Network Monitoring & Management

NETWORK MANAGEMENT SYSTEM

Stands for "Network Management System." An NMS is a system designed for monitoring, maintaining, and optimizing a network. It includes both hardware and software, but most often an NMS refers to the software used to manage a network.

Network management software usually collects information about network devices (which are called Nodes) using protocols like SNMP, ICMP, CDP etc. This information is then presented to network administrators in an easy to understand and accessible manner to help them quickly identify and remediate problems.

Why use an NMS?

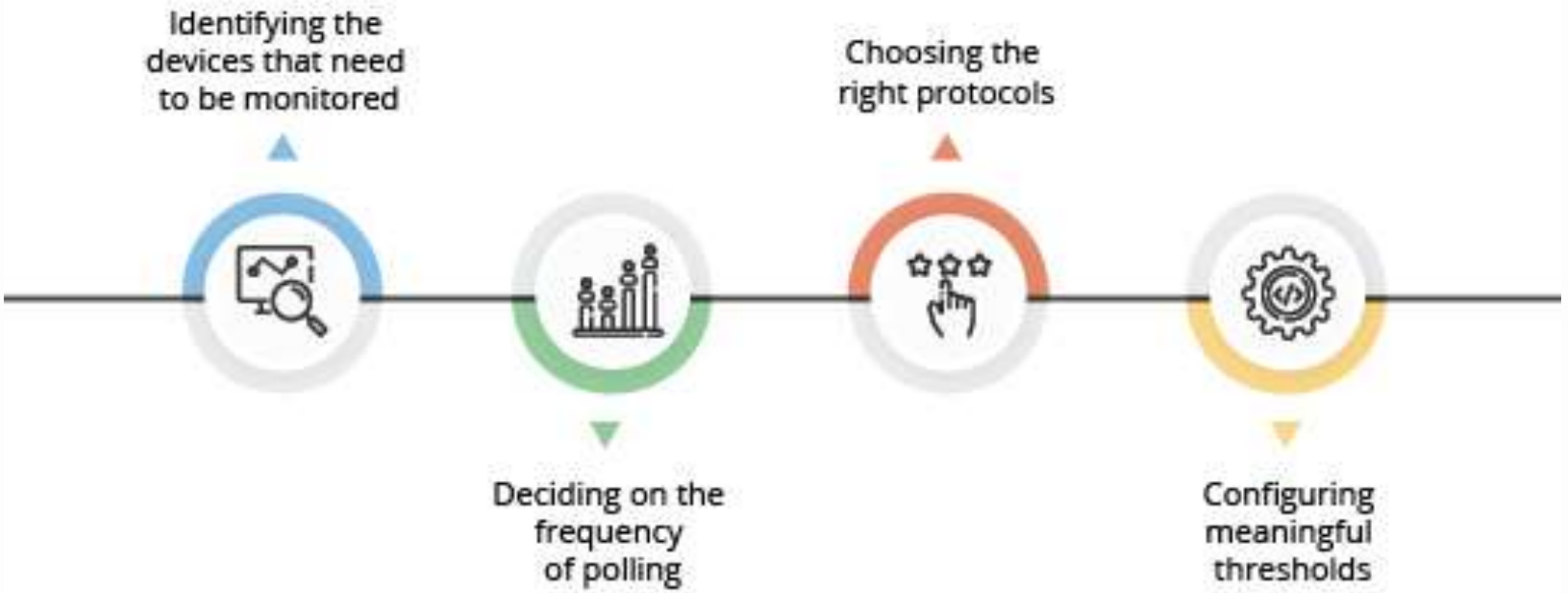
- Server farms, data centers, and corporate networks may have hundreds or thousands of connected devices.
- It is important to have a central network monitoring system in place to manage the devices.
- An NMS provides and efficient way to locate, update, repair, and replace network equipment as needed.

Network management systems provide multiple services. These include, but are not limited to:

- **Network monitoring** - NMS software monitors network hardware to ensure all devices are operating correctly and are not near or at full capacity. Alerts can be sent to network administrators if a problem is detected.
- **Device detection** - When a new device is connected to the network, the NMS detects it so that it can be recognized, configured, and added to the network.
- **Performance analysis** - An NMS can gauge the current and historical performance of a network. This includes the overall performance of the network as well as individual devices and connections.
- **Device management-** An NMS can provide a simple way to manage multiple devices from a central location.
- **Fault management** - If a device or section of a network fails, an NMS may be able to automatically reroute traffic to limit downtime. When a fault occurs, a network alert or notification is usually sent to one or more network administrators.

Network Monitoring & Management

Network monitoring is a critical IT process where all networking components like routers, switches, firewalls, servers, and VMs are monitored for fault and performance and evaluated continuously to maintain and optimize their availability. One important aspect of network monitoring is that it should be proactive. Finding performance issues and bottlenecks proactively helps in identifying issues at the initial stage. Efficient proactive monitoring can prevent network downtime or failures.


Identifying the devices that need to be monitored
Deciding on the frequency of polling
Choosing the right protocols
Configuring meaningful thresholds

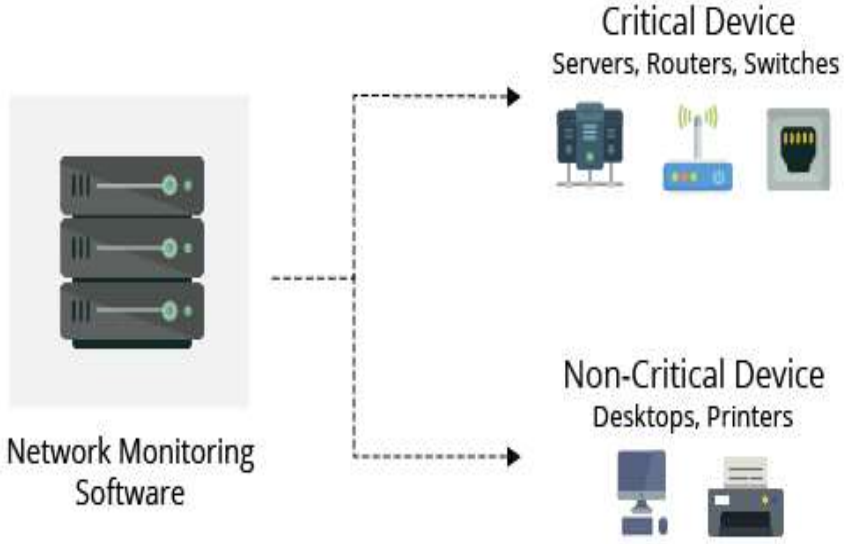
Important aspects of network monitoring

- Monitoring the essentials
- Optimizing the monitoring interval
- Selecting the right protocol
- Setting thresholds

Monitoring the essentials.

- In effective network monitoring, the first step is to identify the devices and the related performance metrics to be monitored.
- The second step is determining the monitoring interval.

Devices like desktops and printers are not critical and do not require frequent monitoring whereas servers, routers and switches perform business critical tasks but at the same time have specific parameters that can be selectively monitored.



Monitoring interval

Monitoring interval determines the frequency at which the network devices and its related metrics are polled to identify the performance and availability status.

Setting up monitoring intervals can help to take the load off the network monitoring system and in turn, your resources. CPU and memory stats can be monitored once in every 5 minutes.

The monitoring interval for other metrics like Disk utilization can be extended and is sufficient if it is polled once every 15 minutes.

Protocol and its types.

When monitoring a network and its devices, a common good practice is to adopt a secure and non-bandwidth consuming network management protocol to minimize the impact it has on network performance.

Most of the network devices and Linux servers support SNMP(Simple Network Management Protocol) and CLI protocols and Windows devices support WMI protocol.

SNMP is one of the widely accepted protocols to manage and monitor network elements.

Allowing SNMP read-write access gives one complete control over the device.

A network monitoring system helps the administrator take charge of the network .

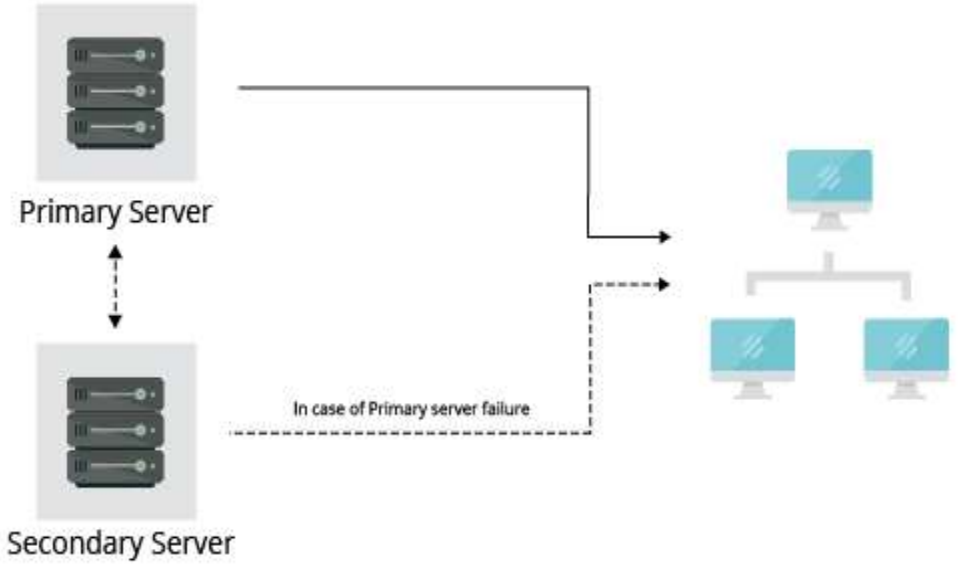
Site monitoring services can check HTTP pages, HTTPS, SNMP, FTP, SMTP, POP3, IMAP, DNS, SSH, TELNET, SSL, TCP, ICMP, SIP, UDP, Media Streaming and a range of other ports.

Proactive monitoring and Thresholds

- Network downtime can cost a lot of money.
- In most cases, the end-user reports a network issue to the network management team.
- The reason behind this is a poor approach to proactive network monitoring.
- The key challenge in real time network monitoring is to identify performance bottlenecks proactively.
- This is where thresholds play a major role in network monitoring. Threshold limits vary from device to device based on the business use case.
- Utilizing thresholds, alerts can also be raised before the device goes down or reaches critical condition.

What happens when your trusted *network monitoring t*ool is running on a server that crashes?

If a failure occurs in the primary server, the secondary server is readily available to take over and the database is secure. This ensures a hundred percent network and device uptime.



Benefits of the Failover system:

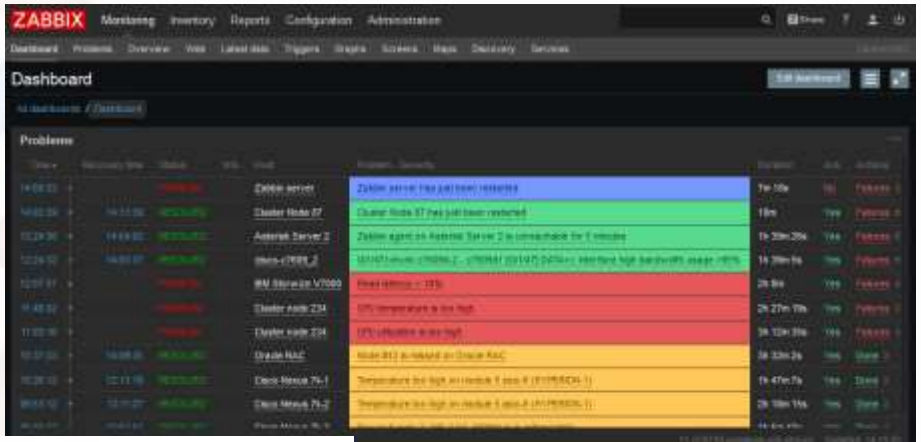
- Instantly recognize primary server failure.
- Immediate notification via email in event of a primary server failure.
- 100% uptime and uninterrupted network management.
- Automated, seamless switching between the Primary server to Standby server and vice versa.

Features of an effective network monitor software:

- Visualizing your entire IT infrastructure with further classifications based on type or logical groups.
- Automatic configuration of devices and interfaces with predefined templates.
- Monitor and troubleshoot network, server and application performance.
- Implement advanced network performance monitoring techniques to quickly resolve network faults by getting to the root of the problem.
- Get advanced reporting features with provision to schedule and automatically email or publish the reports.

Some monitoring tools

- Cacti®
- Zabbix®
- Ntop
- Icinga
- Spiceworks



Conclusion

Monitoring network has become an important aspect of managing any IT infrastructure. Similarly, a network assessment is considered an elementary step in aligning your IT infrastructure towards the business goals, enabled by network monitoring application.

Thank you