NETWORKComputing

Keeping the Business Running with Remote Network Management

Howard M. Cohen, Senior Resultant, HMC Write Now
Rich Korb, Systems Engineering Senior Manager – East Region, Mist, a Juniper Company
Gene Sawyer, Systems Engineering Director, Mist, a Juniper Company

KEY TAKEAWAYS

- WFH has introduced new challenges for IT teams.

- Automation technologies enable IT teams to run data centers without compromising access, control, visibility, or security.

- Artificial intelligence operations, or AIOps, is the future of data center management.

- IT must do more with less—the number of remote users and locations has exploded, but IT teams haven't grown.

- With Mist, IT teams enjoy the benefits of a "self-driving network" supported by integrated AIOps.

- Mist enables reactive and proactive troubleshooting.

- Enterprise, cloud-based network management solutions are agile, secure, and flexible.

in partnership with

JUNIPER NETWORKS | Mist A Juniper Company

OVERVIEW

The COVID-19 pandemic transformed vast numbers of employees into remote workers practically overnight. IT teams are now grappling with new challenges associated with remote network management. Fortunately, nearly all data centers run autonomously and IT staff can monitor operations remotely. IT teams are finding that automation technologies are the key to reducing network outages and delivering services faster. Many see artificial intelligence or AIOps as the future of data center automation and management. Solutions like Mist enable IT teams to do more with less in today's environment. Mist provides agile and secure automation that supports reactive and proactive troubleshooting.

CONTEXT

Howard M. Cohen discussed network management challenges facing IT teams given the explosion of employees working from home. Gene Sawyer and Rich Korb shared how Mist can help network administrators engage in reactive and proactive troubleshooting.

KEY TAKEAWAYS

WFH has introduced new challenges for IT teams.

The world has changed. When the COVID-19 pandemic erupted, employees retreated to their homes and working from home (WFH) is now the norm. No one is sure how long this will last, but many organizations have found that employee productivity has actually increased. In a recent Gartner survey, companies indicated that between 5% and 100% of their employees may work from home permanently.

For IT teams, the WFH movement is like bring your own device (BYOD) on steroids. Challenges include:

- **User-owned devices.** Most employees use home computers to remotely access corporate resources.

- **Residential internet access.** Connectivity varies based on where people live and their internet provider. It is impossible to predict what incoming signals will look like and how well they can be managed.

- **Aging virtual private networks or unknown firewalls.** Many employees have a virtual private network (VPN) and some may be using their computer's default firewall.

- **Uncontrolled endpoint security.** Unless every employee has a company-issued home computer, IT has no visibility into how much or how little security is being used on end points.

- **Increased difficulty with application distribution, upgrades, and patching.** It is hard to ensure consistent service across the board, no matter how much automation the IT team has deployed.

- **Communications-related decisions.** Organizations must implement systems that enable employees to talk together and collaborate, such as voice over IP (VoIP) or unified communications as a service (UCaaS). Every company will take a different approach to the communications challenge.

Automation technologies enable IT teams to run data centers without compromising access, control, visibility, or security.

The nature of the data center has changed and today almost everything can run by itself. Staff no longer need to be on site at data centers, since IT teams can monitor operations remotely. This new environment is conducive to working from home, but IT teams still need to run data centers without compromising access, control, visibility, and security. In addition, they must be able to identify, troubleshoot, and resolve data center problems.

Automation is the answer. According to Gartner, organizations that automate 70% of their network change activities reduce outages by 50% and deliver services 50% faster.

> **Automation can be used for a variety of data center tasks including:**
> - Managing policies and orchestrating network and application performance queries
> - Discovering switches, routers, access points, controllers, and appliances
> - Handling daily routine server activity
> - Performing data backups

With automation, the IT staff role becomes more administrative than operational. As a result, IT teams can hire individuals with little or no training.

In the data center environment, three types of automation technologies can be helpful:

Software-Defined Networking (SD-WAN)	This is an agile technology that enables organizations to move effortlessly between different kinds of communication and select the bandwidth they need for each application. SD-WAN provides true transport independence. It supports any transport protocol, from 3G to 4G LTE, MPLS, wifi, and the soon-to-be-available 5G. SD-WAN was designed for on-premise, public, and private cloud environments.
Intent-Based Networking (IBN)	This technology hides complexity, while offering agility, simplicity, and improved security and management. IBN helps IT teams identify lurking network problems quickly with rich insights. It can troubleshoot and remediate issues without human intervention. IBN also offers powerful security and policy capabilities, simplified segmentation of the network, and consistent policy deployment. It is capable of detecting threats, even those hidden within encrypted traffic. IBN builds on SD-WAN to act as a central network activity management point.
Hyperconverged Infrastructure (HCI	This technology has evolved in recent years. The power of HCI is that it unifies and simplifies data center management. HCI merges all necessary data center functionality into a single infrastructure stack running on top of an efficient, elastic pool of processing elements. It relieves IT managers and IT teams from managing most infrastructure tasks. HCI provides easy infrastructure access from anywhere and enables software-defined networking.

Artificial intelligence operations, or AIOps, is the future of data center management.

Data from the edge can help network administrators make decisions about day-to-day data center management tasks. Technology has accelerated the assessment root causes, which means that IT teams no longer have to spend hours diagnosing problems. Self-aware systems can resolve or proactively alert administrators about nuanced network problems.

Artificial intelligence operations, or AIOps, is a new science that incorporates AI and machine learning into network management. Experts see this technology as the future of data center automation and management. AIOps puts automation at the infrastructure level. It can be used to build more responsive and intelligent networks that run with little or no human intervention. The integration of big data, analytics, and machine learning makes it possible to diagnose critical issues and either report them or automatically resolve them without IT involvement.

One advantage of AIOps is that IT teams can customize service levels based on customers' needs and environments. With AIOps, administrators can set thresholds, monitor them, and take action when thresholds are exceeded.

> AIOps detects issues in the network before they become outages and prevents those issues from happening again in the future. It's seen as the future of operations management.
>
> *Howard M. Cohen, HMC Write Now*

IT must do more with less—the number of remote users and locations has exploded, but IT teams haven't grown.

Prior to the pandemic, most IT teams dealt with a limited number of remote users and locations. The bulk of their work focused on needs of office users. COVID-19 has changed that. Working from home has dramatically increased the number of remote users and locations that need to be managed, yet the size of the IT team has remained unchanged.

The WFH environment presents many places where problems can arise, ranging from wireless access to the wired segment, firewall, the SD-WAN/internet segment, or within the data center. IT teams must be prepared to detect and fix these issues automatically.

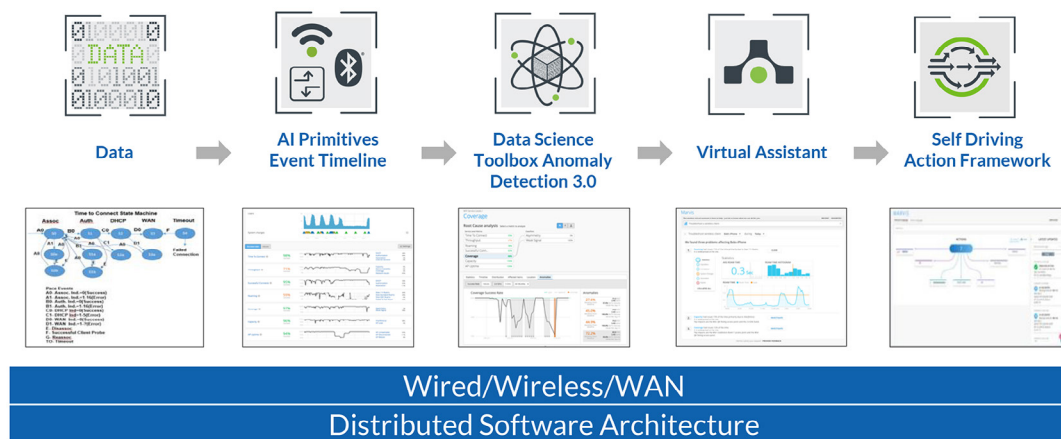**Figure 1: Working from Home—What Could Possibly Go Wrong End-to-End?**
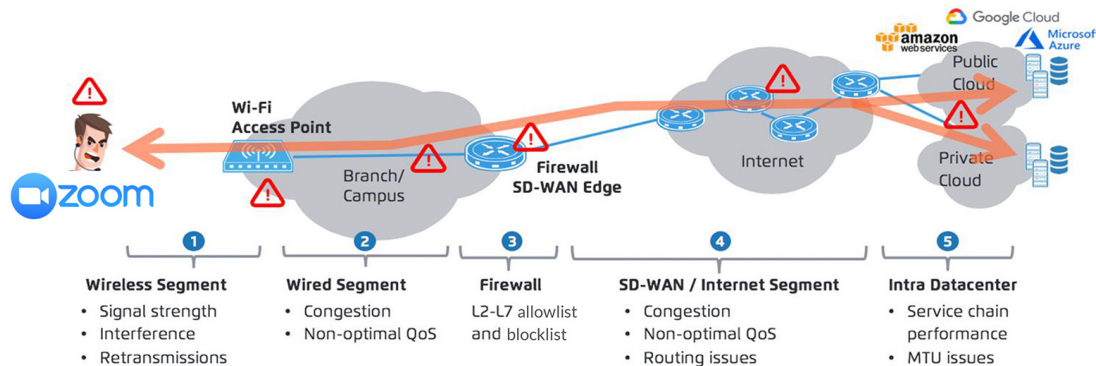
How Do We Detect and Fix These Issues Automatically?

With Mist, IT teams enjoy the benefits of a "self-driving network" supported by integrated AIOps.

Mist's scalable microservices cloud architecture with integrated AI operations starts with data. Rather than collecting massive amounts of information from log files, Mist gathers the right data at the right time from every single client. This enables Mist to detect issues in the network.

Experts in the areas of wireless, wired, routing, and security have collaborated with data scientists to build Mist's AI operations components in the cloud. Marvis, a virtual network assistant, sits on top of the Mist architecture. Marvis can answer end user questions such as "Why is my Zoom audio choppy?" or "Why can't I connect to my wifi network?"

Figure 2: Mist & Marvis—A Journey to an AI-Driven Enterprise

Data → AI Primitives Event Timeline → Data Science Toolbox Anomaly Detection 3.0 → Virtual Assistant → Self Driving Action Framework

Wired/Wireless/WAN

Distributed Software Architecture

> Mist and its artificial intelligence can evaluate system data and then proactively or reactively inform the administrator about what's going on in the network, what problems exist, and how to resolve them. This eliminates a lot of effort and time for IT teams.
>
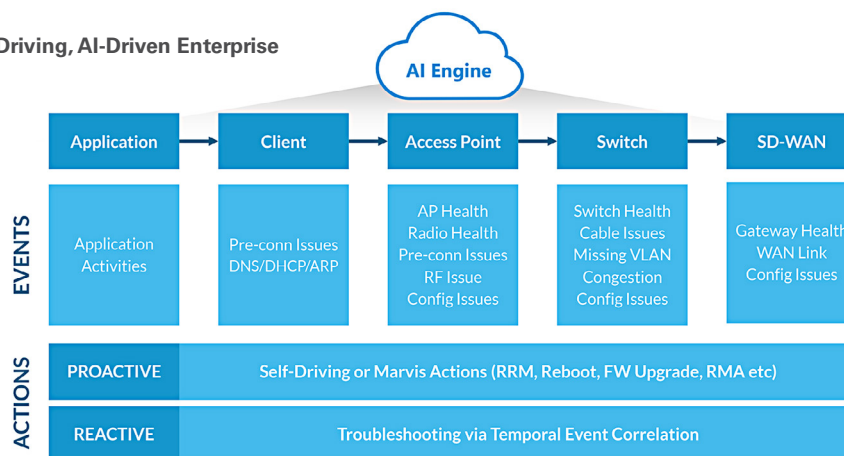> *Rich Korb, Mist, a Juniper Company*

Mist enables reactive and proactive troubleshooting.

Mist focuses on improving the client experience. The system tracks good and bad events, the times clients are connected, and the different flows, services, and systems clients are using. Mist stores about 150 different states for every client and access point event. That data remains in the cloud for a 7-day period. As a result, IT teams can go back in time and replay what happened with different clients and interrogate dynamic packet capture of events.

Mist helps IT teams troubleshoot reactively in real time via temporal event correlation. Marvis, the intelligent virtual assistant, acts as another member of the IT team. Its natural language processing capabilities handle misspellings in inquiries gracefully.

Mist also supports proactive troubleshooting through self-driving or Marvis actions. For example, Marvis may recommend software upgrades to resolve issues or identify defective hardware that must be replaced. If Mist can't automatically resolve problems, Marvis can open a support case that includes the conversation history and client data.

Figure 3: The Self-Driving, AI-Driven Enterprise

AI Engine

Application	Client	Access Point	Switch	SD-WAN

EVENTS

Application Activities	Pre-conn Issues DNS/DHCP/ARP	AP Health Radio Health Pre-conn Issues RF Issue Config Issues	Switch Health Cable Issues Missing VLAN Congestion Config Issues	Gateway Health WAN Link Config Issues

ACTIONS

PROACTIVE — Self-Driving or Marvis Actions (RRM, Reboot, FW Upgrade, RMA etc)

REACTIVE — Troubleshooting via Temporal Event Correlation

NETWORKComputing

Enterprise, cloud-based network management solutions are agile, secure, and flexible.

Enterprise, cloud-managed solutions like Mist offer several advantages:

- **Agile.** IT teams no longer need to pre-stage devices. Mist provides a zero-touch provisioning experience.

- **Secure.** Security is automated and integrated into Mist.

- **Flexible.** IT departments can set, monitor, and enforce service level expectations in Mist for every client on the network.

Mist can be deployed at scale very rapidly. The result is an exceptional user experience and simplified support with minimal effort. One customer averaged around 200 support tickets per month. After installing Mist, their monthly trouble tickets decreased 97%.

Gene Sawyer, Mist, a Juniper Company

BIOGRAPHIES

Howard M. Cohen
Senior Resultant, HMC Write Now

Senior Resultant Howard M. Cohen is a 35+ year executive veteran of the Information Technology industry who today writes for and about the IT channel. He's a frequent speaker at IT industry events that include Microsoft Inspire, Citrix Synergy/Summit, ConnectWise IT Nation, ChannelPro Forums, Cloud Partners Summit, MicroCorp One-On-One, and CompTIA ChannelCon, and frequently hosts and presents webinars for many vendors and publications.

Rich Korb
Systems Engineering Senior Manager - East Region, Mist, a Juniper Company

Rich Korb is the Systems Engineering Senior Manager for the East region at Mist, where he not only manages an incredible team but is also a field SE for the Southeast region. Prior to Mist, Rich was the Director of Systems Engineering of North America for Aerohive Networks. With nearly 2 decades of experience in the industry, Rich has focused the last 10 years on WLAN design and deployment across practically every vertical. He has been instrumental in key customer wins through his technical thought leadership.

Gene Sawyer
Systems Engineering Director, Mist, a Juniper Company

Gene Sawyer is the Director of Sales Engineering at Mist Systems where he leads a team of accomplished Sales Engineers as well as working directly with customers and partners leveraging technology to drive mission-critical business requirements. Gene has been working in the IT industry for over 25 years and has extensive experience with large solution design and deployments across numerous verticals such as retail, hospitality, healthcare, manufacturing, and education.

Before joining the Mist Systems team, Gene spent over 13 years at Cisco Systems in Systems Engineering and leadership roles including Director, Systems Engineering in the Cisco Meraki business unit focused on Cisco's Global Enterprise Segment. Prior to Cisco, Gene worked at Airespace, Trapeze Networks, and Extreme Networks. Gene is also a Certified Wireless Network Expert (CWNE) and Certified Information Systems Security Professional (CISSP).