Network Configuration Management

Contents

Abstract

Many operational problems facing network managers today result from a lack of configuration management capabilities. Configuration management is an essential operational capability. It is foundational for other network management functions and crucial for service management.

This document describes what configuration management is and why it is important for operations and network management and provides next steps for improving this vital function in your organization.

Best Practices for Configuration Management

The document will go into more details about configuration management, but it is important to understand the key factors that have caused configuration management problems in the past. These include failure to:

- Maintain a master device list
- Maintain correct credentials and manageability at 100 percent
- Create relevance for users and management
- Achieve differentiated management; "not all devices are equal"
- Address people, processes, and technology, not just technology
- Develop processes to work for your company
- Commit resources; this is not a project, it is a system

What Is Configuration Management?

Configuration management is a large function inside network management. It covers many areas. Many people think of configuration management as its just managing the configurations of the network devices, but configuration management covers a lot more than this.

Configuration management is not just about a technology to collect device information but also about the processes needed for network support and operations.

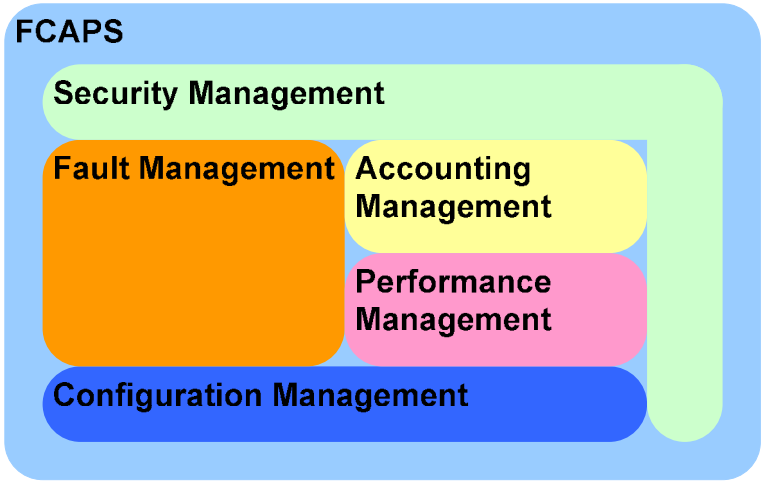
Configuration management can be summarized as:

- Device hardware and software inventory collection
- Device software management
- Device configuration collection, backup, viewing, archiving, comparison
- Detection of changes to configuration, hardware, or software
- Configuration change implementation to support change management

FCAPS

Configuration management is the C from the FCAPS (fault, configuration, accounting, performance, and security) model [1]. Configuration management is a key function of this model, and while many people think of each function of FCAPS as being equal, the situation might look more like that illustrated in Figure 1.

Figure 1. Interactions of the FCAPS Functions



Each of the functions interacts with each of the others. Security has to touch all the functions to be effective, while configuration is the function that holds so much of the important data for all the functions.

Configuration Management Operational Issues

The following are a couple of scenarios that may seem familiar to people working in a production network. Here are some common operational problems that could result from a lack of configuration management capabilities:

- The engineer who makes a configuration change is not available when the impact is realized. For example, change impact from a change on a Sunday, may not be noticed by another engineer until Tuesday when end of month processing causes high load.
- An approved change is implemented but not in the way agreed to by the change approvers, a business impact is experienced, and the approvers are left accountable with no audit trail and no recourse.
- Security alerts indicate impacted devices and workarounds, but the manual effort takes considerable time to determine the exposure, and the possible risk, and then huge amounts of time are required to implement the workaround and software upgrades.
- Configuration changes are being made on the production network with no visibility by management.

IT Infrastructure Library

The IT Infrastructure Library (ITIL) [2] is a framework for service management to help ensure that the IT department and the business group in an organization are aligned. It is a comprehensive framework covering many topics related to operations and network management. ITIL defines a set of processes, of which one is configuration management.

ITIL defines configuration management to assist with the following :

- To account for all IT assets
- To provide accurate information to support other service management processes
- To provide a sound basis for incident, problem, change, and release management
- To verify records against infrastructure and to correct exceptions

These goals are suitable for a discussion on configuration management and specifically network configuration management, especially if the business and IT department have a goal for service management.

The discussion in this document is network focused, and some of the ITIL concepts don't cover network specifics, as ITIL is a framework this is acceptable. The ITIL definitions for configuration management should be used and relevant elements reused and modeled for use within the network.

Network Documentation and Diagrams

Network documentation is critical in a production environment; it provides a static record of the state of the network at a point in time. Because it is static, its useful life is limited to the first change made on any of the elements contained in the documentation. In a static network environment, this may be many years.

Like network documentation, network diagrams are critical, but they are again a static record of the desired state of the network and have no reflection of the current configured or operational state.

Documentation and diagrams form part of the network configuration, and a provision should be made in the configuration management system to support this type of content.

Why Is Configuration Management Important?

Some of the benefits of an effective configuration management system are:

- Reduced downtime through rapid change impact identification
- Productivity improvement for making configuration changes
- Helps ensure compliance for device configuration, software versions, and hardware
- Quick impact determination of security alerts
- Improved visibility and accountability at all levels
- Improved process and approval implementation

Foundational and Fundamental

Configuration management is the cornerstone of the network management system and of the network lifecycle [3]. It knows what is in the network, and it provides control over network elements and linkage between the phases of the lifecycle. Phases in the network lifecycle are:

- Prepare
- Plan
- Design
- Implement
- Operate
- Optimize

The network lifecycle applies to the entire life of the network as well as any smaller projects that extend the network over time. A general definition for a project is anything that requires design, and all designs should fit into the architecture or the architecture should be updated as new requirements are identified. Any change to the network not requiring design, including optimization to the production environment, should be considered operational.

Some of the roles in network delivery and support are:

- Management
- Architecture
- Delivery
- Support

Table 1 shows how the lifecycle is combined with the roles required to deliver and support network services.

Table 1. Lifecyles and Roles for Delivering and Supporting Network Services

	Prepare	Plan	Design	Implement	Operate	Optimize
Management	X	X				
Architecture	X	X				
Delivery			X	X		
Support					X	X

Table 1 shows the flow of work through a network team and the demarcation in responsibilities between roles. Configuration management provides the implementation point for demarcation; from this processes can be developed that supports the network lifecycle and the necessary roles.

Documentation and Diagrams

As discussed earlier, network documentation and diagrams are critical in a production environment. They can provide information when troubleshooting network outages; they are, however, static. When the network is supporting a dynamic business environment, providing agility to meet business demands, static documentation is not suitable.

An effective configuration management capability will provide up-to-date information on the configured state of the network and will be updated dynamically as the network changes. When combined with static documentation and diagrams, it provides more relevant information to support network operations.

Compliance

Compliance is about meeting regulations imposed by government or industry. These regulations have been created to prevent problems like Enron happening again; it is about governance. In total there are many compliances, but only some (if any) will be specific to a business. Sarbanes-Oxley (SOX) [5] is one of the best-known compliances, applicable if a company is listed on the U.S. stock exchange.

With effective configuration management in place along with the appropriate processes, like change management and others, compliance becomes a less daunting challenge. It is not however a matter of buying a product and being compliant; it is about building capabilities to support compliance over time.

Managing Risk

A key issue with network management is the rapid increase in the number of network elements. As the current economic growth increases business opportunities, infrastructure changes to support business growth in the booming world economy are required.

With this multiplication in elements, the ability to understand risk exposure has also become more difficult. There are so many devices, software versions, and configuration combinations. The ability to understand exposure is no longer possible without new capabilities in auditing and reporting.

This also requires appropriate supporting processes and modifications in operational methodologies so that the risk can be understood and expediently mitigated as required.

Time to Resolve

A key measure in many service levels is incident time to resolution. An incident will result from a network outage, and in simple terms, an outage to a production network that is considered stable is caused by one of the following:

- Layer 1 network failure (leased line, fibre cut, and so on)
- Physical infrastructure failure, power, air conditioning
- Hardware failure, power supply, chassis, or module
- Software failure, due to memory leak or bug
- Security exploit, causing DOS or software failure
- A change in configuration, either logical (being a new feature) or physical (being new hardware or connections)

In simple terms, a network outage is caused by a change, a change in state or configuration. Configuration management assists with time to resolution by providing the necessary information to support troubleshooting and decision making. This is especially true of a configuration change. If a network outage is caused by a configuration change, this needs to be eliminated as the root cause in the first instance.

In this manner configuration management is a system that contributes to the overall availability of your network and is a key foundation for a highly available network.

Developing Configuration Management Capabilities

Developing capabilities in configuration management requires a combination of:

- People
- Processes
- Technology

Configuration management as with most network management functions is not a shrink-wrap or an off-the-shelf solution. Technology is available as packaged products, providing many of the required features. Unless the technology is combined with people and processes, the capability is not developed.

For example, the technology will produce the required reports, but until the people read the reports, determine any actions needed, then kick off the necessary processes to carry out the actions, the reports are quite useless. This is why network management systems so often fail to deliver a suitable return on investment.

This section details how to develop configuration management capabilities by identifying the high-level requirements of configuration management, some of the policies that need to be developed, and some of the necessary processes of which the configuration management function will be part.

High-Level Requirements

The following is a list of requirements that define the essence of configuration management. These requirements are not purely technical. They are both technical and functional requirements to support a full configuration management solution.

The requirements for configuration management are:

- Collect network inventory, including chassis and modules as well as serial numbers
- Report on collected network inventory
- Collect device configurations
- Keep multiple versions of device configurations
- Allow comparison between the multiple versions of device configurations
- Detect changes in device configurations (event or polling based)
- Determine which user made changes to device configurations
- Report on configuration changes
- Allow configuration changes to be batched and scheduled
- Report on existing software versions deployed on devices
- Keep a repository of device software versions
- Support upgrading of device software
- Audit configuration to help ensure compliance
- Search device configurations, software, and hardware
- Store or link to static documentation and diagrams
- Support the approval processes and workflows

Asset Management

If the configuration management system needs to support asset management, then the additional requirements needed to support business accounting processes, such as depreciation, are:

- Purchase date
- Purchase price
- Asset number
- Purchasing details, company-specific information (purchase order number, vendor, and so on)

Carrier Service Management

If the configuration management system needs to support carrier service management, then additional requirements that support carrier service management and contract renewal are needed. Some of these requirements are:

- Service number
- Carrier (telco)
- Contract start date
- Contract period
- Currency
- Cost per month

Federated Database

From the requirements, it is clear that a database is needed to store and manage the configuration data. It may be difficult to find a single system that supports all of these requirements, so a federated database model may need to be considered. This means that not all the data has to be in one database, but if there is more than one database, the databases should be linked in some way.

Policies

There are a number of policies needed to be implemented within a configuration management system. A policy in this context is a documented management decision on what and more possibly how the system should work. The policy will determine how the configuration management system itself is configured or set up.

This list is by no means comprehensive but serves as a guide for what needs to be documented as part of a company's configuration management policy. The minimum management policies needed to build a configuration management platform are:

- Length of time device configurations should be kept
- How many versions of device configurations should be kept
- Frequency of full configuration collection
- Frequency of configuration change polling
- Frequency of full inventory collection
- Frequency of inventory change polling
- Length of time inventory changes are kept
- Frequency of device configuration compliance checking
- Which configuration changes can be made automatically

Processes

Processes are important for a successful configuration management system. ITIL provides a good framework for processes relevant to configuration management. There are more generic or general processes that are needed for configuration management in a network.

Related ITIL Processes

The following are the directly related ITIL processes that network configuration management supports:

- Configuration Management including the CMDB
- Change Management
- Incident Management
- Problem Management
- Capacity Management

Configuration Management

Network configuration management is synonymous with ITIL Configuration Management, which defines the important elements of configuration management a network needs. Because ITIL does not define implementation, some of the aspects do not address network specifics but this is acceptable.

More specifically, the Configuration Management Database (CMDB) talks about relationships between Configurable Items (CI), but the definition of a CI gets very vague when talking about switches with hundreds of interfaces.

Service management does not really address the concept of shared infrastructure very well, and as a network is shared by almost all services, this needs to be adapted.

Change Management

Without effective configuration management, change management is somewhat pointless. Currently many organizations implement change management on a trust basis with no real means to audit approved changes against actual configuration changes.

Change management is probably the ITIL process that affects businesses the most; it provides a distinct link between IT operations and the business. It requires IT to coordinate its efforts with the business group to help ensure that the business impact is minimized or avoided.

Incident Management

As discussed in the section “Time to Resolve,” configuration management is important for incident management. It provides up-to-date information about the network.

Problem Management

Configuration management is crucial for problem management. Without this information the problem management process is difficult.

Capacity Management

This is specifically related to the physical capacity of the network. Inventory data provides information about the spare capacity for interfaces, ports, modules, slots, and so on. This is especially true for campus and data center management.

Generic Processes

The following are some generic processes that are made possible with configuration management.

Standard Product Verification

New products, both software and hardware, should be verified before being deployed into the production environment. This process is linked to other process like vulnerability and change management.

Verification should include testing of the required configuration and software to be deployed and should reflect the impact the device has on the network.

Production Handover

When a new device is deployed in the network, make sure that it is added into the management systems, that the configuration templates have been deployed, and that the device is manageable. This process is the demarcation from implementation to operation in the network lifecycle; this is when the device or project is handed into production.

Configuration Change Auditing

There are several aspects to this process. Ultimately this process is to make sure that accountability is enforced with network changes. The two main elements of this process are:

- Support the change management and help ensure that the changes that have been approved are implemented as described
- Audit configuration changes and make sure they are related to an approved change

Vulnerability Management

Look for and review published security advisories from Cisco® (PSIRT) [4] and CERT (Computer Emergency Response Team) [6] and determine which ones affect the production environment and what the risk of an impact to the business is.

For devices that are vulnerable, determine if a software upgrade is necessary or if a configuration workaround is sufficient to mitigate the risk.

End of Life Management

Audit the collected inventory for devices that may be out of depreciation or at the end of support by the vendor or maintenance provider. Determine what the potential risk is and, when necessary, instigate projects to upgrade equipment.

Maintenance

Use the collected inventory information to audit against vendor or partner maintenance and determine that maintenance agreements are correct and that maintenance is not being paid on devices that are no longer in production.

Architecture and Standards

Many network teams will design every deployment or project; this is an engineering way of approaching things. What is required is a paradigm shift in network engineering to allow the network teams to spend more time on network architecture and standard designs.

First, the network architecture has to be documented. Cisco defines many reference architectures, and the network is probably already based on architectural elements. To achieve this, the architecture should be communicated with the ITS department and with business groups. Part of network architecture is about normalizing and generalizing; this creates patterns and building blocks in the network that can be more easily scaled.

The architecture should be hierarchical and structured; this creates points where new infrastructure connects, whether it is a new building, a new floor, or a new remote office. From the building blocks, standard can be developed. These standards include products, configurations and designs.

The standard designs improve the ability to quickly meet business requirements and reduce the total cost of ownership through consistent deployments, in much the same way as desktop teams have an SOE (standard operating environment).

Standardizing products is part of this, and defining a set of network solutions the network team offers to the business. This could be considered the "Service Catalogue" from ITIL.

Initially, work is required to document and build out this architecture and these standards. In time, this reduces load on the network team by providing prebuilt “wheels” that can be used.

Configuration Templates

From the work in standards, configuration templates that represent the functions of devices can be developed. The same basic template can be used for all floor switches where only the hostname, IP addresses, or VLANs, and so on are unique. Further, all Cisco IOS® Software devices can share the same base management template.

Once these templates are developed, they can be set up within configuration management tools and allow rapid deployment and configuration baseline/auditing to verify networkwide compliance of the devices to the template.

This seems like an obvious solution. It is a simple high-value function that will ultimately save a lot of rework by the network engineering team and increase productivity.

Service Provisioning

Extending the idea of architectures and standards as well as configuration templates is called service provisioning. Based on the architecture work and resulting design standards, service provisioning is about using the commonality in the network and creating generalizations.

With this paradigm, projects become very similar and are about providing network access, whether it is for remote office staff or for a server; a network is about providing and controlling access.

To support this, interface configuration templates, which can be easily deployed to network elements, can be developed to provision access for a PC, a phone, a server, or an access switch. These templates can be set up as configuration tasks in tools so that engineers can deploy them more easily. Over time as confidence is established, this work can be delegated to the server or data center teams for server ports or to the desktop team for PC ports.

This capability will extend the productivity of the team and release resources to continue working on architectures and be more proactive with the capacity management of the network.

Automation

Automation provides a solution for scaling operations specifically in the area of resourcing. Going forward, there is little choice to use tools for automation. To handle the size of the network, hiring some additional resources may be required, but network engineering resources are difficult to find and hire, and without these additional resources, it is simply not possible to manage a large network, and important operational functions won't be completed. This is where automation provides a solution to this problem.

Automation has one other problem: people need to gain confidence in the tools and the required processes; otherwise moving towards automation cannot happen. To assist a simple process of testing, gaining confidence is a key factor.

Integrated Confidence Building and Impact Mitigation

For an example, consider a software upgrade to all remote routers in the network. A software upgrade of approximately 2500 devices is required to be completed ASAP; the risk business impact needs to be mitigated as much possible.

The idea here is simple; mitigate risk, and control the rollout of the software, reducing the probability of software causing problems or the tools causing problems.

The metaprocess for the above example would be as follows:

1. A Cisco PSIRT is published.
2. The configuration management system assists in identifying affected devices, 2500 routers, and the proposed resolution.
3. The vulnerability management process is instigated, the impact is verified, and a resolution to upgrade the routers is proposed.
4. The software is certified by the New Product Certification process.

5. The configuration management platform is used to upgrade a lab device of the same type to verify the tools.
6. Changes are raised to upgrade 20 production devices, which cover the hardware and software combinations.
7. Configuration management platform is used to perform the upgrade of 20 devices; engineers manually verify each device to help ensure success and resolve any issues.
8. Twenty-four business hours are left to make sure that devices are stable under production conditions.
9. Go or no go to continue.
10. Changes are raised to upgrade 180 production devices.
11. Configuration management platform is used to perform the upgrade of 180 devices, tools are used to verify all devices, engineers select 20 devices at random and perform a manual verification.
12. Go or no go to continue.
13. The remaining devices are divided into batches of 200 to 600 devices and changes raised for each night over as many required nights.
14. Configuration management platform is used to perform the upgrades, tools are used to verify all devices, engineers select 20 devices at random and perform a manual verification.
15. Twenty-five hundred devices should have been upgraded in less than 2 weeks with the risk managed.

Testing, Change, Configuration, and Release Management

To effectively manage a large Cisco network, testing is crucial. Without testing and verification of changes, especially for large changes, business impact should be expected. In reference to ITIL, this ties into release management, that is, how to verify changes to the production environment without affecting the production environment.

The principles are simple and are considered as best practices by the industry. The test lab should include a representative collapsed topology of the production network derived from the production network, and changes to the configuration or software should be tested in this test lab.

As part of the project to deploy the new network, a test plan will be developed. This test plan should be made of unit tests, regression tests, and acceptance tests. After deployment, these tests will be repeated as part of the release management process.

To determine whether a change needs to be tested, the following tables can be used. The change impact is shown in Table 4, and the change control impact is given in Table 3. The results of these are plugged into the Release Management Policy, and this determines whether testing is required or not.

Test Types

There are different types of testing required to verify production operation. Table 2 is an example of what a release management policy might look like.

Table 2. Test Types

Test Type	Description
Verification	Testing not required if other testing has already been carried out on the same device type, modules, software, feature combination

Unit	• Testing of the components affected by the change in software or hardware; for example: • Software upgrade a maintenance release, for example, 12.4(1) to 12.4(2). • Hardware upgrade between hardware versions • Feature configuration change of a feature already in use
Regression	• All unit tests for that part of the production network should be run. • Software upgrade a major release, for example, 12.4(1) to 12.4(2)T or 12.3(4) to 12.4(5) • New hardware (module) not previously used with this hardware/software combination • New feature on a single element of the production network
Acceptance	Multiple software and hardware upgrades on multiple devices and elements in the production network. Complete testing should be carried out. New feature deployment on multiple elements of the test topology.

This describes the relationship between testing and operations, specifically release management. When the test plans are developed, they should be developed so that they can be reused for ongoing operational testing.

Change Control Impact

This property defines the impact of the element on the production environment. The possible values are:

- High
- Medium
- Low

Table 3 shows the change control impact for network elements.

Table 3. Change Control Matrix

Elements	Change Control Impact
Core	High
Edge	High
WAN access	Medium
LAN access	Low
Service modules	High

Change Impact

The change impact is the possible impact the change can have on the production environment. Possible values are:

- High
- Medium
- Low

Table 4 shows the change type and the possible change impact. The list is order dependent, starting at the top, matching the change type.

Table 4. Change Impact Policy

Change Type	Change Impact
Software upgrade major, for example, 12.3(4) to 12.4(5).	High
Configuration change to packet forwarding capabilities	High
Software upgrade maintenance release, for example, 12.4(1) to 12.4(2)	Medium
New feature deployment	Medium
New hardware deployment	Medium

Configuration change to nonpacket forwarding capabilities	Low

Release Management Policy

Table 5 is an example of what a release management policy might look like.

Table 5. Release Management Testing Policy

Change Control Impact	Change Impact	Test Type Required
High	High	Acceptance
High	Medium	Regression
High	Low	Unit
Medium	High	Regression
Medium	Medium	Unit
Medium	Low	No testing required
Low	High	Regression
Low	Medium	Unit
Low	Low	No testing required

Consequences of Not Acting

There are three major consequences of not acting:

- Limited capabilities and the increasing gap cause risk.
- Effective decision making is slowed down.
- Resourcing and automation are stretched.

Many companies have a gap with capabilities in network operations and maintenance, specifically configuration management, and as time goes on this gap is increasing.

Limited Capabilities and the Increasing Gap

With limited capabilities in configuration management, there is a risk that an incident could occur that requires configuration management capabilities to respond in a timely manner. For example, specifically this is true of critical configuration changes, like password updates, and responding to security incidents. In this sense, configuration management can be likened to virus updates and software patches for PCs.

This is also true of proactive activities, specifically maintenance tasks. There are maintenance tasks needed in an IP network, and these tasks may not be being carried out with the required regularity.

This means there is a gap building between the desired operational state of the network and the current operational state of the network.

This is compounded if your company is expanding its operations and the number of network elements, as the network grows and the volume of work increases, the maintenance tasks increase, and without corrective action, this gap will continue to grow.

Effective Decision Making

Effective decision making is also slowed down and more laborious when the decision requires information on the current state of the network. Depending on the regularity of decisions relating to the network, the time and cost burden of this slowdown could be material.

Resourcing and Automation

Currently there is a global IT skill shortage. This is especially true for network engineers. It is difficult to recruit and retain experienced networking professionals, and equally challenging to use their experience in business impacting efforts.

The lack of automation capabilities in network operations means that experienced resources are being stretched to deliver on repetitive tasks, reducing productivity and potentially reducing job satisfaction. Maturity in configuration management tools and processes will improve automation capabilities and productivity and reduce the likelihood of staff turnover.

References

1. http://www.tech-faq.com/fcaps.shtml
2. http://www.itlibrary.org/
3. http://www.cisco.com/warp/public/437/services/lifecycle/LifecycleServicesWhitePaper.pdf
4. http://newsroom.cisco.com/dlls/2007/prod_010307.html
5. http://knowledgehills.com/Sarbanes/sarbanes-oxley.aspx
6. http://www.cert.org/faq/cert_faq.html

Acronyms

CERT: Computer Emergency Response Team

CI: Configurable Item

CMDB: Configuration Management Database

FCAPS: Fault, configration, accounting, performance, and security (a TMN term)

IOS: Internet Operating System

ITIL: IT Infrastrure Library

PSIRT: Product Security Incident Response Team

VLAN: Virtual local area network

SOE: Standard operating environment

SOX: Sarbanes-Oxley

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-425874-00 09/07

