

## Pari Networks Value-Add for refreshing Networks

1. Why do companies refresh networks?
  - a. There are network devices which are past their life (end of support)
  - b. There are devices that just entered in to their fag end of service (end of life announced)
  - c. Security risks (as these devices may or may not be up to date on the security advisory list, and in most parts vendors does not provide patches to security advisories for end of life products)
  - d. To deploy new applications in the network infrastructure includes voice, video, etc. (existing infrastructure may not be in a position to support these applications)
  - e. Any specific compliance requirements (where a regulatory compliance or corporate compliance mandates to have certain advanced security and other services in the devices)
  - f. Migrating the networks from one location to other or from one vendor to other
2. What are all refreshable?
  - a. Network Devices (Routers, Switches, Firewalls, Access Points, etc.)
  - b. Line Cards/Modules that go the modular chassis
  - c. Operating System or Software that is running in the devices
3. What does Pari Solutions provide?
  - a. Accurate Auto discovery (including serial numbers) of:
    - i. Devices
    - ii. Modules
    - iii. Software
  - b. Complete network inventory including:
    - i. Device, Module & SW inventory (including memory/flash, up time, etc.)
    - ii. Detailed product life cycle information for all devices(End of Life Announced, End of Sale Date, End of Engineering Date, End of Contract Renewal Date, and End of Support Date)
    - iii. Intuitive graphs detailing how many devices are going to be in any of the above states, like end of support in any given quarter, assisting in budget processes for the customers
    - iv. Service Inventory (what services are enabled or disabled on a given device)
    - v. Device Capabilities (whether a given device is capable of a given service, and if not whether you need to change software or hardware to make it capable)
    - vi. Device Configurations (both stored and running), and configuration diff reports (who made what changes)
  - c. Security & Compliance Assessments
    - i. Perform Network Security Audits & provide mitigation/remediation

- ii. Perform Vendor Security Advisory assessments to see how many devices in the network are vulnerable to a given security advisory (PSIRT in case of Cisco)
  - iii. Perform Compliance assessments (regulatory or corporate)
  - iv. Provide compliance capability reports (find out the devices that can never be compliant for a given compliance and what needs to be done to make them compliant)
- 4. Why do I need Pari Solutions if I get the refresh data from vendor themselves?
  - a. Pari Solutions are not just to provide the refresh information, but to provide a lot more information making you an invaluable resource in your customer operations process
  - b. For providing checks and balances with vendor recommendations (as a 3<sup>rd</sup> party validation)
  - c. Looking at the modules & software refresh as well (helping your customers to control their budgets)
  - d. Providing a quarterly refresh schedule rather than one upfront cost to your customers
  - e. If you have a leasing arm, using it to provide all the refresh equipment upfront, but converting lease to a sale every quarter, thus becoming a trusted advisor to your customers
  - f. Proving Security Advisories and determining how much security risk network is facing, during the refresh process itself, and not as an after thought
  - g. Providing Security/Compliance audits & mitigation actions
  - h. Providing service assessment to determine if there are any non-approved services enabled on any device, as well what services to be touched for pushing new applications to the network fabric

# Solutions for Systems Integrators

Pari Networks has developed the key solution for bringing together network operations, compliance and security risk management. Pari is the first centralized view of elements assessed against both internal and external best practices and/or compliance requirements including EoL/EoS while enhancing capabilities for creating and maintaining a secure best practices or compliance posture with Pari's out-of-the-box configuration oversight and one-step centralized viewing, reporting and mitigation solution.

## How an integrator and network administrator can utilize Pari's capabilities:

- Conduct consistently scheduled security & policy assessments, using profile functionality for automatic reporting and mitigation actions for any configuration/policy changes. Know which devices can be brought in to compliance posture, and fully mitigate.
- Enforce compliance monitoring, violation reporting and resolution in an automated manner, easily customized to meet your customers' unique IT environment. Match each element's code revision to current compliance statute.
- Provide effective security policy enforcement coupled with proactive management and monitoring.
- Provide automated network configuration deployment with easy to use and flexible configuration applications.

## Reporting Capabilities of the Paritra Solution:

- Network devices can be discovered and inventoried based on many different discovery mechanisms:
  - Known Devices
  - Protocol based discovery (Cisco Discovery Protocol, OSPF, Routing Tables, ARP, etc.)
  - IP Address Scanning (Ping Sweep)
- Once Discovered data can be collected from many different formats:
  - Telnet
  - SSH
  - HTTP
  - HTTPS
  - SNMP
- Once the discovery and inventory functions are complete data can be reported in many different ways
- Each report can be exported in to many different formats (MS Word, PDF, CSV, Excel, etc.), and can be easily searched, sorted or customized to get to the correct information that is needed
- Each report also comes up with a set of graphing options and every graph can be exported into a JPEG or PNG formats.
- Reports are divided in to Device Reports (device inventory/security/routing/switching, etc.), Service Reports (service & capability reports), Compliance reports (compliance status & compliance capability), Audit Reports (EoX & PSIRT), and Log reports.