Lecture 9. Network monitoring

Definition

Network monitoring is the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages or other trouble.

Network monitoring is part of network 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.

While an intrusion detection system monitors a network threats from the outside, a network monitoring system monitors the network for problems caused by overloaded or crashed servers, network connections or other devices.

For example, to determine the status of a web server, monitoring software may periodically send an HTTP request to fetch a page. For email servers, a test message might be sent through SMTP and retrieved by IMAP or POP3.

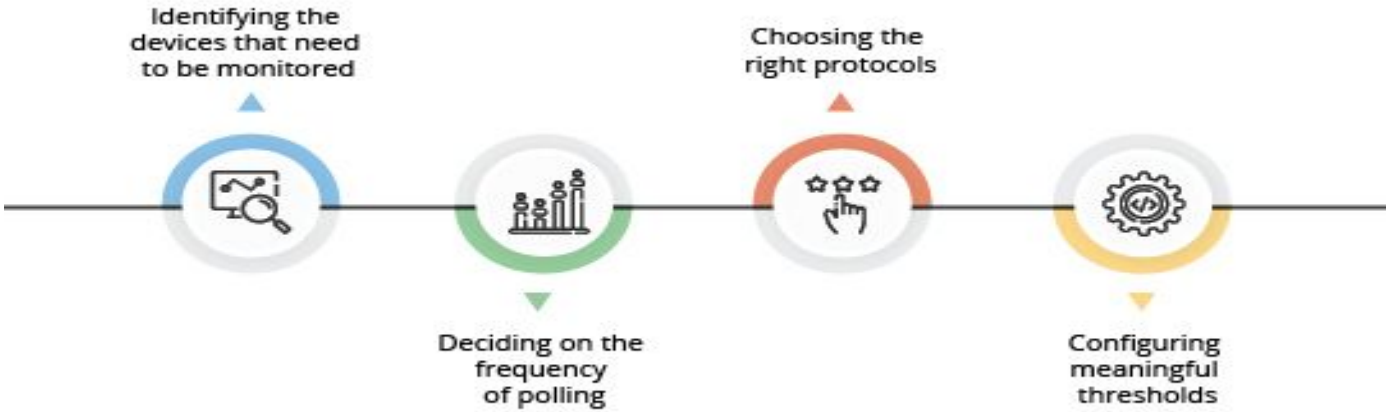
Commonly measured metrics are response time, availability and uptime, although both consistency and reliability metrics are starting to gain popularity. The widespread addition of WAN optimization devices is having an adverse effect on most network monitoring tools, especially when it comes to measuring accurate end-to-end delay because they limit round-trip delay time visibility

Status request failures, such as when a connection cannot be established, it times-out, or the document or message cannot be retrieved, usually produce an action from the monitoring system. These actions vary; An alarm may be sent (via SMS, email, etc.) to the resident sysadmin, automatic failover systems may be activated to remove the troubled server from duty until it can be repaired, etc.

Monitoring the performance of a network uplink is also known as network traffic measurement.

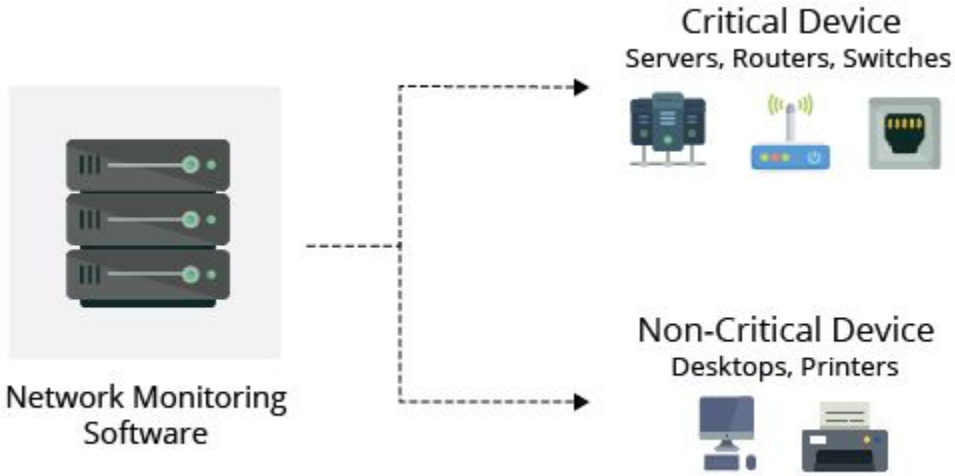
Aspects of Network monitoring

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



Monitoring the essentials

Faulty network devices impact network performance. This can be eliminated through early detection and this is why continuous monitoring of network and related devices is essential. 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. The interval depends on the type of network device or parameter being monitored. Availability status of devices have to be monitored the least interval of time preferably every minute. 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. Monitoring every device at the least interval will only add unnecessary load to the network and is not quite necessary.

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 network protocols to manage and monitor network elements. Most of the network elements come bundled with a SNMP agent. They just need to be enabled and configured to communicate with the network management system (NMS). Allowing SNMP read-write access gives one complete control over the device. Using SNMP, one can replace the entire configuration of the device. A network monitoring system helps the administrator take charge of the network by setting SNMP read/write privileges and restricting control for other users.

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.

Instant alerting based on threshold violations.

Configuring thresholds helps in proactively monitoring the resources and services running on servers and network devices. Each device can have an interval or threshold value set based on user preference and need. Multi-level threshold can assist in classifying and breaking down any fault encountered. Utilizing thresholds, alerts can also be raised before the device goes down or reaches critical condition.

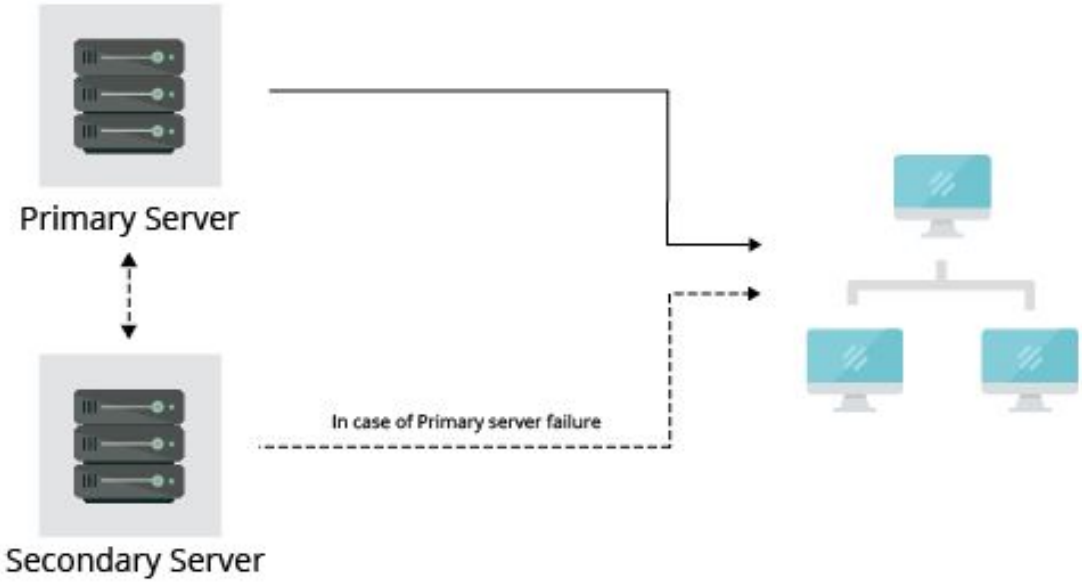
Dashboards and customization

Data becomes useful only when it is presented clearly to the right audience. It is important for IT administrators and users to know about critical metrics as soon as they log in. A network dashboard should provide an at-a-glance overview of the current status of your network, with critical metrics from routers, switches, firewalls, servers, services, application, URLs, printer, UPS and other Infrastructure devices. Support for widgets to monitor the required specifics and real-time performance graphs can help administrators quickly troubleshoot problems and monitor devices remotely.

High Availability and Fail-over

What happens when your trusted network monitoring tool is running on a server that crashes or loses network connection? You will want to be alerted on this and also have the situation automatically remedied using a back-up/stand-by of another twin network monitor application installation. High availability refers to the continuous availability of a monitoring system. Every single network incident - device sickness, unhealthy bandwidth levels, DoS attacks etc., should be immediately brought to your notice so that counter-measures can be taken immediately.

Failover and fail-back functionality ensures an always-monitored network environment by utilizing a secondary standby server. 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.


Primary Server
In case of Primary server failure
Secondary Server

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.

Network monitoring solutions

The process of network monitoring and management is simplified and automated with the help of network monitoring software and network monitor tools. A network monitor system is essential to tackle network bottlenecks and performance woes which might have a negative impact on network performance. With the sudden spurt in enterprise network monitoring, and remote network monitoring, a wide range of network monitoring device and network monitoring solutions are available in in the market. An effective network management system will contain a built-in network monitor tool can help admins cut down on the workforce and automate basic troubleshooting techniques.

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.

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 for your attention!