

Cisco Leading Practices: Cisco IOS Management Operations

Document ID: 27623

Contents

Abstract

Introduction

- Overview
- Objectives
- Audience
- Prerequisites

Creating a Cisco IOS Management Operations Strategy

- Identifying Deliverables
- Identifying Key Device Measurements

Defining Roles and Responsibilities

- Identifying Areas of Expertise Required
- Identifying Key Contributors
- Identifying Responsibilities
- Budgeting Resources

Following a Best Practice Cisco IOS Management Operations Process

- Software Version Control
- Fault Management
- Problem Management
- Configuration Standardization
- Availability Management

Cisco IOS Management Operations Checklist

Related Information

Cisco Services and Support

Abstract

Cisco Leading Practices are a set of codified documents that provide relevant and reliable guidance on networking operations for Cisco products and solutions. The leading practices are developed and supported by award-winning Cisco TAC and Advanced Services engineers who you can use to help create your own set of leading practices to emulate. Cisco customers have applied these leading practices in their network environment to gain network performance and availability.

It is highly recommended to supplement these leading practices with services from Cisco and its partners. For more information on how to optimize your network performance and availability, please contact your services sales representative about the Cisco Advanced Services website and find out more about the Network Optimization Support – Focused Engineering Support, Network Availability Improvement Support (NAIS), Software Management Process Assessment (SMPA), and NAIS–SMPA Implementation.

Introduction

Overview

Operational processes around software management can help reduce network complexity, decrease reactive support issues and improve problem resolution time. This document provides a strategy, tool

recommendations, and best–practices for the overall management of Cisco IOS® software (Cisco IOS).

The Creating a Cisco IOS Management Operations Strategy and Following a Best Practice Cisco IOS Management Operations Process sections in this document discuss the recommended methodology for getting started and lists the best tools to be used for the operations phase. The operations phase includes the best–practice processes for the following:

Process	Description
Software version control	Tracking, validating, and improving software consistency within the identified software tracks.
Fault management	Proactively monitoring and acting upon higher priority SNMP and Syslog messages generated by Cisco IOS.
Problem management	Quickly and efficiently collecting critical problem information for software related issues in order to help prevent future occurrences.
Configuration Standardization	Standardizing configurations to reduce the potential for untested code to be exercised in production and to standardize network protocol and feature behavior.
Availability management	Improving availability based on metrics, improvement goals, and improvement projects

This document assumes that you have implemented the following best–practice processes for the planning, design and implementation of Cisco IOS:

- Identified manageable software areas (software tracks) in your environment based on platform, module, feature, protocol, and topology requirements.
- Selected, certified, and communicated Cisco IOS versions per software tracks.
- Consistently implemented the standard Cisco IOS versions into each of the software tracks.

Objectives

This section assists you in managing and maintaining standardized Cisco IOS versions within defined tracks. You will learn how to:

- Develop a software version control process to ensure software version consistency within the identified software tracks.
- Monitor, notify, and resolve processes based on device fault management messages and alerts (SNMP/Syslog) to help proactively resolve potential software and fault issues.
- Efficient collection of critical problem information for software to help reduce problem resolution time for software–related issues.
- Standardize device configurations to help ensure protocol, feature, access, and security consistency for the environment.

Audience

This document is appropriate for individuals and managers with a technical orientation who are responsible for the daily operation of the network. The document describes how to establish operational processes to help you reduce network complexity, decrease reactive support issues and improve problem resolution time by building network consistency and by improving capabilities for proactive fault management.

Prerequisites

Those involved in Cisco IOS management operations should have a solid knowledge of network infrastructure design, and administration, particularly with Cisco equipment, and must have access to details of the target network's topology, device configuration, activity profile, application usage, and resource utilization policy. Access to, and experience with, information tools available on Cisco Connection Online (CCO), is also required. If you have not already registered with CCO, we suggest you do so for access to the tools described in this document.

Creating a Cisco IOS Management Operations Strategy

Many quality strategies and tools exist to help manage Cisco IOS environments. This chapter focuses on three key strategies for managing Cisco IOS operations in higher availability environments, and includes a matrix of key operational tools that are specifically helpful for managing Cisco IOS and Cisco IOS issues.

The first key strategy is to keep the environment as simple as possible, avoiding variation in configuration and Cisco IOS versions as much as possible. Cisco IOS certification has already been discussed, however configuration consistency is another key area. The architecture/engineering group should be responsible for creating configuration standards. The implementation and operations group then have the responsibility to configure the standards and maintain the standards through Cisco IOS version control and Cisco IOS configuration standards/control.

The second key strategy is the ability to identify and quickly resolve network faults. The operations group should generally identify network problems before users report them, and problems should be resolved as quickly as possible without further impacting or changing the environment. Two key best-practices in this area are problem management and fault management (both are discussed later in this document).

Note: The Cisco IOS stack decoder tool can be used to help quickly diagnose Cisco IOS software crashes.

The third key strategy is to consistently improve. The primary process is to improve a quality-based availability improvement program. By performing root-cause analysis on all issues, including Cisco IOS-related issues, an organization can improve test coverage, improve problem resolution times, and improve processes that will eliminate or reduce outage impact. The organization can also look at common problems and build processes to resolve those issues faster.

Identifying Deliverables

Deliverables from the Cisco IOS Software Management operation process include:

- Software version control processes and tools
- Fault management monitoring and processes
- Problem management processes
- Device configuration standards and audit processes
- Network availability methodology, reporting and review processes

Identifying Key Device Measurements

Metrics should be defined as part of the operations plan and used to determine if the tools and processes are producing the desired results. The following are some examples of useful Cisco IOS software management metrics:

- Network availability (due to software issues)
- % Cisco IOS version compliance to standard (on a per track basis)
- % Device configuration consistency (based on standards)
- Problem management metrics (MTTR, # tickets, Closure codes)

Defining Roles and Responsibilities

Identify, qualify, and assemble a cross-functional group of managers and/or leads from network architecture, network engineering, and implementation/ operations groups to help ensure the successful planning, design, implementation, and operations phases of your IOS upgrade projects.

Identifying Areas of Expertise Required

Assemble a cross-functional group of managers and/or leads from the network management, network engineering, implementation and operations groups to help with the operations phase of your Cisco IOS management project.

Identifying Key Contributors

- Network manager(s):

Manager(s) name, department, contact information

Primary backup name, department, contact information

Secondary backup name, department, contact information if required

- Network architect(s):

Architect(s) name, department, contact information

Primary backup name, department, contact information

Secondary backup name, department, contact information if required

- Network engineer(s):

Engineer(s) name, department, contact information

Primary backup name, department, contact information

Secondary backup name, department, contact information if required

- Network Operations (NOC) engineer(s):

Engineer(s) name, department, contact information

Primary backup name, department, contact information

Secondary backup name, department, contact information if required

Identifying Responsibilities

- Network manager(s) are responsible for:
 - ◆ Maintaining the Project Plan
 - ◆ Assigning/reassigning resources
 - ◆ Managing change control
 - ◆ Managing progress
 - ◆ Managing budget reporting
- Network architect(s) are responsible for:
 - ◆ Analyzing network standards and release caveats
 - ◆ Maintaining the Software Upgrade Matrix
 - ◆ Maintaining the Candidate Management Matrix
 - ◆ Maintaining the Memory Requirements Matrix
- Network (NOC) engineer(s) are responsible for:
 - ◆ Implementing and ensuring compliance to network standards
 - ◆ Identifying software problems and root causes
 - ◆ Recommending corrective action
 - ◆ Monitoring the network

Budgeting Resources

Resource requirements should be determined in the operations stage to support the software management strategy for the organization. This will include the required personnel time and capital expenditures needed to support the software strategy.

In many cases, a Return on Investment (ROI) or budgetary plan for software management practices can be generated based on the cost of downtime and availability requirements. If the organization can determine downtime due to software problems, then a majority of this cost can be offset via the identified software management best-practices. If the cost cannot be completely offset, then the organization should consider a more basic software management strategy that will help to improve productivity by preventing additional rework as a result of software problems.

Following a Best Practice Cisco IOS Management Operations Process

Best practices for following an Cisco IOS Management Operations process include:

Best Practice	Detail
Software Version Control	Implementing only standardized software versions and monitoring the network to validate or possibly change software due to non-version compliance.
Fault Management	SNMP & Syslog message collection, monitoring and analysis are fault management processes recommended to resolve more Cisco IOS specific network problems that are difficult or impossible to identify any other way.

Problem Management	Detailed problem management processes that define problem identification, information collection, and a well-analyzed solution path. This data is used to determine root-cause.
Configuration Standardization	Configuration standards represent the practice of creating and maintaining standard global configuration parameters across like devices and services resulting in enterprise wide global configuration consistency.
Availability Management	Quality improvement using network availability as the quality improvement metric.

Software Version Control

Software version control is the process of implementing only standardized software versions and monitoring the network to validate or possibly change software due to non-version compliance. In general, software version control is accomplished using a certification process and standards control. Many organizations publish version standards on a central web server. In addition, an implementation staff is trained to review what version is running and to update the version if it is not standards compliant. Some organizations have a quality gate process where secondary validation is completed through audits to ensure that the standard is followed during implementation.

During network operation, it is also not uncommon to see non-standard software versions in the network, especially if the network is big with a large operations staff. This may be due to one of the following:

- Untrained newer staff
- Mis-configured boot commands
- Unchecked implementations

It is recommended to periodically validate software version standards using tools such as CiscoWorks2000 Resource Manager Essentials (RME) that can sort all devices by Cisco IOS version. When a non-standard version is identified, it should be immediately flagged and a trouble ticket or change ticket be initiated to bring the version to the identified standard.

Available Tools

CiscoWorks2000 RME Inventory manager greatly simplifies the Cisco IOS version management of Cisco routers and switches through web-based reporting tools that report and sort devices based on software version, device platform, and device name.

Fault Management

Fault management is the process of collecting, monitoring and analyzing SNMP and Syslog messages to resolve more Cisco IOS specific network problems that are difficult or impossible to identify any other way.

SNMP Trap Collection

SNMP trap collection and notification is a basic process in fault management used to identify software or hardware events and/or crashes without SNMP polling overhead or delay incurred from polling intervals. Trap

messages are generated directly from the network device to a network management system that provides notification services. The collection and notification of these traps is essential to rapid resolution of many network events including non user–impacting events such as the loss of primary devices or links in a redundant environment.

In order to collect and monitor these traps, the traps must be properly configured on the device as well as the network management systems. The network management systems should alert the network operations group when a trap has been received. Notification can then occur in the form of paging, e–mail or event screens in a NOC environment.

Regardless of how the data is presented, these fault instances, or exceptions, must be analyzed and reviewed on a regular basis (daily preferably) by the network operations and/or network support staff. The causes of all exceptions found should be investigated. Some logged exceptions may not be critical enough to immediately raise an alarm in the Network Operations Center. Proactive review, investigation and resolution of minor exceptions can help network support groups to reduce or prevent network outages.




Syslog Message Collection



Syslog messages are sent by the device to a collection server. These messages can be hardware or software errors or they can be informational (such as when someone has been in configure terminal on a device).

Syslog monitoring requires Network Management System (NMS) tool support or scripts to help parse and report on Syslog data. This includes the capability to sort Syslog messages by date or time period, device, Syslog message type or message frequency. In larger networks, tools or scripts may be implemented to parse Syslog data and send alerts or notifications to event management systems or operations and engineering personnel. If alerts for a wide variety of Syslog data are not used, the organization should review higher priority Syslog data at least daily and create trouble tickets for potential problems. In order to proactively detect network problems that may not be seen through normal monitoring, periodic review and analysis of historical Syslog data should be performed to detect situations that may not indicate an immediate problem, but may provide an indication of a problem before it becomes service impacting.

Available Tools

Some of the more popular SNMP Trap receiver tools include the following:

- HP OpenView Network Node Manager from Hewlett Packard at openview.hp.com 
- Spectrum Integrity from Aprisma at www.aprisma.com 
- NetView from IBM Tivoli at www.tivoli.com 

The most popular Syslog tool for Cisco IOS management is CiscoWorks2000 RME Syslog manager. Other available tools include SL4NT, a shareware program from www.netal.com  leaving cisco.com and Private I from OpenSystems at www.opensystems.com 

Problem Management

Problem management, an aspect of fault management, is the discipline of managing problems from time of occurrence through identification, troubleshooting, resolution and closure.

Many customers experience additional downtime due to a lack of processes in problem management. Additional downtime can occur when network administrators try to resolve the problem quickly using a combination of service–impacting commands or configuration changes rather than spending time on problem identification, information collection, and a well–analyzed solution path. Observed behavior in this area includes reloading devices or clearing IP routing tables before investigating a problem and its root cause. In some cases this occurs because of first level support problem resolution goals. The goal in all software related

issues should be to quickly collect the necessary information needed for root-cause analysis before restoring connectivity or service.

A problem management process is recommended, and should include a certain degree of default problem descriptions and appropriate show command collections before escalating the problem to a second level of support. First level support should never include clearing routes or reloading devices. Ideally, the first level support organization should quickly collect information and then escalate the problem to second level support. By spending a little more time identifying and describing the problem in level one support, a root-cause discovery is much more likely, thus allowing a workaround, lab identification, and bug reporting. Second level support should be well versed in the types of information that Cisco may need to diagnose a problem or file a bug report, including:

- Memory dumps
- Routing information output
- Device show command output

Configuration Standardization

Global device configuration standards represent the practice of maintaining standard global configuration parameters across like devices and services resulting in enterprise wide global configuration consistency. Global configuration commands are commands that apply to the entire device and not to individual ports, protocols or interfaces, and generally impact device access, general device behavior and device security. In Cisco IOS, this includes the following commands:

- Service
- IP
- VTY
- Console port
- Logging
- AAA/TACACS+
- SNMP
- Banner

Also important in global device configuration standards is an appropriate device naming convention that allows administrators to identify the device, device type and device location based on the DNS name of the device. Global configuration consistency is important to the overall supportability and reliability of a network environment because it helps reduce network complexity and enhance network supportability. Support difficulty is often experienced without configuration standardization due to incorrect or inconsistent device behavior, SNMP access, and general device security.

Maintaining global device configuration standards is normally accomplished by an internal engineering or operations group that creates and maintains global configuration parameters for similar network devices. It is also a good practice to provide a copy of the global configuration file in TFTP directories so that they can be initially downloaded to all newly provisioned devices. Also helpful is a web accessible file that provides the standard configuration file with an explanation of each configuration parameter. Some organizations configure all like devices on a periodic basis to help ensure global configuration consistency, or periodically review devices for the correct global configuration standards.

Interface or protocol configuration standards represent the practice of maintaining standards for interface and protocol configuration, which improves network availability by reducing network complexity, providing expected device and protocol behavior and improving network supportability. Interface or protocol configuration inconsistency can result in unexpected device behavior, traffic routing issues, increased connectivity problems and increased reactive support time.

Interface configuration standards may include:

- CDP (Cisco discovery protocol)
- Interface descriptors
- Caching configuration
- Other protocol specific standards

Protocol specific configuration standards may include:

- IP routing configuration
- DLSW configuration
- Access-list configuration
- ATM configuration
- Frame Relay configuration
- Spanning Tree configuration
- VLAN assignment & configuration
- VTP (Virtual Trunking Protocol)
- HSRP (Hot Standby Routing Protocol)
- Others depending on what is configured within the network

An example of IP standards may include subnet size, IP address space used, routing protocol used and routing protocol configuration.

Maintaining protocol and interface configuration standards is normally the responsibility of the network engineering and implementation groups. The engineering group should be responsible for identifying, testing, validating and documenting the standards. The implementation group is then responsible for using the engineering documents or configuration templates to provision new services. The engineering group should create documentation on all aspects of required standards to ensure consistency. Configuration templates should also be created to help enforce the configuration standards. Operations groups should also be trained on the standards and should be able to identify non-standard configuration issues. Configuration consistency is of great assistance in the testing, validation, and certification phase. Without standardized configuration templates, it is nearly impossible to adequately test, validate, or certify an Cisco IOS version for a moderately large network.

Availability Management

Availability management is the process of quality improvement using network availability as the quality improvement metric. Many organizations are now measuring availability and outage type. Outage types may include the following:

- Hardware
- Software
- Link/carrier
- Power/environment
- Design
- User-error/process

By identifying outages and performing root-cause analysis immediately following recovery, the organization can identify methods to improve availability. Almost all networks that have achieved high availability have some type of quality improvement process in place.

Cisco IOS Management Operations Checklist

- Step 1: Define Business Requirements and Goals (registered customers only)**
- Step 2: Assess Current Status of Cisco IOS Software Management Practices (registered customers only)**
- Step 3: Define Roles and Responsibilities (registered customers only)**
- Step 4: Develop a Software Management Project Plan (registered customers only)**
- Step 5: Develop a Software Requirements Matrix (registered customers only)**

Related Information

An appendix has been created to aid the customer in obtaining other valuable Cisco IOS related information such as: Cisco IOS fundamentals, Cisco internal Cisco IOS software processes, software reliability analysis, Cisco internal quality program, Cisco internal testing methodologies, and a field analysis that shows current industry practices and overall customer experiences with Cisco IOS software

- Cisco IOS Management: Additional information on Cisco IOS management and best practices can be found in the Cisco IOS Management for High Availability Networking white paper at the following site:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a00800a998b.shtml
- For specific information on how to run network probes, which CLI commands to use, how to analyze and interpret network traffic data, and how to establish application usage policies, visit <http://www.cisco.com>. This site provides a comprehensive range of support, training, technical reference, and consulting solutions.
- Cisco IOS has specific naming conventions that are defined here:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a0080101cda.shtml
- Information about Cisco IOS release availability is provided here:
http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- Cisco IOS releases are eventually removed from CCO and can no longer be ordered. Please be sure to set customer expectations accordingly.
- Cisco IOS product bulletins are used to announce Cisco IOS releases to customers. They contain brief information about the release content. Check here for availability of new Cisco IOS releases
http://www.cisco.com/en/US/products/sw/iosswrel/products_ios_cisco_ios_software_releases.html
- The Product Security Incident Response Team handles security for Cisco products. Any Cisco IOS security related issues should be referred to this team. Cisco publicly publishes it's security vulnerabilities. <http://tools.cisco.com/security/center/publicationListing>
- Cisco IOS Defects: Serious Cisco IOS defects should be recommended for deferral. Any Cisco employee may make the recommendation.
- Field issues on Cisco IOS are communicated to the customers through Cisco IOS advisories.
http://www.cisco.com/en/US/products/products_security_advisory09186a0080b20ee1.shtml
- Cisco IOS Features: The Feature Navigator tool enables customers to find releases that support specific features, and vice versa. <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>
- The Cisco Software Advisor enables customers to find software support for features or software support for hardware. <http://tools.cisco.com/Support/Fusion/FusionHome.do> (registered customers only)

Cisco Services and Support

- **Technical Support Services**
 - **Services specific to Cisco networking technologies and solutions**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 21, 2006

Document ID: 27623
