

CSE 4616: [Wireless Networks Lab]

Lab # 01

Objectives

- Installing GNS3 client on windows
- Adding, installing and importing Cisco IOS in GNS3
- Introduction to Wireshark

How to install GNS3 Step by Step

What is GNS3?

GNS3 is a network simulator software. It allows us to simulate Cisco devices. As a network administrator, you can use GNS3 as a presentation tool to demonstrate your network or as a testing tool to test any new feature before implementing that feature on the live network.

GNS3 v/s Packet Tracer

Cisco also offers similar software for educational purposes. This software is known as Packet Tracer. The main differences between Packet Trace and GNS3 are the following.

Packet Tracer is mainly developed for educational purposes. It uses a simplified version of IOS. IOS is the operating system of the Cisco device. A simplified version of IOS includes only commands and features that are required to run the device or are tested in exams. You can't add or remove devices in Packet Tracer. You have to use devices as they are available on Packet Tracer. However, if the device supports, you can do a little customization such as adding and removing modules and slots.

GNS3 is mainly developed for network testing and troubleshooting purposes. It uses an actual version of IOS. Since it uses the original version of IOS, it supports all commands and features of the IOS. You can also add or remove devices in GNS3.

Packet tracer is easier to learn and use but it provides limited commands and functions. GNS3 is harder to learn and use but it provides almost all commands and functions. If you are preparing

for any entry-level Cisco exam, you should use Packet Tracer. If you are a network administrator or you are preparing for an intermediate or advanced level exam, you should use GNS3.

Installing GNS3 on Windows

Download the latest version of GNS3 from the following webpage

<https://www.gns3.com/software/download>

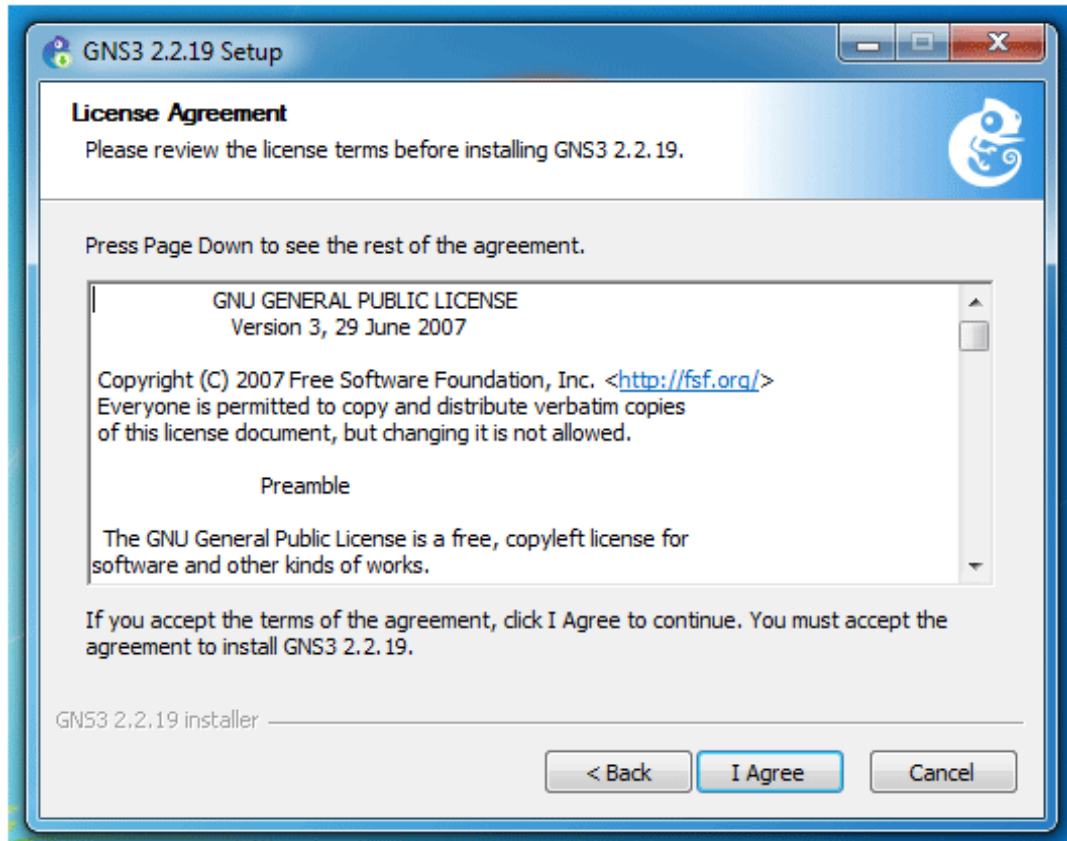
Open the folder that contains the downloaded-file and double-click the installation file.

The first screen of the wizard shows a welcome message and a suggestion to close other applications before starting the installation of GNS3. It's only a suggestion, not a requirement. You can install GNS3 while other applications are running, but in this case, you must have to restart the system before you can use it.

Click the Next button to start the installation.

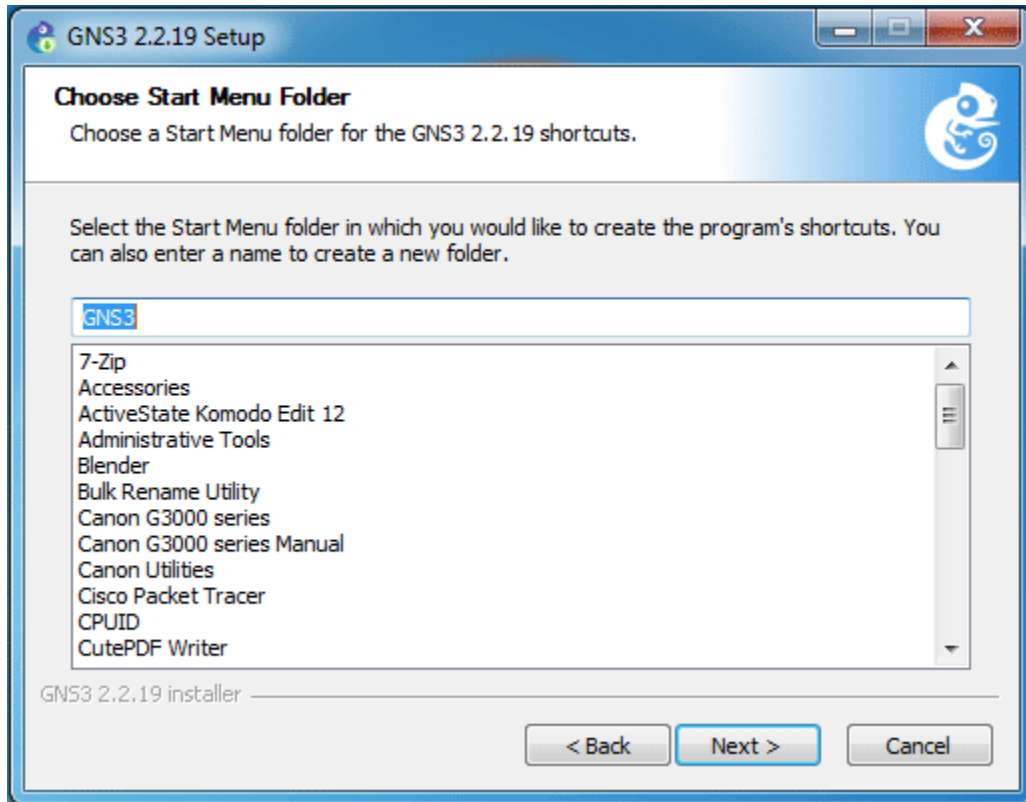


The next screen shows the license agreement. Click the I Agree option to accept the license agreement.



The next screen allows us to customize the Start Menu Folder name. By default, the wizard uses GNS3 as the start menu folder name. If you want to use something else, set the new name. If you want to use the default name, no action is required here.

Make your choice and click the Next button.



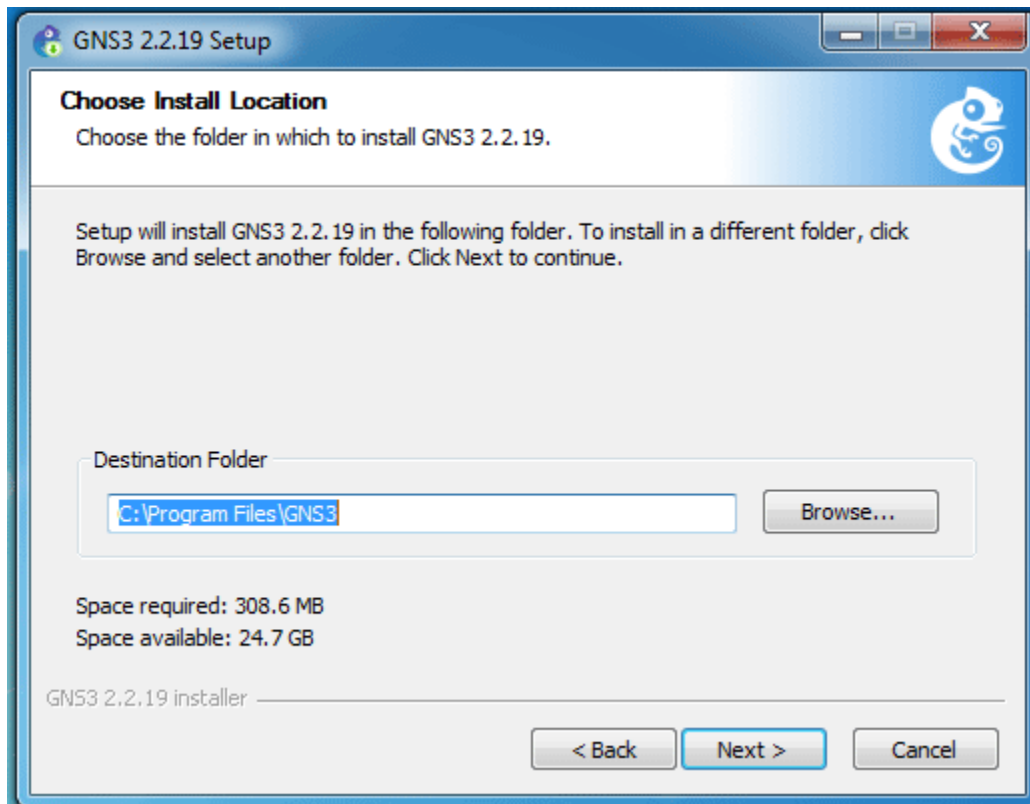
GNS3 installation package contains several additional tools and components. The following table provides a brief description of these tools

Component	Type	Description
WinPCAP	Required	This component connects GNS3 to the host computer's network. It allows the nodes that are simulated on GNS3 to communicate with nodes that available on the host computer's network.
Npcap	Optional	This component is the replacement of WinPCAP. Based on the version of Windows, select either Npcap or WinPCAP. If you are installing GNS3 on Windows 10, select Npcap. If you are installing GNS3 on a previous version of Windows, select WinPCAP.
Wireshark	Recommended	This component is used to capture and view data packets exchanged between nodes.
Dynamips	Required	This component is used to run GNS3 from the host system.
QEMU 3.1.0 and 0.11.0	Optional	This component is used to create a virtual computer and to run GNS3 from that virtual computer. If you want to run GNS3 from a virtual computer, you should use GNS3VM instead of this component.
VPCS	Recommended	This component is used to create a lightweight virtual PC that supports basic testing and troubleshooting commands such as ping and traceroute.
cpulimit	Optional	This component is an add-on to the QEMU component. It is used to limit QEMU using 100% CPU of the host computer.
GNS3	Required	This is the core component of GNS3. It installs and runs GNS3 on the computer.
TightVNC	Recommended	This is a VNC client. It is used to connect to appliance graphical user interfaces.
Solar-Putty	Recommended	This is the default console application of GNS3.
Virt-viewer	Optional	This is an add-on component of QEMU. It provides an alternative display of QEMU desktop.
HAXM	Optional	This component is used for hardware acceleration. This component is available only if the host system uses Intel CPU.

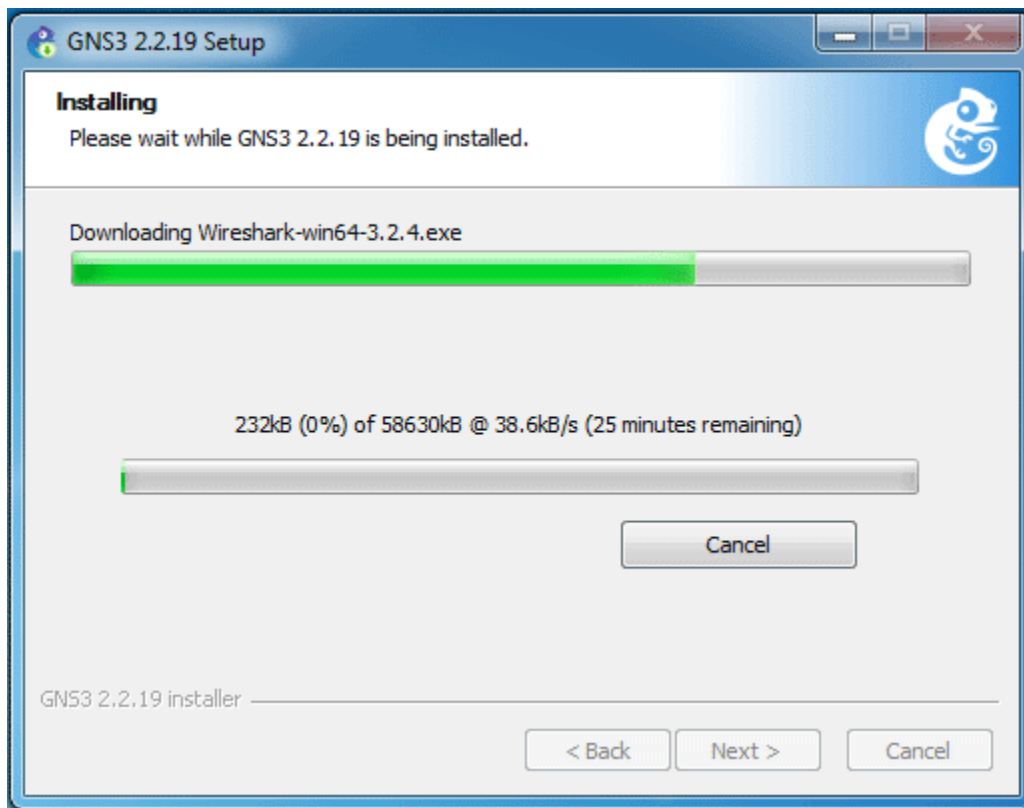
Keep the default setup and click next.

The next screen allows us to customize the installation folder location. By default, wizard installs GNS3 in Windows partition\Program Files\GNS3 folder. If you want to install GNS3 in another folder, update the folder location.

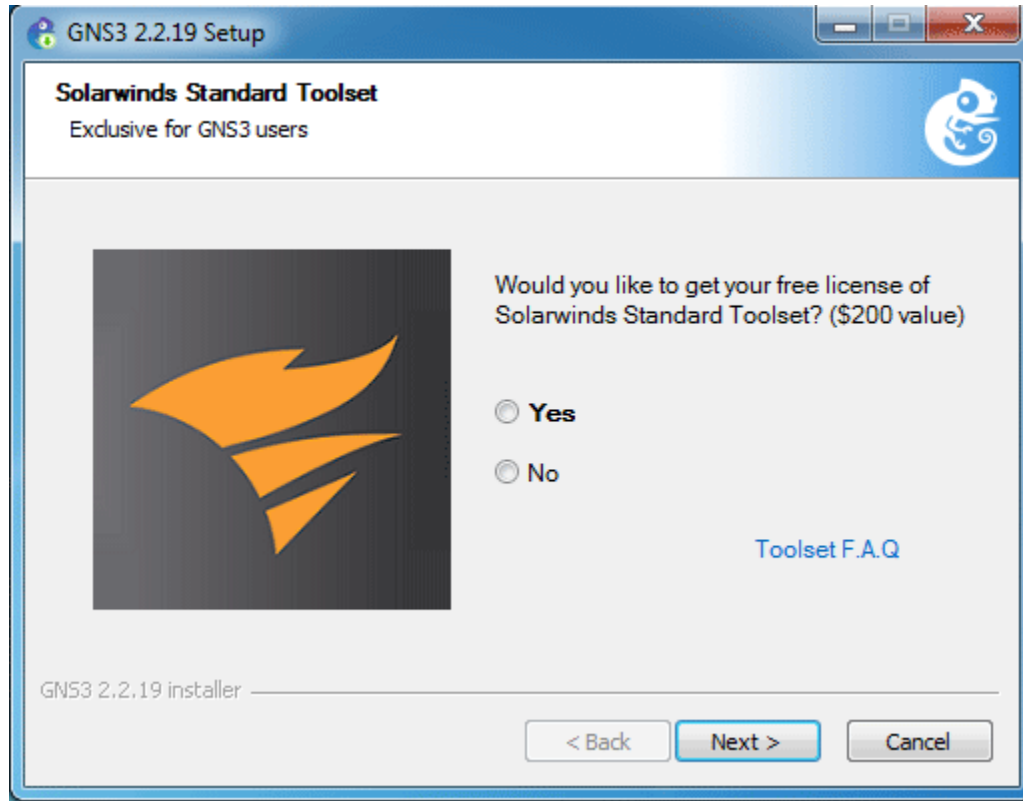
Keep the default location or select the appropriate folder location and click the Install button to start the installation



The installation process installs core GNS3 and all selected components. If you have selected any third-party component, the installation process downloads and installs that component as well.



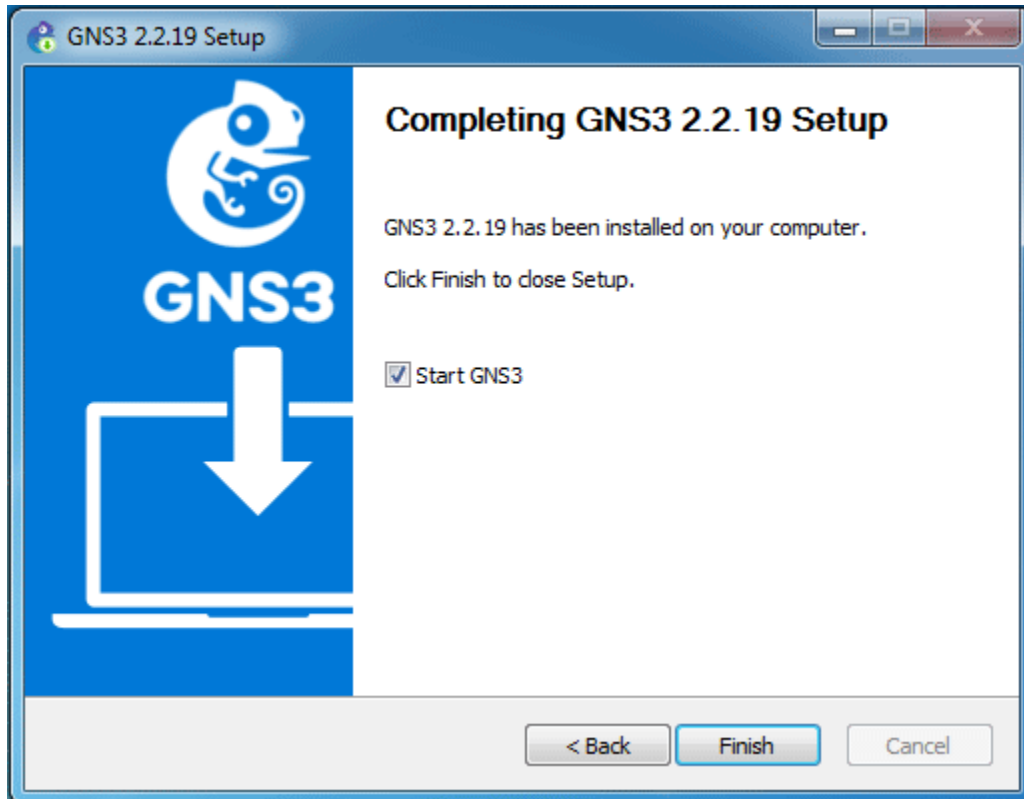
GNS projected is supported by Solarwinds. Solarwinds offers a free standard toolset to GNS3 users. This toolset contains a lot of network testing and troubleshooting tools. If you want to install this toolset, select the **Yes** option otherwise select the **No** option. Select your option, and click the **Next** button.



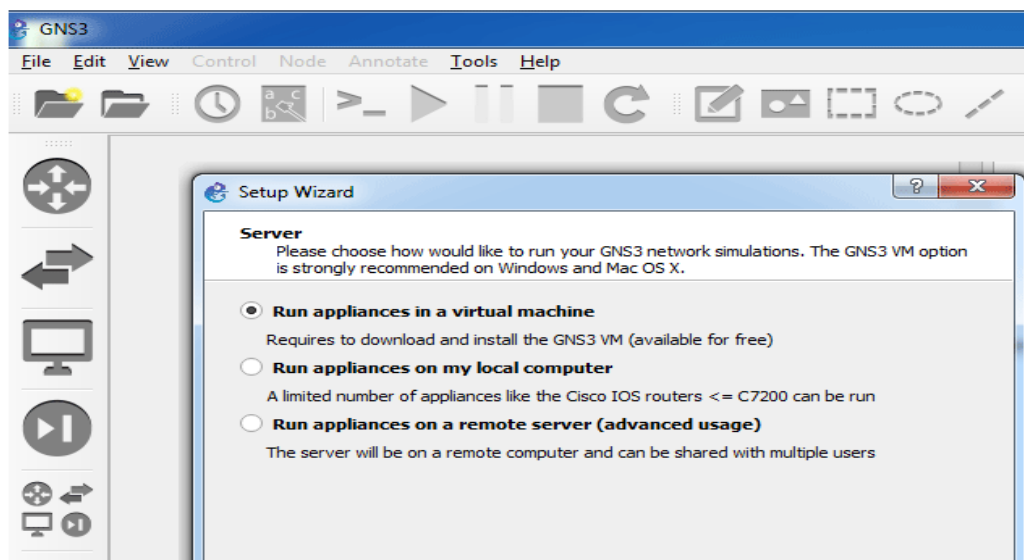
Select No here.

On the last screen of the installation process, the wizard offers an option to start GNS3 just after the installation. By default, this option is selected. If you don't want to run GNS3 just after the installation, uncheck this option.

Click the Finish button to close the installation wizard.



When GNS3 starts the first time, it presents the Setup wizard. This wizard allows us to run GNS3 in different modes.



How to add, install or import IOS in GNS3

GNS3 is a network simulator software. It is used to simulate routers, switches, and other networking devices. Cisco uses proprietary software for its routers and switches. This software is known as Cisco IOS. GNS3 can run Cisco IOS. Since Cisco IOS is protected by copyright laws, GNS3 does not include any Cisco IOS in the default installation. It only provides a platform to use Cisco IOS but it does not provide any Cisco IOS itself. It means, to use any Cisco device in GNS3, you have to install that device's IOS first.

Downloading Cisco IOS

To install a Cisco device in GNS3, you have to obtain its IOS file. There are several sources from where you can obtain a Cisco IOS file. You can get it from a Cisco device or download it from Cisco's official site (it requires a valid Cisco account and license agreement) or download it from educational sites.

You may check the following site.

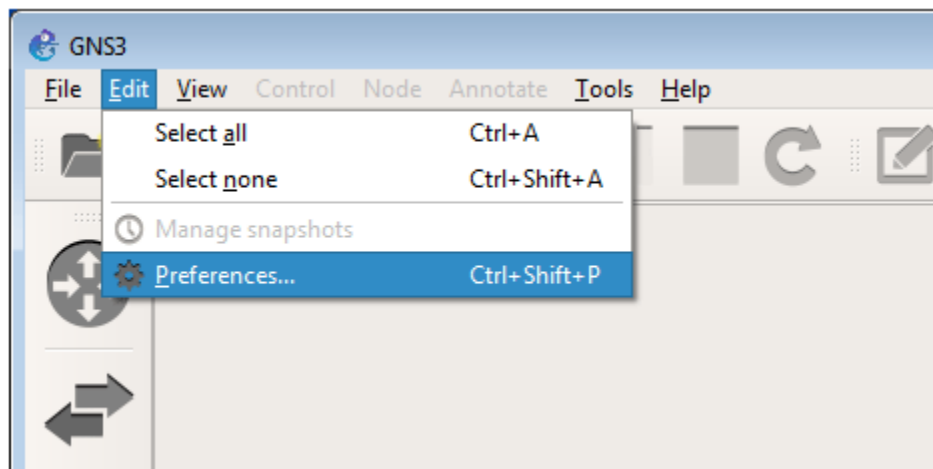
<http://tfr.org/cisco/>

It contains the largest collection of Cisco IOS files.

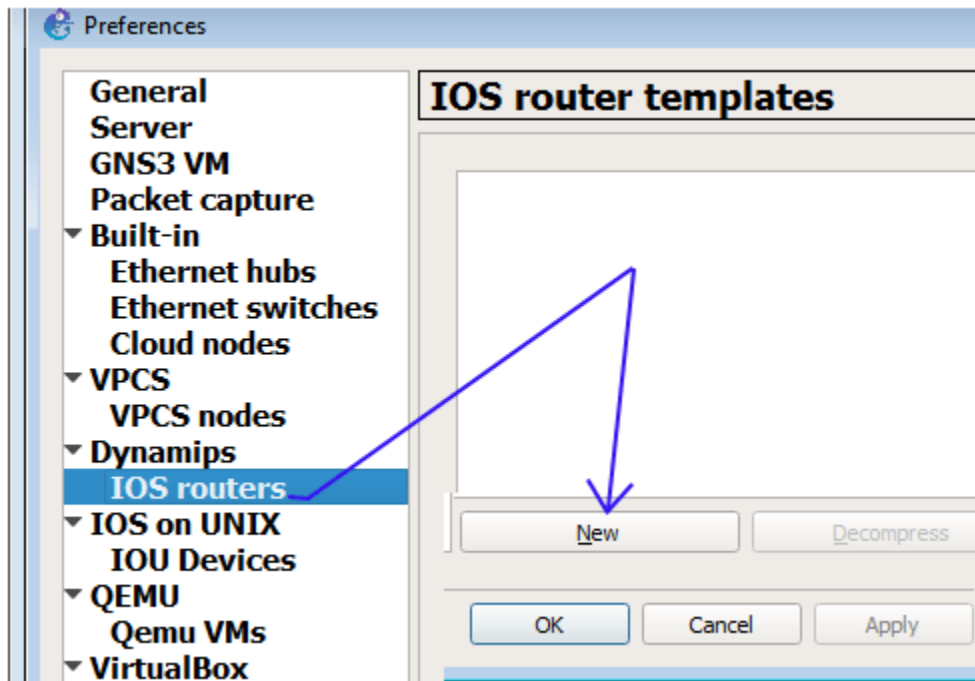
Installing and importing Cisco IOS in GNS3

Download or obtain the IOS file that you want to use on GNS3.

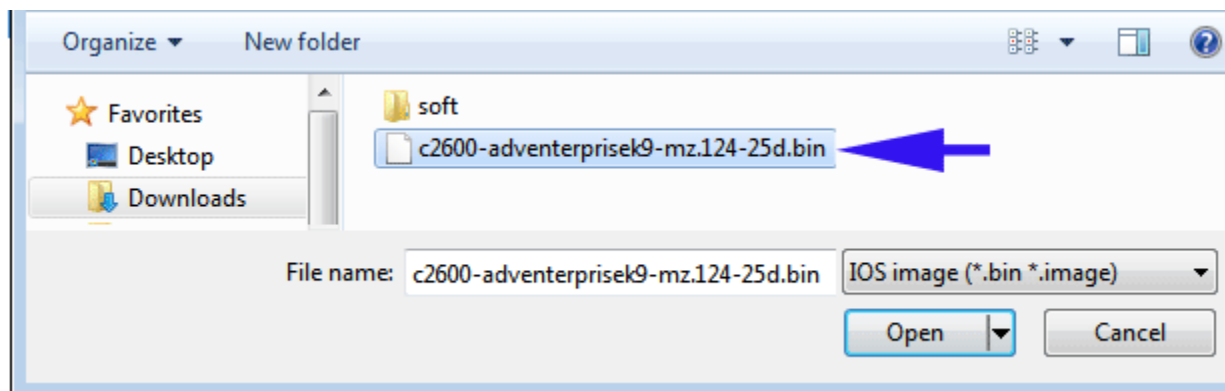
Open GNS3, and click the **Edit** file menu, and from the sub-menu, click the **Preferences** option.



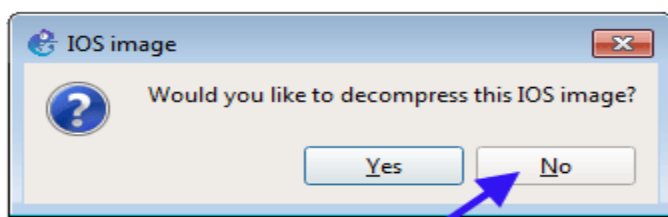
On the opened window, navigate to the **Dynamips -> IOS routers** option in the left pane and click the **New** button in the right pane.



Click the Browse button and select the downloaded IOS image file.



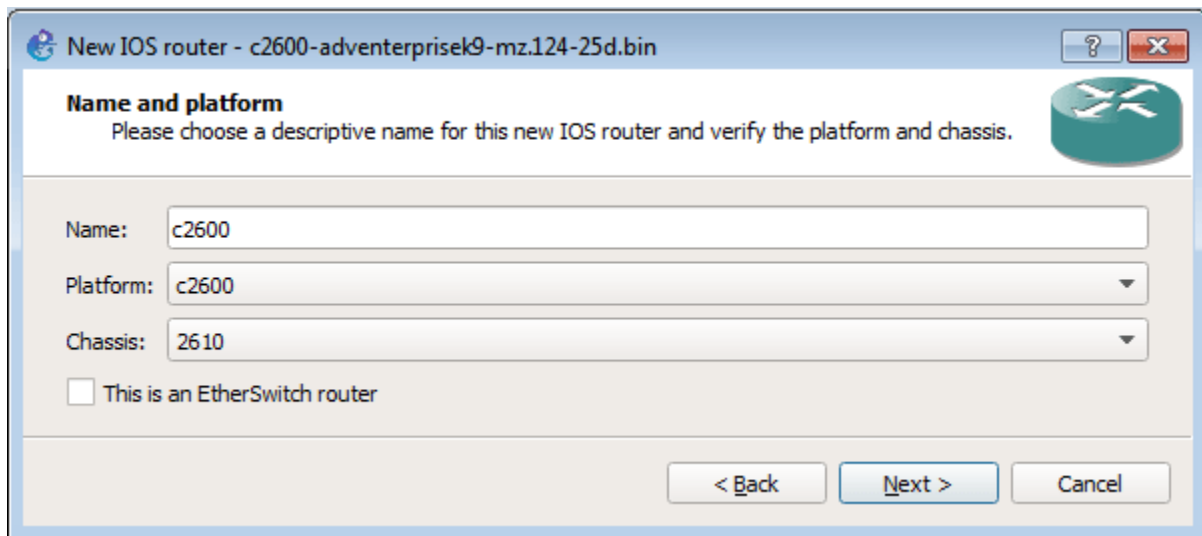
By default, IOS files are compressed. GNS3 supports both compressed and decompressed formats. Compressed files not only consume less space but also easier to manage. Unless you have a particular reason to keep IOS files in their original form, **click the No option to keep them in compressed format.**



On the next step, the wizard extracts the hardware information (platform and chassis number) from the selected IOS file and lists the information on the next screen along with an automatically populated device name.

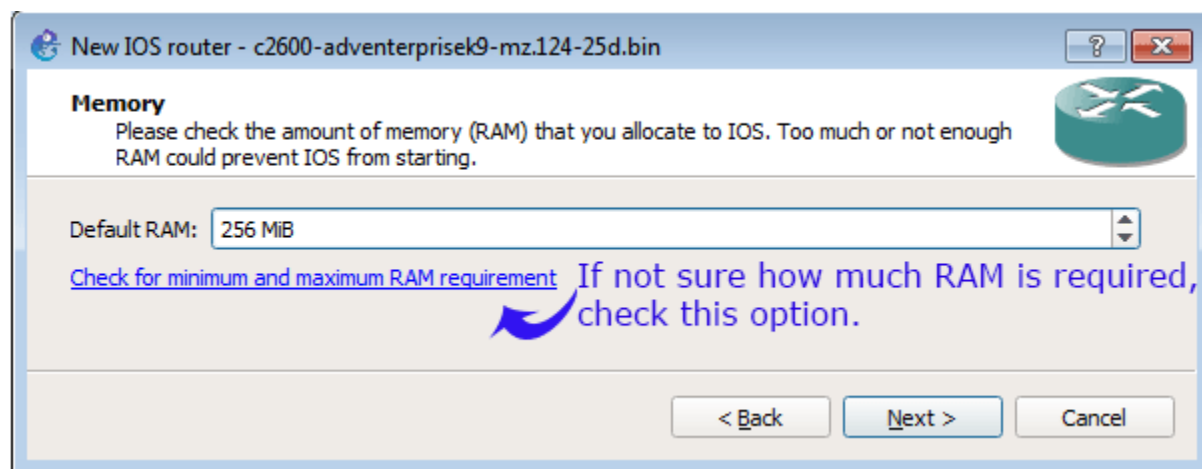
If the extracted information is incorrect, select the correct platform and chassis number from the drop-down. If required, you may adjust the device name as well.

Verify or adjust the information and Click the Next button to continue.



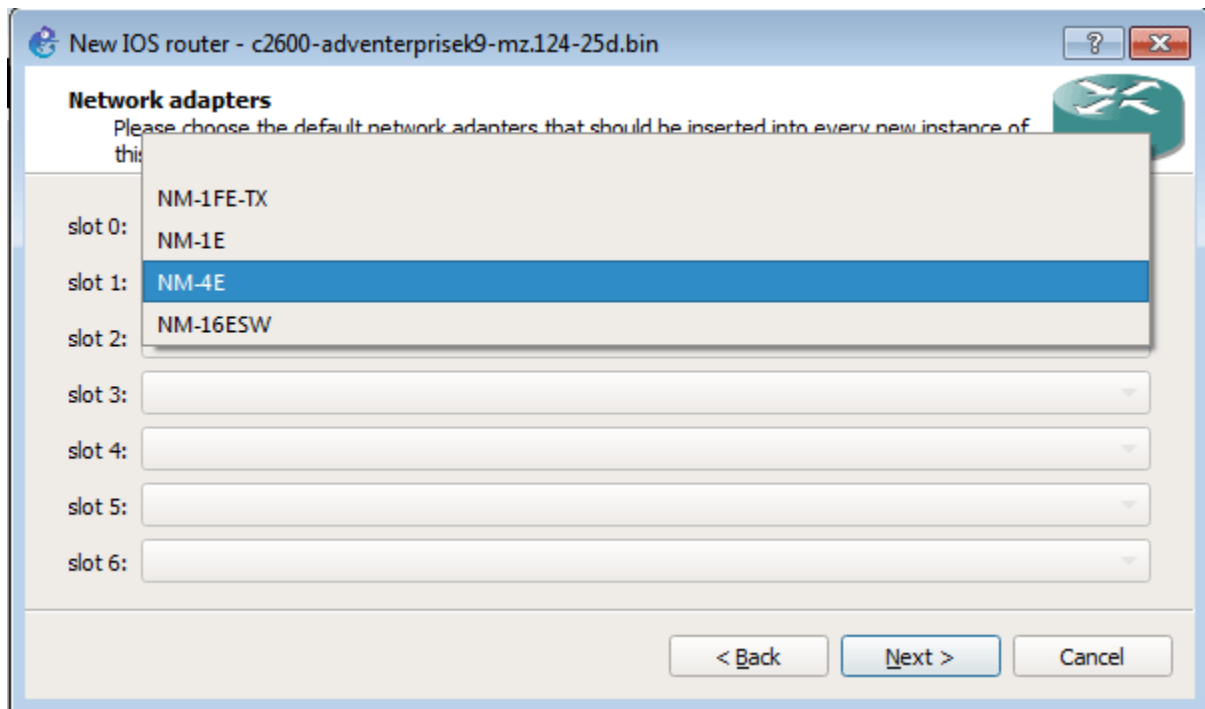
The screenshot shows a window titled "New IOS router - c2600-adventerprise9-mz.124-25d.bin". The main heading is "Name and platform" with a sub-instruction: "Please choose a descriptive name for this new IOS router and verify the platform and chassis." There is a Cisco router icon in the top right. The form contains three input fields: "Name:" with the value "c2600", "Platform:" with a dropdown menu showing "c2600", and "Chassis:" with a dropdown menu showing "2610". Below these is a checkbox labeled "This is an EtherSwitch router" which is currently unchecked. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

The next screen allows us to set the RAM size for this device. By default, the wizard automatically allocates the minimum recommended memory (RAM) for the device. But if required, you can adjust it.



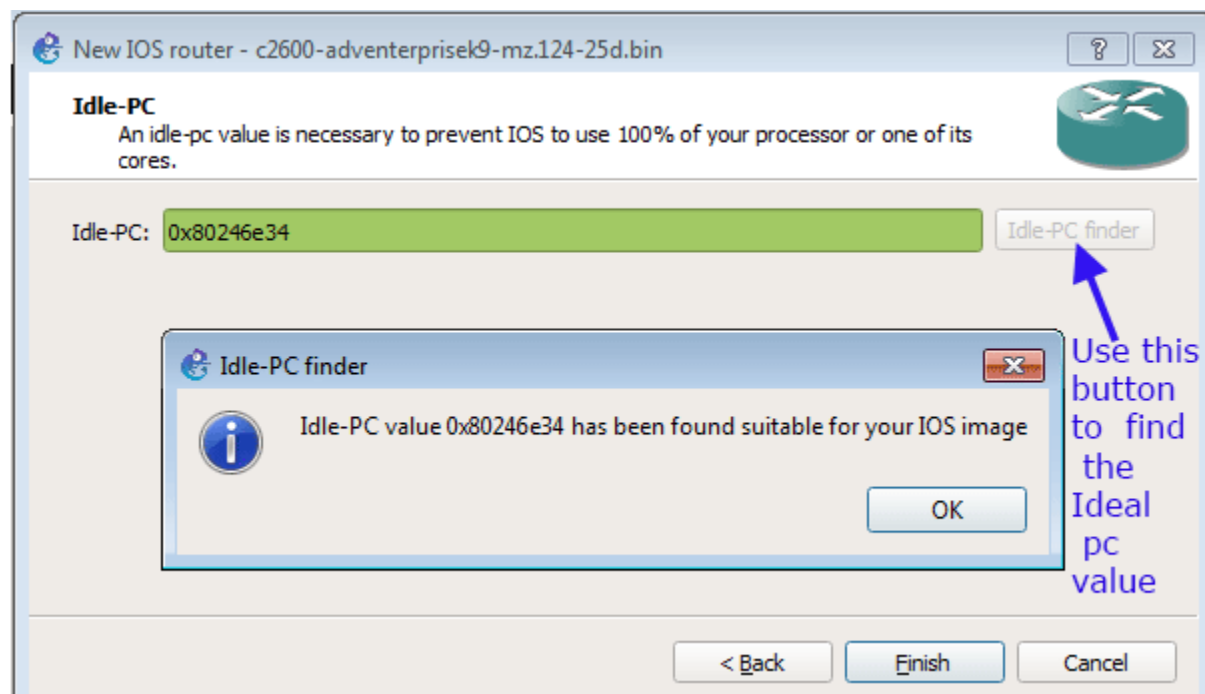
The screenshot shows a window titled "New IOS router - c2600-adventerprise9-mz.124-25d.bin". The main heading is "Memory" with a sub-instruction: "Please check the amount of memory (RAM) that you allocate to IOS. Too much or not enough RAM could prevent IOS from starting." There is a Cisco router icon in the top right. The form contains a "Default RAM:" label followed by a dropdown menu showing "256 MiB". Below this is a blue hyperlink that reads "Check for minimum and maximum RAM requirement". A blue curved arrow points from this link to the text "If not sure how much RAM is required, check this option." At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

If the selected IOS belongs to a modular device, the next screen allows us to install the interfaces in available slots.

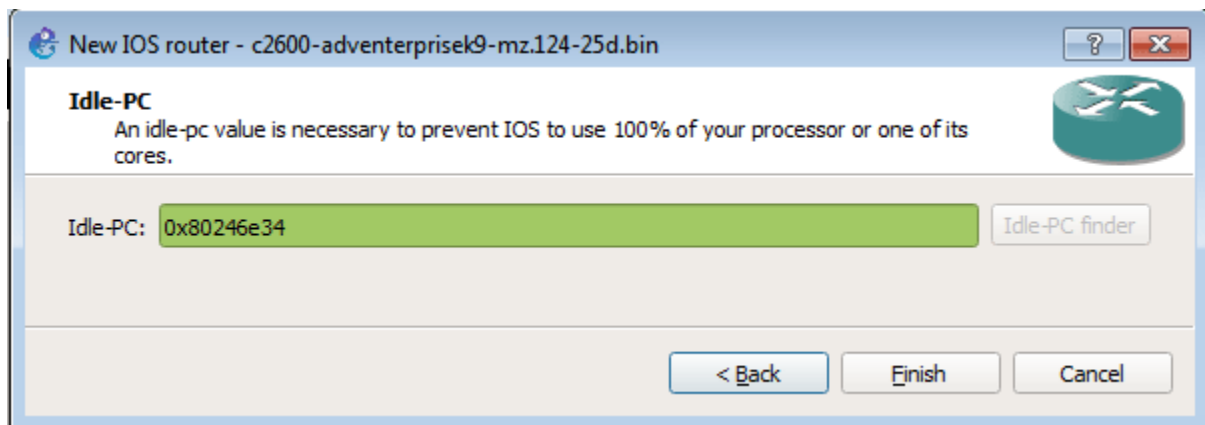


Select appropriate interfaces and click the Next button.

Click the Idle-PC finder button and use the suggested value in this field.



Click the Finish button to close the wizard.



Introduction to Wireshark

What is Wireshark?

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Some intended purposes

Here are some reasons people use Wireshark:

- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals

Wireshark can also be helpful in many other situations.

Features

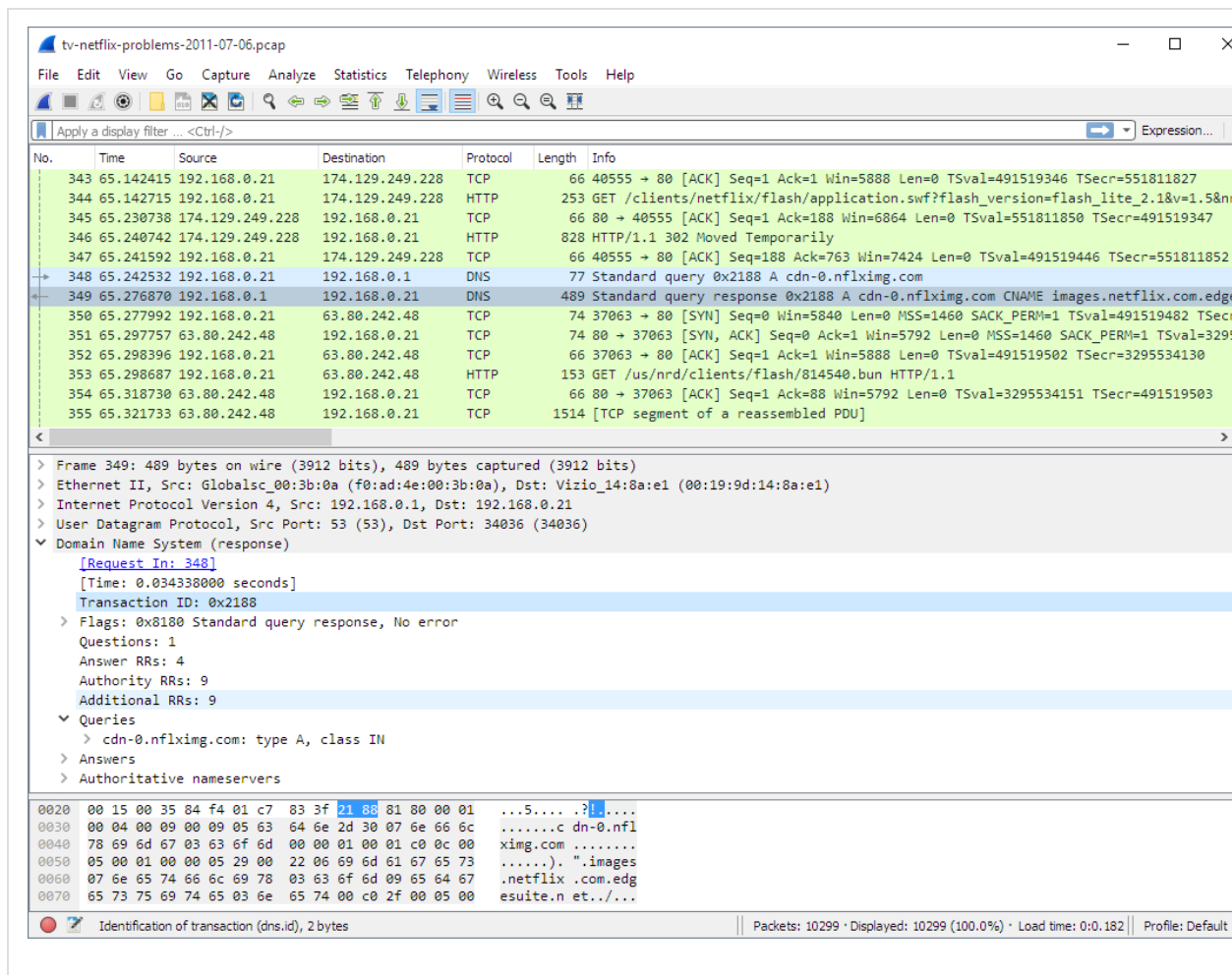
The following are some of the many features Wireshark provides:

- Available for *UNIX* and *Windows*.
- *Capture* live packet data from a network interface.
- *Open* files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- *Import* packets from text files containing hex dumps of packet data.
- Display packets with *very detailed protocol information*.
- *Save* packet data captured.
- *Export* some or all packets in a number of capture file formats.
- *Filter packets* on many criteria.
- *Search* for packets on many criteria.

- *Colorize* packet display based on filters.
- Create various *statistics*.
- ...and *a lot more!*

However, to really appreciate its power you have to start using it.

Figure: Wireshark captures packets and lets you examine their contents.



Live capture from many different network media

Wireshark can capture traffic from many different network media types, including Ethernet, Wireless LAN, Bluetooth, USB, and more. The specific media types supported may be limited by several factors, including your hardware and operating system. An overview of the supported media types can be found

at <https://gitlab.com/wireshark/wireshark/wikis/CaptureSetup/NetworkMedia>.

Import files from many other capture programs

Wireshark can open packet captures from a large number of capture programs.

Export files for many other capture programs

Wireshark can save captured packets in many formats, including those used by other capture programs.

Many protocol dissectors

There are protocol dissectors (or decoders, as they are known in other products) for a great many protocols.

Open Source Software

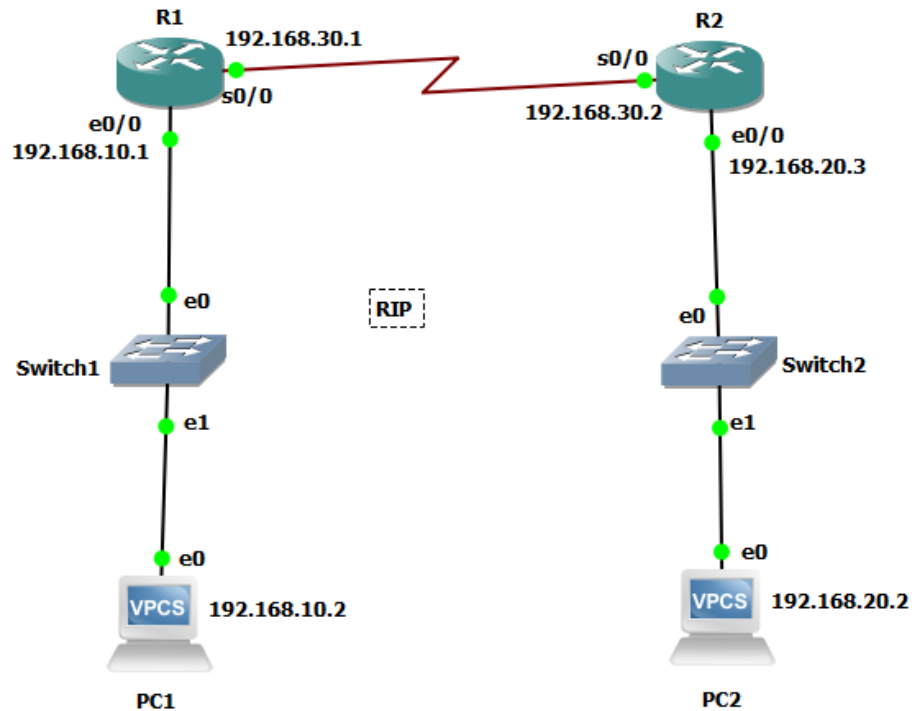
Wireshark is an open source software project, and is released under the GNU General Public License (GPL). You can freely use Wireshark on any number of computers you like, without worrying about license keys or fees or such. In addition, all source code is freely available under the GPL. Because of that, it is very easy for people to add new protocols to Wireshark, either as plugins, or built into the source, and they often do!

What Wireshark is not

Here are some things Wireshark does not provide:

- Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
- Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except domain name resolution, but that can be disabled).

Configuring RIP in a simple Network Topology



Configuring interfaces for R1 & R2:

```
R1(config)#interface s0/0
R1(config-if)#ip address 192.168.30.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#interface e0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
```

```
R2(config)#interface s0/0
R2(config-if)#ip address 192.168.30.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface e0/0
R2(config-if)#ip address 192.168.20.1 255.255.255.0
R2(config-if)#no shutdown
```

Now enable RIPv2 on the routers:

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.10.0
R1(config-router)#network 192.168.30.0
```

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.20.0
R2(config-router)#network 192.168.30.0
```

Check the configuration using **ping** command.