Module 1 Establishing Basic Networks with eNSP

Lab 1-1 Building Basic IP Networks

Learning Objectives

As a result of this lab section, you should achieve the following tasks:

- Set up and navigate the eNSP simulator application.
- Establish a simple peer-to-peer network in eNSP.
- Perform capture of IP packets using Wireshark within eNSP.

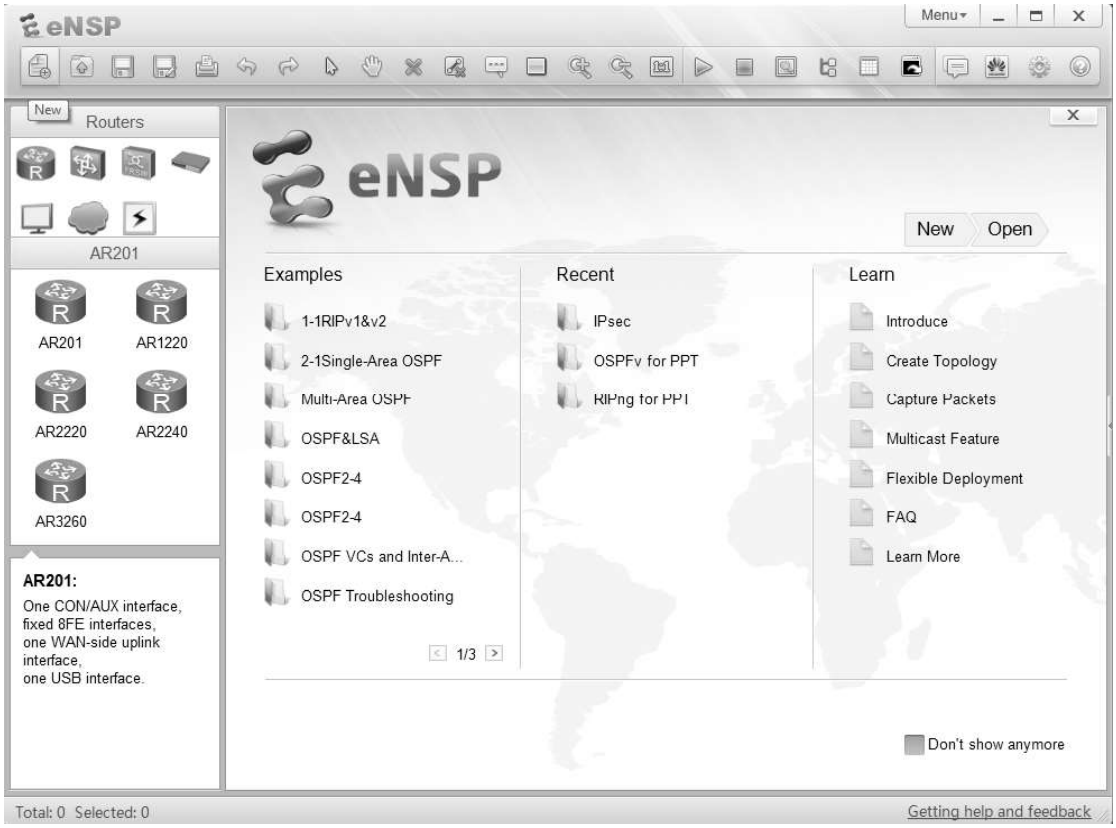
The fundamental network behavior can be understood through the application of packet capture tools to the network. The use of Huawei's simulator platform eNSP is capable of supporting both the implementation of technologies and the capture of packets within the network to provide a comprehensive knowledge of IP networks.

Tasks

Step 1 Initiate eNSP.

This step introduces how to start and navigate the eNSP simulator application for rapid development of TCP/IP knowledge and familiarity with network operation. If eNSP is not available, please inform the course instructor

After launching eNSP, the following application user interface will be presented. The left panel houses the icons that represent the various products and devices that are supported within eNSP, while the central panel provides lab examples for practice scenarios.

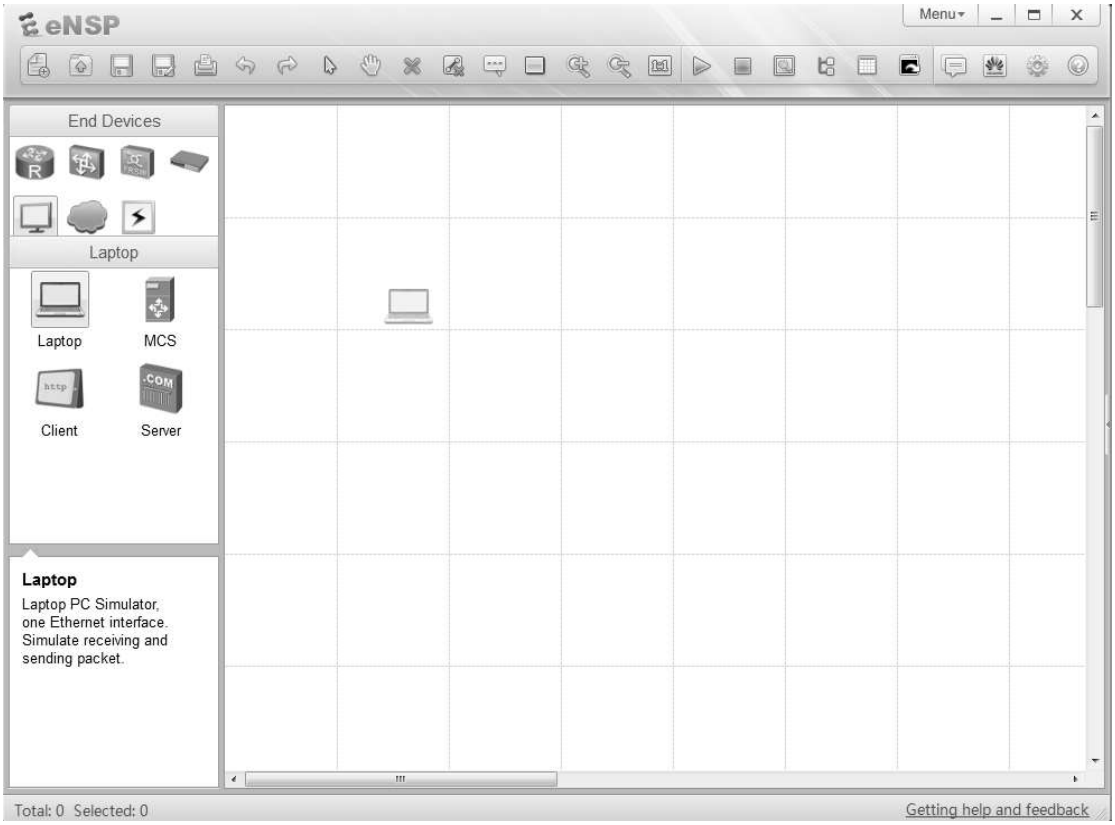


After launching eNSP, users should select the New operator in the top left corner of the application window to begin a new lab session.

The user will be presented with a canvas on which to establish a network topology for practice and analysis of network behavior. In this example a simple peer-to-peer network using two end systems is to be established.

Step 2 **Build a Topology.**

Select the End Devce icon in the top left panel to reveal a list of end devices that can be applied. Select the Laptop icon and drag it to the canvas, release the icon to place it on the canvas.

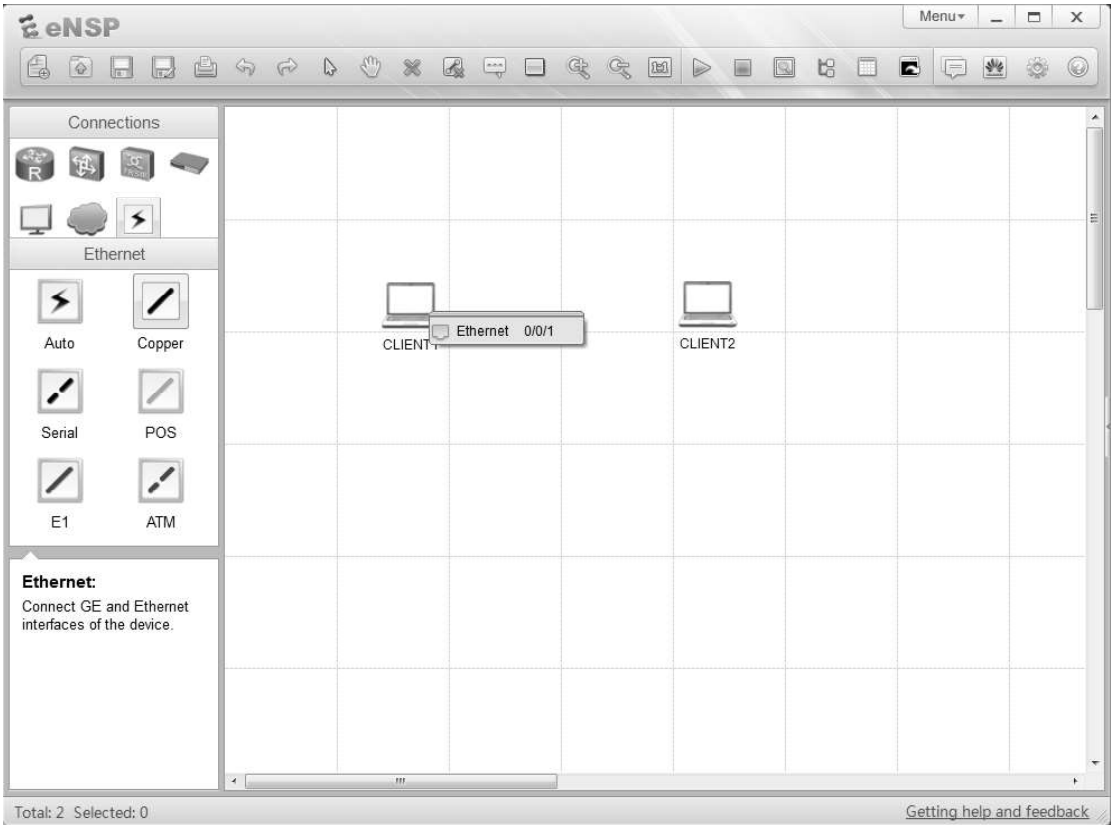


The same action should be taken to position a second laptop on the canvas for establishing the peer-to-peer network topology.

The devices on the canvas represent simulated end systems that can be used to emulate real world operations.

Step 3 **Establish a physical medium.**

Select the connections icon from the upper left panel to reveal a list of media that can be applied to the topology. Select the copper (Ethernet) medium from the list. Once the icon has been clicked, the cursor will represent a connector to show the current role of the cursor as a connector. Click on the client device to reveal a list of port interfaces supported by the simulated device. For the client click the option for Ethernet 0/0/1 to apply the connection.

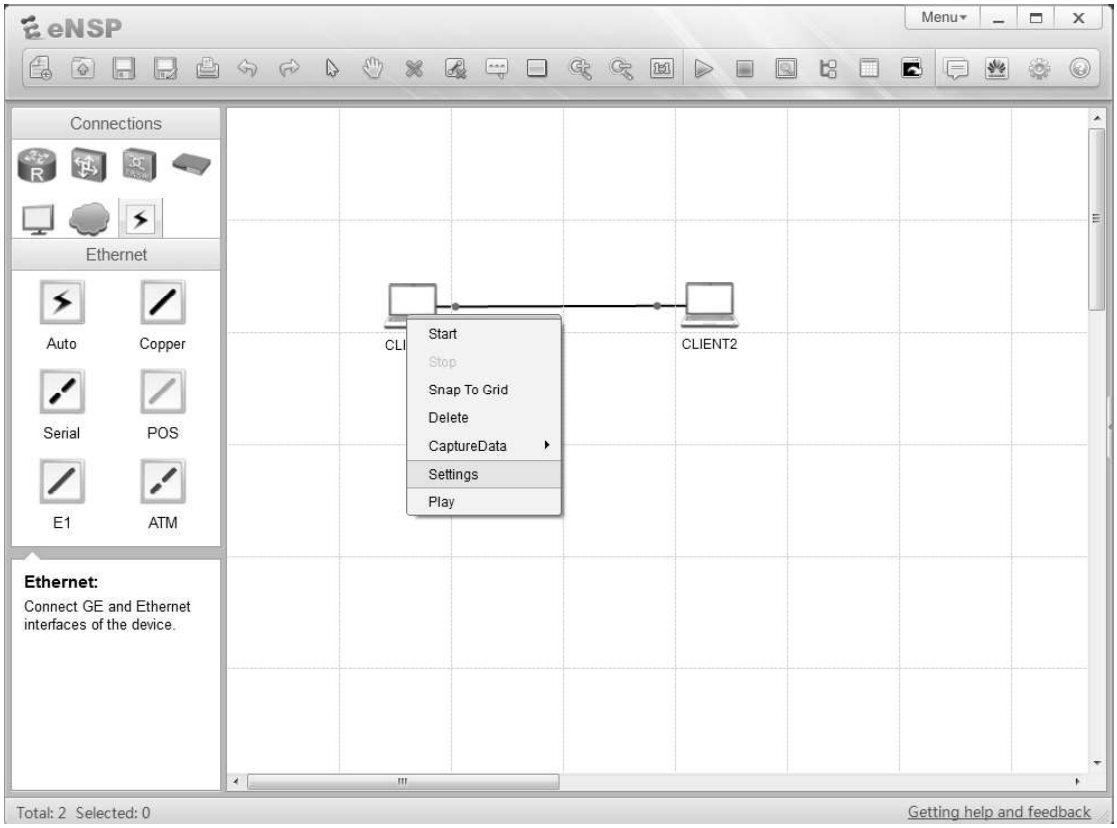


Once this has been achieved, click on the peering device to apply the opposite end of the medium to the end system. Again select the interface Ethernet 0/0/1 to establish the medium between the two devices and complete the construction of a peer-to-peer topology.

The establishment of a point-to-point network reveals a connection with two red dots on the medium that represent the current state of the interfaces to which the medium connects as down.

Step 4 **Access the end system settings.**

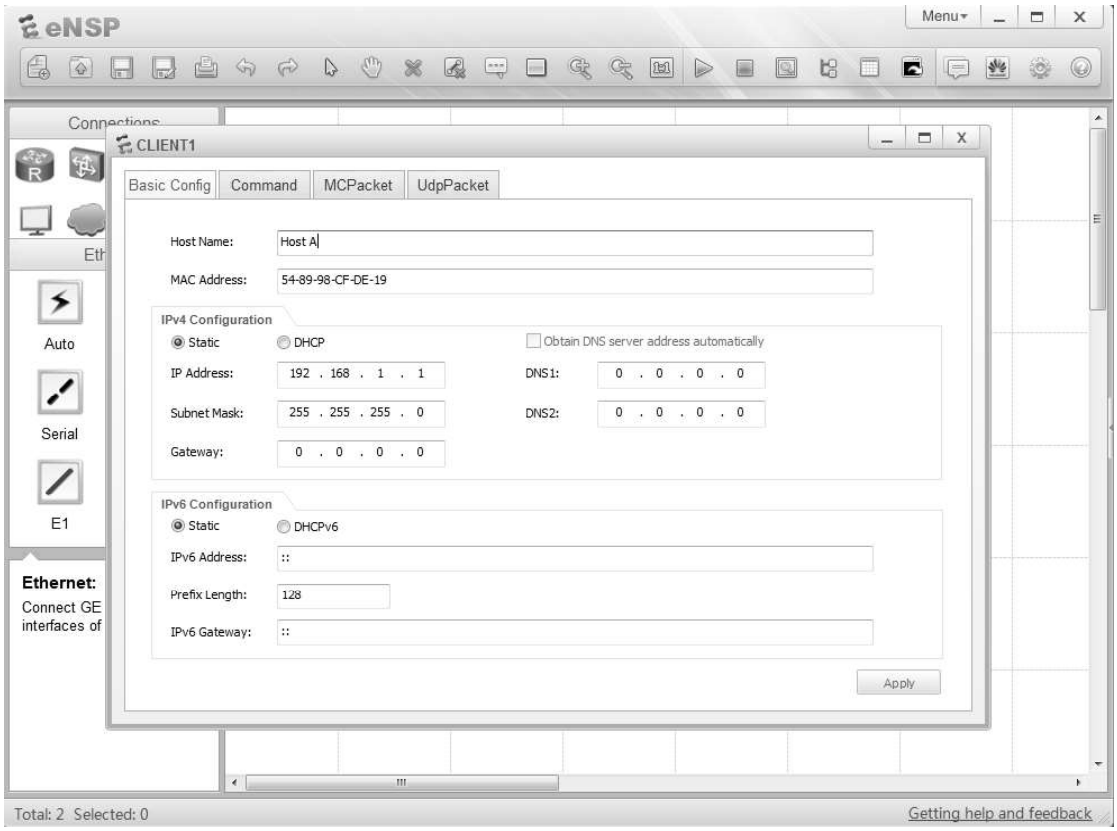
Select the end system and use the right click option to display a properties menu. The settings option should be selected in order to display the current system settings for the end system devices.



The settings option in the properties window reveals a set of four tabs for establishment of basic configuration, the device command line interface, multicast traffic generator configuration, and UDP packet generator configuration.

Step 5 **Configure the end system.**

Ensure the Basic Config tab is selected and enter a host name in the Host Name field window. Ensure the IPv4 configuration is currently set to static and configure an IP address in the IP address window. It is recommended that the address (together with the subnet mask) be configured as shown in the below example. Once this has been configured, click the Apply button in the bottom left corner of the window before closing with the x in the top left corner of the CLIENT 1 window.

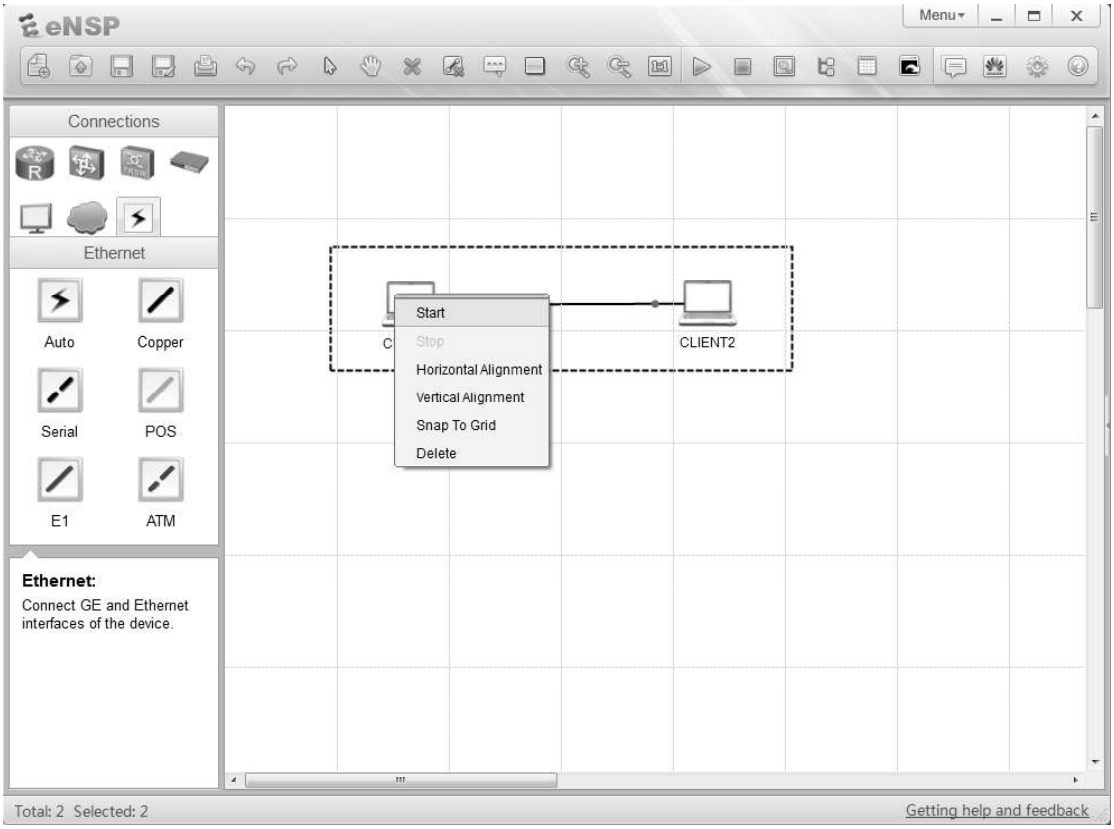


The same process is required for CLIENT2. It is recommended that initially the IP address 192.168.1.2 be configured, with a subnet mask of 255.255.255.0.

The basic configuration enables peer-to-peer communication to be supported between the two end systems.

Step 6 **Initiate the end system devices.**

The devices can be activated using one of two methods. The first involves using the right click option to open the properties menu and select start for the individual icons. The alternative involves dragging the cursor over the icons (as shown) to highlight multiple devices and using the right click settings option start multiple devices simultaneously.

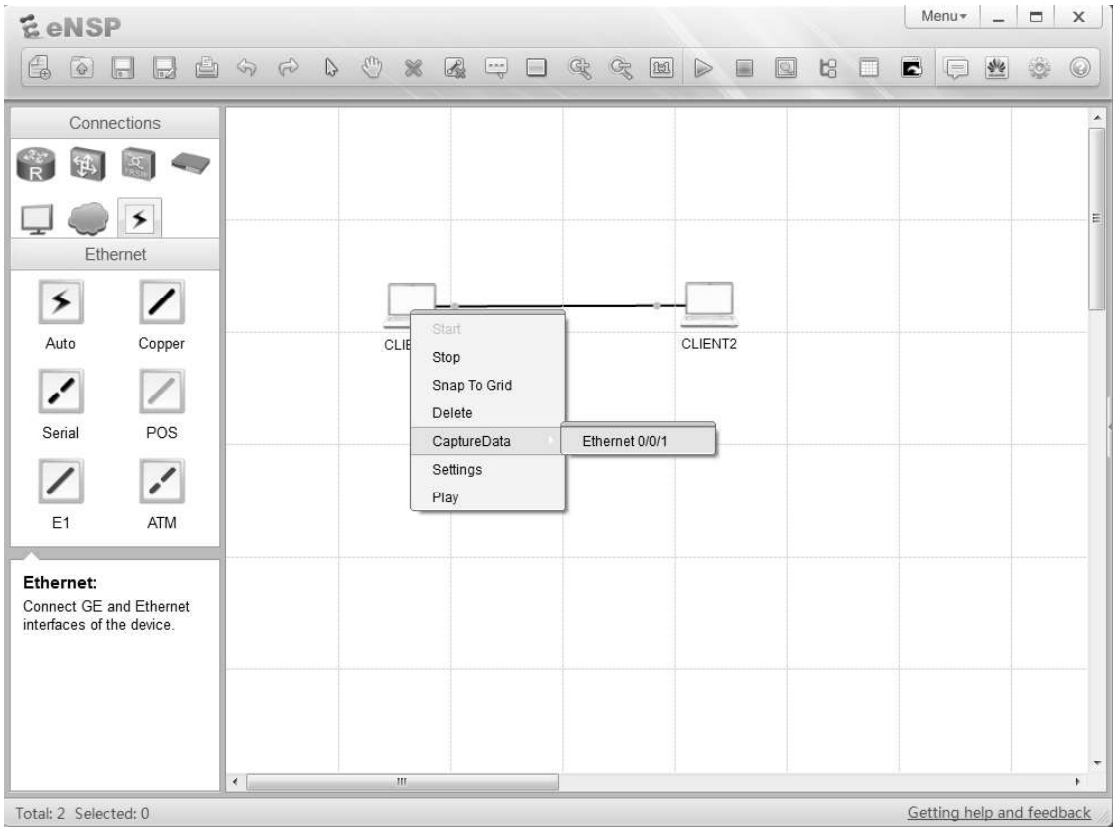


Once the devices are online and active, it is common to notice a change in the status of the connectors through a switch in the colour of the red dot on the medium to green, highlighting that the status of the connectors is now up.

Once the devices within the network topology are operational, it is possible to begin to monitor the flow of traffic that is carried over the medium and the interfaces via which the devices have established a physical peering.

Step 7 **Implement the capture of packets on an interface.**

Select the device to for whose interface is to be monitored and use the right click option to display the settings menu. Highlight the capture data option to reveal a list of interfaces that belong to the device and are available for observation by the packet capture tool. Select the interface from the list that is to be monitored.



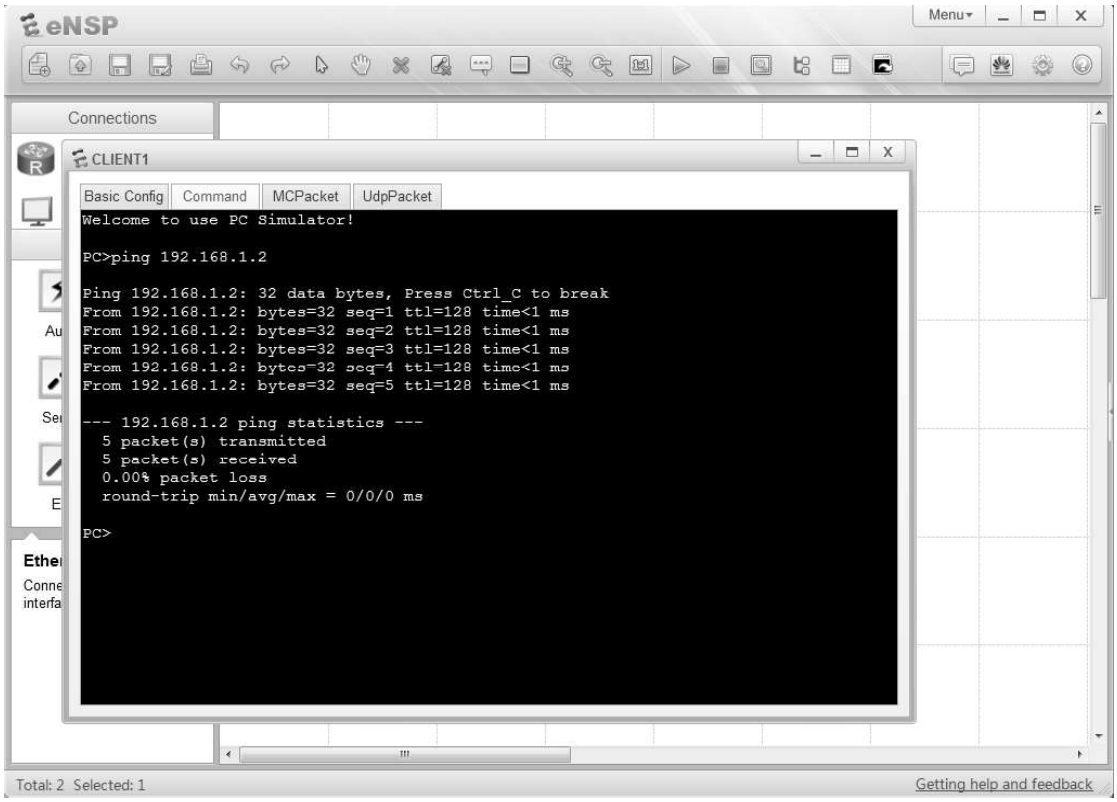
The selection of an interface will result in the activation of the Wireshark packet capture tool for the selected interface. If additional interfaces are to be monitored, separate instances of the same packet capture tool will be activated.

Depending on the devices being monitored, the packet capture tool may or may not begin to generate packet capture results for all traffic that passes through the selected interface. In the case of the peer-to-peer relationship, it will be necessary to generate some traffic.

Step 8 **Generate traffic on the interface.**

Open the command window on the client by either double clicking the client icon and selecting the Command tab, or alternatively use the right click option to enter the properties menu and select settings from which point the Command tab can be selected.

The most basic means for generating traffic is through the ping command. This can be achieved by entering ping <ip address> where the IP address refers to the address of the peer.

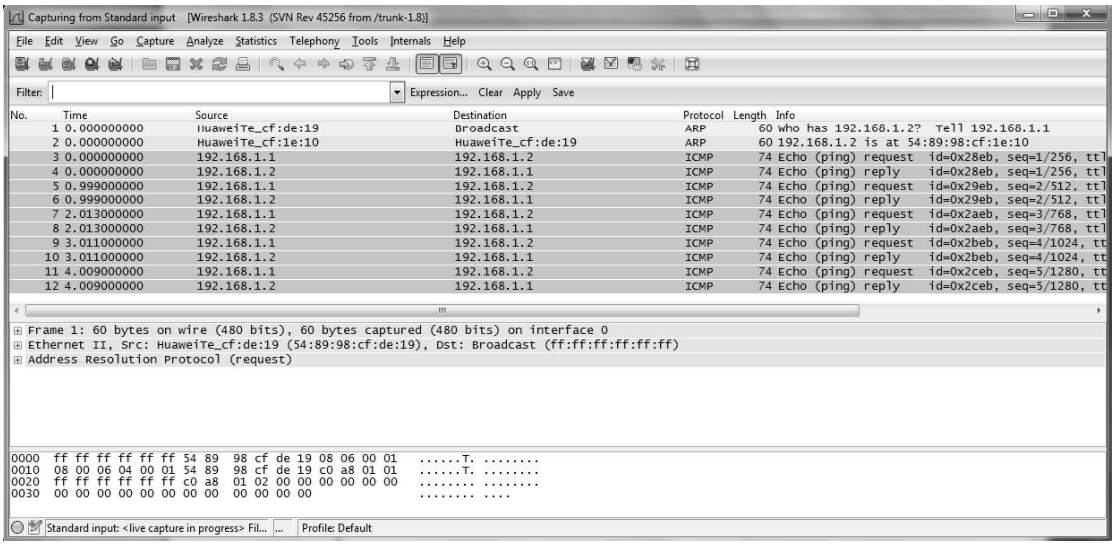


The generation of traffic will be confirmed by the resulting output in which case the number of packets transmitted are shown to also be received.

Following the generation of traffic, the resulting traffic flow shall be captured by the packet capture tool and can be used for observation of the behavior of protocols within the IP network along with details of the various layers as referenced in the OSI reference model.

Step 9 **Observe the captured traffic flow.**

An instance of the Wireshark packet capture tool should currently be active following the action to capture data on the client interface. Maximize the active window to observe the results of the packet capture process.



The Wireshark application contains many functions for management of the packet capture process. One of the more common functions includes the filter function to isolate the packet capture display to a select group of packets or protocols. This can be achieved using the filter field below the menu bar. The simplest filter method involves entering the protocol name (in lower case) and pressing Enter. In the given example packets for two protocols have been captured, entering either *icmp*, or *arp* into the filter window will result in only the protocol entered in the filter field being displayed in the output.

The packet capture tool consists of three panels, to show the list of packets, a breakdown of the content of each packet and finally display the equivalent data format of the packet. The breakdown is invaluable for understanding the format of protocol packets and displays the details for protocols as referenced at each layer of the OSI reference model.