Network Monitoring and Troubleshooting

Conducted by Madawa Senevirathna

RAJARATA UNIVERSITY OF SRI LANKA

FACULTY OF TECHNOLOGY

What Is Network Monitoring

Network monitoring provides the information that network administrators need to determine, in real time, whether a network is running optimally. With tools such as networking monitoring software, administrators can proactively identify deficiencies, optimize efficiency, and more.

What are network monitoring systems

Network monitoring systems include software and hardware tools that can track various aspects of a network and its operation, such as traffic, bandwidth utilization, and uptime. These systems can detect devices and other elements that comprise or touch the network, as well as provide status updates.

Network administrators rely on network monitoring systems to help them quickly detect device or connection failures or issues such as traffic bottlenecks that limit data flow. The ability to detect issues extends to parts of the network traditionally beyond their demarcation boundaries. These systems can alert administrators to issues by email or text and deliver reports using network analytics.

What are the protocols for network monitoring

Protocols are sets of rules and directions for devices on a network to communicate with one another. Network hardware must use protocols in order to transmit data. Network monitoring systems use protocols to identify and report on network performance issues.

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.

Key benefits of network monitoring

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.

Key benefits of network monitoring

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.

Key benefits of network monitoring

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.

Key benefits of network monitoring

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.

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.

Types of network monitoring protocols

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.

Types of network monitoring protocols

Cisco Discovery Protocol

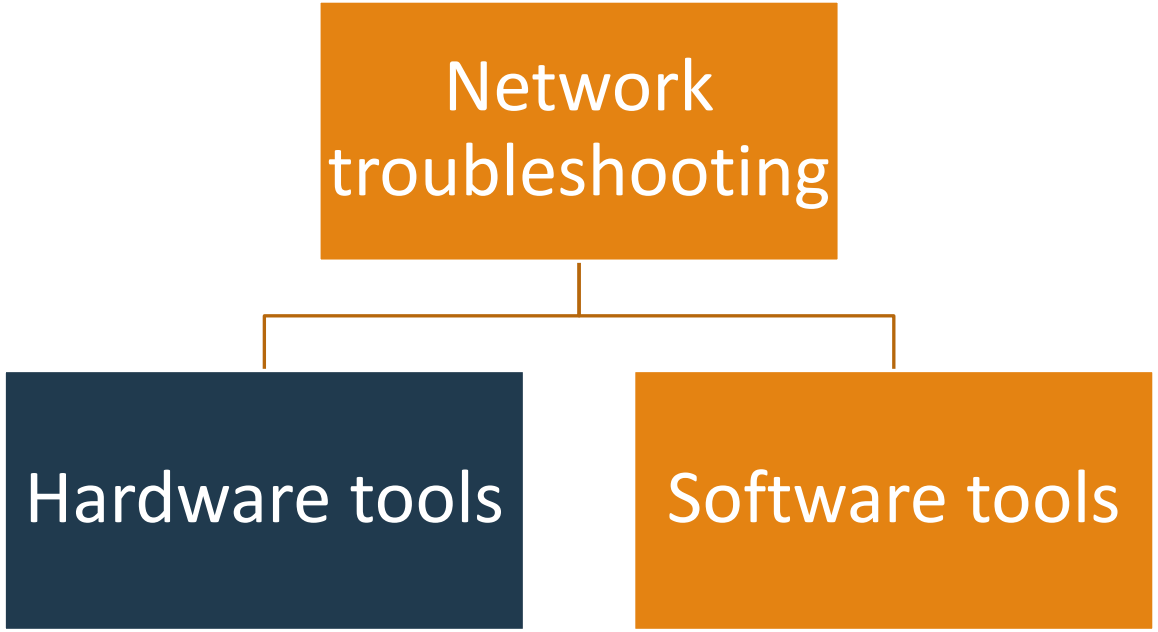
The Cisco Discovery Protocol facilitates management of Cisco devices by discovering these devices, determining how they are configured, and allowing systems using different network-layer protocols to learn about one another.

Types of network monitoring protocols

ThousandEyes Synthetics

ThousandEyes Synthetics is an internet-aware synthetic monitoring solution for proactive detection of modern networked application performance issues.

Network troubleshooting



Cable tester

It is also known as a media tester. It is used to test whether the cable works properly or not. The cable testers will confirm whether a cable works correctly and if there is a problem with the cable. Tools which are used for testing of the cable can be classified as a cable tester.

Protocol analyser

This tool is used to analyse the network protocols like UDP, TCP, and FTP etc. This acts as a software as well as hardware-based tool. This tool is also used to identify malicious networks traffic.

Multimeter

It is used to check shorts in the coaxial cable; it can measure current, resistance and voltage. The new version of multi meter also allows measuring the temperature.

Ping

The ping is a famous tool which is used to perform connectivity tests between the requesting host and the destination host. The Internet Control Message Protocol (ICMP) protocol is used to perform this. If the requesting host receives a response from the destination host the host is reachable otherwise it is not reachable.

Speedtest.net

This is simple software that can be installed in devices or some add-ons in the browsers. This tool allows the user to check the bandwidth available.

Net sat

Net sat means network statistics It is used for finding problems in the network and also it can determine the traffic on the network.

Hardware tools VS Software tools

While we compare both it depends on the use of the tool and for some use software tool is less costly and for some use hardware tool is less costly.

For example, to check the bandwidth online tools which are less costly are used instead of hardware tools and for checking connection in some cases hardware tools are good.

Trouble shooting consists of 3 steps

Different approaches to network troubleshooting are

- Bottom-up
- Top-down
- Divide and conquer

Troubleshooting tools

For internet related problem

Check the connectivity with the default gateway. Check if the DNS server is configured on the PC. Check if the appropriate port number is active using nmap on the DNS server.

Troubleshooting tools

For troubleshoot Ftp server related problems

Test basic connectivity with ping, check with nmap if the ports are open (20and 21)check if a firewall is restricting traffic to the server.

Troubleshooting tools

For DNS problem

Ping the DNS server and check the response. Check with the Wireshark if DNS request and response packets are being sent and receive

Managing troubleshooting security for network system

- Use Encrypted Wireless Network Points
- Track Users and Devices
- Keep Strong Passwords
- Maintain an Inventory
- Perform Security Testing
- Avoid Using Unknown Software

?


thank
you