Automating Network Device Configuration and Compliance Enforcement

Mohit Bajpai

USA

Abstract

Network infrastructures in large organizations are often complex, consisting of a vast array of devices from multiple vendors. Ensuring consistent configuration and compliance across this heterogeneous environment is a significant challenge. This paper explores the use of automation to streamline network device configuration management and enforce compliance with organizational policies. It outlines an architectural approach that leverages a domain-level data model to abstract network design from device-specific configurations, enabling centralized management and automated deployment. The paper also discusses the integration of performance monitoring metrics and proactive troubleshooting capabilities to enhance network operations. (Keith et al., 2010) (Dallaglio et al., 2017)

Keywords: Network automation, configuration management, compliance, performance monitoring, troubleshooting

Introduction

Managing network configurations and ensuring compliance across a large, heterogeneous infrastructure is a significant challenge for network administrators. Traditionally, network device configurations have been manually configured, leading to inconsistencies, errors, and difficulty in maintaining compliance with organizational policies. The problem is compounded by the use of varied, complex, and constantly evolving management interfaces across network devices from different vendors.

To address these challenges, network automation has emerged as a critical capability, enabling consistent and repeatable configuration management, as well as the enforcement of security and compliance requirements. (Bellovin & Bush, 2009) This paper presents a comprehensive approach to leveraging automation to ensure consistency in network device configurations and compliance, including the integration of performance monitoring metrics and automated troubleshooting capabilities.

Architecture Considerations

The proposed architecture for automating network device configuration and compliance leverages a domain-level data model to abstract network design from device-specific configurations (Keith et al., 2010). This approach allows the management plane to operate independently of the data plane, reducing the operational complexity and enabling high-level policy enforcement in a structured manner. The key components of the architecture include:

- A centralized network configuration management system that provides a unified interface for defining and managing network policies, device configurations, and compliance rules.
- An automated deployment engine that translates the high-level network policies into device-specific configurations and pushes them to the corresponding network devices.
- A compliance monitoring and enforcement module that continuously checks the live network configurations against the defined policies and triggers remediation workflows when deviations are det-

ected.

- Integration with a configuration management database and version control system to maintain a comprehensive audit trail of all network changes and provide rollback capabilities.
- Seamless integration with performance monitoring and troubleshooting tools to correlate network issues with configuration changes and automate the troubleshooting process.

Figure 1 below illustrates the key components of the proposed network automation architecture, including the centralized configuration management system, the automated deployment engine, the compliance monitoring and enforcement module, the integration with a configuration management database and version control system, and the seam-less integration with performance monitoring and troubleshooting tools.

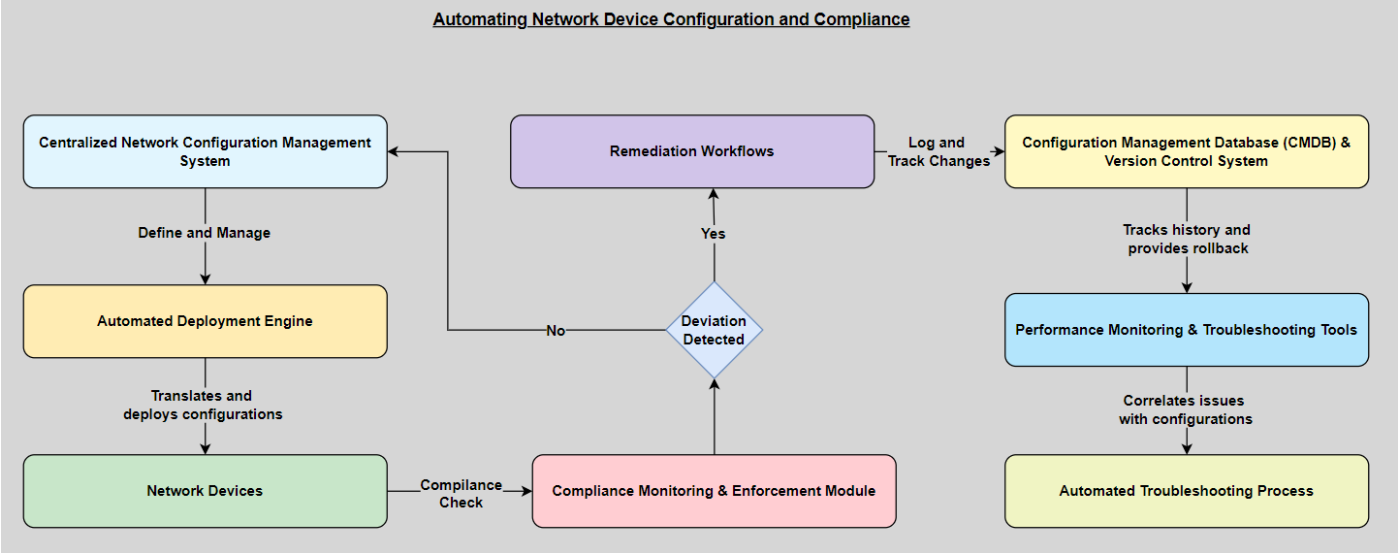

Figure 1: Automating Network Device Configuration and Compliance.

The centralized configuration management system provides a unified interface for defining and managing network policies, device configurations, and compliance rules. The automated deployment engine translates the high-level network policies into device-specific configurations and pushes them to the corresponding network devices. The compliance monitoring and enforcement module continuously checks the live network configurations against the defined policies and triggers remediation workflows when deviations are detected. The integration with a configuration management database and version control system maintains a comprehensive audit trail of all network changes and provides rollback capabilities. The seamless integration with performance monitoring and troubleshooting tools allows for the correlation of network issues with configuration changes and the automation of the troubleshooting process.

Network Device Configuration Automation

One of the core components of the proposed network automation architecture is the Network Device Configuration Automation module. This module is responsible for translating the high-level network policies defined in the centralized configuration management system into device-specific configurations and then deploying those configurations to the corresponding network devices.

The key features of the Network Device Configuration Automation module include:

- **Configuration Template Management**: The module maintains a library of configuration templates for different network device models and vendors, allowing network administrators to define network policies in a vendor-agnostic manner.
- **Dynamic Configuration Generation**: The module dynamically generates device-specific configurations by populating the configuration templates with the appropriate parameter values based on the defined

network policies.

- **Automated Configuration Deployment**: The module automates the deployment of the generated configurations to the target network devices, ensuring consistent and reliable configuration updates across the entire network infrastructure.
- **Configuration Validation**: The module performs validation checks on the deployed configurations to ensure they align with the defined network policies and compliance requirements, triggering remediation workflows if any deviations are detected.
- **Rollback Capabilities**: The module integrates with a version control system to maintain a comprehensive audit trail of all configuration changes, enabling the network administrators to quickly roll back to a known-good configuration if required.

By automating the end-to-end process of network device configuration management, the Network Device Configuration Automation module helps ensure consistency, compliance, and reliability in the network infrastructure, reducing the risk of manual errors and accelerating the deployment of network changes.

Automated Network Monitoring and Troubleshooting

Another key aspect of the proposed network automation architecture is the integration of automated network monitoring and troubleshooting capabilities.

The Automated Network Monitoring and Troubleshooting module includes the following key features:

1. **Real-time Performance Monitoring:** The module continuously collects and analyzes performance metrics from the network devices, such as bandwidth utilization, latency, and packet loss, to proactively identify potential issues.
2. **Anomaly Detection and Alerting:** The module employs machine learning-based anomaly detection algorithms to identify unusual patterns in the network performance data and generate alerts for network administrators, allowing for faster issue identification and resolution.
3. **Automated Troubleshooting Workflows:** The module integrates with network diagnostics tools and automates the execution of troubleshooting workflows, such as running diagnostic tests, collecting relevant logs, and correlating the performance data with configuration changes, to quickly identify and resolve network issues.
4. **Ticketing and Incident Management:** The module automatically generates tickets for identified network issues and tracks their resolution, providing a centralized interface for incident management and ensuring consistent problem-solving procedures.

By integrating these automated monitoring and troubleshooting capabilities, the network automation architecture enables faster issue detection, quicker problem resolution, and improved overall network reliability and uptime.

Automated Remediation Workflows

The proposed network automation architecture consists of several key components that work together to ensure consistency, compliance, and reliability in network device configurations:

1. Network Device Configuration Automation One of the core components of the proposed network automation architecture is the Network Device Configuration Automation module. This module is responsible for translating the high-level network policies defined in the centralized configuration management system into device-specific configurations and then deploying those configurations to the corresponding network devices.(Schönwälder et al., 2010)
2. Automated Network Monitoring and Troubleshooting Another key aspect of the proposed network automation architecture is the integration of automated network monitoring and troubleshooting capabilities.(Lee et al., 2014)

3. Compliance Monitoring and Enforcement: The architecture includes a robust compliance monitoring and enforcement mechanism that continuously monitors the network configurations against the organization's security and operational policies. When a compliance violation is detected, the system automatically triggers remediation workflows to bring the non-compliant device back into a compliant state, ensuring the overall security and operational integrity of the network.(Miller, 2014)
4. Configuration Drift Detection: The architecture incorporates advanced configuration drift detection capabilities to identify and address any divergence from the desired network state. By continuously monitoring the network configurations and comparing them against the approved baseline, the system can detect and remediate any configuration drift, maintaining the consistency and reliability of the network infrastructure.(Sun et al., 2014)

By combining these interconnected components, the proposed network automation architecture provides a comprehensive solution for ensuring consistency, compliance, and reliability in the network infrastructure, ultimately enhancing the overall operational efficiency and security of the organization's network.

Automated Configuration Deployment

The Network Device Configuration Automation module automates the deployment of network device configurations, ensuring consistent and compliant configurations across the infrastructure. This module integrates with the Configuration Management Database to retrieve the necessary configuration data and then uses a templating engine to generate device-specific configurations based on defined policies and best practices. The automated deployment process includes the following key features:

- Consistent Configuration: The module ensures that all network devices are configured according to the predefined policies, promoting uniformity and reducing the risk of manual errors.
- Compliance Validation: The module verifies the generated configurations against the defined compliance requirements, triggering remediation workflows if any deviations are detected.
- Rollback Capabilities: The module integrates with a version control system to maintain a comprehensive audit trail of all configuration changes, enabling the network administrators to quickly roll back to a known-good configuration if required.

  By automating the end-to-end process of network device configuration management, the Network Device Configuration Automation module helps ensure consistency, compliance, and reliability in the network infrastructure, reducing the risk of manual errors and accelerating the deployment of network changes.(Schönwälder et al., 2010)

Network Device Troubleshooting Automation

The network automation architecture includes automated troubleshooting workflows that integrate with network diagnostic tools to quickly identify and resolve network issues. These workflows automate the execution of troubleshooting steps, such as running diagnostic tests, collecting relevant logs, and correlating performance data with configuration changes. This enables faster issue detection and quicker problem resolution, improving overall network reliability and uptime.

The key components of the automated troubleshooting process include:

- Automated Diagnostics: The system automatically runs diagnostic tests on network devices to gather performance data and identify potential issues.
- Log Collection and Correlation: Relevant logs are automatically collected from network devices and correlated with configuration changes and performance metrics to pinpoint the root cause of problems.
- Automated Remediation: Based on the diagnostic findings, the system can automatically execute remediation steps, such as configuration updates or device reboots, to resolve the identified issues.
- Incident Management: The system automatically generates tickets for network issues and tracks their res-

olution, ensuring consistent problem-solving procedures and a centralized interface for incident management.

By integrating these automated troubleshooting capabilities, the network automation architecture significantly reduces the time and effort required to detect, diagnose, and resolve network problems, leading to improved network reliability and uptime.(Jammal et al., 2014)

Conclusion and Future Outlook

The proposed network automation architecture represents a comprehensive solution for ensuring consistency, compliance, and reliability in network device configurations. By integrating key components such as network device configuration automation, automated monitoring and troubleshooting, compliance monitoring and enforcement, and configuration drift detection, this architecture provides a holistic approach to managing the network infrastructure.

The automated configuration deployment process ensures that all network devices are configured according to predefined policies, promoting uniformity and reducing the risk of manual errors. The integration of compliance validation and rollback capabilities further enhances the reliability and operational integrity of the network.(Yemini et al., 2000)

The automated troubleshooting workflows, with their ability to quickly diagnose and resolve network issues, significantly improve the overall network uptime and reliability. The incident management capabilities ensure consistent problem-solving procedures and centralized visibility into the network's health.(Toy, 2014)

Moving forward, the network automation architecture can be further enhanced by incorporating predictive analytics and machine learning techniques to proactively identify potential issues and preemptively address them. Additionally, integrating the architecture with cloud-based network management platforms can provide increased visibility, scalability, and flexibility in managing the network infrastructure.

As organizations continue to navigate the complexities of modern network environments, the adoption of such a comprehensive network automation architecture will be crucial in achieving operational excellence, ensuring regulatory compliance, and maintaining a reliable and secure network infrastructure.

References:

1. Bellovin, S M., & Bush, R. (2009, April 1). Configuration management and security. Institute of Electrical and Electronics Engineers, 27(3), 268-274. https://doi.org/10.1109/jsac.2009.090403
2. Dallaglio, M., Sambo, N., Cugini, F., & Castoldi, P. (2017, February 23). Control and Management of Transponders With NETCONF and YANG. , 9(3), B43-B43. https://doi.org/10.1364/jocn.9.000b43
3. Jammal, M., Singh, T., Shami, A., Asal, R., & Li, Y. (2014, July 25). Software defined networking: State of the art and research challenges. Elsevier BV, 72, 74-98. https://doi.org/10.1016/j.comnet.2014.07.004
4. Keith, A W., Wang, W., Kurt, M P., Daniel, P G., & Dimarogonas, J. (2010, October 1). A domain-level data model for automating network configuration. , 1337-1342. https://doi.org/10.1109/milcom.2010.5680134
5. Lee, S., Levanti, K., & Kim, H S. (2014, March 24). Network monitoring: Present and future. Elsevier BV, 65, 84-98. https://doi.org/10.1016/j.comnet.2014.03.007
6. Miller, G P. (2014, January 1). The Compliance Function: An Overview. RELX Group (Netherlands). https://doi.org/10.2139/ssrn.2527621
7. Schönwälder, J., Björklund, M., & Shafer, P. (2010, September 1). Network configuration management using NETCONF and YANG. Institute of Electrical and Electronics Engineers, 48(9), 166-173. https://doi.org/10.1109/mcom.2010.5560601
8. Sun, P., Mahajan, R., Rexford, J., Yuan, L., Zhang, M., & Arefin, A. (2014, August 12). A network-

state management service. https://doi.org/10.1145/2619239.2626298
9. Toy, M. (2014, January 1). Self-managed Networks with Fault Management Hierarchy. Elsevier BV, 36, 373-380. https://doi.org/10.1016/j.procs.2014.09.008
10. Yemini, Y., Konstantinou, A V., & Florissi, D. (2000, May 1). NESTOR: an architecture for network self-management and organization. Institute of Electrical and Electronics Engineers, 18(5), 758-766. https://doi.org/10.1109/49.842991