

Network Performance Monitoring

Lab 2 : SolarWinds & NetPath



EL HAKOUNI Yassin
01/06/2025

1. Introduction.....	2
2. Environment Setup and Objectives.....	2
3. Probe Deployment and Device Discovery.....	3
4. Alerts and Custom Dashboards.....	5
4.1 Alert Configuration.....	5
4.2 Dashboard Customization.....	6
5. NetPath Setup and Visualization.....	6
6. Conclusion.....	7

1. Introduction

In modern enterprise environments, ensuring network performance and availability is crucial. This project focuses on leveraging SolarWinds Network Performance Monitor (NPM) to monitor network health, configure alert mechanisms, and visualize communication paths through the NetPath module.

The goal was to deploy a complete monitoring workflow for a network node (Student11RTR), from device discovery and SNMP setup to NetPath configuration, dashboard customization, and alert automation. Throughout the process, key metrics such as latency, availability, and response time were captured and visualized to simulate real-world monitoring tasks that network engineers face daily.

This report outlines the entire process, including:

- Setting up SNMP polling to monitor Cisco devices,
- Running a discovery scan to import devices and interfaces,
- Creating a custom NetPath service to trace and analyze network paths,
- Building a custom monitoring dashboard,
- Configuring alerts to track high response time or packet loss.

Each step reflects practical skills in enterprise-grade monitoring and demonstrates the ability to deploy and manage a reliable network observability system. Carefully selected screenshots are included throughout the report to illustrate key configurations and highlight functional results in a clear and concise manner.

2. Environment Setup and Objectives

The goal of this practical lab was to configure SolarWinds NPM to monitor network performance, focusing on response time and packet loss between a Windows probe and a Cisco router (Student11RTR). Through this setup, I aimed to:

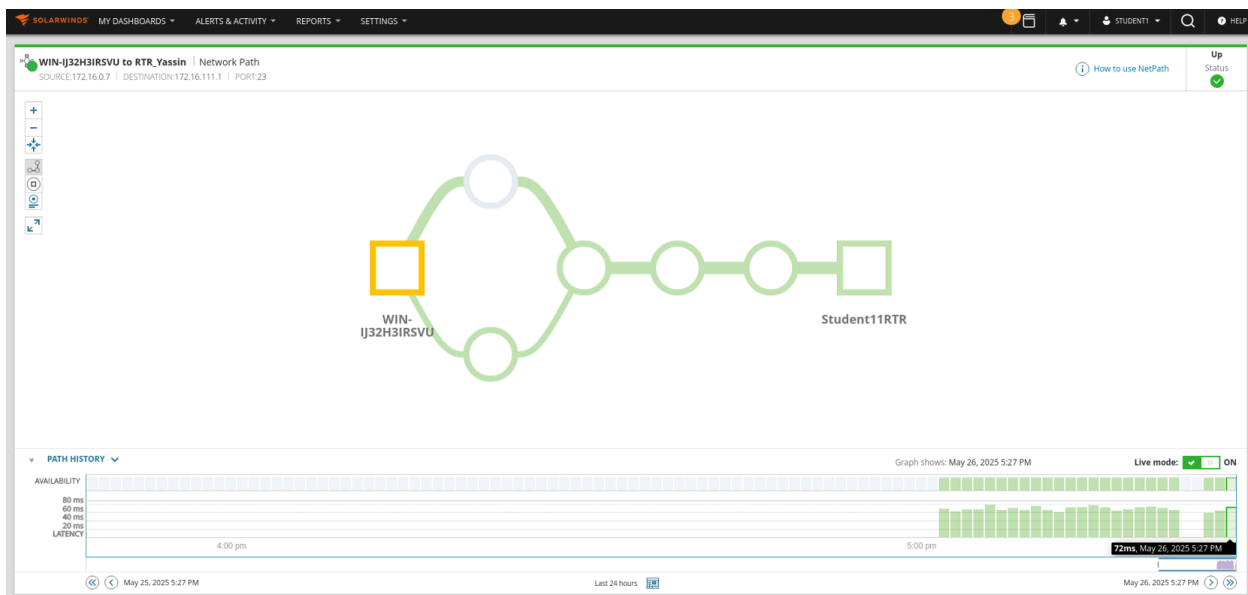
- Deploy a probe on a Windows machine to monitor a target Cisco device.
- Measure network performance over time using relevant metrics.
- Visualize the path and latency variations with NetPath.
- Configure alerts and dashboards to monitor anomalies.

The testbed consisted of:

- A Windows host (**WIN-IJ32H3IRSVU**) acting as a probe.
- A Cisco router (**Student11RTR**) with IP **172.16.111.1**.
- SolarWinds Platform 2025.1.1, hosted on a secured internal network.

The monitoring was designed to reflect real-world scenarios, where an IT department proactively tracks latency issues, network health, and availability through automated visualization and alerts.

This capture shows the network path visualization between the probe and the router, with a consistent flow and measurable latency history :



3. Probe Deployment and Device Discovery

To enable end-to-end monitoring of the Cisco router, I started by deploying a probe on a Windows machine (WIN-IJ32H3IRSVU). This probe acts as the central point of measurement, continuously collecting response time and availability data from the target device.

Once the probe was assigned, I used the Network Sonar Wizard to discover and import the router (Student11RTR) into SolarWinds NPM. The discovery was scoped to a specific IP range (**172.16.111.1** to **172.16.111.2**) to reduce noise and ensure only the relevant device was included in the monitoring scope :

Network Sonar Wizard

Network Selection

How do you want to add devices to SolarWinds Platform monitor? You can use one or more of the options below, but for fastest results, we recommend scanning a maximum of 512 devices at a time.

Using discovery for the first time?

WE RECOMMEND SCANNING...

... a **small subnet (/24)** with your test environment

OR

... a **few individual IP addresses** for servers, routers and switches, and VMs

This will let you see the **wealth of data that SolarWinds Platform provides as quickly as possible**. You can always add more later!

IP RANGES

Start address: 172.16.111.1 End address: 172.16.111.2

+ Add Range

SUBNETS + Add

IP ADDRESSES + Add IP Address

ACTIVE DIRECTORY + Add Active Directory Domain Controller to query...

NEXT CANCEL

After successful discovery, I configured SNMP credentials (**public** and **private**) to allow SolarWinds to retrieve detailed interface-level data from the router. Once the router was detected, I proceeded to import its interfaces into the monitoring system. I filtered by operational status and selected only the relevant Ethernet and logical interfaces :

DEVICES INTERFACES VOLUMES IMPORT PREVIEW RESULTS

Select Interfaces to Import for Monitoring

3 interfaces selected

Selection criteria

Match all selected properties

Status	Port Mode	Monitoring type	Hardware
<input checked="" type="checkbox"/> Operationally up	<input checked="" type="checkbox"/> Trunk	<input checked="" type="checkbox"/> SNMP	<input checked="" type="checkbox"/> Physical
<input type="checkbox"/> Operationally down	<input checked="" type="checkbox"/> Access	<input checked="" type="checkbox"/> WMI	<input checked="" type="checkbox"/> Virtual
<input type="checkbox"/> Administratively shutdown	<input checked="" type="checkbox"/> Unknown		<input checked="" type="checkbox"/> Unknown

Advanced selection options

RESELECT INTERFACES

List of Interfaces

Group by: Interface Type Show: All

Selected (Available)	Interface Type
2 (of 3)	Ethernet
0 (of 7)	Serial
1 (of 1)	Other

3 interfaces selected

BACK NEXT CANCEL

The final result was a fully discovered and monitored Cisco router, ready for performance tracking and alert configuration.

4. Alerts and Custom Dashboards

With the probe and router successfully monitored, the next step was to configure real-time alerts and visualize performance data through custom dashboards.

4.1 Alert Configuration

Using SolarWinds Alert Manager, I set up a high-priority alert to detect any increase in response time from the router **Student11RTR**. The condition was based on predefined thresholds, allowing the system to trigger an alert when the average response time exceeded the expected baseline.

This kind of alert enables proactive troubleshooting by automatically notifying the operations team when performance degradation occurs.

ALERT MANAGER		ACTION MANAGER			
GROUP BY:		+ ADD NEW ALERT EDIT ALERT DUPLICATE & EDIT ENABLE/DISABLE ASSIGN ACTION EXPORT/IMPORT DELETE			
Frequency		Alert Name	Enabled (On/Off)	Alert Description	Property to Monitor
All (99)		High response time	ON	This alert will write to the SolarWinds event log when the a...	Node
15 (8)		High Response Time Monitoring	ON	Response Time	Node
71600 (5)					2 actions
					0 actions

I also reviewed the active alerts to verify that the system had correctly registered the status of my test environment :

The screenshot displays the SolarWinds dashboard with the following sections:

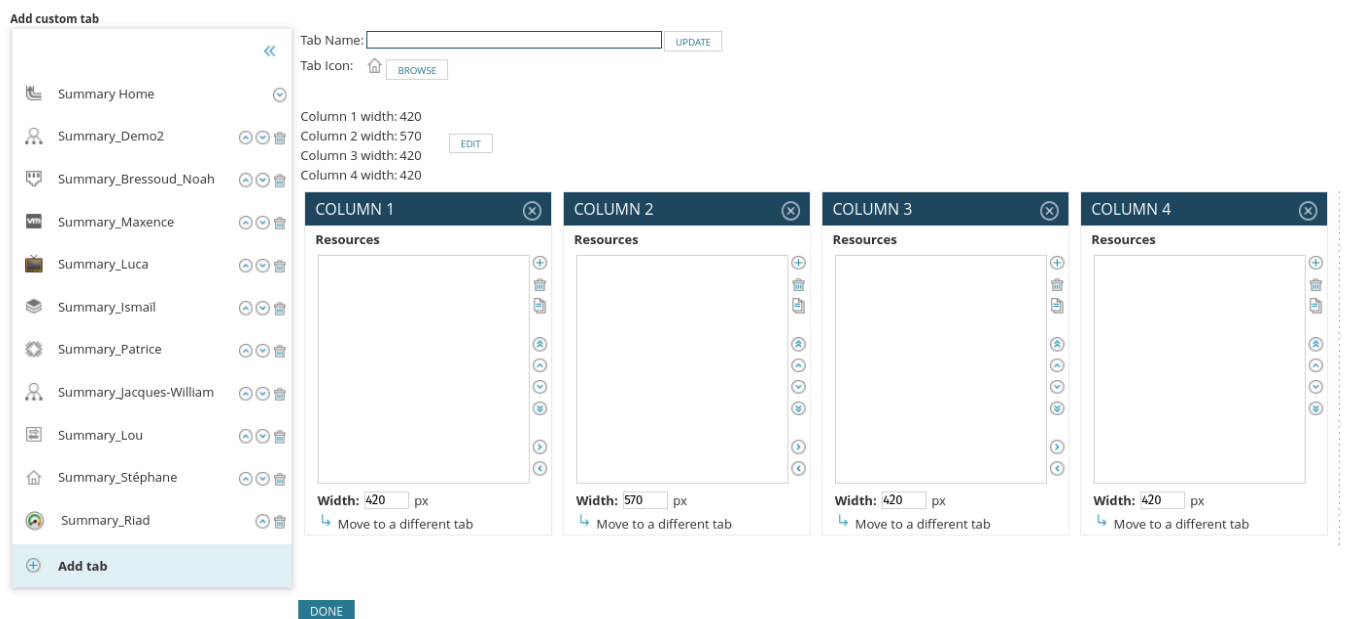
- Summary Home - Summary_Yassin**: Overview of the network status.
- All Nodes**: A list of nodes including 172.16.111.100, ExternalStudent1RTR, ExternalStudent2RTR, ExternalStudent3RTR, Routeur de Jacques-William, Student01RTR, Student02RTR, Student03RTR, Student04RTR, Student06RTR, Student10RTR, Student13RTR, Student14RTR, Student17RTR, Student20RTR, Student17RTR, Student20RTR, and WIN-132H3RSVU.
- Availability of Each Node**: A table showing the availability of each node today.
- Worldwide Map**: A map showing the location of nodes.
- All Alerts (93)**: A list of alerts including "Email me when a Router reboots", "IOS Version change", "IOS Image Family Change", "Duplex mismatch", and "IOS Version change".
- Custom Object Resource**: A section for configuring custom object resources.
- Last 25 Events**: A table showing the last 25 events, including "Node Student14RTR has rebooted", "Student14RTR rebooted at 26/05/2025 16:31:00", "Node Student10RTR has rebooted", "Student10RTR rebooted at 26/05/2025 16:31:00", and "Path WIN-132H3RSVU to 172.16.111.100 changed its status to Critical".

4.2 Dashboard Customization

To centralize key monitoring data, I created a personalized summary tab named **Summary_Yassin**. This dashboard included widgets for:

- Node availability (daily uptime)
- Topology overview
- World map view for location tagging
- Custom object resources (e.g. average response time charts)

This tailored view helps in quickly identifying bottlenecks and visualizing the state of the network from a single interface.

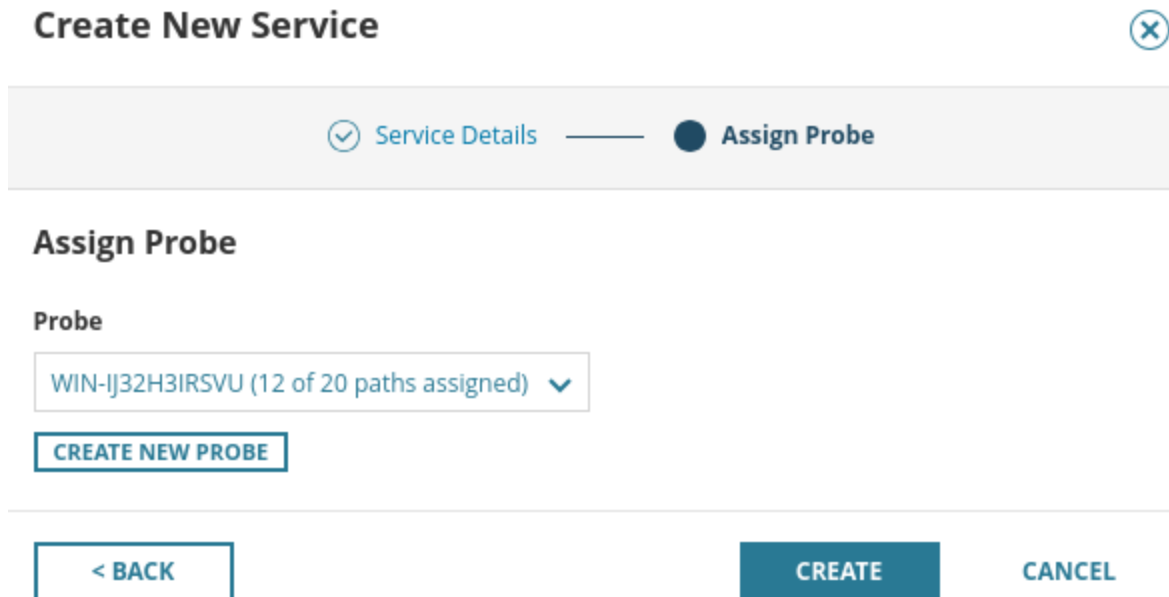


5. NetPath Setup and Visualization

To provide end-to-end visibility into the communication between the monitoring probe and the Cisco router, I configured the NetPath service within SolarWinds NPM. NetPath enables the visualization of all intermediate network hops, latencies, and potential disruptions along the route between a source and destination.

I began by creating a new NetPath service and assigning the Windows probe (WIN-IJ32H3IRSVU) as the monitoring source. The target destination was the Student11RTR router, reachable on TCP port 23. Once configured, NetPath began tracing the communication path and collecting data

such as hop latencies and availability percentages.



The screenshot shows a web interface for creating a new service. At the top, there's a title 'Create New Service' with a close button (X) on the right. Below the title is a horizontal bar with two tabs: 'Service Details' (which is active, indicated by a checkmark icon) and 'Assign Probe' (indicated by a dot icon). Under the 'Assign Probe' tab, there's a section titled 'Assign Probe'. Below this, there's a label 'Probe' followed by a dropdown menu showing 'WIN-IJ32H3IRSUVU (12 of 20 paths assigned)' with a downward arrow. Below the dropdown is a button labeled 'CREATE NEW PROBE'. At the bottom of the dialog, there are three buttons: '< BACK' (outlined), 'CREATE' (solid blue), and 'CANCEL' (outlined).

This visualization provided a clear and interactive view of the network path, including redundant routes and transit nodes. I was able to observe real-time response times and availability variations directly on the NetPath graph, allowing for fast correlation between performance degradation and the network layer responsible for it.

NetPath also offers historical visibility, which is essential for trend analysis. This ability to correlate issues with specific time windows empowers IT teams to investigate degradation patterns and anticipate future problems based on recurring anomalies.

6. Conclusion

This project demonstrated a complete deployment of network monitoring capabilities using SolarWinds NPM, from initial device discovery to advanced visualization with NetPath and automated alerting.

Through each stage of the configuration, I applied critical network monitoring practices that mirror real enterprise workflows:

- Accurate SNMP-based polling and interface tracking,
- Precise NetPath service setup to visualize hop-level latency and availability,
- Targeted alerts to detect anomalies in response time,
- Dashboard customization to enhance network observability.

By working through these steps, I not only deployed a fully functional monitoring system but also gained practical experience in diagnosing network health, identifying performance bottlenecks, and building proactive alert mechanisms.

The result is a modular, scalable setup that can be adapted to larger infrastructures. The ability to monitor latency trends, view hop-by-hop paths, and receive automated alerts reflects core skills expected from network engineers and system administrators in production environments.

This hands-on project helped sharpen my understanding of :

- Network telemetry collection and visualization
- Infrastructure observability
- Proactive monitoring via alert thresholds
- Performance analysis based on real traffic data

This experience allowed me to turn technical configurations into actionable monitoring insights, reinforcing my understanding of network operations in a practical context.