添加属性（不使用添加向导），设置源地址为 “特定 IP 子网:192.168.86.0”，目的地址设置为 “特定 IP 子网:10.0.0.0” –取消选择 “镜像” –协议设定为默认值: “任意”。

3、筛选器操作 (不使用添加向导): 安全措施为“协商安全”, 新增安全措施为“完整性和加密”。

4、身份验证方法, 使用预共享密钥: microsoft。

5、隧道设置, 指定隧道终点 IP 地址（Server B 的外网 IP 地址：166.66.66.213)。

6、连接类型为“所有连接”。

7、重复 2-6, 创建 IP 筛选器列表“B to A”设置从 ServerB 到 ServerA 的 IP 策略。将“源子网 (IP)”和“目的子网 (IP)”互换，隧道终点。

8、在本地安全设置中, 右击策略“AB”—指派。

4.2 创建 ServerB 的 IPSec 策略

1、管理工具中打开“本地安全策略”–右击“IP 安全策略, 在本地计算机”—“创建 IP 安全策略”–命名为“BA”–取消选择“激活默认响应规则”–. 编辑“BA”属性, 添加新规则（不使用添加向导)。

2、添加“IP 筛选器列表”, 命名为“A to B”–添加属性（不使用添加向导）, 设置源地址为“特定 IP 子网:192.168.86.0”, 目的地址设置为“特定 IP 子网:10.0.0.0”–取消选择“镜像”–协议设定为默认值:“任意”。

3、筛选器操作 (不使用添加向导): 安全措施为“协商安全”, 新增安全措施为“完整性和加密”。

4、身份验证方法, 使用预共享密钥: microsoft。

5、隧道设置, 指定隧道终点 IP 地址（Server B 的外网 IP 地址：166.66.66.213)。

6、连接类型为“所有连接”。

7、重复 2-6, 创建 IP 筛选器列表“B to A”设置从 ServerB 到 ServerA 的 IP 策略。将“源子网 (IP)”和“目的子网 (IP)”互换，隧道终点。

8、在本地安全设置中, 右击策略“BA”—指派。

4.3 配置远程访问/VPN 服务器

配置 Server A、Router 和 Server B 为路由器。在“开始”—“所有程序”—“管理工具”菜单中选择“路由和远程访问”，打开“路由和远程访问”管理界面，选择“配置并启用路由和远程访问”，配置为“两个专用网络之间的安全连接”，不选择拨号 VPN，配置完成后，ServerA 可以和 ServerB 互联互通。

4.4 ping 测试（Client A）

在 Client A 的 cmd 中输入 >ping 10.0.0.202，或者在 Client B 的 cmd 中输入 >ping 192.168.86.202。如果两方的 IPsec 策略未配置正确，不会 ping 通。如果正确则说明两个局域网互联互通。在数据通道中的路由器用 wireshark 检测到的是 ESP 数据包，因此实现了数据的完全保密，通信内容无法被窃听。

4.5 做实验并写实验报告

将路由器、Client A 及 ClientB 的 IPv4 地址的第 4 个点分十进制数（如 192.168.86.202 的第 4 个点分十进制数为 202）改成你学号的最后 3 位数字%200（进行“模 200”运算），其他部分的 IP 地址也可能需要修改以避免 IP 地址重复。

这是实验过程截图:

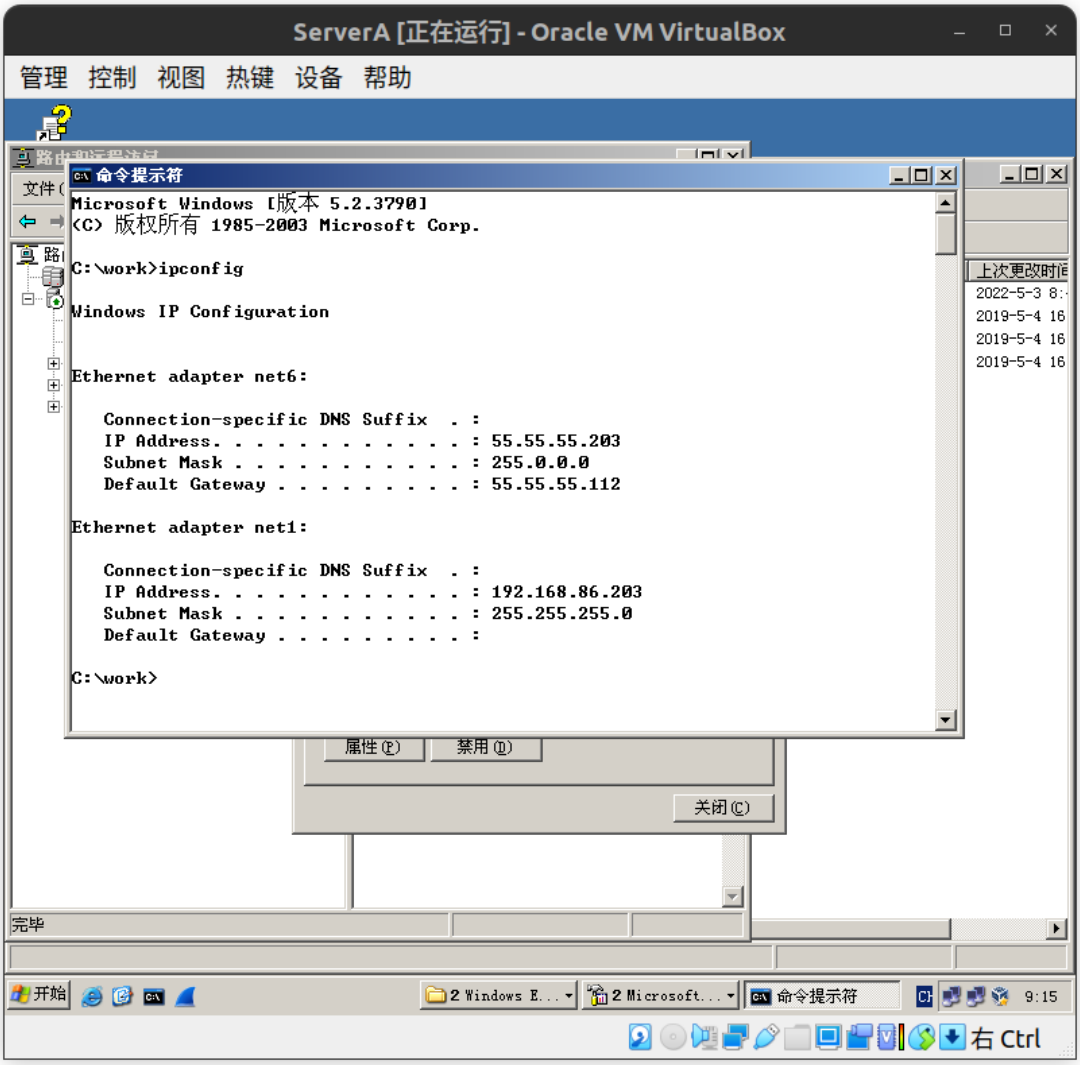

图 2: Client A:ipconfig&&ping

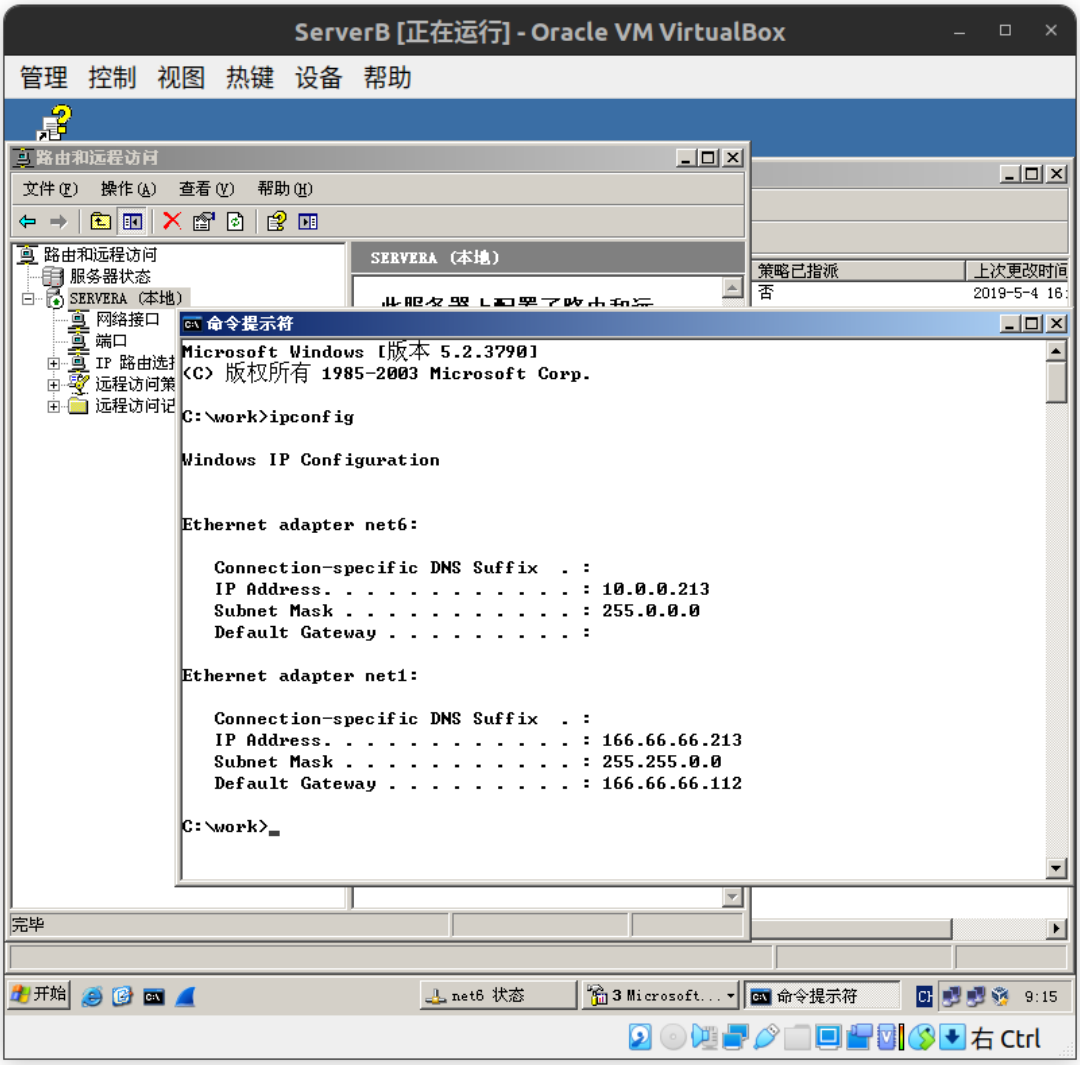

图 3: Client B:ipconfig&&ping

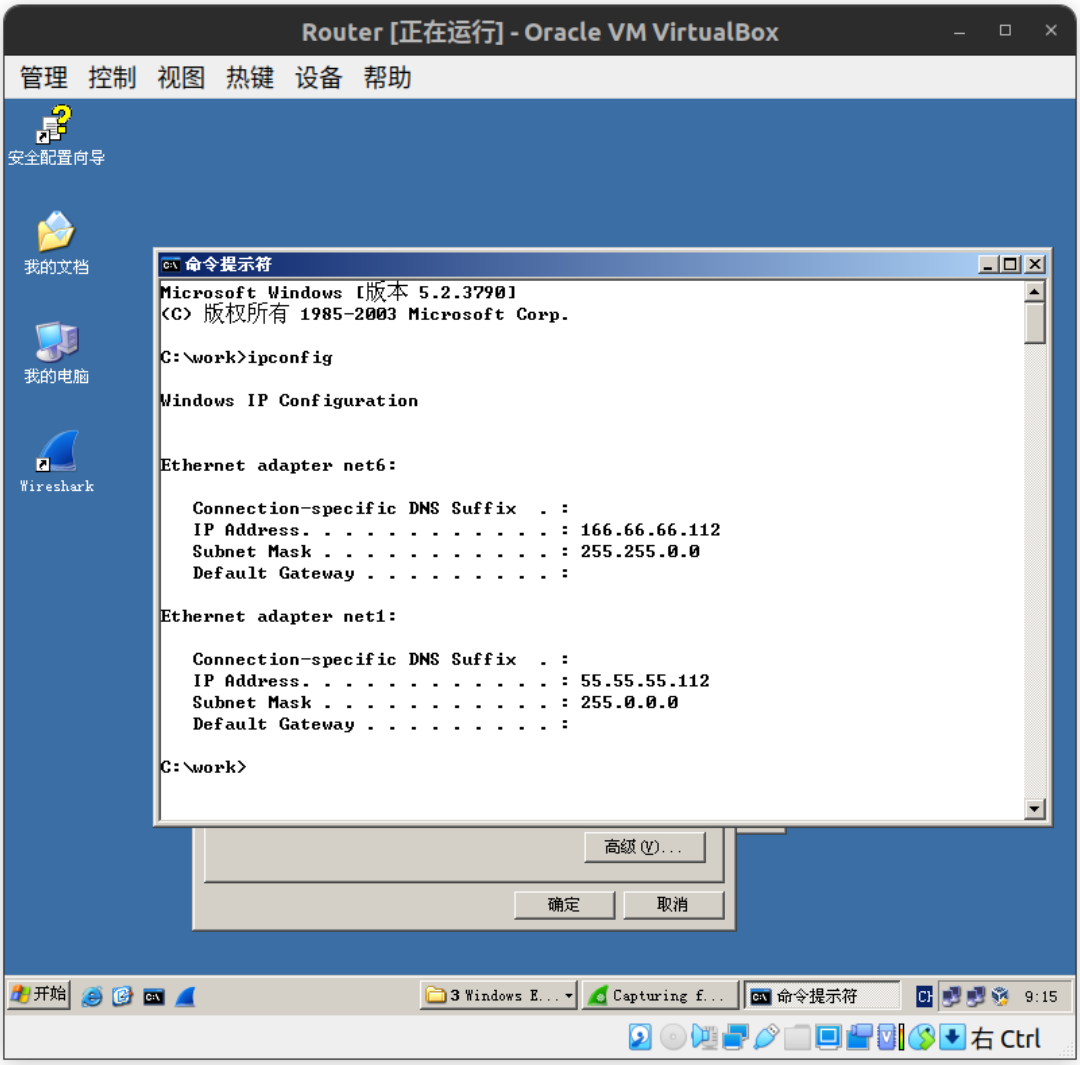

图 4: Router:ipconfig

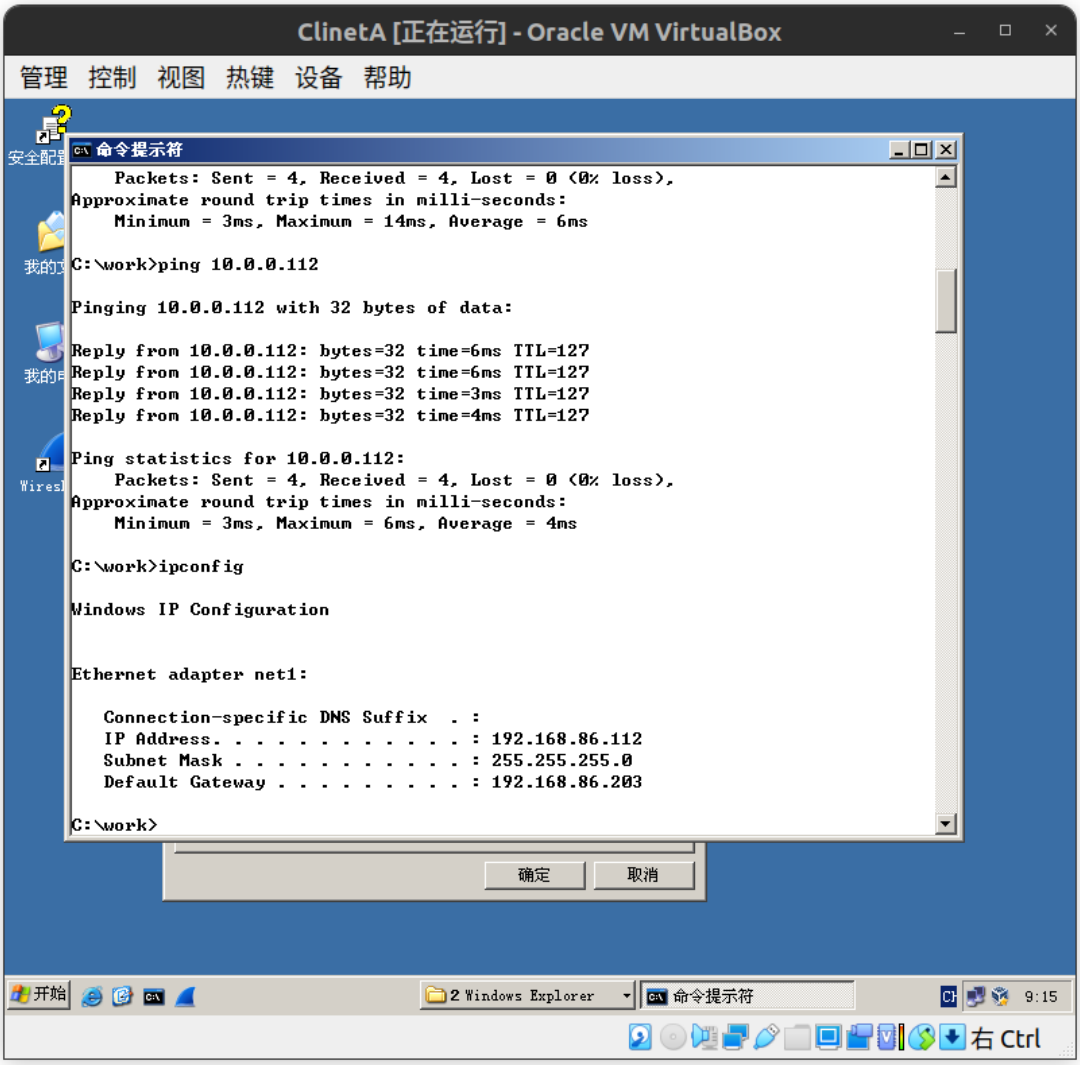

图 5: Server A:ipconfig

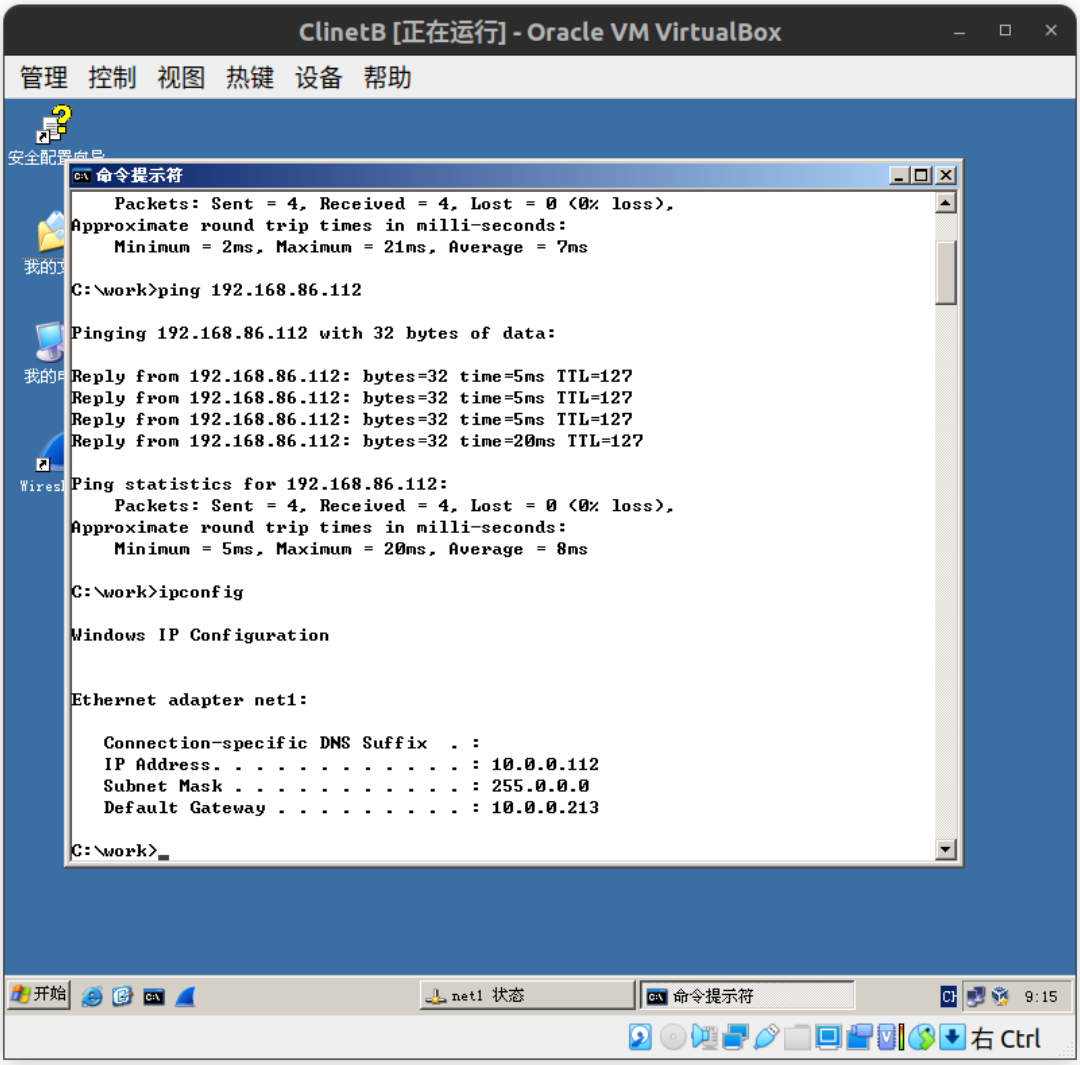

图 6: Server B:ipconfig

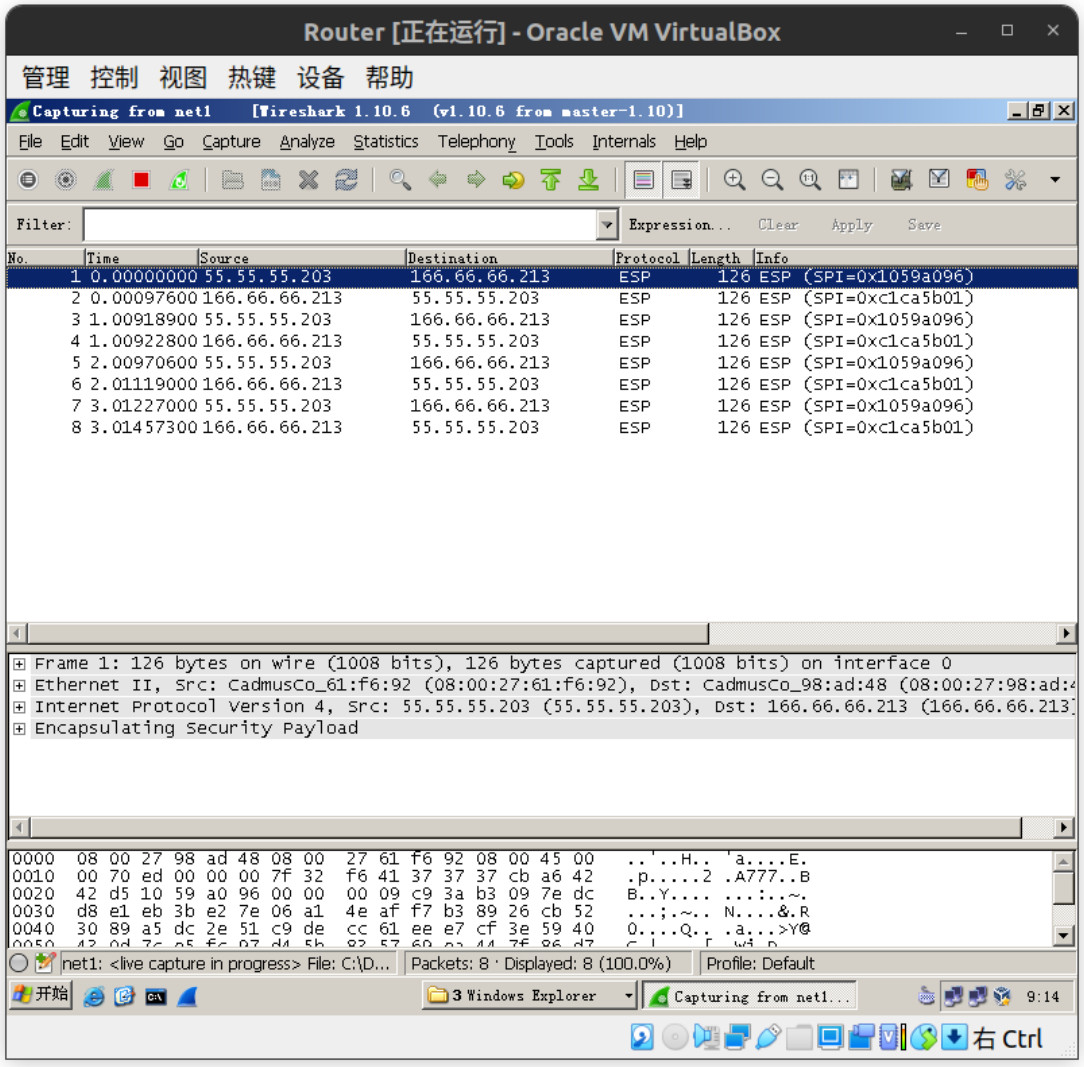

图 7: wireshark 检测

5 实验总结

这次实验中遇到两个问题:

问题 0 在 Virtual Box 中无法配置 IP 地址、子网掩码及网关。

原因 0 在 Virtual Box 配置的是网卡。

解决方案 0 启动虚拟机，在虚拟机内配置 IP 地址、子网掩码及网关。

问题 1 “配置并启用路由和远程访问”项无法点击。

原因 1 “配置并启用路由和远程访问”项已经开启。

解决方案 1 先选用“禁用路由和远程访问”。