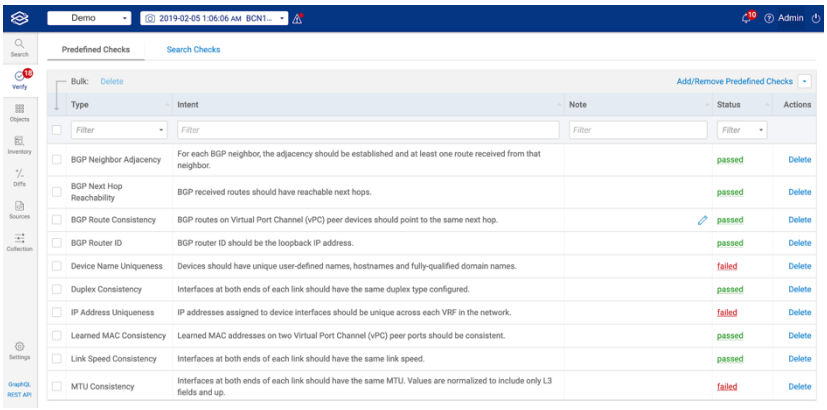
Forward Enterprise Use Case
Network & Configuration Audit

In dynamic, agile network environments, ordinary tasks include updating existing devices and making changes to current configurations. Multiple vendors and diversified networks increase the complexity and the reliability of such changes, making standard configurations harder to enforce. Additionally, every change window can create an opportunity for "configuration drift" from a given desired configuration.

At a large financial services firm, the configuration drifts started to cause network outages. After every change, software or hardware, an army of people was employed to manually verify that the changes were not introducing any error or outage-inducing problem. However, the manual testing and verification was never an exhaustive coverage as the one offered by a mathematical model of a given network. Remediation efforts required teams of engineers performing regular audits as new errors were found. Specifically, simple things like reusing IP addresses (inserted by cut and paste errors) were causing high CPU and increasing troubleshooting time.

Using Forward Networks' ability to create a mathematical model of the network, the configuration and behavior across all devices are audited continuously and automatically. In particular, Forward Verify helps automate the elimination of most common network configuration errors by proactively unveiling silent network configuration errors (for instance, MTU mismatches, VLAN inconsistencies, forwarding loops, etc.) that may lead to expensive outages over time.



With Forward Verify, engineers receive a consolidated report enumerating the errors across the network so they can focus their remediation efforts. As new devices are added to the network, they are added to the Forward model and unit checked for correctness. Finding a single error, which used to take several hours of audit across text-based configuration files, is now immediately reported and is addressed in minutes. An additional report showing the implemented fix is also created for accountability purposes. Configuration errors are eliminated before causing an outage and remediation teams are able to focus their efforts on other initiatives.

INDUSTRY

Financial Services

NETWORK ARCHITECTURE

+ Several data centers located in geographically separated areas connected by a managed core network
+ Mission-critical applications running across data center infrastructure
+ Large virtualization presence on server side
+ Limited network virtualization
+ Mixed leaf-spine or three-tier architecture based for each data center
+ Combination virtual and physical load balancers
+ 10+ network equipment vendors
+ 20+ models of hardware
+ 100+ unique hardware and software combinations