SOLUTION BRIEF

Preventing Network Outages

For decades, IT professionals and business leaders dealt with network outages as a mission-critical situation which severely impacted the business when it occurs but struggled to do anything about it. Today, NetOps continues to run in reactive-mode, repairing situations after they occur. The direct and indirect costs to operate reactively far exceeds what it would be if outages were prevented in the first place.

During much of those years, applications and devices were monolithic in nature, meaning that failures tended to bring entire business functions down. In the era of decomposed applications, microservices, resiliency and cloud-centric infrastructure architectures, network outages take a different form. Modern outages are better described as service degradations, where business services continue to be available, but at a reduced level. In either case, the result is the same: business is impacted.

What if you could simply describe and maintain the network as a set of required network behaviors that support every application? In addition, you could ensure the network adheres to these requirements.

NetBrain defines these as Network Intents. They help maintain ideal network behaviors including connectivity, performance requirements and security attributes required for every application to perform as defined by the solution architects.

Intent-Based Automation Makes Outage Prevention a Reality

NetBrain's intent-based automation maintains network requirements for every application, including its performance requirements and security profile, to proactively prevent outages. By understanding, in real-time, how the network is performing and then comparing that performance to the previous described behaviors (Network Intents), IT can prevent issues before they result in outages or services degradations.

With NetBrain, large enterprises can quickly scale to tens or hundreds of thousands of Network Intents that span a complex hybrid network and the cloud allowing them to continuously compare established network intents against the real-time network.

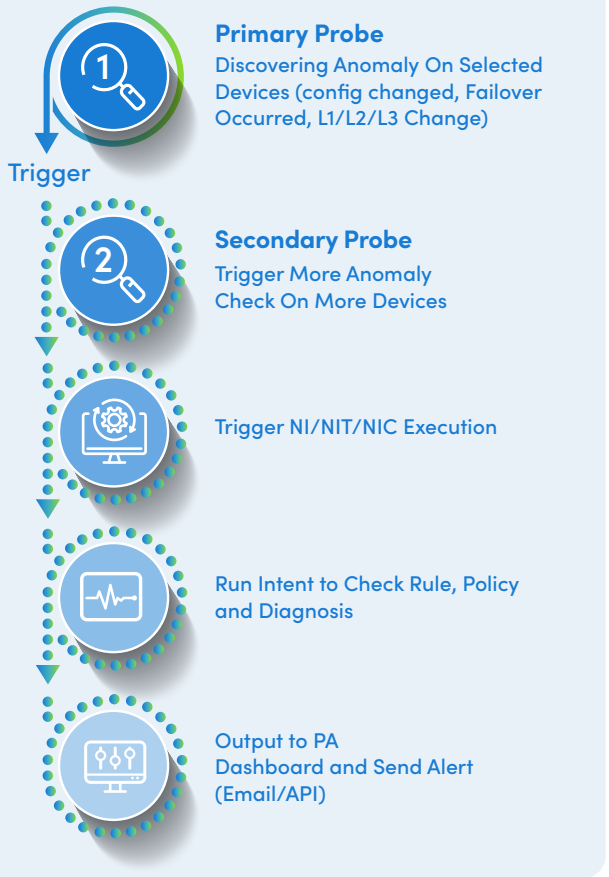
Preventing Outages, Not Reacting to Them

NetBrain's Problem Diagnosis Automation System (PDAS) revolutionizes network automation for ongoing "Day-2" network operations by abstracting Network Intents from the underlying network infrastructure. This allows NetBrain to automate the enforcement of the network design including performance rules and security requirements. NetBrain's intent-based automation allows network operations teams to adopt a preventive infrastructures strategy, greatly reducing the cost and risk.

What makes NetBrain different is its ability to continually validate and verify that the network is providing the exact level of service needed by every business application, and to enforce application performance. NetBrain automatically generates the network intents, based on its unique ability to understand 'similar' situations, even if the underlying hardware or software is dramatically different.

A Preventive Automation Framework (PAF)

NetBrain's PAF provides intelligent and proactive continuous network monitoring and health check of your entire hybrid network. It enables complete compliance verification, including performance and security requirements, and generates alerts when deviations are detected.



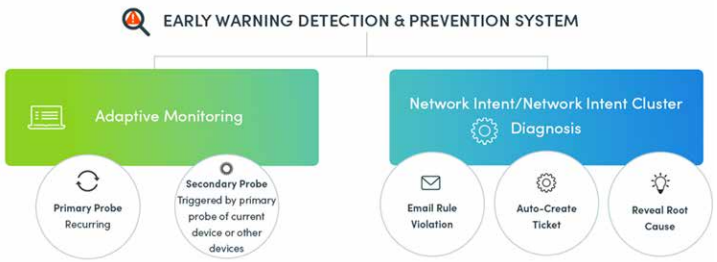
Early Warning Detection System

As NetBrain encodes a hybrid network into a proactive problem diagnosis automation framework that continuously compares the live network against the previously established list of desired results (Network Intents) to identify discrepancies caused by equipment failures, configuration drift and shortsighted configuration changes that may not have considered their effect on the rest of the network and its existing applications.

The PAF is different from the traditional monitoring systems, in that it:

- is designed to proactively enforce design and security rule checks automatically, not monitoring system errors
- can be customized based on network design and the critical path flows, not one-size-for-all
- can serve as a next-gen design compliance check solution – it is continuously running and can be exhaustive in its proactive diagnostics without any laborious setup

NetBrain's PAF consists of two core components.



Network Intent (NI)

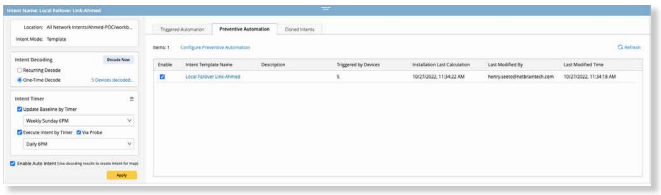
The PAF uses NI to regularly compare the current network status with pre-determined thresholds.

Network Intents describe all the required behaviors of the network in the context of each application and IT service it supports. They:

- quantify the connectivity, performance and security controls that must exist for each service to be successful
- are used interactively to address abnormal behaviors, proactively in response to external events, and preventively to verify the entire network is operating as intended

To reduce the likelihood that minor problems manifest into catastrophic outages or service degradations:

- **Intent Timer** establishes baselines at configured intervals to run Network Intents in support of network compliance and audits. At any desired interval, before deteriorating conditions can generate alerts, it tests network intents against the baselines and provides advanced warning.

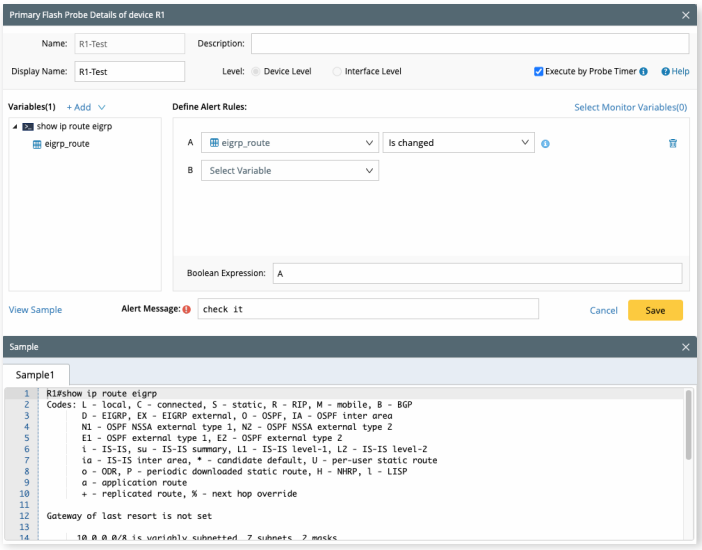


Adaptive Monitoring at Scale

The workhorse of NetBrain's Preventive Automation is its Adaptive Monitoring system which leverages virtual probes to automatically identify when network conditions are violated. The system maintains baselines for expected behaviors across the entire hybrid network as NIs and regularly tests the live network against those baselines, or NIs. It ensures network conditions remain as expected based on application needs.

The PAF triggers virtual probes that run Network Intents on a timer and identify network anomalies and alert you to a first occurrence and transient problems. These consist of:

- **Primary Probes:** Primary probes use Network Intents to check for anomalies (e.g., device configuration changes and interface errors) and poll at any desired frequency. NetBrain supports two types of primary probes:
  - Alert-based Probe: triggered by device-generated anomaly (configuration-related information).
  - Timer-based Probe: triggered by an interval timer and can be used for scheduled CLI and scheduled Network Intent tasks.
- **Secondary Probes:** Secondary probes are only triggered by primary probes because of an alert when more detailed diagnostic investigations are needed.
- **External Probes:** External probes are used for integration with other monitoring systems. Once the integration is complete, the alert triggered by 3rd-party systems can implicitly generate external probes.



When NetBrain probes detect alerts, they automatically send notifications to engineers.

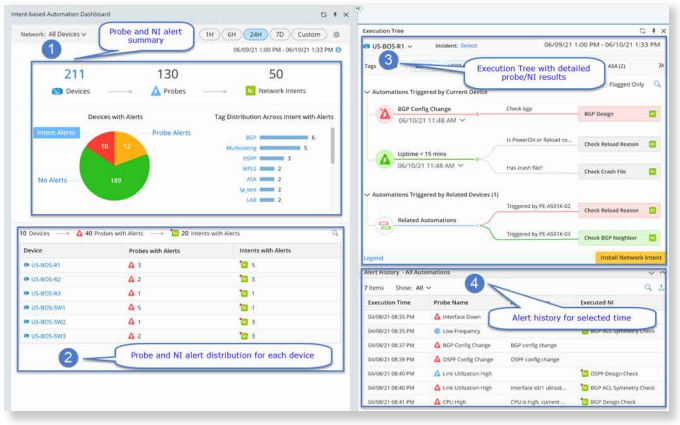
Network Intent Template (NIT) helps users replicate Network Intents for devices across the entire network to scale the troubleshooting performance by simply using the device qualifications (what devices to clone) and the critical variables (how to clone).

Network Intent Cluster (NIC) expands the scope of Network Intent from a specific network design to one type of network design with similar diagnosis logic. Since NI applies to only one network device or a set of devices at a time, it could take effort to create NIs for a large network individually.

- NIC expands the logical scope of an NI from one or a set of devices to the whole network, where similar conditions exist.
- NIC uses cloning through a proprietary no-code process. NIC is used for any complex logic that's not at the individual device level (e.g., to compare one device with another). Use it for customized device groupings for even more control.

NI/NIC/NIT provide the automated diagnoses and rule checks triggered by early warning alerts from any set of logic probes.

PDAS displays the data from the probes in an easy-to-use Preventive Automation Dashboard showing the number of device alerts by probe and by Intent.



NetBrain's intent-based PAF dramatically reduces the number of outages by understanding what your infrastructure should always be doing, every nuance of the network in the context of what is needed by each application and topology. It then proactively verifies that the real-time network is delivering the expected results, including active and standby configurations, security profiles and access control, and even the performance considerations needed for real-time applications like VoIP.

Preventing Outages is Not Just a Dream, It's a Reality

While most organizations have invested heavily in resilient and secured hybrid infrastructures, the reality is services outages are increasing in frequency and severity and it has an impact on both direct and indirect costs. 'Service outages' are no longer limited to the infrastructure being "UP" or "DOWN", in fact most outages today are service degradations, where an application is impacted, but still available at a reduced capacity. For instance, a back-end server may normally be able to process a million record lookups per minute, but due to network infrastructure issues, is now able to process one-third of that number.

The holy grail of network management has always been outage prevention because preventing outages is much less expensive than responding to them in a war room scenario. Every moment infrastructures are degraded contribute to both hard and soft costs, reputation, customer satisfaction, and in the worst-case scenarios, valuations.

About NetBrain Technologies

Founded in 2004, NetBrain is the market leader for NetOps automation, providing network operators and engineers with dynamic visibility across their hybrid networks and low-code/no-code automation for key tasks across IT workflows. Today, more than 2,500 of the world's largest enterprises and managed service providers use NetBrain to automate network problem diagnosis, generate real-time documentation, accelerate troubleshooting, and enforce enterprise architectural rules.

NetBrain

NB-SB-PNO-110422

+1 (800) 605-7964
info@netbraintech.com
www.netbraintech.com