MICROLAND®

Making digital happen

Navigating the New Network

Charting the future of Managed Network Services with Automation, Analytics & AIOps (AAA)

The Networks of today have evolved into an enterprise-wide software platform. They are no longer a set of independent physical boxes, but instead are a series of virtual devices which are software based with the capability to be quickly and easily designed, deployed, and managed. They can be readily updated and scaled, making an enterprise more agile in its ability to respond quickly to business needs and opportunities. As the network evolves into a more dynamic environment, it is clear that Managed Services Providers must automate and orchestrate more than what they had been delivering over the years. They should absorb the introduction of new concepts such as virtualization and software-defined everything to leap-frog into a newer model. Whether it is software-defined WAN, LAN, data center or cloud, the age of network programmability is upon us. What does this mean for automation of the network? How does it evolve to support new technologies while still addressing integration into existing legacy ecosystems? How does it scale to support physical, virtual, and cloud networks? To unlock the truly game-changing potential of automation in Managed Network Services, we require the triumvirate of Automation, Analytics and AIOps (AAA). This paper explores the approach, strategies and toolsets that can enable this.

The Network That Was

In the past, most business leaders didn't give the network a second thought. It was considered a tactical resource that provided little strategic value. Today, for most companies, the network is the business. This is a stark change from the network's role just a few years ago, but it's now a fact, as almost all the enabling technologies of digital transformation are network centric. For example, the Internet of Things (IoT) is now a reality, and businesses are connecting billions of devices through their networks. It is believed that by 2025, there will be 80 billion connected devices enabling companies to gather massive amounts of data that could generate key insights.

The Ghost of Networks Past

The unfortunate truth is that network IT has been unable to maintain stride with other IT services in implementing automation and orchestration over the years. It has instead relied on basic Automation of repetitive tasks and has not actually delved into the art of the possible. These minimal automations cannot scale in speed as frequent change requests are made. Flexible & Hyper automation allows IT to define and implement its own workflows quickly and efficiently enables enterprises to take control of their success, without incurring the debilitating cost of building an automation platform from scratch.

Traditional Network Tools

Traditional Network tools provide siloed monitoring at best. Bereft of the analytics layer, they are time-consuming as the changes need to be done one device at a time. While most traditional tools used Simple Network Monitoring Protocol (SNMP) based monitoring, over the years these have matured to become centralized monitoring tools. They were CLI based and the greatest improvement that happened was to move from CLI to GUI based automation. From these methods evolved separate tools for every activity monitoring, mapping, orchestration and analytics. Some of the bigger tool players tried their best to bring all these into a single unified structure, but these still operated as siloed entities within the Tools framework. As per an EMA's Network Management Megatrends report, 64% enterprises use 4 to 10 tools and 17% use more than that including open-sourced and customer-developed solutions. Enterprises today need to reduce network management tools sprawl by adopting consolidated, multi-functional platform-based toolset to manage networks with IoT-devices, cloud traffic, SDN, SDN-WAN, remote workers, 5G etc.

User-experience is the ultimate source-of-truth compared to siloed monitoring of application, network & infrastructure, analysis and remediation. Relying on disparate, narrowly focused, siloed performance monitoring tools does not provide the depth and breadth needed to diagnose complex problems. A unified networking monitoring, orchestration solution gathers all packets and all device-metrics, all the time, across onpremise and cloud environments. A strategic selection approach is required for tools to draw out effective network maps, support quick network discovery & automated data polling for all connected devices, balance active and passive network monitoring, configuring networking devices correctly and scaling with growth.

Understanding the Changing Tools landscape

Networks have changed more in the last four years compared to the last 40. To address end-to-end availability and performance concerns in new-age enterprise networks, NetOps must also transform. AIOps is intrinsic to the future of IT Operations. Today, AIOps platforms are shifting toward domain agnostic functionalities to give increased flexibility in processing highly diverse datasets.

From a network automation & orchestration (NA/O) perspective, Gartner identifies three categories of tools that need to be adopted:

- **Network Con iguration & Change Management (NCCM)** delivering accurate device-state information: set-up, inventory configuration, patching, roll-out, roll-back, resource use, change history
- **Network Automation (NA)**: task-oriented programmatic control of network elements (e.g. changing quality-of-service setting on a router)
- **Network Orchestration (NO)**: coordinated manipulation of devices from a specific set of plans intended to achieve a business outcome

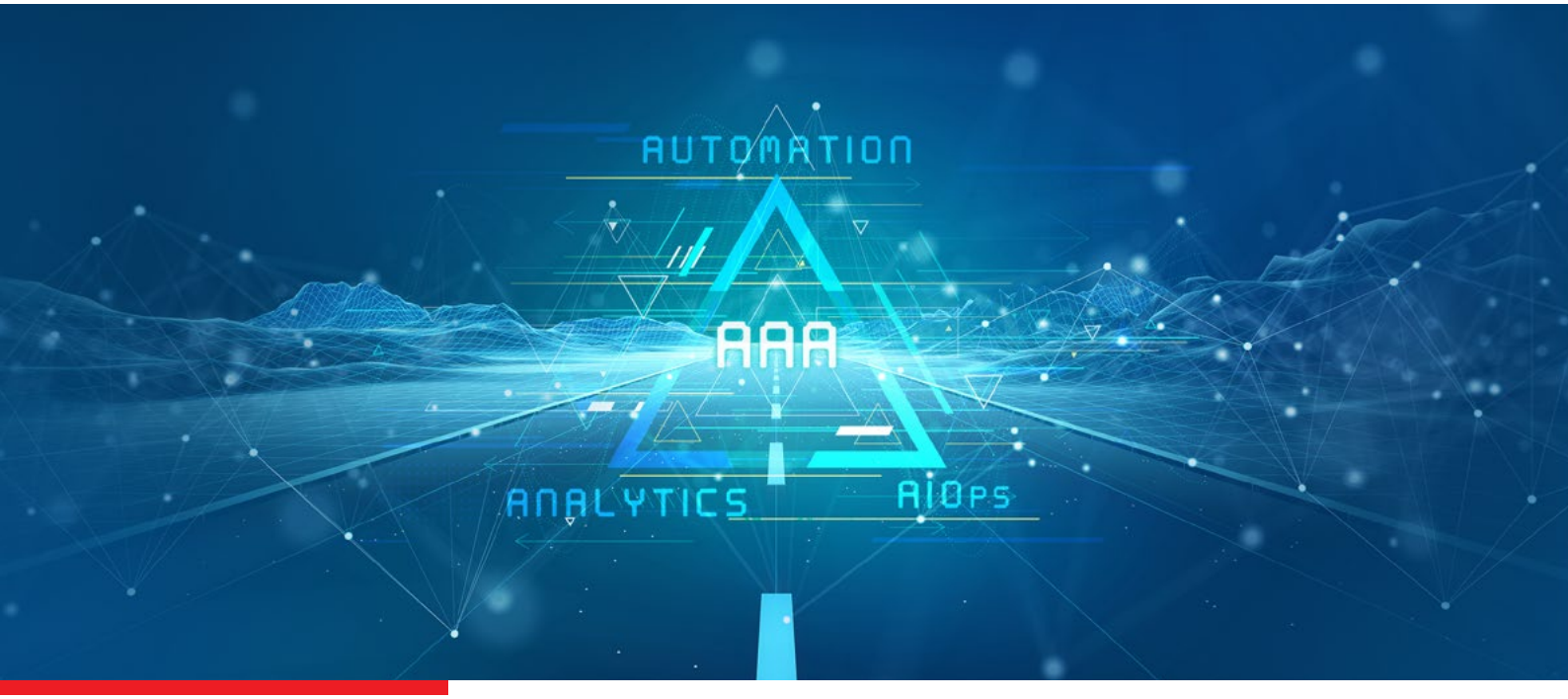
Key principles for NA/O tool adoption needs to focus on network optimization, cost control and simplification/agility

Optimization	Reduced Costs	Simplificatio n & Agility
Manual handoff & error reduction • Improve efficiency through reduced effort and rework • Increase service delivery quality • Overall quality improvements due to automation	Decrease time to make changes, troubleshoot issues, and improve Mean Time to Repair (MTTR) • Improve Mean Time to Discover (MTTD) • MTTD improvement of service interruption	Reduce human errors • Improve availability • Reduce integration complexities • Flexibility for rapid changes • Iterative delivery of network capabilities • Introduction/ retirement of network assets with minimal disruptions

From an infrastructure automation perspective, the need is to go beyond classic configuration management and automation orchestration use-cases to network modelling, compliance and vulnerability management capabilities.

- Advanced visual models should offer text-based infrastructure models to automation workflows and cost-vs-capacity analytics
- Support CIS, PCI DSS, HIPAA and SOX compliances out-of-the-box with dashboards and integrations with engines such as Qualys, Rapid7 and Tenable

The Triumvirate
Automation, Analytics, AIOps



Bringing the three orces o Automation, Analytics and AIOps together can unlock the true potential of the new network.

Here's a look at how Microland approaches this triumvirate and has leveraged its 30+ years of Network Management experience to develop a comprehensive and advanced platform—the Intelligeni NetOps Platform utilizes the AAA framework as its foundational elements:

intelligeni® netops

Automation	Analytics	AI Ops
Rapid Incident Response & Resolution • Improved Network Performance • Enhanced User Experience • Resource Optimization	End-to-End Visibility • Data-driven Insights for Decision Making • Increase Predictiveness • Capacity Planning	Predictive Maintenance • Autonomous & Self-healing Network • Enhanced Network Performance • Increased Cost Efficiencies

Network Automation

While the idea of network automation has been around for as long as there have been networks, up until now the adoption has been delayed. But as network teams shrink and organizations are being approached to accomplish more with less, network automation allows for the capacity to keep on achieving everyday tasks and stay concentrated on broader challenges. The objective is to make an abstraction layer among assets and clients and achieve efficiencies by removing the point-by-point technical knowledge from the hands of the integrators and placing it into a software-defined environment, by means of an automation tool, that enables agencies to create policies to drive their work.

Networks have on a very basic level moved with intent-based networking to turn out to be progressively flexible, instinctive and interoperable—upheld through automation and machine learning to become predictive and self-recuperating. Organizations can concentrate on repeatable changes that have a high achievement rate historically and apply end-to-end automation to implementation and governance processes.

Additionally, the ascent of software-defined networks (SDN), including software-defined WANs & LANs (SD-WAN & SD-LAN), have empowered network-automation tools to develop from operationally focused point products that address things like change management and setup, into policy management and orchestration tools. Today, network automation tools are vital, empower business alignment and give a guide to the idealistic condition of a completely intent-based system where the network runs and verifies itself.

Robotizing the WAN

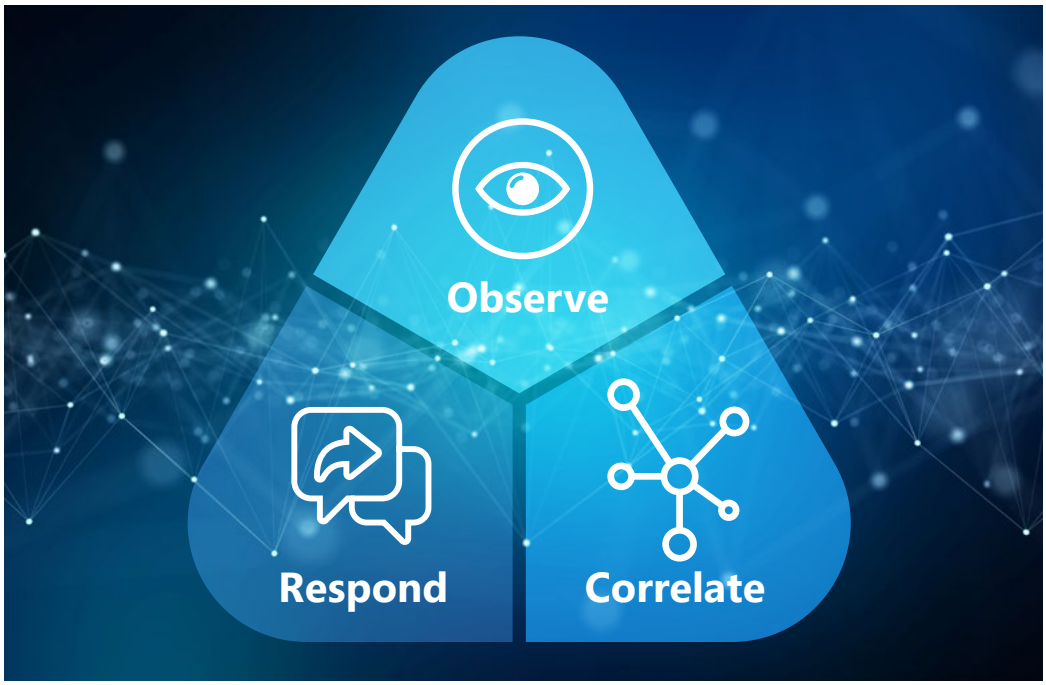
The wide-area network is another territory ready for change through automation. Albeit numerous customary WAN models are monolithic and built over the course of the years, the cutting edge world requires agility. Having the option to rapidly develop and tear down an area and give communication services – the network, telephones or anything else is required – is a significant part of numerous organizations' missions. Being able to connect a device to a network, consequently, snatch its configuration and afterward connect reliably across a satellite connection is critical.

Network Analytics

Network analytics involves the analysis of network data and statistics to identify trends and patterns. Once identified, operators take the next step of 'acting' on this data—which typically involves a network operation or a set of operations. For example, if a network operator finds that there may be a congestion problem in a certain area of the of the network, traffic can be routed through a different part of the network to meet service performance objectives. Typically, this type of operation has been a manual process.

But now, vendors are augmenting traditional analytics with automation and artificial intelligence technologies to enable the next generation of highly intelligent networks—a network capable of dynamically self-configuring or self-optimizing based on changing network conditions.

AIOps



Observe

- Network Monitoring
- Anomaly Detection
- Troubleshooting Analytics

Quickly identify & understand performance & connectivity anomalies from user to application access, converging monitoring across wireless, switch, firewall, SD-WAN etc.

Correlate

- WAN/LAN Firewall Correlation
- Incident Triage Automation
- Change Management

Analyze WAN, LAN, device & cloud events quickly and thoroughly by incorporating and accelerating policies designed to identify root-causes and end-user performance issues

Cut through noisy alerts – automated critical issue resolution

Respond

- Integrated Workflow Engines
- Automation Scripts

Remediate issues before they arise: stay ahead of critical network events using AI/ML based security orchestration, automation and response

Automation Automation in IT Operations is a new frontier, based on advanced data integration and analytics, according to growing trends and many in our industry. Humans and manual processes can no longer keep pace with network innovation, evolution, complexity, and change. That's why we're hearing more about "self-driving networks," "self-healing networks," "intent-based networking," and other concepts which aim to apply artificial intelligence (AI), machine learning (ML), and automation to support modern network operations.

Collectively, this shift is being referred to as "AIOps" (i.e. artificial intelligence for operations). In the simplest form, an AIOps approach is one that leverages multiple sources of real-time and historical monitoring data, adds contextual enrichments, applies AI/ML to recognize patterns and anomalies worthy of actions, and automates corrections, however and wherever practical. Such systems can operate around the clock, at any hour of the day, and respond long before humans can manually sift through vast swaths of data to make discoveries themselves

The potential benefits of AIOps, which include significantly improving responsiveness and effectiveness, are what makes the approach highly appealing. For instance, by better leveraging existing, available network data, AIOps can reduce the most time-consuming manual troubleshooting and analysis tasks, so that networking teams can focus more on growth rather than firefighting. AIOps concepts can also be applied to enhancing awareness and accuracy for better network engineering, capacity management, and cost control. Further, AIOps includes integrated automations to address and correct issues, ultimately ensuring fast, secure, and performant delivery of digital services.

That doesn't mean that networking professionals need to worry about their jobs being replaced. Instead, AIOps means that the most mundane and routine elements of managing networks will be handed over to machine learning models that can weed the noise out of the vast number of tickets, security alerts, and other networking notifications

Looking Ahead

Demands from the business and the shift in application development to continuous deployment and continuous integration are raising the expectation that enterprise networking keeps up with the pace of changes. The expectation that network IT staff become programmers or that the enterprise undertakes a massive development effort is ill-advised. Successful enterprises will adopt automation platforms that allow IT to focus on building automation workflows quickly while allowing application architects to develop applications on the platform. The collaboration between network teams that provide expertise on operational requirements and outcomes and developers that bring application architecture skills is at the heart of DevOps. Collaboratively, these teams combine their skills, unlocking the potential of Analytics and AIOps to hone the automation edge.

Ultimately, the AAA framework for Network IT is going to reduce the time required to manage the changes to the network and adapt to new demands in a dynamic environment, which allows decision makers to focus on work that adds value to the business such as enhancing application delivery, optimizing application traffic, and designing robust and reliable networks. Self-healing, predictive networks will reduce downtime significantly by anticipating outages before they happen. This is the brave new world that the New Network is all about.

MICROLAND®

Making digital happen

Authors

Robert Wysocki

Senior Vice President & Global Client Solutions Leader - Networks & Cybersecurity

Kumaran Rangaswamy

Vice President and Global Head of Marketing

About Microland

Microland's commitment to "Making Digital Happen" allows technology to do more and intrude less. We make it easier for enterprises to transition to nextGen digital infrastructure through our extensive service portfolio including Cloud and Data Center, Networks, Digital Workplace, Cybersecurity and Industrial IoT. We ensure that the embrace of the digital services is predictable, reliable and stable. In the COVID impacted world, Microland is making digital happen for enterprises with a laser focus on services that are more relevant to our clients and prospects than ever before, guaranteeing business outcomes. Incorporated in 1989 and headquartered in Bengaluru, India, Microland has more than 4,500 digital specialists across offices and delivery centers in Asia, Australia, Europe, Middle East and North America.

Read more here: **www.microland.com**