Lab - Install Wireshark

Objectives

Download and Install Wireshark

Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC, or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting. This lab provides instructions for downloading and installing Wireshark.

Required Resources

- 1 PC (Windows with internet access)

Instructions

Wireshark has become the industry standard packet-sniffer program used by network engineers. This open source software is available for many different operating systems, including Windows, Mac, and Linux. In this lab, you will download and install the Wireshark software program on your PC.

Note: Before downloading Wireshark, check with your instructor about the software download policy of your academy.

Step 1: Download Wireshark.

a. Wireshark can be downloaded from www.wireshark.org.

b. Choose the software version you need based on your PC's architecture and operating system. For instance, if you have a 64-bit PC running Windows, choose **Windows Installer (64-bit)**.

After making a selection, the download should start. The location of the downloaded file depends on the browser and operating system that you use. For Windows users, the default location is the **Downloads** folder.

Step 2: Install Wireshark.

a. The downloaded file is named **Wireshark-win64-x.x.x.exe**, where **x** represents the version number if you downloaded the 64bit version. Double-click the file to start the installation process.

Respond to any security messages that may display on your screen. If you already have a copy of Wireshark on your PC, you will be prompted to uninstall the old version before installing the new version. It is recommended that you remove the old version of Wireshark prior to installing another version. Click **Yes** to uninstall the previous version of Wireshark.

b. If this is your first time to install Wireshark, or after you have completed the uninstall process, you will navigate to the Wireshark Setup wizard. Click **Next**.

c. Continue advancing through the installation process. Click **I Agree** when the License Agreement window displays.

d. Keep the default settings on the Choose Components window and click **Next**.

e. Choose your desired shortcut options and click **Next**.

f. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location. Click **Next** to continue.

g. To capture live network data, Npcap must be installed on your PC. If Npcap is already installed on your PC, the Install check box will be unchecked. If your installed version of Npcap is older than the version that comes with Wireshark, it is recommended that you allow the newer version to be installed by clicking the **Install Npcap x.x.x** (version number) check box. Click **Next** to continue.

h. **Do NOT** install USBPcap for normal traffic capture. **Do NOT select the checkbox to install USBPcap**. USBPcap is experimental, and it could cause USB problems on your PC. Click **Install** to continue.

i. Wireshark starts installing its files and displays with the status of the installation.

j. In a separate window, accept the license agreement in the Npcap Setup Wizard if installing Npcap. Click **I Agree** to continue. Click **Install** to install Npcap. Click **Next** to finish the Npcap installation and click **Finish** to exit the Npcap installation.

k. Click **Next** when the Wireshark installation is complete.

l. Click **Finish** to complete the Wireshark install process. Reboot the computer if necessary.