NetMRI™ Policy Management Technology Module

A Multi-Vendor Configuration Analysis Engine

Dynamic Module Monitors Configurations, Automates Changes, and Drives Policy

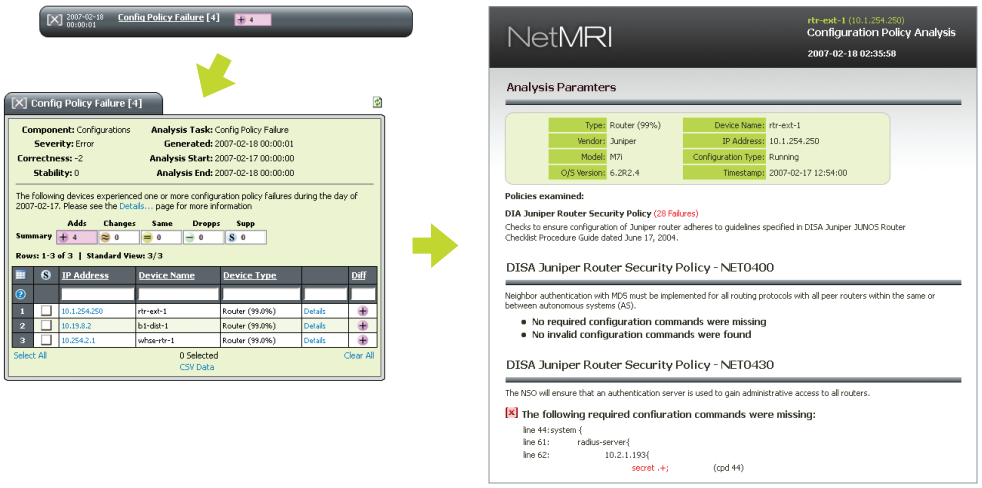
Managing the configurations on your network is a vital, multi-faceted responsibility that affects all aspects of your organization—and has become a base requirement. You need to collect and archive configurations continually, both to safeguard recovery and to enforce changes whenever necessary. Additionally, recent regulatory requirements have mandated adherence to design and compliance standards, making the detection of unauthorized changes and the ability to recover device configurations two mission-critical goals for all public companies and government entities.

The NetMRI Policy Management Module empowers you to catalog configurations, monitor changes, enforce policies and standards, and execute changes.

This all-encompassing approach gives different groups in your organization the tools to manage change and ensure the stability and quality of your network.

Configuration Archiving and Comparison

Maintaining copies of both current and previous configurations is a fundamental requirement for any organization. This archiving function is critical to network restoration in the event of equipment failure or disaster. Also, organizations need the ability to revert to earlier configurations when a change does not work as planned or when network requirements change. The ability to compare configurations—both iterations on the same device, as well as configurations on different devices—is also a vital tool for troubleshooting and optimizing network performance. NetMRI meets these needs with automatic archiving and ad hoc comparison capabilities.



NetMRI continuously detects out-of-policy configuration settings across all network elements.

Features and Benefits

- Proactively detects configuration changes and deviations from policy—from a single location
- Automatically archives network device configurations for multiple vendors
- Compares running configurations against previous configurations to identify changes
- Creates an issue and sends report for any configuration that has not been saved
- Helps ensure that all configurations meet regulatory and corporate compliance requirements
- Automates configuration changes across devices from multiple vendors
- Allows you to supplement the NetMRI expert rules engine with customized, organizational-specific rules

Netcordia™
Simply a better way to manage

NetMRI automatically archives device configurations on an hourly basis, and automatically stores a copy of the new configuration whenever differences are detected. With the aid of an intuitive visual interface that automatically highlights additions, deletions, and changes, a NetMRI user can view configurations at any time, and is able to select different configurations at will for easy diagnostic comparison.

Configuration Policy Issues

The NetMRI Policy Management Module enables NetMRI to notify engineers about configuration issues. NetMRI detects configuration changes, and because it also collects configurations continuously, engineers are able to see the changes readily for remediation. This alert function acts as a watchdog over the network, ensuring unauthorized changes are detected almost instantaneously.

NetMRI also creates an issue and sends an alert when it detects that a running configuration has not been saved. This common mistake can be devastating, should the device unexpectedly lose power or require a reload. Any changes since the last saved configuration would be lost, and the effect on the network could potentially be catastrophic.

Compliance

Regulatory requirements—such as Sarbanes-Oxley and HIPAA—have upped the ante on network compliance, necessitating that organizations archive configurations, detect unauthorized changes, and ensure that their networks match design standards.

NetMRI uses the capabilities of the NetMRI Policy Management Module to help you meet these compliance objectives. First, the Configuration Archive feature addresses the need to store configurations and to notify you when changes occur. Second, your engineers can use NetMRI to set up Configuration Policy Definitions (CPDs) to match against running configurations in order to ensure that design standards are maintained on the network. This feature generates an issue when configurations do not meet the defined policies.

Policy Enforcement Technology

NetMRI's policy enforcement technology lets you quickly develop scripts to interact with a single device or a group of devices. The intuitive design of this feature allows network engineers to focus specifically on the actions desired and easily write scripts to push configurations out to devices. Scripts can either be executed ad hoc or scheduled through the batch processing facility. This feature enables engineers to manage the development and execution of all scripting in a single managed environment.

Using the policy enforcement capabilities of NetMRI, network managers can make powerful changes across multiple platforms and multiple vendors, including Cisco, Juniper, Foundry, Nortel, HP, and Alcatel. NetMRI executes Command Line Interface (CLI) commands, scans the output for the desired data variables, computes "if-then" logic based on those variables, and then takes further actions based upon one or more processing triggers. NetMRI makes all of this possible without significant programming. Network engineers only have to enter the desired CLI commands and define a few directives to control all script processing—NetMRI automatically handles the rest.

Expert best practices have been "pre-built" into NetMRI. With policy enforcement capabilities, you and your network engineers can now create your own custom best practices—your own site-specific, tailored rules. Examples include updating passwords across hundreds of devices, changing dial plans in multiple voice gateways around the world, or guaranteeing consistent logging configurations across the entire infrastructure. This combination of industry and customized best practices then runs automatically, providing audit and exception reporting for both the standard best practices and the ones you have created.

For more information on Netcordia and our full range of automated network management solutions, please call **410-266-6161** or visit **netcordia.com**

Netcordia™
Simply a better way to manage