The bridge to possible

Preventing Network Service and Security Disruptions Through Automation

The Modern Approach to NetOps

Mark Harris, SVP of Marketing, NetBrain Technologies, Inc.
@Mark_J_Harris

cisco Live!

BRKPAR-2911

ABSTRACT:

Network Automation is the biggest untapped opportunity for NetOps. We'll demonstrate how Network Automation can be leveraged by everyone using a No-Code approach to reduce service delivery and outage risks, scale resources without the typical rise in headcount, and reduce the operational costs associated with the network. This session will demonstrate the means for network engineers and operators to proactively address outages, automate remedial diagnosis, identify application performance issues, enforce network security architectures, and defend change management processes to eliminate unintended consequences. We'll discuss how subject matter expert can leverage No-Code approaches to make their expertise available to all others across any organization, and even collaboratively with related ops teams. We'll also discuss how that same captured knowledge can be executed by less experienced operators and automatically by the machine, dramatically reducing the time it takes for operators to resolve network problems of any size.

Agenda

- The Problem with Today's NetOps
- Forward-Looking Operational Plans
- Focusing on Outcomes, Rather than Devices
- The False Sense of Security
- Real-World Use Cases and Scalability
- No-Code and Subject Matter Experts
- Conclusion

FACT #1:

"According to a report published by the Identity Theft Resource Center (ITRC), a record number of 1862 data breaches occurred in the USA in 2021, up 68% from 2020"

https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/

FACT #2a,b,c,d:

- The average cost of a breach is $4.62M
- 39% of all remediation costs occur more than a year after detection
- Breach conditions persist for up to 287 days before being reported
- It takes an average of 80 days to contain a breach and much longer to restore normal operations

https://www.varonis.com/blog/data-breach-statistics

FACT #3:

"Study Reveals that 96% of Enterprises face on the average of FIVE severe Network Outages and IT Service Degradations per year, with staggering hard and soft costs."

https://www.globenewswire.com/news-release/2019/09/24/1919728/0/en/New-Study-Reveals-that-96-of-Enterprises-Face-Costly-IT-Outages-Though-IT-Says-51-of-Downtime-Is-Avoidable.html

The Problem with Today's NetOps

"Are you behaving tactically or strategically?"

- Security compliance and Outage prevention must be proactive
- Modern network technologies are managed using DECADES old approaches
- NetOps is focused on device health rather that business outcomes
- SMEs exist locally, but can not be leveraged effectively
- Resources are not as plentiful as they had once been
- NetOps is consumed with Tickets, solving the same problem over and over
- Escalations take time, increasing MTTR, risk and costs
- Nearly all NetOps is reactionary, IT needs pro-active management

Forward Looking Operational Plans

"How can we operate differently?"

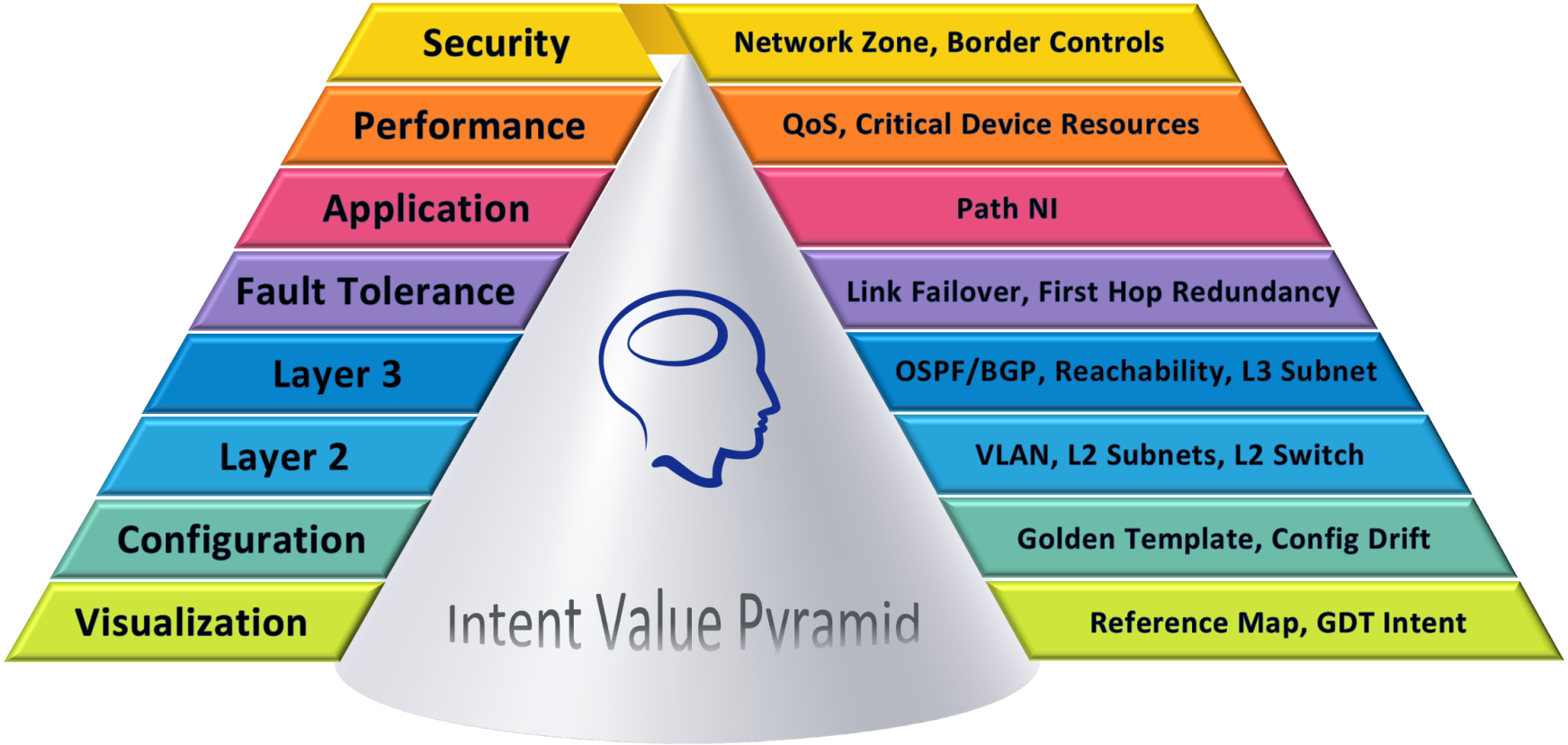
- Current NetOps is reactionary, inefficient, inconsistent, labor intensive, engineer specific, redundant, time-consuming, not sharable, not scalable
- How can we capture the expertise of our SMEs?
- How can we share that experience across the organization?
- How can we execute knowledge more automatically?
- How can we apply that experience pro-actively?
- How can we continuously verify the network supports the business?

Focus on Outcomes, Not Devices

"Do you know how your network actually supports your business needs?"

- Think of your network as 100,000 desired outcomes instead of 1000 boxes
- The business defines the outcomes, and IT must deliver all of those
- When outcomes are intact, business applications and services perform
- The outcomes can be quite diverse, and championed by different groups

Focus on Outcomes



The False Sense of Security

“Are You Really Protected?”

- Far beyond purchasing the latest H/W and S/W
- Every part of a security architecture must be continuously verified
  - Do you know ALL of your Device, Border, Edge and Zone requirements?
  - Examples: Does TELNET traverse the network? Are specific ports open?
- Continuous Observability and Control verification at scale
- Application-aware security, manage specific requirements and control
- Security Orchestration Automation and Response

Real-World Use Cases

"Did you know that relatively few BUT SIMILAR problem types occur?"

- Outages can be prevented by looking at configurations that drift from design
- Issue reports can be addressed by using previously captured best practices
- Application and service performance can be assured though continuous verification
- Change Management must be executed within eye on ALL other services
- Security must be continuously verified at every device, border, edge and zone

Scaling our SME Knowledge

"Do you solve the same problems over and over again?"

- Most network problems occur repeatedly if 'similar' is understood
- Problem resolution is inconsistent from engineer to engineer
- Without understanding the context of outcomes, changes to the network will yield unintended consequences

No-Code and the Subject Matter Expert

"You already know how to solve any problem, but not at scale"

- No-Code approaches allow SME knowledge about preserving outcomes can be captured and made re-usable
- SME knowledge can be applied at scale for continuous verification

But What About AIOps?

"Isn't AIOps the answer to everything?"

- Hardly. Huge investments, limited/no results, failed projects…
- It's because AIOps is attempting to answer the wrong question:
  - "What is the resolution to this problem?" In reality, NetOps already knows the answer, they just haven't captured it and consequently can't re-use at scale.
- Security and service degradations can always be prevented one situation at a time, but to do so at scale requires an automated approach

Conclusion

"What can you do Today?"

- Network Automation is one of the rare opportunities to fundamentally solve operational challenges at scale
- Networks should be described by the capabilities they deliver and the attributes of those delivered services
- By focusing on Security and Service Delivery outcomes, all other operational processes become more relevant and aligned with the business itself
- Subject Matter Experts can be leveraged far more effectively by converting their expertise into executables that can be shared


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN