# Managing Distributed Systems

## Overview

Network Operations Centers act as the hub for all the systems they support. Without their ever-vigilant eye over all aspects of performance, the stability of critical systems simply cannot be assured. As networks become more complex so too must the tools used for managing them. While the current approach for monitoring contiguous networks (SNMP, etc.) have many foundations on which a distributed networks operations center can be built, there are limitations of certain technologies that need to be addressed.

## Current Challenges in Network Management

Much of the history of monitoring can be summed up by one word, reactionary. Most of the current landscape for monitoring software employs this approach, with varying levels of success, to provide a watchful eye on the system and alert personal of one thing, failures. While some monitoring on a network is vastly better than no monitoring on a network, this approach contains some pretty large pitfalls. Simply reacting to issues when they arise does not allow technical resources to be applied efficiently. Trends are difficult to quantify as they are generally represented by little more than the gut feeling of a skilled few. Further to this idea, there is cause for concern surrounding the scalability of the protocols used within the industry for managing devices. SNMP, while inarguably the industry standard for local network alerts, is not a silver bullet, and in many cases due to poor or limited implementation the presence of the protocol in a device provides no useful information for the ongoing health and wellbeing of equipment.

To truly make a distributed network effective we must use the right tool for the job, and in this case, it means not using SNMP for something it was never intended, distributed network management. SNMP thrives at monitoring status alerts from devices on a single local network, datacenters for example where there is an extremely high concentration of very capable objects on a contiguous network. A power supply in a server fails, an SNMP trap is an excellent way to notify a piece of supervisory software running on premise. Where SNMP struggles however is when one needs to manage a network, or network of smaller networks, that spans across multiple physical locations. Of course, there have been attempts made to patch some of the issues that present themselves when managing distributed networks, such as security or data transport, but the underlying problem is that SNMP was traditionally only intended to be a local broadcast protocol.

Lastly there is the challenge of disparate data. As alluded to previous, the quality of a particular products SNMP capabilities are subject to a great many factors. Manufactures do not have to adhere to a standard for what information is or is not present but merely how the information they decide to give will be sent, and event within this there is a great many interpretations. SNMP, being event based, does not often allow for the polling of health status without manual interaction. Further complicating factors are that to this day not all devices can communicate using SNMP and that often the equipment that does not can still pose a large single point of failure in a network. Eg. Generators

## A Modern Approach to Network Management

Gone are the days of NASA like control rooms with round the clock staff, eyes intently fixed on a wall plastered with monitors. The time of a technician is too valuable and there are often simply too many concurrent problems for this to be practical anymore. The modern approach to network management revolves around **Intelligible Data**. Without a mechanism in place to have information filtered and prequalified even the best organized personal will become quickly overwhelmed. The problem is only further compounded when talking about distributed networks where it is sometimes not only impractical but impossible to deploy a technician due to distance, current conditions, etc.. It is vital therefore that the best most intelligible information be made available wherever, whenever, and to whomever is required to aid in their deciding on the best allocation of resources.

A second core concept the modern approach to network management is the notion of proactive prevention rather than reactive action. It is far less impactful to schedule a network outage to replace a component or replace a soon to be dead battery at your next scheduled visit than it is to work through the night, in a panic, trying to restore system functionality after a catastrophic outage. By employing a proactive stance on network functionality, a systems support structure can be best optimized and utilization of key resources can be truly managed ultimately greatly reducing the overall cost of managing complex networks.

## Apex System Manager

Apex System Manager is the 4th generation of monitoring and control software developed by TASC Systems. The current generation of software incorporates TASC’s existing alarm / eventing system with its well-defined approach to SNMP management all while improving on its data acquisition capabilities. Further, the latest software release will allow users a more flexible deployment environment with both hosted and on-premise solutions available. Apex System Manager lastly will give technicians a simple interface to the historical performance their devices as well as a window into the future with the ability to employ predictive analysis on their data to anticipate failures and better allocate resources moving forward.

Designed with service providers in-mind, Apex System Manager allows for various levels of permissioned access as well as logical segregation of networks. For example, a service reseller is not only able to view and manage their clients network and devices but can also give a dedicated access portal to their client should they wish to have their own window into the functioning of their system. A hosted solution ensures 24/7 uptime and the ability for connectivity to the network anywhere an internet connection is present, all without the need to deploy and maintain costly infrastructure.

## Monitoring Hardware

To ensure the integrity and security of the data being captured it is vital that an end to end solution be employed. For the purpose of secure and reliable data capture TASC Systems has developed a number of hardware gateways for interface to all means of information, both physically and logically.

### Ridge

Ridge is a gateway that allows for the reception of SNMP in Apex. Ridge receives and interprets SNMP traps from a device at site and forwards them on to the Apex System Manager. Ridge provides multiple layers of security as well as simple connectivity for devices that otherwise would be unable to securely connect and communicate over the internet. Ridge provides added layers of redundancy by monitoring the communication link between the equipment and Apex, something not possible with standard SNMP

### Peak

Peak is a gateway that provides a physical interface for an array of common devices into Apex. Peak can be deployed with up to 4 devices in a range of common monitoring and control applications in areas such as, RF, Environmental, Power, Site Control, and many others. Peak also provides by-directional audio streaming and GPS location information. Peak is a simple to deploy, very flexible, low cost, static or mobile gateway.

### Plateau

Plateau is a gateway specifically engineered for remote low power applications. When power consumption is a key concern often backhaul is a big challenge. Plateau provides sub 20mA idle current with single analog radio channel backhaul capabilities.

### Summit

TASC Systems flagship gateway allows for the physical interface of over 100 points of digital, analog, and serial I/O to be captured and interfaced with Apex. Due in part to its scale it is generally suited to more complex environments where large amounts of I/O need to be efficiently interfaced.

TASC Systems product family provides effective end to end monitoring and management solutions for all networks, regardless of size, scale, or scope.