WHITE PAPER

What is Network Monitoring?

A Complete Handbook

PARK PLACE TECHNOLOGIES

ParkPlaceTechnologies.com

Table of Contents

PARK PLACE TECHNOLOGIES

What is Network Monitoring?

Network monitoring is the practice of identifying characteristics and behavior within network components that are indicative of the need to intervene to address problems, including but not limited to performance, availability, latency, and reachability.

Network monitoring solutions are designed to monitor network components while providing operators with sufficient information to do their job: keep things running smoothly.

Concurrently, network monitoring software provides information to operators who may have subtly different objectives, such as improving the performance of the network rather than fixing it. Network monitoring solutions can help network professionals who are responsible for capacity planning, anticipating trends based upon previous behavior, identifying future investments, and determining the necessary changes for accommodating organizational growth.

What are Today's Network Monitoring Challenges?

It's difficult to describe the changes taking place in the industry which introduce complications to the network without establishing the technological history that precipitated network monitoring. Essentially, it all began with the onset of virtualization.

For well over a decade, virtualization in various forms has been sweeping through information technology. Its initial impact was on server hosting; the virtualization of servers is where it made its first appearance, which in many ways simplified provisioning.

While the inception of virtualization made life simpler and more efficient, as with any new technology it also created a new set of challenges. In the beginning stages of virtualization, the introduction of new technologies often called for a complete rewrite of the monitoring strategy. Network monitoring was created to alleviate these problems, allowing organizations to adopt emerging technology without starting from ground zero.

Today, virtualization has moved into the software defined world, shifting the philosophy of virtualization into the network as opposed to server hosting. Software defined networking and software defined wide area networks have made their way to the forefront, with SD-WAN positioned to promise enterprises the ability to freely utilize transport services, from MPLS and LTE to broadband internet.

In many ways, SD-WAN is a reinvention of technologies that have been around for a long time, just as Ethernet switching was a reinvention of bridging (although with a few improvements that made it more palatable). First there were bridges; then there were routers, designed to overcome the problems created by bridging. Next, Ethernet switching was born to improve the performance of local area networks, avoiding some of the pitfalls that bridging ran into.

Today, SD-WAN provides a way to optimally take advantage of multiple wide area connections. There also remains commodity internet, offered at the lowest prices. In addition, there are higher performing, but more expensive circuits frequently provided via IP-VPNs which are backend provisioned using MPLS. Finally, there are wireless backup circuits and various other technologies for interconnecting on a wide area basis. The objective of SD-WAN is to enable the ability to optimally use any combination of these technologies to achieve the best connectivity cost-effectively, and for the most appropriate application.

Here's the problem: there is no consistent management interface for the multitude of different SD-WAN products available. Historically, simple network management protocol (SNMP) held the network management world together. However, especially in the case with SD-WAN, SNMP has been eschewed while proprietary APIs have been introduced – many of which are based on RESTful API principles. Consequently, SD-WAN products are incompatible, necessitating separate development operations for every vendor. This practice is time consuming, expensive, and risky in consideration of the fact that many SD-WAN vendors are likely to eventually be absorbed by competitors or fade away.

This technological evolution brings us to the present day, complicating the lives of network administrators, analysts, and managers. Every new technology engenders new concerns for network professionals charged with keeping networks running smoothly while avoiding distractions that aren't a priority.

What Do Network Monitoring Solutions Actually Monitor?

Network monitoring needs to be aware of the equipment in the network: routers, switches, firewalls, load balancers, etc.

Identifying these devices and how they're constructed is critical because many of them are multi modular. It's important to understand their modular nature, configuration, and individual components right down to the asset information, including make, model, version, and serial number. This makes it easier to keep maintenance contracts up-to-date and troubleshoot when things go wrong.

It's also important to be aware of how the network is interconnected via cabling and which wide area connections are available. The network team needs to know what is connected to the network, how, and where.

Underlying the technology itself is the need to appreciate that networks change. Configurations are fluid, particularly where virtualization and software defined designs are concerned. Network changes are taking place with increasing frequency, and if they're not handled as automatically as possible by a network monitoring system, they'll bog down the network team with the burden of an excessive volume of manual overhead. Given the complex nature of modern networking, manual intervention will result in a network management system fraught with inaccuracies, unreliability, and eventually distrust among network operators.

Much of network monitoring consists of overseeing network resources. Consider the following examples:

- **Network Traffic:** Circuits have LAN speed settings that typically can't be exceeded, leading to bandwidth utilization constraints. The amount of traffic that can flow on a circuit is a finite resource.
- **Devices:** Devices have processors with limited capabilities, such as memory. For instance, an access layer Ethernet switch will have several, if not many ports providing connections to multiple endpoints. With a limited number of ports, resource limitations become a concern.
- **VPN Firewalls:** Consider the onset of the COVID-19 pandemic when there was a sudden rush to enable all employees to work from home, often via VPNs. Practically overnight, VPN firewalls were facing limitations, unable to support legions of concurrent VPN tunnels (depending on the license purchased from the manufacturer). E.g., if a company's VPN device can handle up to 300 VPN tunnels but the organization is running at 290 when an onslaught of 50 users need to make a connection, problems ensue.

All the above are examples of finite resources which require constant monitoring to effectively anticipate problems and be aware of capacity.

Given the complex nature of modern networking, manual intervention will result in a network management system fraught with inaccuracies, unreliability, and eventually distrust among network operators.

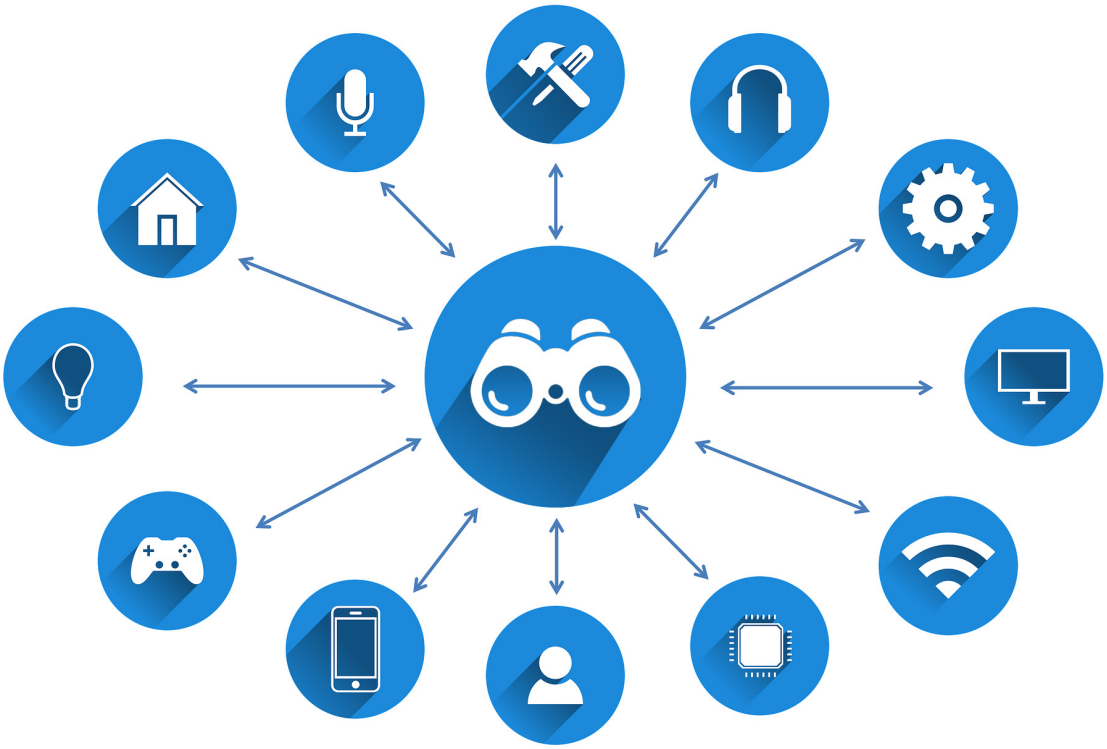
How Does a Network Monitoring System Work?

A network monitoring system performs a multitude of operations, starting with discovering the network devices and its interconnections. The system must know what it's monitoring and how it's configured before it can do the monitoring. It will poll information from the network, typically at regular intervals, although different information may be polled at different periods.

The network monitoring system is also responsible for listening for events such as unsolicited SNMP traps. Devices can also alert network management systems of problems through syslog messages. In addition, there are other forms of monitoring such as NetFlow and other flow protocols which originate from devices and must be interpreted or "listened to."

Polling itself has largely been focused on the use of SNMP protocol. However, there are other monitoring approaches and protocols being used increasingly, including:

- RESTful API communications
- WinRM
- WMI
- SSH



What are the Core Functionalities of a Network Monitoring Solution?

1. **Network Discovery** is the most basic functionality. Providing efficient, meaningful monitoring doesn't make much sense without knowing what the network comprises. Networks change, and the network management system therefore must stay up to date with the changes. Using network discovery functionality, it should be relatively easy to discover, add, and configure devices quickly.

2. **Network Topology** Instant identification and visibility of incidents and their severity across the network is essential to any business, regardless of their size and geographical spread. It should be intuitive and easy to see where there are problems, how serious they are, and what those problems might be affecting. This means being able to represent network equipment and the interconnections between them in a graphical, maintained format that is up to date so that users can see it in the form of a topology map.

3. **Reporting** A good network monitoring solution will offer the ability to build custom reports and dashboards to see the whole network. It's important to be able to build usable, comprehensive network reports that cater to the needs of the business.

4. **Event Management** allows for the is all important when detecting anomalies – a big part of what network monitoring is all about. An advanced event management system organizes network alert data into high-level incidents.

   The single biggest complaint among users of network monitoring systems is that they generate too much event noise. As a result, being able to refine raw detection of anomalies to present to end users is key. Event management allows for the intelligent processing of what's been detected in real time to allow users make sense of it is important.

5. **Application Path Analysis** helps maintain application performance by enabling the ability to visualize precisely how an application's traffic travels through the network. Application path analysis identifies traffic bottlenecks that slow application performance and exposes how the network is being used; not just how busy it is, but how it's providing connectivity between clients and servers.

6. **Flow and NBAR** allow for detailed analysis of flow information, including conversations between source and destination ports. It becomes possible to observe network traffic patterns, trends, and drill down to the exact cause of issues. This uncovers the nature of traffic, who's talking to who, and what they're doing at a high level. It also provides metadata about conversations on the network.

7. **Business Service Modeling** There is a time and a place for thinking at a higher level when it comes to business services. For example: Consider a payroll system which involves multiple servers. There are several things that must function properly for paychecks to come out at the end of the month. In this scenario, the thought process is not centered on individual network components, but rather a collection of equipment.

   One of the key elements of business service modeling is being able to figure out overall availability. In other words, it should determine whether problems exist that could impact the availability of a particular service which could be running interdependently alongside many other services. In the event of a problem, it's crucial to understand the relationship between individual components and all the services they're supporting.

What are the Core Functionalities of a Network Monitoring Solution? (Cont.)

8. **Configuration Management** It's important to note that configuration monitoring and configuration management mean two subtly different things; they're related, but different. Configuration monitoring involves the awareness of device configurations and the changes happening to them. Configuration management involves applying changes from the management system to the devices in the network and allowing operators to execute on these changes in a controlled way.

   Most of the time it's preferred to restrict operator capabilities. For example, it's generally not advisable to allow all operators to run loose about the network, making changes freely. Configuration management is a technique for locking down changes.

   Configuration management is important because a lot of equipment is individually configured. When it comes to traditional switches and routers, each individual device must be individually configured by an operator. In the world of SDN, configurations are set up as policies centrally. When individual devices require separate configurations, being able to monitor configurations and whether they have resulted in the violation of policies is critically important.

9. **APIs** are defined ways of moving data between systems, and they're becoming progressively more crucial – both for talking to devices in the network and interlinking management applications. In some cases, one management application does not address every dimension of requirements, and under those circumstances, it can be very important to integrate with other applications. The richness of an API (how many different functions it allows to be performed, and with what level of flexibility) becomes increasingly important in achieving that.

10. **Predictive Trending** introduces the concept of machine learning and AI, wherein the monitoring system performs additional algorithmic processing on the data that it's gathering to look forward based upon previous behavior. Some network connection problems lend themselves to such a paradigm; others don't. If evidence is building up that a problem is brewing and the system is clever enough to figure that out and provide an early warning, the network team is saved considerable risk, time, and trouble.

11. **Fault Monitoring** is also a fundamental aspect of a network monitoring system. To return to the event noise problem, issues with excessive information often arise in the network monitoring world. To avoid overwhelming operators with irrelevant warnings, it's necessary to differentiate between symptomatic problems and root
    cause problems.

12. **Performance Monitoring** There are many aspects of the network which require performance metrics: levels of traffic, responsiveness of devices and applications within the network, slow or failing components, etc.

What are the Benefits of Network Monitoring?

Networks are too complicated for humans to keep an eye on unassisted. They have thousands, tens of thousands, hundreds of thousands or even millions of individual data points (not necessarily equipment, but things that are going on in that equipment). If network operators were able to watch only the components that matter, life would be easier – but how does one figure out what matters?

This is the idea behind network monitoring. It delivers appropriate automation which observes the network to figure out when intervention is needed. Without appropriate automation to maintain the accuracy of the system's model of the network, monitoring is worthless.

What is the Difference Between Agent-based and Agentless Monitoring?

- **Agentless Monitoring:** First things first: despite the nomenclature, all management requires an agent, whether it's an individually installed piece of software, in a management platform, or in a managed device. That being said, agentless monitoring does not require separate installation or licensing because the management agent is embedded in the device software or as a capability of the manager. Basically, agentless monitoring just refers to the use of embedded capabilities that already exist.

  Fundamentally, if the equipment in the network can provide the desired information, either via polling or through alert such as traps and syslog messages, there is no need for an agent.

- **Agent-based Monitoring:** Agent based monitoring requires an agent to be installed into the node and generally allows for more comprehensive monitoring and management.

  If there is no way to gather relevant information without a mechanism for obtaining it, an agent is necessary. The agent itself may be part of a physical monitoring probe, or it could simply be a background process running on a server. There are many forms of agents.

It can be argued that most network devices, particularly those instrumented through SNMP, already have a pre-installed agent as part of the equipment. Operators do have to configure it, but there's no need to install it since it's already part of the equipment. However, this is not universally true – sometimes agents are necessary. Some network monitoring functions can only be executed via an agent, while other functions can only be executed agentlessly. Ultimately, it comes down to the objective and whether it extends beyond the instrumentation that's already in the equipment.

Without appropriate automation to maintain the accuracy of the system's model of the network, monitoring is worthless.

PARK PLACE TECHNOLOGIES

What is the Role of Cloud in Network Monitoring?

With the rise of cloud in recent years, it's worthwhile to identify its role in the context of network monitoring. Organizations from all industries are hybridizing workloads traditionally processed in their own data centers and often offloading to the cloud. Regardless of deployment methodology, monitoring is still necessary.

When working within the cloud, the cloud vendor is performing the network management and is therefore responsible. However, in the event of problems with workloads processed in the cloud, immediate alerts are key for efficient response times. Some monitoring can be performed from cloud hosted monitoring applications.

What are the Differences Between "Freeware" Network Monitoring Solutions and Commercial Network Monitoring Solutions?

To be clear, freeware is not free – ever. Total cost of ownership is always part of the equation. To that end, it's useful to ask the following questions when making a comparison between the two:

- What level of staff capabilities are necessary for implementing and using a particular monitoring application?
- How much effort is required for implementation?
- How much effort is required for maintenance?
- Does the solution address the requirements for a network monitoring system, or would it be necessary to acquire multiple applications?
- How will staff turnover be handled?
- Does software support consist of relying on an ad hoc international community, or a professional services organization? What are the consequences of each?
- How important is the behavior of the network to the company's functioning?
- How much disruption can be tolerated?
- If there's a problem in the network, how is it going to negatively impact the business?
- What is necessary for appropriately mitigating risk?

Know this: even if network equipment is purchased inexpensively, that doesn't mean commercial monitoring can't be justified. Any busines that will be severely impacted by a network disruption must consider that risk. Remember that the cost of equipment doesn't factor into risk management economics.

What are the Top Network Monitoring Best Practices?

1. **Upfront Planning.**
   Don't just throw a system together; plan for what you're doing. The more upfront planning you do, the more likely you are to get a successful outcome.

2. **Geographic Diversity.**
   Instrument where equipment is located, particularly in the case of a geographically diverse organization. Make sure that the location of all equipment is properly understood and programmed into the equipment so that it can be automatically obtained by the network management system. Plan for how the location information is to be specified so that it's not ad hoc based upon whoever happened to be configuring a piece of equipment.

3. **Identify User Communities who will Benefit from the Monitoring System (Not Just the Network Operators.)**
   Determine ahead of time who wants some level of access to better tailor the system to the needs of each user community. Some users won't be in the trenches solving problems but want a high-level dashboard summarization or reporting type of output.

4. **Minimize Administrative Overheads Using Appropriate Automation.**
   Never automate for the sake of it. Automate to make the lives of network administrators as easy as possible.

5. **Reduce Event Noise.**
   Reduce event noise to prevent operators from the affliction of alert fatigue. When excessive alerts are generated, and a majority are irrelevant, alerts get ignored.

Never automate for the sake of it. Automate to make the lives of network administrators as easy as possible.

PARK PLACE TECHNOLOGIES