AUTOMATED POLICY COMPLIANCE AND CHANGE DETECTION MANAGED SERVICE IN DATA NETWORKS

Saeed M. Agbariah

Department of Electrical and Computer Engineering,
George Mason University, Virginia, USA
sagbaria@gmu.edu

ABSTRACT

As networks continue to grow in size, speed and complexity, as well as in the diversification of their services, they require many ad-hoc configuration changes. Such changes may lead to potential configuration errors, policy violations, inefficiencies, and vulnerable states. The current Network Management landscape is in a dire need for an automated process to prioritize and manage risk, audit configurations against internal policies or external best practices, and provide centralize reporting for monitoring and regulatory purposes in real time. This paper defines a framework for automated configuration process with a policy compliance and change detection system, which performs automatic and intelligent network configuration audits by using pre-defined configuration templates and library of rules that encompass industry standards for various routing and security related guidelines.System administrators and change initiators will have a real time feedback if any of their configuration changes violate any of the policies set for any given device.

KEYWORDS

Compliance and Real-time Change Detection, Policy Management

1. INTRODUCTION

Current networks are evolving rapidly, this rapid growth of networks and services has introduced new complex large networks that are made up of heterogeneous equipment from multiple vendors, and as these networks continue to grow their systems and services, the tasks of configuration management for IP network devices are becoming more and more difficult. Not only are these heterogeneous equipment's supporting different techniques in conjunction with their own configuration methods; it is often a common practice to find the same device deployed in the network in different roles, each with its unique configuration requirements and policies governing the device within the organization, or even policies that differ from one business unit to the other within the same organization. All these complications increase the chances of faulty configurations, and to the difficulty of anticipating how changing one configuration parameter may bring a complex chain of changes to the network. As a result network administrators dealing with the existence of a huge set of configuration parameters, and the implicit dependencies between these parameters, are confronted with the challenge of configuring these services and their network elements without committing a single mistake.

Sundarapandian et al. (Eds) : ICAITA, SAI, SEAS, CDKP, CMCA-2013
pp. 01–12, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3801

Current networks require ad-hoc changes by network administrators to continuously conduct provisioning or performance tuning. These configuration changes are costly, error prone, can result in unpredictable failures and inefficiencies, or may lead to inefficient allocation of underlying resources, turning the active device into a traffic bottleneck, or an inconsistent configuration may cause not only traffic loss, but also intermittent crashes of the network devices [1]. The study in [2] has found that 50 percent of network errors are configuration errors and 75 percent of all Time to Repair hours are due to administrator errors. Another study has revealed that 80 percent of IT budget in enterprise networks are dedicated just to maintain the current operating environments [3].

1.1 Framework for Automate Template Compliance and Change Detection System

The proposed framework for automated template compliance and change detection system, performs automatic and intelligent network configuration audits by using pre-defined configuration templates and a library of rules that encompass industry standards for various routing and security related guidelines, a system that will provide a real time alerts for any configuration changes that violates any of the policies set for any given device. The suggested architecture achieves a high level of security, compliance, and reduces complexity in network configuration without adding any functions on the managed entity.

The central idea for the proposed framework seeks to replace labor-intensive configuration management that is error prone, and often result in unpredictable failures and inefficiencies, with one that is automated, reduces errors, and inefficiencies. The framework seeks to define the following areas:

1) A common policy language to use to represent device, organizational, industry best practices and any other regulatory policies or guidelines, needed for any of our network elements; in a structured document format that can be retrieved and manipulated with ease.
2) A centralized repository where policies could be stored, allow policy changes to propagate to the subjects, and allow subjects to detect policy changes in an automated way.
3) Secure policy exchange procedure.
4) A proposed framework that permits any given device to be configured, in its current native state, without any further burdens to the network administrator , or system owner, and be able to detect whether the proposed configuration violate any of the policies set in 1.
5) A protocol to provide mechanisms for an immediate feedback to the change initiator, and to a centralized alarm system, alerting them of the conflict.

In summary the change initiator will access his device, type his/her changes and immediately know whether the changes he/she committed violated and policy set for the device. The aim is to prevent inconsistent configuration states resulting in operational failures and inefficiencies.

2. THE EVOLUTION OF NETWORK MANAGEMENT

The variety of challenges in networks meant the need to create a network management model, that could enable network administrators, designers, planners, and operators to perform strategic and tactical planning of engineering, operation, and maintenance of the network service for current and further needs at minimum cost [4], functions such as initial network planning, resource allocation, predetermined traffic routing to support load balancing, access control, authorization, and a verity of other activities.

There are few reference models that have been widely established for network management, one of them is the Fault, Configuration, Accounting, Performance, and Security model, commonly referred to as FCAPS. The FCAPS model was originally designed by International Telecommunication Union (ITU-T), and as its name indicates, it divides management functions into five categories: fault management, configuration management, accounting management, performance management, and security management. The ITU-T organization dates back to 1865 with original responsibilities of ensuring efficient and on-time production of high-quality recommendations covering all fields of telecommunications [5]. In 1996, the ITU-T created the concept of the Telecommunications Management Framework (TMN), which was an architecture intended to describe service delivery models for telecommunication service providers based on four layers: business management, service management, fault and performance management, and element and configuration management [6]. Because TMN standards are mainly business focused not managing IP networks focused, the ITU-T refined the model in 1997 to include the concept of FCAPS [7]. FCAPS, as shown in Figure 1, expanded the TMN model to focus on the five functionally different types of tasks handled by network management systems: fault management, configuration management, accounting management, performance management, and security management. Table 1 describes the main objectives of each functional area in the FCAPS model.

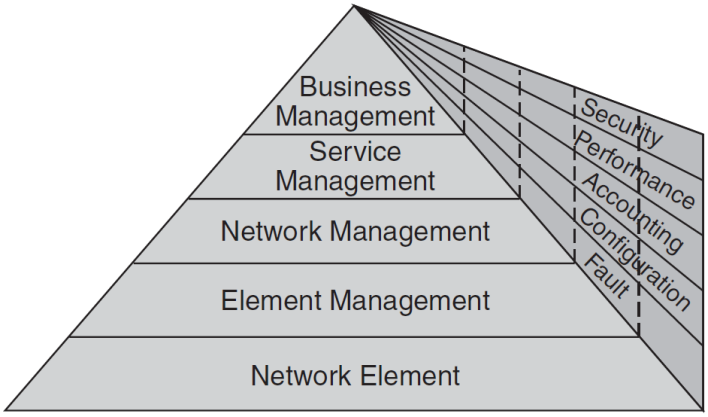

Figure 1 TMN Reference Model Refined with FCAPS[8]

Table 1 describes the main objectives of each functional area in the FCAPS model

Table 1. FCAPS Objectives

Management Functional Area (MFA)	**Management Function Set Groups**
Fault	Alarm surveillance, fault localization and correlation, testing, trouble administration, network recovery
Configuration	Network planning, engineering, and installation; service planning and negotiation; discovery; provisioning; status and control
Accounting	Usage measurement, collection, aggregation, and mediation; tariffing and pricing
Performance	Performance monitoring and control, performance analysis and trending, quality assurance
Security	Access control and policy; customer profiling; attack detection, prevention, containment, and recovery; security administration

2.1 Change Management

The FCAPS model is useful for understanding the goals and requirements of Network Management, and also helps to build a foundation for understanding the significance of Network Management to compliance efforts [8], but it does not address change, or how to handle change in an active network. Change in today's network has become inevitable, it also has become one of the most prominent sources of risk in the network, and it has a direct impact on the time, cost and quality of the services provided, to cope with change and their impact, Change Management has become an IT Service Management discipline, it is one of the most critical processes in IT management. Some of the reasons are the sheer number of changes and the difficulty of evaluating the impact of changes on the network or the services it provides in real-time [9]. The main goal of change management is to ensure that the network and/or its services risk and business impact of each change is communicated to all impacted and implicated parties, and to coordinate the implementation of approved changes in accordance with current organizational best practices [10].

Changes in the networks may arise reactively in response to problem resolving errors and adapting to changing circumstances, change can also arise due to externally imposed requirements, e.g., a new policy, or proactively from seeking imposed efficiency and effectiveness or , seeking business benefits such as reducing costs, improving services, or from new projects. However it may be, Change Management in the context of this paper is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the number and impact of any related incidents upon service. Change Management seeks to ensure standardized methods, processes, and procedures are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of change [11].

For the most part, changes are evaluated by stake holders. In most organizations a team is designated to evaluate the proposed change by trying to understand its impact on the network or the service it offers. This requires the change management team to have a good understanding of the change and its impact on the network, and to keeping track of the details of the system's past and future goals. There are four major roles involved with the change management process, each with separate and distinct responsibilities. Change initiator, the person who initially perceives the need for the change. Change Manager, leading a team to review and accept completed change request. Change Advisory Board that exists to support the authorization of changes and to assist change management in the assessment and prioritization of changes. Change implementation team (operations), responsible for carrying out the actual change and reporting results.

Many organizations use a simple matrix like the one shown in Figure 2 to categorize risk [10]. The "Probability axis" denotes the probability of each identified risk. For this, each risk is listed to the smallest detail possible and the probability of its occurrence is predicted. The "Impact Axis", assigns a percentage of impact, in the event that the risk does occur [11]. As results the category of changes that has low impact in the event of failure and low probability of failure becomes a candidate for a streamlined approval path [10].

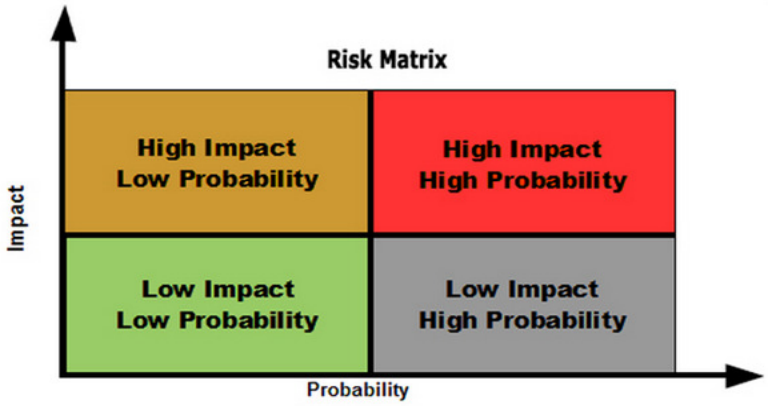

Figure 2 Risk Matrix[26]

In a recent survey conducted by Author and Information Technology Service Management expert, Harris Kern, he reports that of 40 corporate IT infrastructure managers a surprising 60% admitted that their processes to handle change are not effective in communicating and coordinating changes occurring within their production environment. Table 2 lists the key findings of the study [12].

Table 2. Change Management Study Surprising Results

Not all changes are logged 95%
Changes not thoroughly tested 90%
Lack of process enforcement 85%
Poor change communication and dissemination 65%
Lack of centralized process ownership 60%
Lack of change approval policy 50%
Frequent change notification after the fact 40% [13]

The above statistics are not hard to image, particularly for IT technicians, for whom change is a constant, almost daily occurrence, whether it is for business requirement, or for emergency changes, in response to an incident or problem requiring immediate action to restore service or prevent service disruption, or to an expedited change that must be implemented in the shortest possible time for business or technical reasons. Unfortunately, Change Management often fails to handled changes quickly in a uniform way and have the lowest possible impact on the networks and its services. However; all changes have a disruptive potential for the business, and controlling change through an agreed change management process is critical. Change management can even be more effective in reducing service disruptions when coupled with the central thesis of this paper, if change is communicated immediately to the stake holders via notification system, and violations to any policy is immediately reported to the change initiator we can both assess and control the impact of our change.

2.2 Policy-Based Network Management

As already noted the considerable growth of computer networks has produced a significant scalability and efficiency limitations to the traditional management techniques, the tendency to use diverse management and Operational Support Systems (OSS) that are not tightly integrated together, has encouraged the use of “stovepipe” applications, which are applications that maintain their own definition of data, that cannot be shared with other stovepipe applications [14]. This

means that management is often fragmented and intensely human-driven. The need to manage large networks and services efficiently and with speed has given rise to the idea of Policy-Based Network Management (PBNM).

The concept of using Policy-Based Network Management (PBNM) to reduce the complexity of the management task, has been being researched in the Policy Framework Working Group, the Resource Allocation Protocol Working Group, the IP Security Policy Working Group of IETF(Internet Engineering Task Force), and DMTF(Distributed Management Task Force) [15]. The PBNM concept comprises of policies which can be processed by automated systems. The resulting policies are rules governing the choices in behavior of set of network elements, and network conditions, which trigger the policy executions [16]. Therefore, policy-based network management (PBNM) is a condition-action-response mechanism which provides automated responses to changing network or operational conditions based on pre-defined policies [17].

In essence, the policy-based networking framework allows network operators to express their business goals as a set of rules, or policies, which are then enforced throughout the network. The architecture allows such rules to be defined centrally but enforced in a distributed fashion. In addition, the goal of policy-based networking systems to allow for the automation of manual tasks performed by network operators [18][19].

For networks consisting of various network elements of different vendors and all the systems that provide for the one converged network, Policy-Based Network Management (PBNM) is a priority in order to solve this management dilemma [20]. In particular Policy-based management provides a way to allocate network resources, primarily network bandwidth, QoS, and security, according to defined business policies. The success of management depends on the specification of unified and scalable administered policies. These policies must then map to the configuration of the multiple heterogeneous system, devices, applications and networks, for the purpose of policy enforcement [21]. However; the main challenge facing the deployment of PBNM systems is the variety of policy representation forms at different levels of the hierarchy. High level business policies may be defined and stored in a database system then various applications may retrieve and convert the data to different forms for processing. These conversion procedures add complexity to the internal structure of PBNM systems, leading to efficiency and interoperability concerns [22].

2.3 Configuration Auditing and Policy Compliance

The preceding sections illustrated how the current network management systems fails network providers to face the challenge of running their network without service disruption in the presence of constant network change. Configuration auditing aims to verify that the configuration of any network element comply with the stated policy of the device, and that the information about the network is current, without this function, a network administrators or stakeholders would have a very hard time understanding what is going on in a network and why it is going on. The importance of this process is that it could lead to isolating network troubles due to discrepancy between what is currently configured and what should or should not have been configured on the managed entity. Obviously, manual auditing of individual device configuration for networks with a few devices is an option; however; for a large network such option simply does not scale. While, this paper aims to present an automated way for administrators to identify discrepancies, or misconfiguration and hopefully avoid potential catastrophic service disruptions and other adverse fallouts, we will discuss the current tools used by large service providers [23].

In addition to the tools discussed in this paper there are many products available today with capabilities to integrate dynamic audits of network configuration changes with service

performance and infrastructure optimization, as well as compliance, security and other initiatives. However, they lack the ability to provide audit in real-time.

What the industry needs is an interactive system, with real-time reporting; why wait hours or even minutes to discover than a change made on a network element has violated a policy and potentially could be service impacting, having such system could reduce hours of troubleshooting, and save companies from expensive service interruptions. The aim of this paper is to describe the framework and all the pieces that are required to develop such a system.

3. PROPOSED RESEARCH FOR A COMPREHENSIVE CHANGE MANAGEMENT FRAMEWORK

The ramifications of one small change to network devices whether the change is desired or not can be catastrophic; however, for large networks constant change is simply a fact of life. Automated policy compliance and change Detection system can reduce these risks significantly.

I will present a system that will ensure device configurations remain compliant with internal and regulatory compliance policies. From a high level point of view, the protocol will operate as follows: once activated on a given device, it will check whether the current configuration state violates any of the rules set in the policy, for performance considerations, the policy will be stored locally as the first preference and to a centralized location as second option, in case of any inconsistencies or violations an alarm is generated describing the findings, if none found the system enter monitoring state. In monitoring state the protocol will check if any of the new entered configurations violate the policy and if so a report/alarm is generated; otherwise continue monitoring. Figure 2, illustrates the concept.

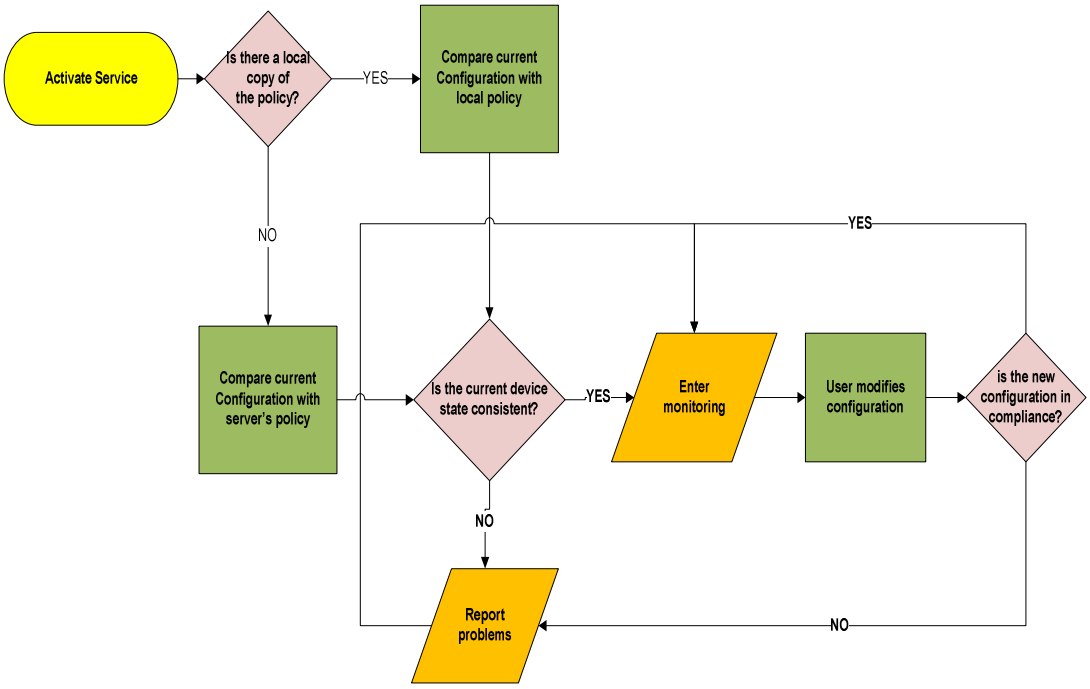

Figure 2 Process Flow

To keep the local policy and the centralized copy in synchronization, I will define a process, in which the administrator has the option to manually push changes to all devices, from the client side I will define a process in which a device will seek to verify every given interval whether it has the most current version of the policy, if not the client will be able to retrieve the latest copy and store it locally. This process will ensure the ease of manipulating and maintaining policies, only one copy per device type/function needs to be maintained. Figure 3, illustrates the push process, and Figure 4 illustrates the client request process.

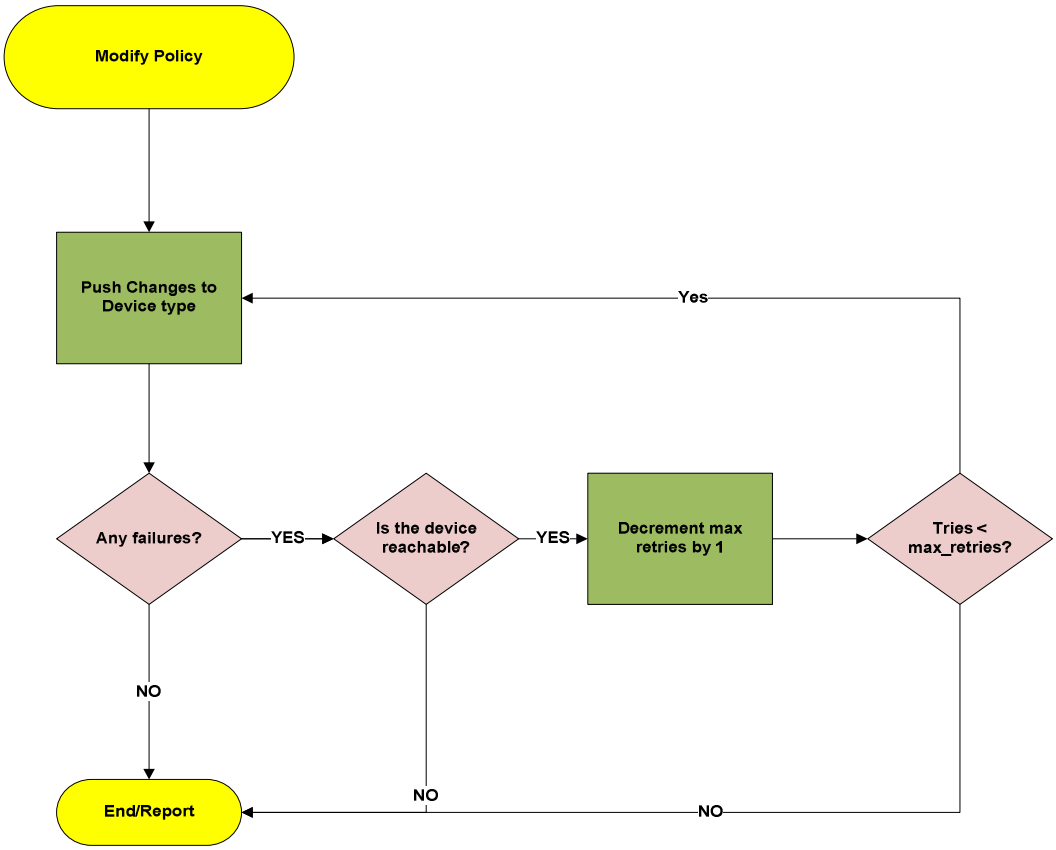

Figure 3. Server Push Process

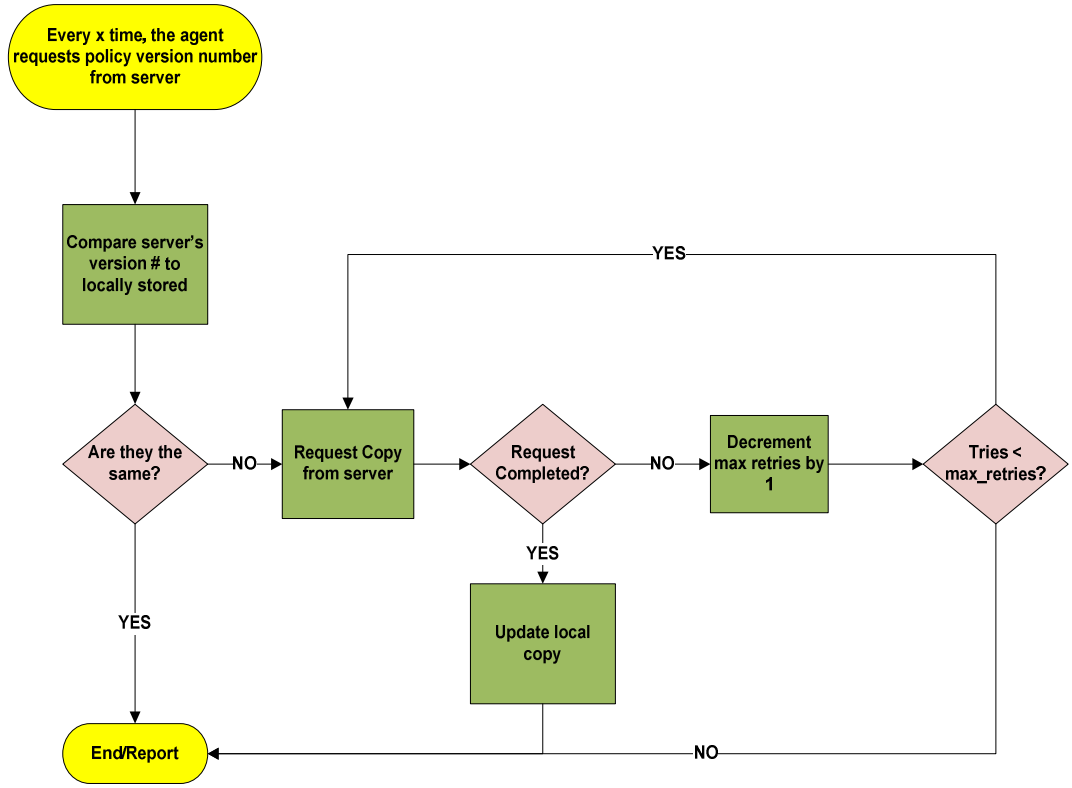

Figure 4. Client Request Process

3.1 The Need for Common Policy Language

One of the core requirements for the proposed Automated Policy Compliance and Change Detection framework is to have a common language for expressing device and organizational policies; a common policy language will ease the enforcement of such policies to all components of the network. Furthermore, using a common language brings numerous practical advantages, such as lower implementation overhead, as well as the possibility to user the same or at least similar tools to maintain the policies.

Extensible Markup Language (XML) has become the lingua franca of interchange, providing a flexible but fully specified encoding mechanism for hierarchical.The flexibility of XML has led to its widespread use for exchanging data in a multitude of forms. In its 54th birds of a feathers (BoF) meeting, the IETF was very interested in discussing XML as base for configuration management. In this informal session the participant discussed the requirements for a network configuration management, and how the existing XML technologies, could be used to meet those requirements. As a result the Network Configuration (netconf) Working Group [24] was formed in May 2003 and produced Network Configuration Protocol (NETCONF) [25].

XML was chosen due to the ease with which its syntax and semantics can be extended to accommodate the unique requirements of many network elements, and because of the widespread support that it enjoys from all the main platform and vendors. Because of its flexibility but fully specified encoding mechanism for hierarchical content [26], XML can be used to hold network management data, thus making it vendor and platform independent. In addition, XML standards in network management allows for SNMP-to-XML , and XML-to-SNMP data mapping. Furthermore; conversion of XML documents into readable formats can be

accomplished using the XML Stylesheet Language Transformation (XSLT), thus facilitating the ability to recast data in differing lights and convert it to and from common formats [27].

In future papers I will show how XML can be play role as the common policy language in the proposed framework.

3.2 Keeping the Master Policy in SYNC with the Agents

In this section we need to address two issues: first, for systems being added to the Automated Policy Compliance and Change Detection system, we need to define a method to push the master policy to the new element, this could be a newly provisioned system, or a system that for any reason has lost his contact with the master server. The second issue is the issue of synchronization, synchronization needs occur when a record is changed in the master policy, here I will define the processes needed to establish consistency among the source and the targets (network elements), and the continuous harmonization of the data over time.

3.3 Securing the Policy Propagation and Synchronization Process

Our system may be vulnerable to a variety of malicious attacks. For instance the system may be a subject to wiretapping attacks, where another system may masquerade itself as our primary server. These attacks cause transmission of fictitious policy exchange, modification or replay of valid messages, or suppression of valid messages. How do we know that the policy updates from the server to one of the network elements really came from a trusted source? One option is to allow for client to server authentication to occur whenever updates are exchanged. This authentication ensures that a client receives reliable policy information from a trusted source. Without neighbor authentication, unauthorized or deliberately malicious policy updates could compromise the enforcement of our policies.

In this paper, I acknowledge the paramount importance of security, and in future publication I will define the mechanisms to prevent fraudulent policy updates by protecting the update process.

3.4 Device Policy Compliance and Change Detection

Configuration changes may lead to inconsistent configuration states resulting in operational failures and inefficiencies. In the section of the paper I aim to define the portion of the framework whose primary objective to monitor the user activity in configuration mode, intercept the commands entered by the change originator, compare them to the predefined policies for the device, and then alert the user of any inconsistencies.

3.5 Policy Violation and Inconsistent State Reporting

It is important for the compliance and change detection portion of the system to provide sufficient information about differences between the active configuration, or the newly entered configurations to those specified in our policy for that device, such that the operators who are configuration experts can quickly grasp the context of the differences, and for the casual alarm monitor to have enough hints about the change to be able to correlate network events. We will explore using XML (Extensible Markup Language) which is supported by many modern routers and which offer the key benefit of having a well-structured syntax, and the ability to converts XML data to SNMP data.

4. CONCLUSION AND FUTURE WORK

In this paper we descried the challenges facing network operators in maintaining and detecting changes in network devices configuration that deviate from the standards set by the stake holder for such device. Changes may lead to potential configuration errors, policy violations, inefficiencies, and vulnerable states, and while, manual and labor intensive network auditing or more recently products using dedicated configuration compliance scanning appliances for verifying individual system configuration, can lead to the discovery of configuration errors, and policy violations, however; we believe the framework describe here, is capable of providing real time auditing and insure consistent configuration state, that can guarantee compliance and reduce outage minutes.

In future papers I'll describe in details the building blocks of the framework and devote time to describe the language needed to build a common template language.

REFERENCES

[1] Elbadawi, K.; Yu, J., "Improving Network Services Configuration Management" Computer Communications and Networks (ICCCN), pp. 1-6, 2011.
[2] D. Opeenheimer, A. Ganapathi, and A. Petterson, "Why do internet services fail and what can be done about it?" in USITS'03: Proceedings of the 4th USENIX Symposium on Internet Technologies and Systems, Seattle, WA, USA, Mar. 2003.
[3] Z. Kerravala, "As the value of enterprise networks escalates, so does the need for configuration management," The Yankee Group, Jan. 2004.
[4] Subramanian M., Gonsalves T., Usha N. (2010). Network Management: Principles and Practice. Pearson Education India. pp. 63-64
[5] Shields, G., (2010). The Shortcut Guide to Network Management for the Mid-Market.Realtime publishers. pp. 2
[6] Shields, G., (2010). The Shortcut Guide to Network Management for the Mid-Market.Realtime publishers. pp. 3-5
[7] Claise, B., Wolter R. (2007). Network Management: Accounting and Performance Strategies. Cisco Press. pp. 120-122
[8] Ding J. (2010). Advances in network management.Auerbach Publications. pp. 90-95
[9] Reboucas, R. ; Sauve, J. ; Moura, A. ; Bartolini, C. ; Trastour, D., "A decision support tool to optimize scheduling of IT changes" IFIP/IEEE International Symposium on network management, pp.343-352, May, 2007
[10] Change Management: Best Practices [Online], Available: http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-458050.html
[11] Risks and Dangers of Change Management [online]. Available: http://www.buzzle.com/articles/risks-and-dangers-of-change-management.html
[12] *Harris K. (2000). IT Organization; Building A Worldclass Infrastructure, Prentice Hall, pp. 110-112*
[13] "Change Control vs. Change Management: Moving Beyond IT" [online]. Available: http://www.itsmwatch.com/itil/article.php/11700_3367151_4/Change-Control-vs-Change-Management-Moving-Beyond-IT.htm
[14] Strassner, J. (2004). Policy-Based Network Management, Solutions for the Next Generation.Morgan Kaufmann Publishers. pp. 4-6
[15] Kim G. , Kim J, and Na. J. "Design and implementation of policy decision point in policy-based network Computer and Information Science, 2005.Fourth Annual ACIS International Conference.April 2006
[16] Kowtha S. ; Xi J. "An N-state driven policy-based network management to control end-end network behaviors" Seventh IEEE International Workshop on Policies for Distributed Systems and Networks, 2006. Pp 75-80, June 2006
[17] Berto-Monleon, R.; Casini, E., "Specification of a Policy Based Network Management architecture" .Military communications conference. 2011 - MILCOM 2011 , pp. 1393 – 1398, 2011

[18] "What You Should Know Before Investing in Policy-Based Network Management" [online]. Available: http://sysdoc.doors.ch/AVAYA/AvayaWhitePaper.pdf
[19] Kosiur D. (2001).Understanding Policy-Based Networking Wiley Computer publishing. Pg. 70-73
[20] Policy-Based Management. [Online], available http://www.linktionary.com/p/policy.html
[21] Ki-Sang Ok ; Hong, D.W. ; Byung-Soo Chang "The Design of Service Management System based on Policy-based Network Management" International conference on Networking and Services, 2006. pp. 59-64, September 2006
[22] Felix J. G. Clemente et al, "An XML-Seamless Policy Based Management Framework," in Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2005, Sep. 2005, pp. 418–423.
[23] Drogseth D. (2009). Network Change and Configuration Management: Optimize Reliability, Minimize Risk and Reduce Costs. An Enterprise Management Associates (EMA™)
[24] IETF, "Network Configuration (Netconf)", http://www.ietf.org/html.charters/netconf-charter.html.
[25] R. Enns, "NETCONF Configuration Protocol" [Online]. Available http://tools.ietf.org/html/rfc4741, IETF, Dec. 2006.
[26] W3C, "Extensible Markup Language (XML)," 2005, <http://www.w3.org/XML/>.
[27] J. Martin-Flatin, "Web-Based Management of IP Networks and Systems," Ph.D. dissertation, Swiss Federal Institute of Technology, Lausanne (EPFL), Oct 2000.