Network Monitoring

Description

Network Monitoring

What Is Network Monitoring?

Network Monitoring Is The Process Of Continuously Monitoring The Availability And Performance Of It Entities Accessed Over The Network, Both Lan And Wan. These It Entities Include Applications, Servers, Storage Devices, Virtual Machines, Cloud And User Devices, As Well As Network Switches, Routers And Firewalls. Network Monitoring Tools Collect Data Relating To Availability, Throughput, Delay, Delay Variation And Packet Loss. If The Observed Performance Data Breaches Any Of The Configured Thresholds, Alerts Are Raised, So That The Network Administrator Can Take Remedial Steps.

Business Performance In Today's Globalised Environments Is Dependent On Network And Application Performance Utilizing It On-Premises, In Data Centers, Iaas Cloud And Saas Environments. As Networks Grow Larger And More Distributed Utilizing These Environments, It Becomes More Complex For Administrators To Manage Issues Relating To Network Availability, Security Vulnerabilities And Other Issues That Can Affect Network Performance. Network Monitoring Provides The Capabilities That Enable Administrators Can Use To Detect And Overcome Problems That Arise In The Network.

In The Following Sections, We Will Cover How Network Monitoring Works, How It Benefits Every Organization, And How To Go About Selecting The Right Network Tool For Your Organization.

Table Of Contents

Network Monitoring Overview

Explanation Of Network Monitoring Metrics

Network Monitoring Tools Can Continuously Measure A Set Of Metrics That Indicate The Network Performance Issues In The It Infrastructure. Common Metrics Include:

- **Availability:** Availability monitoring helps administrators track the uptime of switches, routers, firewalls and other critical infrastructure components so they can address problems before they impact the business.
- **Throughput:** Throughput is the rate of data delivered successfully from a given source to the destination over a specified channel.
- **Delay (or latency):** Network delay or latency is the amount of time it takes for a data packet to go from the source to the destination and is primarily caused by the distance between them.
- **Delay variation (or jitter):** Delay variation or Jitter is defined as a variation in the delay of

received packets. It can be caused by a number of factors including network congestion, collisions, and signal interference.
- **Loss**: Packet loss occurs when one or more transmitted data packets fail to arrive at their destination. This can cause noticeable application performance issues, since packets have to be retransmitted before they can be received and processed.

Why Is Network Monitoring Important?

Network Monitoring Offers Many Benefits, Including:

- **Reduced downtime:** The network is a critical aspect of any digital business and involves heterogenous components both in the LAN and the WAN, with some portions which are not in direct control of the organization. The availability and performance of various IT entities accessed over the network need to be monitored continuously in order to ensure that business operations are not impacted and that downtime can be minimised by both pro-active and reactive approaches. Understanding the network's normal performance and behavior is essential for determining its efficiency and how it can be improved.
- **Improved efficiency and reduced MTTR:** Network monitoring helps reduces mean time taken to repair (MTTR), that is the amount of time the IT team needs to spend to resolve issues, since they now know what specific issues are impacting performance and therefore are in a better position to troubleshoot and resolve them.
- **Better visibility across networks:** As systems extend beyond on-premises and include hybrid (on-premises and cloud) approaches as well as multi-vendor environments, visibility becomes increasingly difficult to achieve. Network monitoring could provide a way to ensure their performance and security.
- **Capacity planning**: Network monitoring allows you to identify application performance and other trends and extract data to be used to justify the need for upgrading capacity or technology to meet business needs.

What Are Different Network Monitoring Methods?

Network Performance Monitoring Is Achieved Using Passive And Active (A.k.a. Synthetic) Methods. In Addition, Monitoring Of Network Traffic Data Is Accomplished Passively As Explained Below.

What Is Active Or Synthetic Network Monitoring?

In Active Monitoring Methodology, Specialized Monitoring Probes Are Used For Performance Measurements. The Advantage Of This Approach Is That It Is Not Dependant On The Availability And Proper Functioning Of The Network Devices And Would Have The Capability To Provide Higher Frequency Fine-Grained Measurements, Without Loading The Network. Hence This Capability Will Increasingly Be Deployed For Monitoring Critical Resources In Today's Business Critical Environments. However, Some Organizations Do Not Prefer This Approach Since Additional Probes Need To Be Introduced In Their Network.

What Is Passive Network Monitoring?

In Passive Monitoring Methodology, The Devices In The Network Themselves Provide The Necessary Metrics. The Advantage Of This Method Is That The Monitoring Tool Can Perform Monitoring By Polling The Network Devices For Determining All The Metrics. While This Approach Is Popular And Most Common, The Disadvantage Of This Method, Is That If The Network Devices Malfunction Or Fail, The Relevant Metrics Cannot Be Relied Upon Or Be Available. Also, This Ideally Requires A Separate Management Network To Connect The Management Interfaces Of The Network Devices, Though Many Organizations May Choose Not To Do So.

What Is Network Traffic Monitoring Or Network Flow Monitoring?

Network Traffic Monitoring Is A Passive Monitoring Methodology For Observing And Analyzing Network Traffic For Network Performance, Availability Or Security. It Incorporates Network Sniffing And Packet Capturing Techniques In Monitoring A Network And Generally Requires Reviewing Each Incoming And Outgoing Packet.

While Network Performance Monitoring Provides Performance Metrics At The Infrastructure Level, Network Traffic Monitoring Gives Visibility Of Performance Metrics Actually Experienced By The Various Traffic Flows, End To End.

One Of The Common Industry Approaches Is The Use Of Netflow, A Network Protocol System Defined By Cisco. Netflow Is Now Part Of The Internet Engineering Task Force (Ietf) Standard As Internet Protocol Flow Information Export (Ipfix), And Is Widely Implemented By Many Network Equipment Vendors. Though This Is A Popular Approach, One Disadvantage Is That It Uses Sampling Of The Data, Resulting In Reduced Network Visibility That Makes It Challenging For Teams To Troubleshoot Critical Security Threats Or Performance Issues.

What Are Challenges In Network Monitoring?

It Operations In Most Organizations Are Typically Occupied With Day-To-Day Activities Required To Administer And Keep It Infrastructure Running. Their Key Focus Would Primarily Be To Ensure Uninterrupted Availability Of Resources Required For Optimal User Experience.

The Network Is The Common Factor That Connects All Of Them Together And Since This Involves Both Lan And Wan, Any Performance Issues Faced By End Users In Running Their Applications Is Usually First Attributed To Network Problems. Often When That Is The Case, If Network Administrators Don't Have Sufficient Visibility Of The Performance Of All The Networks, Trouble-Shooting And Rcas Can Take Much Longer.

Thus, Typical Challenges Network Administrators Face Include:

- Lack of control and visibility of WAN and its impact on end-to-end performance of business-critical applications
- Network monitoring tools that provide monitoring based on passive methods like SNMP, cannot be relied upon when device failures occur, since then no information is available just when they are needed the most
- Troubleshooting poor digital experience of remote users who are accessing enterprise applications over the internet, can be challenging especially when the monitoring tool used by the network administrator does not report any performance issues.
- Supporting hybrid environments – on-premises and cloud-based to provide a seamless experience can be difficult, especially when there isn't sufficient visibility into cloud.

What Are Common Monitoring Systems?

Network Monitoring Tools Are Of Broadly Two Types: Hardware-Based And Software-Based.

Hardware-Based Network Monitoring Typically Having Traffic Monitoring Capabilities As Well But Can Prove Too Expensive For Many Organizations.
Software-Based Network Monitoring Tools Are More Affordable And May Support One Or More Of The Following Methodologies – Passive (Polling/Snmp Based), Flow Monitoring, Active Monitoring:

- On-premises software-based tools are those which installed in an organization's servers. This is a traditional software model that is generally priced with a license fee and a maintenance plan for ongoing support.
- Cloud-based tools are those that are installed in public cloud. Because no software needs to be installed directly within the organization's infrastructure, these tools can be installed and

launched quickly. Cloud-based monitoring tools are licensed in a pay as you go, subscription model, offering a high level of flexibility.

How To Find The Best Network Monitoring Tool?

When Considering A Network Monitoring Tool, You Want To Assess These Key Network Monitoring Capabilities:

Ease Of Use: Does The Tool Provide An Intuitive User Interface That Makes It Easy To Monitor Events, Perform Triage, And React To Problems Quickly?

Automatic Discovery: Does The Tool Provide Full Visibility Into Every Device On The Network? A Tool With Automatic Discovery Can Be Really Helpful By Scanning The Network For Connected Devices And Automatically Discovering New Devices When They Are Added

Path View: Does The Tool Provide Visual Representation Of The Network Showing How Devices Are Connected To Each Other? This Would Aid In Easier Analysis Of Performance Issues.

Customizable Dashboards: Does The Tool Provide The Option To Customize And Filter What Data Is Displayed On Graphs And Dashboards? This Helps Network Administrators To Ensure To Focus On Specific Data Sets.

Intelligent Alerting: Is It Possible To Set Up Thresholds Such That Multiple Alerts Are Avoided? How Are Alerts Delivered? Can The Alerts Be Received On Itsm Tools Deployed In The Organization?

Critical Resource Monitoring: Is It Possible To Monitor Specific Resources Which Are Mission-Critical, At Higher Granularity And Accord Higher Priority While Triaging?

Diagnosis And Root Cause Analysis (Rca) Capabilities: Does The Tool Automatically Include Context And Provide Correlation Capabilities (With Ai/Ml Or Without) To Help Trouble-Shoot Problems Quickly

Scalability: Is Network Monitoring Tool Be Able To Scale As Needs Of The Business Grow?

Flexibility For On-Premises Or Cloud Licensing: Does The Tool Provide Support For The Type Of Deployment That Your Organization Needs?

Support Policy: What Types Of Support Options Are Available And Are They Aligned To Your Organizational Needs And Expectations?

Conclusion

Network Architectures Are Constantly Evolving And Continue To Grow Increasingly Complex As Applications And Business Demands Increase. Network Monitoring Provides The Toolsets Needed To Stay Ahead Of Performance Problems And Security Threats — And Resolve Such Issues Before They Impact Users And The Business. With The Right Tool, Digital Businesses Can Be Prepared To Face The Above Challenges.

Contact VeryxBack To Top