NETWORK SPI
SCOPE, PLAN, IMPLEMENT

Network Services Validation & Modeling

Network SPI Pro Services provides complete network assurance, improving security, reliability, and performance beyond standard audits.

Multi-Vendor Support: Enterprise networks often use equipment from multiple vendors. Network SPI supports industry-standard network device configurations, making it versatile and applicable in diverse environments.

Risk Identification and Mitigation: Enterprise networks often have complex and critical infrastructures. Network SPI can detect security vulnerabilities and compliance violations in configurations, allowing network administrators to address them before attackers exploit them.

Simulation and What-If Analysis: Network SPI can enable network administrators to simulate network changes or model "what-if" scenarios without making actual modifications to the live network. This feature is valuable for testing changes, such as adding new services, locations, bandwidth, or broadband services, to assess their impact before implementation.

Fault and Root Cause Analysis: When an issue occurs in the network, Network SPI can identify the fault and provide a root cause, along with configuration recommendations and/or standardizations by analyzing configurations of the impacted segment. This can increase meantime between faults and overall availability for that network segment.

Network Validation and Verification: Network SPI can analyze the configurations of all devices (optical, switches, routers, firewalls, etc.) in the Enterprise's network and identify potential issues or misconfigurations. This helps ensure the network is set up correctly and adheres to industry best practices, reducing the risk of downtime or security breaches.

Documentation and Change Management: After validation of a network or network segment, Network SPI can create detailed documentation of the network's current state and provide configuration recommendations with appropriate MOPs (method of procedures), along with a change schedule and policy based on ITIL v4 standards. This aids in the change management process, allowing your team to focus on execution. Deliverables include configuration recommendations, standards-based MOPs, and change schedule with management procedures based on the specific network.

NETBEEZ

Batfish Enterprise

GNS3®

Network Analysis, Validation & Modeling

Analysis

Configuration Standards
Configuration standards are critical for operations; clean and uniform configurations can reduce operational complexity and cost.

We analyze:
- Base configurations to ensure they follow the “Golden Config” Model. All like network elements should have identical base configs and follow like Naming/Labeling conventions.
- Interface and Services to ensure they follow clear uniform standards that are universal to the customer.
- Security policies and services to ensure uniform standards are followed that are appropriate for that segment.

Layer 2
Layer 2 domains at any scale can cause issues if not maintained properly. In some instances, the L2 domain has grown to an unsupportable scale or unknowingly overlaps with other segments, resulting in network instability under failure scenarios or even normal operations.

We analyze:
- FDB tables to ensure L2 traffic is traversing the network as expected.
- Interface and VLAN configuration to identify any potential overlap or loop scenarios.

Layer 3
Layer 3 is a great way to segment a network but brings high complexity to a network.

We analyze:
- L3 Route Tables
- L3 Route Policies
- Assigned Network Space

Validation
Once the configuration analysis of the network or segment is completed, we will build an initial topology with our modeling tools with a report of the initial findings for customer validation.

- Validate Configuration Standards.
- Validate Transit interfaces to ensure all potential paths are identified.
- Validate Interface statistics for throughput and errors that might hinder network performance.

Modeling
Once validation has been completed, all data compiled will be ingested into our modeling software to run simulations. These simulations are generally based off questions posed by the customer to provide feedback on specific scenarios.

Below are a few examples. The simulations are not limited to just failure events—changes in L2, L3, and routes are also common simulations.

- Simulate existing infrastructure under normal operation.
- Simulate existing infrastructure under single failures at various points in the network.
- Simulate existing infrastructure under multiple failures at various points in the network.
- Simulate bandwidth increases or decreases at various points in the network.
- Simulate alternative routing protocols supporting existing services.