

10 BEST PRACTICES TO STREAMLINE NETWORK MONITORING

By: Vinod Mohan



10 BEST PRACTICES TO STREAMLINE NETWORK MONITORING

INTRODUCTION

As a network admin, you are tasked with keeping your organization's network functioning smoothly, whether your organization has a legacy network with old-fashioned devices and policies, or a rapidly growing network with the latest networking technologies. There are network monitoring tools available on the market—expensive enterprise solutions, 3rd-party software, and open source tools—that can help you stay ahead of network breakdowns by alerting and reporting on the health of your IT infrastructure. But there are other best practices you can follow to help streamline your day-to-day network monitoring processes and successfully implement your [network monitoring software](#). Let's walk through some best practices that can simplify network administration and help you become a network rock star.

1. CONDUCT NETWORK PERFORMANCE BASELINING

A network performance baseline is a set of metrics that define the standard, or normal working conditions, of the network infrastructure. Baseline becomes critical in network performance monitoring when we set up thresholds for performance alerting. To set the right alerting levels for network performance you need to run network baseline tests and understand what the standard working conditions are for your networking devices and hardware. You'll get to know where your network break point is based on increasing network load.

The key objectives of a network performance baseline are to:

- » Determine current status of network devices.
- » Compare current status to standard performance levels.
- » Set thresholds to alert you when the status exceeds those levels.

Once this is done, it's easier to set these alerting conditions on your [network management system](#) (NMS), allowing it to monitor network performance and sound alerts if the device performance deviates from the baseline. Baseline also helps keep you informed about when and where to spend your IT budget on network upgrades.

To start, consider running a baseline test on your network devices (routers, switches, firewalls, etc.) to standardize the following parameters on all your network locations.

- » Traffic on backbone network links.
- » Traffic on WAN links and devices.
- » Traffic for business applications.



- » Traffic to and from critical systems.
- » Traffic for backup systems and storage devices.
- » Traffic on Internet backup lines.
- » Wireless traffic.

Some network monitoring tools offer dynamic baselining to calculate baseline thresholds from historical network performance data.

2. PERFORM NETWORK DEVICE INVENTORY MANAGEMENT

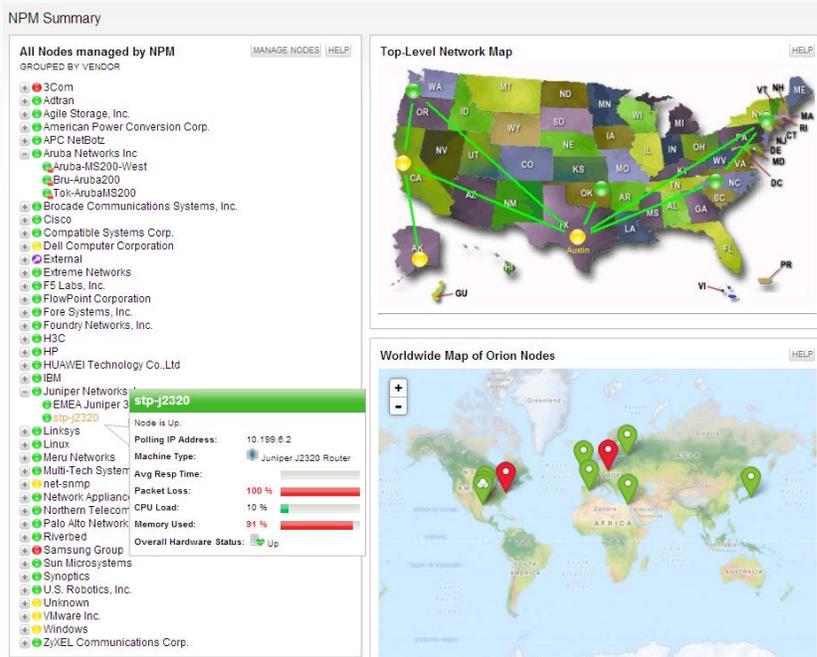
Network inventory management is a key factor in effective network monitoring. You need to keep an inventory of the network devices, ports, and interfaces being used for network connections, network hardware (links, network controllers, power supply, etc.), servers, virtual machines, and SAN devices. Why is this required? Because these are the network elements you need to monitor for network performance. Maintaining a proper asset database helps you track IT equipment for used and unused device count, device EOL information, device configuration changes, and device IP address assignment and utilization status.

The best way to start building your network inventory is to:

1. Discover all the devices you need to monitor.
2. Add those devices as nodes to your network monitoring software.
3. Group them by vendor, location, data center, etc.
4. Track and update [changes to configuration](#), [device location](#), [IP address assignment](#), etc.

After you discover all your devices and have a network asset database, it will be useful to arrange your devices on a network map and make connections to represent your networking topology. This helps you understand the placement of devices with respect to geographic locations. Network mapping helps present a visual representation of your network inventory across your environment. For the best view of your network, you can customize how your maps are structured and nested. [Network discovery](#) and [network topology mapping](#) are essential processes to easily and intuitively maintain network asset inventory for advanced network performance and availability monitoring.





3. UPDATE YOUR MIB DATABASE TO MONITOR CUSTOM NETWORK DEVICES

Typically, your network monitoring software offers you an extensive SNMP management information base (MIB), a database that allows you to poll a range of performance statistics for network devices from various manufacturers. If you have a device that is not supported by the vendor-provider MIB database, you can manually update it with the specific object identifiers (OIDs) of the device that you want to poll using SNMP for performance monitoring.

Some network monitoring software offers the provision of a **custom MIB poller** to add a custom OID or a new MIB from virtually any network device to its original MIB database. This allows you to extend monitoring to cover unconventional and natively unsupported devices, and poll metrics from them, such as:

- » Interface traffic.
- » CPU temperature.
- » Address errors.
- » UPS battery status.
- » Current website connections.



Keeping your MIB database updated to support SNMP polling of unsupported devices helps your network monitoring software encompass virtually any SNMP-enabled network device.

4. CONFIGURE SNMP ON NETWORK DEVICES

If you are using SNMP to retrieve performance metrics from your network devices, you must configure SNMP on them or your NMS will not be able to poll data. For example, if you need to enable SNMP for a Cisco® router or switch, you can telnet to the device, go to the configuration mode, and add a read-only or read-write community string to enable SNMP. SNMP community strings are like passwords that enable monitoring on network devices. You can also allow SNMP traps to receive unsolicited trap notifications, or inform requests on the status network device. Typically, trap notifications indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.



Step 1: Telnet to the Cisco Router

```
prompt#telnet x.x.x.x (IP address of the router)
```

Step 2: Enter the enable password at the prompt in order to enter the enable mode

```
Router>enable  
Password:  
Router#
```

Step 3: Display the running configuration and look for the SNMP information

```
Router#show running-config  
Building configuration...  
....
```

Step 4: Go into the configuration mode

```
Router#configure terminal  
Enter configuration commands, one per line.  
End with CNTL/Z.  
Router(config)#
```

Step 5: Use this command to enable the read-only (RO) community string

```
Router(config)#snmp-server community public RO  
where "public" is the read-only community string
```

(or)

Use this command to enable the read-write (RW) community string

```
Router(config)#snmp-server community private RW  
where "private" is the read-write community string
```

Based on the type of SNMP polling you want to perform (SNMP v1, SNMP v2c, or SNMP v3), enable the corresponding SNMP settings on the target devices and disable the ones you don't want for polling.

5. ENABLE FLOW TECHNOLOGIES ON ROUTERS AND SWITCHES

If you are looking to analyze the traffic packet, network bandwidth utilization, and traffic data, you need to enable one of the flow technologies on the network router or switch. This helps ensure that all the network devices you want to monitor are configured for flow-based packet analysis and remind you not to omit any intended devices for network traffic and bandwidth monitoring.



For example, if you want to enable NetFlow™ on a Cisco router, you can use the following commands on the command line interface (CLI).

Step 1: Specify the interface, and enter interface configuration mode

```
Router(config)# interface type slot/port-adapter/port (Cisco 7500 series routers)
```

(or)

```
Router(config)# interface type slot/port (Cisco 7200 series routers)
```

Step 2: Enables NetFlow for IP routing

```
Router(config-if)# ip route-cache flow
```

Most 3rd-party [network bandwidth monitoring software](#) supports flow-based monitoring for various industry-standard flow technologies such as NetFlow v5 and v9, sFlow® v2, v4 and v5, IPFIX, J-Flow®, HUAWEI® NetStream™, and more.

6. DEFINE OPTIMUM NETWORK MONITORING POLICIES

Every organization should have a well-defined network monitoring policy in place to allow or disallow network monitoring activities based on organizational compliance. The network administration team should outline the scope of network monitoring activity to define:

- » The devices and IT equipment to be monitored.
- » The data to be collected.
- » The purpose of collecting network availability and performance data.
- » The people who should have access to this data.
- » Where the data should be stored and secured.
- » How the data could be used, including for compliance, auditing, and reporting purposes.

Network monitoring policies make it easy to deploy and run an NMS. They also help you define guidelines for carrying out network monitoring activities.

7. IDENTIFY WHO WILL RECEIVE NETWORK ALERTS AND DEFINE AN ESCALATION MECHANISM

Depending on the network baseline thresholds, your network management system will trigger alerts for network performance issues, downtime, faults, errors, etc. You need to determine an alert routing algorithm to define who will receive the alert (IT admin, network admin, network



engineer, or a group of IT pros, etc.) and how the alert should be escalated based on severity or resolution service levels. You can choose to [integrate your NMS with your IT help desk](#) so your network alerts are automatically converted to trouble tickets in your help desk. You can use [alert management software](#) for auto-escalation of alerts to the right recipients based on custom business logic.

8. PREPARE FOR FUTURE NETWORK EXPANSION

Your network evolves based on business and technology requirements. Before deploying a network management system, factor in a network growth forecast analysis to leave license room for more devices and interfaces to be monitored as they are added to your network. Choose a network performance monitoring solution that performs capacity planning so you can receive alerts about projected capacity exhaustion for key metrics, such as bandwidth usage, memory usage, disk space, etc. Forecast when critical capacity will be exhausted, based on peak and average use calculation.

9. PLAN FOR NMS FAILOVER AND HIGH AVAILABILITY

Should there be a server hardware failure, power failure, or scheduled or unplanned maintenance upgrade, it's possible that your NMS will not be available, leaving your network unmonitored. Prepare for your network to have [failover options for your NMS](#) to maintain consistent monitoring. NMS is a critical component of daily operations, especially MSPs. They must run optimally to maintain consistent network fault, availability, and performance monitoring.

10. INTEGRATE NETWORK MONITORING WITH OTHER IT MANAGEMENT PRODUCTS

Enhance the efficiency of your IT infrastructure by unifying the different products you may have deployed for [server and application monitoring](#), [network configuration management](#), [virtualization management](#), etc. Once these are unified on a single console along with your NMS, you will have a single-pane-of-glass view to monitor your IT landscape. This makes it easy to troubleshoot and identify the root cause of application downtime issues and remediate them quickly.

The key benefits of using an NMS integrated with other IT management modules:

- » Save time by accessing just one management console.
- » No need to educate your IT workforce about different monitoring platforms.
- » Save user access management overhead with single user logins.

The sections above provide some best practices that any organization implementing a network monitoring software should follow. Doing so will provide the best benefit of your NMS implementation, and allow you to manage your network more efficiently.



RESOURCES FOR ADDITIONAL LEARNING

1. White paper [Network Management Back to the Basics](#)
2. Buyer's guide [A Guide to Enterprise Network Monitoring](#)
3. Research paper [Seven Priorities for Network Management](#)
4. Case studies [Rightsizing Your Network Performance Management](#)

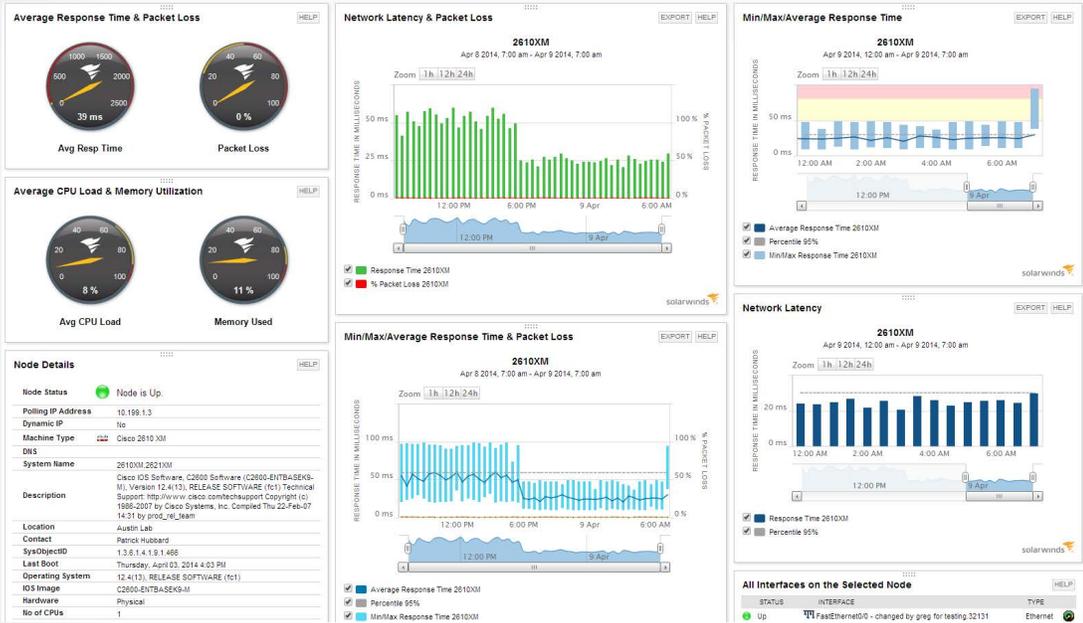
ABOUT SOLARWINDS NETWORK PERFORMANCE MONITOR

SolarWinds® Network Performance Monitor (NPM) makes it easy to detect, diagnose, and resolve performance issues before outages occur. SolarWinds NPM is an affordable, easy-to-use tool that delivers real-time views and dashboards, enabling you to visually track and monitor network performance at a glance. Plus, using automated network discovery, network topology maps, capacity forecasting, alerting, and reporting you can keep up with your evolving network without breaking a sweat. Discover, map, and monitor your network in about an hour!

Feature Highlights:

- Speeds detection, diagnosis, and resolution of network issues before outages occur.
- Monitors and displays response time, availability, and performance of network devices.
- Automatically discovers and maps network devices and typically deploys in about an hour.
- Improves operational efficiency with out-of-the-box, customizable dashboards, alerts, and reports.
- Get an enhanced view of your network with automatic capacity planning, wireless heat-maps, and topology-aware intelligent alerts.
- Automatically calculates network latency and correlates to end-user experience.





ABOUT SOLARWINDS

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide. Focused exclusively on IT pros, we strive to eliminate the complexity in IT management software that many have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use, and maintain, while providing the power to address any IT management problem on any scale. Our solutions are rooted in our deep connection to our user base, which interacts in our online community, [thwack®](http://thwack.com), to solve problems, share technology and best practices, and directly participate in our product development process. Learn more at <http://www.solarwinds.com>.