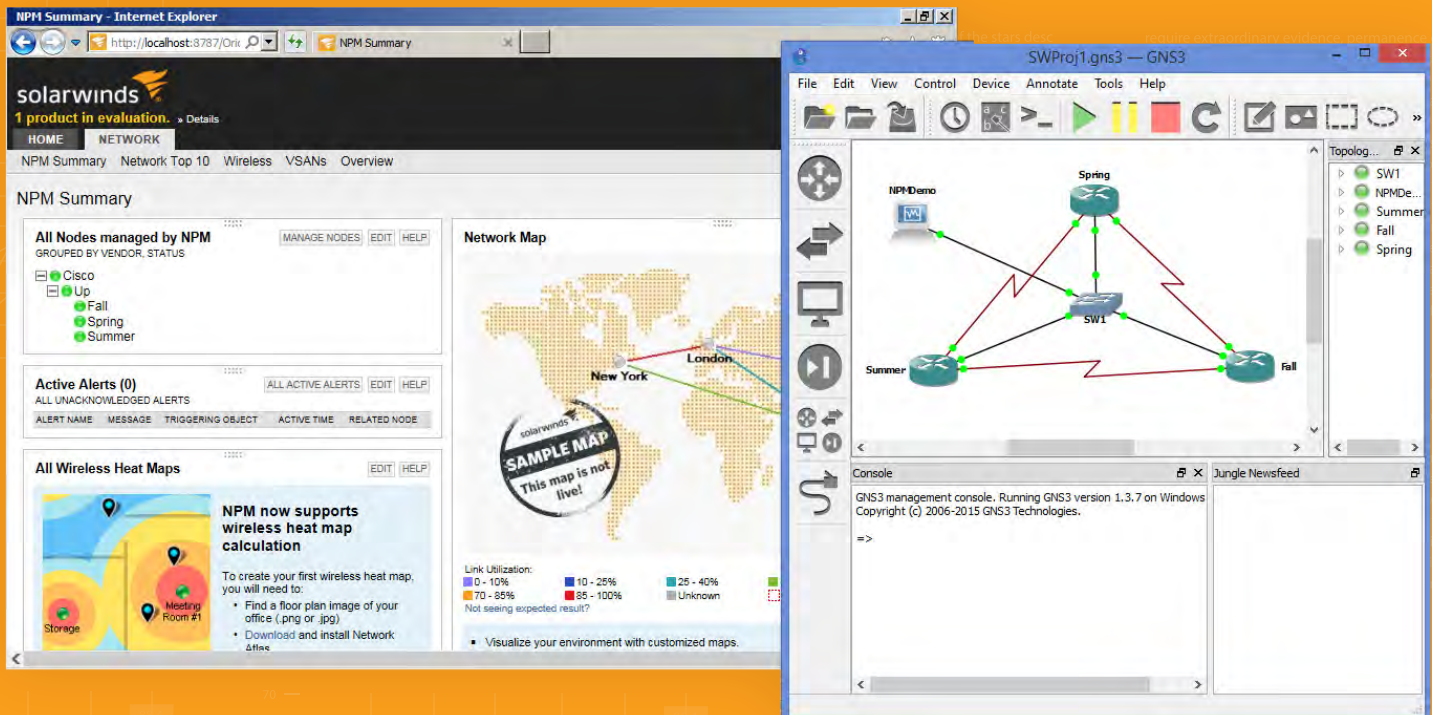




HOW TO GUIDE INSTALLING AND INTEGRATING NETWORK PERFORMANCE MONITOR & GNS3



INSTALLING AND INTEGRATING GNS3 AND NPM



IT'S ALL IN YOUR MIND (OR ON YOUR LAPTOP)

Using GNS3 and SolarWinds® to create a completely virtualized monitoring environment.

This guide provides detailed step-by-step instructions for setting up GNS3, creating a network, and then setting up a virtual machine running the SolarWinds Network Performance Monitoring solution.



INTRODUCTION

About GNS3

GNS3 is a tool that lets you create virtual network devices that act like real network devices. Why would you want to do this? Well, for years, GNS3 has been the go-to solution for people who wanted to pass their network certification exams (without having to drop thousands of dollars on actual network gear), and creative-but-frugal network professionals who wanted to mock up and test their network designs before rolling them out in a real production environment.

About SolarWinds Network Performance Monitor (NPM)

NPM is the flagship product from SolarWinds, Inc. It monitors devices for availability (up/down), performance, capacity, and more using agentless techniques, including SNMP and WMI. Devices which can be monitored include servers running Windows®, Linux®, UNIX®, and MacOS® network devices like routers, switches, and wireless access points, and any device with an IP address.

GNS3 + SolarWinds = Awesome

With a relatively recent update, GNS3's support of virtual PCs (and servers) via Oracle® and their open source VirtualBox® tool, a whole new class of IT pro has a reason to be really excited. Monitoring engineers who want to test new software and/or versions can now set up an entire "fake" network, which could include servers, routers, switches, and more, and perform test monitoring against that network.



ABOUT THIS GUIDE

Monitoring engineers might be unfamiliar with setting up networks (in GNS3 or otherwise). Also, GNS3 users might be unfamiliar with the conventions of monitoring solutions like SolarWinds NPM.

Which is where this guide comes in.

This document provides step-by-step, command-by-command, show-me-with-pictures instructions for installing GNS3, setting up a network, installing NPM, and adding the GNS3 network devices to NPM for monitoring. This guide assumes (almost) nothing about the reader's background and expertise and provides detailed instructions for all processes.

So, if you are a GNS3 guru and can set up a hybrid OSPF-BGP-EIGRP-RIP network before your morning coffee, you can probably skip ahead to the NPM part. And if you are a veteran SolarWinds expert who has installed NPM so many times that you have the screens memorized, you can probably stop reading once you get your network installed.

For those of you who likely fall somewhere in the middle, I hope this guide helps you to get to the part that's actually useful—testing your network and/or monitoring changes in a safe environment before rolling them out to your production environment.

Let's get started:

Here's an overview of what we're going to do:

1. Download everything.
2. Install PuTTY™.
3. Install VirtualBox®.
4. Install GNS3.
5. Configure GNS3.
6. Set up a simple network.
7. Add a virtual server to the network.
8. Install Windows® on the virtual server.
9. Install NPM on the virtual server.
10. Configure NPM to monitor the devices.

Before you start, verify your hardware

You may be wondering, "What am I installing all this stuff on?"

The answer is "whatever you want, really." But, of course, we all know there are a few requirements:

- You should have at least a quad-core processor on the machine because you will be running at least one virtual machine along with a few virtual network devices—not to mention your host operating system.
- You should probably have over 4GB of RAM. You can run with 4, but things are going to be pretty slow for the same reasons as the CPU requirement above.
- Disk space is less of an issue, given today's standards. GNS3 needs only about 100MB, but you also need to allow for the network device images, plus at least one Windows virtual machine running SolarWinds NPM. So you should figure your disk needs to have 200GB to 300GB free.

Step 1: Download everything

NOTE: You'll need to create an account for the GNS3 community before the download link will work. This is a Very Good Thing™ and I strongly recommend you do that anyway. (See instructions below.)

- GNS3: <https://community.gns3.com/community/software/download>
- PuTTY: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>
- VirtualBox: <https://www.virtualbox.org/wiki/Downloads>
- NPM: <http://www.solarwinds.com/network-performance-monitor.aspx>
- A copy of Windows
- The "images" of the network device operating system (Cisco® IOS® or other)
 1. Create an account at GNS3, and download the package from here:
<https://gns3.com/software/download>



Next, grab a copy of VirtualBox: <https://www.virtualbox.org/wiki/Downloads>. On that same page, you can download the extensions. While you don't have to have them, they're good to help normalize the hardware interactions, which is worth the extra 10-second download.

Of course, you'll need the 30-day demo of SolarWinds NPM: <http://www.solarwinds.com/network-performance-monitor.aspx>

Finally, to make your life easier, make sure you have PuTTY (or a similar telnet/ssh utility) installed: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

Another item you need to have handy is a copy of Windows. SolarWinds NPM will install on any version of Windows from Win7 up (although, server versions are better, and 64-bit server versions are best) so make sure you have that ready to go.

You'll also need IOS images to create routers and switches within GNS3. For my example, I'm limiting myself to using an image for a Cisco® 3600 router, using the image "c3640-ik9s-mz.124-25b.image."

Before you get on my back about NOT providing a link here, I would like to point you to this section of the GNS3 For Windows Getting Started Guide:

Step 3 - Defining Cisco IOS files

As mentioned earlier, due to licensing issues, you must provide your own Cisco IOS and license for IOU to use with GNS3.

GNS3 is meant to be used in a lab environment for testing and learning. Once you have obtained your own copy of a Cisco IOS for one of the supported platforms, you are ready to continue. Supported platforms are Cisco 7200, 3600 series (3620, 3640, and 3660), 3700 series (3725 and 3745), and 2600 series (2610 to 2650XM and 2691).

What this means is if you have a Cisco support contract, you can download images from the Cisco.com website. There are probably other sources for IOS images on the Internet. However, that is beyond the scope of this document and is left to the resourcefulness and ethics of the reader.

Step 2: Install PuTTY

And by "install," I mean unzip the package and put the executables someplace in your path.

Step 3: Install VirtualBox (and extensions)

I'm going to start by installing VirtualBox so GNS3 can detect it when I install it next. But I'm not going to set up the NPM server just yet.

There's really nothing special about the VirtualBox install. Follow the prompts, accept the defaults, and let it rip.

Once the main installer finishes, start VirtualBox, and install the extension pack (you DID download the extension pack, right?).

1. Go to File, Preferences, Extensions, and click the Add new package button (the blue box with the yellow arrow on the right).
2. Select the extension pack, and click Open.
3. Accept the license agreement.
4. Follow the prompts until everything is installed.

TOP 5 FREE TROUBLESHOOTING & NETWORK MONITORING TOOLS

Response Time Viewer for Wireshark®

Response Time Viewer for Wireshark® analyzes a packet capture (PCAP) file to help you determine if it's the network or the application

[DOWNLOAD NOW »](#)

Network Analyzer & Bandwidth Monitoring Bundle

Quickly identify the types of network traffic by flow data capture and interface monitoring for bandwidth usage in real time.

[DOWNLOAD NOW »](#)

Network Device Monitor

Monitor any statistic on any SNMP-enabled network device using a groovy desktop dashboard!

[DOWNLOAD NOW »](#)

IP Address Tracker

Scan, track, and consolidate your IP address information in one easy place, saving you time and eliminating errors (and headaches)!

[DOWNLOAD NOW »](#)

Wake-On-Lan

Remotely power up network PCs.

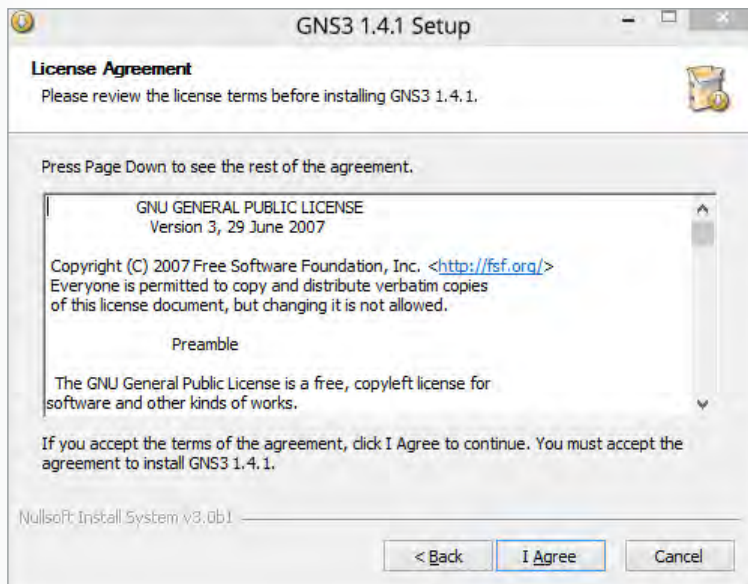
[DOWNLOAD NOW »](#)

Step 4: Install GNS3

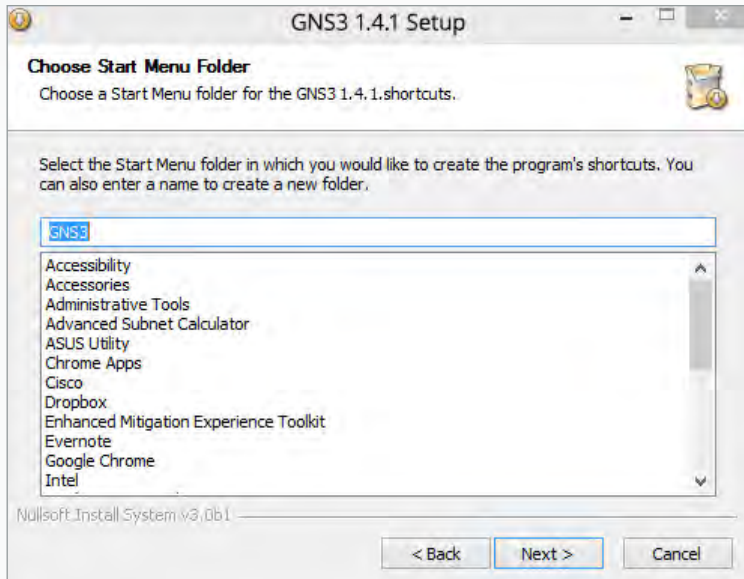
1. Double-click the GNS3 installer.
2. If you have User Access Control on, confirm that you REALLY want to start the GNS3 installer.
3. Click Next on the splash screen.



4. Accept the license agreement.

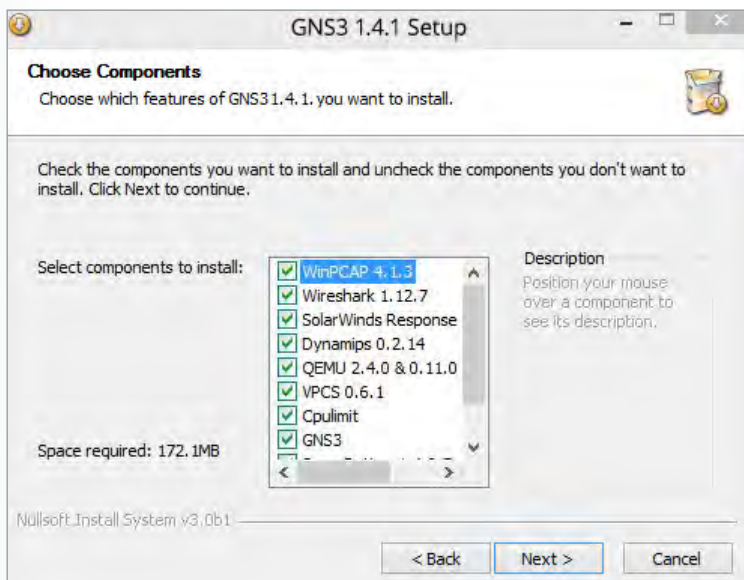


5. Select the Start menu location where GNS3 programs should appear.

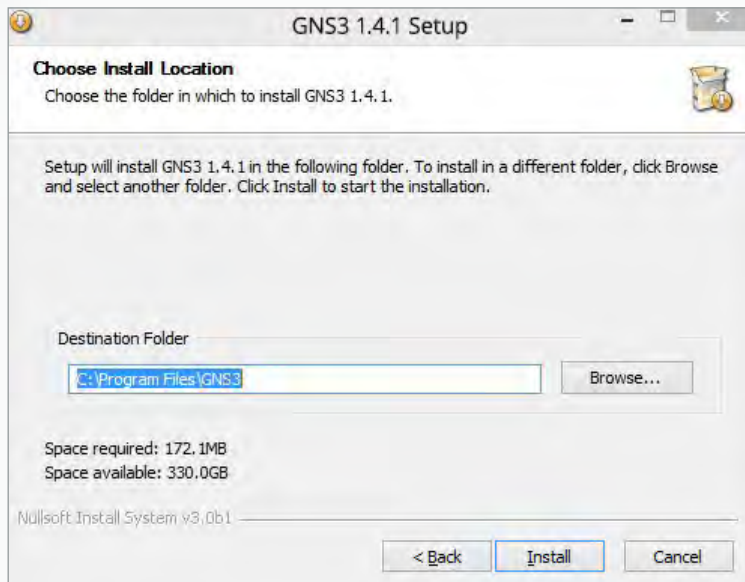


6. And select the GNS3 elements.

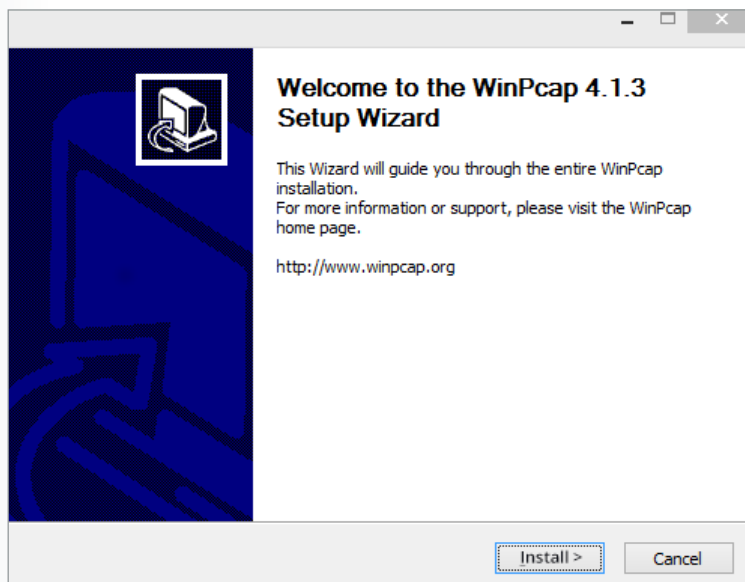
HINT: TAKE ALL OF THEM!!!!



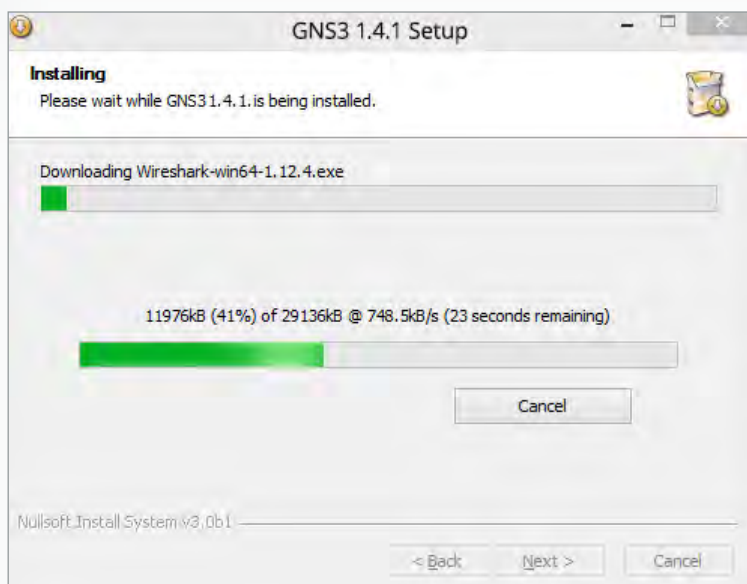
7. Select the directory where GNS3 will be installed.



8. And finally, click Install.



9. During the install,

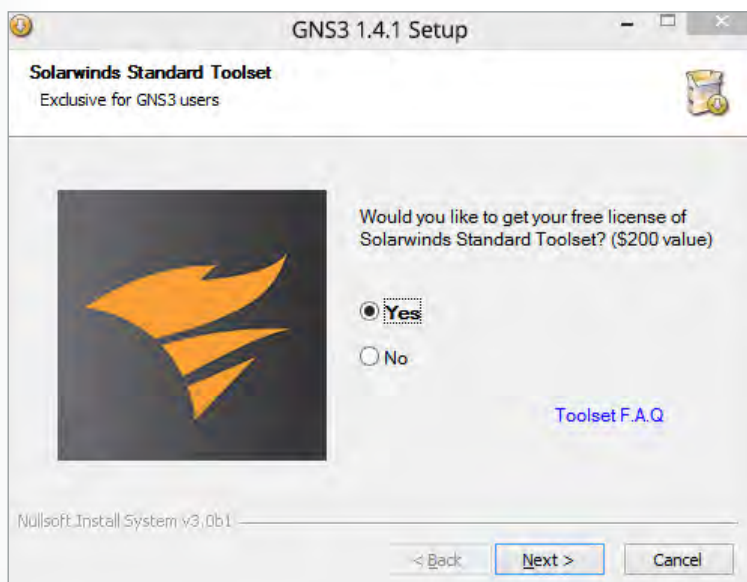


the sub modules (WinPCAP, Wireshark, SolarWinds Response Time Viewer, etc.) you selected have their own installer.

Go ahead and click through those as well, selecting the defaults, unless you have a compelling reason not to do so. Note that some of the sub-installers will pop under the main screen, so you should probably minimize all open windows and keep an eye out for new items on the taskbar just so you aren't waiting for a confirmation box which is hidden somewhere on the desktop.

Certain items, such as WinPCAP, may attempt to install twice (once because it's in the GNS3 list of installers, and again because it's part of the Wireshark install, which GNS3 also installs).

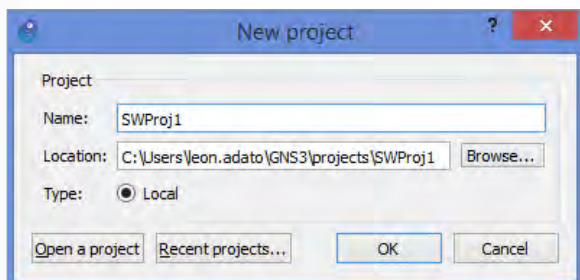
10. Also note that from time to time GNS3 bundles in offers of free software from other vendors. As with all installers, a modicum of common sense is always advisable. Although, the offer pictured below is a GREAT deal!



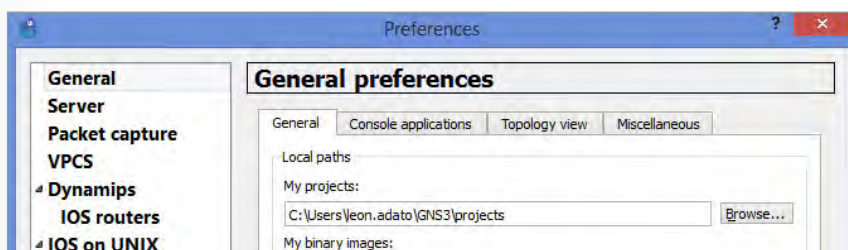
Step 5: Start and configure GNS3

Once the GNS3 installer ends, there is a checkbox to start GNS3. Go ahead and check that box and click Finish.

After a brief bit of screen splashing, you'll be in the main GNS3 screen, and will be prompted to start a new project. Go ahead and name your project, and click OK.



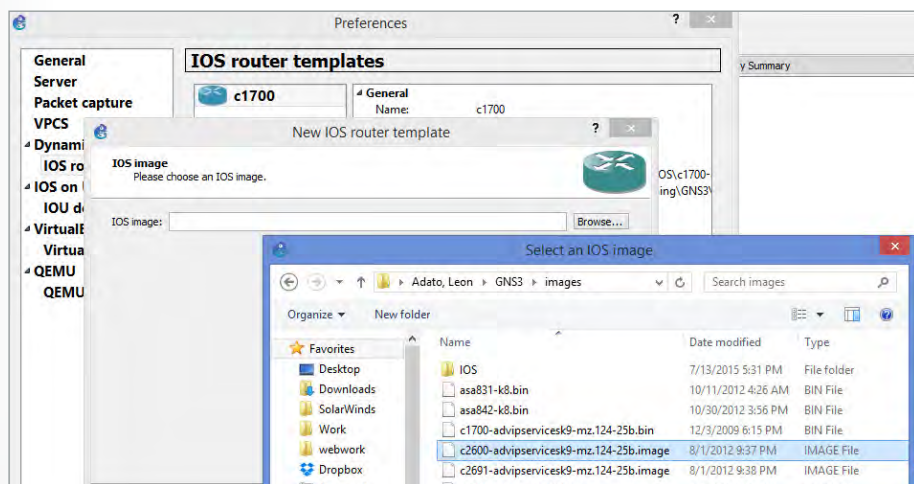
Before you do anything else, let's check some configuration settings by going to Edit, Preferences, and looking at the General tab:



Note the location of binary images. That's where your IOS images need to go. Go ahead and copy them into that directory (create it if you need to).

NOTE: Although we have mentioned and used Cisco IOS throughout the document, GNS3 can also emulate a number of other vendor hardware products. For a comprehensive list of hardware that can be emulated using GNS3, check the supported hardware documentation page or the GNS3 community page.

Now, you need to add images to the list of available routers. Click down to the IOS routers option on the left, and click New. Click the browse button, and go to the location where you just placed all your IOS images. Select an image, and click Open.



Follow the prompts, taking the default options unless you have a compelling reason to change them. Repeat this process until have added all IOS images.

Step 6: Create your network

For the following example, I'm setting up three Cisco 3600s connected via EIGRP. This is a very simple setup intended for readers who may not have much experience configuring a network. If you want to set up something different, be my guest.

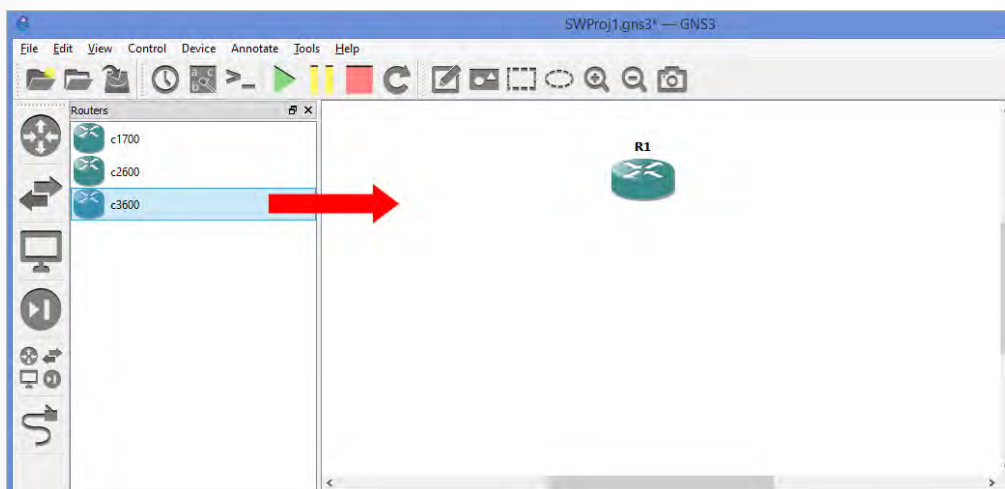
Here are some notes about what this will look like when we're done. A downloadable version of this project (which may require some updates depending on your installation of GNS3) is available at:

GNS3 Sample Network

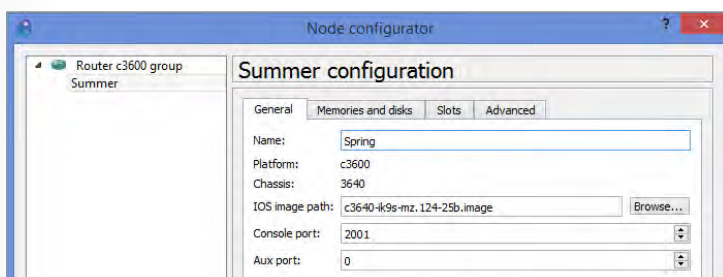
Complete these steps to create your network:

1. From the main screen, click the router icon, and drag a 3600 router onto the main page.

TRICK: To get all three routers at once, press SHIFT-drag. You'll get a popup asking for the number of routers and you'll be done.



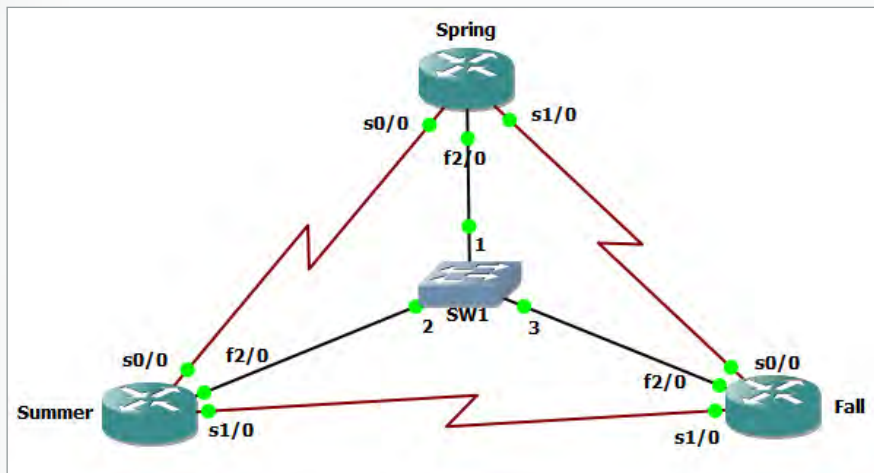
2. Right-click the R1 router, and choose Configure.



- a. On the General tab, set the name to Spring.
 - b. On the Slots tab, set slots 0 and 1 to NM-4T (serial).
 - c. Set slot 2 to NM-1FE-TX (FastEthernet).
3. Click OK to finish, and repeat these steps for Routers 2 and 3, naming them Summer and Fall, respectively.

Now that the routers are all placed and provisioned, we need to configure them. We're going to set up three network connections on each router, and then connect each of the routers together using the EIGRP protocol. The remaining (FastEthernet) interface is going to be on a "management" network, which is how monitoring will be done.

First, a picture:



And here's a description of the interfaces on each device:

Router 1 name: Spring

- Interface 1 (serial):
 - 10.1.1.1/24 (i.e.: gateway 255.255.255.0)
 - Connects to Summer
- Interface 2 (serial):
 - 10.1.2.1/24
 - Connects to Fall
- Interface 3 (FastEthernet):
 - 10.1.100.1/24
 - Will be default gateway for management network

Router 2 name: Summer

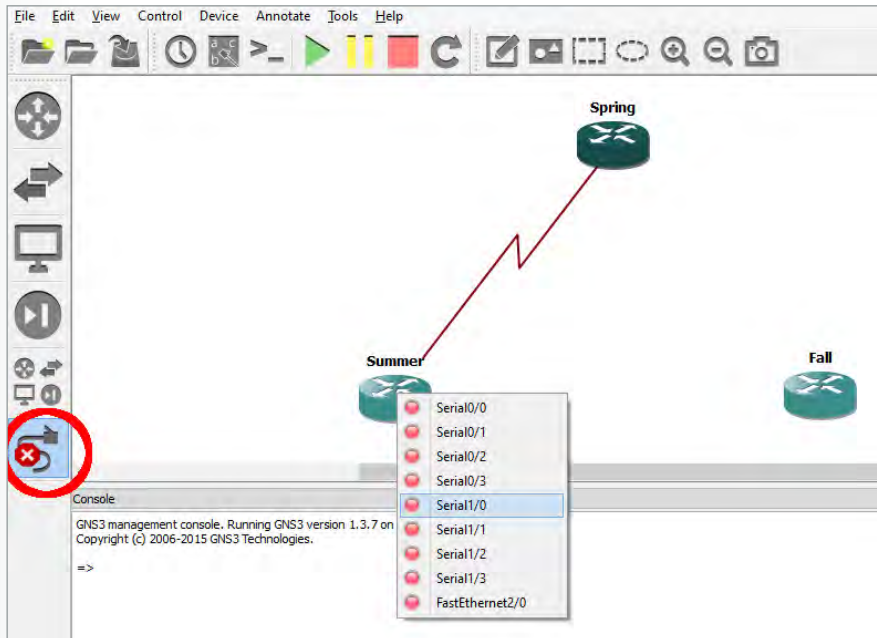
- Interface 1 (serial):
 - 10.1.2.2/24
 - Connects to Spring
- Interface 2 (serial):
 - 10.1.3.1/24
 - Connects to Fall
- Interface 3 (FastEthernet):
 - 10.1.100.2/24
 - Connects to management network

Router 3 name: Fall

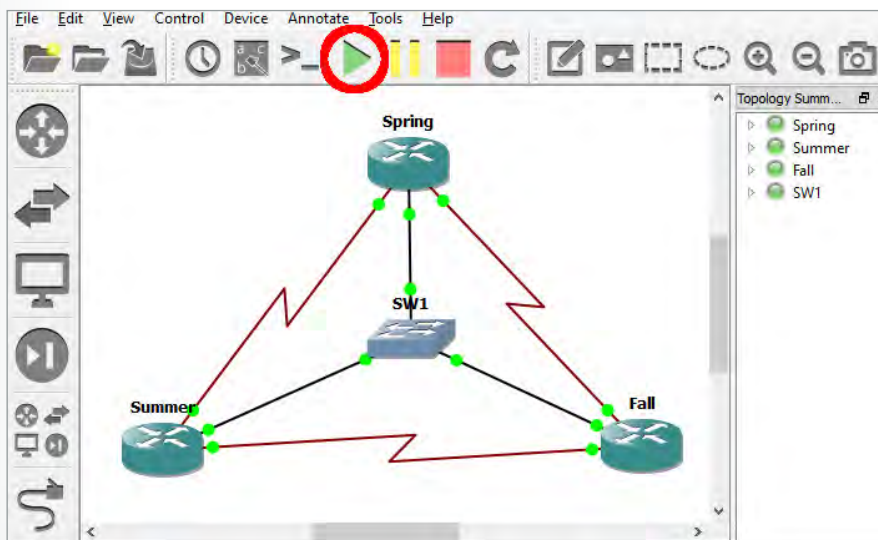
- Interface 1 (serial):
 - 10.3.1.2/24
 - Connects to Summer
- Interface 2 (serial):
 - 10.1.2.2/24
 - Connects to Spring
- Interface 3 (FastEthernet):
 - 10.1.100.3/24
 - Connects to management network

With that design in mind, let's get to configuring.

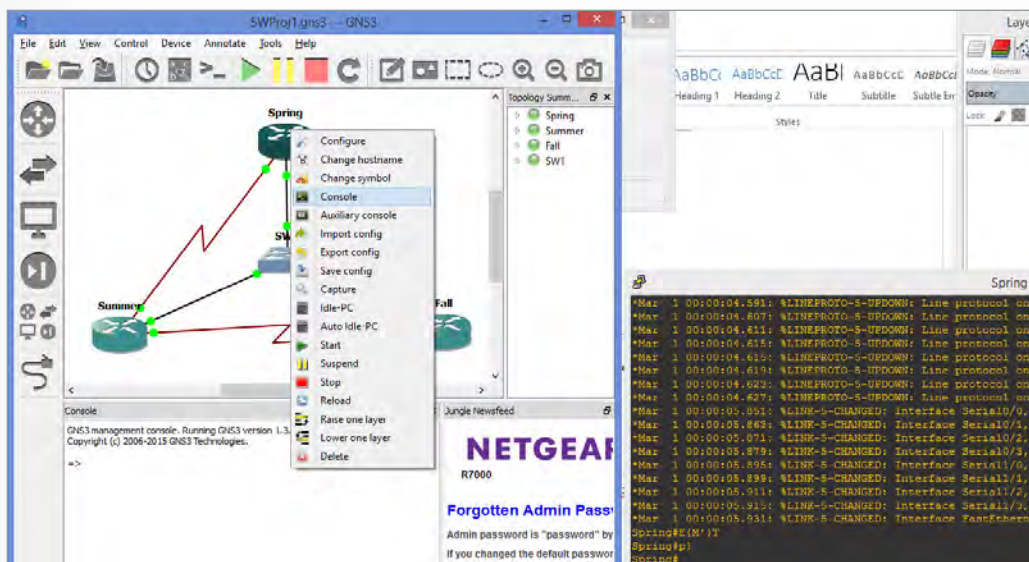
1. Click the Connection button.
2. Click Spring, and select interface Serial0/0.
3. Click Summer, and select interface Serial 0/0.



4. Continue to connect routers as follows:
 - a. Spring, Serial1/0 to Fall, Serial0/0
 - b. Summer, Serial1/0 to Fall, Serial0.0
5. Click the switch icon and drag an "Ethernet switch" onto the screen.
6. Click the connector icon again and connect each router's FastEthernet2/0 interface to the switch.
7. Now let's turn it on. Click the "play" button to ensure that all your devices are running.



8. Right-click Spring and choose Console to open a telnet/ssh terminal. Press ENTER a couple of times, if necessary, to get things moving.



9. Set up SNMP:
 - a. Type this to enter config mode:
`configure terminal`
 - b. Type this to set up a SNMP read-only string so you can monitor with NMP:
`snmp-server community GNS3plusSWrocks ro`

10. Set up the interfaces:
 - a. Type this to edit the first interface:
`interface S0/0`
 - b. Type these commands to set up the first interface:
`ip address 10.1.1.1 255.255.255.0`
`no shutdown`
 - c. Exit back to interface mode.
`exit`
 - d. Type these commands to set up the second interface:
`int S1/0`
`ip address 10.1.2.1 255.255.255.0`
`no shutdown`
 - e. Exit back to interface mode.
`exit`
 - f. Type these commands to set up the third (FastEthernet) interface:
`int Fa2/0`
`ip address 10.1.100.1 255.255.255.0`
`no shutdown`
 - g. Exit back to interface mode, and set up EIGRP routing.
`exit`
`router EIGRP 1`
`network 10.1.1.0 0.0.0.255`
`network 10.1.2.0 0.0.0.255`
 - h. Exit all the way out, and save your configuration.
`exit`
`exit`
`write memory`

11. Set up EIGRP on the other two routers.

- a. Right-click on the router "Spring" and open a console, then enter the following commands:
configure terminal

```
snmp-server community GNS3plusSWrocks ro
interface S0/0
ip address 10.1.1.2 255.255.255.0
no shutdown
exit
int S1/0
ip address 10.1.3.1 255.255.255.0
no shutdown
exit
int Fa2/0
ip address 10.1.100.2 255.255.255.0
no shutdown
exit
router EIGRP 1
network 10.1.1.0 0.0.0.255
network 10.1.3.0 0.0.0.255
exit
exit
write memory
```

- b. Right-click on the router "Fall" and open a console, then enter the following commands:

```
configure terminal
snmp-server community GNS3plusSWrocks ro
interface S0/0
ip address 10.1.2.2 255.255.255.0
no shutdown
exit
int S1/0
ip address 10.1.3.2 255.255.255.0
no shutdown
exit
int Fa2/0
ip address 10.1.100.3 255.255.255.0
no shutdown
exit
router EIGRP 1
network 10.1.2.0 0.0.0.255
network 10.1.3.0 0.0.0.255
exit
exit
write memory
```


12. Ensure that your network is working by issuing the following commands on all three routers:

```
ping 10.1.1.1
ping 10.1.1.2
ping 10.1.100.1
ping 10.1.2.1
ping 10.1.2.2
ping 10.1.100.2
ping 10.1.3.1
ping 10.1.3.2
ping 10.1.100.3
```

You should see the following type of response each time:

```
Spring#
Spring#ping 10.1.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.3.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/11/20 ms
Spring#
```

13. If you receive failure messages, you will need to review your configuration and make the necessary changes.

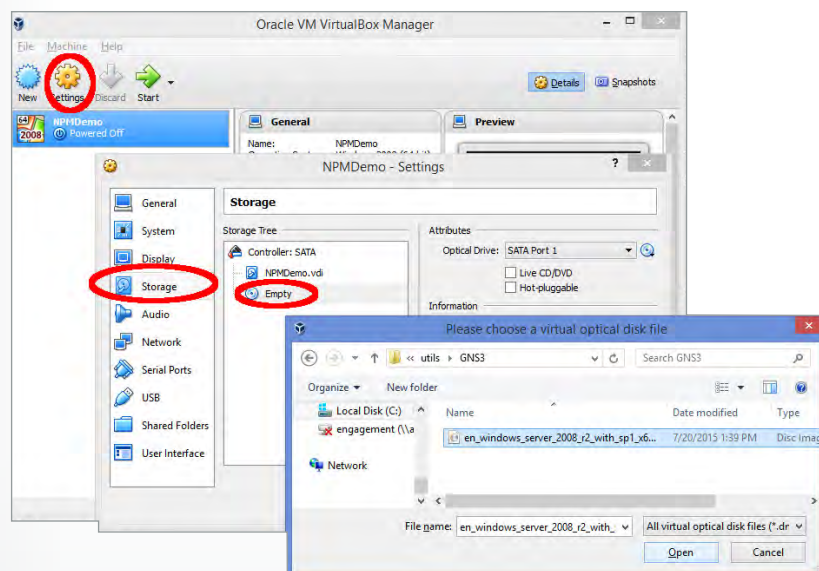
CONGRATULATIONS!! You now have a functioning network that you can use for all manner of processes. Here's the one we're going to use:

Step 7: Create a virtual machine

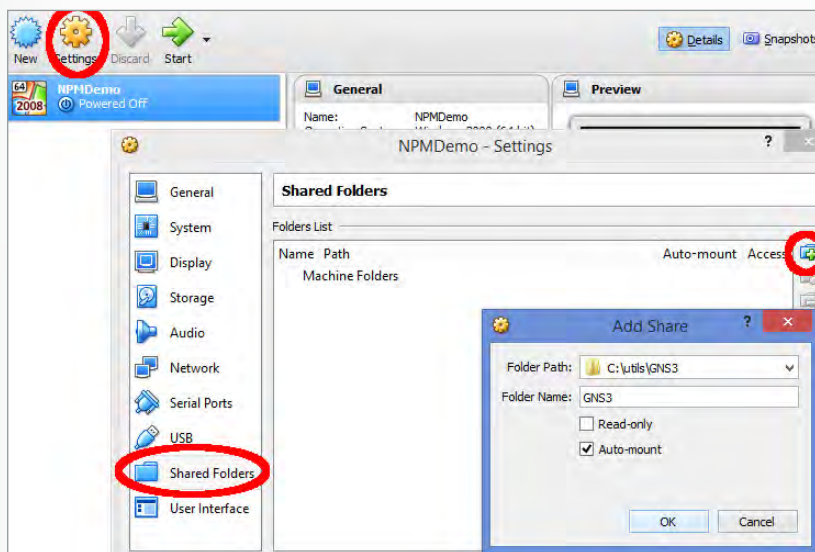
1. Start VirtualBox.
2. Click New to create a new system.
3. In the next screen, provide a name (we're using NPMdemo), and select the operating system you intend to install.

NOTE: NPM will install on any 64-bit version of Windows from Windows 7 and later. But a server version is best if this is going to be anything but a small test.

4. Determine how much RAM, CPU, and disk space you wish to allocate.
5. Complete your new virtual machine.
6. If you have a physical copy of Windows, insert it in your computer. If not:
 - a. Go to Settings, Storage, and select the Empty CD/DVD drive. Then navigate to your copy of Windows.



- Go to Settings, Shared Folders, and add a new folder that points to where you have the NPM installation files.



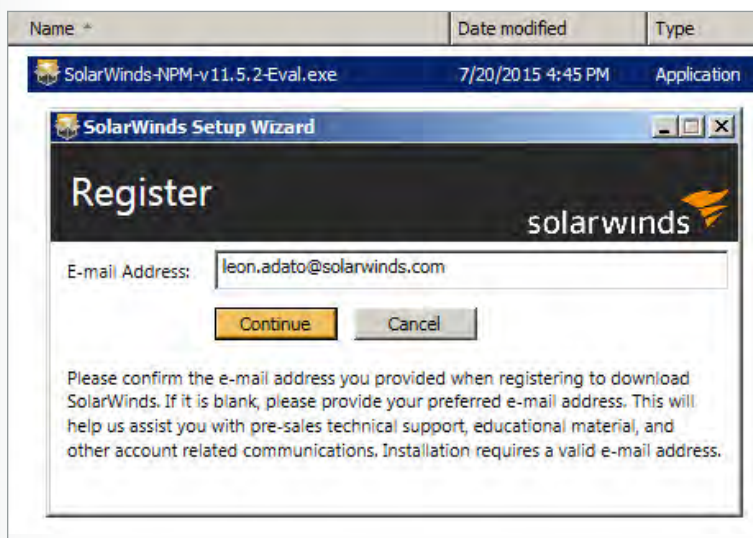
- Back at the main screen, click Start to fire up your new virtual machine.
- At this point, the Windows installer should kick in. I'm just going to leave the instructions here with this bit of sage advice: "Install Windows."

TIP: You'll probably need to restart the computer a few times during installation and patching. To send Ctrl-Alt-Del to the virtual machine, use the "hostkey"+Del combination, where "hostkey" is usually the right Ctrl key.

Step 8: Install NPM

NPM installation is straightforward.

- After clicking the installer, enter your email address, and click Next.



KEY FEATURES OF NETWORK PERFORMANCE MONITOR

Multi-vendor network monitoring software for fault, performance and availability monitoring

Quickly detect, diagnose, and resolve network performance issues and avoid downtime with **network optimization software**

[WATCH THE VIDEO »](#)

Dynamic network maps

Automatically map devices and display performance metrics, and link connection and utilization

[WATCH THE VIDEO »](#)

Wireless network monitoring and management

Retrieve performance metrics for autonomous access points, wireless controllers, and clients

[LEARN MORE »](#)

Customizable network topology & dependency-aware intelligent alerts

Respond to multiple condition checks, correlated events, **network topology**, and device dependencies

[WATCH THE VIDEO »](#)

End user quality of experience with Packet Capture and Analysis

Determine if changes in end user experience are caused by the application or the network

[WATCH THE VIDEO »](#)

Automated device discovery

Schedule automated discovery of SNMP & WMI-enabled network devices

[LEARN MORE »](#)

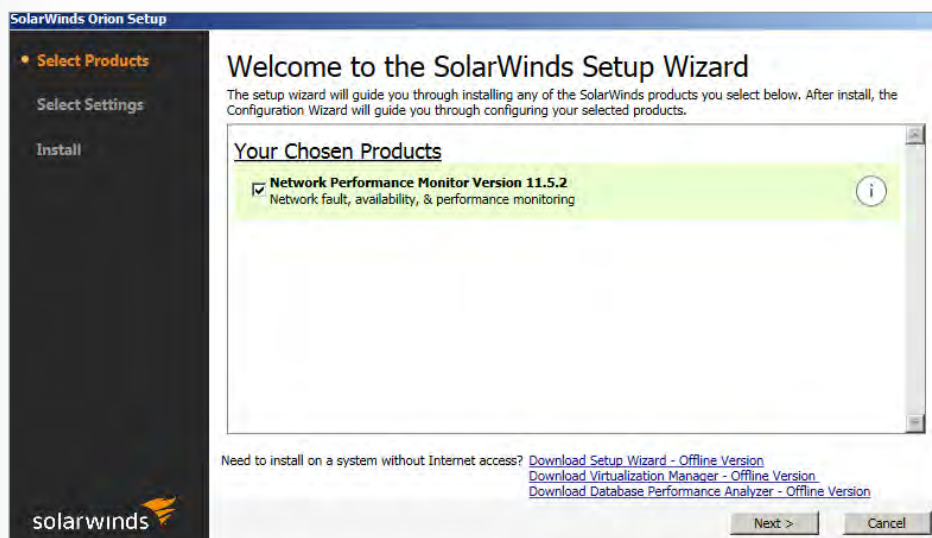
Automated capacity forecasting, alerting, and reporting

Automatically calculate exhaustion dates using customizable thresholds based on peak and average usage

[WATCH THE VIDEO »](#)

2. On the welcome screen, confirm the installation of NPM.

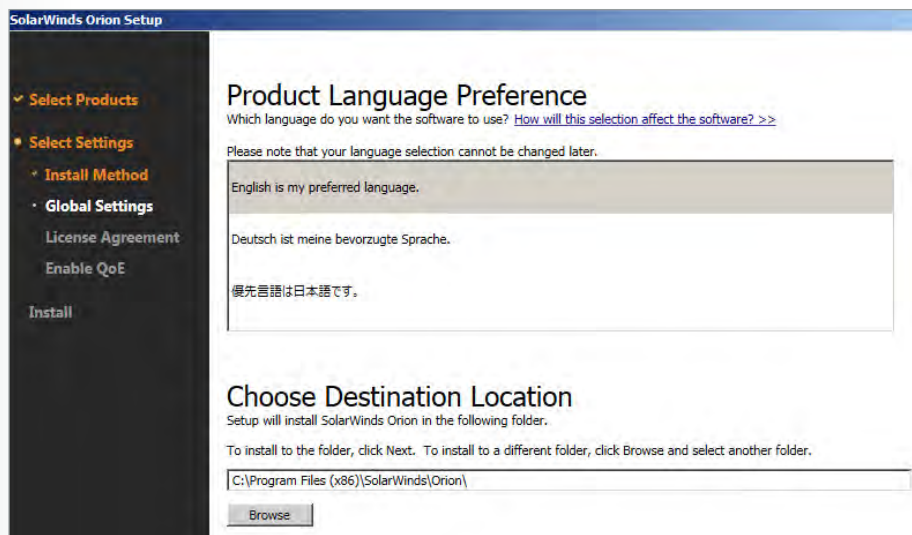
NOTE: If this machine (the host machine or the VM) does not have Internet access, use the link at the bottom of the screen to download the offline version of the installer and use that instead.



3. On the next screen, select Express Install.

HINT: the advanced install is used if you use a separate SQL server for database storage. In most cases, for this kind of test environment, the Express install (which installs a local copy of SQLExpress) is sufficient.

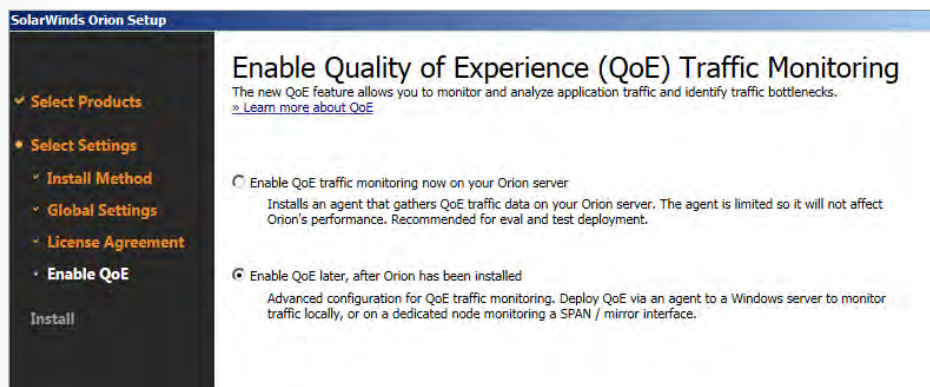
4. Select your preferred language.



5. Accept the license agreement (the checkbox at the bottom of the screen) and click Next.



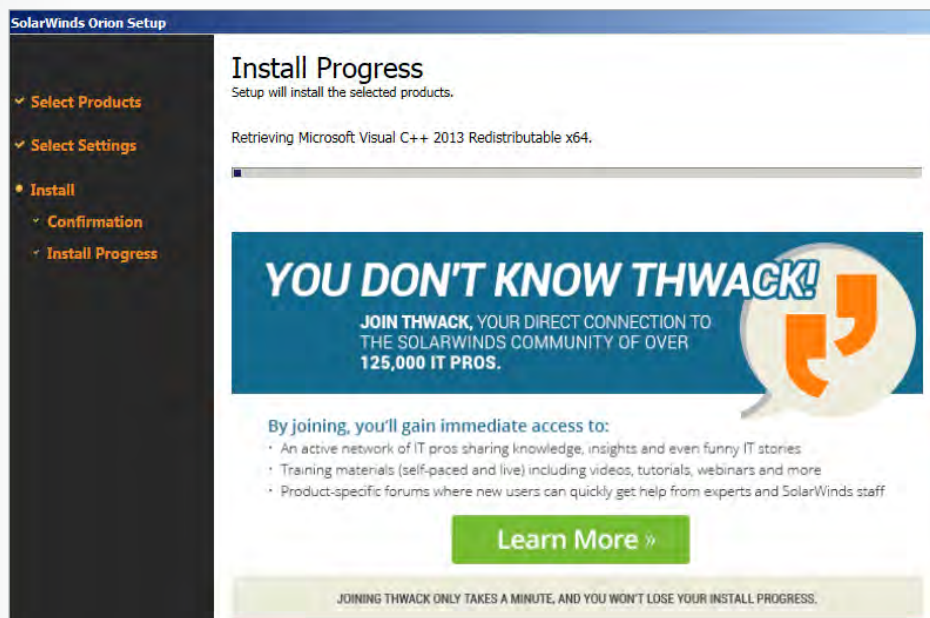
6. In this example, we won't be testing the Quality of Experience monitoring, so select the Enable later radio button, and click Next.



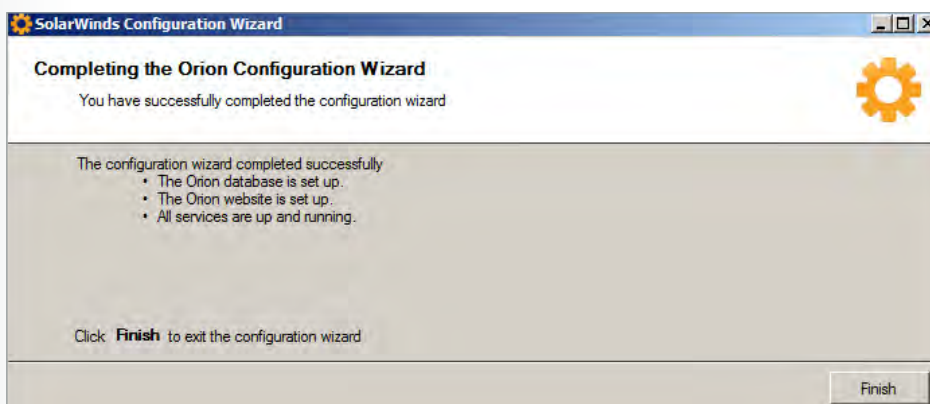
7. One final confirmation to click Next past...



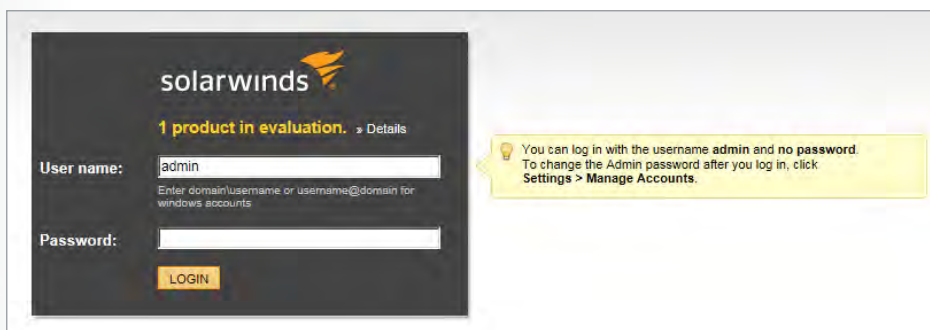
8. The installer should proceed without any other confirmations.



9. Once the installation is complete, you will see this confirmation dialogue:



10. At that point, your default browser will start up, and the SolarWinds® Orion® login page will display:



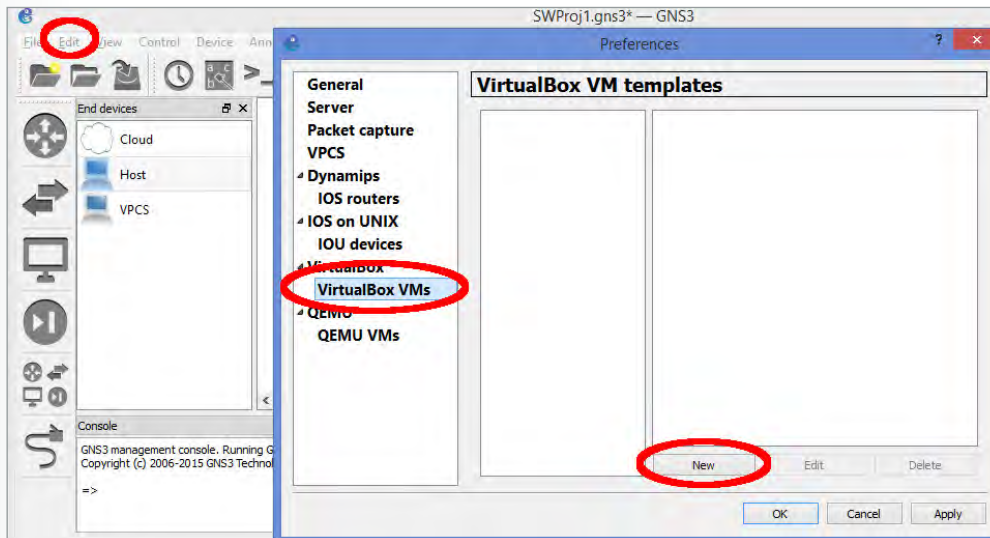
Congratulations! NPM is now installed and ready to go.

In order to add this new virtual machine into GNS3, shut down the VM.

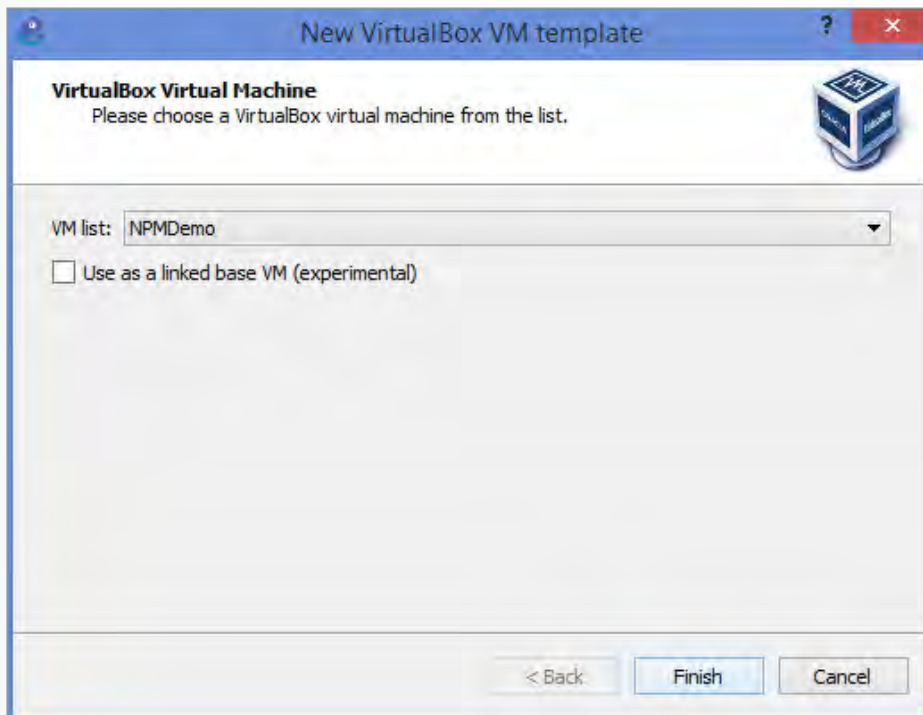
Step 9: Add the new virtual machine to GNS3

At this point, all of the required software is installed and ready to go. The next stage is to add the new virtual machine into the GNS3 environment. This section will run best if you start while running both GNS3 and VirtualBox (although with no virtual machines open).

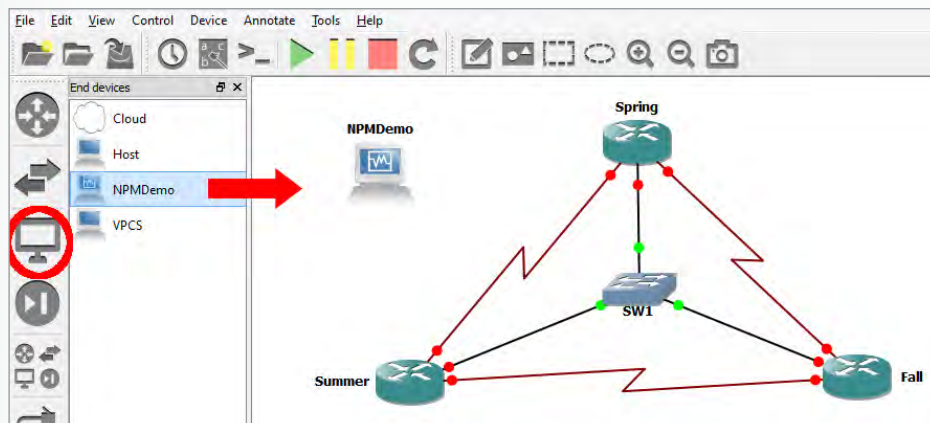
1. Back in GNS3, go to Edit, Preferences, and choose VirtualBox VMs from the sidebar, then click New.



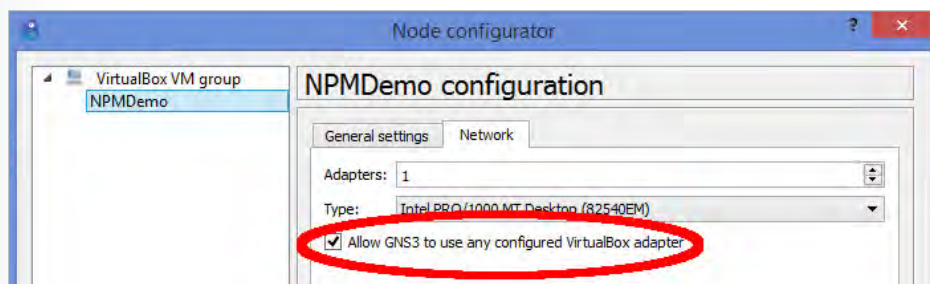
2. Select your NPM virtual machine from the list, and click Finish. Then click OK to exit the Preferences dialogue.



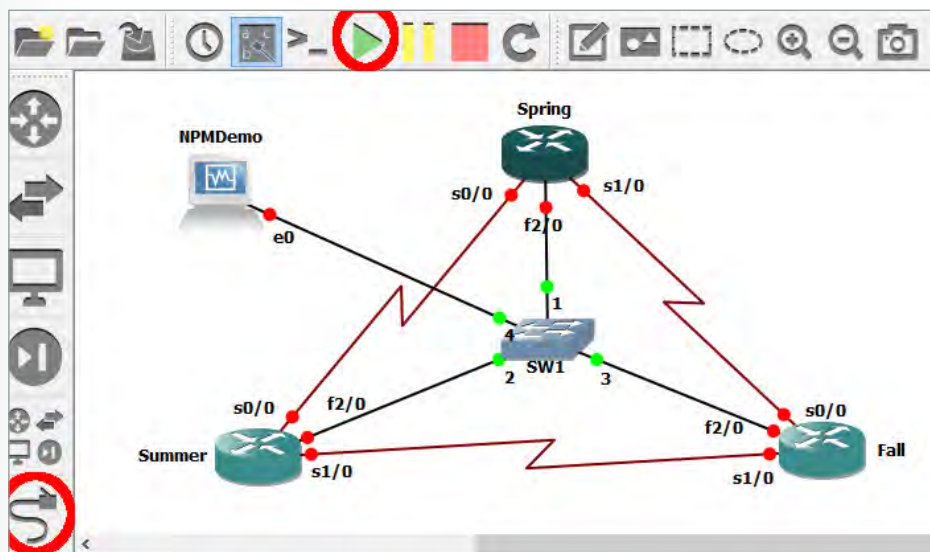
3. Back on the main GNS3 screen, click the End Devices button, and then drag the NPM virtual machine into the main area.



4. Right-click the NPMDemo machine and choose Configure. Select the NPM Demo machine on the left-hand list, and click the Network tab. Finally, check the box that says Allow GNS3 to use any configured VirtualBox adapter, and click OK.



5. Use the connector icon to create a connection from port 4 on the switch (SW1) to the Ethernet 0 on the NPMDemo machine. Then cross your fingers, click the "play" button, and see what happens!



If everything is set up correctly, all the routers will start up, AND the VirtualBox machine will start.

Step 10: Configure NPM to monitor the devices within the GNS3 environment

Now that everything is installed, configured, connected, and running, go back to the NPMDemo machine. Before we can add devices, we have to make sure the NPM server is able to connect to the routers. Normally, this would all be handled by DHCP and DNS. But because we're in a small test environment, we have to set it manually.

Remember how we set up the third adapter on each router to be on the 10.1.100.x network? That's what we're using for management.

Set your NPM server's network card with the following information:

- IP Address: 10.1.100.100
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.1.100.1 (the Spring router)

Once you've done that, test your settings by running the following commands at a DOS prompt (yes, it IS called a DOS prompt, you whipper snapper!).

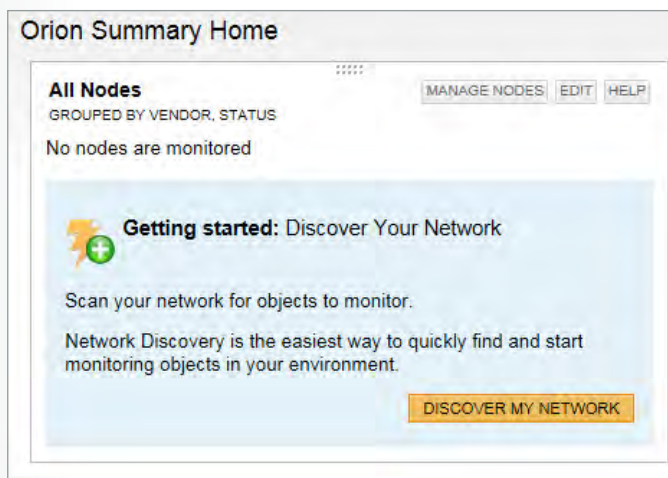
```
ping 10.1.100.100
ping 10.1.100.1
ping 10.1.100.2
ping 10.1.100.3
```

All four commands need to work before we move on. Troubleshoot as needed.

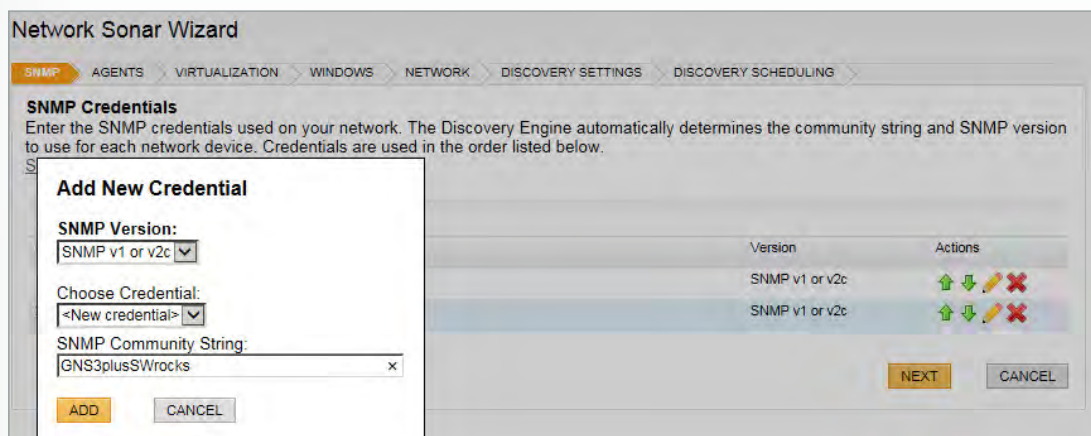
Now we'll fire up the NPM portal and add our routers.

NOTE: NPM is an extremely powerful tool which can monitor not only SNMP devices, but also Windows servers via WMI, as well as Cisco UCS®, VMware®, and Microsoft® devices via their specific APIs. All of that is beyond the scope of this guide, so some of the steps below are extremely abbreviated in order to move us to the primary goal: monitoring the routers Spring, Summer, and Fall. I leave it to the curious readers to explore all the other amazing features of NPM at their leisure.

1. Start your browser, and go to either <http://<machinename>:8787/> or <http://localhost:8787>.
2. Log in using the default credentials.
3. If NPM is running for the first time, you will automatically end up at the Add new devices page. If not, use the Discover My Network button on the main screen.



- On the first screen, we need to add the proper SNMP credentials. This would be GNS3plusSWrocks if you were following the directions back at the start of this document. If not, add whatever SNMP or string your devices use. You can also remove unneeded strings (like "private") from the list before clicking Next to proceed.



Network Sonar Wizard

SNMP AGENTS VIRTUALIZATION WINDOWS NETWORK DISCOVERY SETTINGS DISCOVERY SCHEDULING

SNMP Credentials
Enter the SNMP credentials used on your network. The Discovery Engine automatically determines the community string and SNMP version to use for each network device. Credentials are used in the order listed below.

Add New Credential

SNMP Version:
[SNMP v1 or v2c]

Choose Credential:
[<New credential>]

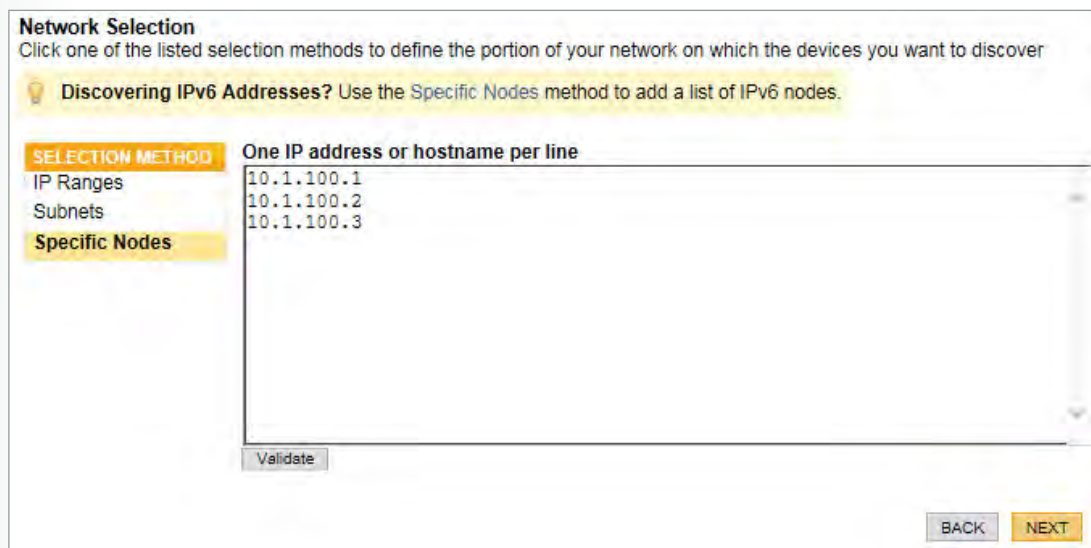
SNMP Community String:
[GNS3plusSWrocks]

ADD CANCEL

Version	Actions
SNMP v1 or v2c	↑ ↓ ✎ ✕
SNMP v1 or v2c	↑ ↓ ✎ ✕

NEXT CANCEL

- Because none of our devices are using agents, you can click Next to move past that screen.
- Similarly, we aren't monitoring any virtual machines, so on the next screen, un-check Poll for VMware, and click Next.
- And, once again, no Windows servers will be monitored as part of this exercise, so click Next past the screen where you would add your Windows credentials.
- The next screen lists several ways to add devices (scanning subnets, using a seed router, etc.). In the name of expediency, we're going to list the specific IPs to add. Click Specific Nodes and add the IPs of the three routers before clicking Next to continue.



Network Selection
Click one of the listed selection methods to define the portion of your network on which the devices you want to discover

Discovering IPv6 Addresses? Use the Specific Nodes method to add a list of IPv6 nodes.

SELECTION METHOD

IP Ranges

Subnets

Specific Nodes

One IP address or hostname per line

```
10.1.100.1
10.1.100.2
10.1.100.3
```

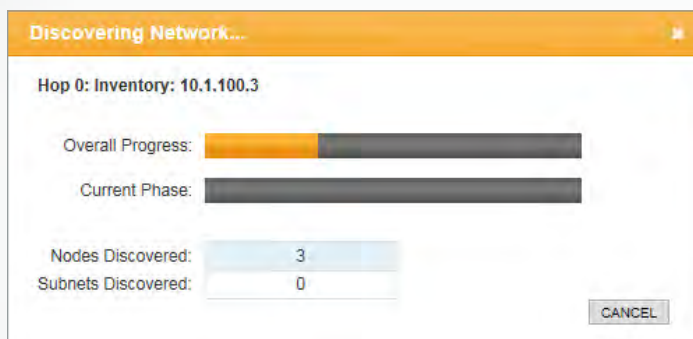
Validate

BACK NEXT

The following screen has settings (timeouts, etc.) which are useful in a production environment, but shouldn't make a difference to us here.

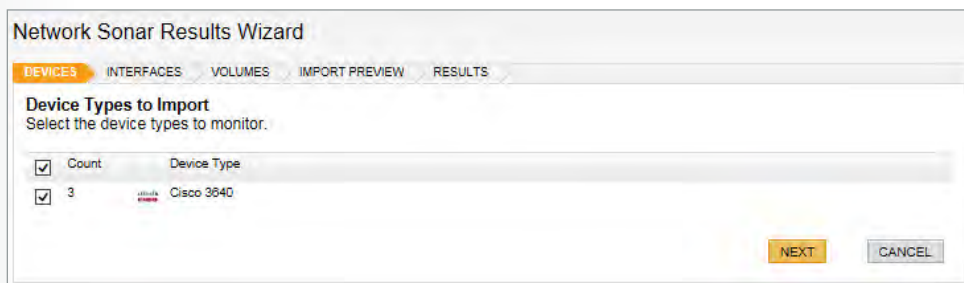
- Click "Next" to proceed.
- On the final screen, we don't need to change any scheduling options. Simply click Discover to get the show on the road.

11. The discovery shouldn't take long.



You will see the results page, which should include three Cisco 3600 routers (or whatever your network is made up of, if you did something different).

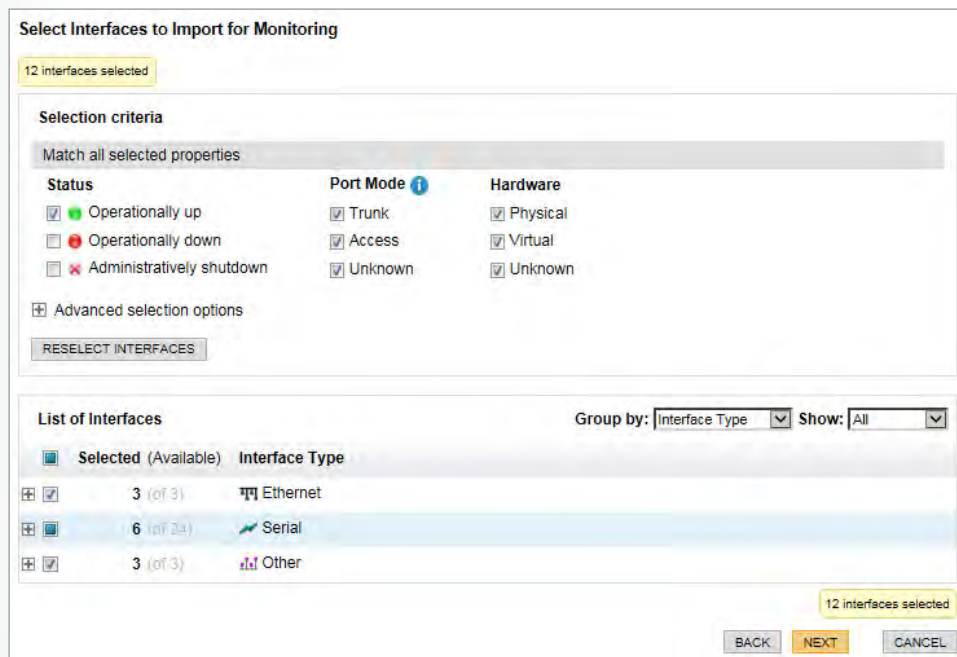
12. Click Next to confirm the changes.



13. On the next screen, you can select the interfaces to monitor.

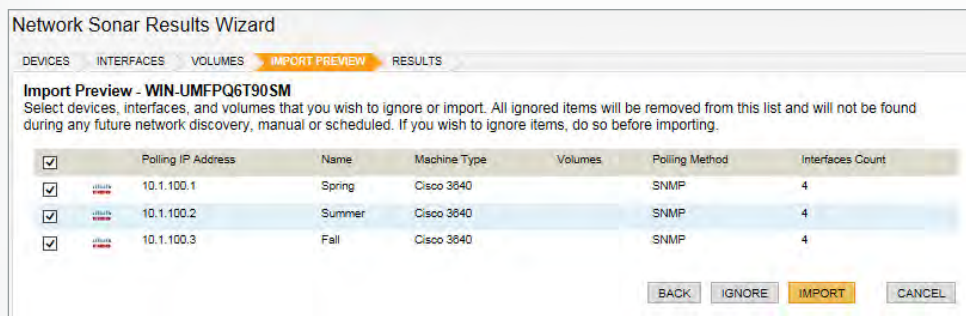
By default, all interfaces that are Up are selected. Once you've adjusted your choices, click Next.

NOTE: While NPM requires an IP address to monitor a device, non-routable interfaces (i.e.: interfaces that do NOT have IPs assigned) can still be monitored for availability, bandwidth, and more. In our example, you probably want to choose all the interfaces.

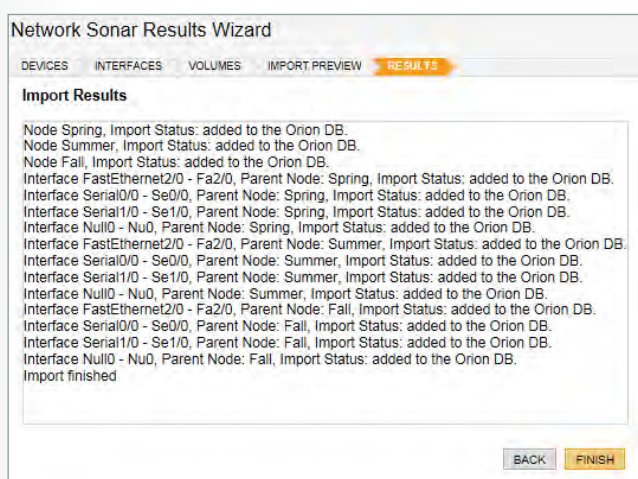


14. Because there are no volumes (disks) on this device, you can click Next to move past that screen.

15. On the final preview screen, make sure your devices are listed, and click Import.



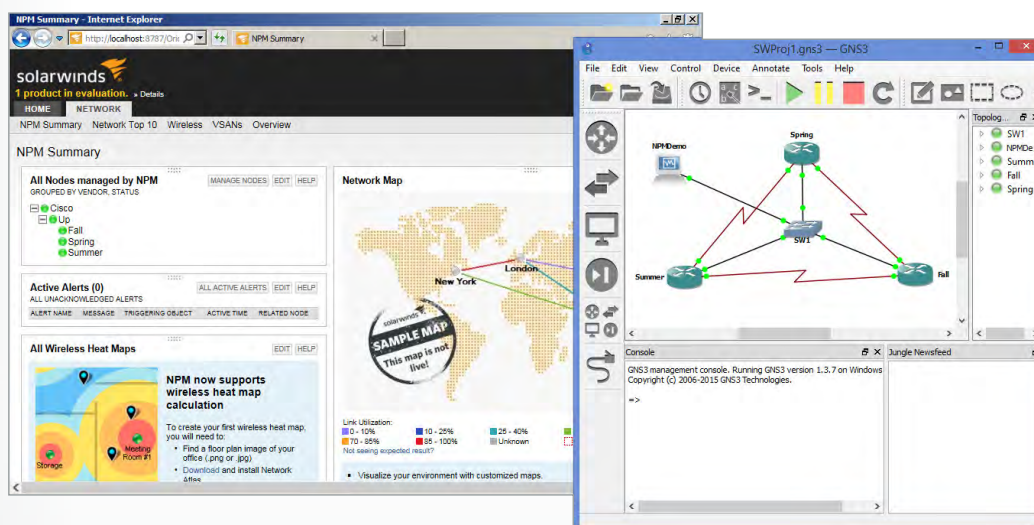
16. Once the import completes, click Finish.



17. Click Home to get back to the main screen.

SHAKE, CHILL, AND SERVE

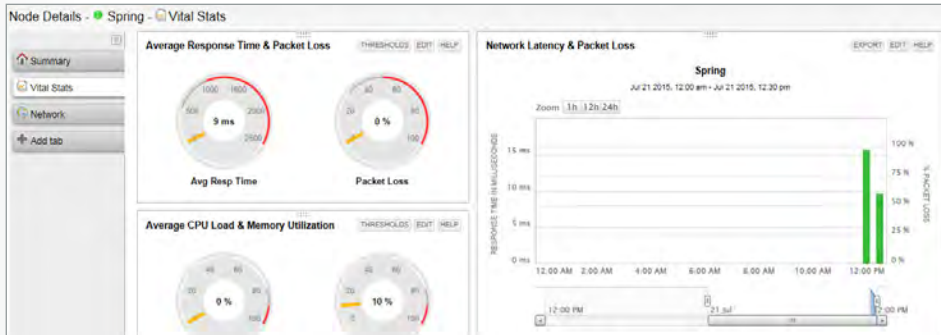
18. Congratulations! You're now up and running with a completely virtualized network that is monitored by a completely virtualized instance of SolarWinds NPM.



Appendix 1: Using SolarWinds® Network Performance Monitor

As mentioned earlier, exploring all the nooks and crannies of NPM is outside the scope of this document. However, here are a few items to whet your appetite for exploring the monitoring data available:

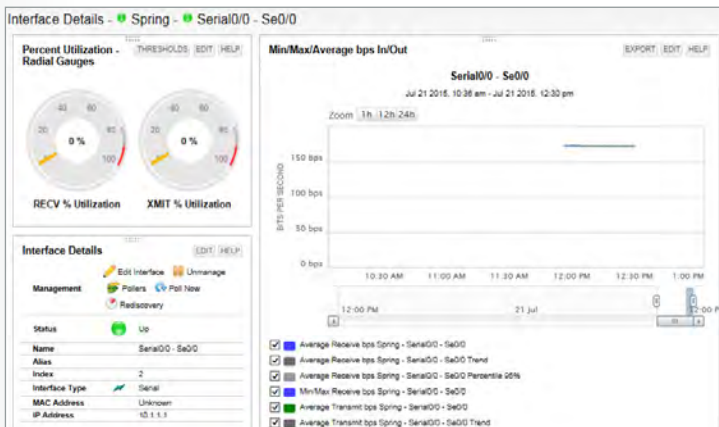
On the main screen, under “all nodes,” you can click any of the routers to get to the Node Details page:



“We decided to use SolarWinds based on it being a tool that was vendor agnostic and easy to use.”

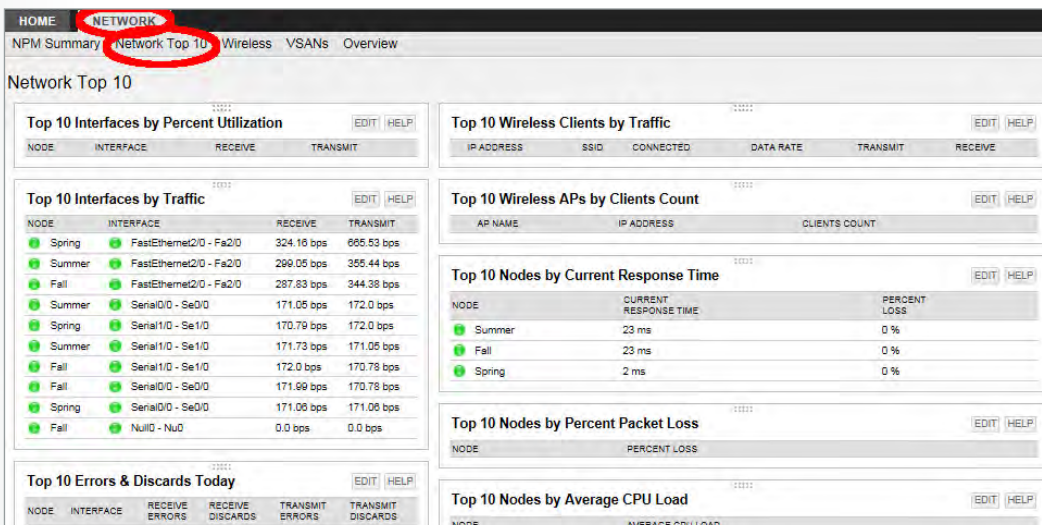
Daniel Cleary
Network program leader
Deakin University

This includes detailed information about each interface:



...as well as other elements on each box.

Under the Network tab, the Network Top 10 menu shows a variety of elements and data points that are useful to the network professional.



“We have a high level of visibility of each device and recent changes made to it. The visibility helps us to understand the root cause of each incident.”

Daniel Cleary
Network program leader
Deakin University

SUMMARY

Obviously, this is only scratching the surface of what you can do.

For more help getting started with NPM, check out these resources:

- [NPM Interactive Demo](#)
- [NPM Core Training](#)
- [Administrator Guide](#)

With regard to SolarWinds, it's entirely possible to install additional SolarWinds modules, such as Network Configuration Manager (NCM), Server & Application Monitor (SAM), and even NetFlow™ Traffic Analyzer (NTA) to test each of those capabilities within a safe sandbox environment.

On the GNS3 side, as long as you have images, you can add a wide variety of routers, switches, ASAs, and IDSs from Cisco, as well as Jupiter® M-series boxes. This lets you mimic a significant aspect of most production networks.

Finally, VirtualBox will permit you to create VMs for practically any version of Windows and Linux, which also opens the door to a variety of appliances built on those OSs.

Enjoy enhancing and exploring this new option for creating reliable test environments for both your network and your monitoring solutions.

TOP 5 NETWORK TROUBLESHOOTING & MONITORING TOOLS

Network Performance Monitor

- Speeds network troubleshooting
- Monitors response time, availability, and performance
- Calculates network latency
- Automatically discovers and maps network devices

[DOWNLOAD FREE TRIAL »](#)

Fully Functional For 30 Days

Bandwidth Analyzer Pack

- Detect, diagnose, and resolve network performance issues
- Track response time & availability of SNMP-enabled devices
- Analyze and monitor network bandwidth and traffic patterns
- Graphically display network performance metrics in real time

[DOWNLOAD FREE TRIAL »](#)

Fully Functional For 30 Days

NetFlow Traffic Analyzer

- Monitors network bandwidth & traffic patterns
- Identifies users, applications & protocols consuming bandwidth
- Highlights IP addresses of top talkers
- Analyzes Cisco® NetFlow™, Juniper® J-Flow & other flow data

[DOWNLOAD FREE TRIAL »](#)

Fully Functional For 30 Days

IP Address Manager

- Centralized IP infrastructure management and monitoring
- Proactively monitors your IP resources with alerts and reports
- Active IP address conflict detection and preventive alerts
- Delivers real-time dashboard visibility along with historical IP tracking

[DOWNLOAD FREE TRIAL »](#)

Fully Functional For 30 Days

Network Configuration Manager

- Enables bulk change deployment to thousands of devices
- Performs automatic, scheduled network configuration backups
- Protects against unauthorized & erroneous network changes
- Detects & reports on network compliance policy violations

[DOWNLOAD FREE TRIAL »](#)

Fully Functional For 30 Days