

# Lab 10: HP Networks Node Manager

NET311 - Computer Network Management

Instructor: Dr. Mostafa Dahshan

## Objectives

1. Deploy Network Management System Software.
2. Install and configure HP NNMi.
3. Troubleshoot network problems.

## References

1. [HP NNMi](#).
2. [Configuring Communication Protocol](#).

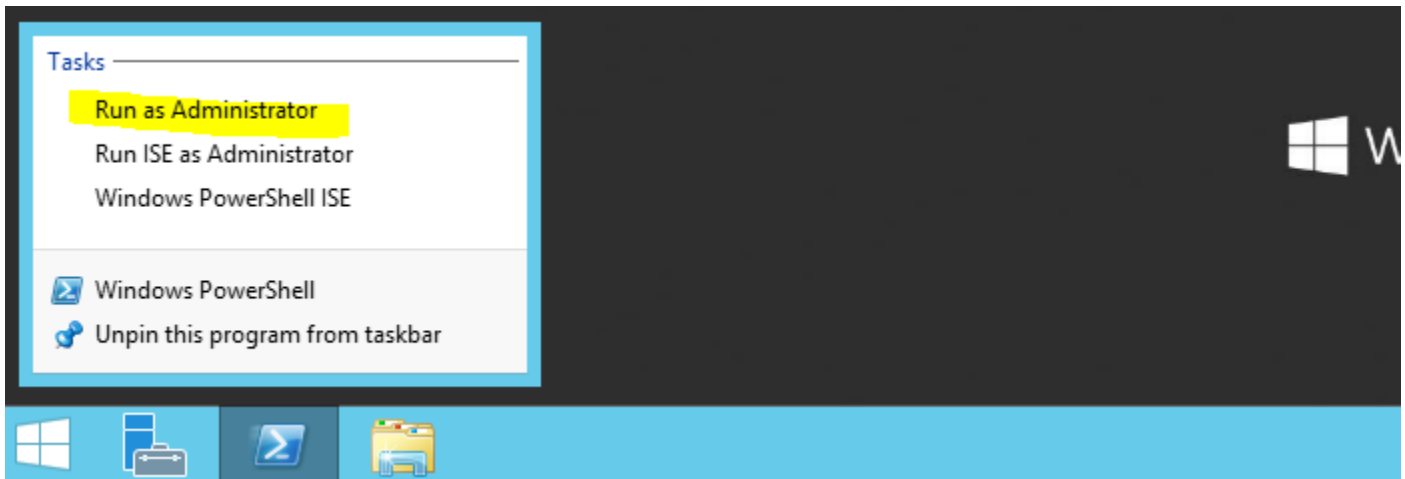
## Instructions

1. Read the lab instructions.
2. Provide question answers and screenshots in the supplied answer sheet.
3. After finishing the lab, upload your saved answer sheet to LMS.

## Part 1: Lab Setup

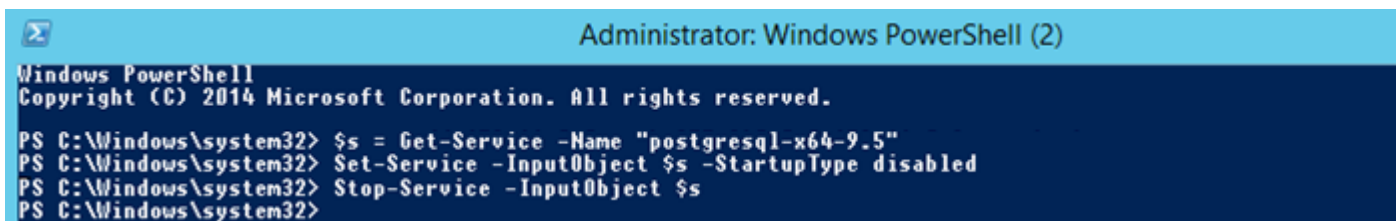
The lab setup required is the same as the lab setup for Lab 5. If you have not performed Lab 5, you must perform Part 1 in Lab 5 before completing this lab.

### 1. Run **PowerShell** as **Administrator**.



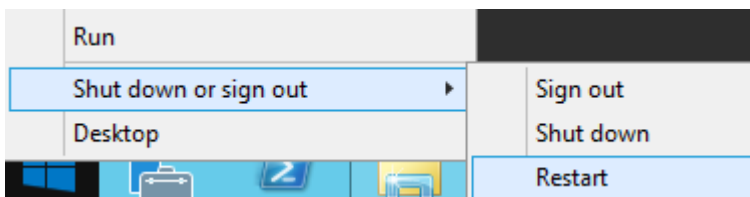
2. Type the following commands to stop the PostgreSQL service. This is important because this service conflicts with the PostgreSQL database used in HP NNMi.

```
$s = Get-Service -Name "postgresql-x64-9.5"
Set-Service -InputObject $s -StartupType disabled
Stop-Service -InputObject $s
```

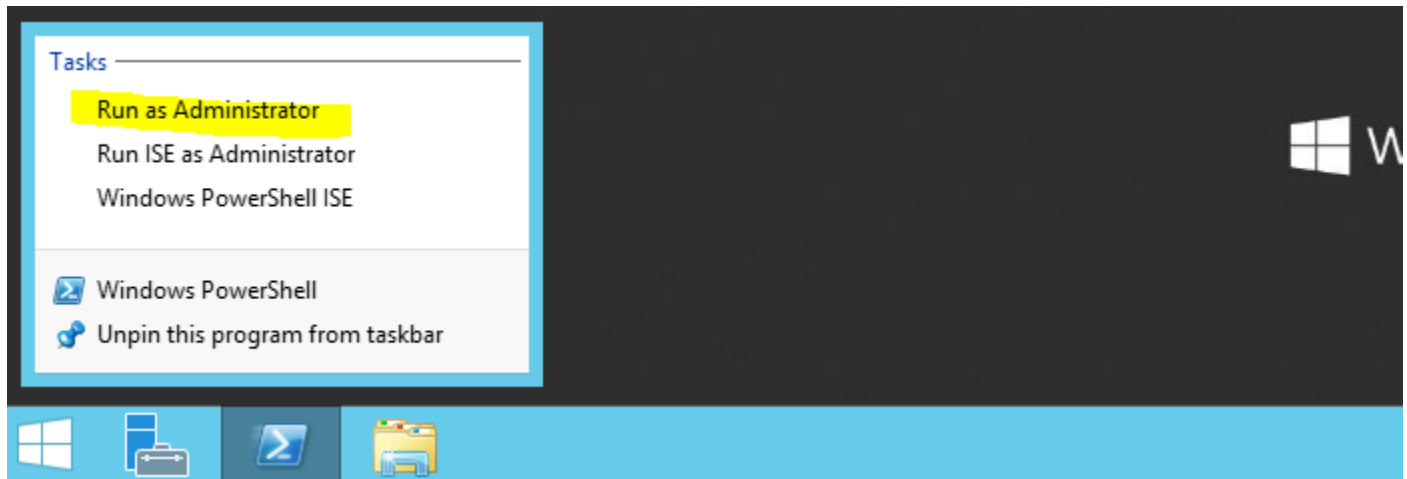


Lab sheet 1.1: provide a screenshot of the PowerShell screen.

### 3. Save your lab sheet, then restart the computer.



4. Run **PowerShell** as **Administrator**.



5. Type the following command to configure the route to the lab network:

```
Route add 172.16.0.0 mask 255.240.0.0 172.16.0.2 metric 1
```

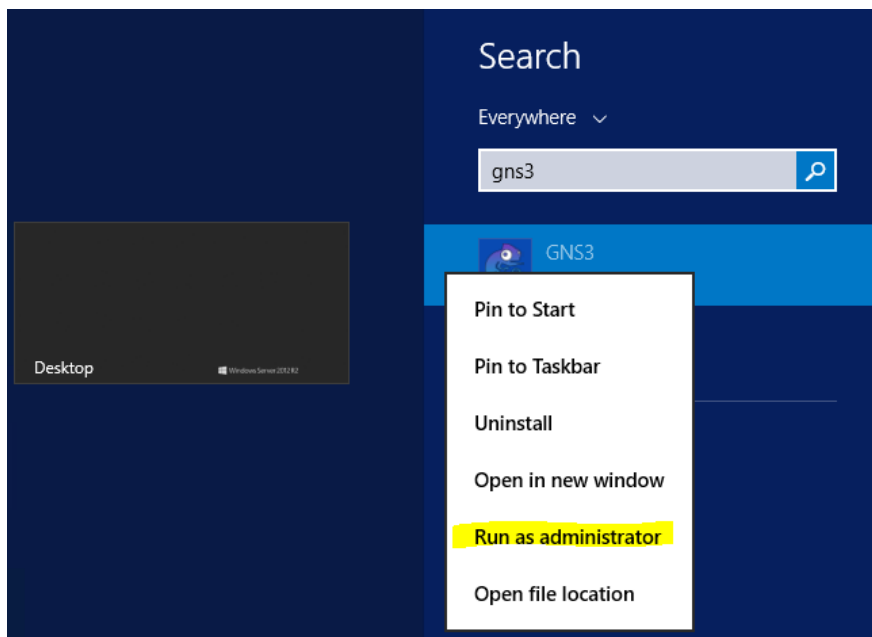
A screenshot of a Windows PowerShell command prompt window. The title bar is light blue and reads 'Administrator: Windows PowerShell (2)'. The window has a dark blue background with white text. The text shows the PowerShell prompt 'PS C:\Windows\system32>' followed by the command 'Route add 172.16.0.0 mask 255.240.0.0 172.16.0.2 metric 1'. The command is executed, and the output 'OK!' is displayed. The prompt returns to 'PS C:\Windows\system32>'.

```
Administrator: Windows PowerShell (2)
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

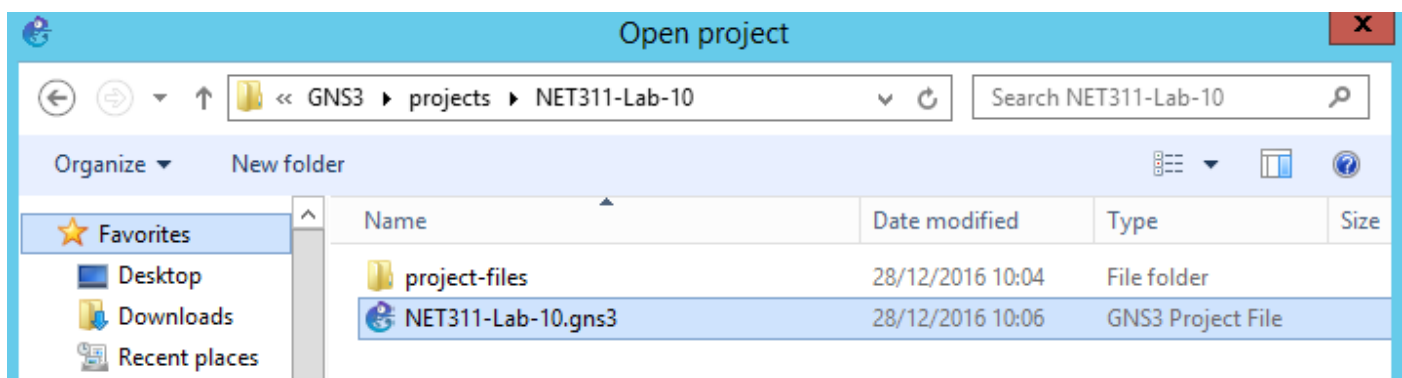
PS C:\Windows\system32> Route add 172.16.0.0 mask 255.240.0.0 172.16.0.2 metric 1
OK!
PS C:\Windows\system32>
```

## Part 2: Starting the Network

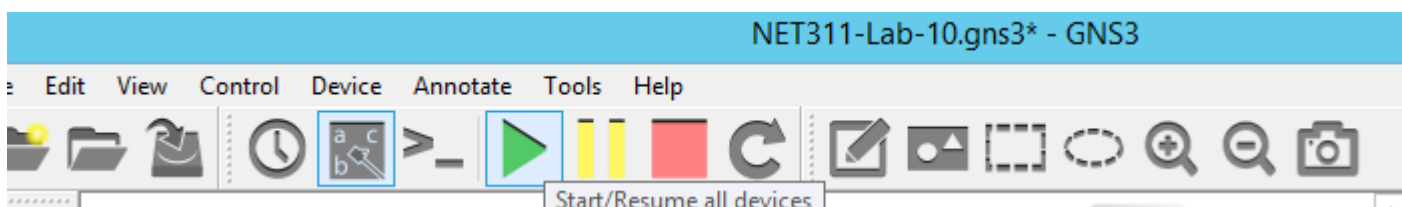
1. Run **GNS3** as an **administrator**.

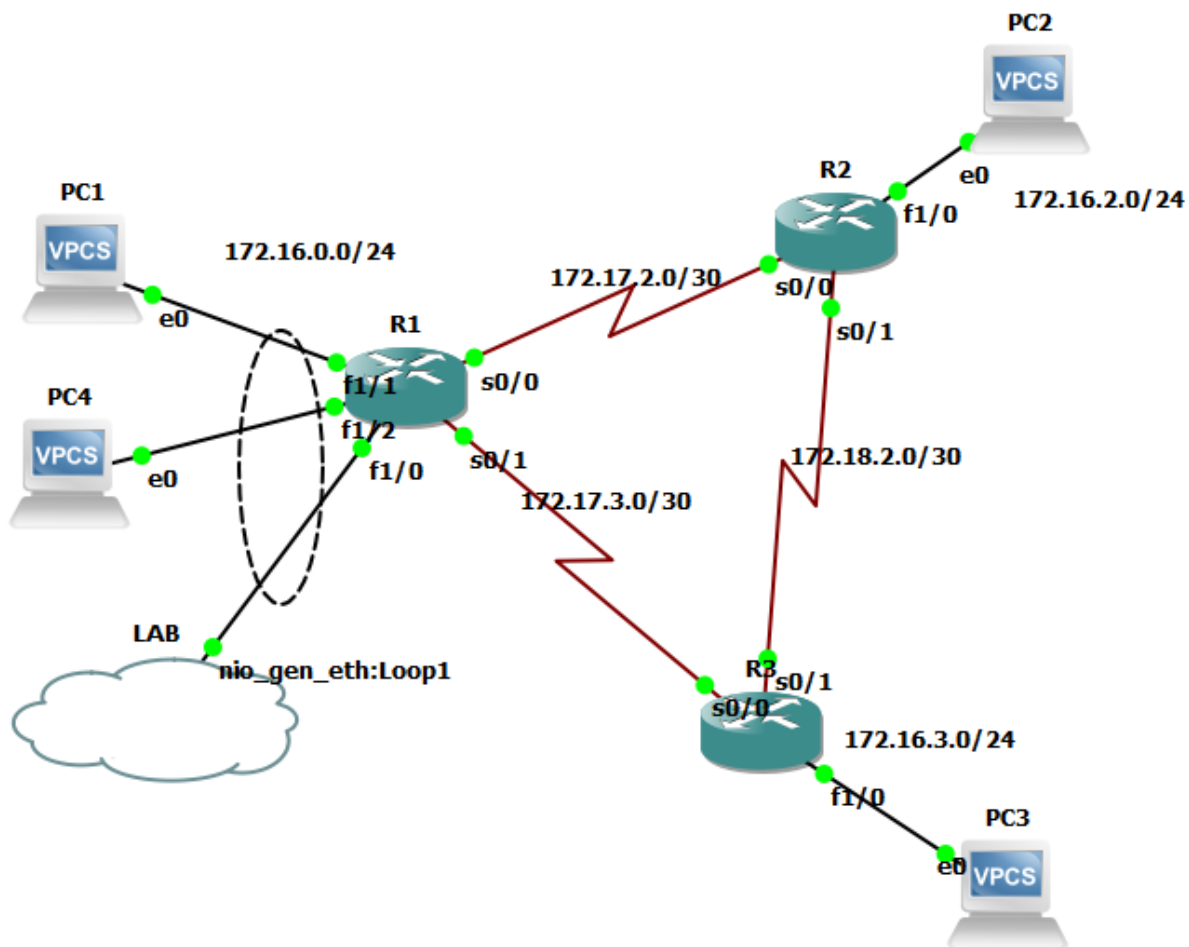


2. Open the GNS3 project **NET311-Lab-10-.gns3**.



3. Start all devices

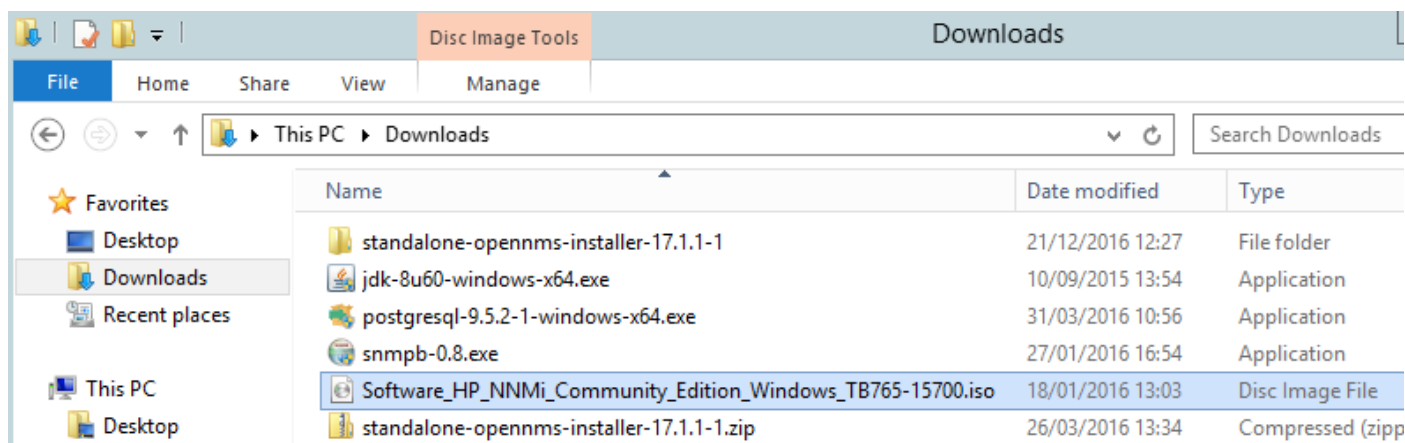




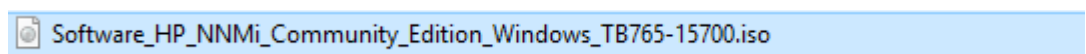
Lab sheet 2.1: provide a screenshot of the running network.

## Part 3: Install HP Network Node Manager

1. Locate the Disc image **Software\_HP\_NNMI\_Community\_Edition\_Windows\_TB765-15700.iso** under **Downloads**.



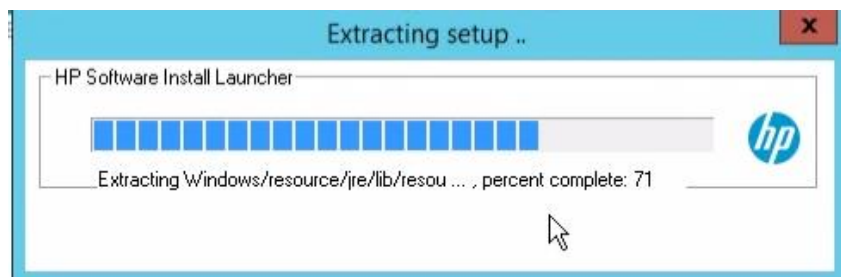
2. Double click on the image to mount it.



3. Locate and open the mounted DVD drive on your computer.



4. Start the **setup** program.



5. Follow the steps of the setup program. **Keep the default settings** unless otherwise specified.



6. In the System Account Password field, type **net311**.



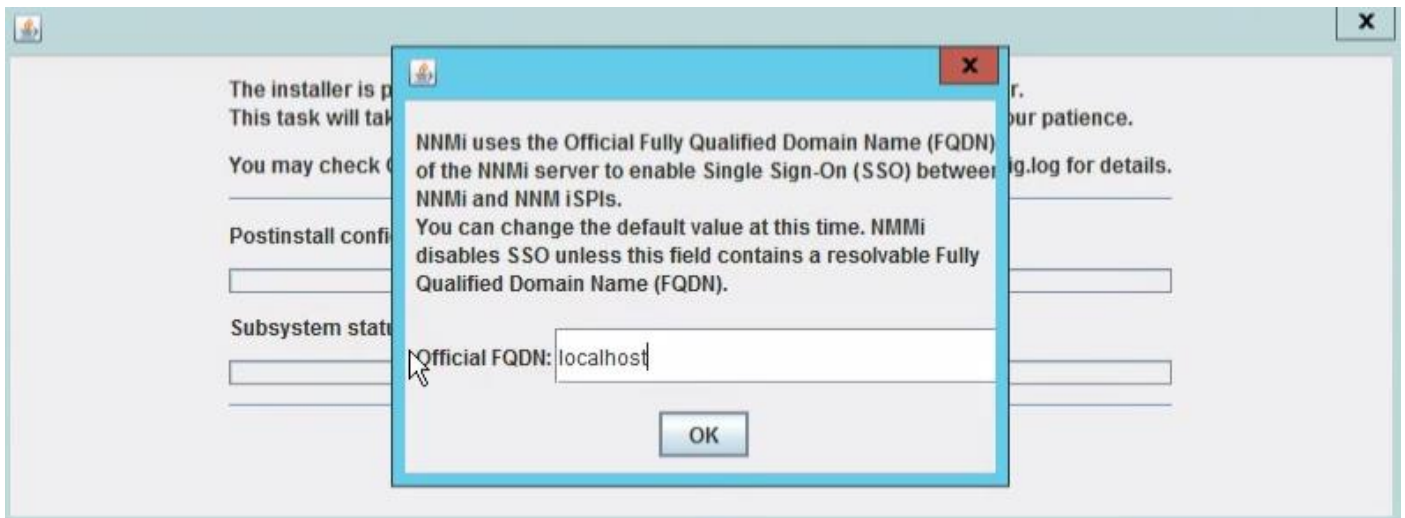
The dialog box is titled "System Account Password". It contains the following text: "You need an account to access the NNM Console. A default account 'system' has been created for you. You must change the password before you log on to the NNM Console." Below this text are three input fields: "Name" with the value "system", "Password" with masked characters "•••••", and "Retype Password" with masked characters "•••••". At the bottom are "OK" and "Cancel" buttons.

7. Keep the default ports 80 and 443.



Two side-by-side dialog boxes for port configuration. The left box has a "Port" field with the value "80" and an "OK" button. The right box has a "Port" field with the value "443" and an "OK" button.

8. In the Official FQDN field, type **localhost**.



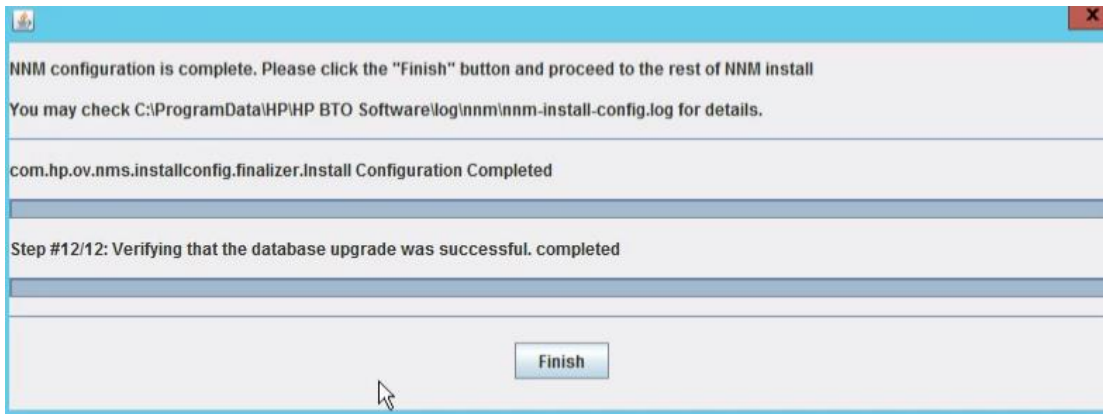
A dialog box titled "Official FQDN" is shown over a background window. The dialog box contains the following text: "NNMi uses the Official Fully Qualified Domain Name (FQDN) of the NNMi server to enable Single Sign-On (SSO) between NNMi and NNM iSPis. You can change the default value at this time. NNMi disables SSO unless this field contains a resolvable Fully Qualified Domain Name (FQDN)." Below the text is an input field labeled "Official FQDN:" with the value "localhost". An "OK" button is at the bottom.

9. Click on **Skip Patching**.



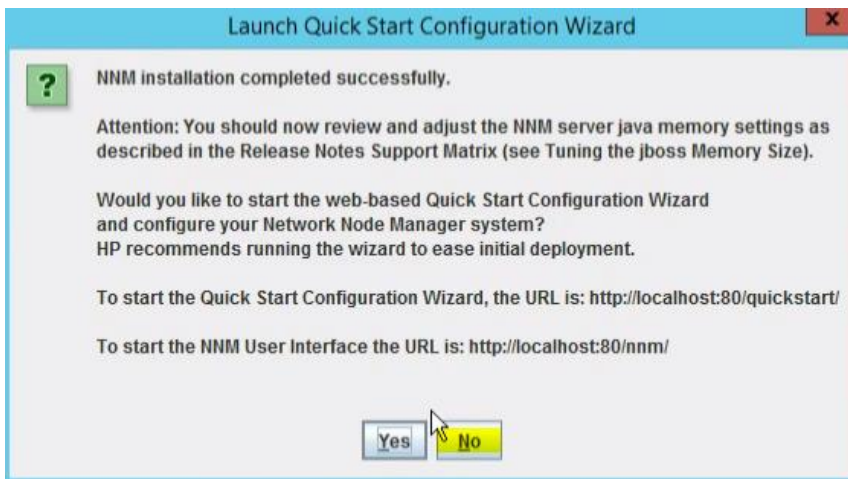
The dialog box is titled "NNMi Patch Install". It contains the following text: "NNMi Patches can additionally be installed before NNMi is started. If you have any NNMi patches to install at this time, please provide the directory path where the patch files are located." Below this text is a label "NNMi Patches Directory:" followed by an input field containing the path "D:\packages\patches". At the bottom are two buttons: "Skip Patching" and "Install Patches". A mouse cursor is pointing at the "Skip Patching" button.

10. Click on **Finish**.



Lab sheet 3.1: provide a screenshot showing the Finish screen of NNM setup.

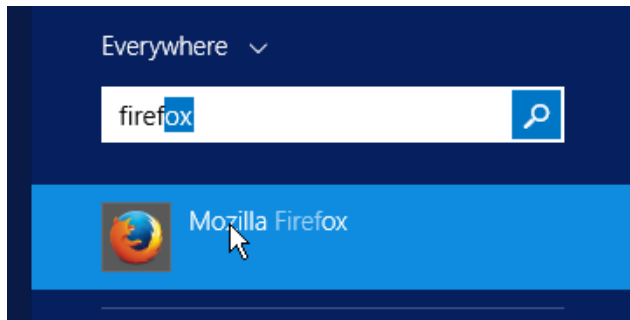
11. Click **No** to skip the Quick Start Configuration Wizard.



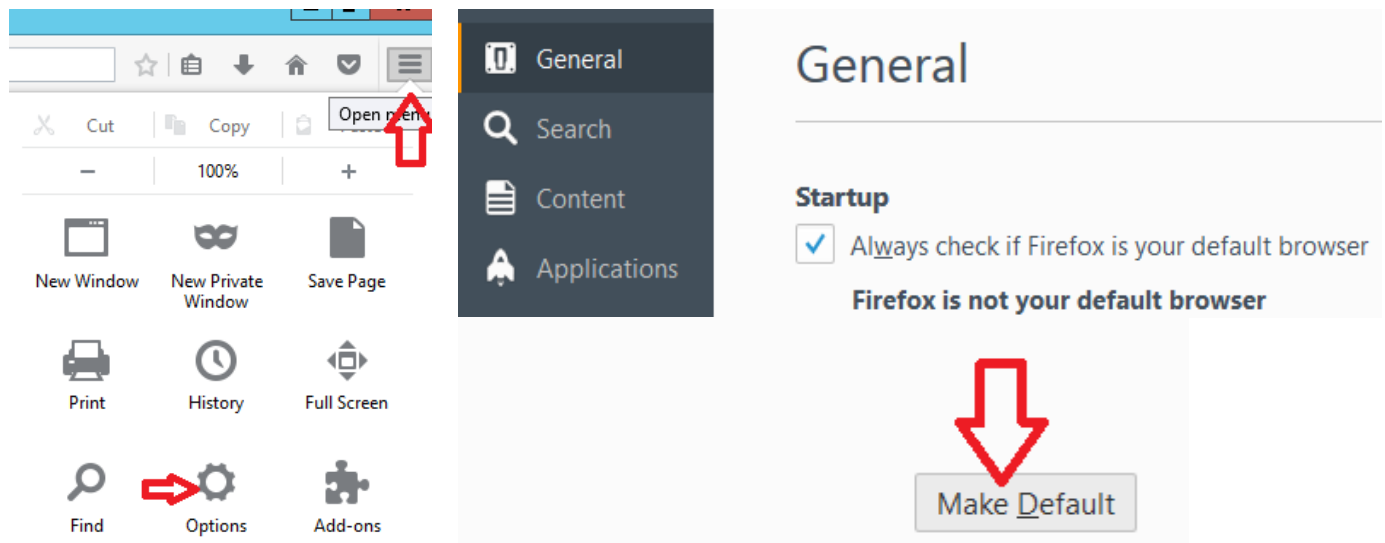


## Part 4: Configure HP NNM Communication and Discovery

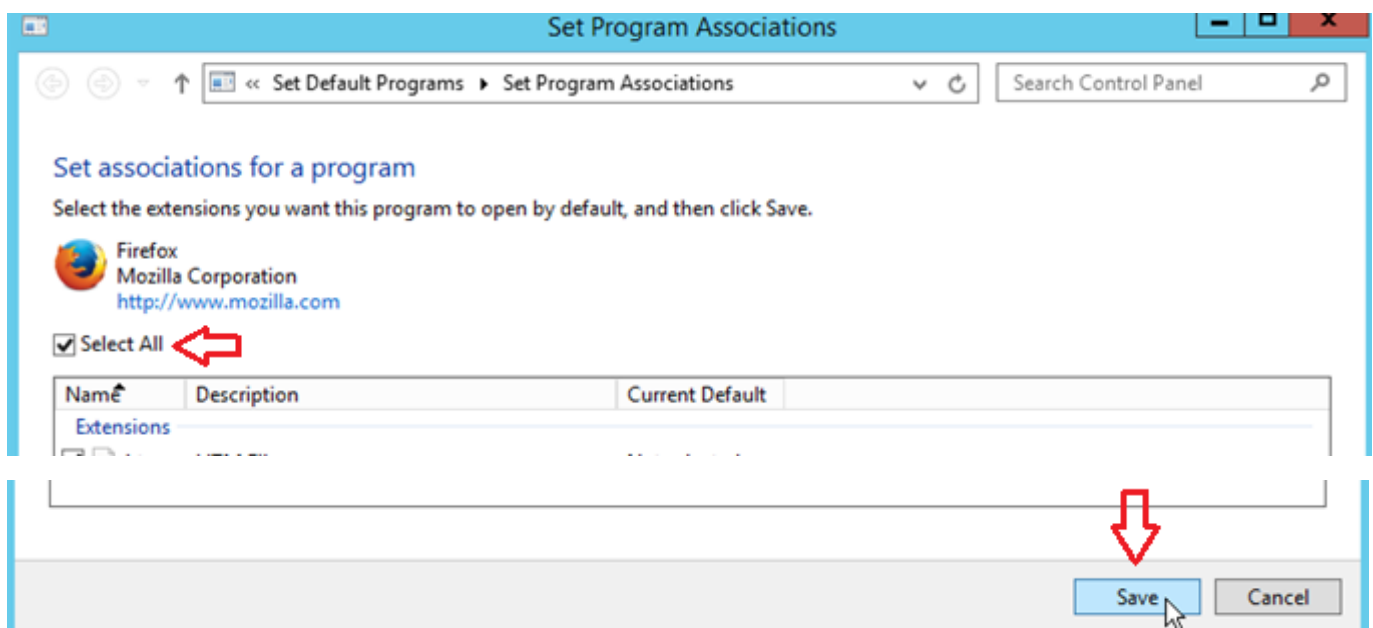
1. Run the Firefox web browser.



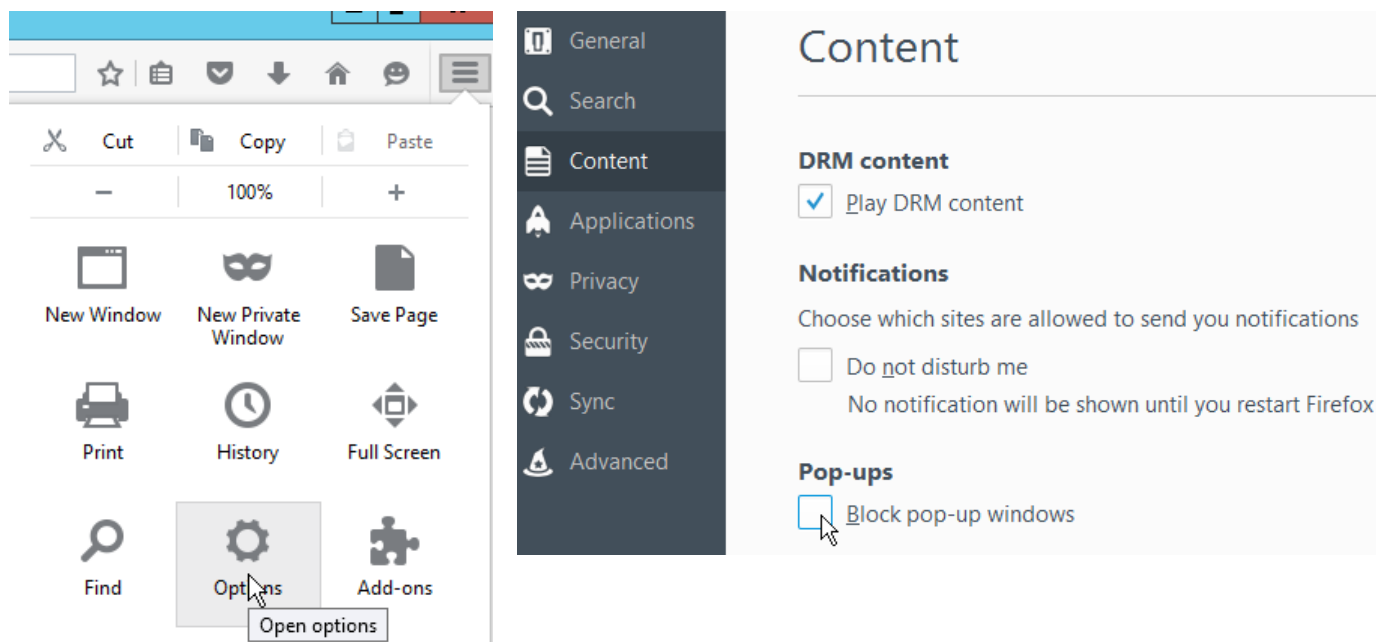
2. From the top right corner, open **Options**. In the **General** tab click on **Make Default**.



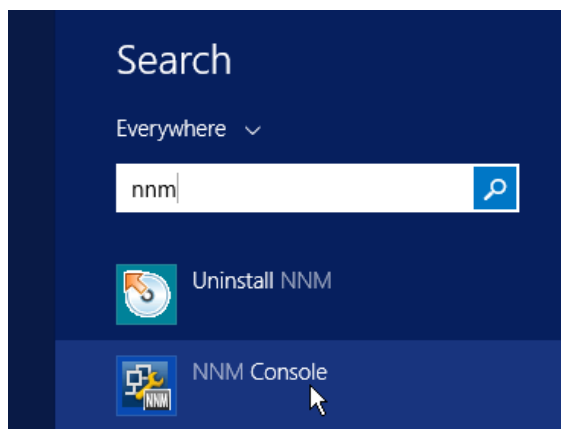
3. Check the **Select All**, then click **Save**.



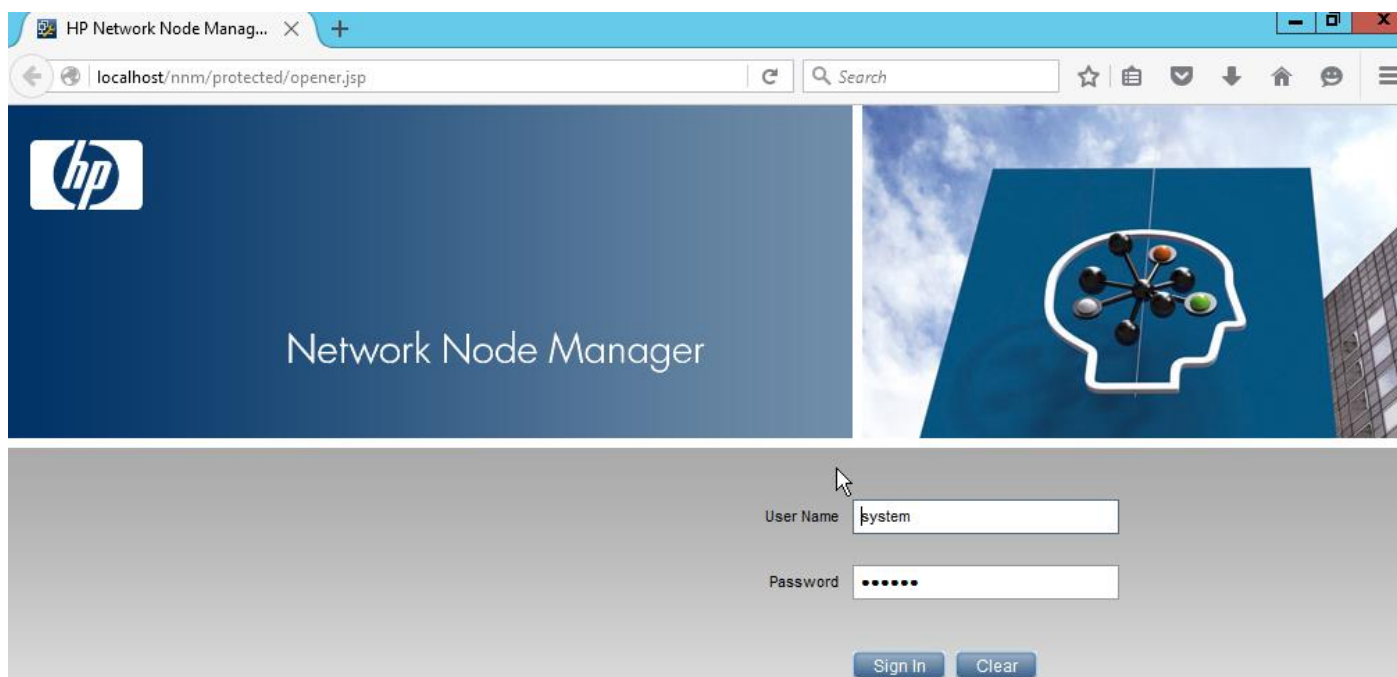
4. In the **Content** tab, uncheck the “Block pop-pup windows” option.



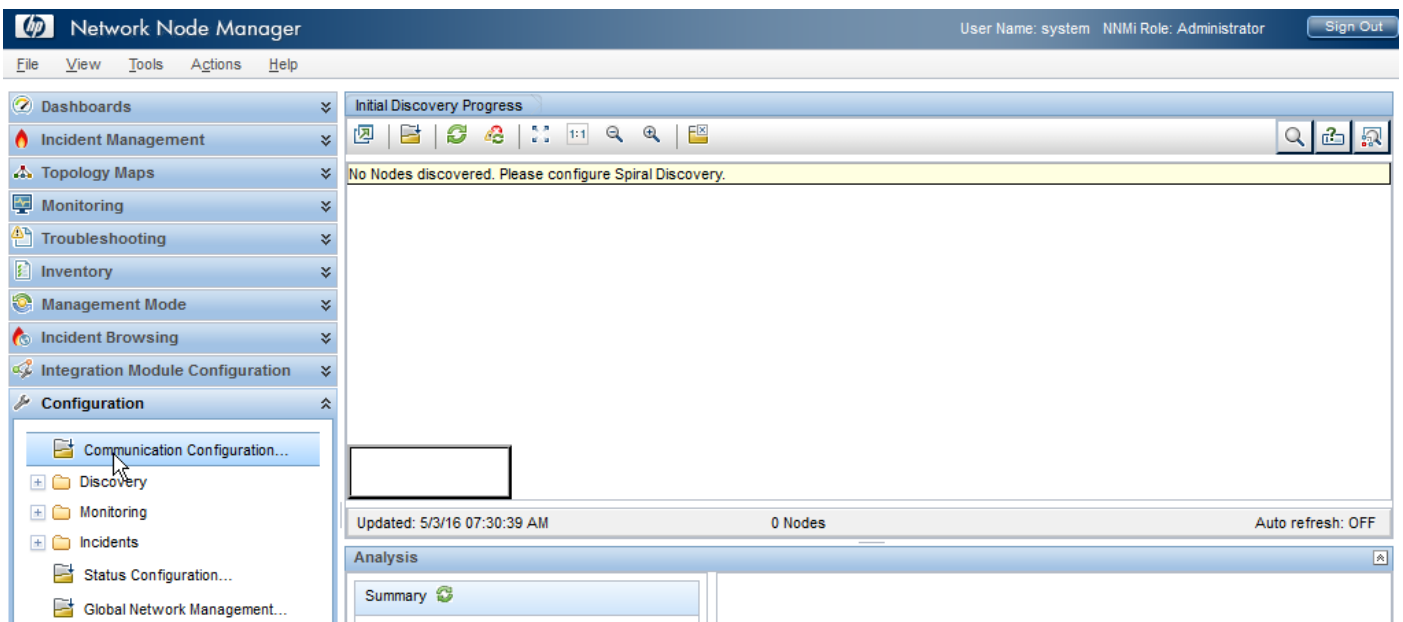
5. Locate and run the **NNM Console**.



6. Sign in with user name **system** and password **net311**.

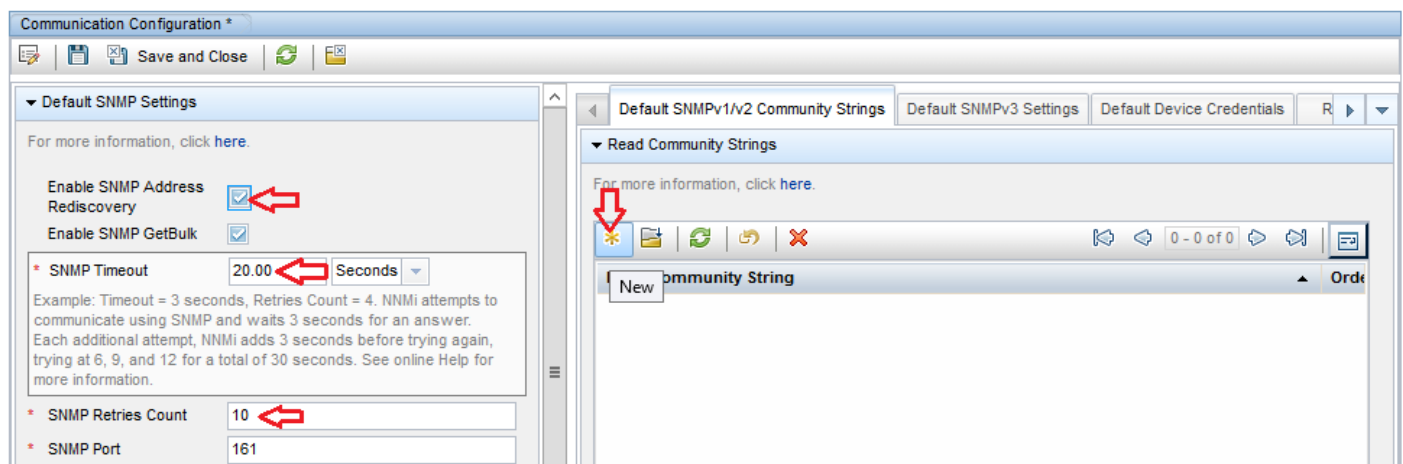


7. In the Network Node Manager window click on **Configuration** tab, then click on **Communication Configuration**.

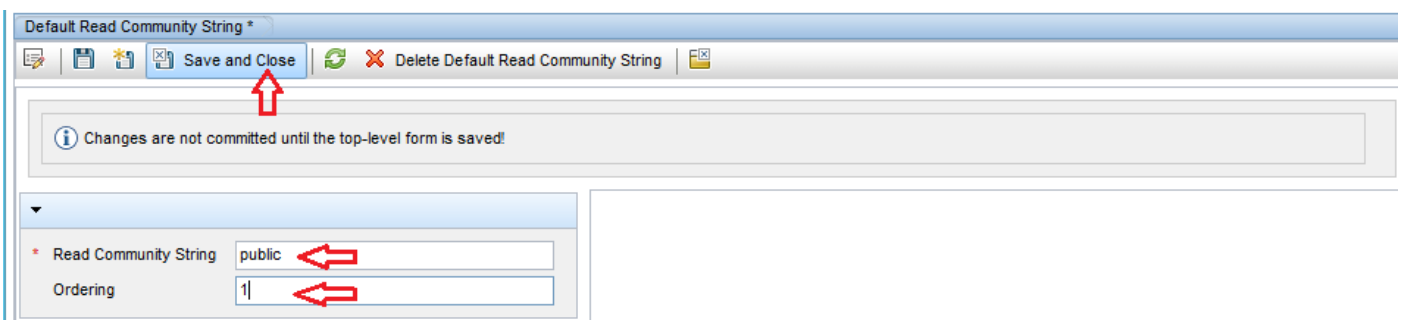


8. Check **Enable SNMP Address Rediscovery**. Set the **SNMP Timeout** to **20** and **SNMP Retries count** to **10**.

9. Click the **New** button under Default SNMPv1/v2 Community Strings.



10. Add the Read Community String **public** and Ordering **1**. Click on **Save and Close**.



11. In **Write Community String**, type **private** and **private**.

HP Network Node Manager i: LS1 - Mozilla Firefox

localhost/nnm/protected/showInNewWindow?cmd=showForm&formInfoId=communicationConfigurationFormInfo&entityClassName=com.hp.ov.nms.comm.config.model.c

File View Tools Actions Help

Communication Configuration \*

Save and Close

Default SNMP Settings

For more information, click [here](#).

Enable SNMP Address Rediscovery ☒

Enable SNMP GetBulk ☒

\* SNMP Timeout 20.00 Seconds

Example: Timeout = 3 seconds, Retries Count = 4. NNMI attempts to communicate using SNMP and waits 3 seconds for an answer. Each additional attempt, NNMI adds 3 seconds before trying again, trying at 6, 9, and 12 for a total of 30 seconds. See online Help for more information.

\* SNMP Retries Count 10

\* SNMP Port 161

SNMP Proxy Address

SNMP Proxy Port

\* SNMP Minimum Security Level Community

Management Address Selection

If you choose Seed IP / Management IP, NNMI uses the Seed IP only for initial discovery. Otherwise, NNMI uses the current Management Address. For more information, click [here](#).

\* First Choice Seed IP / Management IP

\* Second Choice Interface Matching

\* Third Choice Lowest Loopback IP

Interface Matching lo0

To limit management addresses to certain interfaces, type any index, name, alias, or description value (separate more than one with commas). For each node, NNMI searches for interface values (no wildcards, quotes, or commas) in this order: index, alias, name, and description.

\* IP Version Preference IPv4

Default SNMPv1/v2 Community Strings

Read Community Strings

For more information, click [here](#).

Read Community String

Community String	Order
public	1

Total: 1 Selected: 0 Filter: OFF Auto refresh: OFF

Write Community String (Set Community String)

For more information, click [here](#).

Write Community String

.....

.....

12. Scroll down then change the **ICMP Timeout** to **20** and **ICMP Retries Count** to **10**.

Communication Configuration \*

Save and Close

SNMP Proxy Address

SNMP Proxy Port

\* SNMP Minimum Security Level Community

Management Address Selection

If you choose Seed IP / Management IP, NNMI uses the Seed IP only for initial discovery. Otherwise, NNMI uses the current Management Address. For more information, click [here](#).

\* First Choice Seed IP / Management IP

\* Second Choice Interface Matching

\* Third Choice Lowest Loopback IP

Interface Matching lo0

To limit management addresses to certain interfaces, type any index, name, alias, or description value (separate more than one with commas). For each node, NNMI searches for interface values (no wildcards, quotes, or commas) in this order: index, alias, name, and description.

\* IP Version Preference IPv4

Default ICMP Settings

For more information, click [here](#).

\* ICMP Timeout 20.00 Seconds

\* ICMP Retries Count 10

ICMP works the same way as SNMP timeout and retries count, see online Help for more information.

Default SNMPv1/v2 Community Strings

Read Community Strings

For more information, click [here](#).

Read Community String

Community String	Order
public	1

Total: 1 Selected: 0 Filter: OFF Auto refresh: OFF

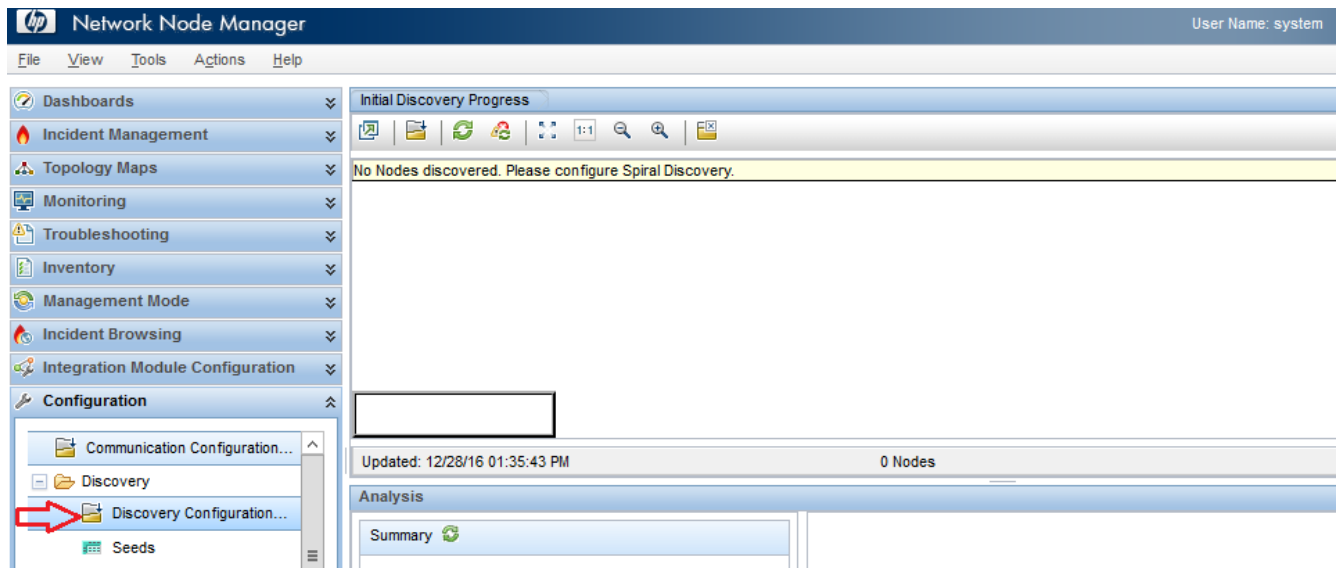
Write Community String (Set Community String)

For more information, click [here](#).

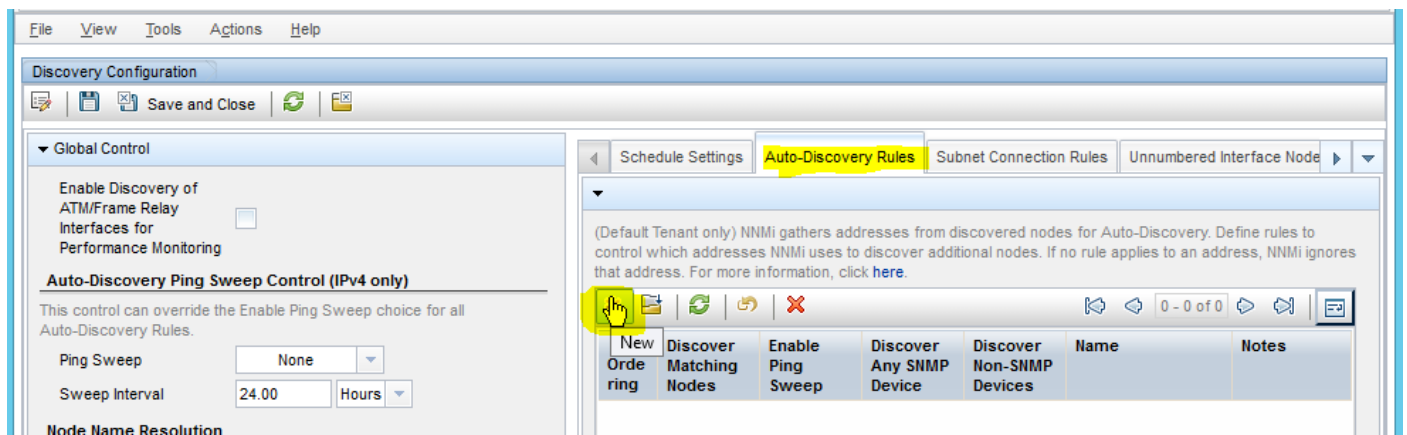
Lab sheet 4.1: provide a screenshot showing the Communication Configuration screen.

13. Click on **Save and Close**.

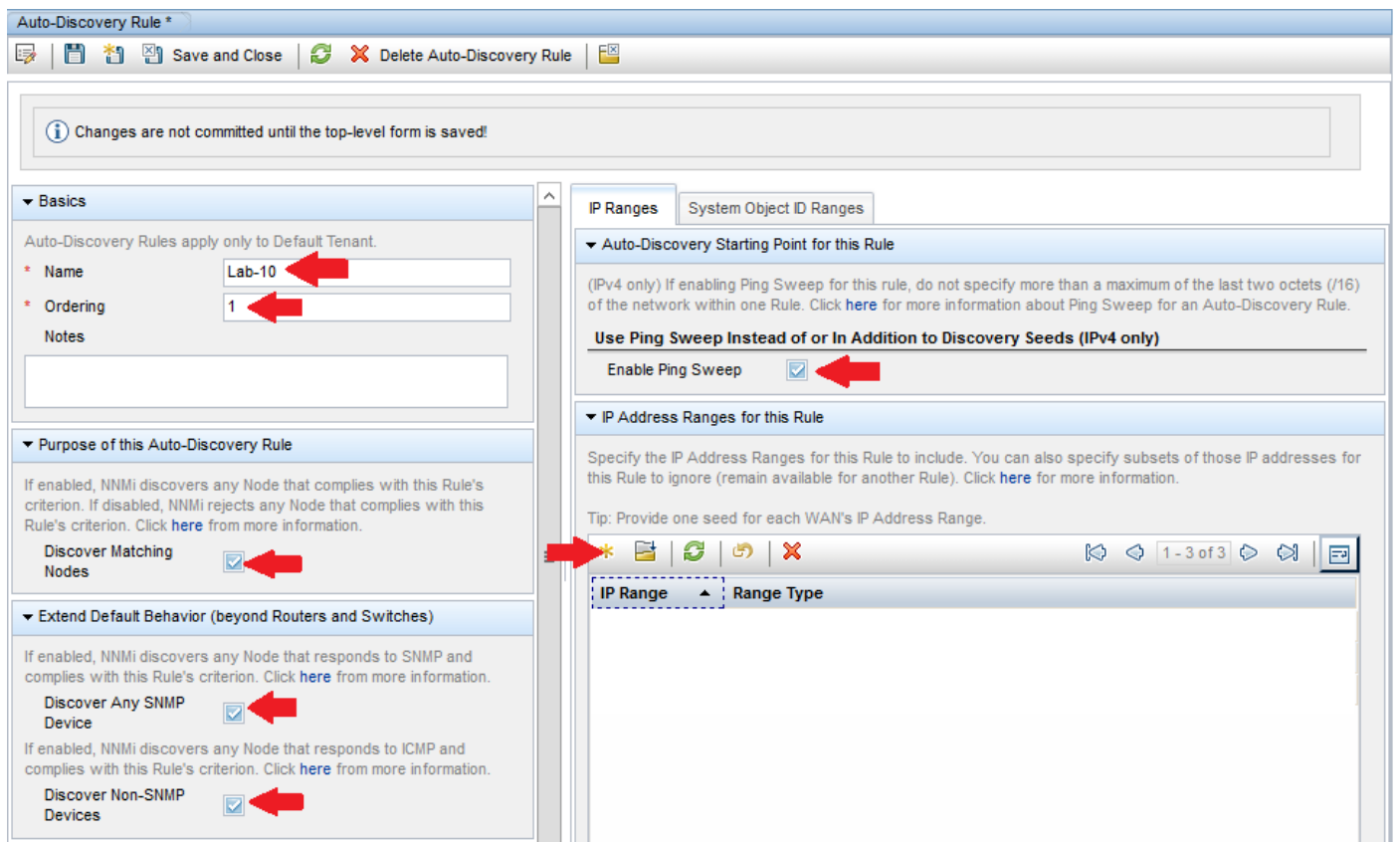
14. Click on **Discovery** then click on **Discovery Configuration**.



15. Open the **Auto-Discovery Rules** tab, then click on **New**.



16. Add the Name **Lab-10**, Ordering **1**. Check the options **Discover Any SNMP Device**, **Discover Non-SNMP Devices** and **Enable Ping Sweep**. Then click **New**.

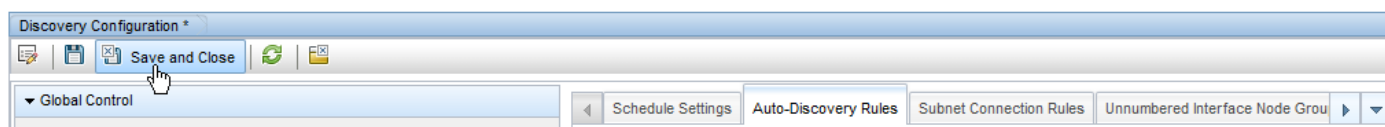


17. Add the IP Ranges **172.16.0.0/24**, **172.16.2.0/24**, **172.16.3.0/24**. Click **Save and Close**.

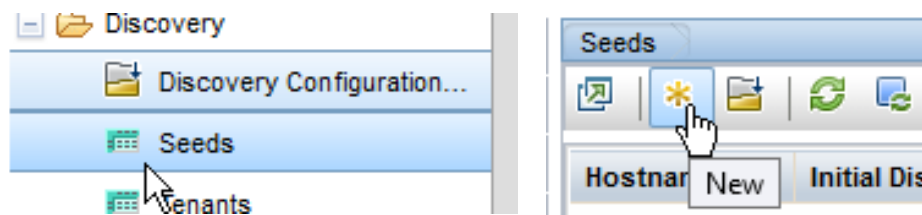
Lab sheet 4.2: provide a screenshot showing the Auto-Discovery Rule screen.

18. In the Auto-Discovery Rule window, click **Save and Close**.

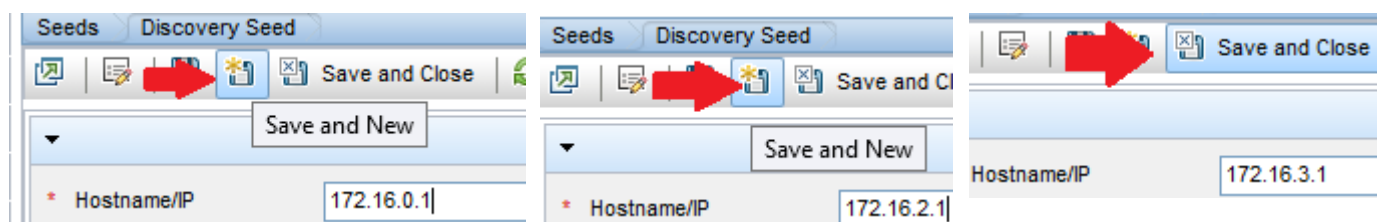
19. In the Discovery Configuration window, click **Save and Close**.



20. Click on **Discovery** then click on **Seeds**. Then click on **New**.



21. Enter Hostname/IP values: **172.16.0.1**, **172.16.2.1** and **172.16.3.1**. Click **Save and Close**.



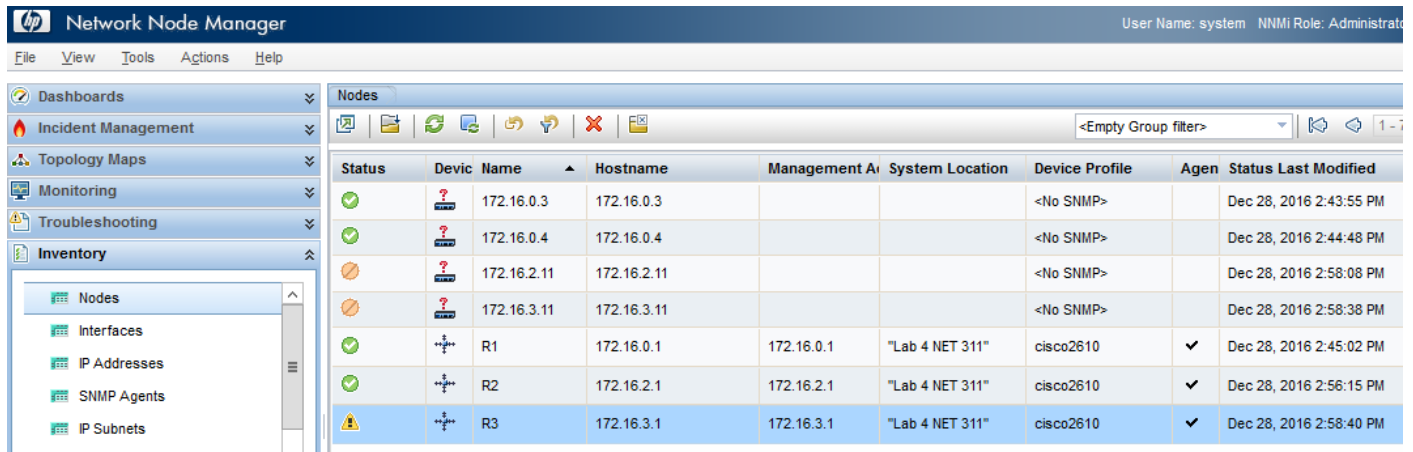
Seeds				
Hostname/IP▲	Initial Discovery Ter	Discovery Seed Results	Last Modified	Notes
172.16.0.1		Node not created (duplicate seed)	Dec 28, 2016 2:40:10 PM	
172.16.2.1		In progress	Dec 28, 2016 2:42:58 PM	
172.16.3.1		In progress	Dec 28, 2016 2:43:48 PM	

Lab sheet 4.3: provide a screenshot showing the Seeds screen.




## Part 5: Inspect Network Devices using HP NNM

1. Click on **Inventory**, then click on **Nodes**.

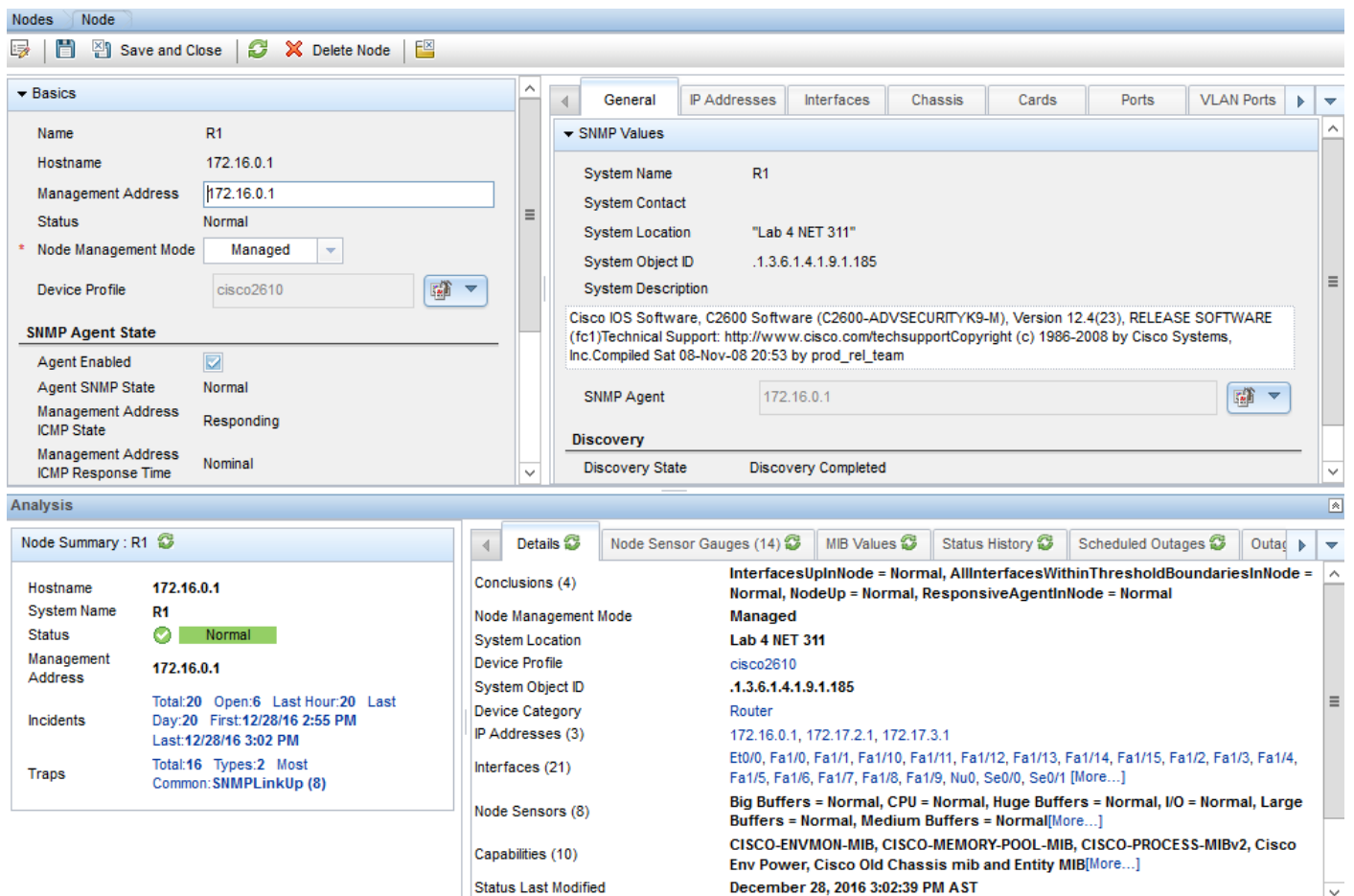


Status	Device	Name	Hostname	Management Address	System Location	Device Profile	Agent	Status Last Modified
✓	?	172.16.0.3	172.16.0.3			<No SNMP>		Dec 28, 2016 2:43:55 PM
✓	?	172.16.0.4	172.16.0.4			<No SNMP>		Dec 28, 2016 2:44:48 PM
✗	?	172.16.2.11	172.16.2.11			<No SNMP>		Dec 28, 2016 2:58:08 PM
✗	?	172.16.3.11	172.16.3.11			<No SNMP>		Dec 28, 2016 2:58:38 PM
✓	+	R1	172.16.0.1	172.16.0.1	"Lab 4 NET 311"	cisco2610	✓	Dec 28, 2016 2:45:02 PM
✓	+	R2	172.16.2.1	172.16.2.1	"Lab 4 NET 311"	cisco2610	✓	Dec 28, 2016 2:56:15 PM
✗	+	R3	172.16.3.1	172.16.3.1	"Lab 4 NET 311"	cisco2610	✓	Dec 28, 2016 2:58:40 PM

Lab sheet 5.1: provide a screenshot showing the Nodes screen.

2. Double click on **R1** and view its information. You can view in a separate window by clicking on .

3. Browse the different tabs on R1.



**Basic Information**

Name: R1  
Hostname: 172.16.0.1  
Management Address: 172.16.0.1  
Status: Normal  
Node Management Mode: Managed  
Device Profile: cisco2610

**SNMP Agent State**

Agent Enabled: ☒  
Agent SNMP State: Normal  
Management Address: Responding  
ICMP State: Nominal  
Management Address: Nominal

**Analysis**

**Node Summary : R1**

Hostname: 172.16.0.1  
System Name: R1  
Status: Normal  
Management Address: 172.16.0.1  
Incidents: Total: 20 Open: 6 Last Hour: 20 Day: 20 First: 12/28/16 2:55 PM Last: 12/28/16 3:02 PM  
Traps: Total: 16 Types: 2 Most Common: SNMPLinkUp (8)


**Details**

Conclusions (4)  
Node Management Mode: Managed  
System Location: Lab 4 NET 311  
Device Profile: cisco2610  
System Object ID: .1.3.6.1.4.1.9.1.185  
Device Category: Router  
IP Addresses (3): 172.16.0.1, 172.17.2.1, 172.17.3.1  
Interfaces (21): Et0/0, Fa1/0, Fa1/1, Fa1/10, Fa1/11, Fa1/12, Fa1/13, Fa1/14, Fa1/15, Fa1/2, Fa1/3, Fa1/4, Fa1/5, Fa1/6, Fa1/7, Fa1/8, Fa1/9, Nu0, Se0/0, Se0/1 [More...]  
Node Sensors (8): Big Buffers = Normal, CPU = Normal, Huge Buffers = Normal, I/O = Normal, Large Buffers = Normal, Medium Buffers = Normal [More...]  
Capabilities (10): CISCO-ENVMON-MIB, CISCO-MEMORY-POOL-MIB, CISCO-PROCESS-MIBv2, Cisco Env Power, Cisco Old Chassis mib and Entity MIB [More...]  
Status Last Modified: December 28, 2016 3:02:39 PM AST

4. Click on the **Interfaces** tab of R1. You can view it in a separate window by clicking on .

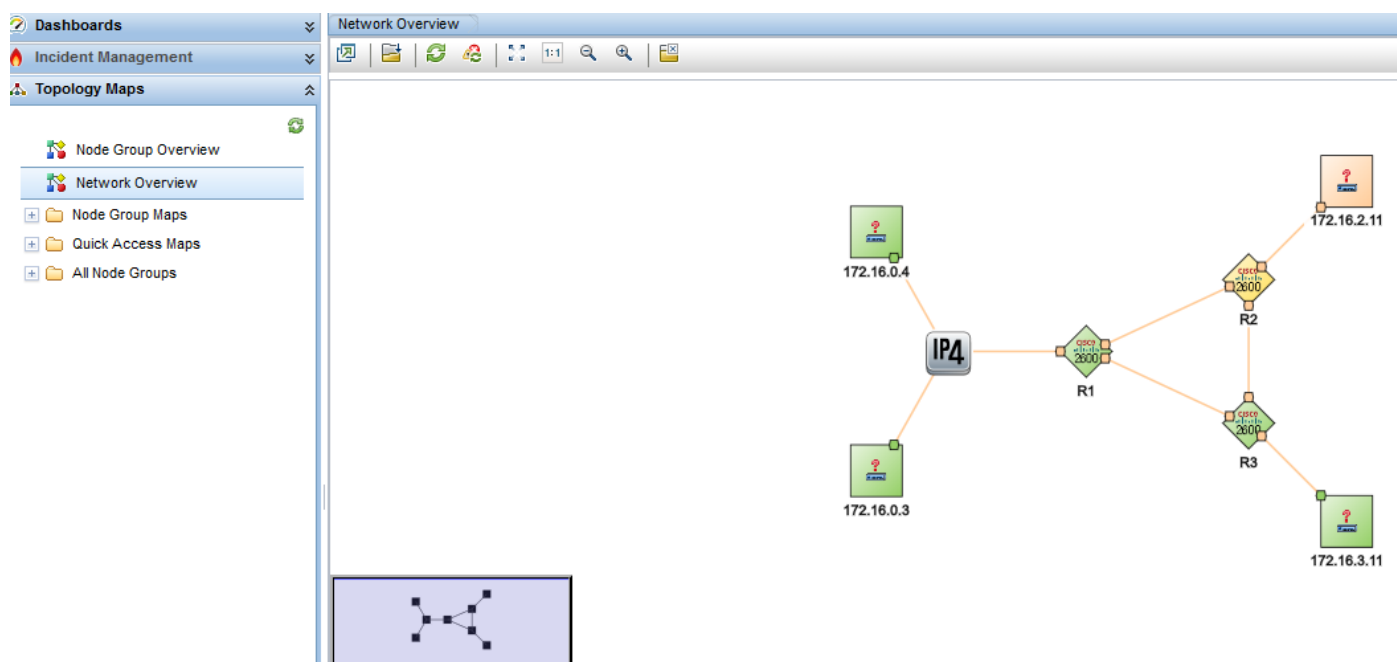
Status	Admi	Oper	ifName	ifType	ifSpeed	ifIndex	ifAlias	Physical Address	Layer 2 Conn
			Se0/1	propPointToPointS	1.5 Mbps	3			Small Subnets-
			Se0/0	propPointToPointS	1.5 Mbps	2			Small Subnets-
			Vl1	ethernetCsmacd	100 Mbps	21		C8010AE00000	
			Fa1/15	ethernetCsmacd	100 Mbps	19		C8011410F10F	
			Nu0	other	10 Gbps	20			
			Fa1/0	ethernetCsmacd	100 Mbps	4		C8011410F100	

Lab sheet 5.2: provide a screenshot showing the Interfaces of ESW1.

5. Close the Interfaces window by clicking on .

Status	Admi	Oper	Name	ifType	ifSpeed	ifIndex	ifAlias	Physical Address	Layer 2 Connection
--------	------	------	------	--------	---------	---------	---------	------------------	--------------------

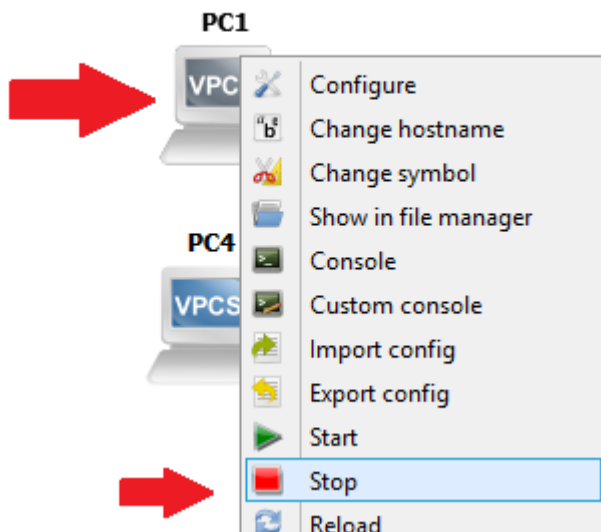
6. Under **Topology Maps**, click on **Network Overview**.



Lab sheet 5.3: provide a screenshot showing the Network Overview screen.

## Part 6: Network Troubleshooting using HP NNM

1. **Stop** one of the nodes in the network, for example **PC1**.



2. Under **Incidents**, click on **All incidents** and locate the **Node Down** incident for the IP of PC1.

The screenshot shows the HP NNM Incidents screen. The left sidebar lists various incident categories, with 'All Incidents' selected. The main area displays a table of incidents, with the 'Node Down' incident for IP 172.16.0.3 highlighted. Below the table, the 'Analysis' section provides details for the selected incident.

Severity	Priority	Lifecycle	Last Occurrence Time	Assigned To	Source Node	Source Object	Category	Family	Origin	Correlation Nature	Message
Critical	5	Registered	12/28/16 3:38:57 PM		172.16.0.3	172.16.0.3	Fault	Node	NNMi	Root Cause	Node Down
Info	5	Registered	12/28/16 3:38:40 PM		R3	Se0/1	Fault	Node	NNMi	Root Cause	Agent Interface Up (linkUp Trap) on interface 3
Info	5	Registered	12/28/16 3:38:39 PM		R3	Se0/0	Fault	Node	NNMi	Root Cause	Agent Interface Up (linkUp Trap) on interface 2
Info	5	Registered	12/28/16 3:38:39 PM		R3	Se0/0	Fault	Node	NNMi	Root Cause	Duplicate Correlation for SNMPLinkUp: Agent Interface Up (linkUp Trap) on interface 2
Info	5	Registered	12/28/16 3:38:21 PM		R1	Se0/1	Fault	Node	NNMi	Root Cause	Agent Interface Up (linkUp Trap) on interface 3

Updated: 12/28/16 03:42:04 PM Total: 156 Selected: 1 Filter: ON

### Analysis

#### Incident Summary : NodeDown

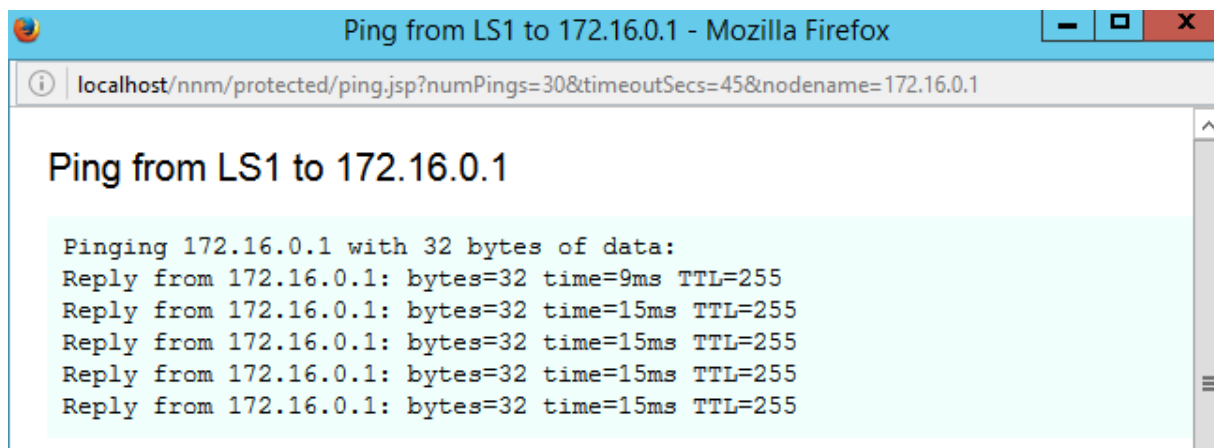
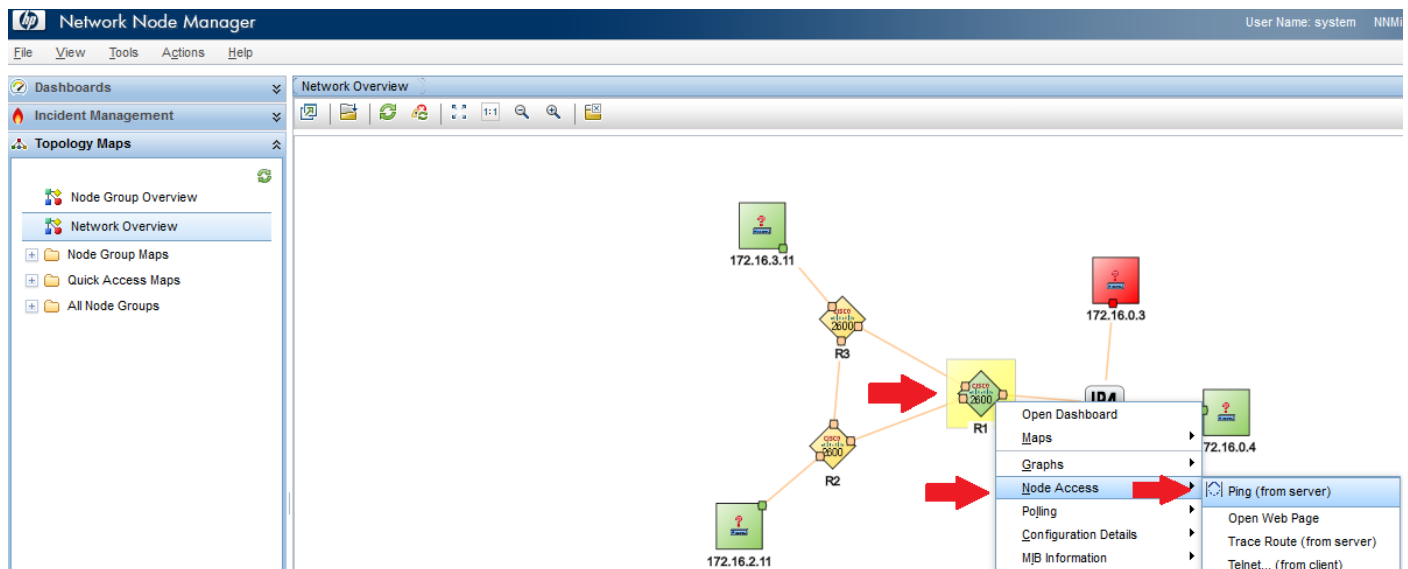
Message	Node Down
Severity	Critical
Lifecycle State	Registered
RCA Active	true
Source Object	172.16.0.3 (Node)
Created/Opened	12/28/16 03:39 PM (Open for 4 minutes)

#### Details

Category	Fault
Family	Node
Correlation Nature	Root Cause
Origin	NNMi
Last Occurrence Time	December 28, 2016 3:38:57 PM AST
Source Node	172.16.0.3
Source Object	172.16.0.3

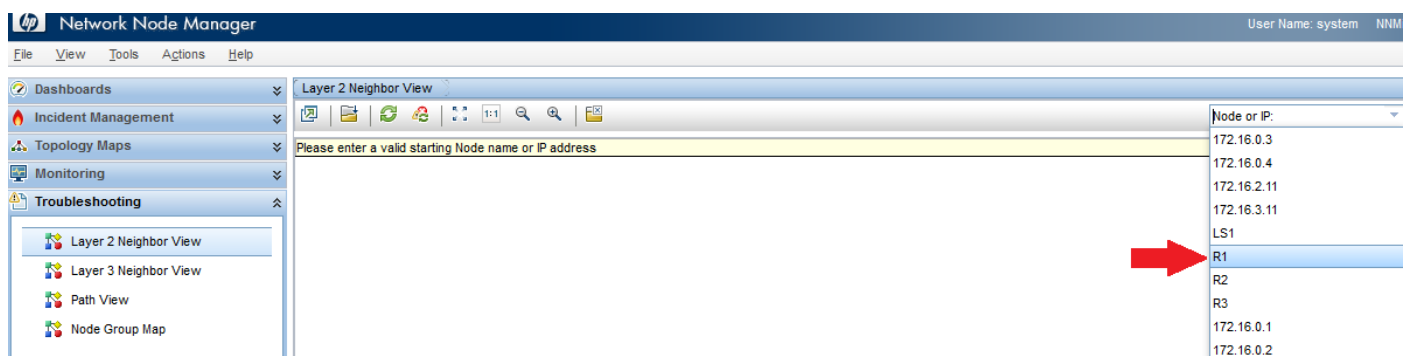
Lab sheet 6.1: provide a screenshot showing the Incidents screen.

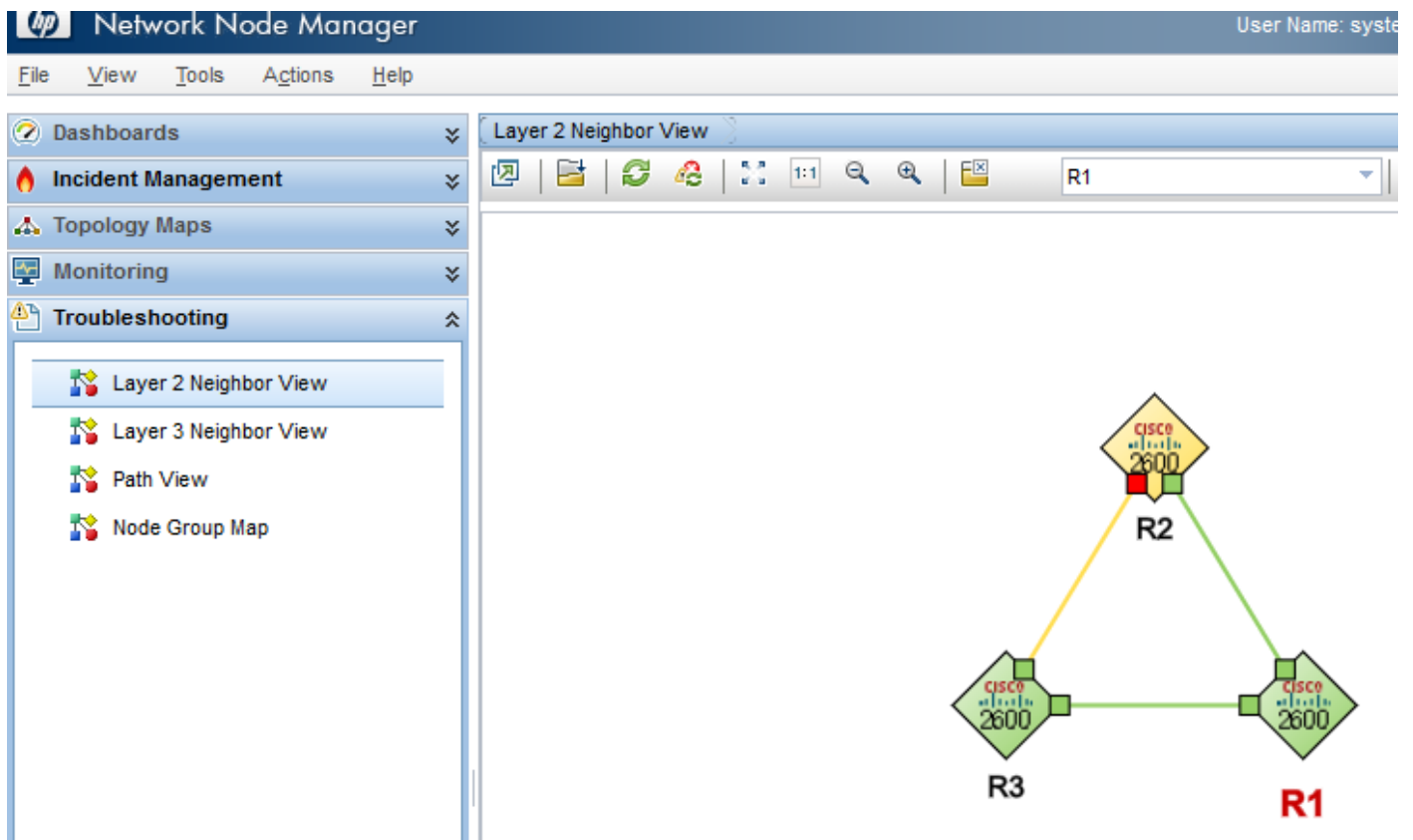
3. In the **Topology > Network Overview** screen, right-click on **R2** then click on **Node Access > Ping (from server)**.



Lab sheet 6.2: provide a screenshot showing the output of the Ping screen.

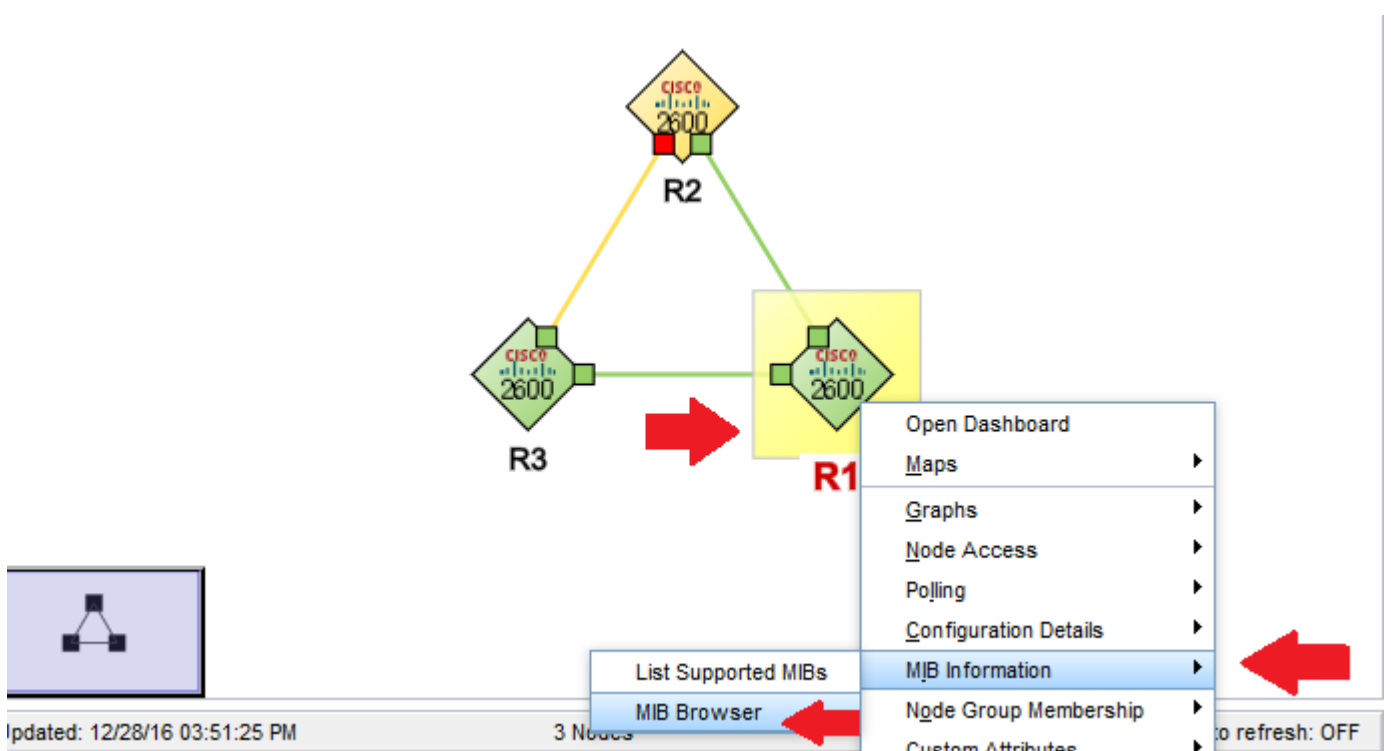
4. In the **Troubleshooting** click on **Layer 2 Neighbor View** screen, then select the IP of **R1**.



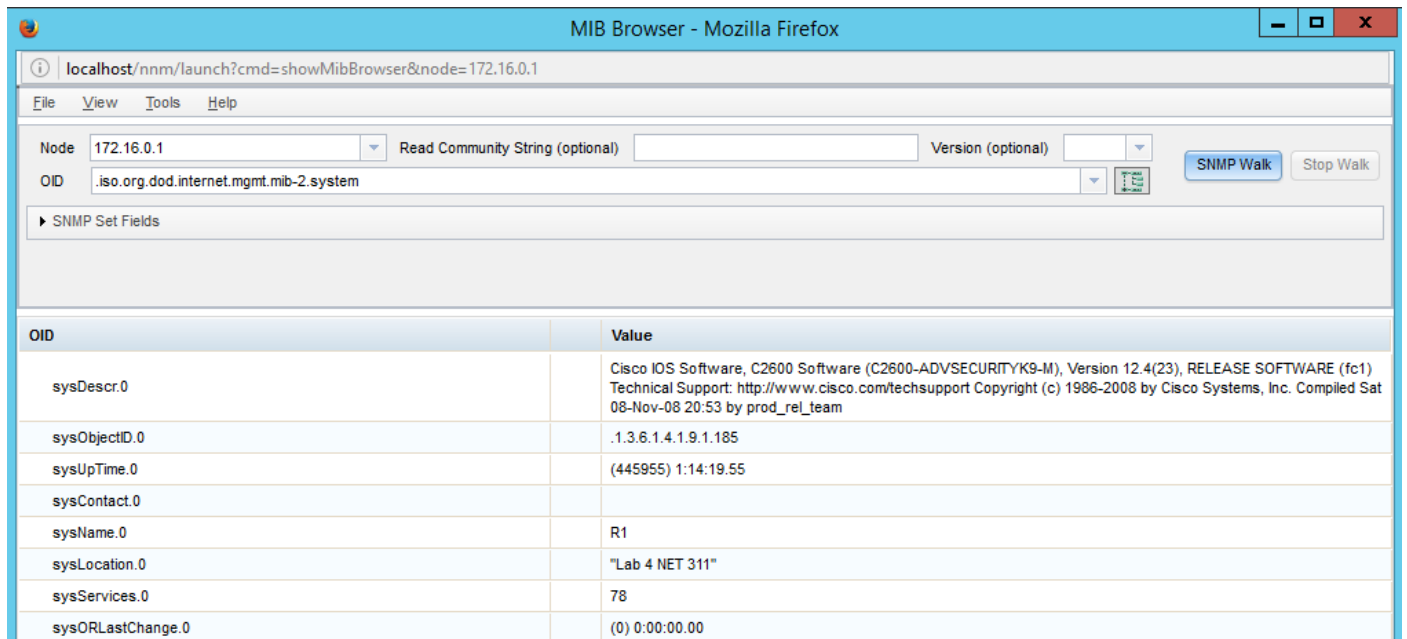
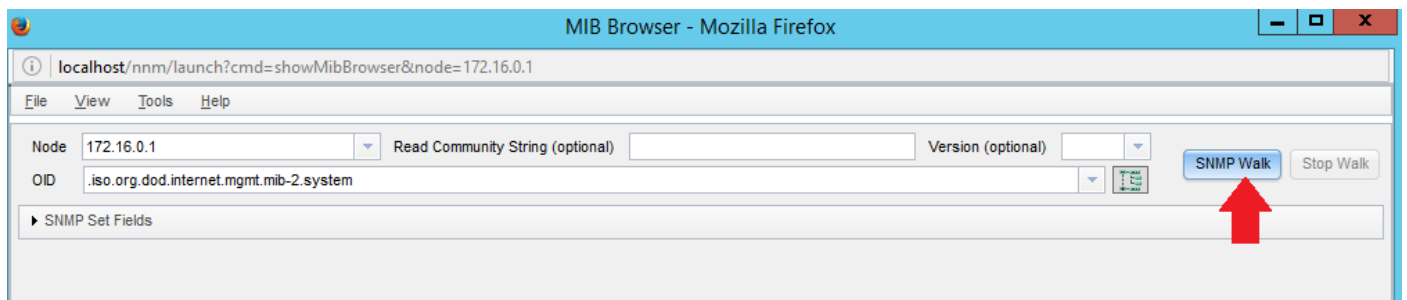


Lab sheet 6.3: provide a screenshot showing the output of the Layer 2 Neighbor View screen.

5. Right-click on **R1**, then click on **MIB Information** -> **MIB Browser**.



6. Click on SNMP Walk.



Lab sheet 6.4: provide a screenshot showing the output of SNMP Walk in the MIB Browser.