Lecture 9
ITT565
Network Monitoring

- **Types of Network Monitoring**
- **Network Design**
- **Network Monitoring Scenarios**

Introduction: Network Characteristics

- **The significance and relevance of network characteristics vary with applications.**
- **A content distribution network may be interested in measuring latency from its clients to the application server, whereas a load balancing application may find available bandwidth as a useful criterion to adjust the load on the servers.**
- **Other network characteristics such as congestion, queuing delay, network failure, topology discovery, and bottleneck determination also have great significance.**
- **However, there are four network characteristics that constitute the basic paradigm of network measurements and could be utilized in the computation of other related network characteristics.**

Ref: Shamsi.J, Principle of Networking, 2009.

- **Four network characteristics that constitute the basic paradigm of network measurements:**
  1. **Latency**
  2. **Packet Loss**
  3. **Path Detection**
  4. **Bandwidth**

Ref: Shamsi.J, Principle of Networking, 2009.

- **Latency:**
  - **Latency refers to the time taken by the message to traverse from the sending host to the destination host.**
  - **It is usually measured in milliseconds (ms).**
  - **Latency of a path has great significance for many applications.**
  - **For many applications latency is used to determine the availability of the servers and select the nearest available server in terms of latency, specifically in the *content distribution* networks.**
  - **Further, variation in latency (i.e. the deviation between the successive latency measurements) is used to determine the quality of the path and detect network congestion.**

Ref: Shamsi.J, Principle of Networking, 2009.

- **Packet Loss:**
  - **If the rate of packets sent from the source host is not equal to the rate of packets received at the destination host, then the path experiences packet loss.**
  - **Loss rate of a path is the rate (in percentage) at which packets are being lost while traversing through the network path.**
  - **Lost packets affect the performance of the application as they are often required to be retransmitted.**
  - **Even when the packets cannot be retransmitted (for example, the live transmission of audio or video streams), a high packet loss could lead to low application performance.**
  - **Due to these reasons, selecting paths with a low loss rate is always desirable.**

Ref: Shamsi.J, Principle of Networking, 2009.

Path Detection:

- When a message is sent across the Internet, it traverses through various intermediate routers to reach the destination.
- Path detection is the process of determining the actual path taken by the message in reaching from source to destination.
- Since there are many possibilities for a path from one host to another, path detection enables an application to determine the actual path taken by the message during transmission.
- Path changes are possible on the Internet therefore path detection also facilitates determining a change in the path between two nodes.
- It can also be used as a sanity check to determine or isolate network failure.

Ref: Shamsi.J, Principle of Networking, 2009.

- **Bandwidth:**
  - **Bandwidth refers to the capacity of the path to transfer data in a unit of time.**
  - **It is measured in bits per second (bps).**
  - **Bandwidth has great implications for multimedia applications. Such applications generally have high bandwidth requirements.**
  - **If the available path has limited bandwidth then the multimedia application suffers degraded performance.**
  - **Bandwidth detection tools can be used to infer the path quality and select the appropriate path.**

Ref: Shamsi.J, Principle of Networking, 2009.

Types of Network Monitoring

- active monitoring
- passive monitoring.

Ref: Shamsi.J, Principle of Networking, 2009.

Active **Monitoring**

- **Active Monitoring**
  - **Active monitoring involves injecting probes in the network, specifically for the purpose of monitoring.**
  - **Active monitoring bears the cost of sending additional traffic in the network; however, under most scenarios, the packet size is relatively small compared to the actual capacity of the network, therefore the cost of injecting additional traffic is minimal.**
  - **The cost of injecting traffic can be reduced by decreasing the probing rate; however, this may reduce the quality of the measured characteristics.**
  - **Active monitoring provides full control with respect to monitoring interval, packet size and the path to be monitored.**
  - **Further, the data obtained is not specific to any particular application.**

Passive Monitoring

- **Passive monitoring is the process of observing the existing network traffic and collecting information from it without injecting additional monitoring probes into the network.**
- **In a passive measurements, based system, network measurement information is retrieved through the packets which are sent as a part of another application.**
- **Packets are captured by monitoring the application, which is deployed either on the source and the destination hosts or along the path through a tap.**

Passive Monitoring

- The passive mode of monitoring avoids the overhead of introducing measurement traffic in the network and evades the use of stale data for measurements.
- However, in passive mode the monitoring application has little or no control over probing interval, packet size or the path to be monitored.
- Further, due to the increase in the capacity of the core links, it is expensive to identify and measure the packet of a particular flow. Passive monitoring could also raise privacy concerns.

- The preference for the type of monitoring varies with the application.
- passive approach:
  - intrusion detection system (application measuring the performance of an existing application)
- Active approach:
  - load balancing (application employing performance enhancement)

- **An application may also employ a combination of passive and active schemes for higher efficiency.**
- **The Wren grid monitoring system utilizes such a scheme, in which the passive mode is used when an application is sending messages, whereas the active mode is used when the application is silent**

Network protocol

- For passive monitoring, the measurement system has no choice for the underlying protocol of network measurement i.e. the monitoring application monitors packets that are sent as a part of another application.
- However, in the active mode, the measurement system must decide about the underlying protocol used for sending probes.
- The protocol involves are: ICMP, TCP, UDP

- **ICMP**
  - ICMP or Internet Control Message Protocol is the underlying protocol for the famous ping utility.
  - It operates at the networking layer. The principal advantage of the ICMP-based measurement tools is simplicity and ease of use.
  - ICMP-based schemes do not require connection setup or handshake.
  - Further, they do not require any specific implementation at the recipient end, i.e. only the host sending the active probes implements a mechanism for sending the ICMP probes.
  - Since ICMP messages are control messages, an ICMP request is automatically replied to by the destination host.
  - However, the automatic response capability of the host could be exploited by attackers and is seen as a security vulnerability.
  - A continuous ping will cause buffer overflow at the target system and will cause the target system to crash.
  - ping utility is implemented using the ICMP echo request and echo reply messages.

- **TCP**
  - TCP (Transmission Control Protocol) is the underlying protocol for many internet applications including WWW and FTP.
  - It operates at the transport layer.
  - Unlike ICMP-based tools, TCP-based utilities bear the overhead of the TCP handshake.
  - TCP-based tools also require that the destination host runs a service on a designated port.
  - The sending host establishes a TCP connection to the destination through the TCP handshake and sends probes to the destination host at the server port.
  - The server at the destination replies with a response that is used for network measurement.

TCP

- An important limitation of the TCP-based tools is that since TCP is not a packet-based protocol, it makes its own decisions about sending packets,
- By using various optimizations, including the Nagle algorithm [34], TCP coalesces packets of small sizes.
- Since TCP has a large overhead including a 40-byte header (20 bytes for IP and 20 for TCP), these optimizations allow TCP to conserve bandwidth.

TCP

- **In some cases, the requirement of a running service at the destination can be eliminated using TCP ACK and RST.**
- **According to RFC 793 [33], if a sender sends a TCP ACK packet to a closed TCP port, then the TCP at the destination will reply with the TCP RST packet and the same sequence number as of the TCP ACK packet in the request.**
- **In such a case, the TCP RST can be used as a response.**
- **However, this type of request-response method can be used only if the response from the destination host is not specific to the request, i.e. the response is not generated based on the contents in the request.**

UDP

- **UDP (User Datagram Protocol) is a datagram-based protocol that operates at the transport layer.**
- **Unlike TCP, UDP does not require a handshake.**
- **Additionally, UDP has an 8-byte header (plus 20-byte IP header) that results in lower overhead than TCP.**
- **Since UDP is a packet protocol it allows sending probe packets at controlled intervals.**
- **Moreover, UDP is a connectionless protocol in which a lost request (or a response) can be effectively used to detect packet loss.**

UDP

- Like TCP, UDP can also eliminate the need to run a service at the destination port.
- If a UDP request is received at a port at which the service is not running, then it responds by sending an ICMP destination unreachable message to the sender.
- Many other choices such as DCCP (Datagram Congestion Control Protocol) and SCTP (Stream Control Transmission Protocol) also exist.
- The selection of underlying protocol for network monitoring is based on the requirements and restrictions of an application.

Network Monitoring

- **In today's world, the term network monitoring is widespread throughout the IT industry.**
- **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.**

Ref: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html

Network Monitoring

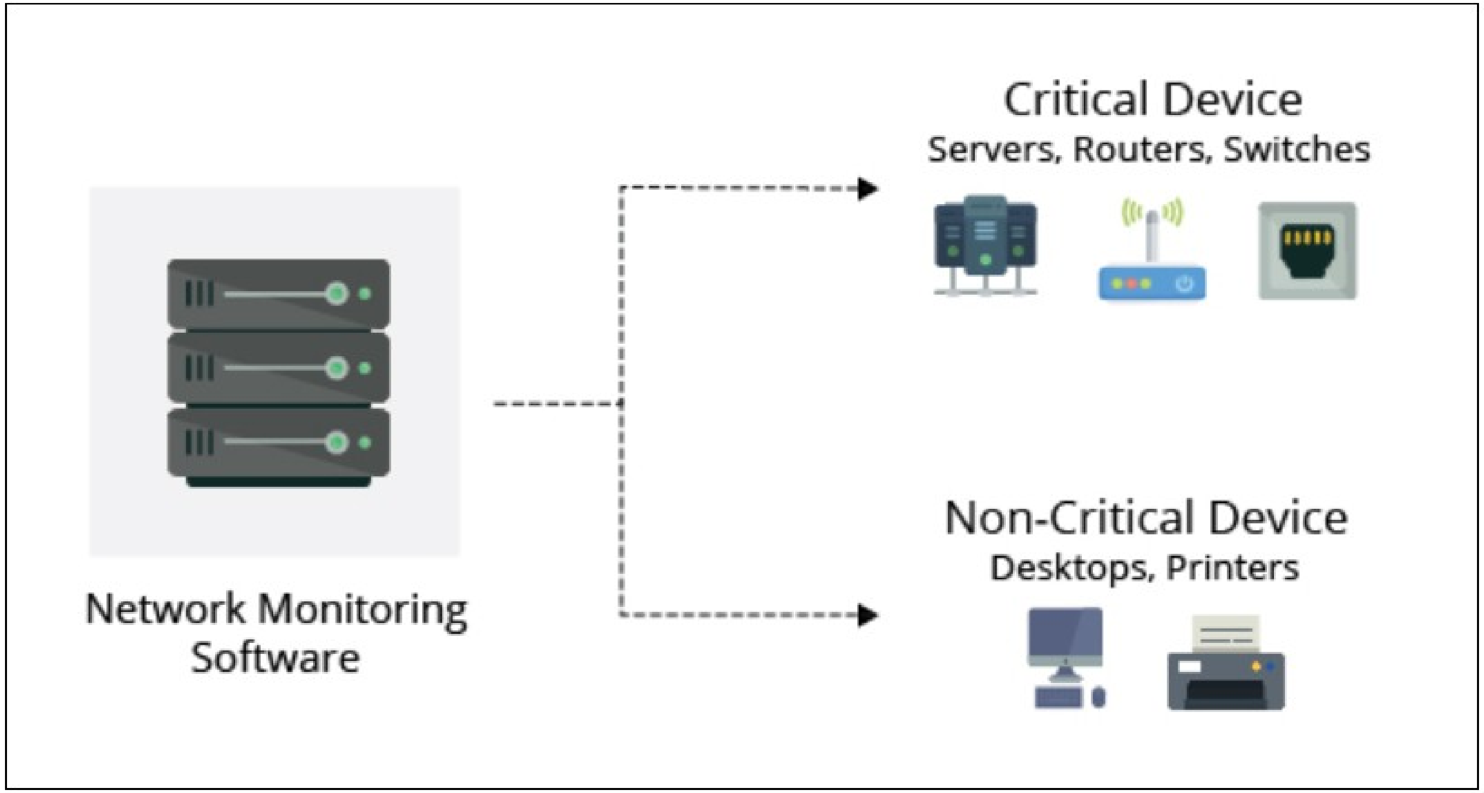
- **Important aspects of network monitoring:**
  - Monitoring the essentials
  - Optimizing the monitoring interval
  - Selecting the right protocol
  - Setting thresholds

Ref: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html

- **Monitoring the essentials**
  - **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.**
  - **Servers, routers, and switches perform business-critical tasks but at the same time have specific parameters that can be selectively monitored.**

Ref: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html

Monitoring the essentials



Ref: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html

- **Optimizing the monitoring interval**
  - Monitoring interval determines the frequency at which the network devices and their 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. The availability status of devices has to be monitored at the least interval of time preferably every minute. CPU and memory stats can be monitored once 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.

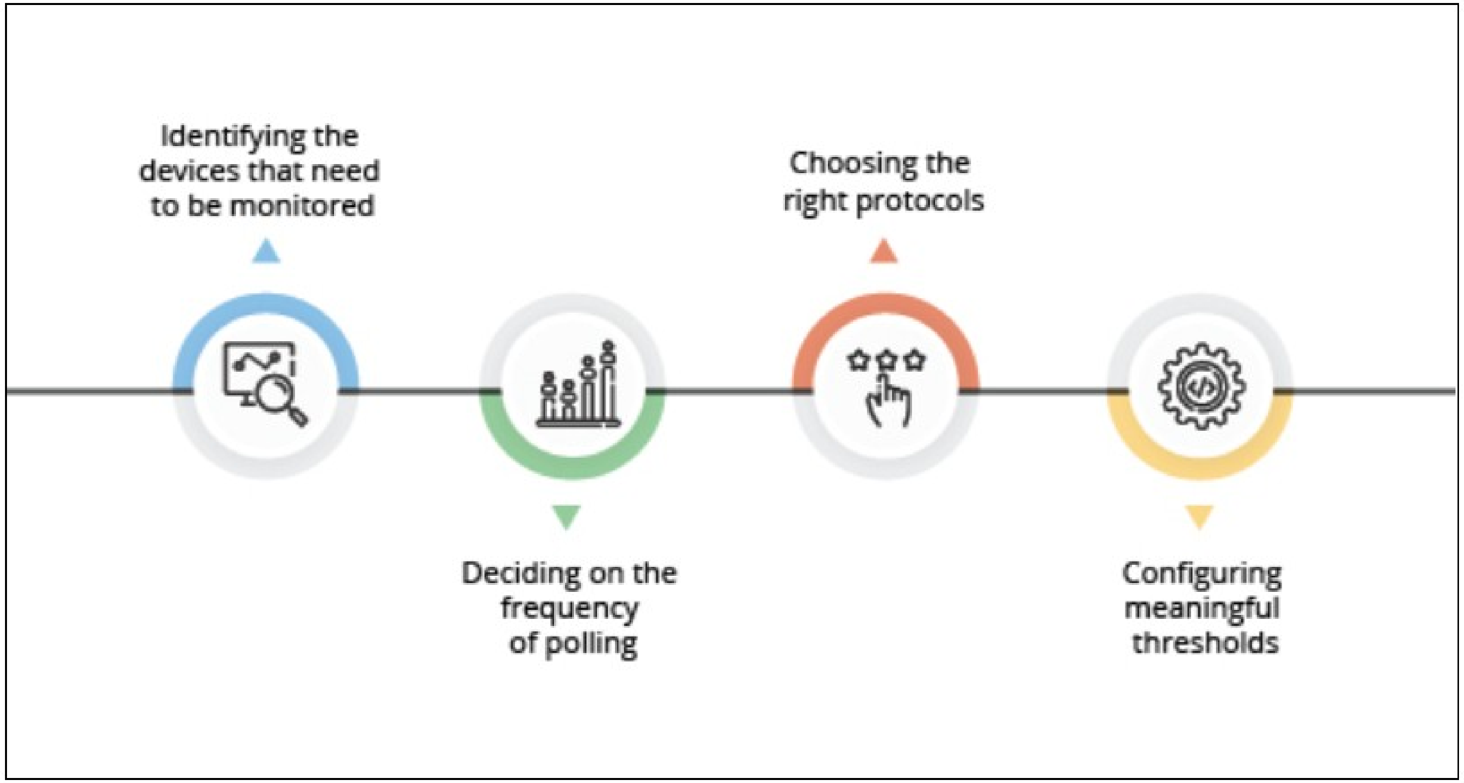
Ref: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html

- ## Selecting the right protocol
  - 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.
  - Windows devices support **Windows Management Instrumentation (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 an 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 to read/write privileges and restricting control for other users.

Ref: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html

- **Setting thresholds**
  - Thresholds are used to identify performance bottlenecks proactively.
  - Threshold limits vary from device to device based on the business use case.
  - Configuring thresholds help 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 a critical condition.

Ref: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html



Identifying the devices that need to be monitored

Deciding on the frequency of polling

Choosing the right protocols

Configuring meaningful thresholds

Ref:https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html

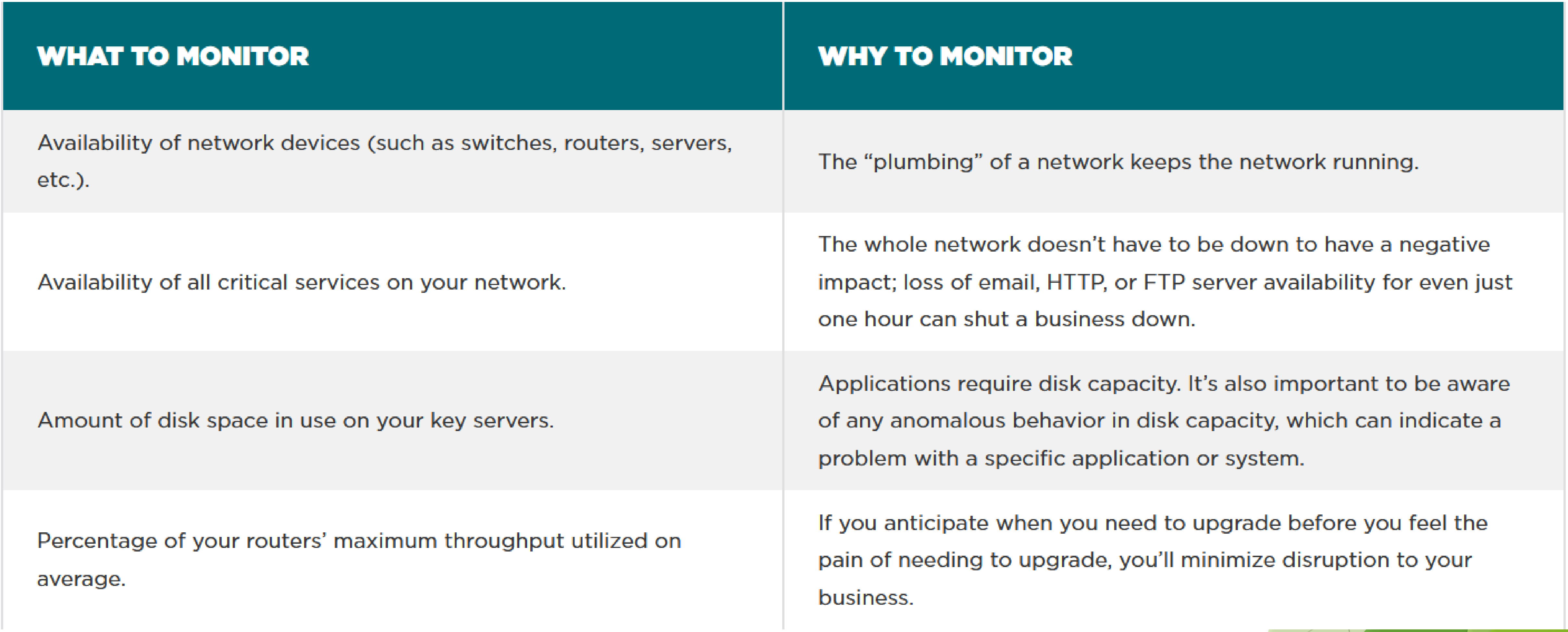
Design a Network Monitoring Strategy

- Network monitoring strategy consists of tools and techniques to analyze and measure network performance.
- The strategy examines how your company monitors and interprets the performance of a network.
- This includes what performance metrics you look at and the actions your network team takes to establish performance-related fixes.

ef: https://solutionsreview.com/network-monitoring/how-to-design-a-successful-network-monitoring-strategy/

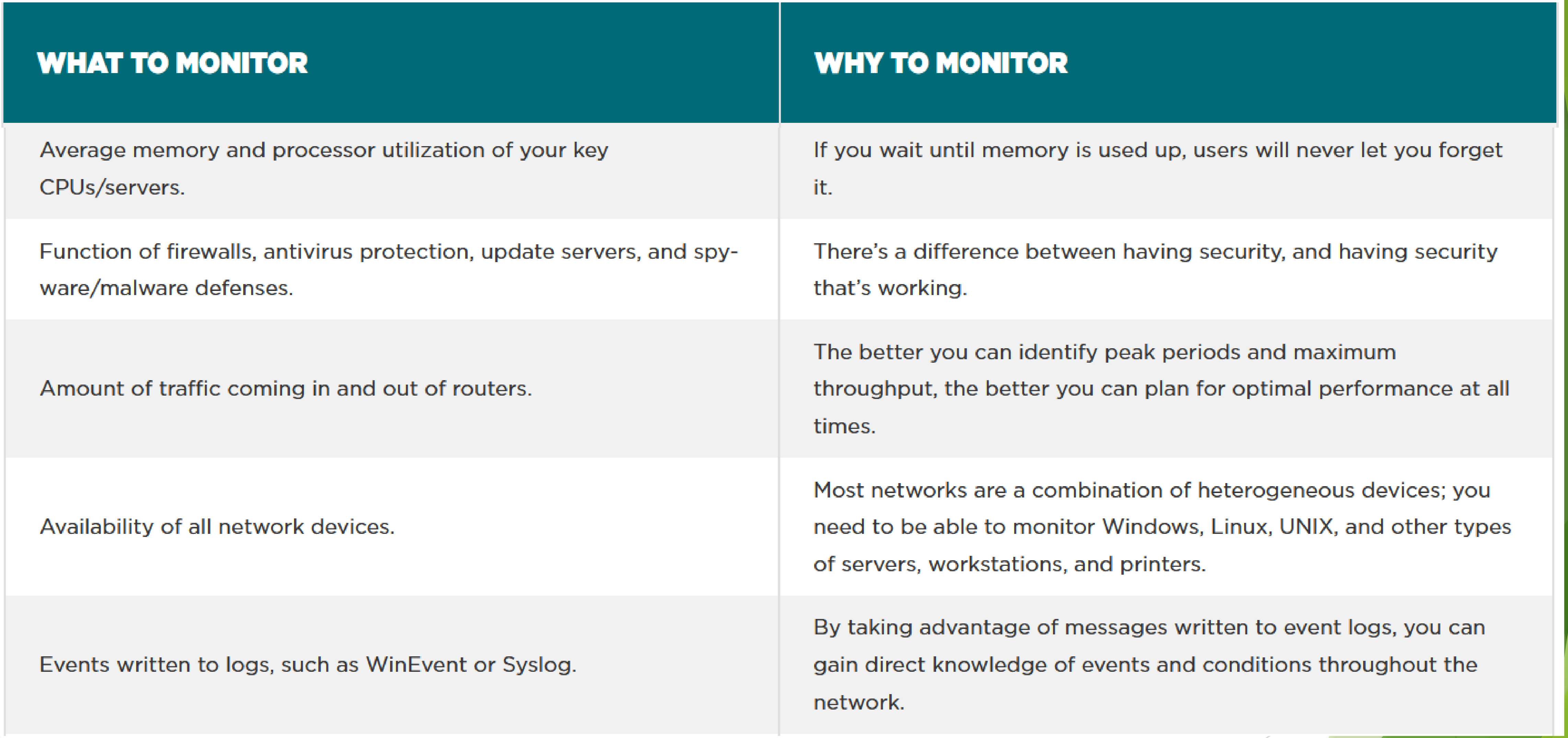
- **Network monitoring systems include software and hardware tools that can track various aspects of a network and its operation, such as traffic, bandwidth utilization, and uptime.**
- **These systems can detect devices and other elements that comprise or touch the network, as well as provide status 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.**
- **These systems can alert administrators to issues via email or text and deliver reports via network analytics.**

ef: https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html



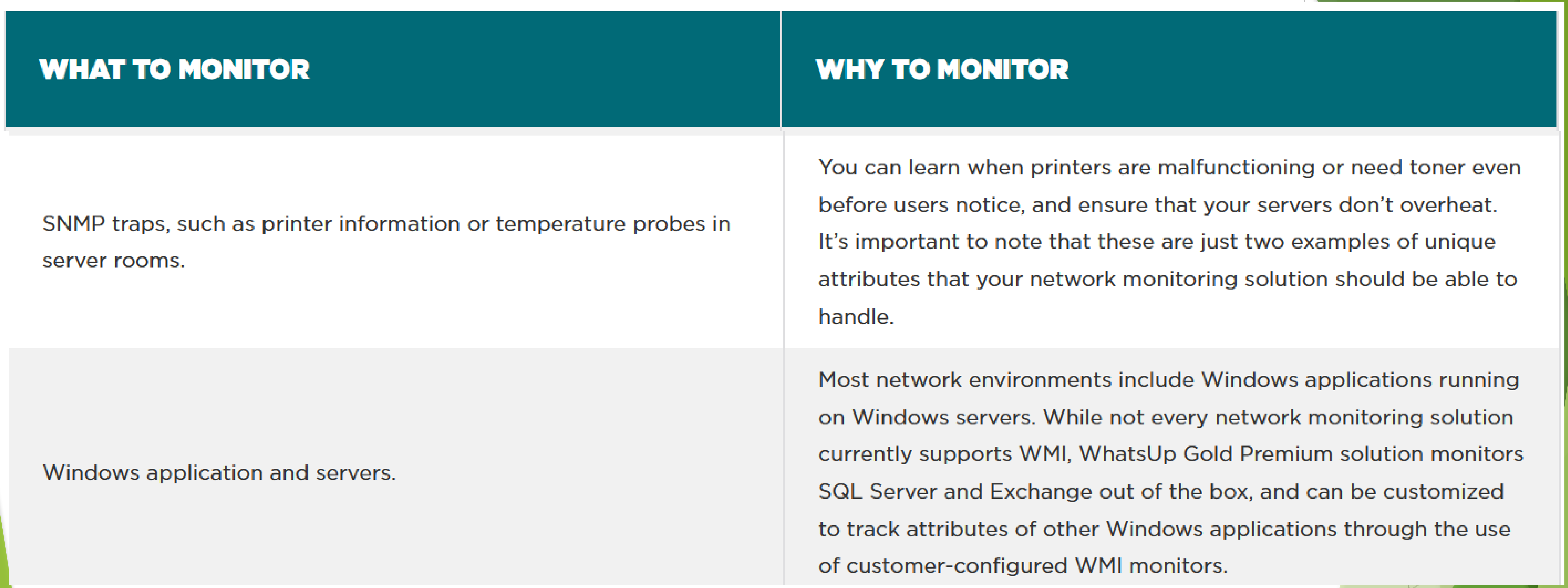
WHAT TO MONITOR	WHY TO MONITOR
Availability of network devices (such as switches, routers, servers, etc.).	The “plumbing” of a network keeps the network running.
Availability of all critical services on your network.	The whole network doesn’t have to be down to have a negative impact; loss of email, HTTP, or FTP server availability for even just one hour can shut a business down.
Amount of disk space in use on your key servers.	Applications require disk capacity. It’s also important to be aware of any anomalous behavior in disk capacity, which can indicate a problem with a specific application or system.
Percentage of your routers’ maximum throughput utilized on average.	If you anticipate when you need to upgrade before you feel the pain of needing to upgrade, you’ll minimize disruption to your business.

https://www.whatsupgold.com/resources/best-practices/network-monitoring



WHAT TO MONITOR	WHY TO MONITOR
Average memory and processor utilization of your key CPUs/servers.	If you wait until memory is used up, users will never let you forget it.
Function of firewalls, antivirus protection, update servers, and spy-ware/malware defenses.	There’s a difference between having security, and having security that’s working.
Amount of traffic coming in and out of routers.	The better you can identify peak periods and maximum throughput, the better you can plan for optimal performance at all times.
Availability of all network devices.	Most networks are a combination of heterogeneous devices; you need to be able to monitor Windows, Linux, UNIX, and other types of servers, workstations, and printers.
Events written to logs, such as WinEvent or Syslog.	By taking advantage of messages written to event logs, you can gain direct knowledge of events and conditions throughout the network.

https://www.whatsupgold.com/resources/best-practices/network-monitoring



WHAT TO MONITOR	WHY TO MONITOR
SNMP traps, such as printer information or temperature probes in server rooms.	You can learn when printers are malfunctioning or need toner even before users notice, and ensure that your servers don't overheat. It's important to note that these are just two examples of unique attributes that your network monitoring solution should be able to handle.
Windows application and servers.	Most network environments include Windows applications running on Windows servers. While not every network monitoring solution currently supports WMI, WhatsUp Gold Premium solution monitors SQL Server and Exchange out of the box, and can be customized to track attributes of other Windows applications through the use of customer-configured WMI monitors.

https://www.whatsupgold.com/resources/best-practices/network-monitoring

Design a Network Monitoring Strategy

- **Each business network operates differently, and thus requires its own strategy for proper performance measurement.**
- **Refer to paper (Oss); A Design and monitoring of Network Monitoring System Using Open Source Software Case of University of Dodoma Network, 2011**
- **https://www.researchgate.net/publication/258224888_Design_and_Implementation_of_Network_Monitoring_System_Using_Open_Source_Software_Oss_A_Case_of_University_Of_Dodoma_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.**
- **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.**

ef: https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html

What are protocols for network monitoring?

- Protocols are sets of rules and directions for devices on a network to communicate with one another.
- Network hardware can't transmit data without using protocols.
- Network monitoring systems use protocols to identify and report on network performance issues.

ef: https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html

Types of network monitoring protocols

- The Simple Network Management Protocol(SNMP) is an application-layer protocol that uses a call-and-response system to check the statuses of many types of devices, from switches to printers. SNMP can be used to monitor system status and configuration.
- 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.
- The Cisco Discovery Protocol facilitates the 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.

ef: https://www.cisco.com/c/en/us/solutions/automation/what-is-network-monitoring.html

- **Network monitoring systems, at their most basic, are tools that help administrators monitor their networks more effectively.**
- **The specifics of the system, however, vary widely based on the company's size and needs.**
- **The following are a few examples of how network monitoring systems vary:**

Ref: https://worldwideservices.net/how-network-monitoring-works/

The variation of network monitoring systems is based on the following:

- **Size and scale:**
  - **Some network monitoring systems are simple, pinging hosts to check for availability.**
  - **Some are even achieved using a patchwork of various software and hardware in tandem.**
  - **More advanced systems, on the other hand, monitor all areas of even the most complex networks with a single comprehensive system.**
- **Ease of use:**
  - **Interfaces vary wildly depending on the type and sophistication of the network monitoring system.**
  - **While some offer only simple alerts and command-based interfaces, others may provide a graphical user interface to improve functionality.**
  - **Many modern network monitoring tools have web-based and mobile-based interfaces.**

Ref: https://worldwideservices.net/how-network-monitoring-works/

- **Automation:**
  - **Basic monitoring systems rely on an administrator to see results and act on them, but many companies are turning to automated systems that handle events themselves.**
  - **These systems are designed to trigger events when network data falls outside set parameters, functionally eliminating the middle man and improving response time for network errors.**

Ref: https://worldwideservices.net/how-network-monitoring-works/

- **One important point to network monitoring systems is that they are not necessarily security systems.**
- **While network monitoring can serve as a helpful tool to protect against network gaps and slowdowns that could lead to a breach, network monitoring systems are not intrusion detection systems or intrusion prevention systems.**
- **While these other systems detect and prevent unauthorized access, network monitoring systems let you know how well the system is running during regular operations.**

Ref: https://worldwideservices.net/how-network-monitoring-works/

- Focus on network monitoring:
  - **Bandwidth use**: Monitoring network traffic, how much bandwidth your company uses, and how effectively it's used helps ensure that everything runs smoothly. Devices or programs that hog your bandwidth may need to be replaced.
  - **Application performance**: Applications running on your network need to function properly, and network monitoring systems can test to be sure that they do. Network monitoring systems can test the response time and availability of network-based databases, virtual machines, cloud services, and more to be certain that they are not slowing down your network.
  - **Server performance**: Email servers, web servers, DNS Servers and more are the crux of many functions in your business, so it's essential to test the uptime, reliability, and consistency of each server.
  - **Network configuration**: Network monitoring systems can supervise many kinds of devices, including cell phones, desktops, and servers. Some systems include automatic discovery, which allows them to log and track devices continuously as they are added, changed, or removed. These tools can also segregate devices according to their type, service, IP address, or physical location, which helps keep the network map updated and helps plan for future growth.

Ref: https://worldwideservices.net/how-network-monitoring-works/

- Monitoring isn’t limited to any single type of network. Any network of any level of complexity can be monitored with a sufficient network monitoring system.
- Some of the most common network types include wireless or wired, corporate LAN, VPN, and service provider WAN. Voice over internet protocol (VoIP), video on demand (VOD), and internet protocol TV (IPTV) are also common additions to modern networks that can add complexity to network monitoring.
- With monitoring, however, managers can allocate resources properly regardless of all the complexities of their network.

Ref: https://worldwideservices.net/how-network-monitoring-works/

How Does Network Monitoring Work?

- **Network monitoring uses a variety of techniques to test the availability and functionality of the network.**
- **Some of the more common general techniques used to collect data for monitoring software are listed below:**
  - **Ping: A ping is one of the most basic techniques that monitoring software uses to test hosts within a network. The monitoring system sends out a signal and records data such as whether the signal was received, how long it took the host to receive the signal, whether any signal data was lost, and more. The data is then used to determine whether the host is active, how efficient the host is, the transmission time and packet loss experienced when communicating with the host, and other information.**
  - **SNMP: Simple network management protocol (SNMP) monitors individual devices in a network through monitoring software. In this system, each monitored device has monitoring software installed that sends information about the device's performance to a central SNMP manager. The manager collects this information in a database and analyzes it for errors. This is the most widely used protocol for modern network management systems.**
  - **Syslog: Syslog is an automated messaging system that sends messages when an event affects a network device. Technicians can set up devices to send out messages when the device encounters an error, shuts down unexpectedly, encounters a configuration failure, and more. These messages often contain information that can be used for system management as well as security systems.**
  - **Scripts: In networks with gaps in network monitoring software functionality, scripts may be used to fill small gaps. Scripts are simple programs that collect basic information and instruct the network to perform an action within certain conditions. A common example would be a scheduled task like resetting and reconfiguring a public access computer every night. Scripts can also be used to collect data for network monitoring.**
  - **Once this data is collected, the network monitoring software sends out an alert if results don't fall within certain thresholds. Network managers will usually set these thresholds of acceptable performance, programming the network software to send out an alert if its data indicates slow throughput, high error rates, unavailable devices, or slow response times.**

Ref: https://worldwideservices.net/how-network-monitoring-works/

Simple Network Management Protocol

- **Simple Network Management Protocol is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.**
- **Port(s): 10161, 10162 (Trap)**
- **OSI layer: Application**
- **RFC(s): 6353**

Ref: https://worldwideservices.net/how-network-monitoring-works/

- **SNMP can comprehensively monitor not only the network elements like routers and switches but can also be used to monitor network servers. Details like server hardware description, physical location, IP address, available disk space, and server uptime can be monitored through SNMP.**
- **SNMP works by sending messages, called protocol data units (PDUs), to devices within your network that “speak” SNMP. Using these requests, network administrators can track virtually any data values they specify. All of the information SNMP tracks can be provided to a product that asks for it.**

Ref:

- Simple Network Management Protocol, an application level, IP-based protocol, is the most widely used network discovery and monitoring technology around, with most hardware manufacturers providing SNMP-enabled devices.
- Management Information Base (MIB)
  - At the core of the SNMP technology is the Management Information Base (MIB).
  - MIB are database-like structures in each device, containing device-related information stored as variables and definitions – for instance,
    - a router's MIB would contain network traffic and forwarding information;
    - a switch's MIB would contain spanning tree, VLAN, and bridging information;
    - A server's MIB might contain data on CPU, memory utilization, location, uptime, and so on.
  - Each object in the MIB is identified by a Unique Object Identifier (OID).

: https://www.whatsupgold.com/resources/best-practices/using-snmp-to-monitor-servers

How SNMP Works

- SNMP works by exchanging SNMP information between SNMP managers and agents.
- The manager is a software module present in the network management tool, while the agent software is embedded by vendors into network devices.
- Using SNMP queries, and by studying the replies sent by the agent software, the manager first identifies and locates the devices.
- It then periodically polls the devices and obtains device-related information. The network monitoring tool then records and analyses the information to monitor device performance and health.
- Additionally, SNMP allows remote device configuration through SNMP control commands. Administrators can also set up “SNMP traps” – data packages sent to the manager when a user-defined threshold is reached. Traps trigger alarms in the network management tool, which can be configured to send email/SMS notifications to the administrator.

: https://www.whatsupgold.com/resources/best-practices/using-snmp-to-monitor-servers

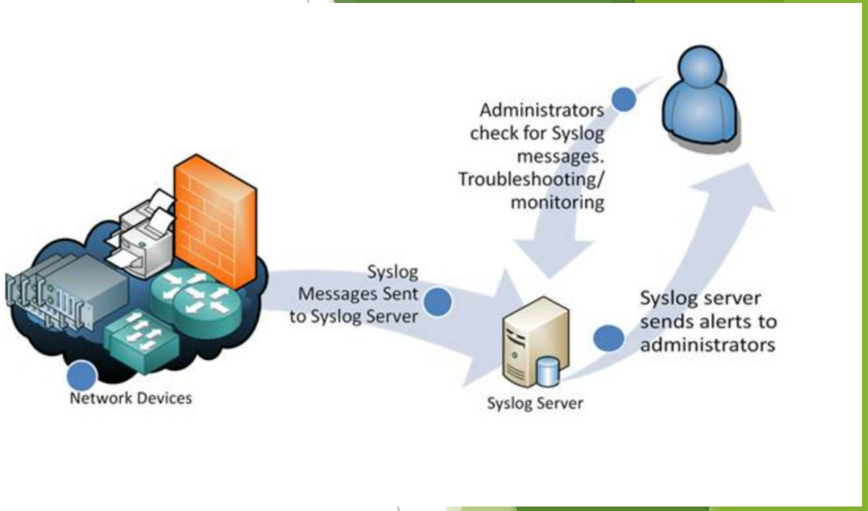
- **Unlike SNMP, Syslog can’t be used to “poll” devices to gather information.**
- **For example, SNMP has a complex hierarchical structure that allows a management station to ask a device for information on things like temperature data or available disk space.**
- **That’s not possible with Syslog – it simply sends messages to a central location when specific events are triggered.**

ef: https://www.networkmanagementsoftware.com/what-is-syslog/

- **Syslog Servers**

Syslog is a great way to consolidate logs from multiple sources into a single location. Typically, most Syslog servers have a couple of components that make this possible.

- **A Syslog Listener:**
  A Syslog server needs to receive messages sent over the network. A listener process gathers Syslog data sent over UDP port 514. UDP messages aren't acknowledged or guaranteed to arrive, so be aware that some network devices will send Syslog data via TCP 1468 to ensure message delivery.
- **A Database:**
  Large networks can generate a huge amount of Syslog data. Good Syslog servers will use a database to store Syslog data for quick retrieval.
- **Management and Filtering Software:**
  Because of the potential for large amounts of data, it can be cumbersome to find specific log entries when needed. The solution is to use a Syslog server that both automates part of the work and makes it easy to filter and view important log messages. Syslog servers should be able to generate alerts, notifications, and alarms in response to select messages – so that administrators know as soon as a problem occurs and can take swift action!


Administrators check for Syslog messages. Troubleshooting/ monitoring
Syslog Messages Sent to Syslog Server
Syslog server sends alerts to administrators
Network Devices
Syslog Server

Ref: https://www.networkmanagementsoftware.com/what-is-syslog/

- **Syslog Messages**
- **The importance of Syslog: Messages are sometimes in a descriptive, human-readable format – but not always!**
- **Syslog uses a concept called “facility” to identify the source of a message on any given machine.**
  - **For example, a facility of “0” would be a Kernel message, and a facility of “11” would be an FTP message.**
  - **Syslog’s UNIX roots.**
- **Most Cisco network equipment uses the “Local6” or “Local7” facility codes.**
- **Syslog messages also have a severity level field.**
- **The severity level indicates how important the message is deemed to be.**
  - **A severity of “0” is an emergency, “1” is an alert that needs immediate action, and the scale continues right down to “6” and “7” – informational and debug messages.**

Ref: https://www.networkmanagementsoftware.com/what-is-syslog/

The Downsides to Syslog

- **There are a few downsides to Syslog.**
- **First, the problem of consistency.**
- **The Syslog protocol doesn’t define a standard way for the message content to be formatted – and there are as many ways to format a message as there are developers.**
- **Some messages may be human-readable, but some aren’t. Syslog doesn’t care – it just provides a way to transport the message.**
- **There are also some problems that arise because of the way Syslog uses UDP as a transport. UDP is connectionless and not guaranteed – so it could be possible to lose log messages due to network congestion or packet loss.**

ef: https://www.networkmanagementsoftware.com/what-is-syslog/

- **Finally, there are some security challenges with Syslog.**
- **There is no authentication on Syslog messages, so it could be possible for one machine to impersonate another machine and send bogus log events. It is also susceptible to replay attacks.**
- **In spite of this, many administrators find that the Syslog is a valuable tool and that the downsides are relatively minor.**

ef: https://www.networkmanagementsoftware.com/what-is-syslog/

- **Summary**
- **Syslog can be a powerful tool that can make it easier for administrators to manage complex networks.**
- **The biggest challenge with Syslog is the volume of data. The logging server software must simplify log management, and help admins filter and focus on messages that truly matter.**
- **Example tool to get the most out of the Syslog, - Free version of Kiwi Syslog**

ef: https://www.networkmanagementsoftware.com/what-is-syslog/

- Free IT Monitoring & Analysis Tools
- https://www.solarwinds.com/free-tools?CMP=BIZ-TAD-NMS

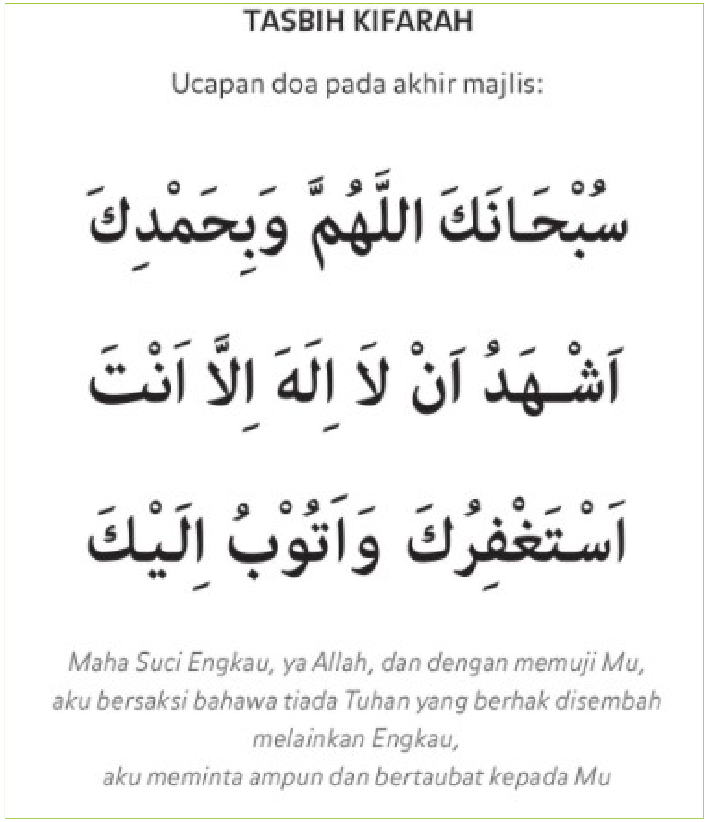
- **References**

1.Shamsi.J, Principle of Networking, 2009

2.J.Matogoro, Design and Implementation of Network Monitoring System Using Open Source
Software (Oss); A Case of University of Dodoma Network, 2011

3.DNSStuffm , Ultimate Guide to Network Monitoring, 2019

The End



TASBIH KIFARAH

Ucapan doa pada akhir majlis:

سُبْحَانَكَ اللَّهُمَّ وَبِحَمْدِكَ

اَشْهَدُ اَنْ لَآ اِلَهَ اِلَّا اَنْتَ

اَسْتَغْفِرُكَ وَاَتُوْبُ اِلَيْكَ

Maha Suci Engkau, ya Allah, dan dengan memuji Mu,
aku bersaksi bahawa tiada Tuhan yang berhak disembah
melainkan Engkau,
aku meminta ampun dan bertaubat kepada Mu