高等院校计算机应用系列教材

计算机网络实验教程

刘晓青　颜丽君　编著

清华大学出版社
北　京

内 容 简 介

本书是一本面向“新工科”人才培养的计算机网络实验教材，以五层模型为主线，系统介绍了从物理层到应用层所涉及的实验与工程场景。本书共分 6 章，32 个实验案例，将企业真实网络案例与课程内容深度融合，以华为 eNSP+Wireshark 软件为实验平台，采用“案例驱动＋故障注入”的新范式，实现“零门槛”部署与“高保真”体验。实验内容梯度清晰，从基础型 (验证原理)、提高型 (综合配置) 到拓展型 (故障排除与创新设计)，教师可按学时、学生水平自由裁剪。

本书实验丰富、典型，所有实验均提供理论视频讲解、完整步骤截图、故障现象剖析、实验总结分析以及习题思考探索等，既可用于高等院校计算机网络相关课程的配套实验教材，也可作为华为认证及企业运维技能提升的自学指南。

图书在版编目(CIP)数据

计算机网络实验教程 / 刘晓青, 颜丽君编著.
北京 : 清华大学出版社, 2026. 1. -- (高等院校计算机
应用系列教材). -- ISBN 978-7-302-70549-9

Ⅰ. TP393-33

中国国家版本馆CIP数据核字第20255EW829号

责任编辑：刘金喜
封面设计：高娟妮
版式设计：妙思品位
责任校对：成凤进
责任印制：刘　菲

出版发行：清华大学出版社
网　　址：https://www.tup.com.cn，https://www.wqxuetang.com
地　　址：北京清华大学学研大厦A座　　**邮　编：**100084
社 总 机：010-83470000　　**邮　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市科茂嘉荣印务有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　张：**10.75　　**字　数：**236千字
版　　次：2026年4月第1版　　**印　次：**2026年4月第1次印刷
定　　价：49.80元

产品编号：114243-01

前　言

计算机网络是高等院校计算机、通信、电子信息等专业的核心必修课程，肩负着为学生奠定“网络思维、工程能力、创新意识”三重底座的使命。这一课程既要讲透 OSI 七层模型与 TCP/IP 协议簇的理论脉络，更要让学生在真实链路、真实设备、真实故障中学会“让网络通、让业务稳、让问题现形”。遗憾的是，当下课堂“重理论、轻实践”的痼疾依旧明显，学生能够熟练背诵三次握手流程，却不一定能在真实网络中发现一条ping不通的链路；能够画出OSPF 区域划分示意图，却不一定能让设备正确下发一条 LSA。教材与工程现场之间的巨大鸿沟，已成为人才培养的“最后一公里”难题。为此，我们在十余年一线教学与数十个企业真实项目历练的基础上，编写了这本《计算机网络实验教程》。本教材通过“案例驱动＋故障注入”的新范式，即“以真实网络案例为主线、以解决实际问题为目标”，在每个实验项目中预设典型故障点(如 VLAN 漏配、路由环路、NAT 地址池耗尽、TCP 半连接队列溢出)，让学生通过“日志分析→抓包比对→命令调试→现象复现”四步排障法，在“踩坑→定位→修复→验证”的闭环中养成工程师思维。内容编排遵循“由浅入深、层层递进”的原则。

第 1 章：先用ping、Tracert、Netstat等最基础的命令，帮学生建立“先诊断、再动手”的网络思维。

第 2 章：回到物理层，亲手制作双绞线并进行测试，体会“底层不牢、地动山摇”。

第 3 章：聚焦数据链路层，从集线器冲突域到交换机 VLAN 隔离、STP 防环、链路聚合，呈现二层技术的演进脉络。

第 4 章：深入网络层，静态/动态路由、策略路由、ARP、OSPF、ACL、NAT技术一气呵成，打通“路由可达”与“策略可控”的“任督二脉”。

第 5 章：在传输层深度剖析 TCP三次握手、四次挥手、流量控制、拥塞控制、Keepalive 与 UDP 实时性对比，再现“可靠”与“高效”的设计权衡。

第 6 章：登上应用层，综合演练 DNS、WWW、DHCP 等主流协议，将网络视角延伸至最终用户的业务体验。

本教材的特色在于：(1)企业真实案例驱动；(2)全流程视频/截图指导，操作直观；(3)提供分级实验库，适配不同教学需求；(4)采用“案例驱动+故障注入”实验新范式，设置典型故障点培养学生的排错能力，突出实战性，有效解决传统教材重理论轻实践的问题。

本教材实验丰富、典型，所有实验均提供理论视频讲解、完整步骤截图、故障现象剖析、实验总结分析以及习题思考探索等，既可用于高等院校计算机网络相关课程的配套实验教材，也可作为华为认证及企业运维技能提升的自学指南。

本教材配套的实验理论视频讲解可通过扫描书中二维码观看，也可将二维码图片传至电脑微信中，通过识别二维码的方式在电脑中播放。

本教材由刘晓青和颜丽君共同编著，在编写过程中，特别感谢清华大学出版社的大力支持和楚雄师范学院网络工程教研室教师提出的宝贵意见。

由于时间仓促，加之编者水平有限，书中难免有不足之处，敬请广大读者批评指正。

编　者

2026年1月

目　录

第 1 章

常用网络命令及实验环境

在数字化时代，计算机网络是现代信息技术的基石，掌握基本的网络命令和如何搭建实验环境是学习网络技术的首要步骤。本章将深入聚焦网络技术学习中最为实用的命令行工具，逐一详解其基本用法。通过这些命令的学习，读者将能够轻松诊断网络故障、洞察网络状态，从而在面对复杂的网络问题时，迅速找到症结所在并加以解决。同时，本章还会指导读者搭建简单实用的eNSP网络实验环境，eNSP(Enterprise Network Simulation Platform)是一个功能强大的网络仿真平台，它能够模拟真实的网络环境，让读者在虚拟的环境中进行各种网络实验。通过搭建eNSP实验环境，读者可以在安全、可控的条件下，实践所学的网络知识，加深对网络原理的理解，为后续深入探索网络世界的奥秘铺设坚实的前进道路。

1.1 常用网络命令

网络命令和实验环境

一、实验目的

(1) 熟悉常用网络命令的基本用法。
(2) 掌握网络诊断和故障排查的基本技能。
(3) 理解网络通信的基本原理。

二、实验理论知识概述

网络命令是管理和诊断计算机网络的工具。它们可以帮助用户检查网络连接、配置网络设备、监控网络流量以及进行故障排查。以下是一些常用的网络命令及其理论知识。

1．ping 命令

ping命令是网络诊断中最基础且广泛使用的命令之一，用于测试目标主机的网络可达性。该命令通过向目标主机发送ICMP(internet control message protocol，因特网控制消息协议)回显请求消息，并监听回显响应，以此来验证网络连接的有效性。若目标主机在网络可达范围内，将返回相应的回显响应；反之，若无法接收到响应，则表明目标主机不可达或网络连接存在问题。ping命令常用参数及功能如表1-1所示。

ping命令的格式：

```
ping [参数] [目标主机名或IP地址]
```

表 1-1　ping 命令常用参数

参数	功能	示例
-t	持续发送回显请求，直到用户通过Ctrl+C或者Ctrl+Break组合键手动中断	ping -t www.baidu..com
-n count	指定发送回显请求的次数，如count为10，则向目标主机发送10个回显请求	pint -n 10 www.baidu.com
-l size	指定向目标主机发送的以字节为单位的数据报大小(默认发送32字节)	ping -l 64 www.baidu.com
-i TTL	指定发送的数据包的生存时间(TTL, time to live)	ping -i 10 www.baidu.com

2．ipconfig 命令

ipconfig命令用于显示和配置当前计算机的网络配置信息。在Windows系统中，ipconfig可以显示所有网络接口的IP地址、子网掩码和默认网关。ipconfig命令常用参数及功能如表1-2所示。

ipconfig命令的格式：

```
ipconfig 参数
```

表 1-2　ipconfig 命令常用参数

参数	功能	示例
/all	显示完整的网络配置信息，包括IP地址、子网掩码、默认网关、DNS服务器等	ipconfig/all
/release [adapter]	释放指定适配器(如以太网或Wi-Fi)的IP地址	ipconfig/release "Ethernet"
/renew [adapter]	重新获取指定适配器的IP地址	ipconfig /renew "Wireless Network Connection"
-/flushdns	清除DNS解析缓存	ipconfig/flushdns
/displaydns	显示本地计算机的DNS解析缓存内容	ipconfig/displaydns

3．tracert 命令

tracert命令用于追踪数据包从源主机到目标主机的路径。它们通过发送带有递增TTL(生存时间)值的数据包来实现这一点。每经过一个路由器，TTL值减1，当TTL值减

到0时，路由器会返回一个ICMP超时消息，从而揭示了数据包的路径。tracert命令常用参数及功能如表1-3所示。

tracert命令格式：

```
tracert [-d] [-h 最大跳数] [-w timeout] [-R]  追踪的目标主机名或IP地址
```

表 1-3　tracert 命令常用参数

参数	功能	示例
-d	不解析地址为主机名，直接显示IP地址	tracert -d www.baidu.com
-h 最大跳数	指定搜索目标的最大跳数	tracert -h 10 www.baidu.com
-w timeout	指定等待每个回复的超时时间	tracert -w 5000
-R	跟踪往返路径(仅适用于IPv6)	tracert -R

4．nslookup 命令

nslookup命令用于查询DNS(domain name system，域名系统)服务器，以获取与域名相关的各种信息，如IP地址、MX记录(邮件交换记录)等。 nslookup命令常用参数及功能如表1-4所示。

nslookup命令格式：

```
nslookup [选项] [查询类型] [域名]
```

表 1-4　nslookup 命令常用参数

参数	功能	示例
域名	查询域名对应的 IPv4 地址	nslookup www.baidu.com
-query=AAAA	查询域名对应的 IPv6 地址	nslookup -query=AAAA www.baidu.com
-query=MX	查询域名的邮件服务器记录	nslookup -query=MX baidu.com

5．netstat 命令

netstat命令用于显示网络连接、路由表、接口统计等信息。它对于监控网络状态和诊断网络问题非常有用。netstat命令常用参数及功能如表1-5所示。

netstat命令格式：

```
netstat [选项]
```

表 1-5　netstat 命令常用参数

参数	功能	示例
-a	显示所有连接和监听端口(包括服务器和客户端的连接)	netstat -a
-at	仅显示所有 TCP 连接，不包括 UDP 连接	netstat -at
-anl	以数字形式显示所有监听状态的端口，常用于查找服务绑定的端口	netstat -anl

(续表)

参数	功能	示例
-r	显示路由表信息	netstat -r
-s	显示TCP、UDP和IP协议的统计信息，如传输的数据包数量、错误数量等	netstat -s
-i	显示网络接口的统计信息，包括发送和接收的数据包数量、错误数量等	netstat -i
-e	显示以太网的统计信息，如发送和接收的字节数、冲突次数等	netstat -e

6．arp 命令

arp命令用于显示和修改ARP缓存，ARP是地址解析协议，它将IP地址解析为MAC地址。通过arp命令，可以查看和修改本地主机的ARP表。

arp命令是网络管理员和IT专业人员工具箱中的重要工具，它对于日常的网络管理和故障排查至关重要，可以帮助用户更有效地与网络进行交互，并快速解决网络问题。arp命令的常用参数及功能如表1-6所示。

arp命令格式：

```
arp [选项] [IP地址] [MAC地址] [接口]
```

表 1-6　arp 命令常用参数

参数	功能	示例
-a	显示当前 ARP 缓存中的所有条目	arp -a
-d	删除所有接口的ARP表项	arp -d
-d IP地址	删除指定的 IP 地址条目	arp -d 192.168.2.100
-s IP地址 MAC地址	添加静态 ARP 条目，将 IP 地址与 MAC 地址绑定	arp -s 192.168.2.100 FF:1A:2B:3C:4D:5E

三、实验内容

案例 1：使用 ping 命令检测网络中的延迟和丢包率

案例背景：小明访问百度网站时感觉网速较慢，怀疑网络延迟较高，使用ping命令检查网络中的延迟和丢包率。

1．打开命令行界面

在 Windows 中，使用cmd或PowerShell；在macOS或Linux中，使用 Terminal。

2．使用 ping 命令测试

用ping命令测试与www.baidu.com的连通性，结果如图1-1所示。

```
ping  www.baidu.com
```

图 1-1　ping 测试结果

3．检查延迟和丢包率

ping命令会发送 ICMP(internet control message protocol)回显请求消息到指定的目标，并等待 ICMP 回显响应。每个响应的时间就是一次往返时间(round-trip time，RTT)，也就是从发送请求到接收响应的时间。这个时间通常以毫秒(ms)为单位。

如果ping命令发送的请求没有收到响应，就会被认为是丢包。ping命令会显示丢包的数量和丢包率。丢包率是丢包数量与发送的总数据包数量的比例。

图1-1中数据分析字节为32，表示ICMP回显响应数据包的大小是32字节，这里同样指的是数据负载的大小。

时间=33ms：表示从发送ICMP回显请求到接收到回显响应的时间是33毫秒。这是一个网络延迟的度量，也称为往返时间(RTT)。33毫秒是一个相对较好的延迟时间，表明网络连接响应迅速。延迟时间会受到多种因素的影响，包括物理距离、网络拥堵、路由器处理速度等。

TTL=42：TTL值是42，表示数据包在被丢弃之前可以经过的路由器数量。TTL的初始值通常取决于操作系统，Windows系统通常是128，而Linux/UNIX系统通常是64。每经过一个路由器，TTL值就会减少1。TTL值减少到0时，数据包将不会被进一步转发，而是被丢弃，并且发送ICMP超时消息给发送者。

在这个例子中，TTL=42意味着数据包在到达你的计算机之前已经经过了一定的网络距离。例如，如果一个Linux/UNIX系统以64为TTL开始，那么42的TTL值表明数据包已经经过了64－42＝22个路由器。这个数字是关于数据包所走路径长度的粗略估计。

综上所述，这条 ping 回复表明计算机与IP地址157.148.69.74之间的网络连接表现良好，延迟较低，且数据包已经经过了一定数量的网络跳数。利用TTL的值可以推断出目标主机相对于用户所在网络的位置。

4．使用参数控制 ping 命令

发送特定数量的包：使用 -c参数(在 Linux/macOS 中)或 -n 参数(在 Windows 中)来指定发送的 ICMP 请求的数量。

```
ping -c 数量 IP地址/域名  # Linux/macOS
ping -n 数量 IP地址/域名  # Windows
```

向百度网站发送10个ICMP 请求，如图1-2所示。

图 1-2　ping -n 测试结果

持续发送包：使用-t参数(在 Windows 中)持续发送 ICMP 请求。

```
ping -t [目标IP地址或域名]
```

会持续发送 ICMP 请求，直到手动停止(通常是通过按 Ctrl+C组合键)，如图1-3所示。

图 1-3　ping -t 测试结果

5．分析结果

延迟：查看每个响应的时间，如果时间稳定且短，说明网络延迟低。如果时间波动大或很长，则可能存在网络延迟问题。

丢包：如果ping显示有丢包(例如，“请求超时”或“无响应”)，表明网络中可能存在丢包问题。高丢包率通常意味着网络连接不稳定。

6．记录和报告

在进行网络故障排查时，记录ping命令的输出结果非常重要。可以将输出复制到文本文件中，或者使用命令行的重定向功能将输出保存到文件中，例如：

```
ping IP地址|域名 > 文件名
```

这个文件的位置取决于执行命令时所处的目录和指定的输出目录。如果在命令行中

直接输入这个命令，并且没有指定特定的目录，那么文件将会保存在当前的工作目录中。如果希望将文件保存在特定的目录，比如D盘，则可以使用绝对路径或者相对路径来指定目录，例如ping www.baidu.com > d:/文件名，如图1-4所示。

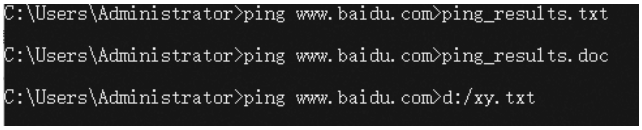

图 1-4　重定向功能

通过这些步骤，可以使用ping命令检测网络中的延迟和丢包率，从而帮助诊断网络问题。

案例 2：解决家庭网络连接问题

案例背景：小明在家中使用笔记本电脑，突然遇到网络连接不稳定的情况：网页打开缓慢，有时甚至无法加载，可以按以下的步骤进行检查。

1．检查物理连接

确认网线是否插好，或者尝试重启路由器和调制解调器。

2．使用 ipconfig 查看网络配置

使用Win + R组合键打开“运行”对话框，输入cmd命令并按Enter键。在命令提示符中输入ipconfig命令并按Enter键，会显示当前的网络配置，包括IP地址、子网掩码、默认网关和DNS服务器，如图1-5所示。

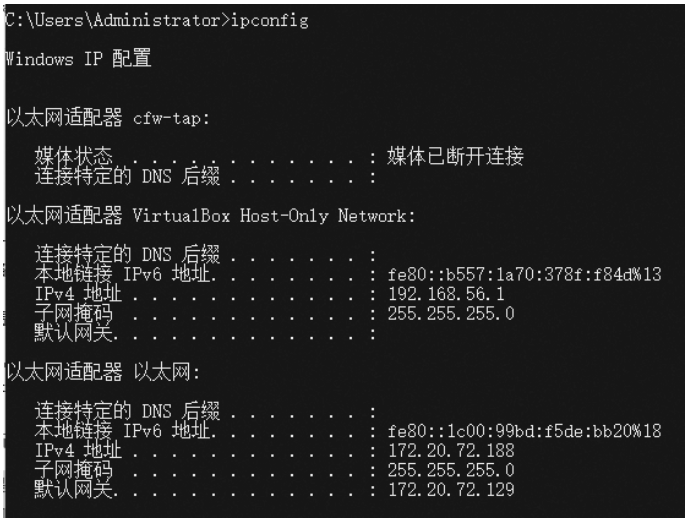

图 1-5　ipconfig 测试结果

3．观察并分析输出结果

IPv4 地址：确保你的设备获得了有效的IP地址，如果显示为0.0.0.0或者是 169.x.x.x(链接本地地址)，则可能存在 DHCP 问题，本案例中的IP地址是192.168.56.1。

子网掩码：通常为255.255.255.0或类似数值，确定网络位数，本案例的子网掩码是255.255.255.0，表示它有24位网络位。

默认网关：确认默认网关(通常为路由器的接口IP地址)是否正确。如果不存在或不正确，可能需要重置路由器或重新配置网络设置。本案例中的默认网关是172.20.72.129。

4．输入 ipconfig /all

使用 ipconfig /all命令可查看更详细的网络配置信息，包括物理地址、DHCP服务器，如图1-6所示。

```
C:\Users\Administrator>ipconfig/all

Windows IP 配置

   主机名  . . . . . . . . . . . . . : PC-20221120ZODF
   主 DNS 后缀 . . . . . . . . . . . :
   节点类型 . . . . . . . . . . . . : 混合
   IP 路由已启用 . . . . . . . . . . : 否
   WINS 代理已启用 . . . . . . . . . : 否

以太网适配器 cfw-tap:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : TAP-Windows Adapter V9
   物理地址. . . . . . . . . . . . . : 00-FF-0E-BB-C3-10
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

以太网适配器 VirtualBox Host-Only Network:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   物理地址. . . . . . . . . . . . . : 0A-00-27-00-00-0D
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::b557:1a70:378f:f84d%13(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.56.1(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 671744039
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-2B-0B-8D-B2-58-11-22-A8-9E-A4
   DNS 服务器  . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用

以太网适配器 以太网:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Realtek Gaming 2.5GbE Family Controller
   物理地址. . . . . . . . . . . . . : 58-11-22-A8-9E-A4
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::1c00:99bd:f5de:bb20%18(首选)
   IPv4 地址 . . . . . . . . . . . . : 172.20.72.188(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 172.20.72.129
   DHCPv6 IAID . . . . . . . . . . . : 106434850
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-2B-0B-8D-B2-58-11-22-A8-9E-A4
   DNS 服务器  . . . . . . . . . . . : 211.83.176.32
                                       211.83.176.33
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

图 1-6　ipconfig/all 测试结果

DNS服务器：查看是否存在有效的DNS服务器地址，如果不确定，可以手动设置为公共 DNS 服务器，如百度 的180.76.76.76。本案例的DNS服务器是211.83.176.32，备用DNS服务器是211.83.176.33。

物理地址：即网卡地址，本案例的网卡地址为58-11-22-A8-9E-A4。

5．尝试释放并重获 IP 地址

使用 ipconfig /release命令释放当前IP地址。

使用 ipconfig /renew命令尝试获取新的IP地址。

6．检查 DNS 解析

使用nslookup [hostname]查询DNS服务器来解析域名，如图1-7所示。

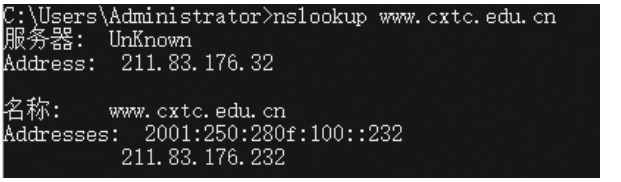

图 1-7　用 nslookup 查询 DNS 服务器

(1) 服务器：显示正在使用的DNS服务器的IP地址。

(2) Address：再次确认DNS服务器的IP地址。

(3) 名称：显示所查询的域名。

(4) Addresses：列出与域名关联的IP地址，表明www.cxtc.edu.cn对应的IP地址是211.83.176.232。

如果想使用指定的DNS服务器，可以使用-server参数，如图1-8所示。

```
nslookup  www.cxtc.edu.cn 180.76.76.76
```

图 1-8　使用指定的 DNS 服务器

这里的180.76.76.76是百度提供的公共DNS服务器地址。

7．清除 DNS 缓存

使用 ipconfig /flushdns 清除DNS缓存。

如果怀疑DNS解析问题，使用此命令清除DNS缓存，然后重新尝试访问网页。

8．联系 ISP

如果以上步骤都无法解决问题，可能需要联系互联网服务提供商(ISP)查询服务端是否存在问题。

经过上述步骤，用户可能发现并解决了网络连接问题。如果是DHCP服务问题，释放并重获IP地址通常能解决问题；如果是DNS缓存问题，清除DNS缓存可能有助于恢复正常的域名解析。如果这些步骤都不能解决问题，联系ISP可能是最后的办法。

案例 3：使用 tracert 命令诊断网络延迟问题

案例背景：如果用户想检查从自己的计算机到 www.baidu.com的网络路径，可以使用 tracert 命令查看数据包在到达目的地之前所经过的每个网络跳数(路由器或网络设备)。这个工具可以帮用户诊断网络延迟问题，因为它能够显示每个网络跳点的延迟时间。

1．执行 tracert 命令

```
tracert 域名|IP地址
```

tracert www.baidu.com 运行情况如图 1-9 所示。

图 1-9　执行 tracert 命令

2．分析输出结果

tracert 命令将显示一系列跳点，每个跳点代表数据包经过的一个网络设备(如路由器或网关)。

每一行：代表一个网络跳数。第一行(跳数 1)是用户的本地网络，通常是路由器。最后一行是目标服务器。

数字：每个数字代表到达该跳数所需的时间(毫秒)，对于每个跳点，tracert会显示三次尝试到达该跳点的时间(即时延)。

请求超时：表示在该跳数中，数据包没有收到响应，可能是因为网络拥堵或路由器配置问题。

3．识别延迟问题

高延迟：如果某个跳点的延迟时间显著高于其他跳点，可能表明该网络设备或连接存在问题。

丢包：如果某个跳点显示为星号(*)或“请求超时”，则表示数据包在该跳点丢失，这可能是由于网络不稳定或硬件故障。

通过以上步骤，可以使用 tracert 命令诊断和定位网络延迟问题，这对于解决网络连接问题和优化网络性能非常有帮助。

案例 4：使用 netstat 命令监控网络连接的实时状态

案例背景：小明的电脑运行速度较慢，怀疑电脑中毒，准备使用netstat命令监控网络连接的实时状态，排除潜在的网络问题。

1．输入 netstat 命令

netstat -ano运行情况如图1-10所示。

```
C:\Users\Administrator>netstat -ano

活动连接

  协议  本地地址          外部地址        状态           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1072
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       4340
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       4340
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       4532
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       7100
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       868
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       132
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1492
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1524
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       3812
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING       3980
  TCP    0.0.0.0:49673          0.0.0.0:0              LISTENING       840
  TCP    0.0.0.0:54523          0.0.0.0:0              LISTENING       35112
  TCP    127.0.0.1:4709         0.0.0.0:0              LISTENING       35112
  TCP    127.0.0.1:8440         0.0.0.0:0              LISTENING       4260
  TCP    127.0.0.1:8680         0.0.0.0:0              LISTENING       38788
  TCP    127.0.0.1:13013        0.0.0.0:0              LISTENING       38788
  TCP    127.0.0.1:13016        0.0.0.0:0              LISTENING       38788
  TCP    127.0.0.1:61910        0.0.0.0:0              LISTENING       4260
  TCP    127.0.0.1:65193        127.0.0.1:65194        ESTABLISHED     4260
  TCP    127.0.0.1:65194        127.0.0.1:65193        ESTABLISHED     4260
  TCP    172.20.72.188:139      0.0.0.0:0              LISTENING       4
  TCP    172.20.72.188:49409    14.205.45.88:443       CLOSE_WAIT      35112
  TCP    172.20.72.188:49410    14.205.45.88:443       CLOSE_WAIT      35112
```

图 1-10　netstat 命令运行情况

2．分析输出结果

协议：协议类型，如 TCP 或 UDP。

本地地址：本地 IP 地址和端口号。

外部地址：远程 IP 地址和端口号。

状态：连接状态，如 LISTENING(监听)、ESTABLISHED(已建立)、CLOSE_WAIT (等待关闭)等。

PID：与网络连接相关的进程 ID。

第一条数据是指协议是TCP；本地地址为0.0.0.0，端口号为135；外部地址为0.0.0.0，端口号为0；连接状态为监听，进程号为1072。

3．查看特定服务的网络连接状态

如果发现一个特定的进程正在监听自己不熟悉的端口，或者怀疑有恶意软件，则可以使用 -ano 和 -p 选项找出进程的名称。

netstat -ano | findstr “服务端口号”这个命令将显示所有使用特定端口服务的网络连接状态，其中服务端口号需要替换为想要监控的服务的实际端口号，如图1-11所示。

```
C:\Users\Administrator>netstat -ano|findstr "4260"
  TCP    127.0.0.1:8440         0.0.0.0:0              LISTENING       4260
  TCP    127.0.0.1:61910        0.0.0.0:0              LISTENING       4260
  TCP    127.0.0.1:65193        127.0.0.1:65194        ESTABLISHED     4260
  TCP    127.0.0.1:65194        127.0.0.1:65193        ESTABLISHED     4260
  TCP    172.20.72.188:65151    111.62.167.239:443     ESTABLISHED     4260
```

图 1-11　netstat 监控 4260 端口

4．查看所有 TCP 连接

使用netstat -p tcp命令查看所有TCP连接，如图1-12所示。

```
C:\Users\Administrator>netstat -p tcp

活动连接

  协议  本地地址          外部地址        状态
  TCP    127.0.0.1:65193        ieonline:65194         ESTABLISHED
  TCP    127.0.0.1:65194        ieonline:65193         ESTABLISHED
```

图 1-12　查看 TCP 连接

使用 netstat 命令可以监控特定服务的网络连接状态，及时发现并处理潜在的网络问题。

案例 5：使用 arp 命令诊断和解决网络访问问题

案例背景：在一个局域网环境中，公司员工报告其电脑无法访问网络。网络管理员怀疑可能是ARP缓存问题导致的网络访问问题。

1．打开命令行工具

在Windows系统中，选择“搜索栏”使用 cmd命令，打开命令提示符。

2．检查 ARP 缓存表

在命令行中使用 arp -a 命令查看当前的ARP缓存表，系统将列出所有已知的IP地址及其对应的MAC地址，如图1-13所示。

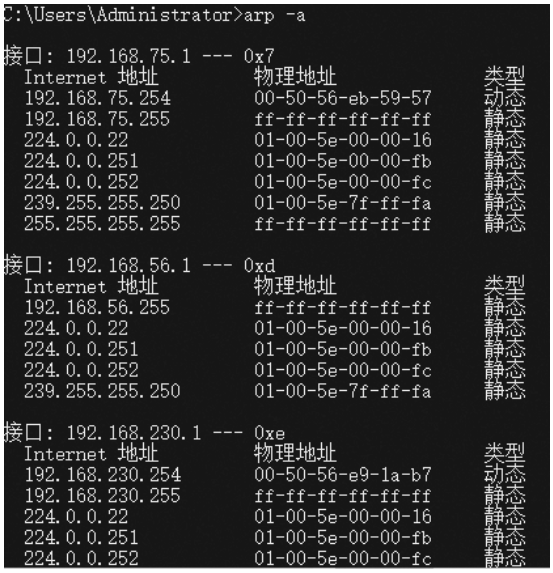

图 1-13　查看 ARP 缓存表

3．分析 ARP 缓存表

检查是否有错误的MAC地址与目标IP地址关联。例如，如果一个IP地址对应的MAC地址看起来异常(如全零或全FF)，这可能表明ARP缓存表已损坏或存在ARP欺骗问题。

4．清除 ARP 缓存

如果发现ARP缓存表有问题，可以使用 arp -d 命令清除特定的ARP缓存，或者使用 arp -d * 清除所有的ARP缓存，如图1-14所示。

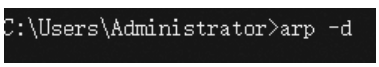

图 1-14　使用 arp -d 清除 ARP 缓存

5．重新获取 MAC 地址

清除ARP缓存后，尝试重新访问网络，让系统自动重新获取正确的MAC地址。绑定IP和MAC地址，查看新的ARP缓存，如图1-15所示。

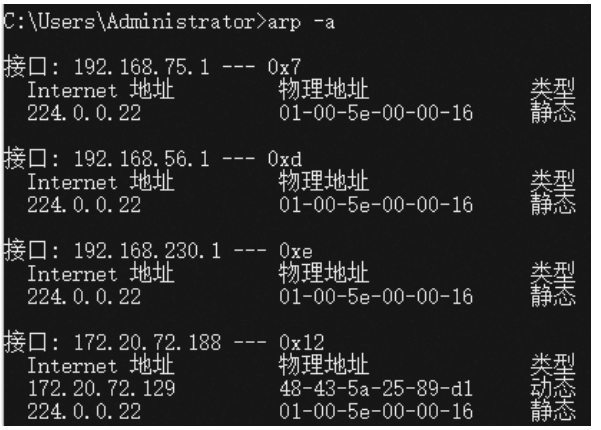

图 1-15　显示当前 ARP 缓存

6．静态绑定

如果是由于ARP欺骗引起的问题，可以使用 arp -s 命令静态绑定IP地址和MAC地址，以防止ARP欺骗。

```
ARP -s ip地址 mac地址
```

例如，arp -s 192.168.0.123 00-00-00-00-00-00-00-E0表示将IP地址192.168.0.123与MAC地址00-00-00-00-00-00-00-E0进行绑定，创建静态ARP条目。当访问192.168.0.123时直接找MAC地址00-00-00-00-00-00-00-E0，而不再动态发送请求寻找对应的MAC。

通过以上步骤，网络管理员成功清除了错误的ARP缓存，员工的电脑恢复了正常的网络访问。此外，通过绑定IP和MAC地址，管理员还增强了网络的安全性，防止了未来的ARP欺骗攻击。

arp 命令是网络诊断的重要工具，可以帮助网络管理员识别和解决ARP缓存问题、ARP欺骗问题。通过定期检查和维护ARP缓存表，可以确保网络的稳定性和安全性。

四、实验注意事项

(1) 权限问题：某些网络命令(如 tracert、ping 等)需要管理员权限才能执行，确保你有足够的权限来运行这些命令。

(2) 安全性：在使用网络命令时，要确保不会违反任何网络安全政策。避免使用这些工具进行未经授权的扫描或探测。

(3) 隐私考虑：某些命令可能会显示敏感信息，如IP地址和端口。在使用这些信息时，要尊重用户隐私和数据保护法规。

(4) 网络影响：频繁使用某些命令(如 ping 洪水或 traceroute)可能会对网络性能产生影响。在生产环境中使用这些命令时要谨慎。

(5) 命令参数：正确使用命令参数，避免误用。例如，tracert 命令的 -n 参数可以防止DNS解析，直接显示IP地址。

(6) 输出解读：学会正确解读命令输出。例如，netstat 命令的输出包含了许多信息，理解这些信息对于网络诊断至关重要。

总之，使用网络命令时，应确保具备适当权限，遵守安全政策，尊重用户隐私。注意命令参数的正确性，避免对网络造成不必要的负担。记录命令输出，以便追踪和报告问题。

五、实验小结

在本次实验中，我们探讨了几种常用的网络诊断命令，包括 ping、tracert、netstat 和 arp，它们对于排查网络故障和分析性能至关重要。这些命令可以帮助我们测试网络连通性、追踪数据包路径、查看网络连接状态和管理系统的ARP缓存表。使用时需注意权限要求、安全性、隐私保护以及命令的输出解读，以确保网络的稳定性和安全性。

总体来说，网络诊断命令是IT专业人员的重要工具，它们不仅能够快速定位和解决网络问题，还能够确保网络环境的高效运行。在实际操作中，应结合具体情况灵活运用这些命令，并遵守安全和隐私规定，以实现最佳的网络管理和维护效果。

六、实验思考

(1) 如何通过 netstat 和 arp 命令排查网络攻击？

(2) 如何综合使用 ping、netstat 和 traceroute 命令进行网络性能优化？

1.2 eNSP 仿真模拟器的安装与使用

一、实验目的

(1) 掌握eNSP模拟器的安装过程。

(2) 熟悉eNSP模拟器的基本操作。

(3) 学会使用Wireshark 进行抓包操作。

二、实验理论知识

1．eNSP 简介

eNSP(enterprise network simulation platform)是华为提供的一款网络仿真模拟器，主要用于学习、实践和测试企业网络场景。它可以模拟各种网络设备(如交换机、路由器、防火墙等)，创建以太网、无线网络等多种网络拓扑，并提供完整的网络设备配置和监控功能。eNSP还提供了丰富的实验场景，包括企业网络的基本搭建，VLAN、STP、OSPF、BGP等协议的配置和调试，帮助用户深入理解网络知识和技术。VirtualBox用于提供虚拟环境，支持eNSP的运行。

2．eNSP 基本配置模式

eNSP设备主要有三种基本配置模式：用户模式、系统视图、接口视图。

(1) 用户模式：这是设备的初始状态，用户可以查看设备的简单信息，但不能进行配置。

(2) 系统视图：通过输入system-view命令，用户可以进入系统视图，这是进行设备配置的主要模式。在这个模式下，用户可以进行VLAN配置、路由配置、用户密码设置等多种配置。

(3) 接口视图：通过interface GigabitEthernet0/0/1等命令，用户可以进入特定的接口进行配置，例如，设置IP地址、子网掩码等。

此外，eNSP还支持其他高级功能，如链路聚合和路由协议配置，这些功能对于构建复杂的网络拓扑和进行网络实验至关重要。链路聚合可以提高网络带宽和可靠性，而路由协议则允许设备在不同的网络之间传递路由信息，实现数据的正确路由。

使用quit命令可退回上级模式。无论当前处于哪种模式下，使用return命令都可直接返回用户模式。

3．Wireshark 简介

Wireshark 是一款广泛使用的开源网络协议分析工具，它能够捕获和分析网络上的数据包。以下是 Wireshark 的一些基本介绍和使用场景：

(1) 网络故障排查：Wireshark 可以帮助网络管理员快速定位网络问题，如丢包、延迟等。

(2) 安全分析：网络安全工程师可以使用 Wireshark 检测网络攻击、分析恶意软件的通信机制等，为网络安全研究提供支持。

(3) 协议开发：Wireshark可以帮助网络协议开发人员了解协议的实际运行情况，从而优化协议设计。

(4) 教学与研究：Wireshark 也广泛应用于计算机网络的教学与研究领域，帮助学生和教师深入了解网络通信原理。

Wireshark 的安装相对简单，可以从官方网站下载适合操作系统的安装包进行安装。

安装完成后，启动 Wireshark，选择要分析的网络接口，然后开始捕获数据包。Wireshark 提供了丰富的过滤器功能，包括捕获过滤器和显示过滤器，可以帮助用户快速找到感兴趣的数据包。

在使用 Wireshark 时，用户可以通过设置过滤器来筛选特定的数据包，例如根据 IP 地址、端口号或协议类型。Wireshark 还支持将捕获的数据包保存为文件，以便后续分析。

Wireshark 的界面包括菜单栏、工具栏、数据包列表面板、数据包详细信息面板和数据包字节信息面板。用户可以通过这些界面组件进行数据包的捕获、查看和分析。

总之，Wireshark 是一个功能强大的网络分析工具，适用于各种网络分析场景。通过学习和实践，用户可以掌握 Wireshark 的使用技巧，为网络通信研究和实践提供有力支持。

三、实验步骤

案例 1：实验环境的搭建

案例背景：小明需要做计算机网络的仿真实验，需要下载并安装eNSP仿真模拟器。实验环境的详细需求如表1-7所示。

表 1-7　安装环境需求

项目	最低配置	推荐配置	扩展配置
CPU	双核2.0GHz	四核2.0GHz或以上	八核2.0GHz或以上
内存	2 GB	4 GB	8 GB或以上
空闲磁盘空间	2 GB	4 GB	4 GB以上
操作系统	Windows XP	Windows 7	Windows 10
VirtualBox	VirtualBox 4.2.3 以上	VirtualBox 5.1 以上	VirtualBox 5.2 以上
最大组网设备数(台)	10	24	最大为50

备注：eNSP上每台虚拟设备都要占用一定的资源。每台电脑支持的虚拟设备数，根据配置的不同而有差别。扩展配置的最大组网设备数可根据内存增加而扩展，最大为50。

1．下载 eNSP

从华为官方或可信的第三方网站下载eNSP安装包。

eNSP下载地址：https://support.huawei.com。

VirtualBox下载地址：http://www.virtualbox.org。

Wireshark下载地址：http://www.wireshark.org/。

2．安装 Wireshark

找到Wireshark安装包，双击鼠标左键，打开Wireshark对话框，如图1-16所示。

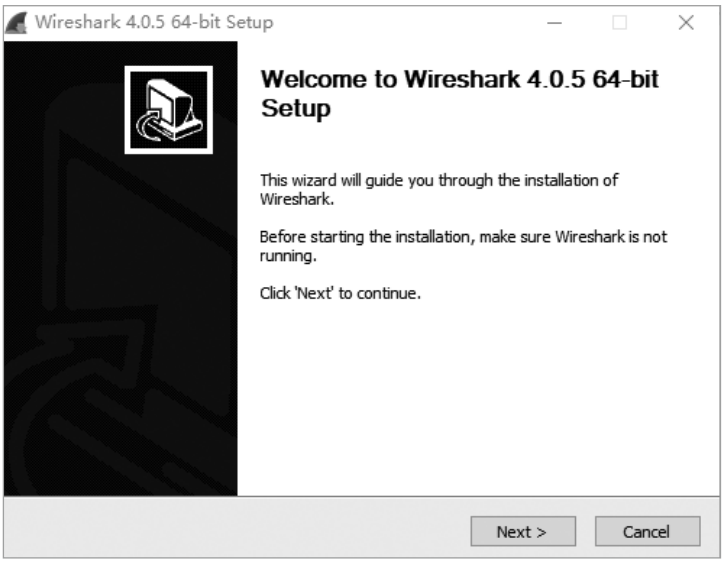

图 1-16　Wireshark 安装界面

在图1-16中单击Next按钮根据提示安装完成即可。

3．安装 VirtualBox

找到VirtualBox安装包，双击鼠标左键，打开VirtualBox对话框，如图1-17所示。

图 1-17　VirtualBox 安装界面

在图1-17中单击“下一步”按钮根据提示安装完成即可。

4．安装 eNSP

找到eNSP安装包，双击鼠标左键，打开“选择安装语言”对话框，首先选择安装期间使用的语言，如图1-18所示。

图 1-18　选择安装语言

在图1-18中单击“确定”按钮，进入eNSP的安装向导，如图1-19所示。

图 1-19　eNSP 安装界面

在图1-19中单击“下一步”按钮根据提示安装完成即可。

案例 2：认识 eNSP

案例背景：eNSP新手小白使用eNSP构建简单的拓扑结构。

1．认识 eNSP 的基本界面

eNSP的主界面主要由工具栏、网络设备区、工作区组成，如图1-20所示。

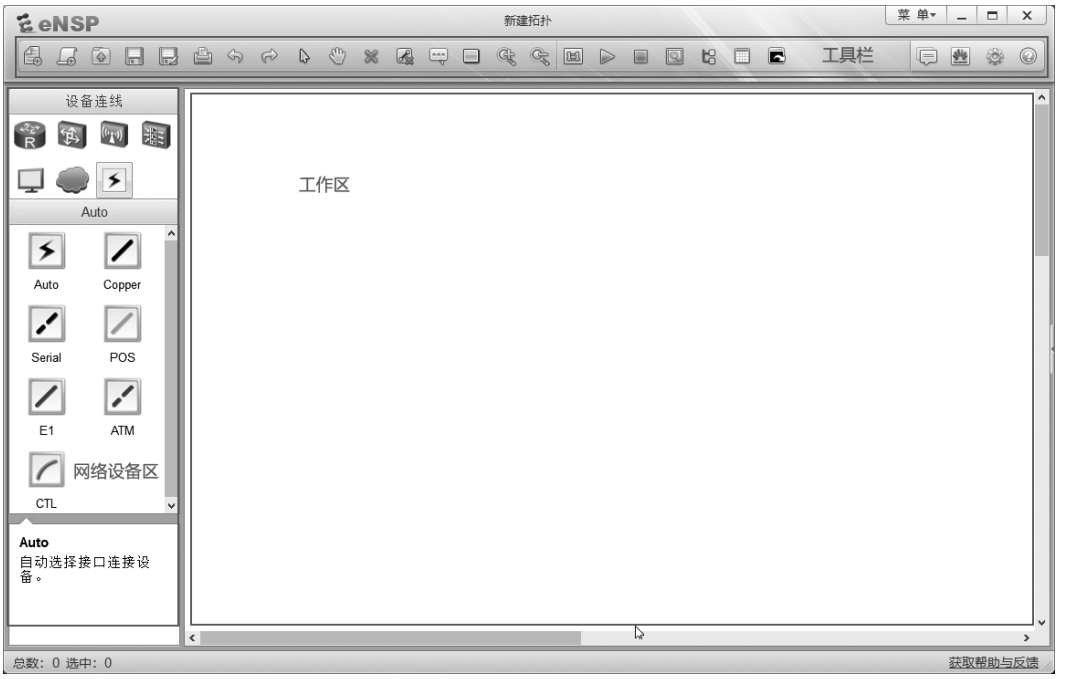

图 1-20　eNSP 主界面

工具栏：提供新建、打开项目，控制模拟器等快捷操作。

网络设备区：列出所有可用的网络设备，如路由器、交换机等。

工作区：用于绘制和展示网络拓扑结构。

2．创建项目

选择工具栏上的“新建拓扑”图标，或者选择菜单选项下的“新建拓扑”，在工作区新建网络拓扑。

3．构建拓扑

(1) 添加和连接设备

在设备面板中选择所需设备，按住鼠标左键不放拖到工作区域松开。此案例的网络拓扑需要两台PC机、一台S5700的交换机、一台AR1200的路由器，如图1-21所示。

设备放好后，用户可选择Auto设备连接线，eNSP 会根据情况自动为用户选择设备连接线类型和设备接口。若需要自己选择设备连接线类型和设备接口，如选择双绞线，则可在设备型号区中单击Copper，然后在工作区依次单击设备，并选择连接网线的接口。

选中设备，通过单击右键，选择“启动”“删除”“设置”“抓包”CLI进行相关设置。

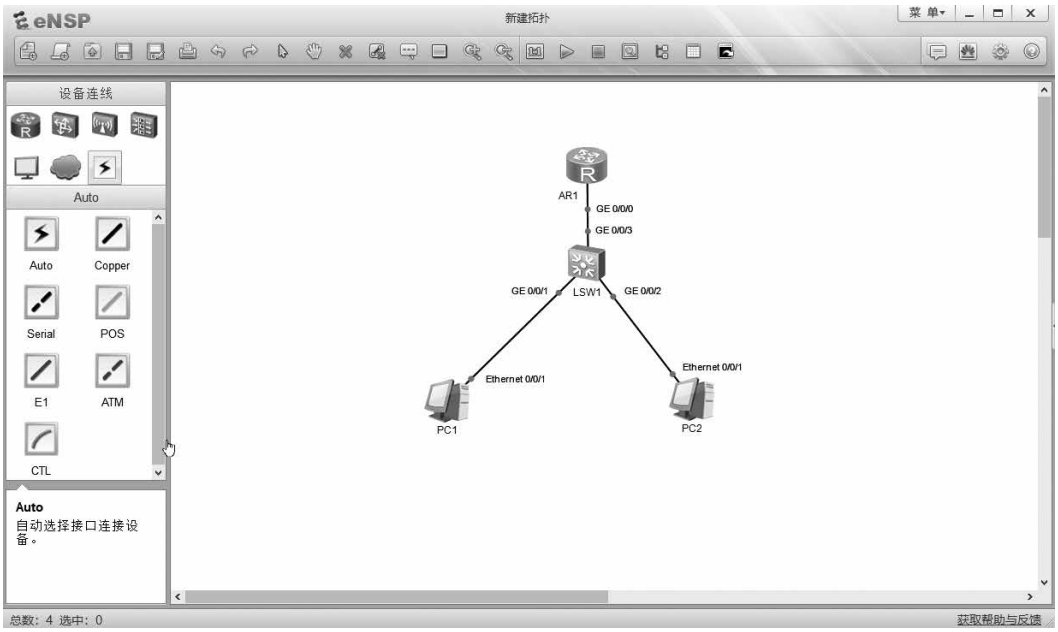

图 1-21　在 eNSP 中构建拓扑

(2) 开启设备

按住鼠标左键不放框选所有图标，选择工具栏的绿色开机按钮，开启设备；或者选中该设备，右键单击后选择“启动”，开启设备。

(3) 配置设备参数

选中交换机LSW1，用左键双击或用右键单击选择CLI，进入命令行界面，如图1-22所示。

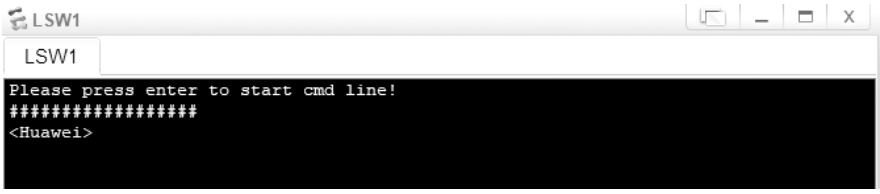

图 1-22　交换机的命令行界面

案例 3：认识 Wireshark Version 4.0.5

案例背景：小明想用Wireshark Version 4.0.5 获取访问百度网站的数据包信息。

1．打开 Wireshark Version 4.0.5

Wireshark主界面如图1-23 所示。

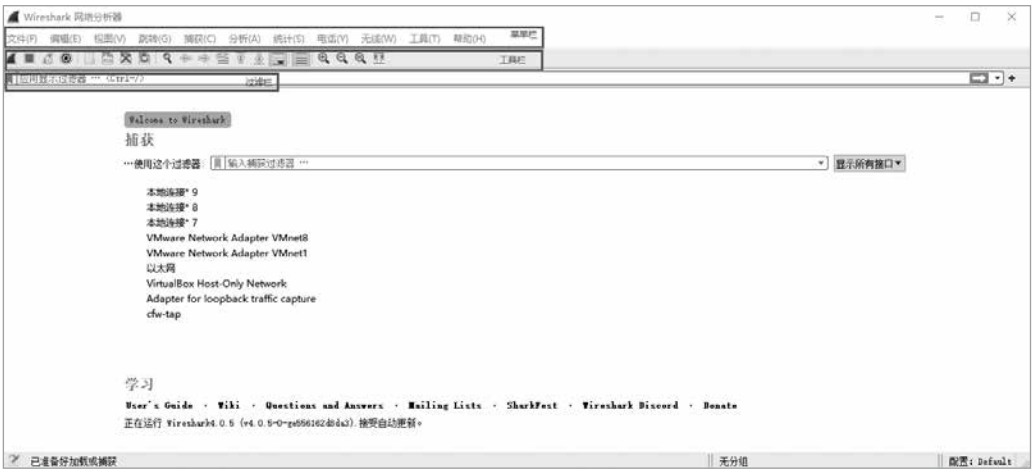

图 1-23　Wireshark 主界面

菜单栏：用于网络数据包的捕获、分析和处理。

工具栏：包括常用功能的快捷方式。

过滤栏：指定过滤条件，过滤数据包。

2．启动捕获配置

选择菜单栏上的“捕获”|“选项”命令，选中网卡复选框(这里根据各自电脑网卡使用情况选择，简单的办法是看使用的IP对应的网卡)，单击“开始”按钮，启动捕获功能，如图1-24所示。

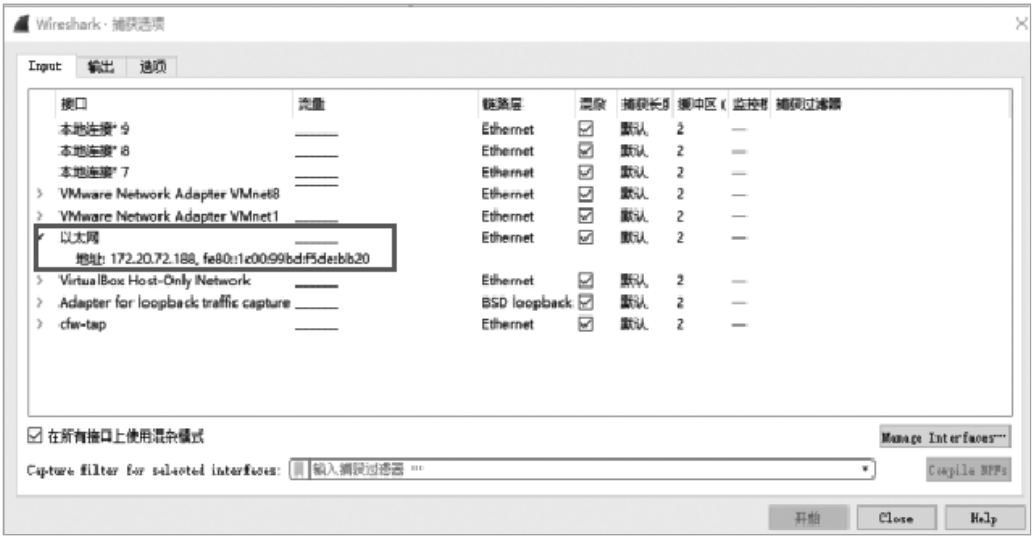

图 1-24　Wireshark 捕获选项

Wireshark启动后，处于捕获状态中，捕获输入如图 1-25 所示。

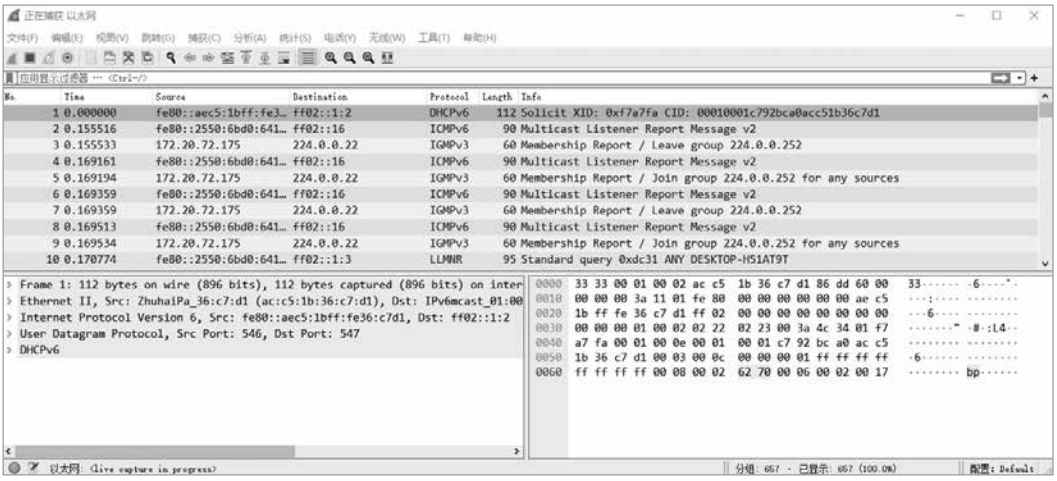

图 1-25　Wireshark 捕获数据

3．执行需要捕获的操作

选择“运行”命令，打开命令窗口，执行ping www.baidu.com命令，如图 1-26 所示。

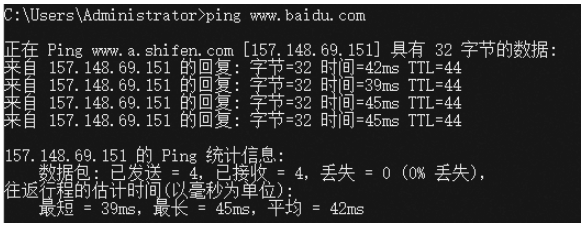

图 1-26　执行 ping 命令

使用Wireshark软件捕获的数据如图 1-27 所示。

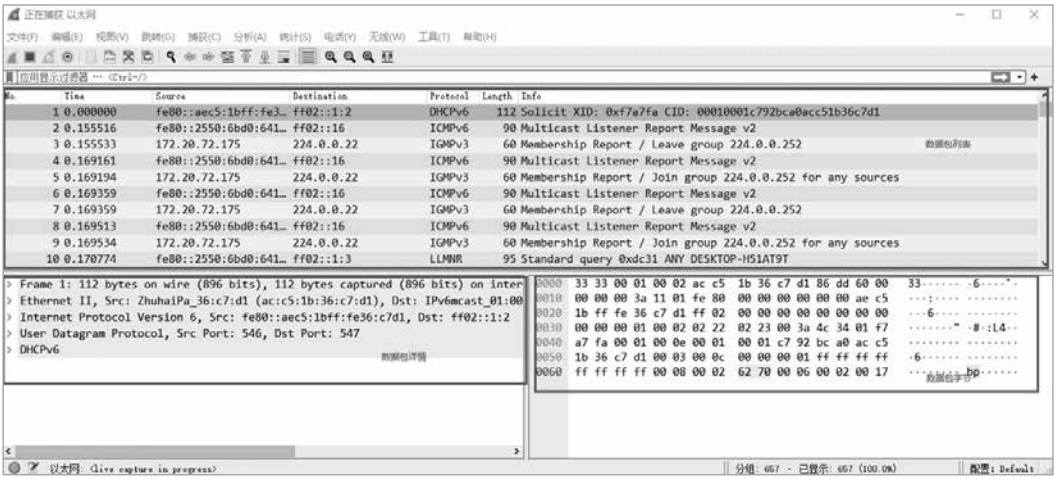

图 1-27　Wireshark 数据分析

(1) 数据包列表：核心区域，每一行就是一个数据包。

(2) 数据包详情：数据包的详细数据。

(3) 数据包字节：数据包对应的字节流。

四、实验注意事项

(1) 确保安装路径为英文，避免使用中文路径，这可能会导致安装失败。

(2) 在安装过程中，可能需要关闭Windows防火墙以避免潜在的冲突。

(3) 如以前安装过eNSP，注意清理干净再重新安装，安装时先安装插件，再安装eNSP。

(4) 在使用eNSP之前，阅读官方文档或教程，以便更好地理解其功能和操作步骤。

五、实验小结

通过本次实验，我们不仅掌握了eNSP和捕获软件的使用，还加深了对网络协议和网络通信原理的理解。这些知识和技能将为我们今后的网络学习和实践提供坚实的基础，帮助我们在网络设计、配置与故障排查等方面更加得心应手。

六、实验思考

(1) 当网络中出现丢包现象时，如何通过捕获软件分析确定丢包的原因是网络拥塞、设备故障还是其他原因？

(2) 如何利用捕获软件监测网络的带宽利用率？如何根据监测结果优化网络配置，提高网络性能？