whitepaper

Practitioners Guide to Improving Network Device Configuration & Change Management

solarwinds

whitepaper

solarwinds

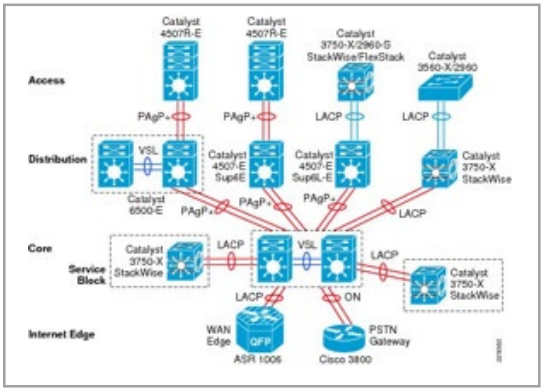
Introduction

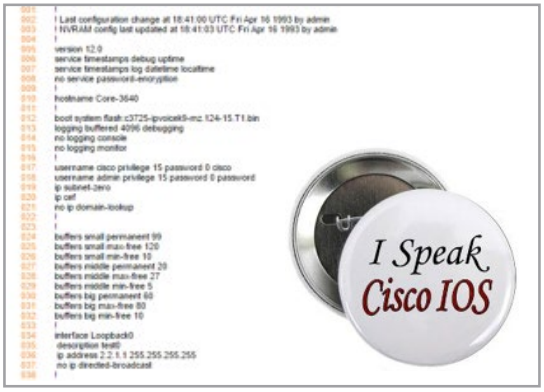
Networks must constantly evolve to meet business requirements. Recently, Gartner® predicted that BYOD, Mobile Apps, "Internet of Things," Cloud, Software Defined (SDx), and Smart Machines will have a significant impact on organizations over the next three years. For an IT organization, these trends mean managing change. So the question each organization must ask is *"do we have the know-how and tools needed to manage the changes which lay ahead?"*

The Problem

For all of the advances in network management capabilities, the management of device configurations continues to have significant limitations. These limitations impact your ability to manage network change. Consider the following scenarios:

- **Devices are still independently managed. While a network functions as a cohesive system, it is still composed of individual devices. With few exceptions, complex service changes still require separate and detailed configuration changes to each device. The same also holds true for disaster recovery. Measures to protect the network are still applied at the device level.**





- **Configuration interfaces are still overly complex. Many devices are managed using techniques that have not changed in decades. Configuration changes are often manually deployed via remote login and entering commands into the device.**
- **Managing configurations requires advanced technical skill. Each vendor supports its own complex command syntax. For example, IOS contains roughly 17,000 commands. Therefore, making configuration changes in a mixed-vendor network require a thorough understanding of all syntaxes and commands used by each device.**

For these reasons, making wide-scale network changes can quickly turn into formal projects which can be costly and impede agile operations. But as costly as this might be, it's even more costly to make ad-hoc or loosely managed wide-scale network configuration changes because they increase your risks of making a mistake. One simple mistake is all it takes to bring down a critical route and impact business-critical applications. Because of this, industry experts warn that most network outages are due to configuration errors and that outages can cost an organization $1,000 to $3,000 for each hour of downtime .

Managing network configurations is a complex process which requires a disciplined

whitepaper

approach. This white paper provides some recommendations for how you can minimize the chances and impact of these network problems.

Identify Network Devices to Manage

Configuration and change management begins with knowing what you are managing and understanding what the configuration state is for each item.

Many managed devices use SNMP, which allows the device to self-report configuration details. This information is stored in a database, which can then be linked to other data sources to form a comprehensive configuration management database (CMDB). When you are able to collect and maintain device-level information, you can see what the current configuration is, when it was last changed, what was changed, and who made the change.

Whether you manage tens, hundreds, or thousands of devices, identifying these devices and keeping details current using manual and ad-hoc methods is time-intensive. Therefore, look for a solution which lets you automate the discovery and inventory of each network device you manage. This allows you to capture and manage extensive device details including:

- **Device type, ID's, location, owner, operating status, etc.**
- **Key part numbers, service dates, and end-of-life dates**
- **Group devices by type, function, location, etc. for easier navigation and management**

Adopt Standardization

When you have many devices being managed by many network admins and engineers, you run the risk of more errors, disruptions, and support costs. Standardization can help avoid these problems. You can apply standardization to work processes and actual configurations.

You should standardize work processes to help you: 1) design and verify new services prior to deployment, 2) manage and protect in-use configurations, and 3) ensure that configurations consistently meet SLA and compliance requirements.

[1] Gartner: Ronni J. Colville and George Spafford Configuration Management for Virtual and Cloud Infrastructures

[2] Information Technology Intelligence Consulting: One Hour of Downtime Costs > $100K For 95% of Enterprises

CASE STUDY GOVERNMENT – STATE AGENCY

Situational background: This state government agency comprises multiple regional authorities, and each region had its own IT department up until two years ago when the decision was made to centralize and standardize IT operations.

Challenge: Many tools were in use across the regions, and some regions didn't have any proper configuration management, instead relying on purely manual processes. The initial challenge was getting all the devices discovered and under management to ensure that configurations could be regularly and consistently backed up and that all changes could be logged. However, additional challenges lay further ahead that involved establishing a true, formalized structure for change management and creating and using standardized configuration templates.

SolarWinds® NCM solution: SolarWinds NCM is now deployed as a fully integrated component with SolarWinds NPM. The team is using the SolarWinds solution to manage 1000 nodes, which includes network switches and routers as well as some servers. Anywhere from 15 to 20 people interact with NCM on a daily basis. The entire network team uses NCM, and the security teams also have access to the tool. NCM is used to perform inventory of physical infrastructure devices on the network as well as to back up configuration files and, if necessary, restore configurations. The team found that the tool is easy to use and did not require training for new operators.

Benefits: Moving from a manual to a structured configuration process has helped them achieve greater consistency across all devices. The ability to limit access through rights and limitations has also helped prevent unauthorized access to network nodes. The ability to manage change and have visibility into what has changed has not only helped save time when resolving configuration issues, but it has also established greater accountability. For example, an administrator in another district installed a new Cisco® switch into a stack and because the switch had been set with an incorrect priority, it conflicted with the master switch and wiped out the configuration information on the rest of the stack. With NCM, the network engineer was able to retrieve the configuration information from the previous stack and restore it, saving hours of time in restoration. Further, the manager-level reporting within NCM helps keep the agency's upper management in the loop.

You should also standardize your configurations by adopting conventions for: 1) naming and logic flow, 2) in-line comments and documentation, 3) logic reuse using variable substitutions, and 4) scheduled executions.

Look for a solution that allows you to enforce change controls in work processes, create custom and standardized configuration templates, and use scheduling to make rapid standardized changes and updates across similar devices.

Protect Devices from Failures or Unauthorized Changes

Too often when a network failure has occurred, the cause is due to a recent configuration change. Sometimes changes can be made out-of-process or in a way that produces an unwanted result. Therefore, it's important to be aware of device configuration changes.

It's important to be aware of a configuration change. However, it's equally critical to know what changed. Many configuration files are complex. When an unwanted change has occurred, it's imperative that you can identify and correct the errant changes quickly. There are some general purpose utilities to help with this, but they take time and require a high level of skill to use.

In addition, sometimes in order to restore service you need to do a configuration rollback. A rollback can be used to reverse an error or to quickly reconfigure a replacement hot-spare device. Again, there are general purpose utilities that you can use to archive and restore configuration files. But "homegrown" solutions tend to be fragile and require regular, time-consuming maintenance.

Look for a solution that detects configuration changes, identifies specific changes made within a configuration, and lets you automate configuration, archive, and restore tasks.

Audit Configurations for Policy Compliance

Network security is an integral part of defending the confidentiality, integrity, and availability of protected data. Many security configuration settings are defined by various policies. For example, financial and retail firms must protect cardholder data and comply with PCI DSS. Organizations in healthcare must protect patient confidentiality and comply with HIPAA standards. Firms and organizations connecting to US government networks must comply with FISMA and DISA STIG guidelines.

Failure to consistently comply with regulatory standards can result in the loss of your data and reputation and even lead to financial and punitive penalties.

Look for a solution that can quickly tell you whether your device configurations conform to internal and regulatory operating policies.

Summary

The recommendations discussed in this white paper can significantly simplify and improve your ability to manage change across hundreds or even thousands of device configurations. In addition, using a network configuration and change management (NCCM) application greatly increases the accuracy and efficiency of your network management processes. Used together, these practices and an NCCM solution will help you not only manage changes, but also reduce labor opex. Consider the following examples[3]:

Task/Event	# Devices	Labor - without NCCM (assume $35 per hour)	Labor - using NCCM	Savings
24-port switch failure with no backup configuration (per failed device)	1	3 hrs.	1 hr.	2 hours labor, $70 labor cost
Bulk configuration updates (per update)	300	25 hrs.	10 minutes (automated)	25 hrs. labor, $875 labor cost
Configuration audits (per audit)	300	1,200 hrs.	0 minutes (automated)	1,200 hrs. labor, $42K labor cost
New device rollouts (112 ports) with standardized configuration	4	16 hrs.	2 hrs.	12 hrs. labor, $490 labor cost

In addition to time and cost savings, organizations will also see improvements in

- **Operational agility**
- **MTTF and MTTR**
- **Policy compliance**

To learn more about how SolarWinds can help you manage your network configurations, please visit our website.

[3] ENTERPRISE MANAGEMENT ASSOCIATES: ROI for NCM Solutions in Enterprise Environments