Network Monitoring

What is Network Monitoring?

- Network monitoring is the process of constantly monitoring a computer network for problems such as slow traffic or component failure.
- Network Monitoring tools are always scanning the network and are designed to automatically notify network administrators via text, email, or other application such as Slack when a problem occurs.
- Network monitoring software differs from network security or intrusion detection systems in that network monitoring is focused on internal network issues such as overloaded routers, server failures, or network connection issues that could impact other devices.

What is Network Monitoring?

- Indicating any out-of-norm parameters that require further examination or components such as switches, routers, firewalls, servers, and software services, applications, or URLs that could be the source of network disturbances
- Network Monitoring should provide:
  - Visualization of the organization's complete IT and network infrastructure
  - Monitoring, troubleshooting, and remediation of network performance issues.
  - Root cause analysis tools when problems occur.
  - Dashboard with clear visualization tools and reports

Why is Network Monitoring important?

- Network failures can impact overall IT performance and cause availability issues across the organization. Network monitoring has several important benefits to the organization by enabling early detection of issues including:
- Cost savings realized by reducing downtime and speeding remediation by assisting with root cause analysis or displaying network elements that are being over- or under-utilized. Network resources can focus on productive tasks instead of constantly looking for problems.
- Performance problems can be caught before they impact business operations or lead to a degraded customer experience.
- Network security enhancements can be realized by detecting unexpected traffic or unknown devices connecting to the network. These could be early indicators of cyberattacks or ransomware attempts.
- Usage spikes such as logon storms or seasonal traffic jumps can be indicated early on, enabling network administrators to take remedial action to ensure that usage is not impacted.
- Rogue application usage can be caught. Each business unit may have a group of applications they want tracked and network monitoring can establish which applications and users are doing what on the network.

Key benefits of network monitoring

Clear visibility into the network

Through network monitoring, administrators can get a clear picture of all the connected devices in the network. See how data is moving among them, and quickly identify and correct issues that can undermine performance and lead to outages.

Increasing complexity

Modern enterprises rely on a host of internet-dependent, business-critical services. This includes cloud service providers, ISPs, CDNs, as well as SaaS, UCaaS, VPNs and SECaaS providers. Each service operates over the internet, making them susceptible to performance fluctuations caused by internet outages or routing issues. Visibility into the network components beyond your control allows you to monitor issues that might impact employees or customers.

Better use of IT resources

The hardware and software tools in network monitoring systems reduce manual work for IT teams. That means valuable IT staff have more time to devote to critical projects for the organization.

Early insight into future infrastructure needs

Network monitoring systems can provide reports on how network components have performed over a defined period. By analyzing these reports, network administrators can anticipate when the organization may need to consider upgrading or implementing new IT infrastructure.

The ability to identify security threats faster

Network monitoring helps organizations understand what "normal" performance looks like for their networks. So, when unusual activity occurs, such as an unexplained increase in network traffic levels, it's easier for administrators to identify the issue quickly--and to determine whether it may be a security threat.

How does Network Monitoring work?

- There are many types of network monitoring. For instance email network monitoring might involve sending test emails and measuring the response time, while web server testing could entail sending an HTTP request to access a given page and log the time until it is served.
- First, devices and network connections are identified as are their related performance metrics. Next, the organization determines how frequently to monitor each function. For example, client laptops and printers are not 'network critical' and can have much longer monitoring intervals than routers, switches, and servers that comprise the network backbone.
- Most network monitoring tools utilize the simple network management protocol (SNMP) to manage and monitor the elements of the network. Most network components are delivered with an SNMP agent which can be used to reconfigure devices, take them offline if they are performing erratically, or to collect information about the device's performance. Network monitoring systems 'ping' the various system ports, and If a device reports a parameter outside of the established threshold an alert is automatically generated so remediation can occur before device failure. Typically, network components are pinged between once a minute and once an hour.
- Some network devices such as routers and switches utilize the Internet Control Message Protocol (ICMP) to relate information regarding internet protocol (IP) operations and to create error messages when devices fail.

What are the types of Network Monitoring?

- Different devices and protocols are used in network monitoring.
- **Network packet analyzers** examine the data in each packet moving through the network, and the information within the packets can determine if they are being routed correctly, if employees are visiting prohibited websites, or if sensitive data including personally identifiable information (PII) such as social security number is being exfiltrated from the network.
- **Application and services monitoring** focuses on those systems and devices needed to maintain network integrity to ensure they are operating within normal limits as well as indicating which applications are being used by which business units organization-wide.
- **Access Management monitoring** ensures that intruders are not granted access to network resources, for example if an employee suddenly logs on from an IP address on another continent. This can quickly spot network vulnerabilities and help remediate them and detect intruders before they can do harm.
-

Types of network monitoring protocols

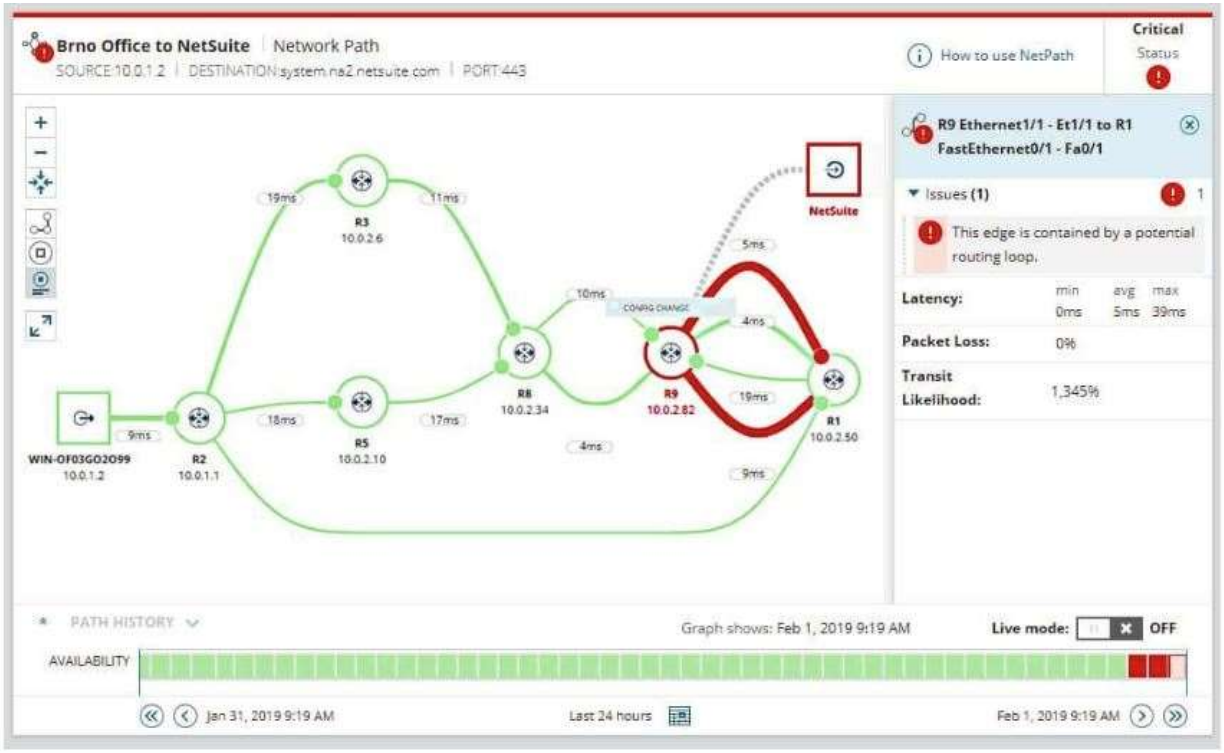
SNMP	The Simple Network Management Protocol (SNMP) is an application-layer protocol that uses a call-and-response system to check the status of many types of devices, from switches to printers. SNMP can be used to monitor system status and configuration.
ICMP	Network devices, such as routers and servers, use the Internet Control Message Protocol (ICMP) to send IP-operations information and to generate error messages in the event of device failures.
Cisco Discovery Protocol	The Cisco Discovery Protocol facilitates management of Cisco devices by discovering these devices, determining how they are configured, and allowing systems using different network-layer protocols to learn about one another.
ThousandEyes Synthetics	ThousandEyes Synthetics is an internet-aware synthetic monitoring solution for proactive detection of modern networked application performance issues.

Types	Pros	Cons
SNMP	• Detect hardware failures and overload of system resources • Provide bytes in/out network interfaces • Always on monitoring (24×7) • Fairly easy to setup	• Lack of end-to-end visibility • Not appropriate for troubleshooting network performance issues • Hardly circumvent network complexity and virtualization • Cannot detect software configuration errors (routing policies, ACL, ...) that affect user traffic
TRAFFIC FLOW	• Accounting and statistics about traffic flows • Protocols breakdown across network links • Identify top talkers • Deep packet inspection analysis	• High disk space consumption • Limited historical data • In-line devices (taps) introduce another point of failure • Taps are generally expensive so cannot be installed everywhere • Mirror ports consume system resources and cannot capture all the flows traversing the node • Require expertise and training • Reactive troubleshooting
ACTIVE	• Detect performance degradation and trends • Always on monitoring (24/7) • Can hold large amount of historical data • Does not require real user traffic to generate KPIs • Test network infrastructure in the pre-deployment phase • Validate configuration changes	• In performing real transactions, these tools consumes network and/or application resources • To be successfully implemented, several hardware or software agents must be deployed in the network

Network monitoring tools

1. SolarWinds Network Performance Monitor –An SNMP-based network monitoring system that includes automated device discovery and a constantly updated network inventory and topology map. Runs on Windows Server.
2. Site24x7 Network Monitor –A tool provides both network device monitoring with SNMP procedures and NetFlow-based traffic monitoring. This is a cloud-based system.
3. Atera – A SaaS platform of tools for managed service providers that includes a remote monitoring system for networks, servers, and applications.
4. Paessler PRTG –A collection of network, server, and application monitors that includes both device monitoring and traffic tracking. Runs on Windows Server.
5. **ManageEngine OpManager** A combination of network and server monitors, this system implements autodiscovery, network topology mapping, and device monitoring thanks to SNMP. Available for Windows Server and Linux.
6. **ITRS OP5 Monitor** A monitoring system that watches all IT infrastructure and includes business operations issues, such as SLAs. Runs on Linux, on Windows over a hypervisor, or on major cloud platforms.
7. **Fortra's Intermapper** An autodiscovery and network mapping tool that offers a wide range of layout templates. Installs on Windows, macOS, and Linux.
8. **Progress WhatsUp Gold** An SNMP-based network device monitor with autodiscovery and automated network topology mapping. Runs on Windows Server.
9. **Nagios XI** An infrastructure monitoring tool that features network monitoring and can be extended by free plugins. Runs on Linux.

Network monitoring tools



Network monitoring tools

- The SolarWinds Network Performance Monitor is the most impressive real-time network monitoring tool. The system starts its service life by scanning your network after installation and logging all of the devices that connect your network together. It creates a network inventory and then draws up a network topology map from that information.
- The software inventory and network topology map are updated regularly with information derived from SNMP status checks, so the monitor immediately knows where any devices have been added, moved, or removed. This constant review of the infrastructure will also tell you whether unauthorized devices have been connected to the network.
- Once the network inventory has been created, the Network Performance Monitoring tool starts its real-time tracking of all network issues. The attractive dashboard for the service includes easy-to-read color-coded graphics that assist in instant problem recognition.
- You don’t have to sit and watch the screens of this tool in order to make sure that you don’t miss any problems emerging on the network because the service will notify you if your attention is needed. The system gets status notifications from agent software running on each network device and sends you a warning by email or SMS so you know to come back to the console.
- Other features in this tool include performance analysis features, such as NetPath, which allows you to see the statuses of all connections on a route between any two given points on the network. The tool can reach across the Internet to monitor remote networks and it can also analyze the paths to Cloud-based services.