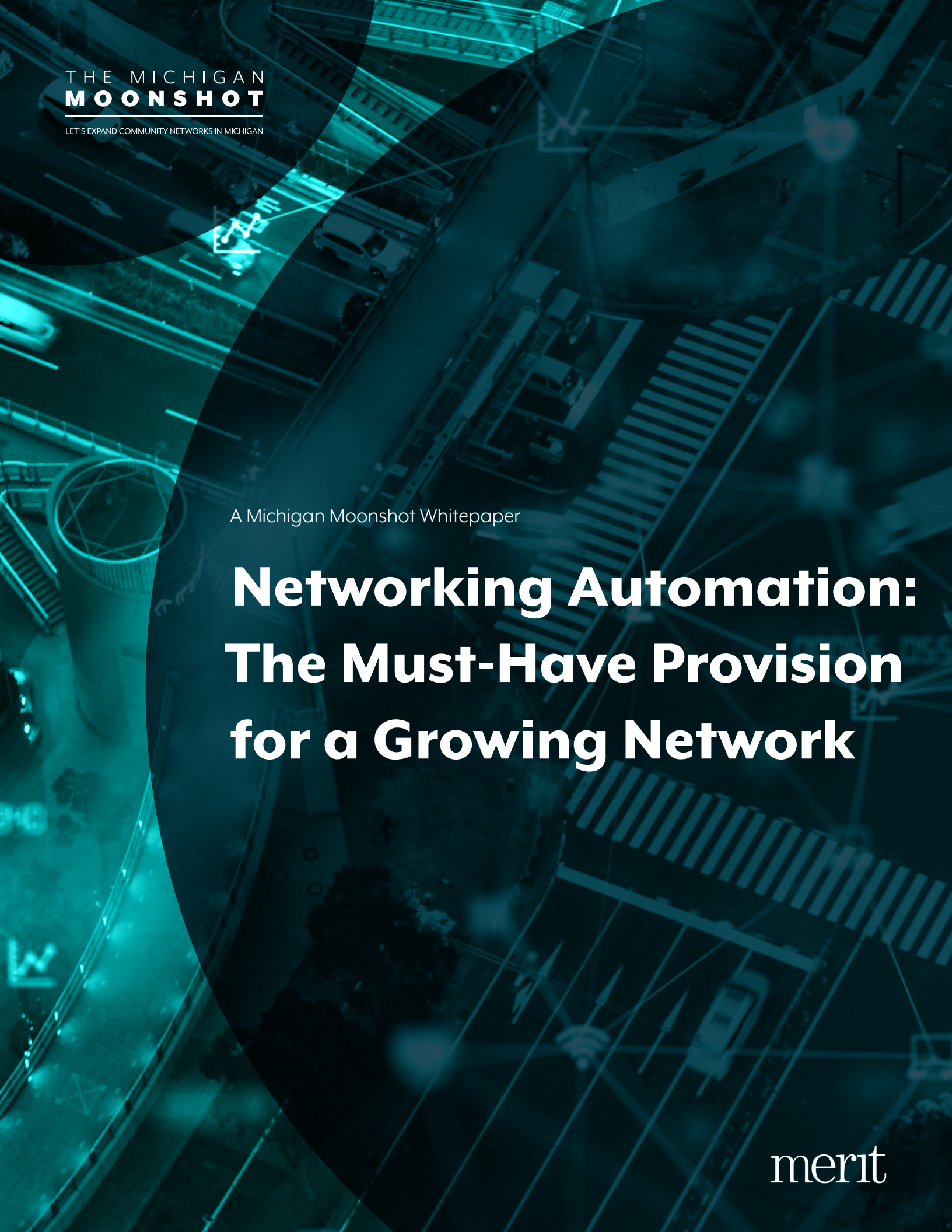

THE MICHIGAN
MOONSHOT

LET'S EXPAND COMMUNITY NETWORKS IN MICHIGAN

A Michigan Moonshot Whitepaper

Networking Automation: The Must-Have Provision for a Growing Network

merit

Presenters:

Bob Stovall
Vice President of Infrastructure
Strategy and Research
Merit Network, Inc.

Michael Milliken
Vice President of Technology Operations
Merit Network, Inc.

Kevin Hayes
Chief Information Security Officer
Merit Network, Inc.

Eric Boyd
(Joined by Fellow U of M Team Members)
Director of Networks in the School's Information and Technology Services Division
University of Michigan

Grover Browning
Manager of Network Automation
GlobalNOC

Karl Newell
Network Software Architect
Internet2

Michael Kowal
Principal Architect
Cisco

Kevin McCartney
North America Business Development
ADVA

Calvin Remsburg
Senior Sales Engineer
Juniper Networks

Introduction

All speakers were part of Merit Network's recent workshop, How to Evaluate Potential Networking Automation Decisions and Craft the Plan. This online workshop provided attendees with the benefits of automation for any organization, presented tools and tips for getting started quickly, and ways to remain cost-effective during each step.

Held on May 11, 2021, as part of Merit's annual Merit Member Conference, the event featured speakers from Merit, the University of Michigan, Internet2, Cisco, GlobalNOC, and ADVA who discussed the ways in which network automation has made their networks more efficient, secure, and up to date.

Getting Started With Network Automation

Network automation is moving from something viewed as impressive but unnecessary to a must-have element of a stable, reliable network.

Network automation is exactly what it sounds like: automating many of the routine, repetitive tasks that engineers perform on network equipment in their workdays. The speakers emphasized that, far from eliminating the need for networking staff, automation frees up engineers' time to finally do the higher-level, longer-view work that so often gets sidelined.

Examples of automated tasks include updates to network equipment, configuration changes across the network, getting an inventory of all devices on the network (key in tightening up security), and "zero touch" provisioning —deploying new equipment to sites with little to no physical handling. "(Automation can) change the way that we interface with devices, change how we can pull data out of our live network and make assertions as to the current health within that environment," said Calvin Remsburg, senior sales engineer with Juniper Networks.

Why Organizations Hesitate

"Two common misconceptions prevent an organization's engineers from taking the first steps to automating network tasks," said Bob Stovall, Merit's vice president of infrastructure strategy and research.

But shops of any size can benefit from being able to, for example, push out security updates en masse instead of one at a time. "This will reduce your risk and make your team look like heroes," Stovall said. The other is the assumption that automation leads to job cuts and smaller staff sizes. This is false, he and other presenters said. Instead, it frees up engineers' time to do higher-level work rather than repetitive manual tasks.

"Utilizing automation saves jobs because it will enable our technical teams to focus on growth and to enable them to deliver new services that they do not have time to investigate and develop because they are using their time to do repeated day-to-day duties that automation could replace," Stovall said. "Every organization can leverage automation at one level or another to save time and to also start creating growth."

Grover Browning, manager of network automation at GlobalNOC, gave the example of having to do thousands of password rotations on network devices. "Instead, we let the automation tools do that, and the network engineers can think about architecture issues and solving bugs that affect multiple people and enhancing services."

Some engineers, in dismissing the need for automation, note that most tasks can be done quickly through the command line. "This is true," said Michael Milliken, Merit's vice president of technology operations, "but the question now more than ever — with cloud-managed resources taking hold — is whether that can be done at scale. The new guard is going in a different direction. The same time could be spent on long-term capacity planning or bringing new technologies into the network."

> "Utilizing automation saves jobs because it will enable our technical teams to focus on growth."
>
> **-Bob Stovall**
> Merit Network, Inc.

Tools of the Trade

As with anything else, network automation comes with some preferred tools.

Calvin Remsburg at Juniper Networks matched the following tools and tasks:

- NetBox and Nautobot for developing a network source of truth
- Python and Golang for programming languages
- Ansible and Terraform for making automation frameworks
- JSNAPy and pyATS for testing frameworks
- GitHub and GitLab for source code management
- Ansible and Cisco NSO are two of the more frequently mentioned names

Ansible, which is open source, is recommended as a good starting tool. GlobalNOC at Indiana University has developed its own suite of automation tools based on Ansible and GitHub tools, allowing it to do things like automatically rotate thousands of passwords or audit thousands of devices at once. “It reduces incidents that cause downtime,” said Grover Browning, manager of network automation at GlobalNOC.

Karl Newell, network software architect for Internet2, said his organization is “heavily into” Cisco NSO, which is a paid product, and likes it for its ability to run configuration commands across many devices at once, from one point of view. NSO also has a feature where it rolls back a task if the command fails on one device, so the engineer isn’t left unaware that the command didn’t take across the whole network.

Newell worked with Michael Kowal, principal architect at Cisco, in 2019 to put together a proof of concept for “Multi Organization Service Orchestration”, or orchestrating a service across multiple domains, not just at Internet2 but also at connecting institutions including higher education campuses. They have been able to use NSO to rapidly develop and provision services for multiple domains.

Newell said NSO also is good at preventing "config drift", where differences in equipment configurations across the network build up over time. This stems from engineers modifying devices to meet changing circumstances, causing the automated system to get out of sync with actual configurations on the ground. "This is a normal challenge" and one that NSO manages well, Newell said. Ansible also is good at preventing configuration drift, noted Browning at GlobalNOC.

Merit Chief Information Security Officer Kevin Hayes says Netdisco and Lansweeper are two great tools for getting an inventory of all the switches and devices on your network. Netdisco goes to all the switches on the network, reads the MAC addresses, and gives a 100% inventory of what's on the network.

Netdisco and Lansweeper also allow engineers to do things like separate user devices into different categories and thereby exert control over them. While engineers may not have control over all devices on a network, such as those of guests, automating the inventorying of them allows security policies to be put in place to manage them. Devices can then be classified and placed in separate wireless networks under different SSIDs, for example.

Typical Uses

Network automation can cover a broad range of tasks. Here are some examples to give newcomers an idea of how it is used:

- Mass changes to wireless access points
- Device upgrades
- Weekly maintenance
- Rotating passwords
- Managing access control lists
- Deploying new services
- Converting configurations between network vendors
- Applying configurations to devices
- Troubleshooting firewall configurations
- Validating state changes before and after a configuration change
- Software upgrades
- Building custom graphical user interfaces

Rapid deployment and "zero touch" provisioning is another area where automation is valuable. It allows teams to deploy new network gear in an organization with little to no physical handling, reducing time in the field and the chances for problematic configuration to occur during setup. Devices can be set up for self-service, "phoning home" to get set up.

A team from the University of Michigan showed how Ansible can be used for this, describing how the school used Juniper Zero Touch Provisioning to set up a new building with 49 switches. "We were able to deploy the entire building without ever physically seeing or touching those devices," said Jeff Hagley with UM.

When it comes to security, automation allows engineers to more practically manage all the monitoring data that comes in from the network. Automation can be tap into read-only dashboards and make working with security rules easier. (See more on security below.)

Protection Against Cyber Threats

Automation can be used to make sure that essential — but too often overlooked — security is in place.

In a world of ransomware and volumetric attacks, there is no room for error, said Merit Chief Information Security Officer Kevin Hayes. "You need to make sure, especially when it comes to automation, that you have those most basic security controls applied to your entire environment, zero exceptions," Hayes said. "We need automation because there is no way for us to do all of this manually. No exceptions. Because those exceptions are always — hands down, without a shadow of a doubt — always the place where an attacker will find a weakness."

Automation makes sure that devices that engineers don't know exist on the network get inventoried and that all devices on the network, including those of guests, are at least known, if not controlled. He noted that the data that comes from scans of networks, revealing such things as security cameras not properly secured, is made available in online database services. Automation reveals long-forgotten servers and web applications set up by systems administrators who no longer work for an organization, so network teams can reassert control over them.

Automation is an effective way to take an inventory of the network. "We can't make sure that security is applied to a thing that we don't know about. It all starts with that accurate inventory, and it doesn't have to be overly complicated," Hayes said.

When a high-profile attack makes headlines, the embarrassed organization eventually comes out with the reason why the attack was successful. Invariably, it's something simple and predictable, like a firewall or basic logging not being enabled, or local administrator rights being handed out where they shouldn't be, Hayes said. Automation ensures these things aren't missed. "You can sleep a lot better at night when you use security automation," Hayes said.

> "Exceptions are always — hands down, without a shadow of a doubt — the place where an attacker will find a weakness."
>
> **-Kevin Hayes**
> Merit Network, Inc.

It Doesn't Take Long To Get Started

"There's no need to be overwhelmed by the idea of automating. It can be done in steps and doesn't have to be done all at once," said Michael Milliken, Merit's vice president of technology operations.

Newell at Internet2 recommends starting with a small set of tasks to automate and taking it from there. "Define a small set of things you want to automate, demonstrate that you can do it, get that deployed, then do it again and keep building on that. Eventually you build in a process where you can operationalize a larger automation workflow, and pretty soon you'll have a lot of your tools and a lot of your configuration under automation," Newell said.

About two-thirds of it is straightforward and can be done immediately, said Browning at GlobalNOC. "Your journey into network automation doesn't have to be hard," Browning said. "What we are generally presented with are the rather sophisticated endgame results that many institutions have worked towards and are now implementing. What we seldom see though are the beginning steps that institutions are taking. Those beginning steps can get us quite a long way down the network automation path … without wasting effort or time or money."

The first steps are to get an inventoried list of the devices on the network and get Ansible installed on the team's laptops or a group server.

The early "two-thirds" part of this includes operational tasks, such as upgrades to routers and switches, and configuration changes to devices where each device is given the same change. The more time-consuming tasks that come later tend to be changes where each device has to be given a different configuration, such as giving them different IP addresses or interface names. "The operational tasks and the part of the config that's supposed to be the same everywhere — these are things that realistically you could have the infrastructure ready to go by end of this week and by the end of next week, working casually, you should have been able to make meaningful upgrades to the network," Browning said.

To learn more about implementing networking automation within your organization, contact your Merit Member Engagement Manager directly or reach out to sales@merit.edu.

About Merit's CISO, Kevin Hayes

Kevin Hayes is the Chief Information Security Officer at Merit Network, Inc. In this role, Kevin is responsible for the management of IT security controls and products, responding to information security incidents big and small, and providing security policy and strategy guidance to Merit members, system administrators, and management. No stranger to the nonprofit world, Kevin has previously worked at Wayne State University, creating and directing the team of cyber professionals dedicated to keeping the organization secure. Kevin holds both CISSP and CISM certifications, is a member of the Governor's Cyber Civilian Corps, and has been heard talking about security issues from time to time on the Detroit television stations WDIV-TV and WXYZ-TV, as well as the Detroit public radio station WDET-FM.

About Merit's Vice President of Technology Operations, Michael Milliken

Michael's responsibilities encompass a wide variety of strategic technology issues including technology adoption, governance and policy, recourse allocations, capacity planning, engineering, network architecture, and operations of Merit's network. Prior to his role as Vice President, and as Executive Director & Director before that, Michael served as a Senior Network Engineer with responsibilities ranging from engineering, field operations, provisioning and service delivery, including network maintenance and monitoring. Michael's background includes over 20 years in the information technology, network operations, cybersecurity and telecommunications industries, with experience in the service provider (SP) and large enterprise arenas, and designing, deploying, securing, operating, maintaining, and troubleshooting large-scale networks.

About Merit's Vice President of Infrastructure Strategy and Research, Bob Stovall

As Vice President of Infrastructure Strategy and research, Bob has an extensive background in networking and has served in several technical and managerial capacities since joining Merit in 1989. Prior to becoming vice president, Bob served as director, department manager, team leader, supervisor, engineer, and technician. He has lead Merit Operations, Engineering, the Network Operations Center, and IT departments. Bob and his team have engineering and operations responsibility for Merit's backbone network, member access circuits and IT services.