

实验 1 搭建基础 IP 网络

eNSP 作为一款网络仿真工具平台，可以模拟华为企业级路由器和交换机的大部分特性，可模拟 PC 终端、集线器、网络云、帧中继交换机等。仿真设备配置功能，用户可以快速学习华为命令行，可以通过真实网卡与真实网络设备的对接，并且还可以模拟接口抓包，只管感受各种协议的豹纹交互过程。

学习目标

掌握 eNSP 模拟器的基本设置方法

掌握使用 eNSP 搭建简单的端到端网络的方法

掌握在 eNSP 中使用 Wireshark 捕获 IP 报文的方法

场景

在本实验中，您将熟悉华为 eNSP 模拟器的基本使用，并使用模拟器自带的抓包软件捕获网络中的报文，以便更好地理解 IP 网络的工作原理。

操作步骤

步骤一 启动 eNSP

本步骤介绍 eNSP 模拟器的启动和初始化界面。通过模拟器的使用将能够帮助您快速学习不掌握 TCP/IP 的原理知识，熟悉网络中的各种操作。

开启 eNSP 后，您将看到如下界面。左侧面板中的图标代表 eNSP 所支持的各种产品及设备。中间面板则包含多种网络场景的样例。

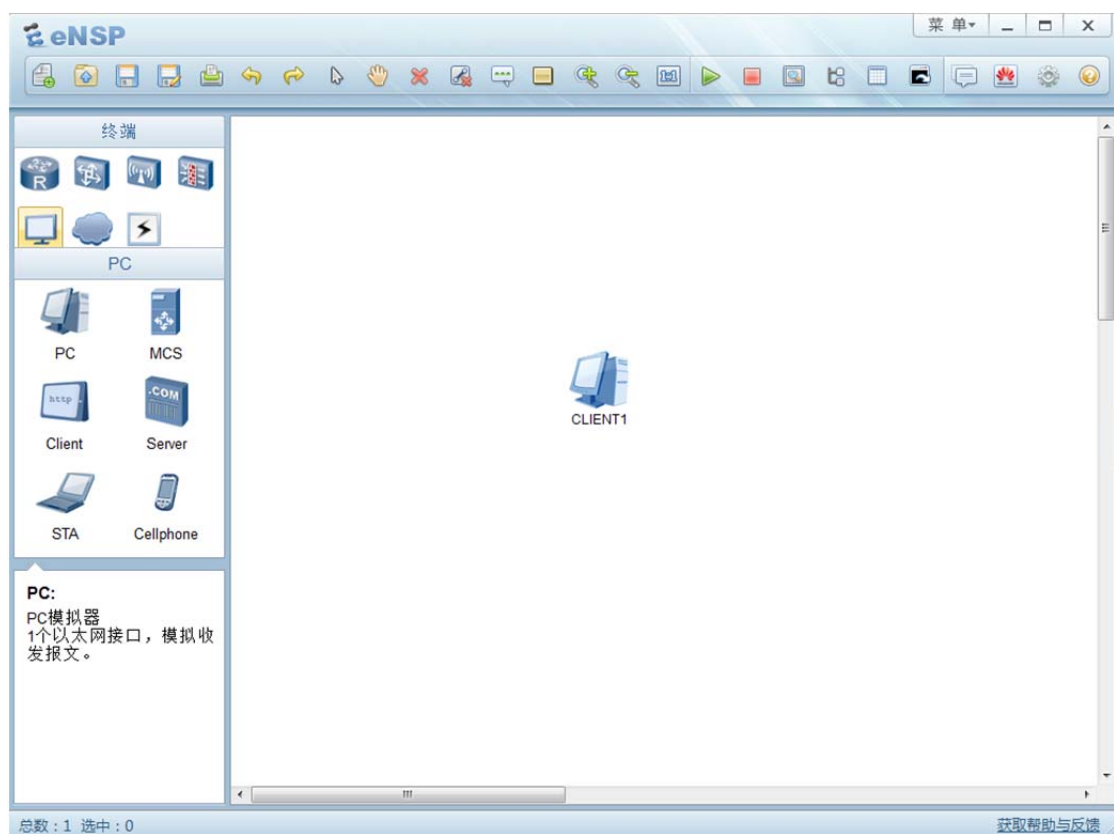


单击窗口左上角的“新建”图标，创建一个新的实验场景。

您可以在弹出的空白界面上搭建网络拓扑图，练习组网，分析网络行为。在本示例中，您需要使用两台终端系统建立一个简单的端到端网络。

步骤二 建立拓扑

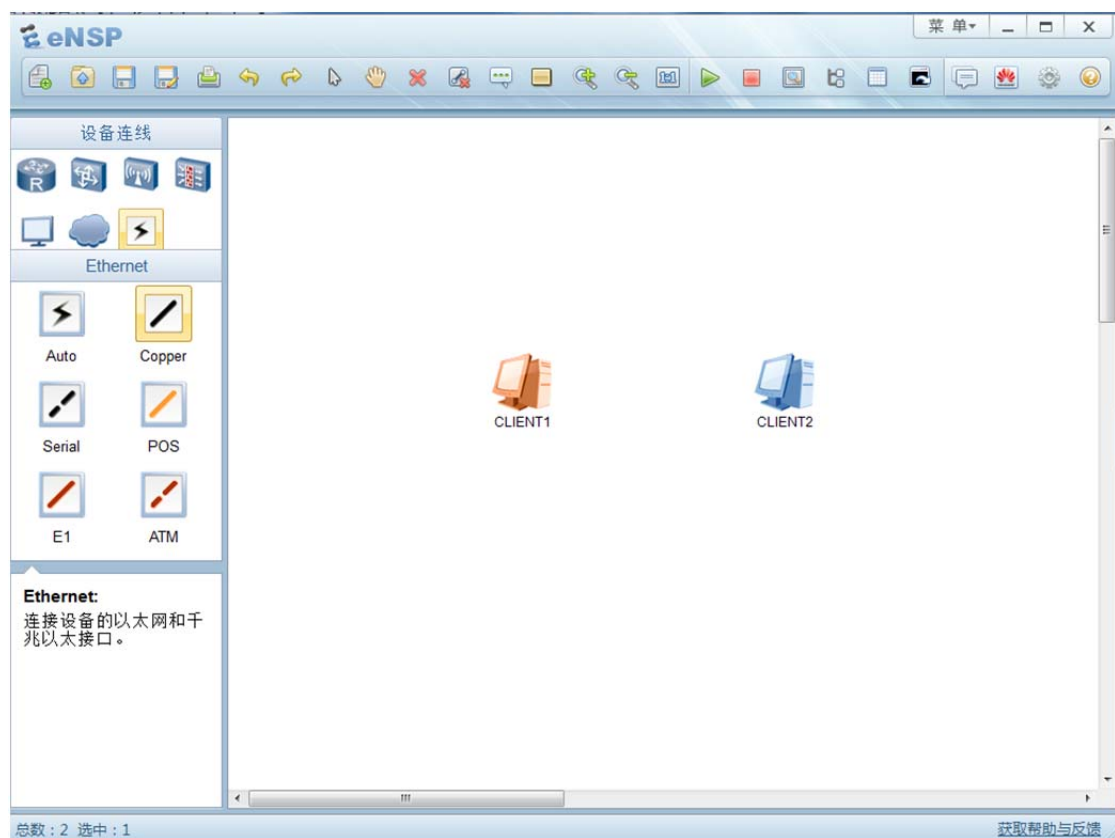
在左侧面板顶部，单击“终端”图标。在显示的终端设备中，选中“PC”图标，把图标拖动到空白界面上。



使用相同步骤，再拖入一个 PC 图标到空白界面上，建立一个端到端网络拓扑。PC 设备模拟的是终端主机，可以再现真实的操作场景。

步骤三 建立一条物理连接

在左侧面板顶部，单击“设备连线”图标。在显示的媒介中，选择“Copper (Ethernet)”图标。单击图标后，光标代表一个连接器。单击客户端设备，会显示该模拟设备包含的所有端口。单击“Ethernet 0/0/1”选项，连接此端口。

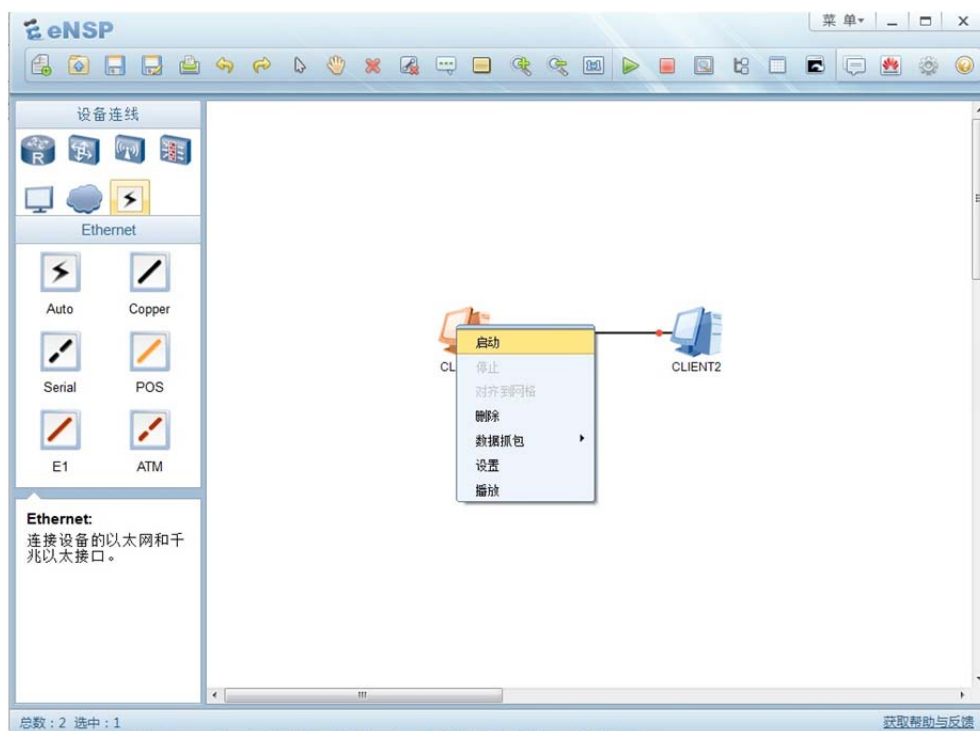


单击另外一台设备并选择“Ethernet 0/0/1”端口作为该连接的织点，此时，两台设备间的连接完成。

可以观察到，在已建立的端到端网络中，连线的两端显示的是两个红点，表示该连线连接的两个端口都处于 Down 状态。

步骤四 进入终端系统配置界面

右击一台终端设备，在弹出的属性菜单中选择“设置”选项，查看该设备的系统配置信息。



弹出的设置属性窗口包含“基础配置”、“命令行”、“组播”、“不”“UDP 收包工具”四个标签页，分别用于不同需求的配置。

步骤五 配置终端系统

选择“基础配置”标签页，在“主机名”文本框中输入主机名称。在“IPv4 配置”区域，单击“静态”选项按钮。在“IP 地址”文本框中输入 IP 地址。建议按照下图所示配置 IP 地址及子网掩码。配置完成后，单击窗口右下角的“应用”按钮。再单击“CLIENT1”窗口右上角“X”的关闭该窗口。



使用相同步骤配置 CLIENT2。建议将 CLIENT2 的 IP 地址配置为 192.168.1.2，子网掩码配置为 255.255.255.0。

完成基础配置后，两台终端系统可以成功建立端到端通信。

步骤六 启动终端系统设备

可以使用以下两种方法启动设备：

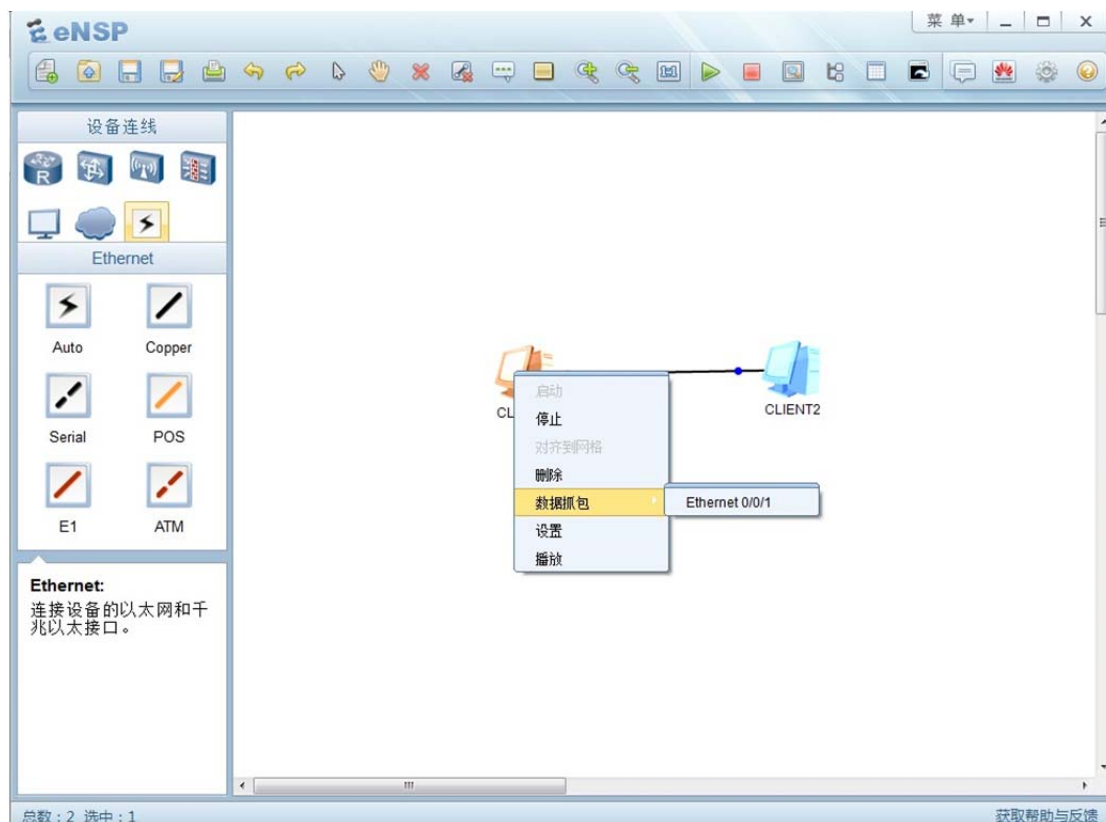
- 右击一台设备，在弹出的菜单中，选择“启动”选项，启动该设备。
- 拖动光标选中多台设备（如下图），通过右击显示菜单，选择“启动”选项，启动所有设备。

设备启动后，线缆上的红点将发为绿色，表示该连接为 Up 状态。

当网络拓扑中的设备发为可操作状态后，您可以监控物理链接中的接口状态与介质传输中的数据流。

步骤七 捕获接口报文

选中设备并右击，在显示的菜单中单击“数据抓包”选项后，会显示设备上可用于抓包的接口列表。从列表中选择需要被监控的接口。



接口选择完成后，Wireshark 抓包工具会自动激活，捕获选中接口所收取的所有报文。如需监控更多接口，重复上述步骤，选择不同接口即可，Wireshark 将会为每个接口激活不同实例来捕获数据包。

根据被监控设备的状态，Wireshark 可捕获选中接口上产生的所有流量，生成抓包结果。在本实例的端到端组网中，需要先通过配置来产生一些流量，再观察抓包结果。

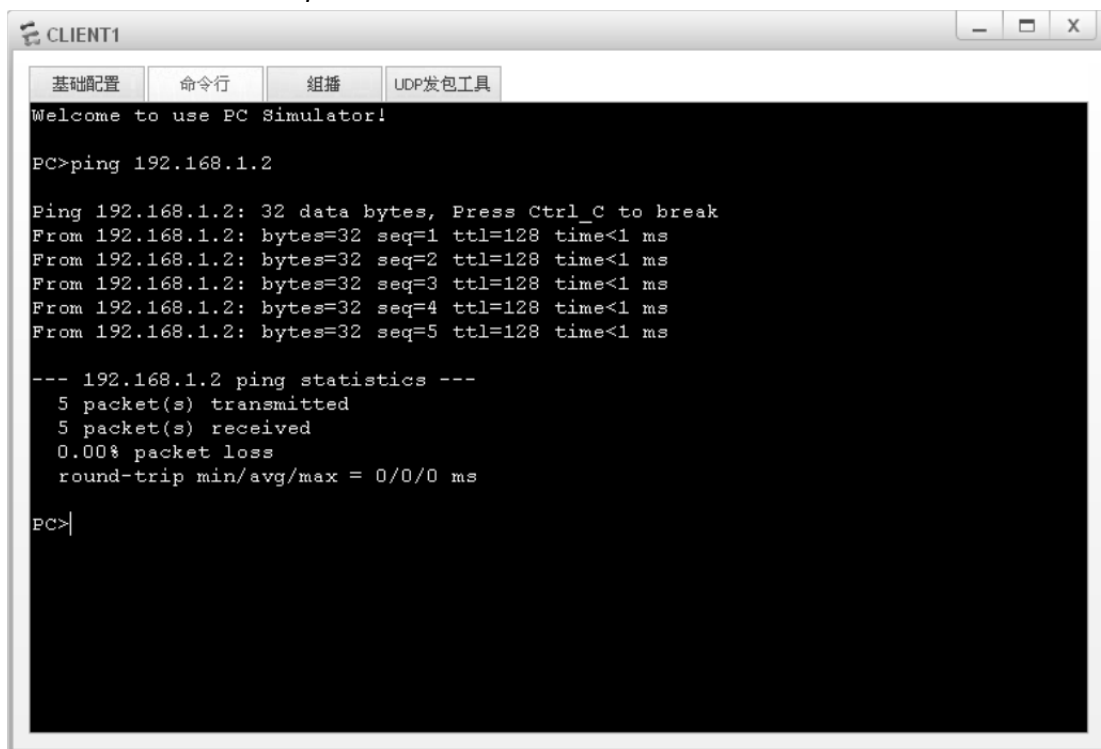
步骤八 生成接口流量

可以使用以下两种方法打开命令行界面：

双击设备图标，在弹出的窗口中选择“命令行”标签页。

右击设备图标，在弹出的属性菜单中，选择“设置”选项，然后在弹出的窗口中选择“命令行” 标签页。

产生流量最简单的方法是使用 `ping` 命令发送 ICMP 报文。在命令行界面输入 `ping <ip address>` 命令，其中 `<ip address>` 设置为对端设备的 IP 地址。



```
CLIENT1
基础配置  命令行  组播  UDP发包工具
Welcome to use PC Simulator!

PC>ping 192.168.1.2

Ping 192.168.1.2: 32 data bytes, Press Ctrl_C to break
From 192.168.1.2: bytes=32 seq=1 ttl=128 time<1 ms
From 192.168.1.2: bytes=32 seq=2 ttl=128 time<1 ms
From 192.168.1.2: bytes=32 seq=3 ttl=128 time<1 ms
From 192.168.1.2: bytes=32 seq=4 ttl=128 time<1 ms
From 192.168.1.2: bytes=32 seq=5 ttl=128 time<1 ms

--- 192.168.1.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 0/0/0 ms

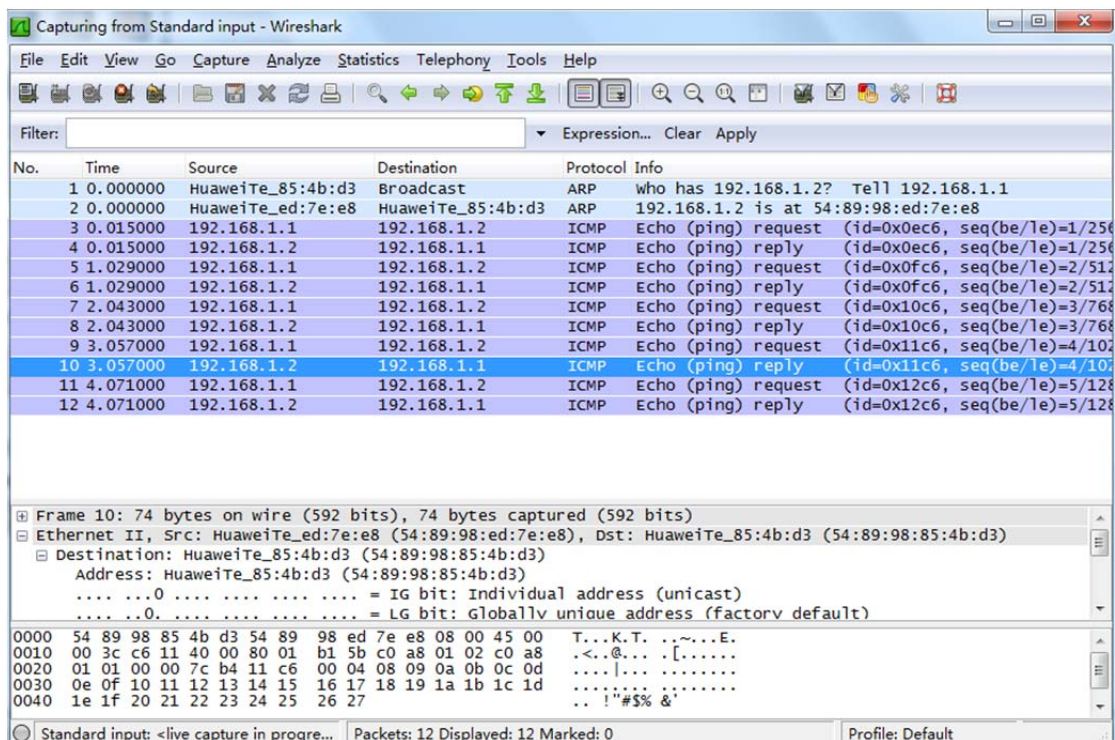
PC>|
```

生成的流量会在该界面的回显信息中显示，包含收送的报文和接收的报文。

生成流量之后，通过 Wireshark 捕获报文并生成抓包结果。您可以在抓包结果中看到 IP 网络的协议的工作过程，以及报文中所基于 OSI 参考模型各层的详细内容。

步骤九 观察捕获的报文

查看 Wireshark 所抓到的报文的结果。



Wireshark 程序包含许多针对所捕获报文的管理功能。其中一个比较常见的功能是过滤功能，可用来显示某种特定报文或协议的抓包结果。在菜单栏下面的“Filter”文本框里输入过滤条件，就可以使用该功能。最简单的过滤方法是在文本框中先输入协议名称（小写字母），再按回车键。在本示例中，Wireshark 抓取了 ICMP 和 ARP 两种协议的报文。在“Filter”文本框中输入 icmp 或 arp 再按回车键后，在回显中就将只显示 ICMP 或 ARP 报文的捕获结果。

Wireshark 界面包含三个面板，分别显示的是数据包列表、每个数据包的内容明细以及数据包对应的 16 进制的数据格式。报文内容明细对于理解协议报文格式十分重要，同时也显示了基于 OSI 参考模型的各层协议的详细信息。