HP Network Node Manager i-series Software

Improving Monitoring Accuracy with ICMP

Software Version 8.13 Patch 6

The out-of-the-box configuration for NNMi exclusively uses SNMP to monitor nodes that support SNMP. Occasionally routers and switches get busy and do not respond to SNMP for periods of time. Sometimes NNMi incorrectly identifies these unresponsive nodes as `down` due to no SNMP response. You can make adjustments to the SNMP monitoring retry and timeout values, but even that may be insufficient to prevent false `NodeDown` notifications.

One way to improve this is to add ICMP monitoring to enhance the monitoring of SNMP capable nodes. This paper explains the steps to use to decrease the number of false `NodeDown` notifications. By following the example shown in this paper, you can implement a similar solution and improve the accuracy and reliability of notifications in NNMi.

NOTE: The author uses ICMP and ping interchangeably throughout this paper.

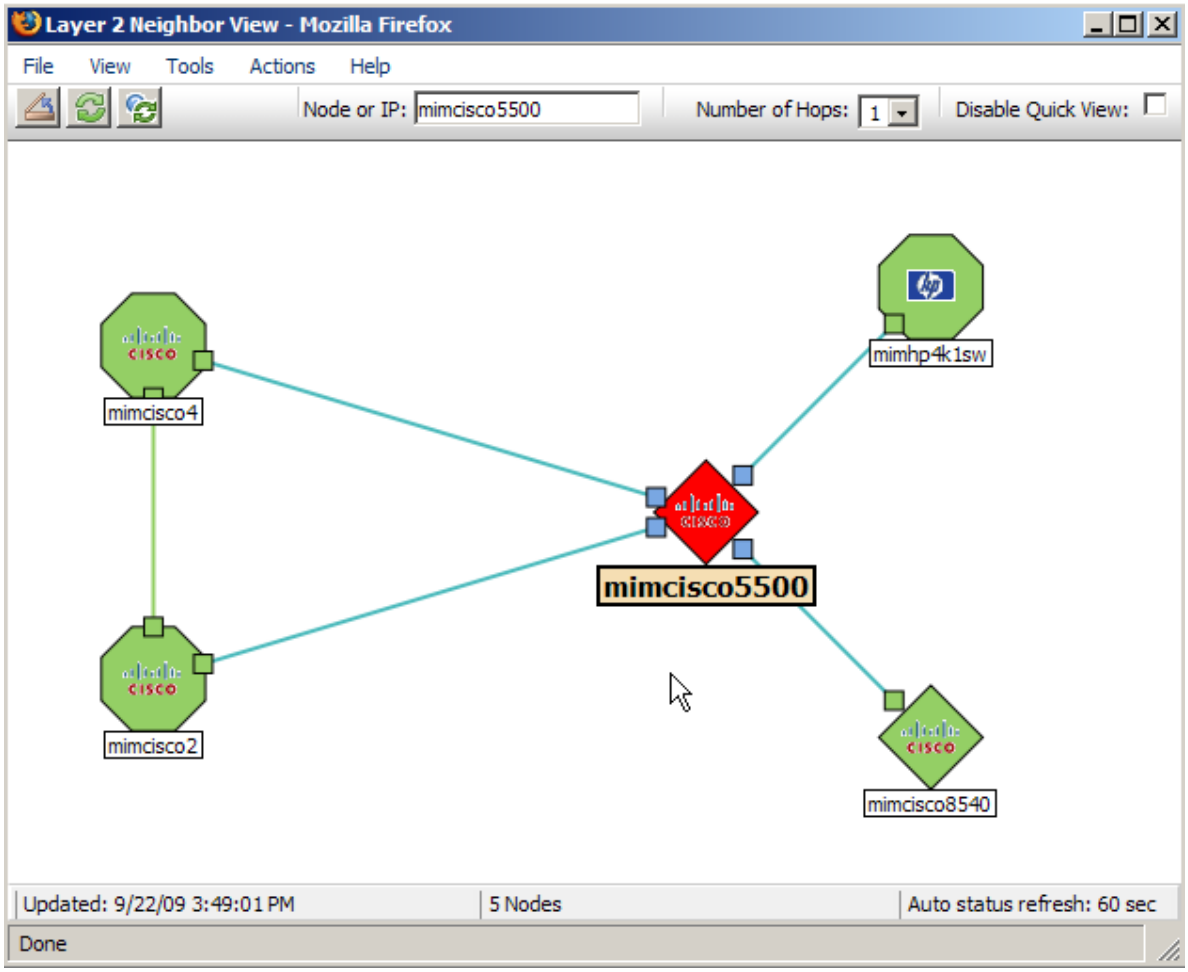
CONTENTS

False Alarms

The following example shows a router that gets too busy to respond to SNMP for long periods of time. Suppose we have a router called `mimcisco5500`. Using the out-of-the-box (default) settings, NNMi does not use ICMP (ping) to monitor nodes. Instead it strictly uses SNMP for monitoring.
NOTE: There is one exception; NNMi uses ICMP to monitor non-SNMP nodes.

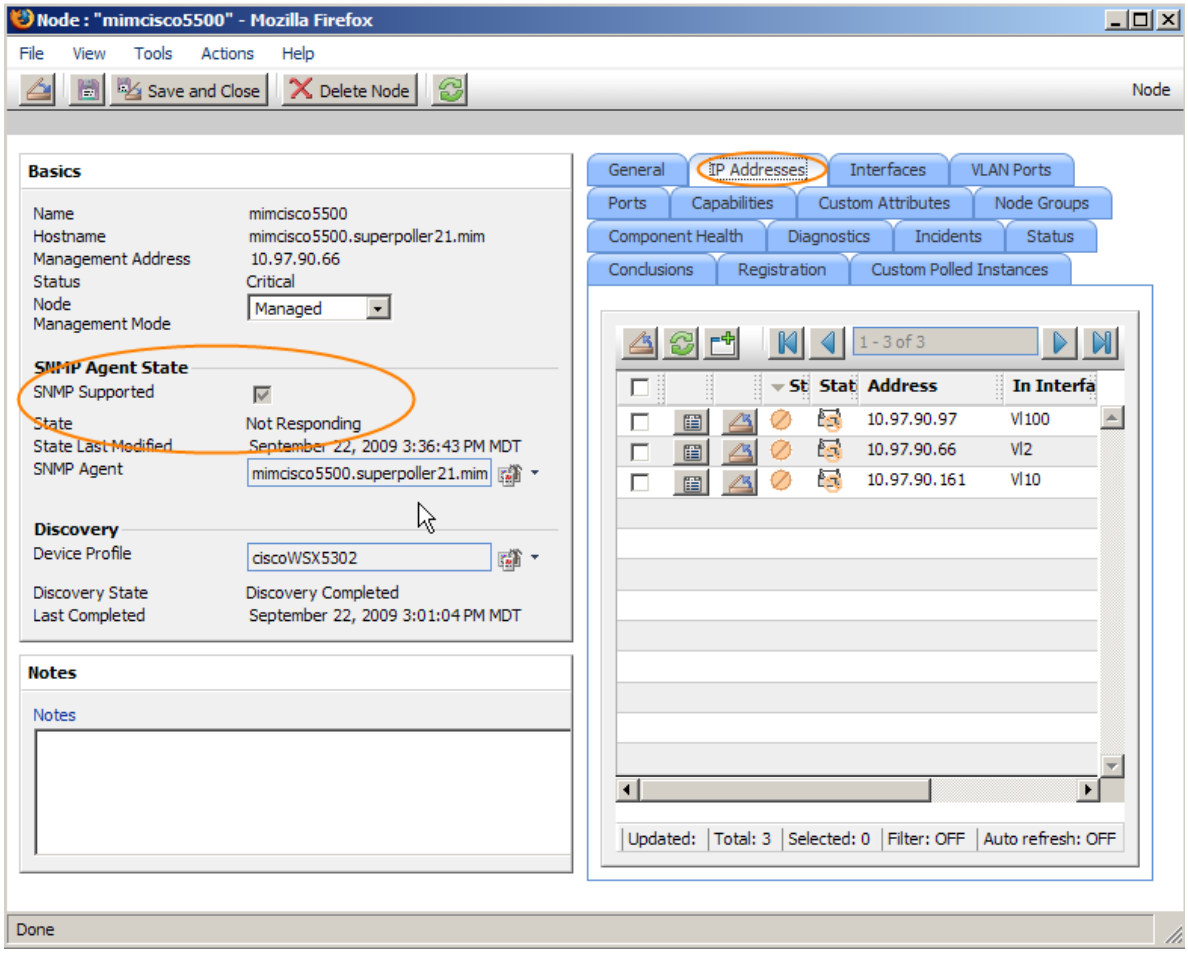
In the example shown in Figure 1, observe that NNMi shows `mimcisco5500` as `critical` or `down`, but the router is actually up and just not responding to SNMP. In addition to the map notification, NNMi generates a `NodeDown` incident. Under these circumstances, you do not want to be alerted that `mimcisco5500` is down.

Figure 1: False Alarm Example



You can see from the node form shown in Figure 2 that NNMi monitors this node using SNMP only; none of the IP addresses are being pinged.

Figure 2: Default Monitoring Uses SNMP not ICMP

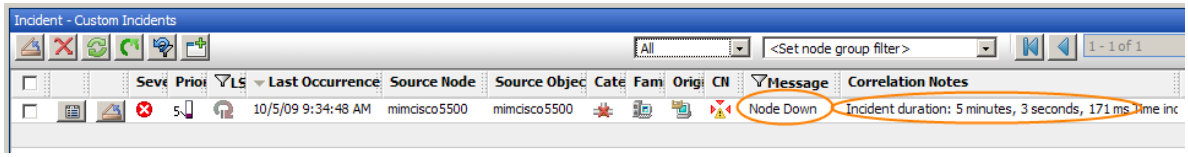


You can see in Figure 3 that the outage lasted almost exactly five minutes, which corresponds to one polling cycle. One easy method to check outage duration from NNMi is to do the following:

1. Open the **Custom Incidents** workspace and filter on `Message=Node Down`.
2. Look at the `Correlation Notes` to see how long the outage lasted.

This feature is only available in NNMi 8.13 Patch 5 or later.

Figure 3: Outage Duration



Since `mimcisco5500` is actually up and functioning in our example, this probably means that `mimcisco5500` stopped responding to SNMP for a period of time. However, when the next polling cycle came around (five minutes by default), `mimcisco5500` resumed responding to SNMP. You can confirm this by manually trying to ping `mimcisco5500` while it is marked as `down`. If it responds to ping, it is not really down.

Adding ICMP for Better Results

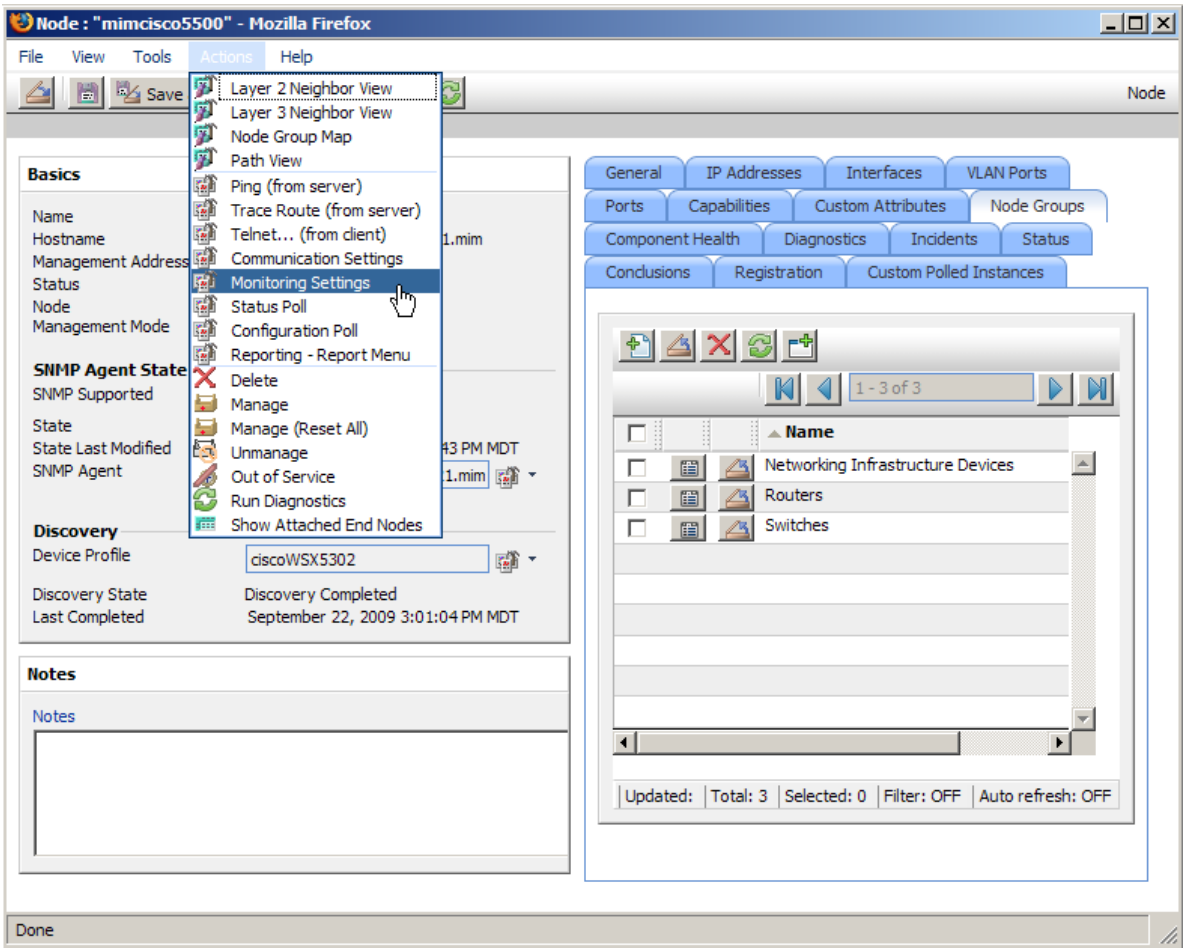
Since `mimcisco5500` responds to ping even when it does not respond to SNMP, you decide to add ICMP monitoring.

```
# ping 10.97.90.66
PING 10.97.90.66 (10.97.90.66) 56(84) bytes of data.
64 bytes from 10.97.90.66: icmp_seq=0 ttl=59 time=3.33 ms
64 bytes from 10.97.90.66: icmp_seq=1 ttl=59 time=2.45 ms
```

`Mimcisco5500` is a router. Suppose you decide to add ICMP monitoring to all of your routers.

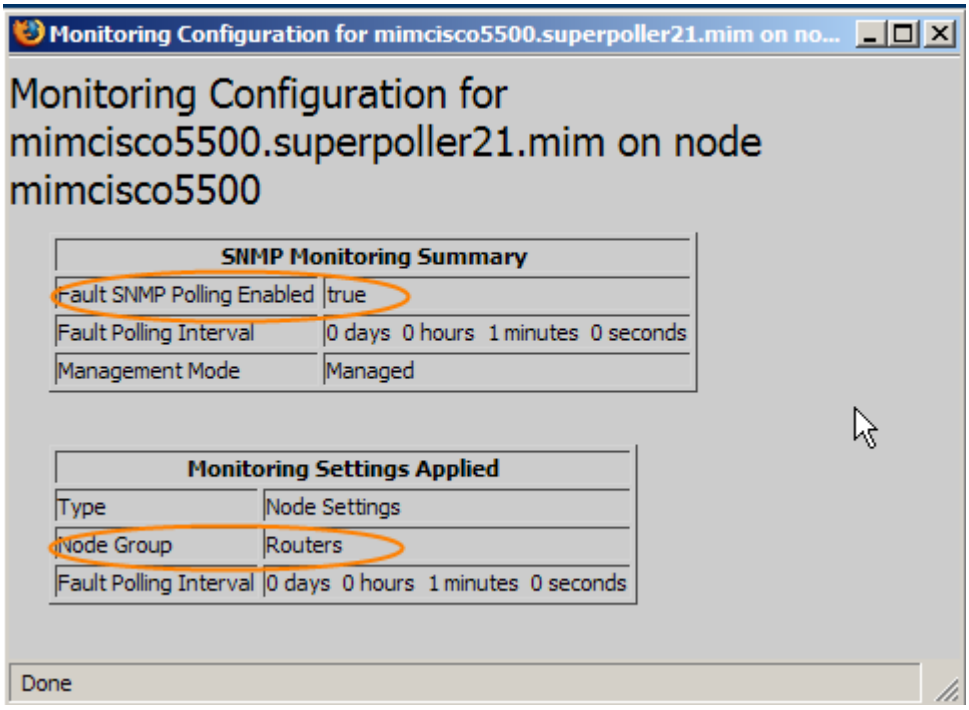
First, check to see which monitoring policy is being used on this node. On the node form shown in Figure 4, select **Actions->Monitoring Settings**.

Figure 4: Checking Monitoring Policy



As you can see in Figure 5, NNMI sets the polling using the `Routers Node Group` monitoring policy.

Figure 5: Routers Node Group Monitoring Policy

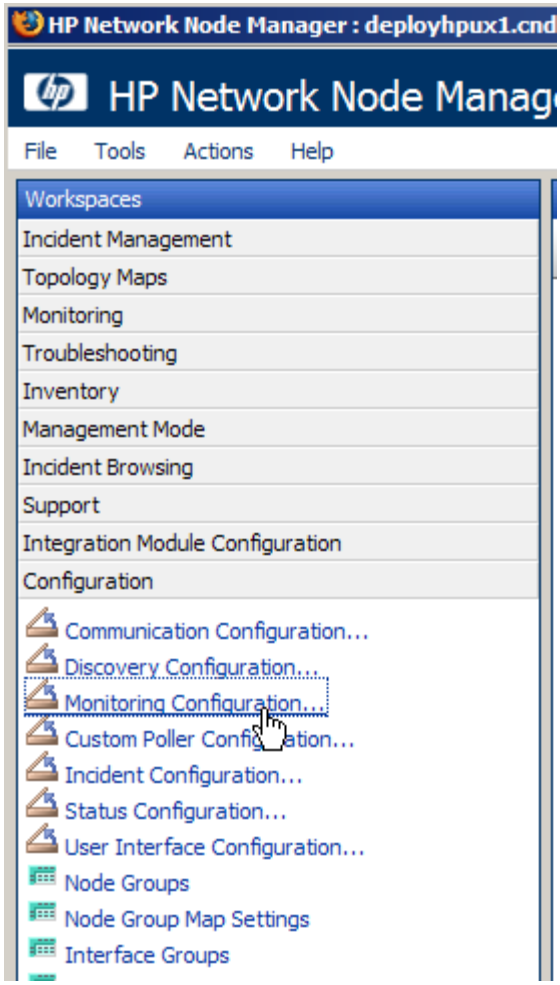


The Wrong Approach

Your first thought might be to enable ICMP for all routers. Suppose you decide to do that now. IMPORTANT: Do not try this on your system right now. This is only for discussion purposes. Continue reading to the end of this paper for a better approach.

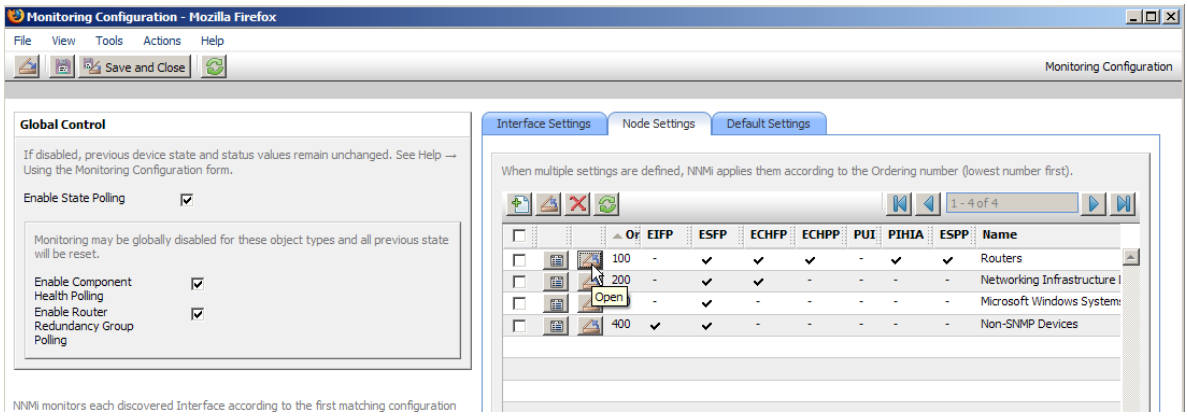
Click **Monitoring Configuration** as shown in Figure 6.

Figure 6: Navigate to the Monitoring Configuration Workspace



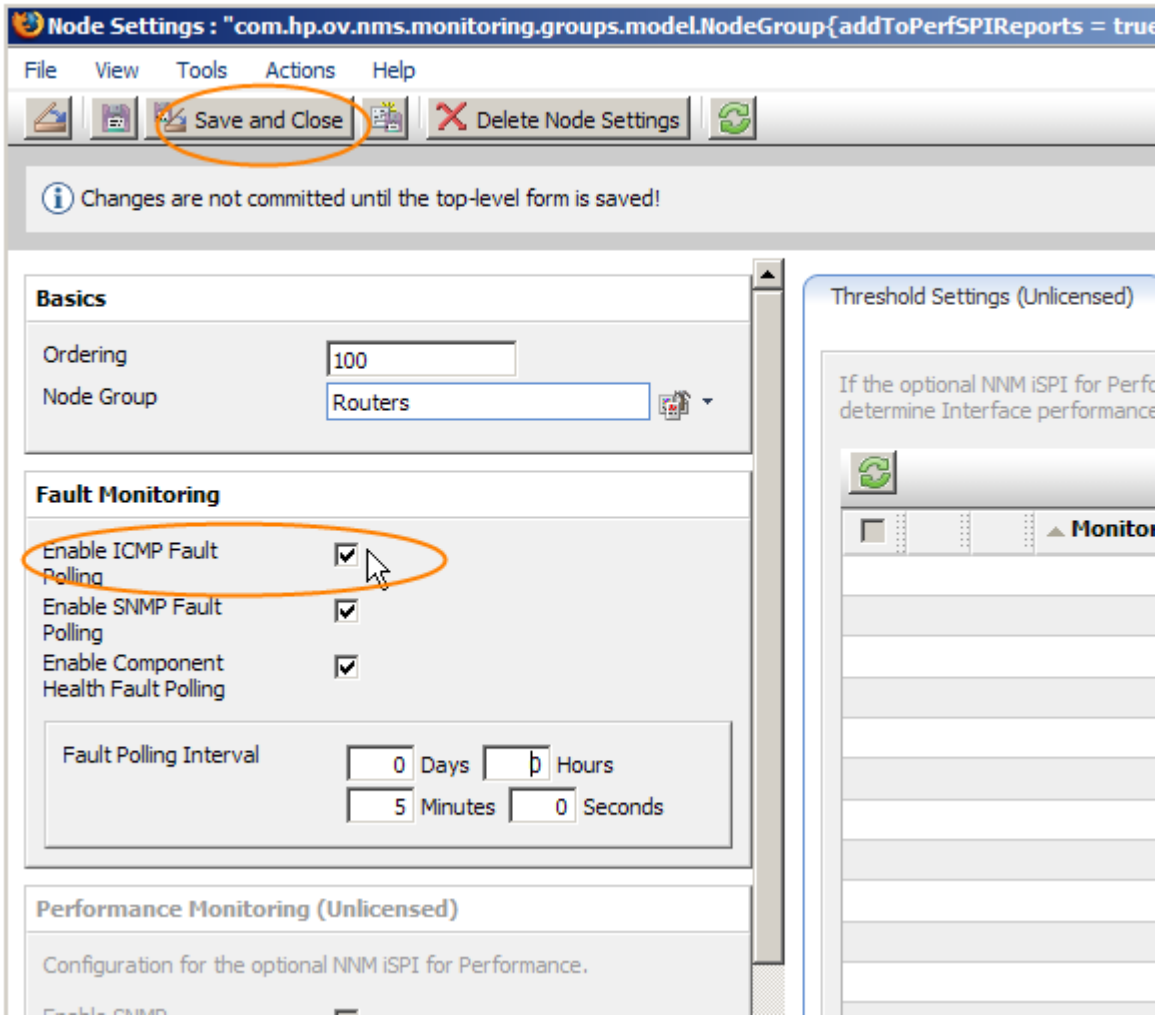
Click the **Node Settings** tab and open the Routers selection as shown in Figure 7.

Figure 7: Open the Routers Selection



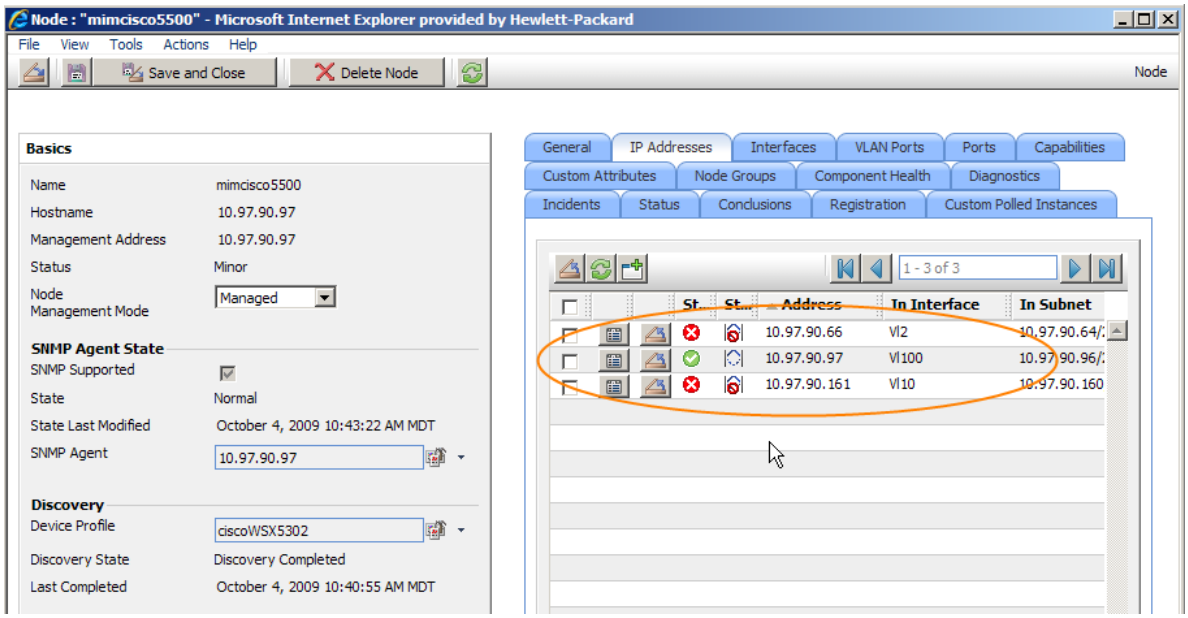
Select the **Enabled ICMP Fault Polling** box; then click **Save and Close** as shown in Figure 8.

Figure 8: Enabling ICMP Fault Polling



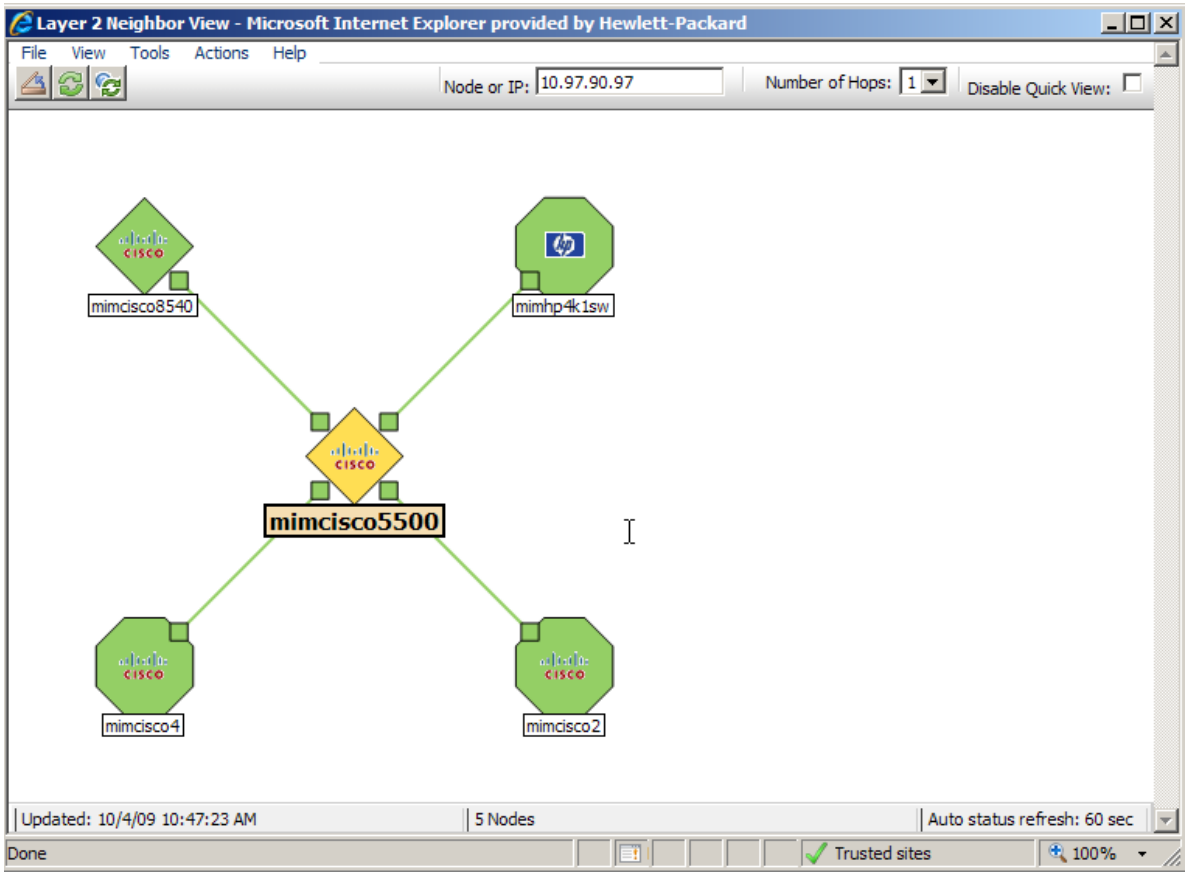
Now all addresses on all routers will be pinged as shown in Figure 9.

Figure 9: NNMi Pings All Addresses on All Routers



This approach has a few problems. First, many routers have addresses that will never be reachable by the NNMi management server. This causes these routers to always have a `Minor` status because not all of the addresses are reachable. This also causes NNMi to generate many `AddressNotResponding` alarms. Second, NNMi issuing so many pings causes undue ping traffic and strain on the NNMi management server. All you really want is NNMi to do a simple ping against just one address on the router. This is illustrated in Figure 10. So you decide to undo this change and consider a better solution.

Figure 10: Router Has Minor Status Due to Unreachable Addresses



The Right Approach

A better solution is to be more selective about the addresses you configure NNMi to ping. You will need to analyze your network to see what the best approach is for your environment. The ideal solution, in most cases, is to ping the management address on nodes; however this currently is not an option in NNMi. Instead, you should work with your network administrator to make a list of the addresses that would be best to monitor using ping.

NNMi distinguishes between interfaces and addresses, but the two are tightly coupled. NNMi does not provide monitor filtering at the address. Instead, you filter based on interfaces; then apply ICMP monitoring to these interfaces. This in turn causes NNMi to ping addresses that are hosted on these interfaces.

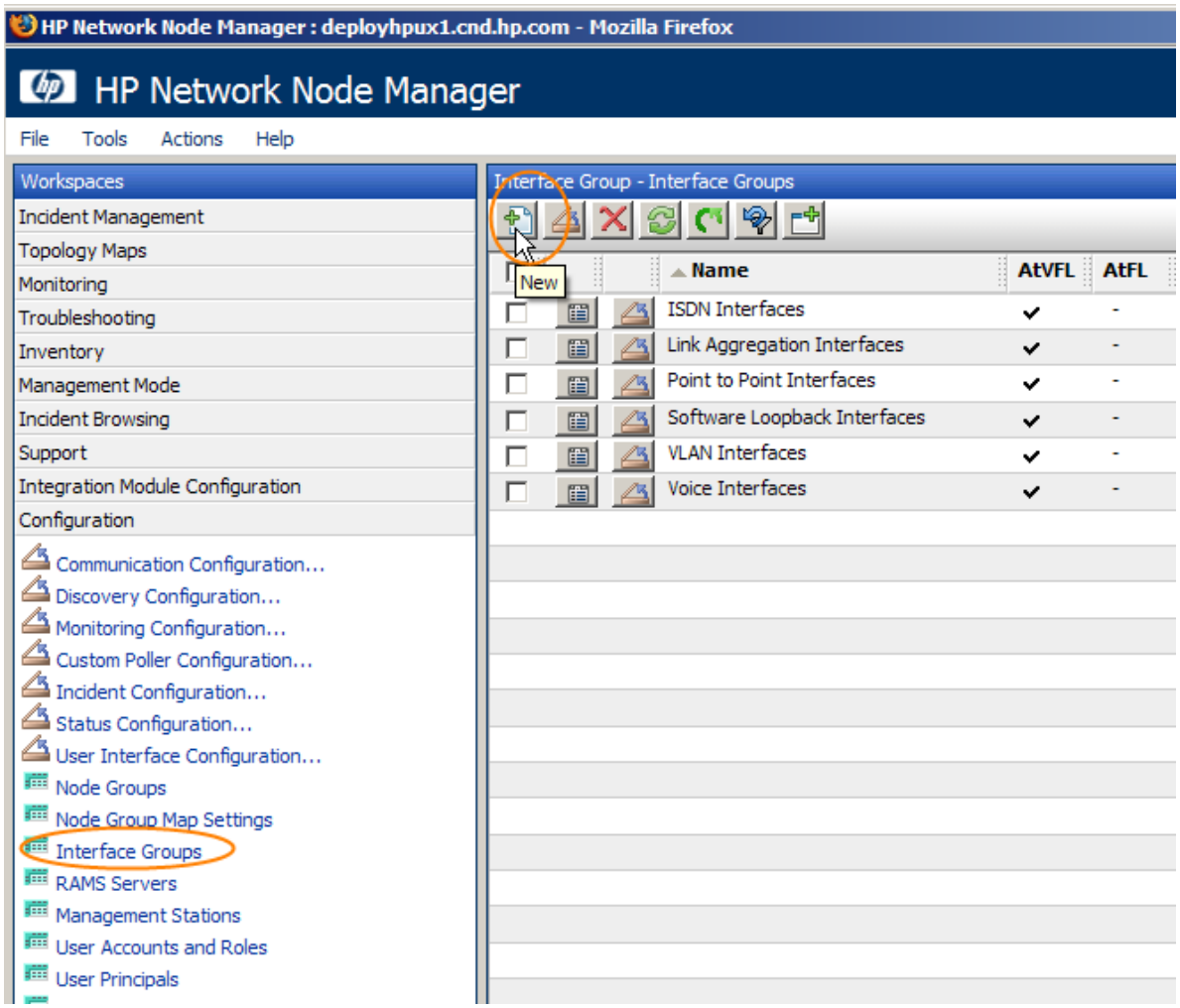
Many customers using Cisco routers will have a loopback interface and address on their routers. These interfaces often have the name `lo0`. These interfaces may host the best address to ping for your environment.

For this example, you do not have an `lo0` interface on this router. Instead you will use addresses hosted on the `Vl100` interface as your best addresses to ping. In this example, this happens to be your management VLAN, which should always be reachable by NNMi. You can change this example to use `lo0` if this is better for you.

Creating an Interface Filter

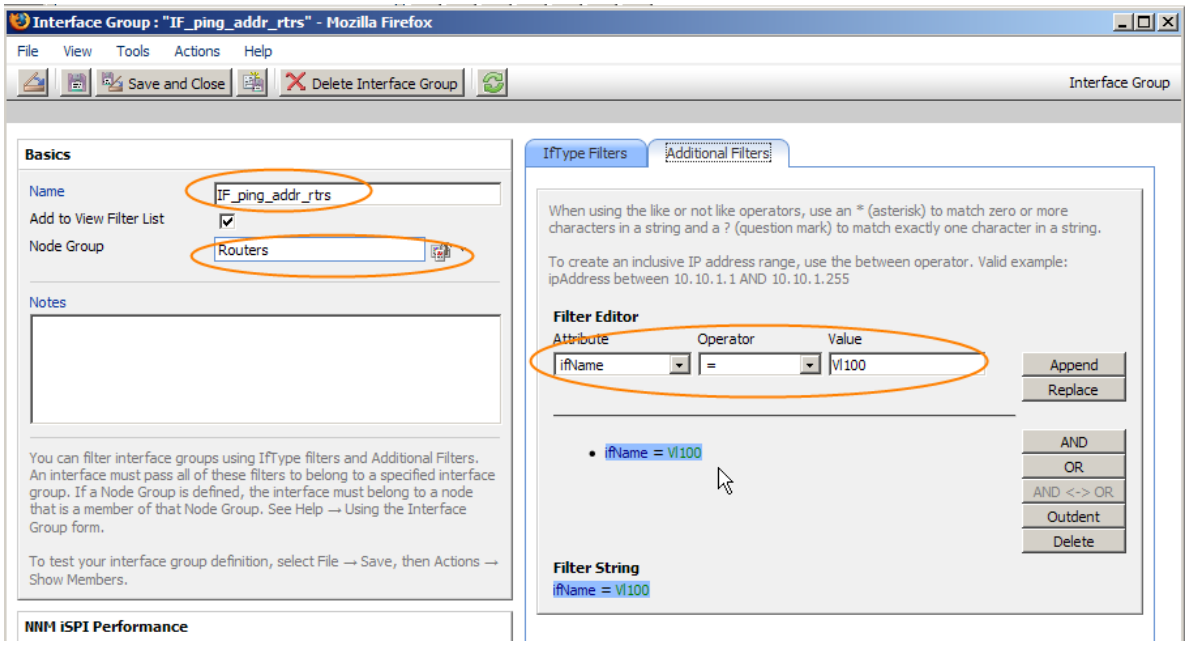
You need to create an interface group for the interfaces named Vl100 residing on routers. To do this, select `Interface Groups` located in the `Configuration` workspace; then click `New` as shown in Figure 11.

Figure 11: Creating an Interface Group



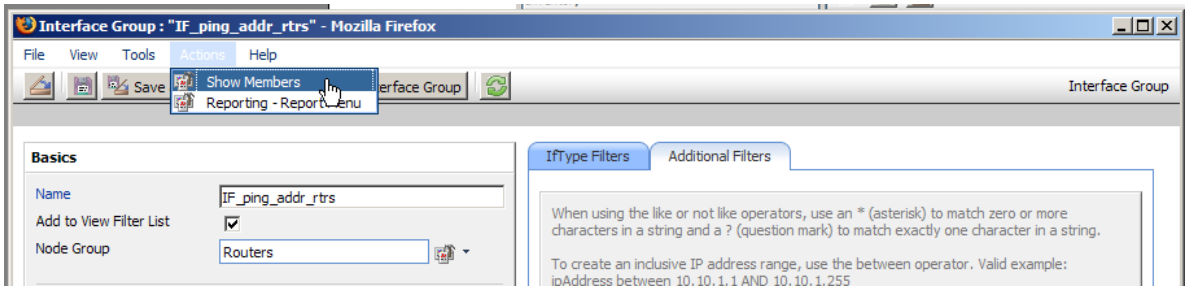
Name this interface group `IF_ping_addr_rtrs`. Select the `Routers` node group; then set up an **Additional Filter** to choose interfaces with `ifName` = `Vl100` as shown in Figure 12.

Figure 12: Filtering Interfaces with ifName=Vl100



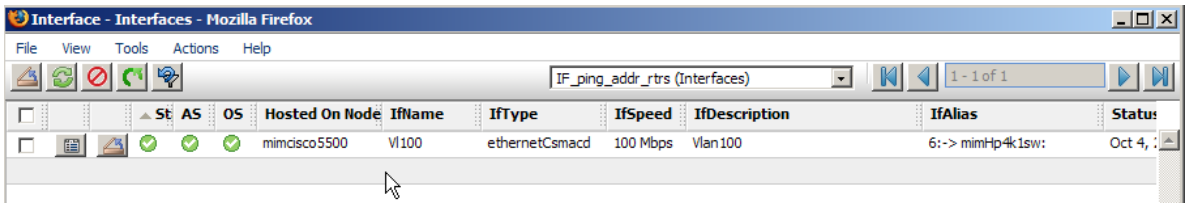
Now validate that this filter is working as expected. After saving the `Interface Group` shown above, select **Actions**->**Show Members** as shown in Figure 13.

Figure 13: Validate the Filter



You should see the interfaces you expect as shown in Figure 14. In this simple example you only have one of these interfaces but in practice you should have many. The goal is to have one interface per router.

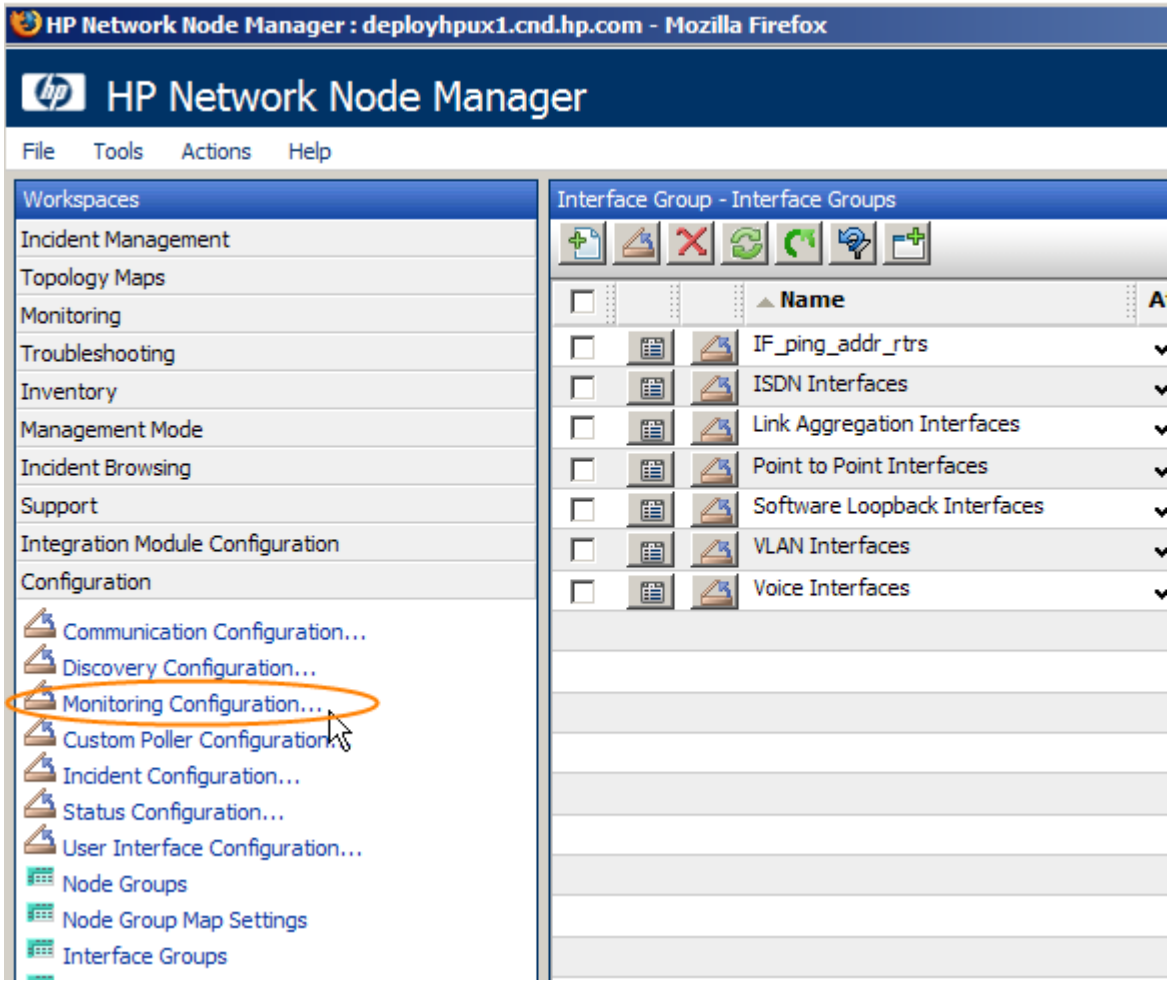
Figure 14: Expected Interfaces



Create a Monitoring Policy

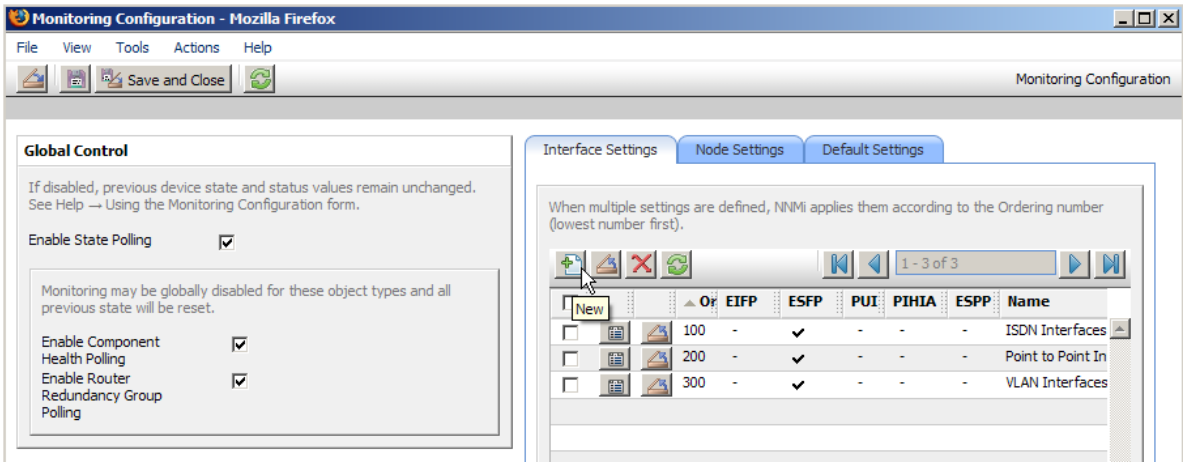
The next step is to create a monitoring policy associated with this interface group. You enable ping in this policy. Click **Monitoring Configuration** under the **Configuration** workspace as shown in Figure 15.

Figure 15: Navigate to the Monitoring Configuration Workspace



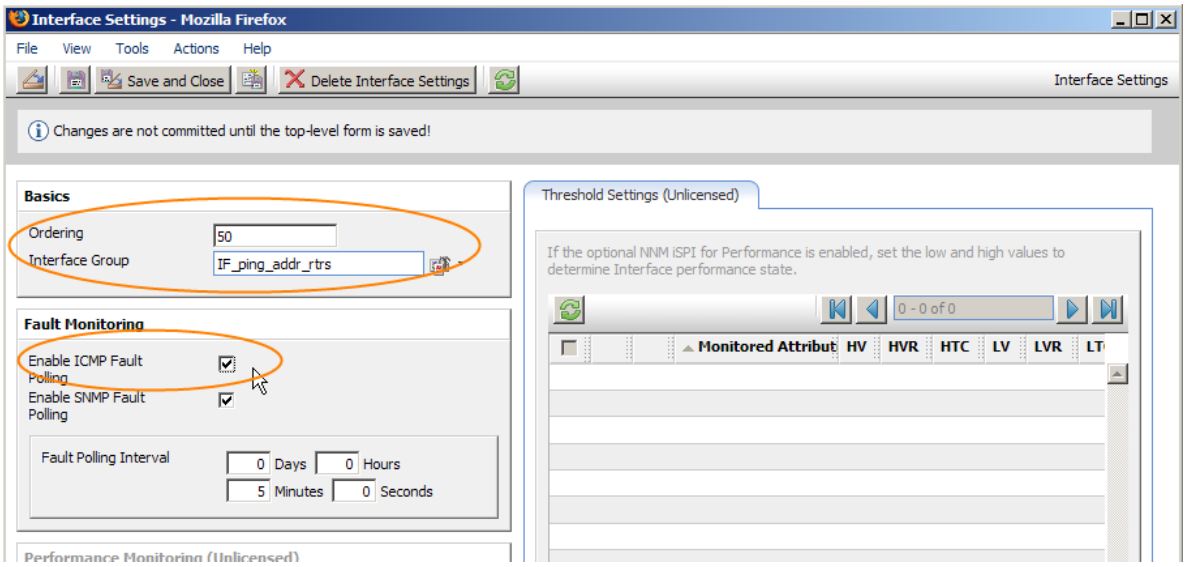
Click the **Interface Settings** tab; then click the **New** button as shown in Figure 16. Take note of the current ordering values. This new policy must be a higher priority (a lower number) than any current policy. In this example, any number lower than 100 is fine.

Figure 16: Click New to Start a New Interface Monitoring Policy



Enter an `Ordering` value, then select the `Interface Group` you previously defined, `IF_ping_addr_rtrs`. Next, check the **Enable ICMP Fault Polling** box as shown in Figure 17. Click **Save and Close** all the way out to the top level.

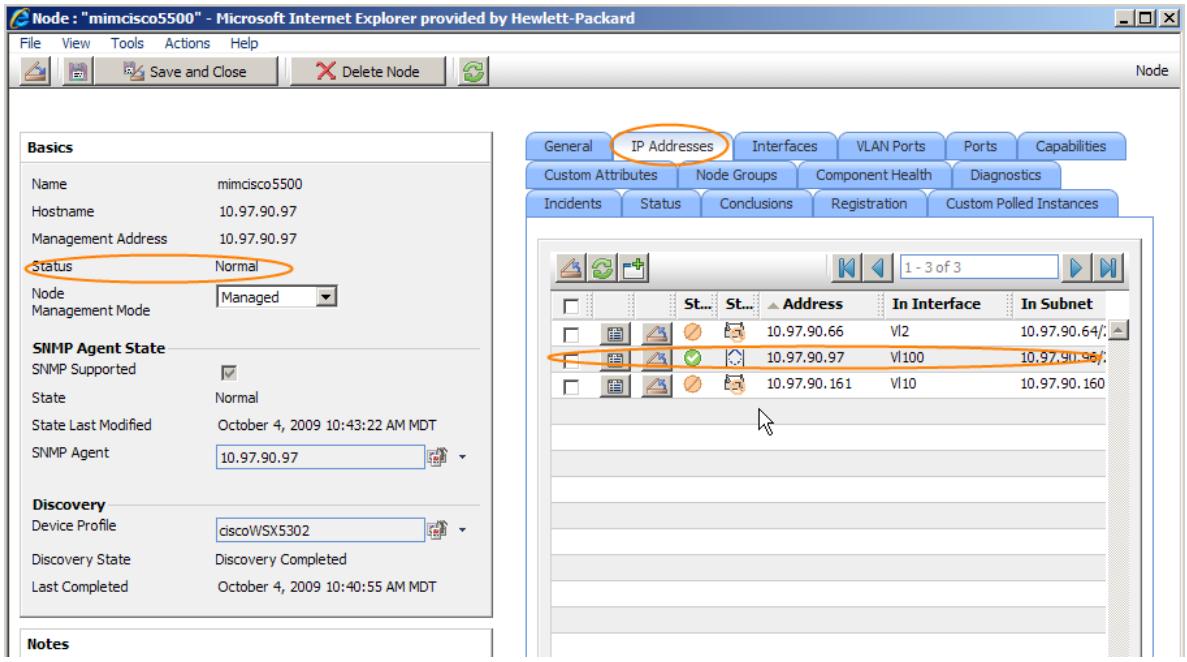
Figure 17: Enabling ICMP Fault Polling



Validate the Monitoring Policy

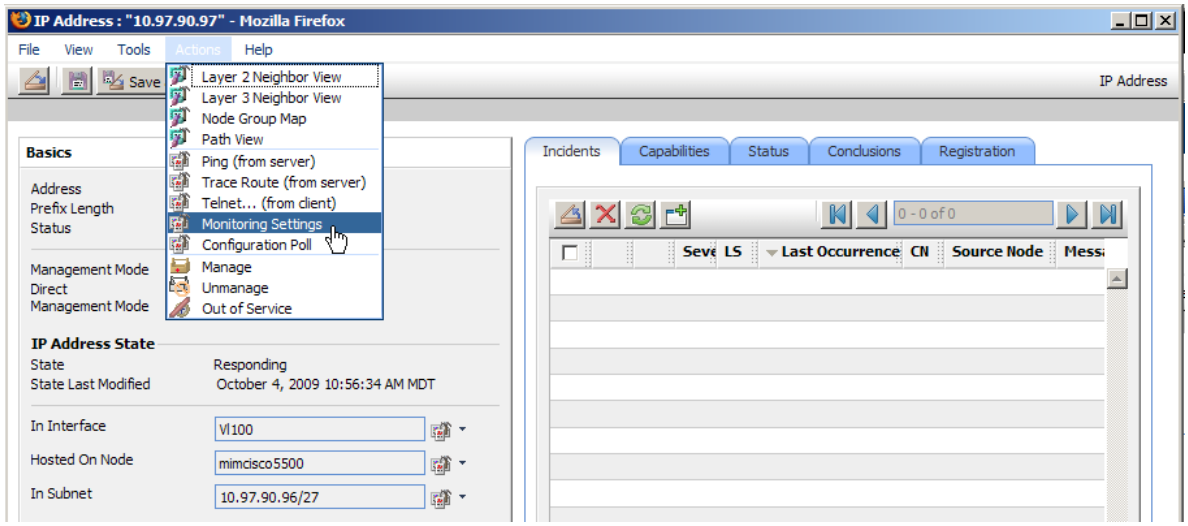
Now open the node form again and look at the `IP Addresses` tab. Notice that NNMi is now monitoring only one address using ICMP as shown in Figure 18. You may need to execute a status poll on the node to make sure you see the new status.

Figure 18: Monitoring One Address Using ICMP



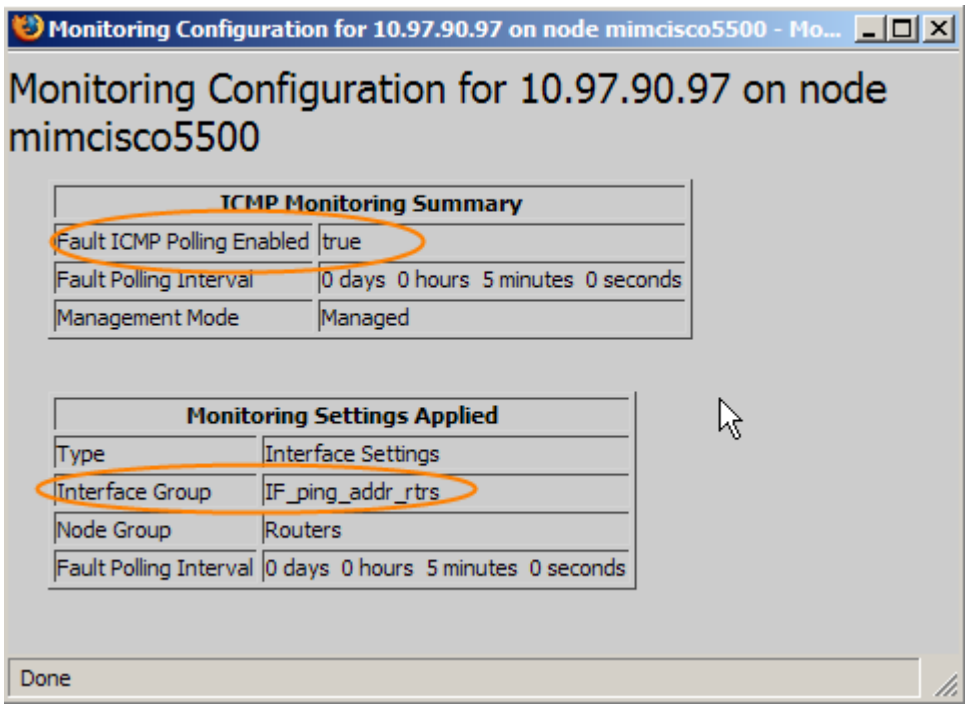
To confirm that the address is being monitored using your newly created policy, open the `Address` form for address `10.97.90.97`. Then select **Actions->Monitoring Settings** for this address as shown in Figure 19.

Figure 19: Select Monitoring Settings



As you can see in Figure 20, `ICMP Polling Enabled` is set to `true`; that is due to the monitoring policy applied to the `IF_ping_addr_rtrs` filter. This is what you expected.

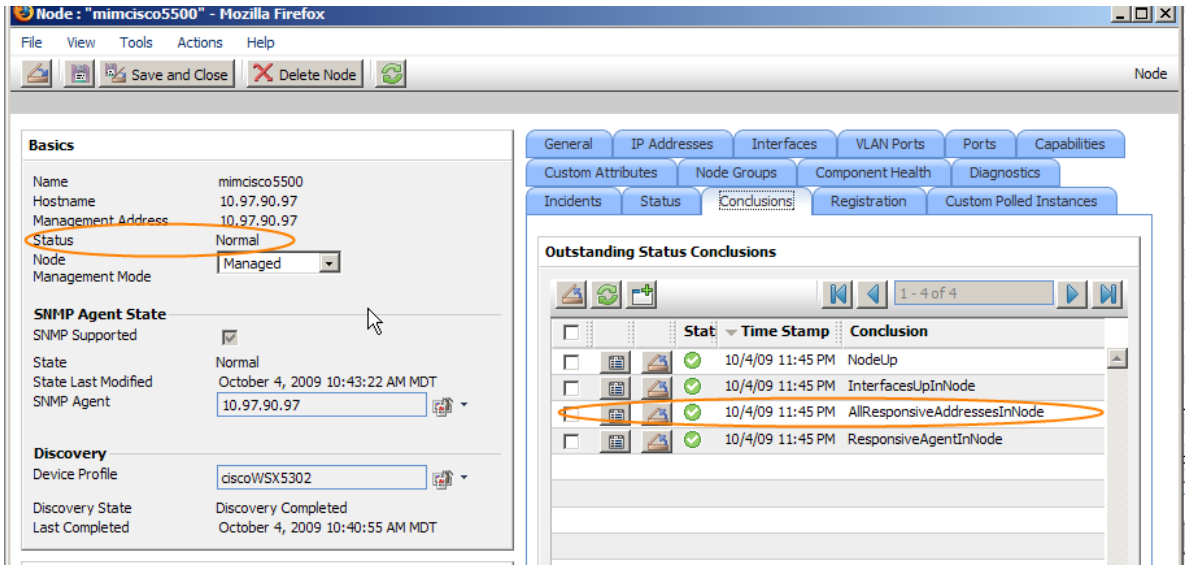
Figure 20: Monitoring One Address as Expected



Validate the Node Status

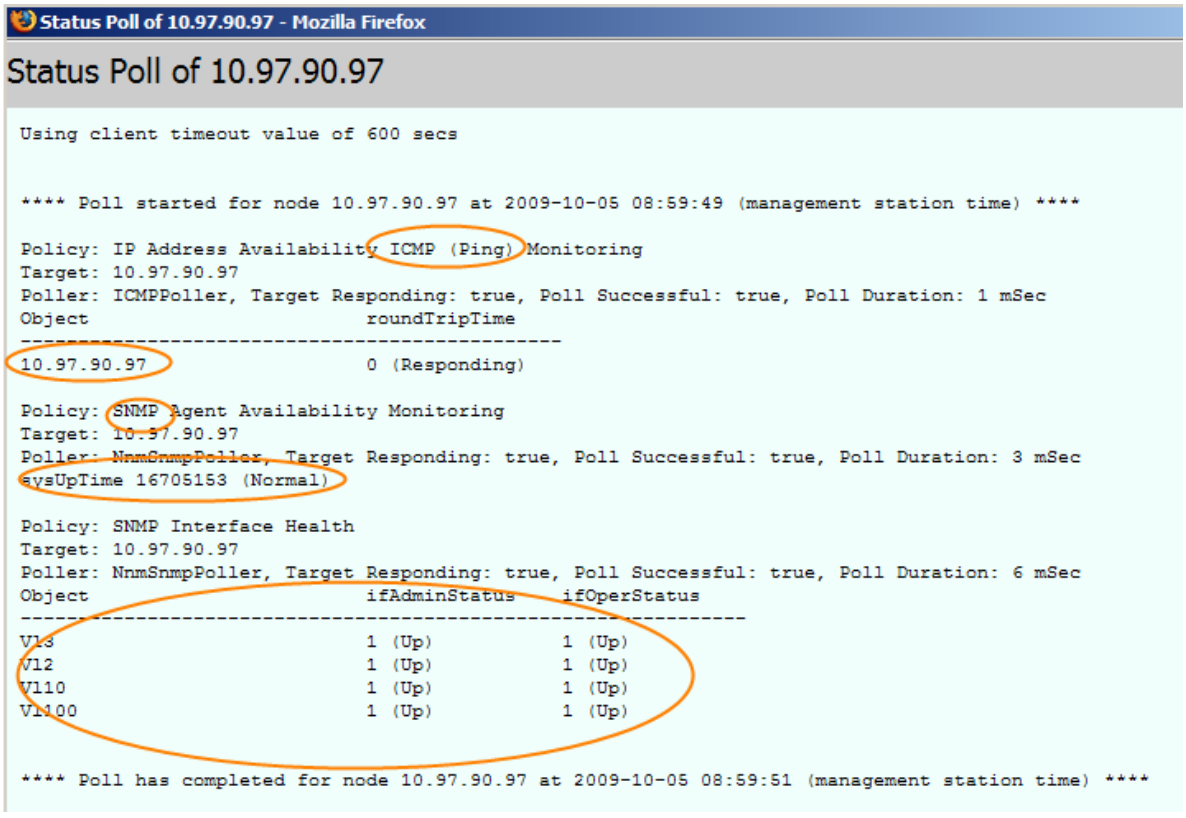
Finally, bring up the node form again and check the status and conclusions. You may need to run a status poll against the node to make sure it has accurate status. You can see in Figure 21 that the node status is `Normal` and conclusions on the node are good.

Figure 21: Validate the Node Status



As you can see from the status poll results shown in Figure 22, reliability and accuracy are increased since NNMi now does both an ICMP poll against the reachable address and SNMP monitoring. This will reduce false notifications.

Figure 22: Status Poll Results



Additional Configuration

Repeat this process for other network gear such as switches. The process may be simpler for switches because many times a switch has only one address. In that case, you can create a monitoring policy for switches and enable ICMP polling for the node group without having to identify specific interfaces.

Conclusion

By adding selective ICMP monitoring to the monitoring policies of NNMi, you increase the reliability and accuracy of monitoring, resulting in fewer false notifications when monitored nodes are simply too busy to respond to SNMP in a timely manner. If you follow the steps presented in this paper, you can improve NNMi monitoring accuracy.