

Cisco – Configuration Management: Best Practices White Paper

Table of Contents

<u>Configuration Management: Best Practices White Paper</u>	1
<u>Introduction</u>	1
<u>High-Level Process Flow for Configuration Management</u>	2
<u>Create Standards</u>	2
<u>Software Version Control and Management</u>	3
<u>IP Addressing Standards and Management</u>	3
<u>Naming Conventions and DNS/DHCP Assignments</u>	4
<u>Standard Configuration and Descriptors</u>	4
<u>Configuration Upgrade Procedures</u>	5
<u>Solution Templates</u>	5
<u>Maintain Documentation</u>	5
<u>Current Device, Link, and End-User Inventory</u>	6
<u>Configuration Version Control System</u>	6
<u>TACACS Configuration Log</u>	6
<u>Network Topology Documentation</u>	6
<u>Validate and Audit Standards</u>	7
<u>Configuration Integrity Checks</u>	7
<u>Device, Protocol, and Media Audits</u>	7
<u>Standards and Documentation Review</u>	8
<u>Related Information</u>	8

Configuration Management: Best Practices White Paper

Introduction

High-Level Process Flow for Configuration Management

Create Standards

- Software Version Control and Management
- IP Addressing Standards and Management
- Naming Conventions and DNS/DHCP Assignments
- Standard Configuration and Descriptors
- Configuration Upgrade Procedures
- Solution Templates

Maintain Documentation

- Current Device, Link, and End-User Inventory
- Configuration Version Control System
- TACACS Configuration Log
- Network Topology Documentation

Validate and Audit Standards

- Configuration Integrity Checks
- Device, Protocol, and Media Audits
- Standards and Documentation Review

Related Information

Introduction

Configuration management is a collection of processes and tools that promote network consistency, track network change, and provide up to date network documentation and visibility. By building and maintaining configuration management best-practices, you can expect several benefits such as improved network availability and lower costs. These include:

- Lower support costs due to a decrease in reactive support issues.
- Lower network costs due to device, circuit, and user tracking tools and processes that identify unused network components.
- Improved network availability due to a decrease in reactive support costs and improved time to resolve problems.

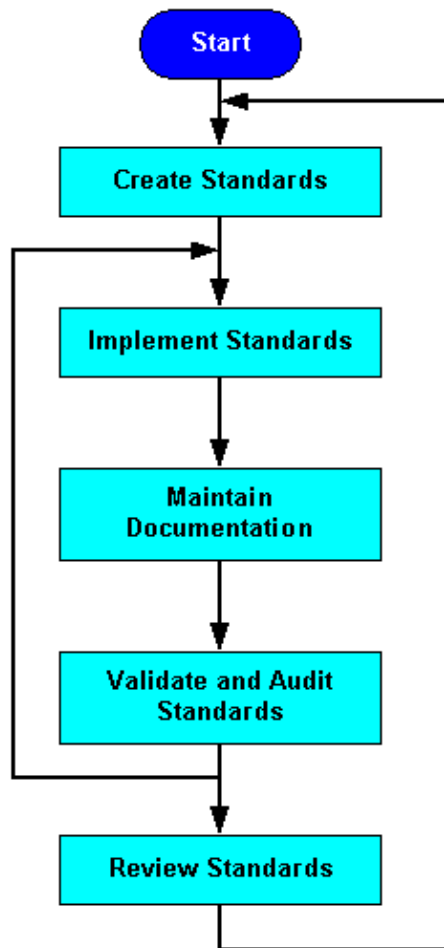
We have seen the following issues resulting from a lack of configuration management:

- Inability to determine user impact from network changes
- Increased reactive support issues and lower availability
- Increased time to resolve problems
- Higher network costs due to unused network components

This best-practice document provides a process flowchart for implementing a successful configuration management plan. We'll look at the following steps in detail: create standards, maintain documentation, and validate and audit standards.

High-Level Process Flow for Configuration Management

The diagram below shows how you can use the critical success factors followed by performance indicators to implement a successful configuration management plan.



Create Standards

Creating standards for network consistency helps reduce network complexity, the amount of unplanned downtime, and exposure to network impacting events. We recommend the following standards for optimal network consistency:

- Software version control and management
- IP addressing standards and management
- Naming conventions and Domain Name System/Dynamic Host Configuration Protocol (DNS/DHCP) assignments
- Standard configurations and descriptors
- Configuration upgrade procedures
- Solution templates

Software Version Control and Management

Software version control is the practice of deploying consistent software versions on similar network devices. This improves the chance for validation and testing on the chosen software versions and greatly limits the amount of software defects and interoperability issues found in the network. Limited software versions also reduce the risk of unexpected behavior with user interfaces, command or management output, upgrade behavior and feature behavior. This makes the environment less complex and easier to support. Overall, software version control improves network availability and helps lower reactive support costs.

Note: Similar network devices are defined as standard network devices with a common chassis providing a common service.

Implement the following steps for software version control:

- Determine device classifications based on chassis, stability, and new feature requirements.
- Target individual software versions for similar devices.
- Test, validate, and pilot chosen software versions.
- Document successful versions as standard for similar–device classification.
- Consistently deploy or upgrade all similar devices to standard software version.

IP Addressing Standards and Management

IP address management is the process of allocating, recycling and documenting IP addresses and subnets in a network. IP addressing standards define subnet size, subnet assignment, network device assignments and dynamic address assignments within a subnet range. Recommended IP address management standards reduce the opportunity for overlapping or duplicate subnets, non–summarization in the network, duplicate IP address device assignments, wasted IP address space, and unnecessary complexity.

The first step to successful IP address management is understanding the IP address blocks used in the network. In many cases, network organizations have to rely on RFC 1918 address space, which isn't Internet addressable, but can be used to access the network in conjunction with Network Address Translation (NAT). Once you have defined the address blocks, allocate them to areas of the network in a way that promotes summarization. In many cases, you'll have to further subdivide these blocks based on the number and size of subnets within the defined range. You should define standard subnet sizes for standard applications, such as building subnet sizes, WAN link subnet sizes, loopback subnet size, or WAN site subnet size. You can then allocate subnets for new applications out of a subnet block within a larger summary block.

For example, let's take a large enterprise network with an east coast campus, a west coast campus, a domestic WAN, a European WAN, and other major international sites. The organization allocates contiguous IP classless interdomain routing (CIDR) blocks to each of these areas to promote IP summarization. The organization then defines the subnet sizes within those blocks and allocates sub–sections of each block to a particular IP subnet size. Each major block or the entire IP address space can be documented in a spreadsheet showing allocated, used, and available subnets for each available subnet size within the block.

The next step is to create standards for IP address assignments within each subnet range. Routers and Hot Standby Router Protocol (HSRP) virtual addresses within a subnet might be assigned the first available addresses within the range. Switches and gateways may be assigned the next available addresses, followed by other fixed address assignments, and finally dynamic addresses for DHCP. For example, all user subnets may be /24 subnets with 253 available address assignments. The routers may be assigned the .1 and .2 addresses, and the HSRP address assigned the .3 address, switches .5 through .9, and the DHCP range from .10 through .253. Whatever standards you develop, they should be documented and referenced on all network engineering plan documents to help ensure consistent deployment.

Naming Conventions and DNS/DHCP Assignments

Consistent, structured use of naming conventions and DNS for devices helps you manage the network in the following ways:

- Creates a consistent access point to routers for all network management information related to a device.
- Reduces the opportunity for duplicate IP addresses.
- Creates simple identification of a device showing location, device type, and purpose.
- Improves inventory management by providing a simpler method to identify network devices.

Most network devices have one to two interfaces for managing the device. These may be an in-band or out-of-band Ethernet interface and a console interface. You should build naming conventions for these interfaces related to the device type, location, and interface type. On routers, we strongly recommend using the loopback interface as the primary management interface because it can be accessed from different interfaces. You should also configure loopback interfaces as the source IP address for traps, SNMP and syslog messages. Individual interfaces can then have a naming convention that identifies the device, location, purpose, and interface.

We also recommend identifying DHCP ranges and adding them to the DNS, including the location of the users. This may be a portion of the IP address or a physical location. An example might be "dhcp-bldg-c21-10" to "dhcp-bldg-c21-253", which identifies IP addresses in building C, second floor, wiring closet 1. You can also use the precise subnet for identification. Once a naming convention has been created for devices and DHCP, you'll need tools to track and manage entries, such as Cisco Network Registrar.

Standard Configuration and Descriptors

Standard configuration applies to protocol and media configurations, as well as global configuration commands. Descriptors are interface commands used to describe an interface.

We recommend creating standard configurations for each device classification, such as router, LAN switch, WAN switch, or ATM switch. Each standard configuration should contain the global, media, and protocol configuration commands necessary to maintain network consistency. Media configuration includes ATM, Frame Relay, or Fast Ethernet configuration. Protocol configuration includes standard IP routing protocol configuration parameters, common Quality of Service (QoS) configurations, common access lists, and other required protocol configurations. Global configuration commands apply to all like devices and include parameters such as service commands, IP commands, TACACS commands, vty configuration, banners, SNMP configuration, and Network Time Protocol (NTP) configuration.

Descriptors are developed by creating a standard format that applies to each interface. The descriptor includes the purpose and location of the interface, other devices or locations connected to the interface, and circuit identifiers. Descriptors help your support organization better understand the scope of problems related to an interface and allows faster resolution of problems.

We recommend keeping standard configuration parameters in a standard configuration file and downloading the file to each new device prior to protocol and interface configuration. In addition, you should document the standard configuration file, including an explanation of each global configuration parameter and why it is important. Cisco Resource Manager Essentials (RME) can be used to manage standard configuration files, protocol configuration, and descriptors.

Configuration Upgrade Procedures

Upgrade procedures help ensure that software and hardware upgrades occur smoothly with minimal downtime. Upgrade procedures include vendor verification, vendor installation references such as release notes, upgrade methodologies or steps, configuration guidelines, and testing requirements.

Upgrade procedures may vary widely depending on network types, device types, or new software requirements. Individual router or switch upgrade requirements may be developed and tested within an architecture group and referenced in any change documentation. Other upgrades, involving entire networks, can not be tested as easily. These upgrades may require more in-depth planning, vendor involvement, and additional steps to ensure success.

You should create or update upgrade procedures in conjunction with any new software deployment or identified standard release. The procedures should define all steps for the upgrade, reference vendor documentation related to updating the device, and provide testing procedures for validating the device after the upgrade. Once upgrade procedures are defined and validated, the upgrade procedure should be referenced in all change documentation appropriate to the particular upgrade.

Solution Templates

You can use solution templates to define standard modular network solutions. A network module may be a wiring closet, a WAN field office, or an access concentrator. In each case you need to define, test and document the solution to help ensure that similar deployments can be carried out in exactly the same way. This ensures that future changes occur at a much lower risk level to the organization since behavior of the solution is well defined.

Create solution templates for all higher-risk deployments and solutions that will be deployed more than once. The solution template contains all standard hardware, software, configuration, cabling, and installation requirements for the network solution. Specific details of the solution template are shown as follows:

- Hardware and hardware modules including memory, flash, power, and card layouts.
- Logical topology including port assignments, connectivity, speed, and media type.
- Software versions including module or firmware versions.
- All non-standard, non device-specific configuration including routing protocols, media configurations, VLAN configuration, access lists, security, switching paths, spanning tree parameters, and others.
- Out-of-band management requirements.
- Cable requirements.
- Installation requirements including environmental, power, and rack locations.

Note that the solution template does not contain many requirements. Specific requirements such as IP addressing for the specific solution, naming, DNS assignments, DHCP assignments, PVC assignments, interface descriptors, and others should be covered by overall configuration management practices. More general requirements, such as standard configurations, change management plans, documentation update procedures, or network management update procedures, should be covered by general configuration management practices.

Maintain Documentation

We recommend documenting the network and changes that have occurred in the network in near real-time. You can use this precise network information for troubleshooting, network management tool device lists,

inventory, validation, and audits. We recommend using the following network documentation critical success factors:

- Current device, link, and end–user inventory
- Configuration version control system
- TACACS configuration log
- Network topology documentation

Current Device, Link, and End–User Inventory

Current device, link, and end–user inventory information enables you to track network inventory and resources, problem impact, and network change impact. The ability to track network inventory and resources in relation to user requirements helps ensure that managed network devices are actively used, provides information needed for audits, and helps to manage device resources. End–user relationship data provides information to define change risk and impact, as well as the ability to more quickly troubleshoot and resolve problems. Device, link, and end–user inventory databases are typically developed by many leading service provider organizations. The leading developer of network inventory software is Visionael Corporation . The database may contain tables for like devices, links, and customer user/server data so that when a device is down or network changes occur, you can easily understand the end–user impact.

Configuration Version Control System

A configuration version control system maintains the current running configurations of all devices and a set number of previous running versions. This information can be used for troubleshooting and configuration or change audits. When troubleshooting, you can compare the current running configuration to previous working versions to help understand if configuration is linked to the problem in any way. We recommend maintaining three to five previous working versions of the configuration.

TACACS Configuration Log

To identify who made configuration changes and when, you can use TACACS logging and NTP. When these services are enabled on Cisco network devices, the userid and timestamp is added to the configuration file at the time the configuration change is made. This stamp is then copied with the configuration file to the configuration version control system. TACACS can then act as a deterrent for unmanaged change and provide a mechanism to properly audit changes that occur. TACACS is enabled using the Cisco Secure product. When the user logs into the device, he/she must authenticate with the TACACS server by supplying a userid and password. NTP is easily enabled on a network device by pointing the device to an NTP master clock.

Network Topology Documentation

Topology documentation aids in the understanding and support of the network. You can use it to validate design guidelines and to better understand the network for future design, change, or troubleshooting. Topology documentation should include both logical and physical documentation, including connectivity, addressing, media types, devices, rack layouts, card assignments, cable routing, cable identification, termination points, power information, and circuit identification information.

Maintaining topology documentation is the key to successful configuration management. To create an environment where topology documentation maintenance can occur, the importance of the documentation must be stressed and the information must be available for updates. We strongly recommend updating topology documentation whenever network change occurs.

Network topology documentation is typically maintained using a graphics application like Visio . Other products like Visionael provide superior capabilities for managing topology information.

Validate and Audit Standards

Configuration management performance indicators provide a mechanism to validate and audit network configuration standards and critical success factors. By implementing a process improvement program for configuration management, you can use the performance indicators to identify consistency issues and improve overall configuration management.

We recommend creating a cross–functional team to measure configuration management success and improve configuration management processes. The first objective of the team is to implement configuration management performance indicators in order to identify configuration management issues. We'll discuss the following configuration management performance indicators in detail:

- Configuration integrity checks
- Device, protocol, and media audits
- Standards and documentation review

After evaluating the results from these audits, initiate a project to fix inconsistencies and then determine the initial cause of the problem. Potential causes include a lack of standards documentation or a lack of a consistent process. You can improve standards documentation, implement training, or improve processes to prevent further configuration inconsistency.

We recommend monthly audits, or possibly quarterly if only validation is needed. Review past audits to confirm that past problems are resolved. Look for overall improvements and goals to demonstrate progress and value. Create metrics to show the quantity of high–risk, medium–risk, and low–risk network configuration inconsistencies.

Configuration Integrity Checks

The configuration integrity check should evaluate the overall configuration of the network, its complexity and consistency, and potential issues. For Cisco networks, we recommend using the Netsys configuration validation tool. This tool inputs all device configurations and creates a configuration report that identifies current problems such as duplicate IP addresses, protocol mismatches, and inconsistency. The tool reports any connectivity or protocol issues, but does not input standard configurations for evaluation on each device. You can manually review configuration standards or create a script that reports standard configuration differences.

Device, Protocol, and Media Audits

Device, protocol, and media audits are a performance indicator for consistency in software versions, hardware devices and modules, protocol and media, and naming conventions. The audits should first identify any non–standard issues, which should lead to configuration updates to fix or improve the issues. Evaluate overall processes to determine how they could prevent suboptimal or non–standard deployments from occurring.

Cisco RME is a configuration management tool that can audit and report on hardware versions, modules and software versions. Cisco is also developing more comprehensive media and protocol audits that will report inconsistency with IP, DLSW, Frame Relay and ATM. If a protocol or media audit is not developed, you can use manual audits, such as reviewing devices, versions and configurations for all like devices in a network, or by spot checking devices, versions and configurations.

Standards and Documentation Review

This performance indicator reviews network and standards documentation to ensure that the information is accurate and up to date. The audit should include reviewing current documentation, recommending changes or additions, and approving new standards.

You should review the following documentation on a quarterly basis: standard configuration definitions, solution templates including recommended hardware configurations, current standard software versions, upgrade procedures for all devices and software versions, topology documentation, current templates, and IP address management.

Related Information

- [More Best Practices White Papers](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.