7 HABITS OF HIGHLY EFFECTIVE DC NETWORKERS

A Packet Pushers White Paper

PACKET PUSHERS

Contents

Introduction

To be a data center network engineer is to live with complexity and uncertainty. A change in one place could have an unintended effect somewhere else. Performance could suffer, workloads could be exposed to security threats, or the network could crash.

To operate successfully in uncertain environments where network requirements constantly evolve, network engineers need to cultivate good habits. Experienced network engineers tend to be careful, thoughtful, and precise.

Traditionally, before making a change, they seek out information about the network through SNMP traps, syslogs, device configurations, packet captures, and streaming telemetry. Some network teams gather this information manually. Others might deploy network sources of truth that centralize essential information. And some organizations take advantage of new tools such as AI for IT operations (AIOps) software and intent-based networking (IBN) that collect and contextualize multiple sources of information about the network.

For instance, AIOps software might alert engineers to a potential problem and offer a fix or provide a virtual assistant that can answer natural language queries with responses drawn from network devices and domain-specific sources, such as vendor documentation and knowledge bases. IBN software can suggest, and then implement, configuration updates that will align with high-level business outcomes, as well as security and performance requirements.

If and when changes need to be made, experienced engineers have processes in place. Typically, these processes are manual, but more and more organizations are incorporating, or want to incorporate, automation. Automation efforts can range from a handful of tried-and-tested scripts to DevOps-like pipelines with well-defined procedures and pre- and post-check stages, to full-blown orchestration in which changes are executed across multiple devices and systems in the correct sequence and then validated to ensure correctness.

Regardless of how you and your team operate, this paper proposes seven habits that can help network engineers better grapple with the uncertainty in data center management and operations.

The seven habits are:

1. Design for business outcomes
2. Automate for reliability and repeatability
3. Learn once, use often
4. Pick the right equipment
5. Validate as you go
6. Be proactive, not reactive
7. Document your work

These habits can be bolstered by good tools. As legacy network management systems modernize and private infrastructure scales, IBN and AIOps are becoming an engineer's best friends. We'll also discuss how these tools complement healthy work processes.

1. Design for Business Outcomes

The reason a data center network exists is to support the applications and services that drive a business. However, a typical data center design tends to start with vendor selection rather than desired outcomes. That selection is often influenced by factors other than business objectives. An executive who's enjoyed many fine lunches with a sales rep may want one product, while the engineering staff who've invested time and money in vendor certifications might want another.

There may be critical differences among products. One vendor's code might be weighed down with "features" that the organization doesn't want or need, but still has to maintain and update. One vendor's hardware specs might be ideal, but its network OS could be buggy. How the vendor implements a key protocol might require extra effort by the engineers to make it work, or require engineers to learn a different or proprietary protocol. And over time, organizations tend to end up with multiple vendors in the network, requiring the networking team to dedicate time to integration efforts just to get basic connectivity.

The result is the demands of actual business applications have to be bent to fit within the quirks and constraints of the network. This means more operational complexity and a greater risk of problems. It slows down the pace at which the network can support new applications and services, so the network becomes a bottleneck.

A better habit is to start with business outcomes and then design the network and choose vendors based on the desired results. That way, data center infrastructure aligns with strategic goals, enhances operational efficiency, and is custom-built to add value to the business.

IBN solutions are a great match for this approach. IBN translates operators' intent into specific configurations and policies across different vendors, abstracting away the complexities of individual interfaces and proprietary protocols. Instead of getting bogged down in different command line interfaces (CLIs), operators can work efficiently, stay focused on business outcomes, and respond to change quickly–even if the company chooses a different vendor the next day.

2. Automate for Reliability and Repeatability

The networking industry has been talking about automation for decades, but most enterprise shops have yet to move past home-grown scripts that engineers use like a multi-function pocket knife: A few handy tools for small jobs.

The truth is, most enterprise data centers are too brittle to support broad, reliable automation that's orchestrated across multiple devices and services. An automated process could kick off a sequence of unintended events that brings down the entire network. And after setup, it's not unusual for configurations to drift away from a baseline. Engineers who write scripts and playbooks have to constantly adjust their code to account for the nuances of the different software versions running on network devices, leading many to defer critical software upgrades.

Network engineers are also missing key elements to support broad-based automation. That includes deep visibility into network state, a reliable source of truth of the expected device configuration, the ability to test changes before being pushed into production, and a mechanism for validating the outcome of a process.

Automation isn't just about getting tasks done faster. The real goals of automation are repeatability and reliability. Good automation should enable engineers to make changes over and over in response to new requirements, and to have processes in place that ensure those changes don't contain errors or will have unintended consequences.

A good IBN solution enables reliable and repeatable automation because it has guardrails in place to prevent unintended problems and to ensure that changes align with the operator's intent. For example, if an engineer makes a configuration change that doesn't align with intent, whether it be a typo in a command or a configuration change that would violate an existing policy, the software will notify the engineer and prevent the change. This dramatically reduces risk across the network lifecycle, from deployment to upgrades and migrations to everyday service delivery.

IBN approaches networking the same way an industrial manufacturer approaches a factory: They both want to operate at high speed with high quality at scale. Reliability and repeatability have to be built in from the ground up, and that means starting with a sound network design. Network operators should leverage validated designs that provide blueprints for architects and engineers to build tried-and-tested data center networks based on best practices and industry-standard protocols. By choosing a validated design, network engineers minimize the technical debt and operational difficulties that inevitably accrue with designs that are highly customized and rely on arcane workarounds and institutional knowledge just to function.

3. Learn Once, Use Often

Anyone who uses a business application only occasionally knows that each time you come back to it to complete a task, you inevitably have to waste time re-familiarizing yourself with how it works.

The same applies to management, monitoring, and automation tools. If they aren't a part of your regular workflow, your task gets delayed as you fumble around the interface. It's a good habit to know your tools well so that you can get the most value from them.

Organizations encounter two common problems with toolsets:

- Dual-vendor strategy is common among enterprises, yet can cause challenges for network operators because they need to become familiar with different management tools and proprietary solutions
- DIY automation tends to happen in ad hoc fits and starts, with shell scripts or in-house tools that can introduce as many problems as they solve

A better habit is to use an IBN tool as a source of truth that operators refer to on a daily basis across various hardware vendors, and build any required higher-layer automation on top of the IBN system so that it remains consistent, regardless of the underlying hardware vendor devices or software versions.

4. Pick the Right Equipment

A smart habit is to choose the right equipment for the job at hand, rather than have to conform operations to fit how a particular piece of equipment works. Vendor lock-in can lead to inefficiencies and higher costs, and no company should work with suboptimal solutions that do not fully meet their requirements just because it's the one currently running in their network.

A vendor-agnostic IBN solution gives network teams the flexibility to get the right hardware to support the company's objectives. If you can slot any vendor's hardware into your network, you have better purchasing leverage, flexibility to deal with supply chain constraints, and, most importantly, freedom to adopt new technologies or solutions that better suit your needs but are not offered by your current vendor.

Good AIOps software can also support multi-vendor strategies by normalizing the various data models and configuration schemes used by individual vendors to provide contextualized output, regardless of the underlying platform. This can streamline operations by reducing the amount of effort engineers have to expend on context-switching in a multi-vendor environment. In addition, AIOps software with virtual assistants can be trained on information from multiple vendors to provide responses that are context-aware and syntactically correct per each vendor's own documentation.

5. Validate As You Go

Tech social media is full of anecdotes about hasty CLI commands, misconfigurations, and typos that resulted in all sorts of exciting and challenging outcomes. The fact is, humans make mistakes, which is why successful engineers check their work before pushing to production.

Those checks can take a variety of forms. Some network OSs check each word in a command string as it's typed to alert engineers to a typo. Engineers might ask a colleague to sanity check a configuration or upload scripts to a repo for others to review. Some organizations rely on ITIL-based change management processes.

A good IBN solution enforces this good habit by automatically generating valid vendor-specific configurations based on the user's intent and then continuously validating device changes to make sure those changes align with intent. Continuous validation limits human mistakes while also ensuring that new changes produce the desired intent. That is, the new changes fit within business-defined parameters regarding reachability, performance, security, and compliance.

6. Be Proactive, Not Reactive

It's a good habit to deal with small problems before they become big ones. For instance, if a switch port goes down intermittently, it's better to find the root cause and address it before the port fails outright.

If you wait, you're going to be swarmed with alerts and logs (and perhaps angry text messages) while you try to figure out what went wrong. If it's a loose cable, you got lucky. If it's a bad network card or optical module, you might wish you'd kept spares on hand.

IBN solutions use advanced analytics capabilities to help network administrators be proactive. They monitor the entire infrastructure, from physical devices to the operational state of the data center. They continually validate against predefined intent. And they flag anomalies that could potentially lead to larger problems so networkers can deal with them quickly. AIOps complements IBN by dynamically adapting to changing network patterns, helping spot anomalies, and offering a more responsive and adaptable approach to network management.

Working together, IBN and AIOps help engineers discover issues before they become problems so they can respond smoothly and efficiently instead of with their hair on fire.

7. Document Your Work

Like eating your vegetables and exercising regularly, everyone knows that documenting your work–be it updating network diagrams, annotating configuration changes, updating process documents, and so on–is a good habit. Documentation explains what and why something was done. It provides a record of what happened. This record can come in handy later on for new changes, troubleshooting, an audit, and so on.

Documentation is important because engineers move into different roles or take a job elsewhere. When they go, they take a lot of operational and institutional knowledge with them. Documentation captures this knowledge so that it can be retained by the organization and shared with operators.

The problem is that documenting your work is tedious and time consuming. It's often the last thing on an engineer's mind when grappling with a tricky new deployment or responding to a crisis. Of all the habits on this list, regular and reliable documentation might be the hardest to maintain.

Using an IBN system eliminates a lot of the pain of outdated or missing documentation because the system maintains a clear view of the user's intent as a source of truth, independent of specific device configurations, and ensures the network's running configuration stays in sync with that intent.

Manage Uncertainty and Complexity with Juniper's Data Center Solutions: A Brief Overview of Apstra and IBN

If you're looking to optimize your daily operations and ease the pain of migrations and upgrades, Juniper's IBN and AIOps solutions can help.

Juniper Apstra empowers service providers and enterprises to manage their private data centers with the same simplicity as running cloud-based infrastructure. With Apstra's IBN automation capabilities and intuitive design, customers can navigate and configure their data center with reduced complexities.

Marvis VNA for Data Center is the industry's only AI-Native virtual network assistant for data center operations. It works in conjunction with Apstra to provide proactive and prescriptive data center actions and simplify knowledge base queries using the Marvis conversational interface (powered by GenAI). Proactive actions by Marvis save time and money and increase network uptime by accelerating problem resolution.

By combining the power of AI and intent-based networking, Marvis VNA and Apstra create an unbeatable operational experience for data center network teams.

To see if Juniper's solutions are right for your data center, learn more about Apstra and Marvis for the DC.