Managing Cisco Catalyst Fixed-Configuration Switches

Contents

1 Abstract 2
2 Introduction 2
2.1 CiscoWorks LMS and CiscoWorks NCM 3
2.1.1 CiscoWorks LMS 3
2.1.2 CiscoWorks NCM 3
3 Mapping CiscoWorks LMS and NCM to the FCAPS Model 4
4 Fault Management 5
4.1 Trap Management 6
4.1.1 Using CiscoWorks DFM with HP OpenView 6
4.2 Syslog Management 6
4.2.1 Using CiscoWorks RME as a Syslog Analyzer Tool 7
4.3 Troubleshooting 8
5 Configuration Management 8
5.1 Switch Configuration Management Using CiscoWorks 9
5.1.1 Using CiscoWorks NCM 9
5.1.2 Using CiscoWorks LMS 10
5.2 Inventory Management 12
5.3 Software Image Management 13
5.4 VLAN Management 14
5.5 Spanning Tree Management 15
6 Accounting 18
6.1 Government and Corporate Compliance 18
6.1.1 Tracking Configuration Changes 19
6.1.2 Configuration and Software Policies 19
6.2 Change Audits 22
6.3 Discovering Switches 23
6.3.1 Capacity Planning 23
7 Performance Management 24
7.1 IP/SLA 24
7.2 Real-Time Statistics Using CiscoView 25
8 Security 26
8.1 Integrating with AAA Server 26
9 Feature Management 27
10 Conclusion 28
11 Appendices 28
11.1 Appendix A: Switch Feature Management Detail 28
11.1.1 For Stack: Enabling Persistent MAC Address 28
11.1.2 Changing Address Aging Time 28
11.1.3 MAC Address Notification Trap 28
11.1.4 Unicast MAC Address Filtering 29
11.1.6 Configuring Switch Database Management Templates 29
11.1.7 Configuring TACACS+ 30
11.1.8 Configuring SSH 30
11.1.9 Configuring a Certificate Authority Trustpoint 30
11.1.10 SmartPort Macro 30
11.1.11 Configuring 802.1x Authentication 30
11.1.12 Configuring PVLANs 31
11.1.13 Configuring MSTP 31
11.1.14 DHCP Snooping 31
11.1.15 IP ARP Inspection 31

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

11.1.16 Configuring Mini-RMON on Desktop Switches 32
11.1.17 Configuring SNMP..... 33
11.1.18 Configuring Cisco EtherChannels 33
11.1.19 Maintenance Management..... 34
11.1.20 Configuring Health Monitoring..... 34
11.1.21 Starting Online Diagnostics 35
12 References..... 35
12.1 LMS References on Cisco.com 35
12.2 Cisco Press Books 36
12.3 Wikipedia Definition of FCAPS 36

1 Abstract

Maintaining a low total cost of ownership (TCO) with limited resources and within increasingly complex networks is a common challenge for today's IT managers. Effective management tools are needed to take advantage of switching solutions while keeping TCO down.

Network management solutions can help control an ever-growing network infrastructure. Unauthorized or unaccounted-for configuration changes can contribute to substantial network downtime. Without effective network management, large portions of an IT budget can be spent on maintenance and operations; causing IT initiatives to be delivered late or compromised. IT managers can use tools such as CiscoWorks LAN Management Solution (LMS) and CiscoWorks Network Compliance Manager (NCM) to address these challenges.

This white paper discusses several aspects of network management. It focuses on managing fixed-configuration switches, such as the Cisco® Catalyst® 3750E and 3560E Series, and discusses how CiscoWorks LMS and NCM can be deployed to meet a wide variety of switch management needs.

2 Introduction

Network management can be divided into five areas: fault, configuration, accounting, performance, and security management. This is also known as the FCAPS model. Unlike the OSI model, in the FCAPS model, each component can operate independently.

Following is a brief description of the FCAPS model:

- Fault management: Network faults and problems are identified and fixed.
- Configuration management: Network hardware and software are tracked; modifications are made while archiving older configurations.
- Accounting management—Network resource usages are tracked for billing or audit purposes.
- Performance management—Network performance statistics are measured. Congestion and bottlenecks are identified and minimized.
- Security management—Not all malicious network attacks originate outside an organization; access to specific network resources is limited to authorized people.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

2.1 CiscoWorks LMS and CiscoWorks NCM

CiscoWorks LMS and NCM are part of the Cisco Proactive Automation of Change Execution (PACE) solution. This solution combines products and services that accelerate operational success by helping IT organizations to securely automate and control configuration and change management in their networks. Cisco PACE helps enterprises meet compliance requirements, ensure business continuity, and increase user productivity. The solution is optimized to help enterprises with challenges concerning compliance, in-house expertise, network complexity, and growth.

2.1.1 CiscoWorks LMS

CiscoWorks LMS is an integrated suite of applications for administering, monitoring, and troubleshooting Cisco networks. It provides a solid foundation of infrastructure management capabilities so that IT organizations can efficiently manage business-critical networks.

CiscoWorks LMS contains the following applications:

- CiscoWorks Resource Manager Essentials (RME): Provides the tools needed to manage Cisco devices. It includes inventory and device change management, network configuration and software image management, network availability, and syslog analysis.
- CiscoWorks Campus Manager: A suite of Web-based applications designed for managing networks powered by Cisco switches. These include Layer 2 device and connectivity discovery, workflow application server discovery and management, detailed topology views, end-station tracking, Layer 2 and 3 path analysis tools, and IP phone user and path information.
- CiscoWorks Device Fault Manager (DFM): Provides real-time fault analysis for Cisco devices. It generates “intelligent” Cisco traps through a variety of data collection and analysis techniques. The traps can be locally displayed, e-mailed, or forwarded to other popular event management systems.
- CiscoWorks Internetwork Performance Monitor (IPM): A network response time and availability troubleshooting application. This tool empowers network engineers to proactively troubleshoot network performance using real-time and historical reports.
- CiscoWorks CiscoView: A Web-based tool that graphically provides real-time status of Cisco devices. The tool can display detailed monitoring information on interfaces and access configuration functions.
- CiscoWorks Common Services: Provides common management desktop services and security across CiscoWorks solutions. It includes the CiscoWorks LMS Portal, a new homepage and portal framework that can be customized to meet your individual management needs, and CiscoWorks Assistant, a new workflow engine for quick troubleshooting of network problems.

2.1.2 CiscoWorks NCM

CiscoWorks NCM is a Web-based network management application that tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides superior visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements. CiscoWorks NCM helps IT staff identify and correct trends that could lead to problems such as network instability and service interruption.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

CiscoWorks NCM helps users meet regulatory compliance goals, such as the Payment Card Industry (PCI) data security standard, Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act of 1999 (GLBA), Sarbanes-Oxley (SOX) Act, and Information Technology Infrastructure Library (ITIL), in several ways:

- Tracks all changes to the network (configuration, software, and hardware changes) in real time and captures them in a detailed audit trail.
- Screens all changes against authorized policies immediately to verify that they comply with regulatory requirements or IT best practices.
- Automatically validates new changes against appropriate policies before they are pushed to the network. If the changes are not compliant, CiscoWorks NCM does not allow them to be deployed.
- Automates the change review process, closing the gap between the approval of a change and the actual configuration change that is pushed to the network.
- Allows managers to enforce the approval of a change through a flexible, integrated approval model, using the exact configuration code that will be pushed to the network. Approvers of a change can review the change in the context of the entire device configuration and the business units it will affect. Event notifications are sent to interested parties, giving network staff immediate visibility into unplanned and unauthorized changes.
- Limits network configuration information to users on a need-to-know basis. CiscoWorks NCM uses highly customizable role-based permissions to control what information a user can view, what actions a user can perform on devices, and which devices a user can gain direct access to.
- Ships with regulatory reports for SOX, HIPAA, GLBA, PCI and ITIL, providing the detailed metrics required by each of these regulations and providing the network information necessary to prove compliance.

Table 1 highlights the overall capabilities of CiscoWorks LMS and NCM.

Table 1. CiscoWorks LMS and NCM

Product	Discovery and Vizualization	Regulatory and Best Practice Compliance Management and Audit	Device Configuration and Change Management	Device Fault Monitoring	Multi Vendor Support
NCM	X	X	X Large networks	–	Cisco and Other Vendors
LMS-RME	–	–	X Enhanced syslog analysis	–	Cisco
LMS (Other applications)	X	–	–	X Fault monitoring, user tracking and IPSLA monitoring	Cisco

3 Mapping CiscoWorks LMS and NCM to the FCAPS Model

CiscoWorks LMS and NCM can systematically manage a Cisco network by using an industry-standard approach to FCAPS.CiscoWorks LMS is modular; each module addresses a specific aspect of network management. Table 2 shows how LMS modules and NCM align with the FCAPS model.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

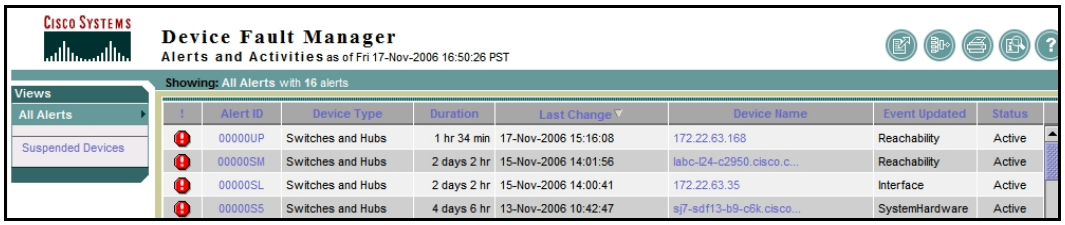
Table 2. FCAPS by LMS and NCM

FCAPS Element	Corresponding CiscoWorks LMS/NCM Tools
Fault management (F)	LMS: Device Fault Manager (DFM) LMS: Device Center (for troubleshooting)
Configuration management (C)	LMS: Resource Manager Essentials (RME) LMS: Campus Manager LMS: Cisco View NCM collects and archives configurations. It can also deploy configurations using its powerful scripting features.
Accounting (A)	LMS: Campus Manager (user tracking) LMS: RME (inventory, change audit, and reports) NCM: Track configuration changes and user sessions CiscoWorks LMS and NCM can also be combined with Cisco Access Control Server (ACS) to provide detailed audit information.
Performance (P)	LMS: Internet Performance Monitor (IPM) LMS: DFM LMS: CiscoView (real-time performance only)
Security (S)	LMS relies on Secure Sockets Layer (SSL), Secure Shell (SSH), Secure Copy (SCP), Simple Network Management Protocol (SNMP) v3, Cisco ACS integration (authentication and authorization), and security audits. NCM supports authentication using Lightweight Directory Access Protocol (LDAP); authentication, authorization, and accounting (AAA); and Secure ID. Security view, user roles and permissions, are built into NCM to enforce security in network management.

4 Fault Management

Fault management refers to tracking and notifying network administrators of potentially disruptive occurrences as they occur within the network. Traps and syslog messages are a common mechanism whereby the switches notify the network management system as soon as an event occurs. CiscoWorks LMS takes a proactive approach to fault management. CiscoWorks DFM proactively polls the network, compares the results with the predefined (yet customizable) thresholds, and generates an alert if the poll value exceeds the threshold (Figure 1).

Figure 1. CiscoWorks LMS DFM Alerts and Activities



All these thresholds are predefined for different devices and their interfaces. Once the user installs the LMS server and populates the device repository, LMS will start to report alerts and activities on the network. The user can also easily adjust the threshold values and the views.

With CiscoWorks DFM, the administrator can see not only current events, but also historical events and alerts. This helps users access the historical reports within a time period related to a switch, providing a deeper perspective of the possible cause of failure. Administrators can see the complete history of the fault to identify how long this condition has existed in the network, and take appropriate action (Figures 2 and 3).

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 2. CiscoWorks LMS DFM Fault History

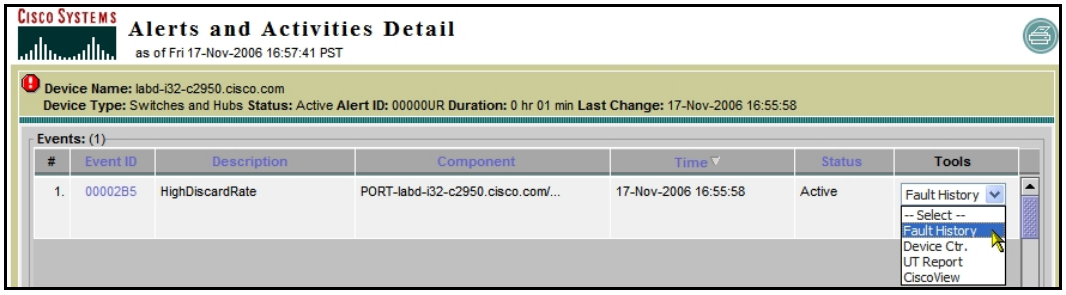
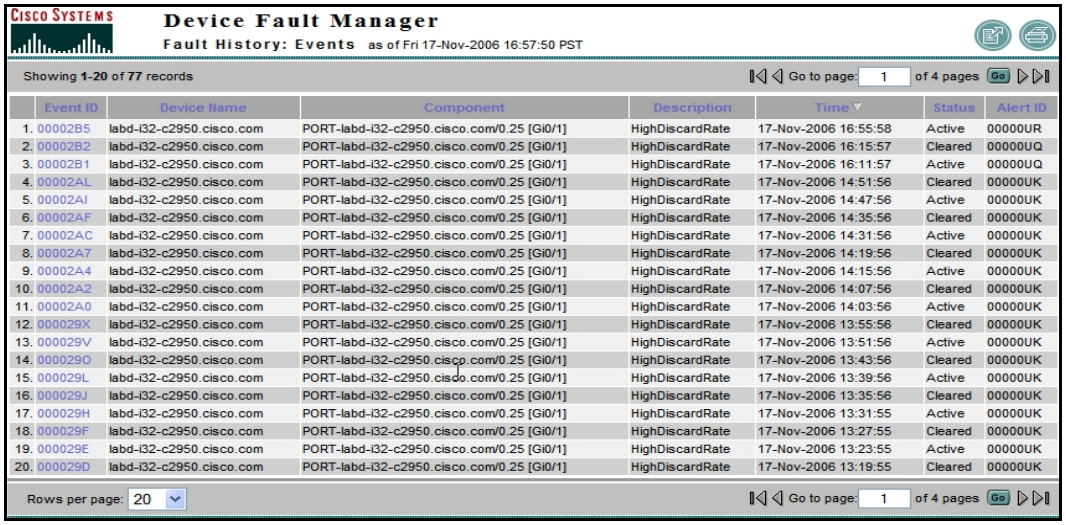


Figure 3. CiscoWorks LMS DFM Fault History



In addition to watching network conditions as they change, you can use notification services to automatically notify users and other systems when specific changes occur on the switches. The forwarded notification could be an e-mail notification, DFM-generated SNMP trap notification, or syslog message. You can also change system-defined event names to names that are more meaningful to you; these names will be reflected in the DFM displays and notifications. Since DFM works right out of the box, it simplifies the mundane task of setting up the software to track faults on your network.

4.1 Trap Management

CiscoWorks DFM can generate a trap from SNMP polling, and can process the traps that are generated from the switch.

4.1.1 Using CiscoWorks DFM with HP OpenView

CiscoWorks DFM integrates with other “managers of managers” (MoMs) such as HP OpenView or IBM Tivoli, so that pass-through traps are forwarded onto the MoM without being processed.

4.2 Syslog Management

Syslog is considered one of the better ways to keep track of the faults in the network. Some network managers like the level of detail and choose to track syslogs instead of SNMP traps. CiscoWorks LMS has a built-in syslog server that runs in the background, collecting syslogs from a wide variety of Cisco switches.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

4.2.1 Using CiscoWorks RME as a Syslog Analyzer Tool

Imagine troubleshooting a particularly transient problem. If that problem generates a syslog, you could catch it in action. CiscoWorks RME collects and parses the syslog, and the Syslog Analyzer module within RME can then generate notifications. Figures 4 and 5 show how CiscoWorks RME can be used to analyse syslog.

Figure 4. CiscoWorks LMS RME: Define New Message Type

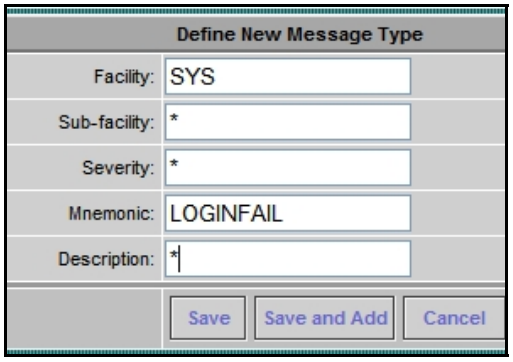
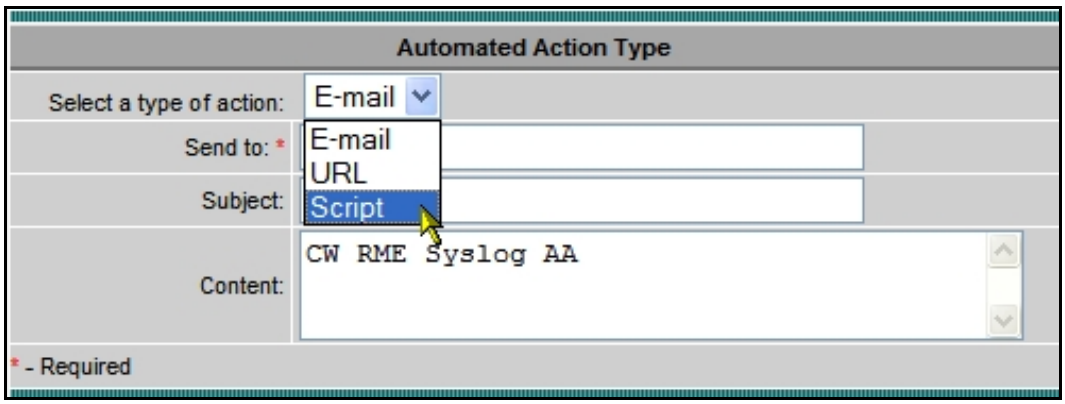
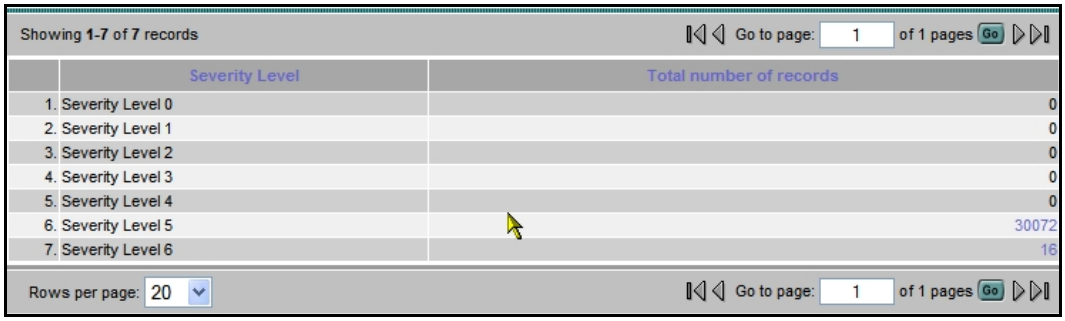


Figure 5. CiscoWorks LMS RME: Automated Action for Syslog Messages



CiscoWorks RME can also generate customized reports based on collected syslogs as shown in Figure 6.

Figure 6. CiscoWorks LMS RME: Customized Syslog Report

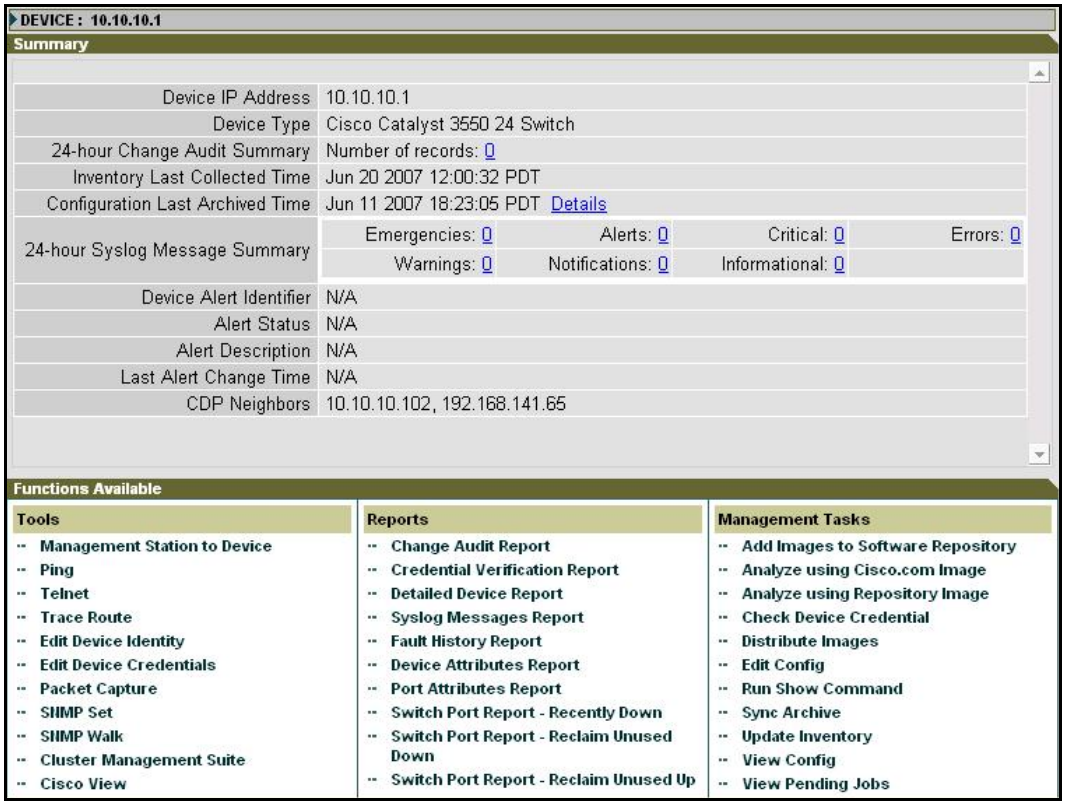


All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

4.3 Troubleshooting

Once the fault has been identified, the next step is to find its cause. CiscoWorks LMS can be used to troubleshoot a variety of network issues. Generic tools such as Ping, TraceRoute, Sniffer Trace, and Reachability come bundled with the application. These tools can be accessed using a GUI or are available at a central dashboard called the Device Center (Figure 7). Once the switch has been selected, all the tools are automatically available for that switch.

Figure 7. CiscoWorks LMS Device Center



5 Configuration Management

Corporate environments continue to become more regulated. The corporate sector must comply with several regulations that require switch configurations to be archived. This can prove challenging for large organizations with thousands of switches in the network.

Configuration management is the process of monitoring configuration changes (hardware or software) throughout the network. This process entails archiving configurations, accurately tracking configuration changes, and being able to quickly deploy a particular configuration to multiple switches. Hardware-related changes could involve inserting a new power supply module into a switch. Software changes could include upgrading the Cisco IOS Software on the switches, or making configuration changes on the switch itself; for example, changing the SNMP community strings or enabling passwords.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Table 3 shows how and when CiscoWorks LMS and NCM can be used to meet an organization's corporate configuration management needs.

Table 3. CiscoWorks LMS and NCM Management Tasks for Configuration Management

Configuration Management Task	LMS	NCM
Basic configuration management	X	X
Advanced and bulk (parameterized and scripting) configuration management	–	X
Creating and checking basic corporate policies	X	X
Automating government agency compliance (SOX, VISA PCI, HIPAA, GLBA, ITIL, Cobit, and COSO)	–	X
Configuration management for non Cisco hardware	–	X

5.1 Switch Configuration Management Using CiscoWorks

5.1.1 Using CiscoWorks NCM

Studies have shown that most network outages are due to manual misconfiguration. It is becoming important to automate configuration deployment jobs involving large number of switches or mundane tasks that must be repeatedly executed, such as password deployment or single-line access control list (ACL) changes. This helps to considerably reduce the manual handling of routine configuration tasks, which in turn reduces manual errors. CiscoWorks NCM offers a variety of automation capabilities, including configuration templates, parameterized scripts, and advanced command scripting capabilities. This increases the stability of the network, engineering efficiency and effectiveness.

Deploying Configurations to a Large Number of Switches

Pushing out individual configurations to large number of switches is tedious, error-prone, and time-consuming. CiscoWorks NCM scripting capabilities can automate configuration deployment.

In CiscoWorks NCM, a small set of CLI commands known as a "configlet" can be created and deployed to a large number of switches using simple command scripts. A command script offers a high degree of versatility in configuration tasks. One example is to assign different values for the same configuration parameter on different switches. A senior engineer, for example, can create a command script and even specify prompts and limit the values that can be assigned to the variables. Then while deploying the script, a junior operator can pick the right values for the variables and deploy the scripts. A CSV file can be used to deploy the same script to multiple devices when the variables for each device are different.

The script deployment can be restricted to authorized users. For example, an "interface up/down" script can be created and relatively inexperienced night shift operators could be authorized to just run this script. The operator can simply select the interface that needs to be shut down or activated and confirm the change. At the same time, the system will prevent this person from inadvertently making other changes that could bring down the network.

CiscoWorks NCM can also includes approval chains. If an approval workflow is set up, the configuration deployment task will be queued for approval. The task can also be scheduled to run at a particular time, such as during a maintenance window. NCM offers an activity calendar where scheduled tasks can be viewed.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Advanced Command Scripts

Similar to the basic command scripts described above, CiscoWorks NCM also enables users to create and execute scripts in advanced scripting languages such as Perl and Expect. NCM allows up to six different scripting languages at a time in the system. If a corporation already has scripts to manage the network, these can be integrated into NCM, standardized across the organization, and made available to all authorized users.

Another way to create an advanced command script is from a Telnet/SSH proxy session log. CiscoWorks NCM can act as a Telnet/SSH proxy. Instead of logging into the switch directly, users can connect to the switch via the proxy using their favorite Telnet or SSH client. Since NCM already has the credentials to log into the switch, this offers users a single sign-on (SSO) experience. Once the user connects to the switch and configures commands, they can return to NCM and look at the complete session log. This log can then be converted into a Perl or Expect script, which in turn can be deployed to hundreds of other switches.

Automating Routine Tasks

CiscoWorks NCM provides several prebuilt scripts to automate routine tasks such as configuring syslog, deploying passwords and community strings, or adding a line to an ACL that will unapply the ACL,add the line and then reapply the ACL as recommended by Cisco.

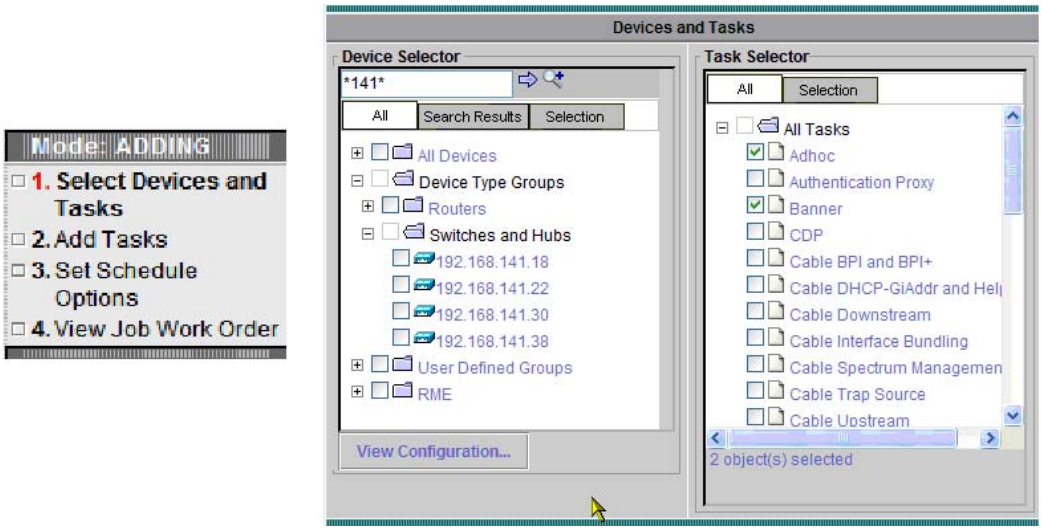
Handling Failure in Tasks

CiscoWorks NCM provides the ability to create advanced workflows to handle failure conditions. For example, if the configuration deployment fails, an e-mail message, syslog message, or SNMP trap can be sent to notify the appropriate persons or management tools. An automatic task can be scheduled to roll back the switch configuration. NCM also provides integration with ticketing systems such as Remedy through its open APIs. This allows trouble tickets to be opened or updated based on task status.

5.1.2 Using CiscoWorks LMS

CiscoWorks LMS NetConfig helps to push out configuration changes to multiple switches. The NetConfig wizard can be used to make scheduled configuration changes (Figure 8).

Figure 8. CiscoWorks LMS RME: NetConfig

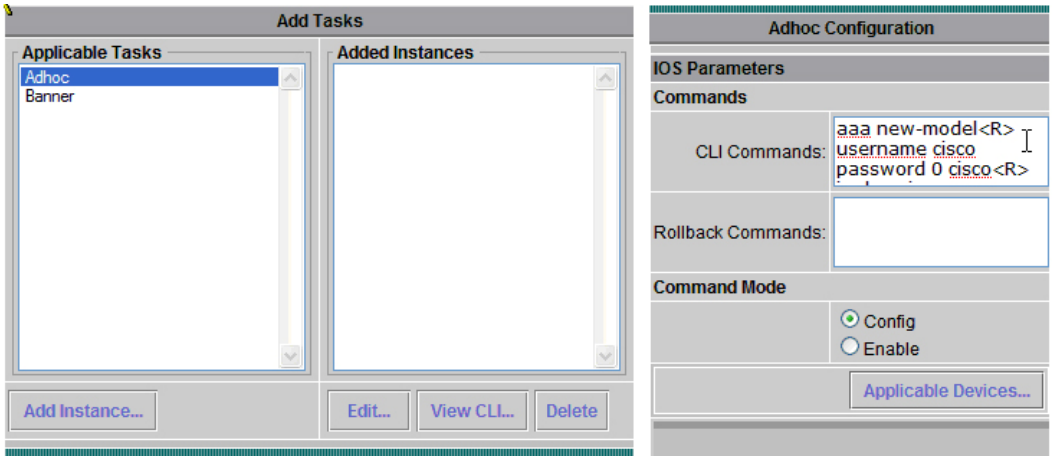


All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Switches can be selected using wildcards as shown in Figure 8. Once the switches are selected, you can select the template for the task or configuration change to be deployed on these switches. For example, if a banner needs to be added or modified on one or more switches, one could select the “Banner” template. With preconfigured templates, users do not need to enter the CLI command to execute the tasks. Users can select multiple types of switches in a single NetConfig job.

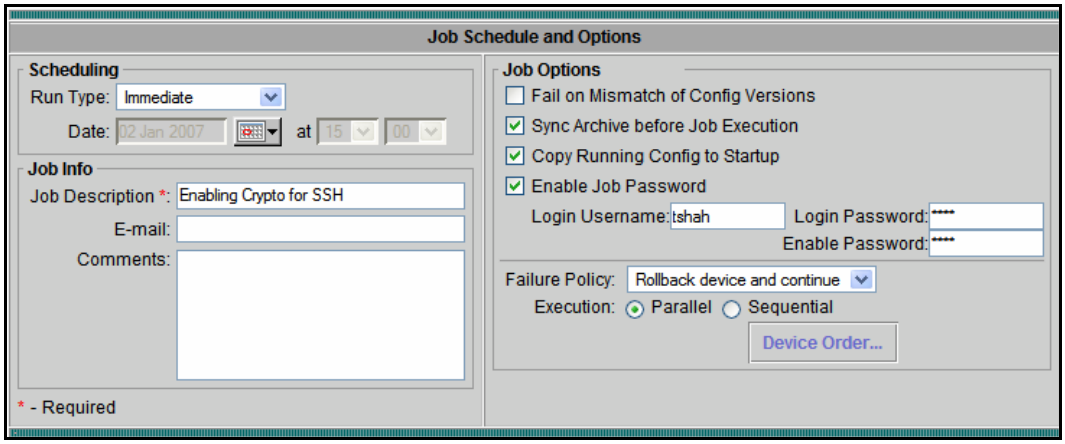
If a task or configlet needs to be deployed to multiple switches but doesn’t exist in the list, you can create your own template using the “Adhoc” template (Figure 9). In order to support interactive commands “<R>“ can also be used to pass hard returns. You can enter multiline commands as part of user-defined and Adhoc tasks. The multiline commands must be within the tag <MLTCMD> and </MLTCMD>. Once the template is selected, you need to instantiate the selected templates with data that needs to be pushed out to the switches.

Figure 9. CiscoWorks LMS RME: NetConfig Adhoc Configuration



In case of Adhoc templates, the data is the actual configuration that needs to be pushed to the switches. NetConfig cannot validate the configuration. You can click “View CLI” to view the actual configurations that will be pushed to the switches. Figure 10 shows job scheduling for configuration changes. Changes to multiple switches can be executed immediately or can be scheduled to deploy once or in a recurring fashion during a later time, perhaps during a maintenance window.

Figure 10. CiscoWorks LMS RME: NetConfig Job Schedule



All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

NetConfig also includes various failure policy options that can be used if the syntax is incorrect or the configuration job fails for another reason. Some of these options can be executed as prerequisites before deploying the configuration, and some can be done after a job has been successfully completed (such as reloading the switches). NetConfig can also follow the approval cycle that corporate policy might mandate.

5.2 Inventory Management

The CiscoWorks LMS RME module can effectively keep track of all Cisco hardware and software in your network. RME does this by polling each switch for a thorough collection of its inventory. The polled data is stored in the database so that reports on such inventory collection can be run at a later time. Figures 11 and 12 show hardware and software distribution in the network. The report in Figure 11 indicates different versions of software images currently deployed in the network; this can be useful in case of a security advisory, or simply to standardize a particular version of an image networkwide.

Figure 11. CiscoWorks LMS RME: Software Distribution Inventory

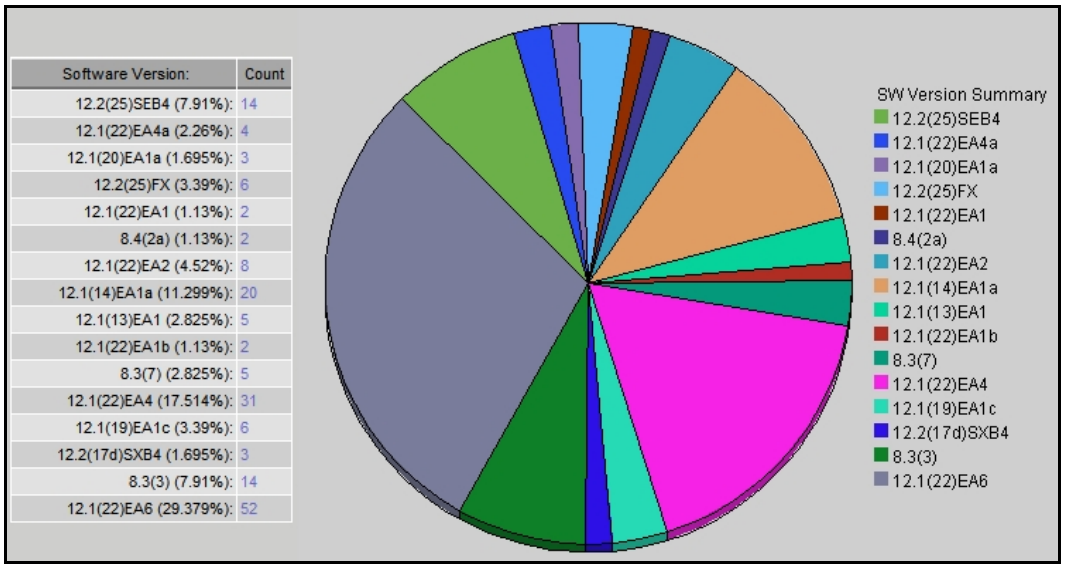
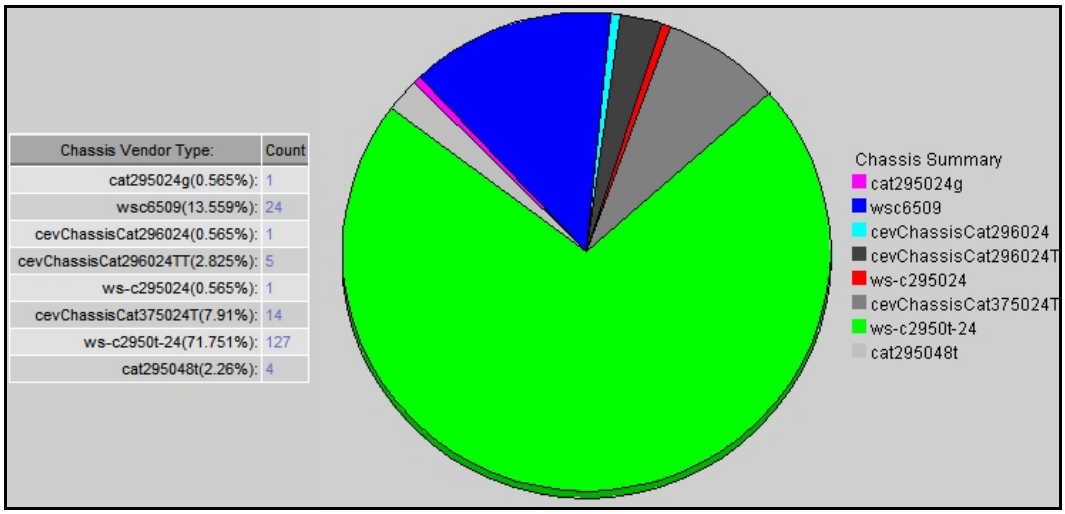


Figure 12. CiscoWorks LMS RME: Hardware Distribution Inventory



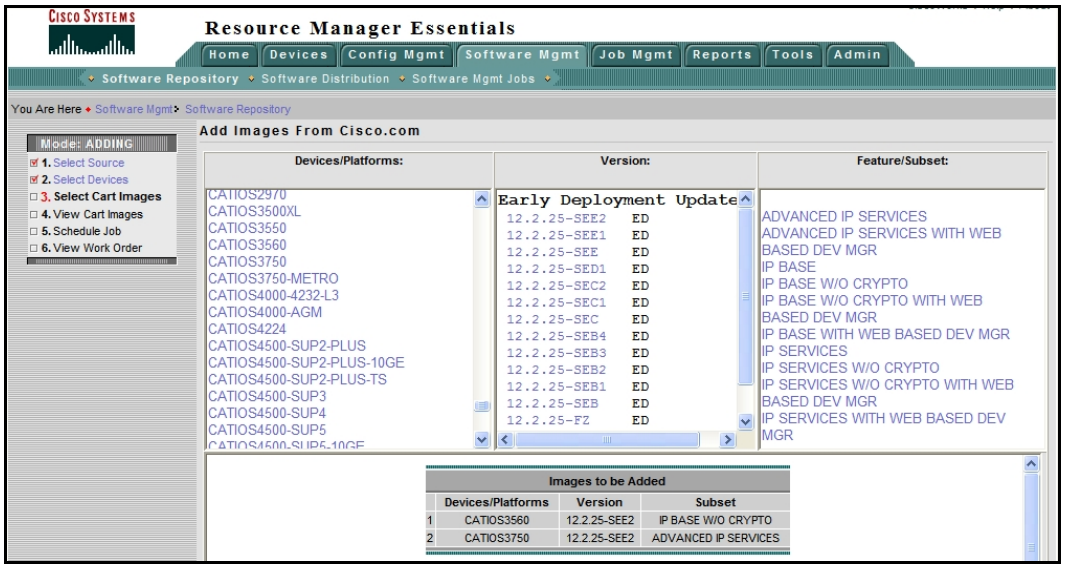
All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

5.3 Software Image Management

Software image management is a critical part of network management. At times, it becomes mandatory to upgrade an OS across thousands of switches, due to security advisories. Since the manual process of upgrading the software on a single switch takes a long time, upgrading hundreds of switches can be challenging. The CiscoWorks RME Software Image Management (SWIM) module can upgrade software on all Cisco switches in three simple steps.

1. Select the switches that need to be upgraded.
2. Select the image that needs to be selected for each switch type. Tight integration of RME with Cisco.com makes this task easy for network managers (Figure 13). Downloading multiple images for multiple switches from Cisco.com is simplified by SWIM.

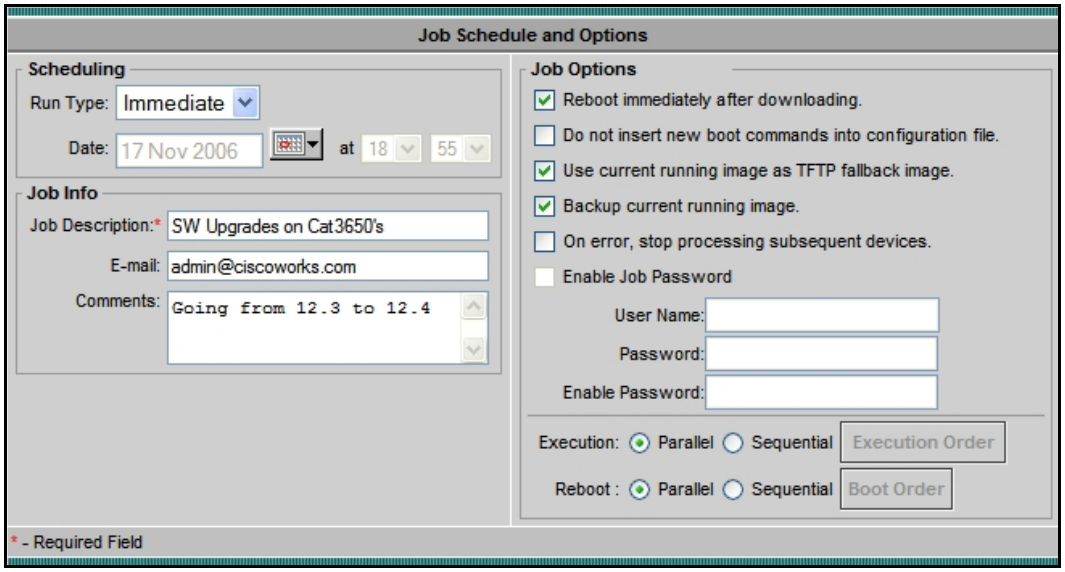
Figure 13. CiscoWorks LMS RME: Software Management Integration with Cisco.com



3. Once the images from the previous step are stored in the SWIM repository, the software can be distributed to the switches. CiscoWorks RME reduces the possibility of human error and helps avoid unplanned downtime. If the image upgrade fails on one of the switches, the job order addresses whether to proceed with the job as highlighted in Figure 14. Once the jobs are created, they can be tracked or resubmitted for greater efficiency.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

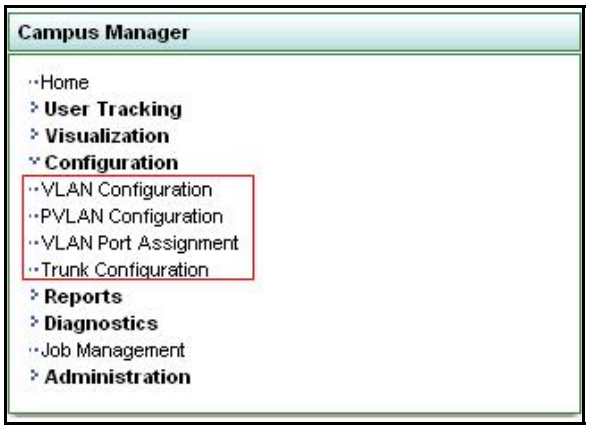
Figure 14. CiscoWorks LMS RME: Software Upgrade Job Schedule and Options



5.4 VLAN Management

VLAN management involves changing the existing configuration on the switch. Using CiscoWorks LMS Campus Manager, you can create, modify, and delete VLANs (Figure 15). You can also create VLANs (Ethernet and TokenRing) from within the network topology map.

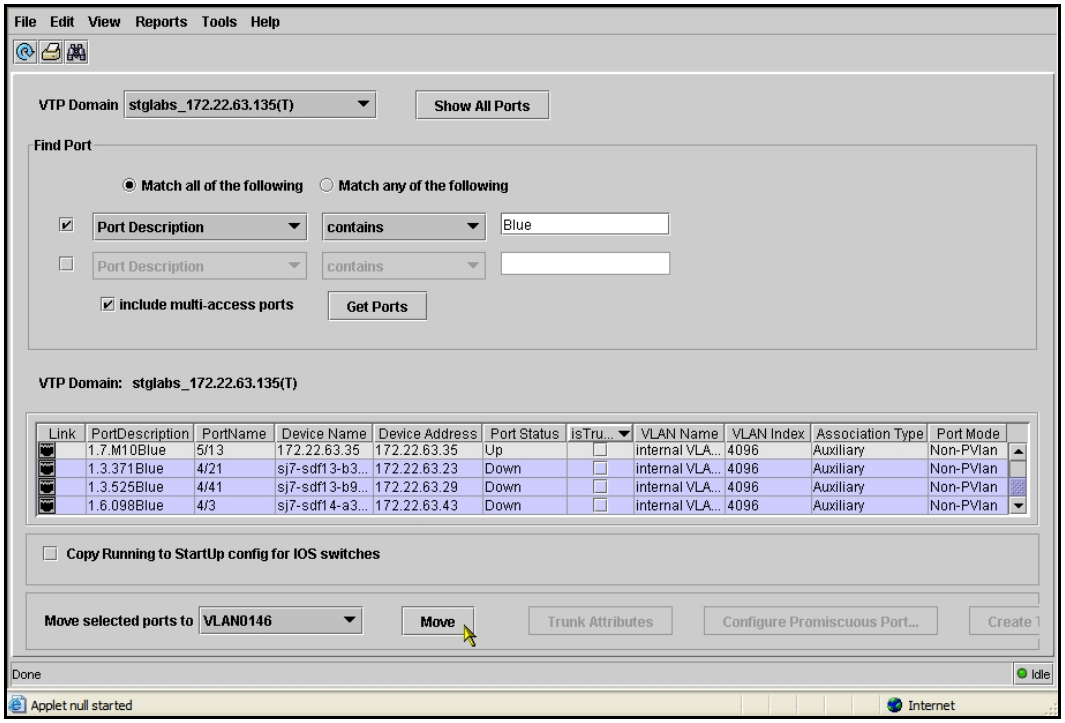
Figure 15. CiscoWorks LMS Campus Manager: VLAN Configuration



Once the Virtual Trunk Protocol (VTP) domains and VLANs are created, the next major task is to assign the ports to a VLAN. CiscoWorks LMS Campus Manager can be used for VLAN port assignment (Figure 16).

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 16. CiscoWorks LMS Campus Manager: VLAN Port Assignment



5.5 Spanning Tree Management

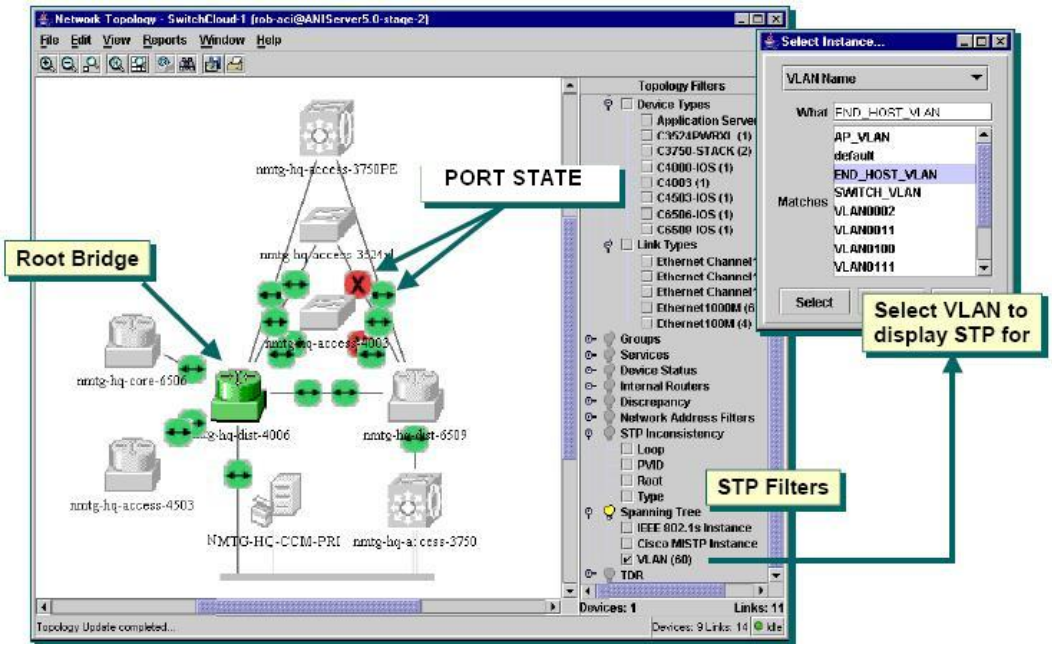
Spanning Tree Protocol (STP) can be a complicated aspect of switch configuration, especially if you have to assign costs and optimize individual network segments. CiscoWorks LMS Campus Manager simplifies this task by offering suggestions through one of four reports:

- Optimal Root Recommendation Report
- Number of Instances Recommendation Report
- Instance Reduction Recommendation Report
- VLAN to Instance Mapping Recommendation Report

Figure 17 shows how Campus Manager enables network engineers to visualize the STP to see what ports are forwarding (shown in green arrow icon) and what ports are blocking (shown in red X icon).

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 17. CiscoWorks LMS Campus Manager: Spanning Tree Management



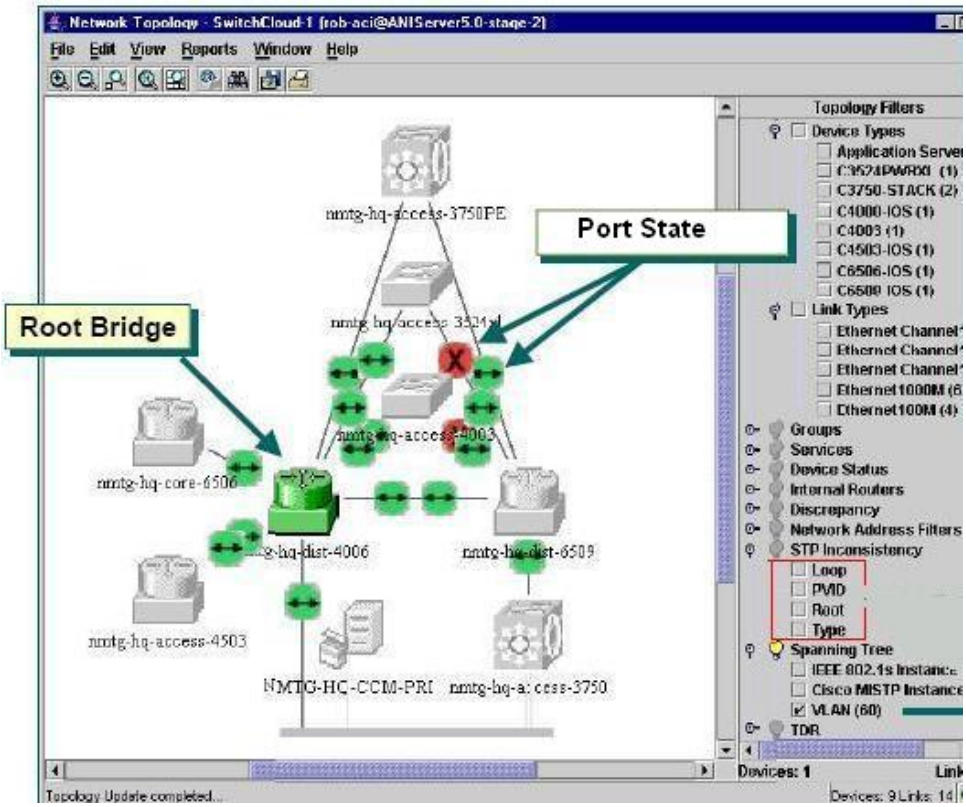
Campus Manager supports various spanning tree protocols such as Per-VLAN Spanning Tree (PVST), Multiple Spanning Tree Protocol (MSTP), and Multiple Instance Spanning Tree Protocol (MISTP). If your network has incorrect configurations, STP stops functioning and you may lose connectivity. The STP Inconsistency feature in Campus Manager detects these incorrect configurations in your network and changes the state to “inconsistent” for corresponding ports, thus preventing the ports from affecting the network.

The Campus Manager Topology Map provides four filters under Spanning Tree Inconsistency (Figure 18):

- Loop (Viewing Spanning Tree Loop Inconsistency)
- PVID (Viewing Spanning Tree PVID Inconsistency)
- Root (Viewing Spanning Tree Root Inconsistency)
- Type (Viewing Spanning Tree Type Inconsistency)

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 18. CiscoWorks LMS Campus Manager: Spanning Tree Filters



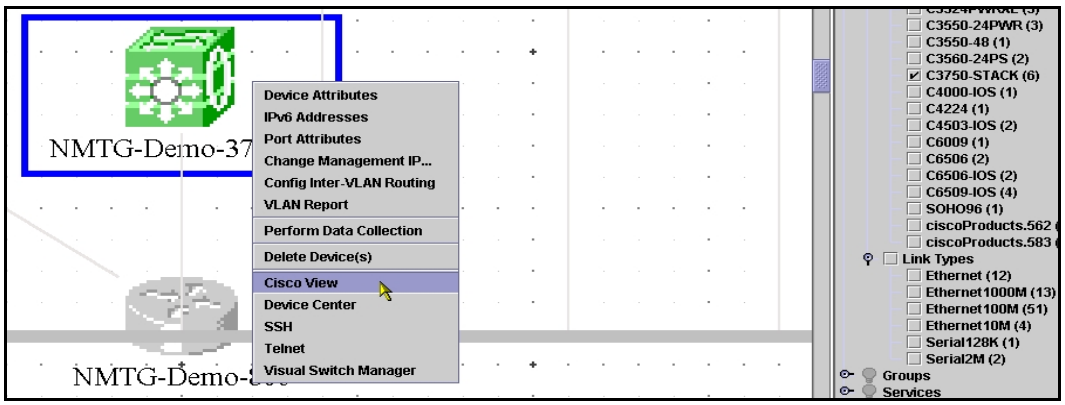
Campus Manager can be used to alter the STP for optimum performance and scenario testing if the cost, ID, and other variables are changed.

5.6 Stack Management

CiscoWorks LMS offers several tools to help network administrators manage Cisco StackWise® technology in Cisco Catalyst 3750 and 3750-E Series switches.

CiscoView is an element manager. It graphically displays the switches, including the stack. Using this view, a network manager can see the front panel of the remote switch in real time (Figure 19). This helps them guide the operations person at the remote location.

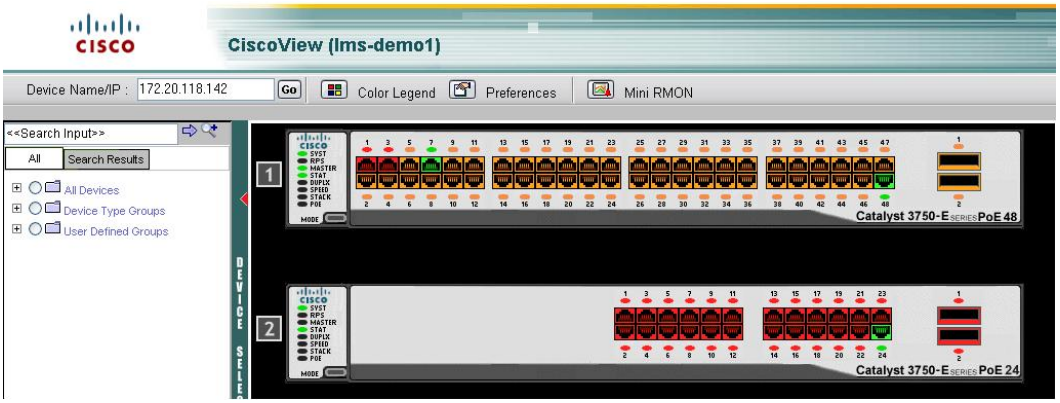
Figure 19. CiscoWorks LMS: Launch CiscoView to Manage Switch Stacks



All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

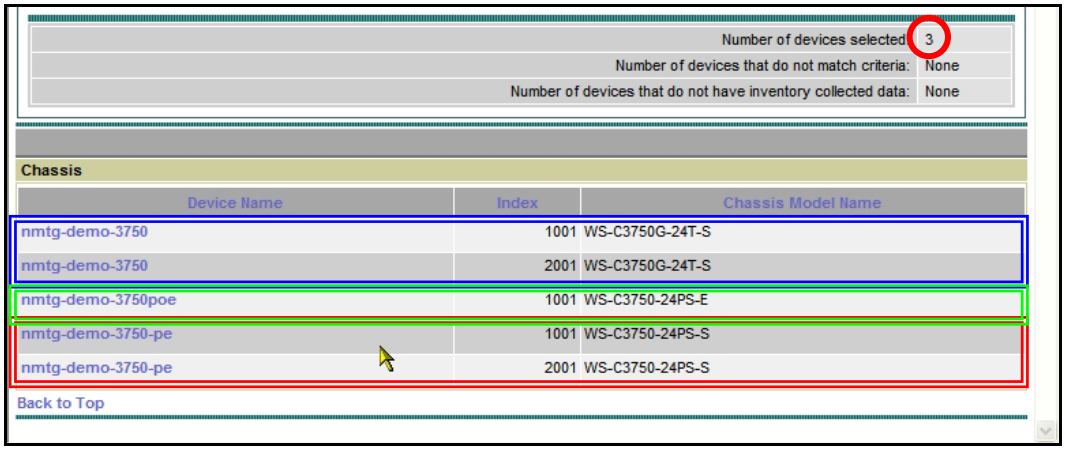
Once launched, complete stack appears in CiscoView (Figure 20).

Figure 20. CiscoWorks LMS CiscoView: Switch Stack Management



At times, there is a need to know how many switches with their chassis type are present in a particular stack. This information becomes crucial especially when taking inventory. CiscoWorks RME reporting capabilities make it easy to access this information. The report in Figure 21 shows three stacks and the number of switches within each stack.

Figure 21. CiscoWorks LMS RME: Device Count in Switch Stacks



6 Accounting

Many compliance certifications mandate that network engineers keep a detailed log of who is accessing the system and who is making changes to the network. Accounting is a process of tracking a user's activity while accessing network resources, including the amount of time spent in the network and the amount of data transferred during the session. Accounting data can be used for auditing, capacity planning, and trend analysis.

6.1 Government and Corporate Compliance

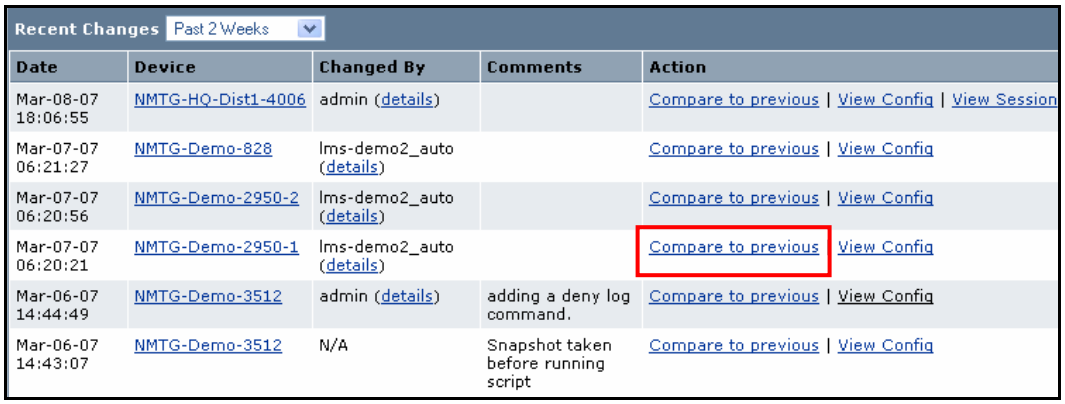
Compliance is a primary concern for many corporations. To be compliant with standards such as SOX, VISA PCI, HIPAA, GLBA, ITIL, CobiIT, and COSO, and with corporate IT standards, security policies, and technology rules, corporations are required to track network changes, apply policies around these changes, and generate reports that can be used by auditors. CiscoWorks NCM can assist with these areas.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

6.1.1 Tracking Configuration Changes

The CiscoWorks NCM homepage lists the recent configuration changes observed on network switches, including the date and time the change was made, the switch affected, who made the change, and comments about what the change was or why it was made (Figures 22 and 23).

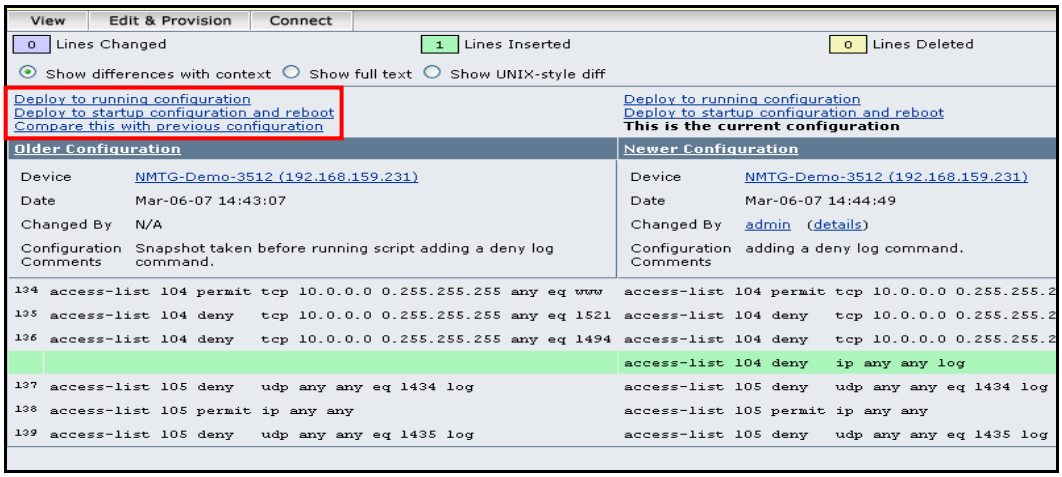
Figure 22. CiscoWorks NCM: Tracking Configuration Changes



Recent Changes Past 2 Weeks

Date	Device	Changed By	Comments	Action
Mar-08-07 18:06:55	NMTG-HQ-Dist1-4006	admin (details)		Compare to previous | View Config | View Session
Mar-07-07 06:21:27	NMTG-Demo-828	lms-demo2_auto (details)		Compare to previous | View Config
Mar-07-07 06:20:56	NMTG-Demo-2950-2	lms-demo2_auto (details)		Compare to previous | View Config
Mar-07-07 06:20:21	NMTG-Demo-2950-1	lms-demo2_auto (details)		Compare to previous | View Config
Mar-06-07 14:44:49	NMTG-Demo-3512	admin (details)	adding a deny log command.	Compare to previous | View Config
Mar-06-07 14:43:07	NMTG-Demo-3512	N/A	Snapshot taken before running script	Compare to previous | View Config

Figure 23. CiscoWorks NCM: Configurations Comparison



View | Edit & Provision | Connect

0 Lines Changed 1 Lines Inserted 0 Lines Deleted

Show differences with context Show full text Show UNIX-style diff

Deploy to running configuration
Deploy to startup configuration and reboot
Compare this with previous configuration

Deploy to running configuration
Deploy to startup configuration and reboot
This is the current configuration

Older Configuration		Newer Configuration	
Device	NMTG-Demo-3512 (192.168.159.231)	Device	NMTG-Demo-3512 (192.168.159.231)
Date	Mar-06-07 14:43:07	Date	Mar-06-07 14:44:49
Changed By	N/A	Changed By	admin (details)
Configuration Comments	Snapshot taken before running script adding a deny log command.	Configuration Comments	adding a deny log command.

```
134 access-list 104 permit tcp 10.0.0.0 0.255.255.255 any eq www   access-list 104 permit tcp 10.0.0.0 0.255.255.2
135 access-list 104 deny   tcp 10.0.0.0 0.255.255.255 any eq 1521  access-list 104 deny   tcp 10.0.0.0 0.255.255.2
136 access-list 104 deny   tcp 10.0.0.0 0.255.255.255 any eq 1494  access-list 104 deny   tcp 10.0.0.0 0.255.255.2
                                                                   access-list 104 deny   ip any any log
137 access-list 105 deny   udp any any eq 1434 log                 access-list 105 deny   udp any any eq 1434 log
138 access-list 105 permit ip any any                              access-list 105 permit ip any any
139 access-list 105 deny   udp any any eq 1435 log                 access-list 105 deny   udp any any eq 1435 log
```

CiscoWorks NCM tracks configuration changes for up to a year for each switch by default. This timeframe is configurable.

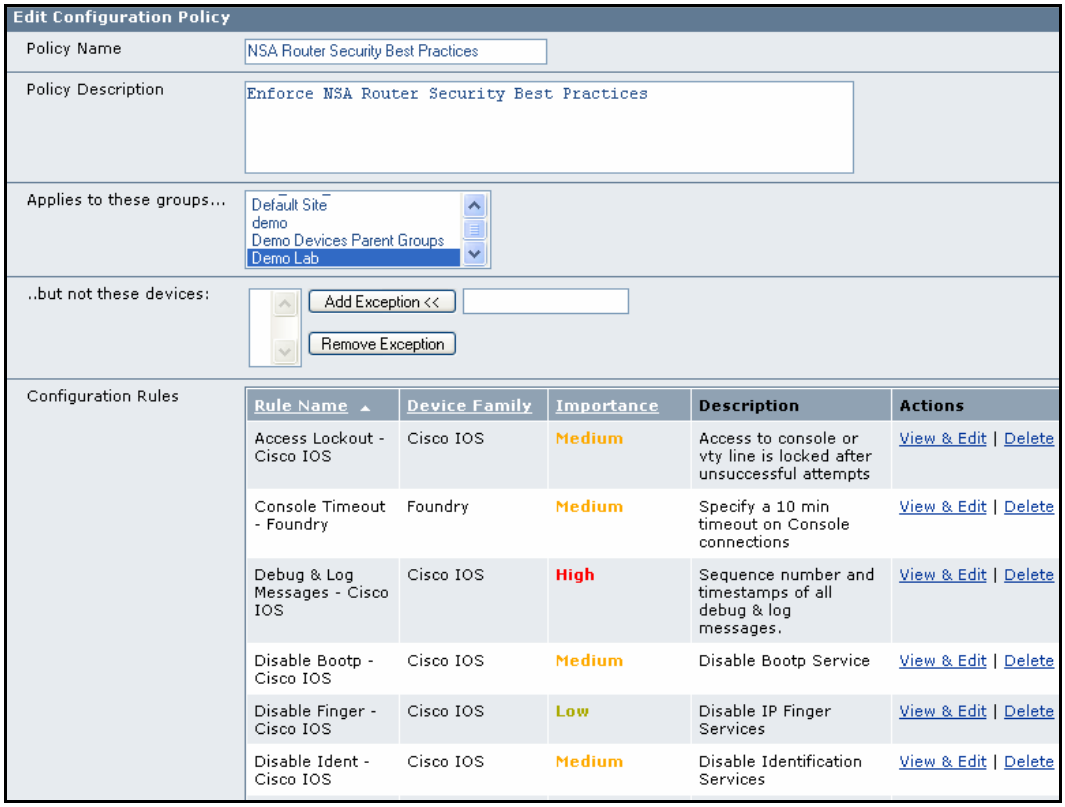
6.1.2 Configuration and Software Policies

A policy is essentially a set of rules that can be applied to a group of switches. Each rule can have an importance level associated with it, which can range from “critical” to “informational”. When a rule of a particular importance level is violated, actions such as sending e-mail, syslog, or SNMP traps; opening a trouble ticket; or running scripts can be triggered.

CiscoWorks NCM can be used to create policies, check if switches are compliant with policies, and generate reports. The NSA Router Security Best Practices (http://www.nsa.gov/snac) policy comes with NCM and is shown in Figure 24.

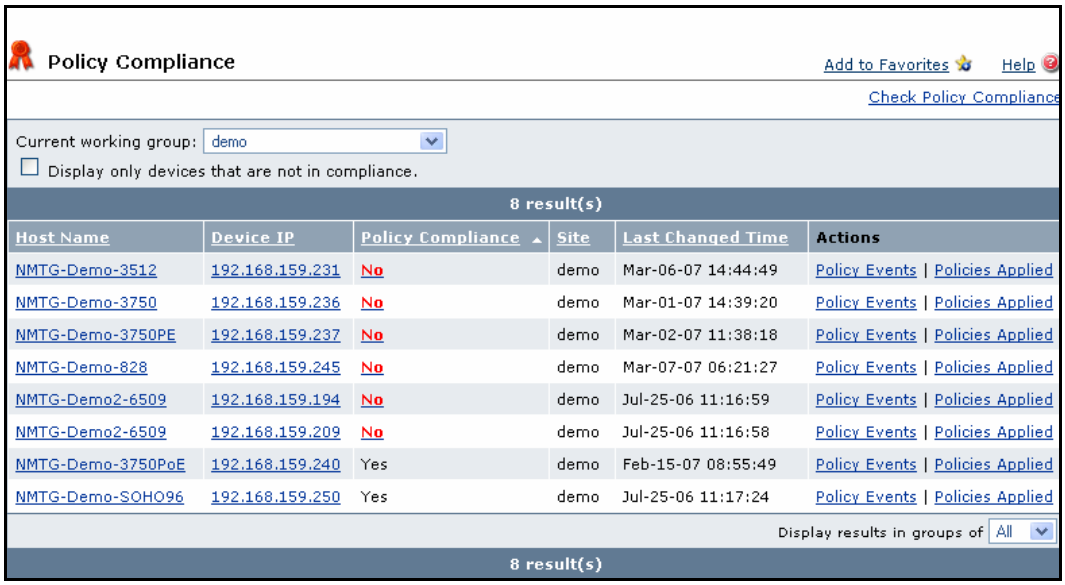
All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 24. CiscoWorks NCM: Compliance Policy



Each rule can be applied to the entire configuration file or to a configuration block. Each interface block must (or must not) contain certain commands. The block start-and-stop pattern is essentially a regular expression that will be matched against the configuration file. The next step is to check if the switches are compliant with these policies (Figure 25).

Figure 25. CiscoWorks NCM: Policy Compliance

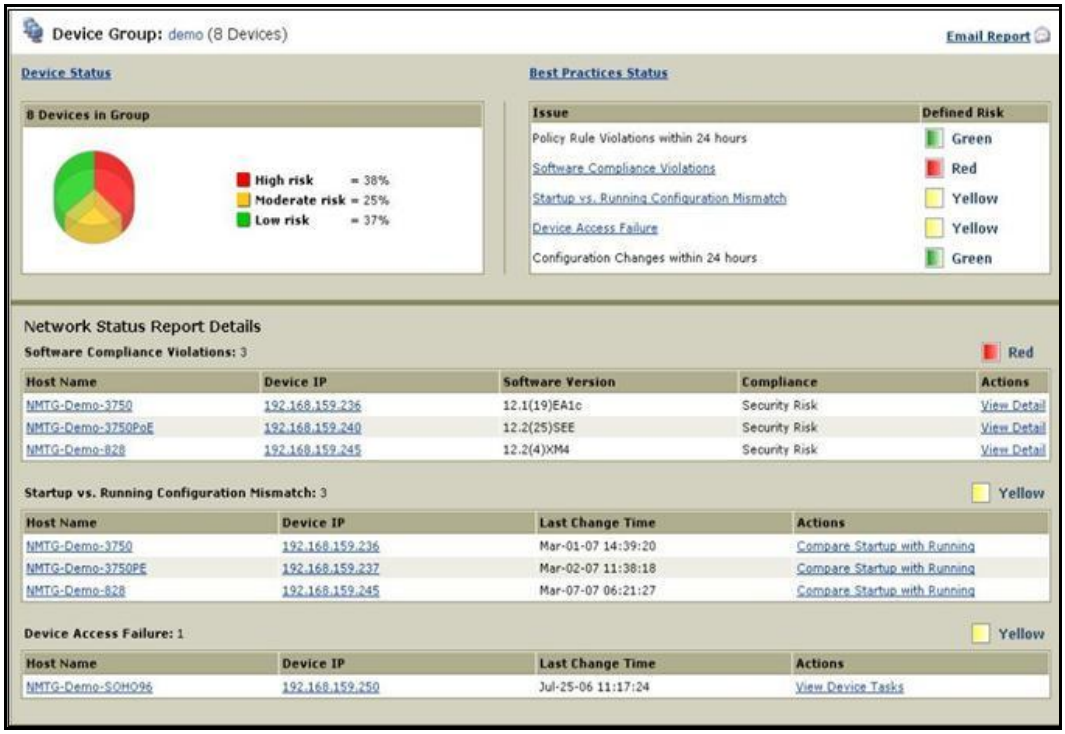


All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

For switches that are out of compliance, clicking on “No” will provide information on which policies are violated. Further on the GUI (not shown), clicking on “Configuration Policy Non-Compliance” will indicate why the switch is out of compliance and provide information on possible remediation.

Similar capabilities are also available for software compliance or assuring that specific software versions are deployed on each type of switch. Reports can be generated for internal network overview and for regulatory compliance audits. The network status report provides an overview of the network, including policy rule violations and software compliance violations (Figure 26). Management can use such reports to allocate resources to solve network problems.

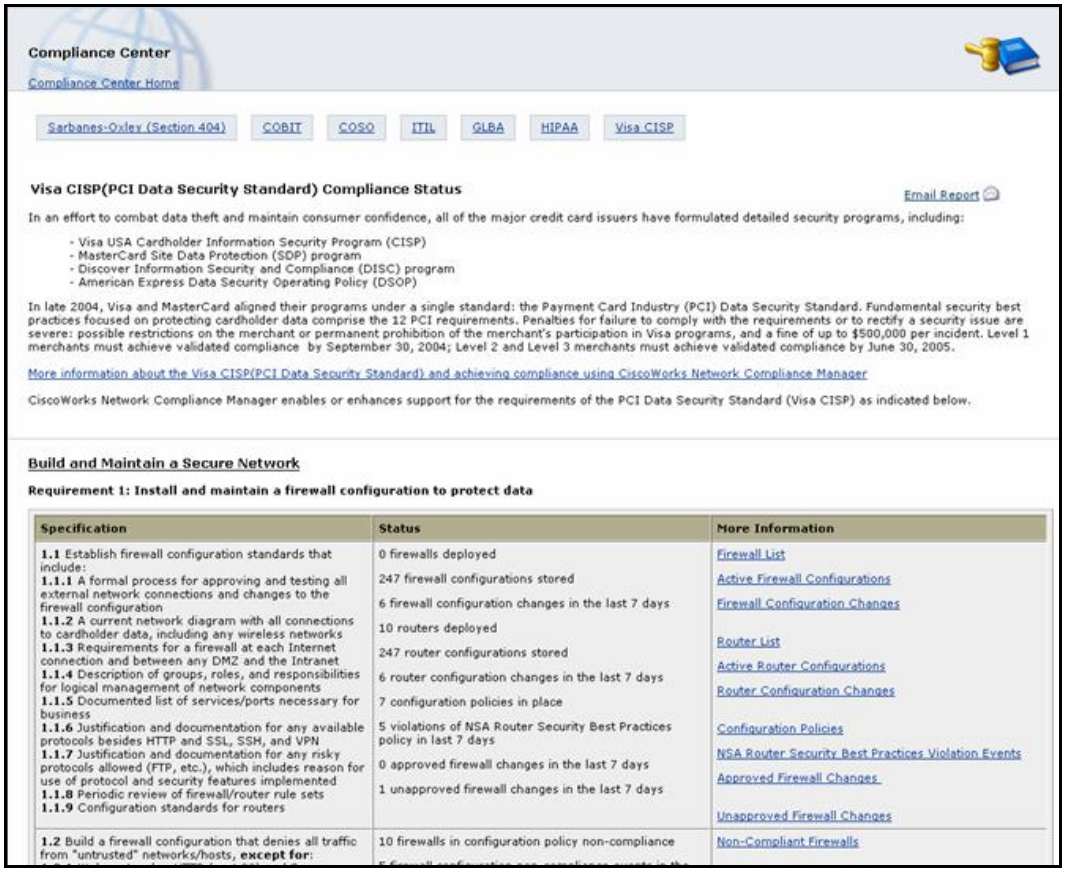
Figure 26. CiscoWorks NCM: Network Status Report



Reports can also be generated for regulatory compliance standards and can be viewed under the Compliance Center (Figure 27). For each standard, there is a link to more information about the standard and tips on how to implement various specifications using CiscoWorks NCM. The report also contains detailed specifications, statistics as related to the specification, and links to more details.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

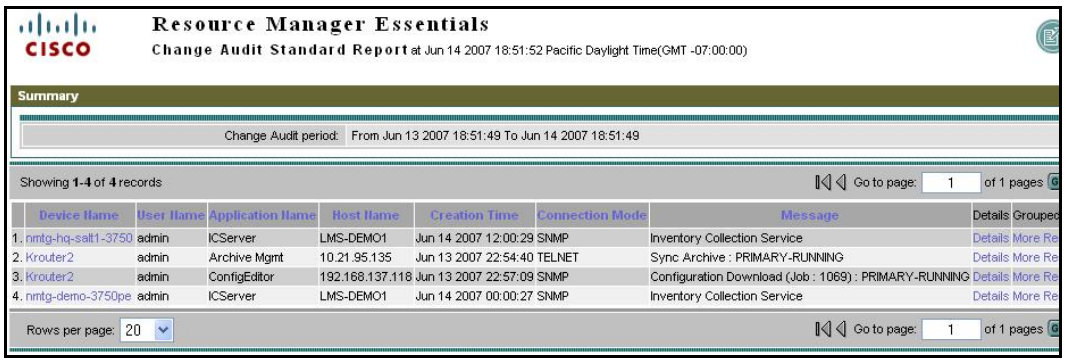
Figure 27. CiscoWorks NCM: Compliance Center



6.2 Change Audits

A change audit is a way to monitor switches as well as the NMS application. Who is logging in and making changes? When are they making changes? What was the nature of the changes that were made? This is useful data, especially when something goes wrong. CiscoWorks LMS supports auditing the switches as well the LMS software itself. A detailed report on these audits can be run from within RME (Figure 28).

Figure 28. CiscoWorks LMS RME: Change Audit Report



All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

6.3 Discovering Switches

Accounting can also mean accounting for all the switches in the network. CiscoWorks LMS Campus Manager can be scheduled to discover existing and new switches. Once discovered, the switches can be viewed in a topology map or can be exported to Microsoft Visio for documentation purposes.

Another challenge in adding new switches is to find out what was added to the network. Multiple new switches could be added in different areas of the network; for example, an employee could add an unauthorized router or wireless access point to their desk. Using the CiscoWorks Campus Manager discovery module, a report can be run that produces a list of newly added network devices (Figure 29). The report provides information not only about the new switch, but also when it was seen on the network.

Figure 29. CiscoWorks LMS Campus Manager: Data Collection Report

Cisco Systems

Campus Manager Administration

Data Collection Metrics as of 07 Mar 2007, 11:00:24 PST

Showing **1-10** of **10** records — Go to page: 1 of 1 pages

	StartTime	PercentComplete	EndTime	TotalTime	TotalDevices	NewDevices	DevicesDeleted	DevicesPerHour	ObjectsPerHour
1.	Mar 7, 2007 8:00:00 AM	100	Mar 7, 2007 8:08:39 AM	8 minutes 38 seconds	79	0	0	548	128700
2.	Mar 7, 2007 4:00:00 AM	100	Mar 7, 2007 4:08:39 AM	8 minutes 38 seconds	79	0	0	548	128692
3.	Mar 7, 2007 12:00:00 AM	100	Mar 7, 2007 12:08:55 AM	8 minutes 54 seconds	79	0	0	531	124864
4.	Mar 6, 2007 8:00:00 PM	100	Mar 6, 2007 8:08:39 PM	8 minutes 38 seconds	79	0	0	548	128742
5.	Mar 6, 2007 4:00:00 PM	100	Mar 6, 2007 4:08:40 PM	8 minutes 40 seconds	79	0	0	546	128390
6.	Mar 6, 2007 12:00:00 PM	100	Mar 6, 2007 12:07:28 PM	7 minutes 28 seconds	79	0	0	634	149038
7.	Mar 6, 2007 8:00:00 AM	100	Mar 6, 2007 8:08:41 AM	8 minutes 41 seconds	79	0	0	545	128105
8.	Mar 6, 2007 4:00:00 AM	100	Mar 6, 2007 4:08:40 AM	8 minutes 39 seconds	79	0	0	547	128556
9.	Mar 6, 2007 12:00:00 AM	100	Mar 6, 2007 12:08:52 AM	8 minutes 51 seconds	79	0	0	535	125624
10.	Mar 5, 2007 8:00:00 PM	100	Mar 5, 2007 8:08:38 PM	8 minutes 37 seconds	79	1	0	549	128987

Rows per page: 20 — Go to page: 1 of 1 pages

6.3.1 Capacity Planning

What would happen if your company were to merge with another one? How will that affect the network? Are there enough ports on the switches to support the merger? Will more switches be required to support the growth? User data can also be used for capacity planning. Campus Manager includes several preconfigured reports that can be run on demand to provide detailed data on how many ports are currently used (Figures 30 and 31).

Figure 30. CiscoWorks LMS Campus Manager: Unused Up Switch Port Usage

Cisco Systems

Campus User Tracking

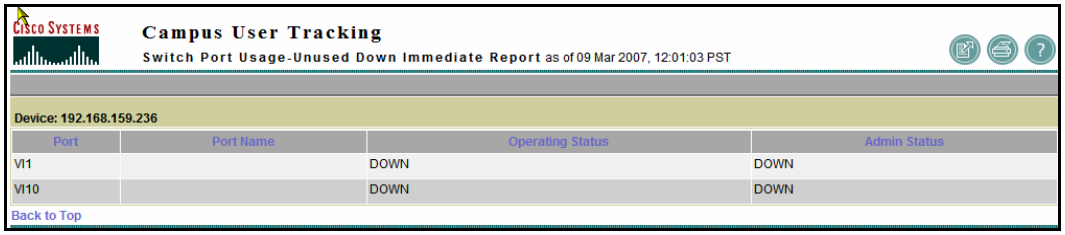
Switch Port Usage-Unused Up Immediate Report as of 09 Mar 2007, 11:59:08 PST

Device: 192.168.159.236

Port	Port Name	Operating Status	Admin Status
Gi2/0/10		DOWN	UP
Gi1/0/21		DOWN	UP
Gi2/0/11		DOWN	UP
Gi1/0/6		DOWN	UP
Gi2/0/13		DOWN	UP

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 31. CiscoWorks LMS Campus Manager: Unused Down Switch Port Usage



Such reports can be run on a per-switch basis or across a network. One can even run custom reports based on a given criteria for capacity planning, such as available Gigabit Ethernet ports.

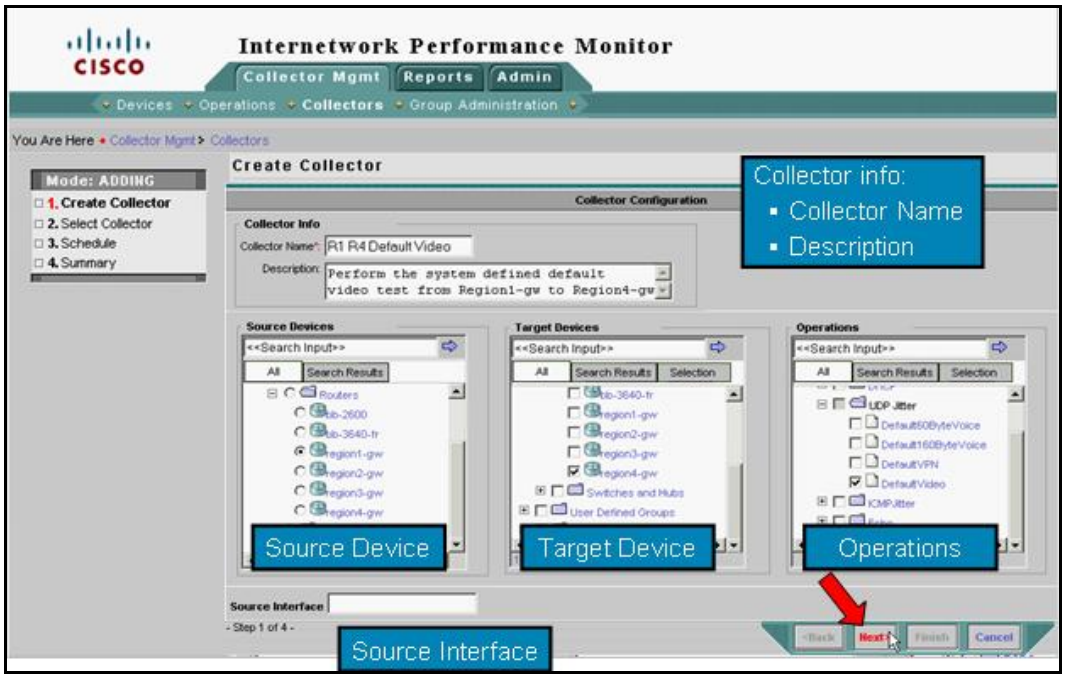
7 Performance Management

7.1 IP/SLA

The CiscoWorks IP/SLA feature can be used to analyze performance on an ongoing basis. Previously known as Services Assurance Agent (SAA) or Real-Time Responder (RTR), IP/SLA is a feature supported by Cisco IOS Software that generates synthetic traffic and sends it across any network where performance needs to be measured. The response time (also known as latency) is then measured and archived for historical purposes. CiscoWorks IPM can deploy and monitor IP/SLA. Deployment can be done in a matter of minutes using the following four steps:

1. Source
2. Target
3. Operations
4. Collector (Figure 32)

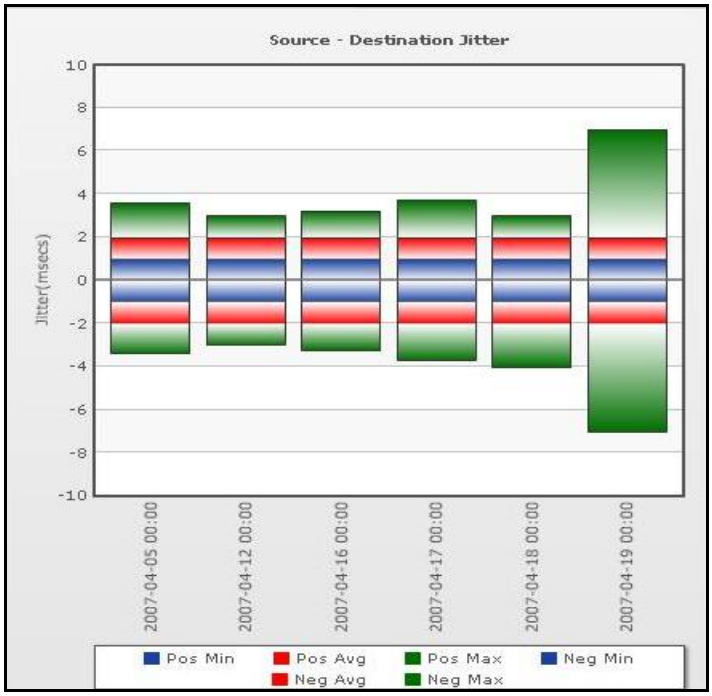
Figure 32. CiscoWorks LMS Internetwork Performance Monitor: Collector Setup



All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Once the IP/SLA configurations are deployed to the switches, real-time or historical statistical reports can be generated (Figure 33).

Figure 33. CiscoWorks LMS IPM: Performance Statistics



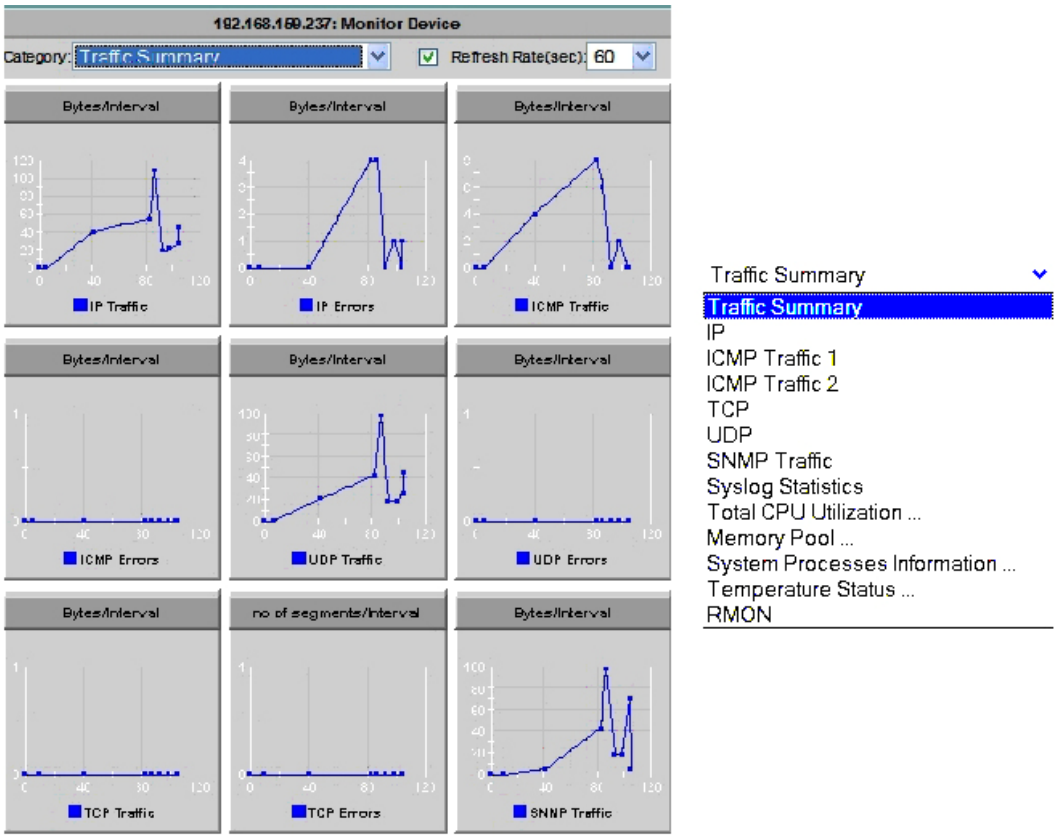
The statistical report shown in Figure 33 was done on a video stream. It shows positive and negative jitter.

7.2 Real-Time Statistics Using CiscoView

Real-time statistics are important at certain times, such as during troubleshooting or when monitoring whether a problem has been fixed on a single switch port. CiscoView can help monitor a wide variety of variables in real time (Figure 34).

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 34. CiscoWorks LMS CiscoView: Device Performance Statistics



8 Security

To secure the network infrastructure, CiscoWorks LMS uses several security features, including:

- Wide choice of applications for user authentication (Cisco ACS, LDAP, Active Directory, etc.)
- Secure HTTPS Web GUI access
- Support for SNMPv3

CiscoWorks NCM includes the following security features:

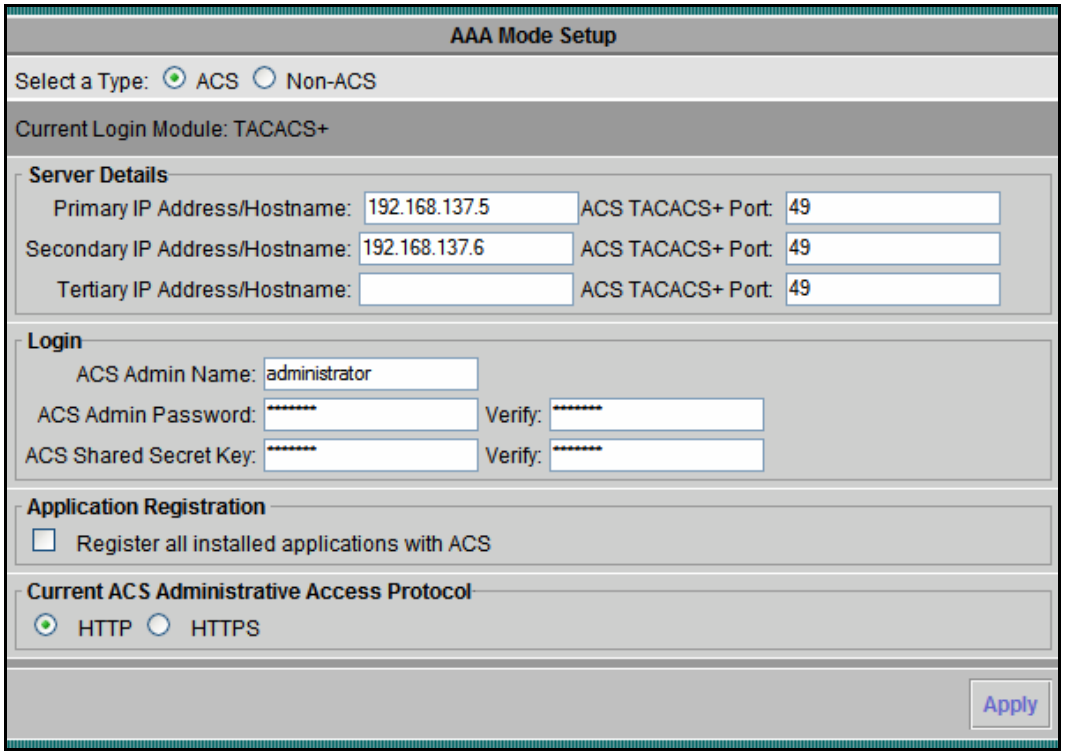
- User authenticate through LDAP, Active Directory, Cisco ACS, Secure ID
- Role-based access control and lock down
- Centralized access control list (ACL) management

8.1 Integrating with AAA Server

CiscoWorks LMS uses the proven Cisco ACS authentication and authorization by integrating with it. Figure 35 shows how a user can enter a minimal amount of information and LMS fills in the rest. Users can log into Cisco ACS and edit the permissions as needed.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 35. CiscoWorks LMS: AAA Mode Setup



9 Feature Management

Table 4 details how each switching feature can be managed using various applications.

Table 4. Feature Management on CiscoWorks LMS and NCM

Feature Management	LMS	NCM
MAC address management	X	X
For stack: enabling persistent MAC address	X	X
Changing address aging time	X	X
MAC address notification trap	X	X
Unicast MAC address filtering	X	X
Administering the switch (NTP, banner, etc.)	X	X
Switch database management templates	X	X
Configuring TACACS+	X	X
Configuring SSH	X	X
Configuring a Certificate Authority trustpoint	X	X
SmartPort macro	X	X
Configuring 802.1x authentication	X	X
Configuring PVLANs	X	X
Configuring MSTP	X	X
Configuring Dynamic Host Control Protocol (DHCP) snooping	X	X
Configuring IP Address Resolution Protocol (ARP) inspection	X	X
Configuring mini-RMON	X	–
Configuring SNMP	X	X

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Configuring Cisco EtherChannel®	X	X
Configuring online diagnostics	X	X
Configuring health monitoring	X	X
Starting online diagnostics	X	X

10 Conclusion

With a wide range of tools and functions, CiscoWorks applications are critical to take full advantage of sophisticated and versatile Cisco switches. CiscoWorks tools enable administrators to:

Discover the composition of the network

Configure a wide range of features on multiple switches simultaneously

Discover potential switch faults or network performance bottlenecks proactively

Get notification of those issues through a wide array of reports

Troubleshoot effectively by isolating the root cause of faults, and mitigate future problems either through a configuration change or a software upgrade

Discover if the network is in compliance with government regulations such as SOX, VISA CISP, HIPAA, GLBA, ITIL, CobiT, COSO, and PCI

11 Appendices

11.1 Appendix A: Switch Feature Management Detail

This section discusses how CiscoWorks LMS and NCM can be used together to deploy some of the basic configurations for advanced features on Cisco Catalyst switches.

11.1.1 For Stack: Enabling Persistent MAC Address

Method: Use NetConfig—Refer to Section 5.1.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
stack-mac persistent timer<R>
copy run start<R>
```

11.1.2 Changing Address Aging Time

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
mac address-table aging-time 20 vlan 10<R>
copy run start<R>
```

11.1.3 MAC Address Notification Trap

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
snmp-server host 172.20.10.10 traps URCommString<R>
```

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
snmp-server enable traps mac-notification<R>
mac address-table notification<R>
mac address-table notification interval 60<R>
mac address-table notification history-size 100<R>
```

11.1.4 Unicast MAC Address Filtering

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
mac address-table static c2f3.220a.12f4 vlan 4 drop<R>
11.1.5 Administering the Switch
```

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: NTP, Banner, and Adhoc

a) NTP: Need to provide basic NTP information.

b) Creating a banner: Provide the appropriate banner text.

c) Sample configuration for adhoc template:

```
service timestamps log datetime msec localtime show-timezone<R>
```

11.1.6 Configuring Switch Database Management Templates

You can use switch database management templates to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network. You can select a template to provide maximum system usage for some functions; for example, use the default template to balance resources, and use access template to obtain maximum ACL usage.

To allocate hardware resources for different usages, the switch database management templates prioritize system resources to optimize support for certain features. You can select switch database management templates for IP Version 4 (IPv4) to optimize these features:

- Routing: Maximizes system resources for unicast routing, typically required for a router in the center of a network.
- VLANs: Disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.
- Default: Gives balance to all functions.
- Access: Maximizes system resources for ACLs to accommodate a large number of ACLs.

The switch supports only the desktop templates.

To revert to the default template:

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
no sdm prefer<R>
end<R>
reload<R><R>
```

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

To configure a switch with the routing template:

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
sdm prefer routing<R>
end<R>
reload<R><R>
```

To configure the IPv4-and-IPv6 default template on a desktop switch:

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
sdm prefer dual-ipv4-and-ipv6 default<R>
end<R>
reload<R><R>
```

11.1.7 Configuring TACACS+

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: TACACS+

11.1.8 Configuring SSH

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: SSH

Assumes that hostname and domain-name are already configured. If not, use the Adhoc template to push out the domain-name by the following command:

```
ip domain-name <domain>
```

11.1.9 Configuring a Certificate Authority Trustpoint

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Certificate Authority

Note: Before you configure a Certificate Authority trustpoint, you should ensure that the system clock is set. If the clock is not set, the certificate will be rejected due to an incorrect date.

11.1.10 SmartPort Macro

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: SmartPort

Note: This template will be added in CiscoWorks LMS 3.0

11.1.11 Configuring 802.1x Authentication

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

```
aaa new-model
aaa authentication dot1x default none
dot1x system-auth-control
```

Use SmartMacros to push out the following configuration at **interface** level:

```
dot1x port-control auto
```

CiscoWorks NCM can also be used to push the configuration pertaining to the interface(s).

11.1.12 Configuring PVLANs

Refer to Section 4.4 on VLAN management. PVLANs are supported in Campus Manager.

11.1.13 Configuring MSTP

Section 4.5 discussed how to configure Spanning Tree Protocol from the Campus Manager. This configuration could also be deployed from the CiscoWorks RME NetConfig module.

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
spanning-tree mst configuration
instance 1 vlan 10-20
name region1
revision 1
exit
<R>
```

11.1.14 DHCP Snooping

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
ip dhcp snooping
ip dhcp snooping vlan 10
ip dhcp snooping information option<R>
```

Use SmartMacros to push out the following configuration at interface level:

```
ip dhcp snooping limit rate 100
```

CiscoWorks NCM can also be used to push the configuration pertaining to the interface(s).

11.1.15 IP ARP Inspection

Dynamic ARP inspection depends on the entries in the DHCP snooping binding database to verify IP-to-MAC address bindings in incoming ARP requests and ARP responses.

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
ip arp inspection vlan 1
```

Use SmartMacros to push out the following configuration at interface level:

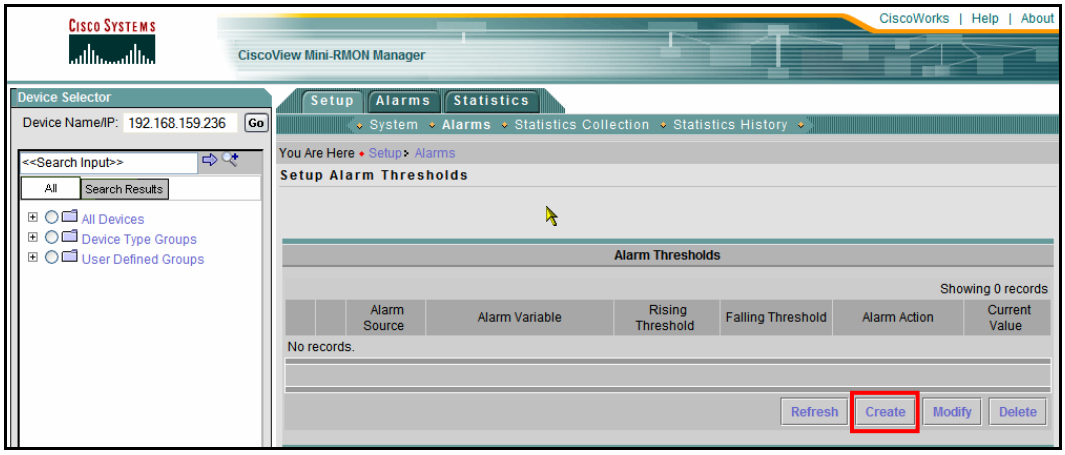
```
ip arp inspection trust
```

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

11.1.16 Configuring Mini-RMON on Desktop Switches

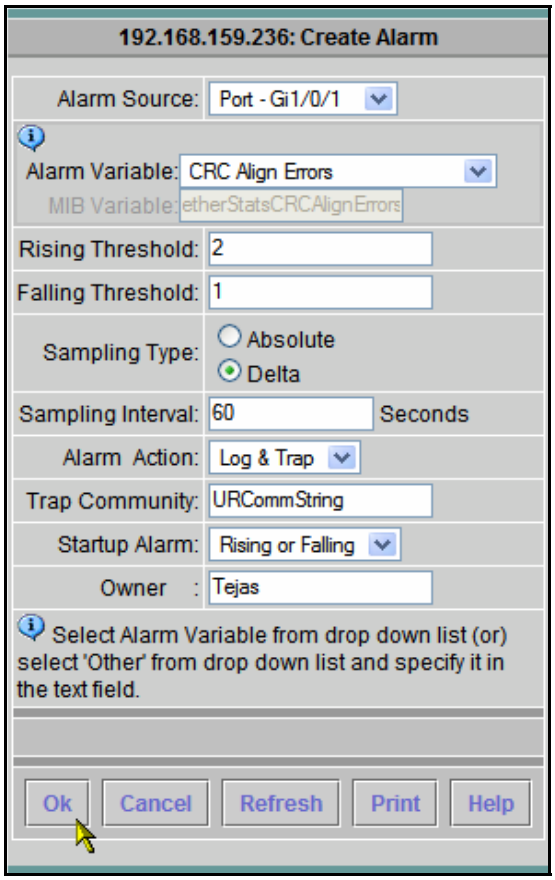
Desktop switches by default support two additional RMON tables: Statistics and History. Routers only support Alarms and Events. The CiscoWorks mini-RMON manager can configure the RMON effortlessly. To start to configure RMON on the Cisco switch, open the mini-RMON Manager from the CiscoWorks homepage or Device Manager or CiscoView. From Setup Alarms , click on "Create" as shown in Figure 36.

Figure 36. CiscoWorks LMS CiscoView: Setup Mini-RMON



Next, begin to define the alarm in the new window (Figure 37).

Figure 37. LMS CiscoView: Create Alarm



All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Click “Ok” to see the new alarm being configured (Figure 38).

Figure 38. CiscoWorks LMS CiscoView: Alarm Thresholds

Alarm Thresholds

Showing 1 records

		Alarm Source	Alarm Variable	Rising Threshold	Falling Threshold	Alarm Action	Current Value
1.	☐	Gi1/0/1	etherStatsCRCAlignErrors	2	1	Log & Trap	0

11.1.17 Configuring SNMP

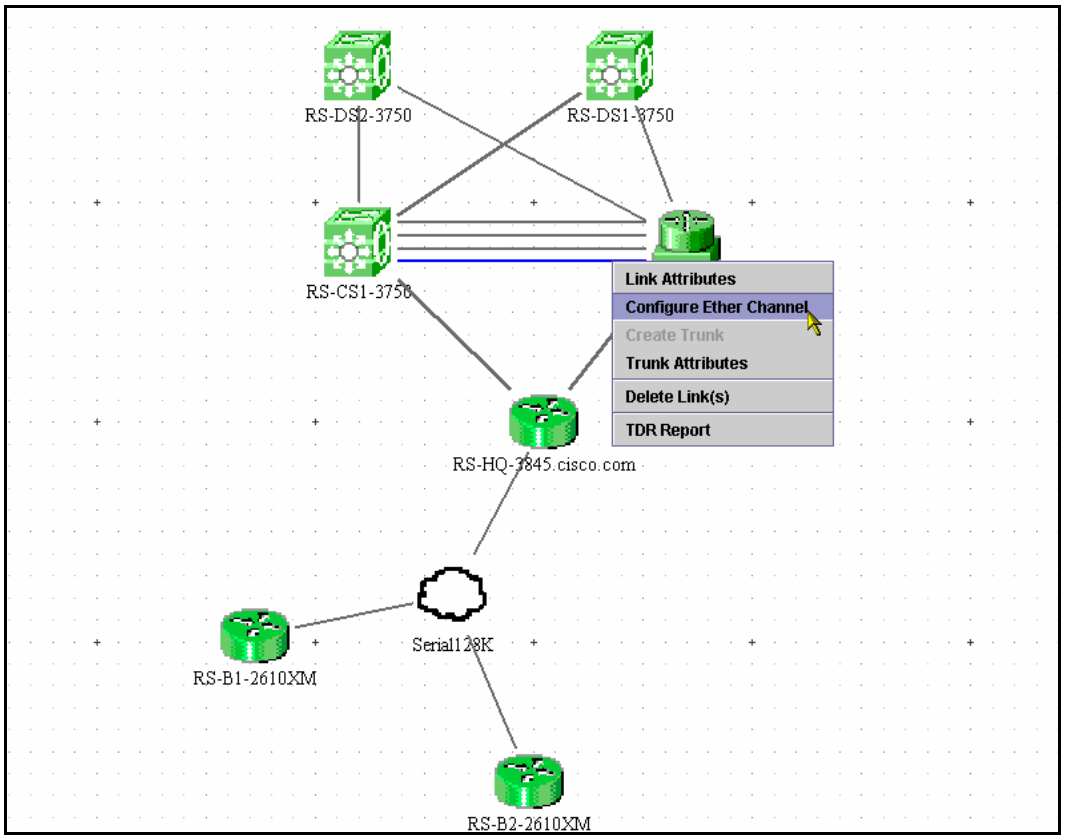
Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: SNMP

11.1.18 Configuring Cisco EtherChannels

Cisco EtherChannels can be quickly configured using CiscoWorks LMS Campus Manager. From within Topology Services, right-click (show as blue link in Figure 39) on any link connecting the two switches where you want to configure EtherChannel. Select “Configure EtherChannel” from the menu.

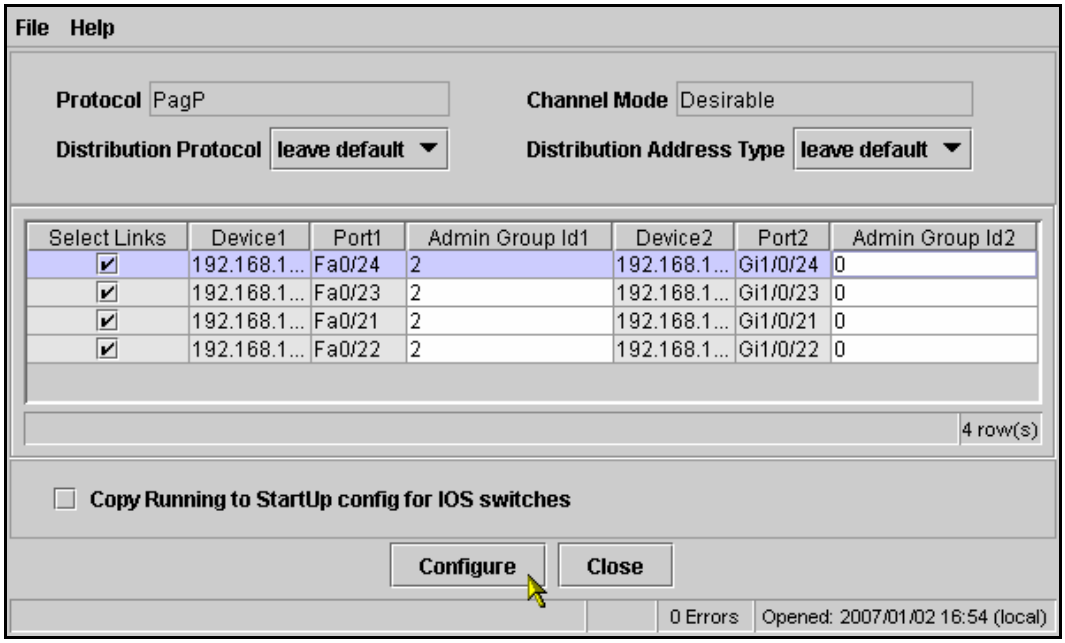
Figure 39. CiscoWorks LMS Campus Manager: Create EtherChannel



All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

A new window appears (Figure 40). Edit the admin groups and other protocol-related information, and click on “Configure”. Campus Manager should configure the EtherChannel.

Figure 40. CiscoWorks LMS Campus Manager: Create EtherChannel



11.1.19 Maintenance Management

Configuring online diagnostics: This example shows how to schedule diagnostic testing for a specific day and time on a Cisco Catalyst 3560-E Series switch:

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
diagnostic schedule test TestPortAsicCam on December 3 2006 22:25
```

This example shows how to schedule diagnostic testing to occur weekly at a specific time on member switch 6 when this command is entered on a Cisco Catalyst 3750-E Series stack master:

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
diagnostic schedule switch 6 test 1-4,7 weekly saturday 10:30
```

11.1.20 Configuring Health Monitoring

This example shows how to configure the specified test to run every two minutes on member switch 2, when this command is entered on a Cisco Catalyst 3750-E Series stack master:

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
diagnostic monitor interval switch 2 test 1 00:02:00 0 1
```

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

This example shows how to set the failure threshold for health-monitoring tests on a Cisco Catalyst 3560-E Series switch:

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
diagnostic monitor threshold test TestMicringLoopback failure count
50
```

This example shows how to enable the generation of a syslog message when any health monitoring test fails:

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
diagnostic monitor syslog
```

11.1.21 Starting Online Diagnostics

This example shows how to start a diagnostic test on a Cisco Catalyst 3560-E Series Switch by using the test name. Note: After starting the tests, you cannot stop the testing process.

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
Switch# diagnostic start test TestInlinePwrCtlr
```

This example shows how to start all basic diagnostic tests on a standalone Cisco Catalyst 3870 Series switch:

Method: Use NetConfig—Refer to Section 4.2 of this document.

Template to be used: Adhoc

Sample configuration for Adhoc template:

```
Switch# diagnostic start switch 1 all
```

12 References

12.1 LMS References on Cisco.com

LMS white papers on Cisco.com:
http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_white_papers_list.html

LMS Quick Start Guide:
http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_installation_guides_list.html

CiscoWorks LAN Management Solution Introduction:
http://www.cisco.com/en/US/products/sw/cscowork/ps2425/index.html

CiscoWorks Network Compliance Manager Introduction:
http://www.cisco.com/en/US/products/ps6923/index.html

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

User Guides for CiscoWorks LMS RME, Campus Manager, and CiscoView, and for CiscoWorks NCM

For LMS:

Find the list at page 19 of the Installation and Getting Started Guide at:

http://www.cisco.com/application/pdf/en/us/guest/products/ps7196/c2001/ccmigration_09186a008085bb19.pdf

For NCM:

http://www.cisco.com/en/US/products/ps6923/products_user_guide_list.html

12.2 Cisco Press Books

The following books are available through Cisco Press®.

LAN Switching First-Step:

http://www.ciscopress.com/title/1587201003

ISBN: 1587201003

Network Management Fundamentals

http://www.ciscopress.com/title/1587201372

ISBN: 1587201372

Performance and Fault Management

http://www.amazon.com/Performance-Fault-Management-Cisco-Press/dp/1578701805

ISBN: 1578701805

Network Administrators Survival Guide

http://www.ciscopress.com/title/1587052113

ISBN: 1587052113

12.3 Wikipedia Definition of FCAPS

http://en.wikipedia.org/wiki/FCAPS

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.**

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0708R)

Printed in USA

C11-426170-00 10/07