NETWORK MONITORING SYSTEM

INTRODUCTION

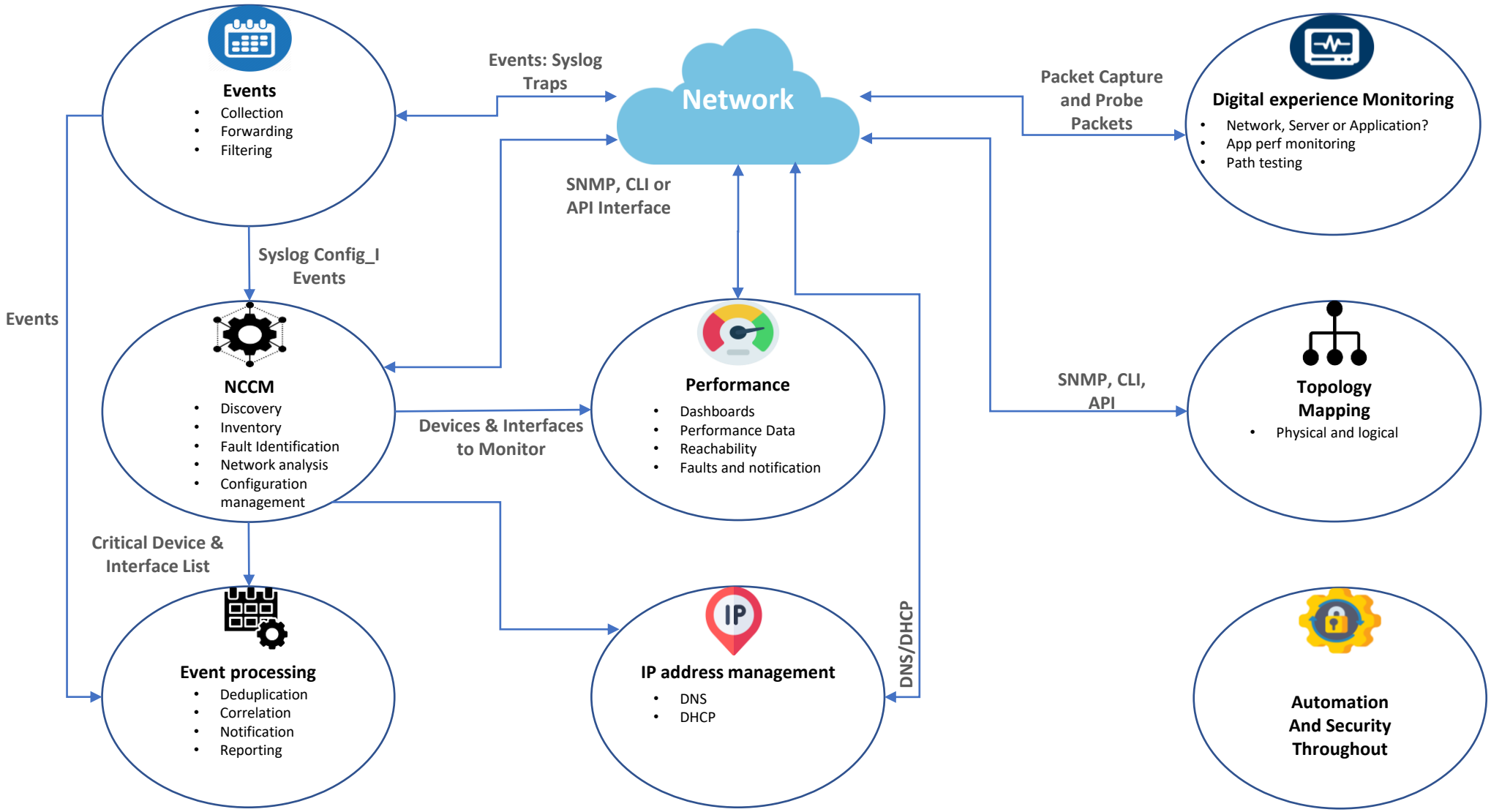
Network monitoring, also frequently called network management, is the practice of consistently overseeing a computer network for any failures or deficiencies to ensure continued network performance. Technically, network monitoring can be viewed as a subset of network management, but the two are considered equivalent in practice.

Network monitoring collects and reports on a variety of data from a computer network, including routers, switches, firewalls, load balancers and even endpoints, like servers and workstations. The collected data is filtered and analyzed to identify a variety of network problems. These network problems can include the following:

device failures, link outages, interface errors, packet loss, application response time, configuration changes

The functions of a network monitoring and management system can be broken down into several categories, each of which performs a specific function.

NETWORK MANAGEMENT ARCHITECTURE



NETWORK MANAGEMENT ARCHITECTURE

Event collection and processing

Event collection relies on Simple Network Management Protocol (SNMP) traps and syslog to collect network event data. Events enable the network to advise administrators of important events without having to poll network devices. Event processing is used to identify critical events, reducing the volume of alerts that network administrators must handle.

Network change and configuration management

Network change and configuration management (NCCM) archives network device configurations and can be used to automate configuration updates. Configurations may be retrieved and updated using any of several mechanisms, including the command-line interface (CLI), SNMP, RESTCONF and NETCONF.

Configuration analysis identifies day-to-day changes (drift) and audit compliance exceptions where configurations don't match network design policies. Both drift and audit are critical functions for ensuring that network configurations match the intended design and operation.

Performance monitoring

Performance monitoring collects device performance data, like central processing unit (CPU) and memory utilization, temperature, power supply voltages and fan operation. Interface performance data is used to identify failures, packet loss, congestion and other network problems.

Data is collected using SNMP, Windows Management Instrumentation (WMI), the CLI or telemetry. Network devices and Linux-based endpoints typically rely on SNMP or telemetry for data collection, while Windows-based devices rely on the WMI remote protocol. WMI is a client-server framework that enables system management using the Common Information Model, which represents the components of the OS.

Telemetry

Newer devices and monitoring systems may employ network telemetry to push network performance data to a network monitoring system. Telemetry may use Extensible Markup Language- or JavaScript Object Notation-encoded data. Some network monitoring systems and related network devices use representational state transfer interfaces to collect data using these same data formats.

NETWORK MANAGEMENT ARCHITECTURE

IP address management

IP address management tracks IP address use and controls the allocation of addresses to network devices. This function typically uses the CLI or an application programming interface (API) to other network management systems.

Topology mapping

The topology and mapping function collects device connection data to create physical and logical topology maps that form the foundation of basic troubleshooting. SNMP polling or the CLI are used to collect data on routing neighbors (Layer 3), switching neighbors (Layer 2), address translation tables (Layer 2 to Layer 3 mapping) and neighbor discovery protocols, like Link Layer Discovery Protocol.

Digital experience monitoring

Digital experience monitoring employs active testing tools, such as ping, traceroute and synthetic monitoring, to test that the network is working as intended. It may also employ software agents that run on endpoints, like servers and workstations, to collect data about application performance and network performance. Combining application performance monitoring with network monitoring enables IT organizations to diagnose whether an application problem is due to the network or some other factor, including external networks.

Security and automation

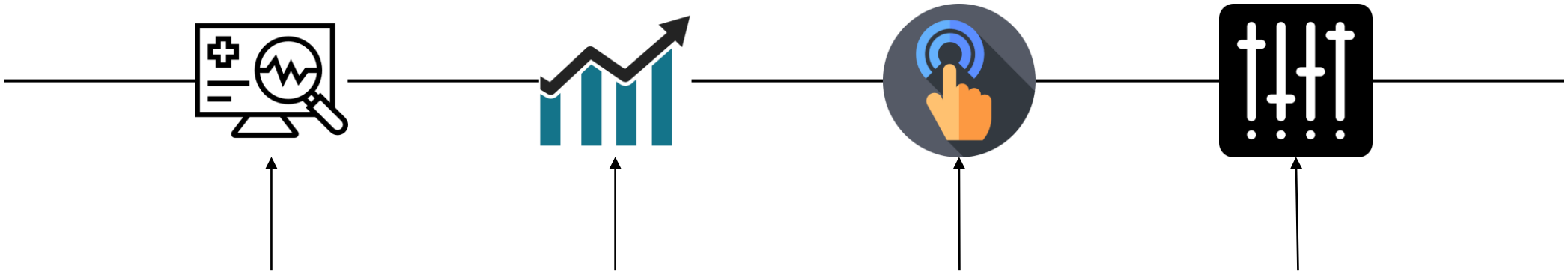
The architecture should include security and automation throughout. Security continues to be an important element of a smoothly running network, and automation is used to guarantee consistent implementation of network policies. The security design should include intrusion detection and intrusion prevention devices and the software to monitor and manage them. Automation may be provided by separate tools or integrated within an NCCM system.

Combining data from multiple sources enables a network monitoring system to identify failures quickly and to report on performance problems before they negatively affect applications that use the network.

HOW TO SUCCESSFULLY CONDUCT NETWORK MONITORING

You must eliminate any extraneous load from the network monitor in order to conduct effective network monitoring. You may do this by:

- Keeping an eye just on the fundamentals
- improving the monitoring interval
- the appropriate procedure selection
- placing limits



Identifying the equipment that has to be watched

Choosing the frequency of the polling

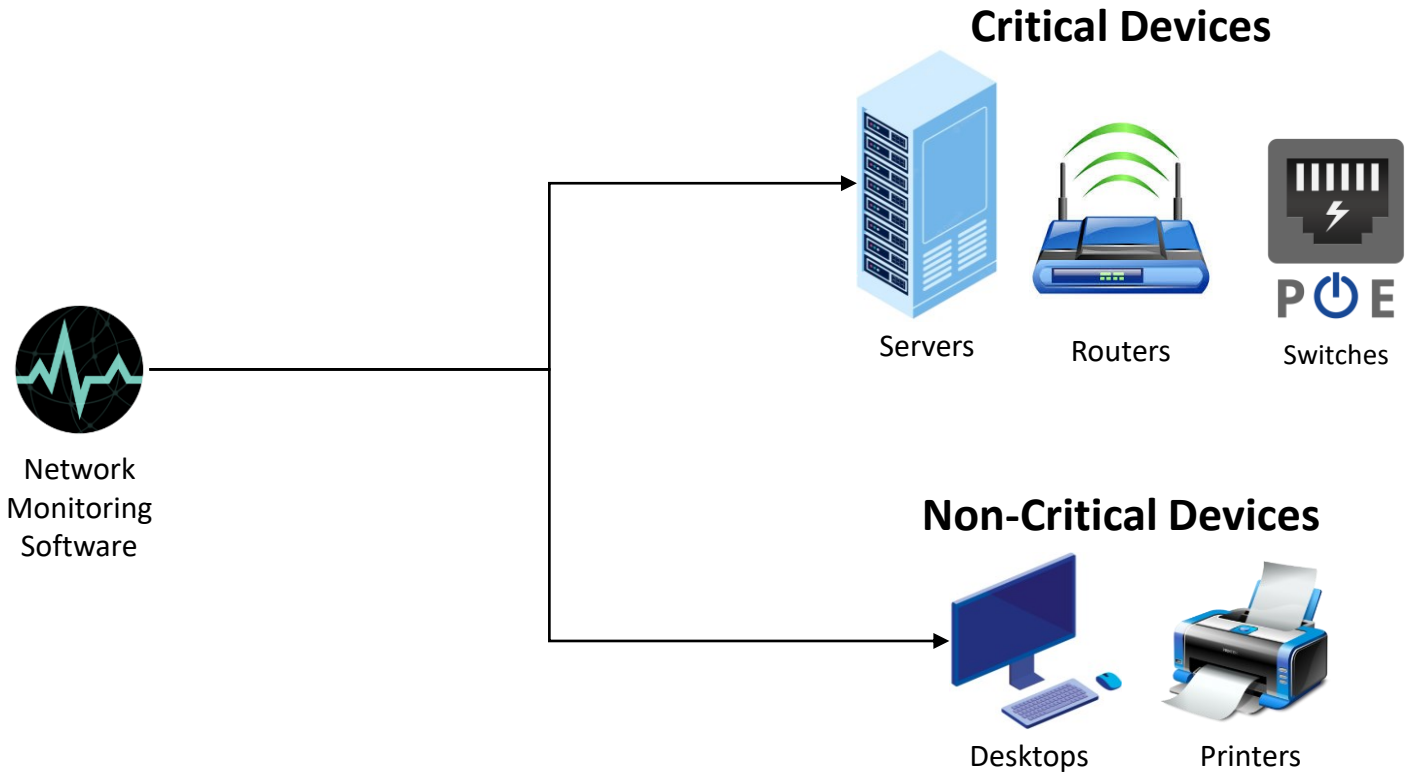
Determining the appropriate protocols

Setting up useful thresholds

HOW TO SUCCESSFULLY CONDUCT NETWORK MONITORING

Keeping an eye just on the fundamentals

Network performance is impacted by faulty network hardware. Early discovery of this can prevent it, which is why network device monitoring is so crucial. Identifying the devices and the relevant performance indicators to be watched is the first step in efficient network monitoring. While servers, routers, and switches carry out business-essential functions but also have particular characteristics that may be selectively monitored, PCs and printers are not vital and do not need frequent monitoring.



HOW TO SUCCESSFULLY CONDUCT NETWORK MONITORING

Keeping an eye just on the fundamentals

The second step, selecting monitoring interval, is necessary since both critical and non-critical devices need to be monitored. The monitoring interval controls how frequently network devices and the metrics associated with them are queried to ascertain their performance and availability status. The burden on your resources and the network monitoring and reporting tools can be reduced by setting up monitoring intervals. Depending on the kind of network device or metric being observed, the interval varies. Device availability has to be checked at least once an hour, ideally every minute. Once every five minutes, CPU and RAM statistics may be checked. Other measures, including disc utilization, can have their monitoring intervals increased; once every 15 minutes is adequate. The network will be overloaded if every device is being watched at the smallest possible interval.

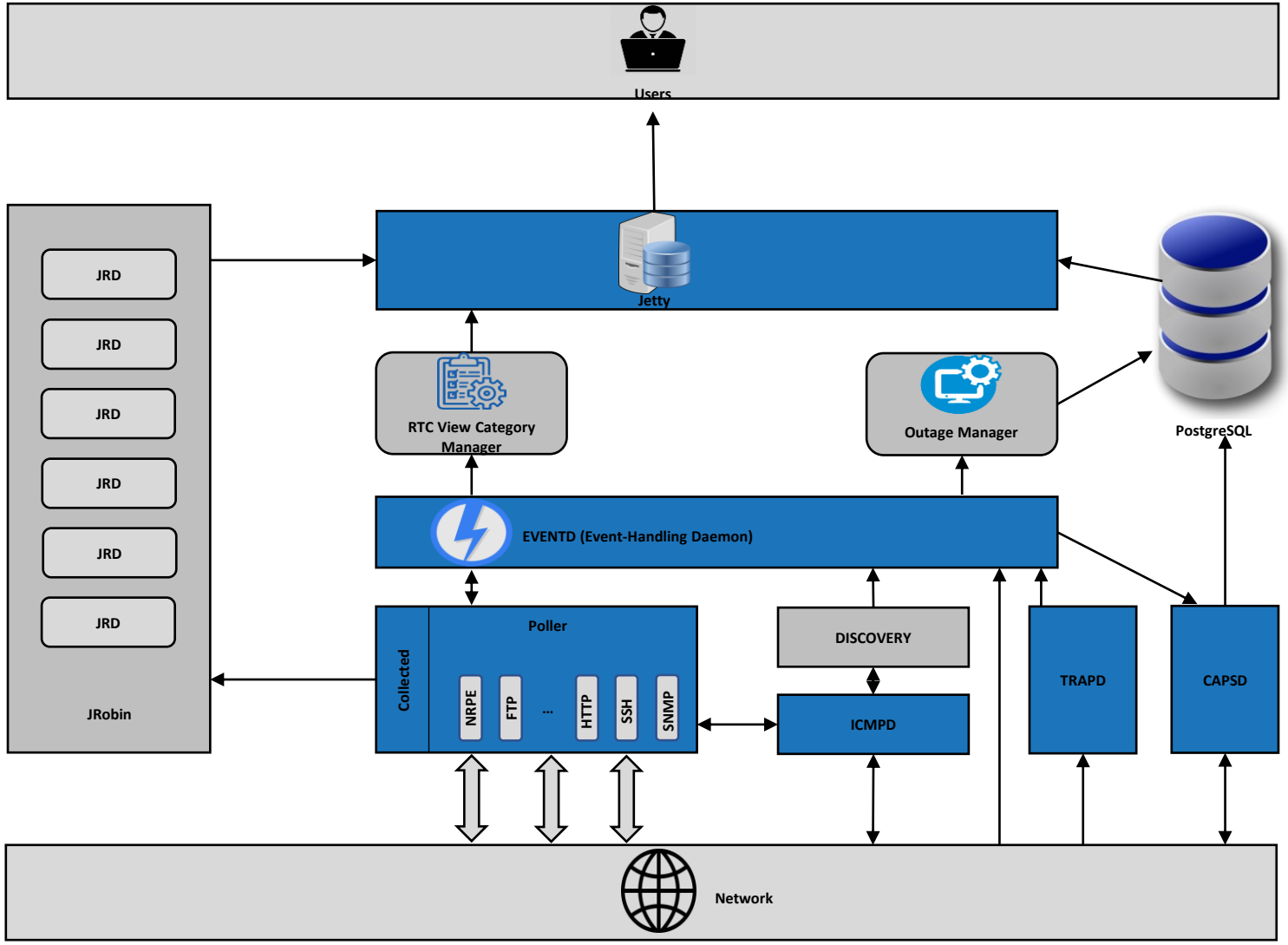
Improving the monitoring interval

The next step is choosing the appropriate network protocol after the devices have been identified and the monitoring intervals have been set. To minimize the impact on network performance when monitoring a network and its devices, it is generally recommended to use a secure, low-bandwidth network management protocol. The majority of network devices, Linux servers, and Windows devices support the SNMP (Simple Network Management Protocol) and CLI protocols. One of the extensively used network protocols for managing and watching over network components is SNMP. An SNMP agent is typically included with network components. For them to be able to connect with the network management system (NMS), they only need to be activated and configured. Giving the device read-write access through SNMP allows for total control. One may change the device's whole settings via SNMP. By establishing SNMP read/write privileges and limiting control for other users, the best network monitor aids the administrator in taking control of the network.

Placing limits

Network outages may be quite expensive. The end user often alerts the network monitoring team of a problem with the network. This is due to a subpar proactive business network monitor strategy. Real-time network monitoring's main problem is proactively identifying performance bottlenecks. Thresholds are crucial in network monitoring applications in this situation. The business use case affects the threshold limitations, which change from device to device.

NETWORK MANAGEMENT ARCHITECTURE



CONTACT US

THANKS!

DO YOU HAVE ANY QUESTIONS?

fly@maplecloudtechnologies.com
+918178803636
www.maplecloudtechnologies.com