Chesapeake
NETCRAFTSMEN

White Paper

CiscoWorks LMS 4.0: Improved with More Integration and a New User Interface

Overview

Cisco is bringing to their customers an improved version of the CiscoWorks LAN Management Solutions (LMS) network management product. Prior versions of LMS were based on a collection of several products that were loosely integrated, and many customers found the collection difficult to use. Cisco has listened to the feedback from customers and evolved LMS into a single integrated product that contains the functionality needed to manage modern networks.

The other key benefits of the enhanced LMS 4.0 include an updated User Interface (UI) in which the functions are more easily accessible, as well as updated and more capable configuration management.

Customer Challenges

Networks are critical to modern business operations, so why are so many networks run using manual processes? One reason is because most network training is on configuring individual network devices, not on network management tools. Since it often takes several tools to create a functional network management system, network management requires significant additional training. The tighter integration of LMS 4.0 functions helps address this issue, making it easier to begin automating manual network management processes.

Automation is particularly important as networks grow to hundreds or thousands of routers and switches. Network discovery, inventory, software updates, configuration management, performance data collection, and troubleshooting are all critical functions that cannot be done using manual processes in a large network. LMS 4.0 allows automation of many of these mundane, day-to-day operational tasks associated with managing a large global network.

Another challenge that Cisco’s customers often face is adopting new technology and capabilities. An example of new technology is EnergyWise, a Cisco technology that allows network administrators to reduce the power consumption of network devices, particularly those supporting Power over Ethernet (PoE) attached devices such as IP phones. There are several operational tasks involved in deploying any new technology into the network. The customer must determine if their existing network hardware and software supports the new technology, and the steps to take if it does not. The customer needs to identify and upgrade specific hardware as needed, update the software on appropriate devices as needed, and then deploy the new configurations. Without automation, many organizations find it nearly impossible to find the time to implement new technologies across their network. LMS 4.0 Work Centers are a set of tools that help organizations implement new technologies. They provide significant value by supporting automated functions for the identification of hardware, software updates, and configuration deployment to devices.

Any given technology can often be deployed in a variety of designs. At NetCraftsmen, we recommend our customers use design templates that can be validated against as-built configurations. As a base tool for template development, we like using the Cisco Validated Designs (CVD, formerly known as Solutions Reference Network Design Guides, or SRNDs). These are designs and templates that Cisco has validated in real networks. At NetCraftsmen, we think of them as initial templates against which we build and then validate customer network designs and configurations. Using the CVD templates can save a lot of time in designing a network. They help create networks that are familiar to the customer and Cisco support engineers and partners, have known failure modes, and are therefore easier to troubleshoot so have less down time. LMS 4.0 includes the ability to check network configurations against configuration templates, so even if the CVD is modified slightly for a given customer, it is relatively easy to adjust the configuration templates that are used to validate the installed configurations.

The result of using a tool such as LMS 4.0 is that the business benefits from less down time, faster adoption of new technologies, and more consistent and easily maintained networks. The only caveat we see is that it is essential that the network staff is adequately trained on the operation of the network management tools. We believe that this training is a small price to pay for the benefits.

Network Management Architecture

At Chesapeake NetCraftsmen, we have developed a network management architecture that we use to recommend and implement the functions required by an enterprise network management system.

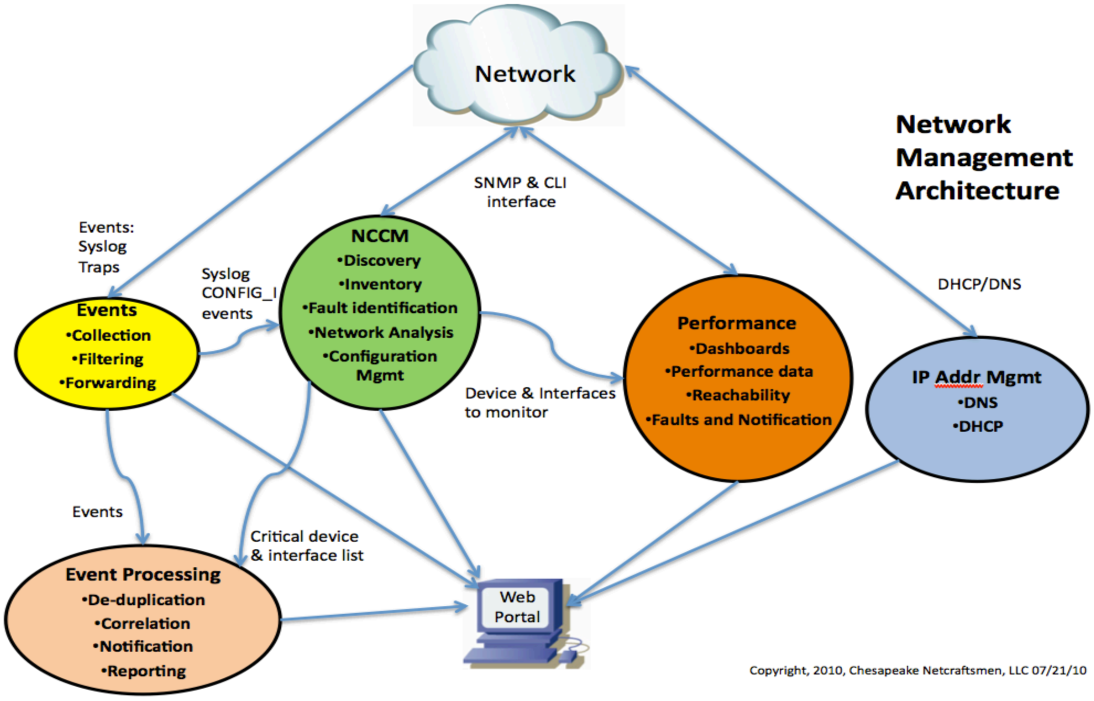


Figure 1: Enterprise Network Management Architecture

The network management architecture includes several key functions:

- Event collection, filtering, and forwarding for syslog and SNMP traps. Events are the notifications that network devices send when something significant happens. For example, a Cisco 6500 has approximately ten times as many syslog events as SNMP trap events, so handling syslog is very important. Events are sent after a problem has occurred, so they are the real-time notification that something has changed, either good or bad.
- Event Processing to de-duplicate, count, correlate, and send notifications of events. An event processing system is needed because the volume of events precludes watching an event log. The best systems will de-duplicate and count events that are alike and will allow correlation of events with each other, allowing things such as an interface down event to be automatically cleared by the corresponding interface up event. A good event processing system provides a good dashboard and notification mechanism, allowing the network staff to quickly see the active events and get real-time notification of significant events.
- Network Change and Configuration Management (NCCM) performs network device discovery, inventory, network analysis, and configuration management. A good network discovery engine that can automatically find network devices, rogue devices, and track users across the network is a critical component of good network management systems. Once the NMS knows of the network devices, it needs to collect inventory information, basic operational data, and configurations. The best products perform analysis on the collected data to reduce the workload of the network staff. The configuration management function must track and highlight configuration changes because that’s the most frequent source of network failures.
- Performance provides performance dashboards, historical performance data display, and fault identification with notification. Tracking network utilization and performance is a key function and one that many network managers emphasize. Performance dashboards and reports are key to good functionality in this module.
- IP Address Management (IPAM) manages the IP address space and provides DNS and DHCP services. Managing the IP address space and address allocations is a big task that is frequently implemented with spreadsheets, with the resulting problems of maintaining a single document. Because DNS and DHCP are frequently implemented on separate servers, we often see this function outside the normal NMS platform, either on a dedicated set of appliances, or running on self-maintained servers.

We see that LMS 4.0 provides many of the functions identified in our enterprise network management architecture. LMS 4.0 performs event collection, network discovery, inventory, network analysis, network configuration archive, software image management, performance data collection, fault identification, notification, and provides customizable dashboards.

User Interface

The revamped user interface (UI) is more functional and removes the barriers to operation that made prior versions of LMS more difficult to learn and use. One example of the UI improvement is that commonly used functions can be added to a “My Home” page for rapid access. Another UI enhancement is that custom “portlets” can be created to add any web content to any page, such as showing a weather site along side the page that displays network events, so that you can watch a storm travel across a region and track network outages as the storm moves.

Device support continues to be impressive, with 600 to 800 known devices, depending on the LMS function being used. Although you should not have that many different device types in your network, LMS 4.0 should know about it if you do. For example, the new Nexus products are supported in LMS 4.0, except by the LMS User Tracking function. [Note: some of the Nexus performance data is not instrumented so LMS cannot access it – this issue is not an LMS problem, and it is being addressed.]

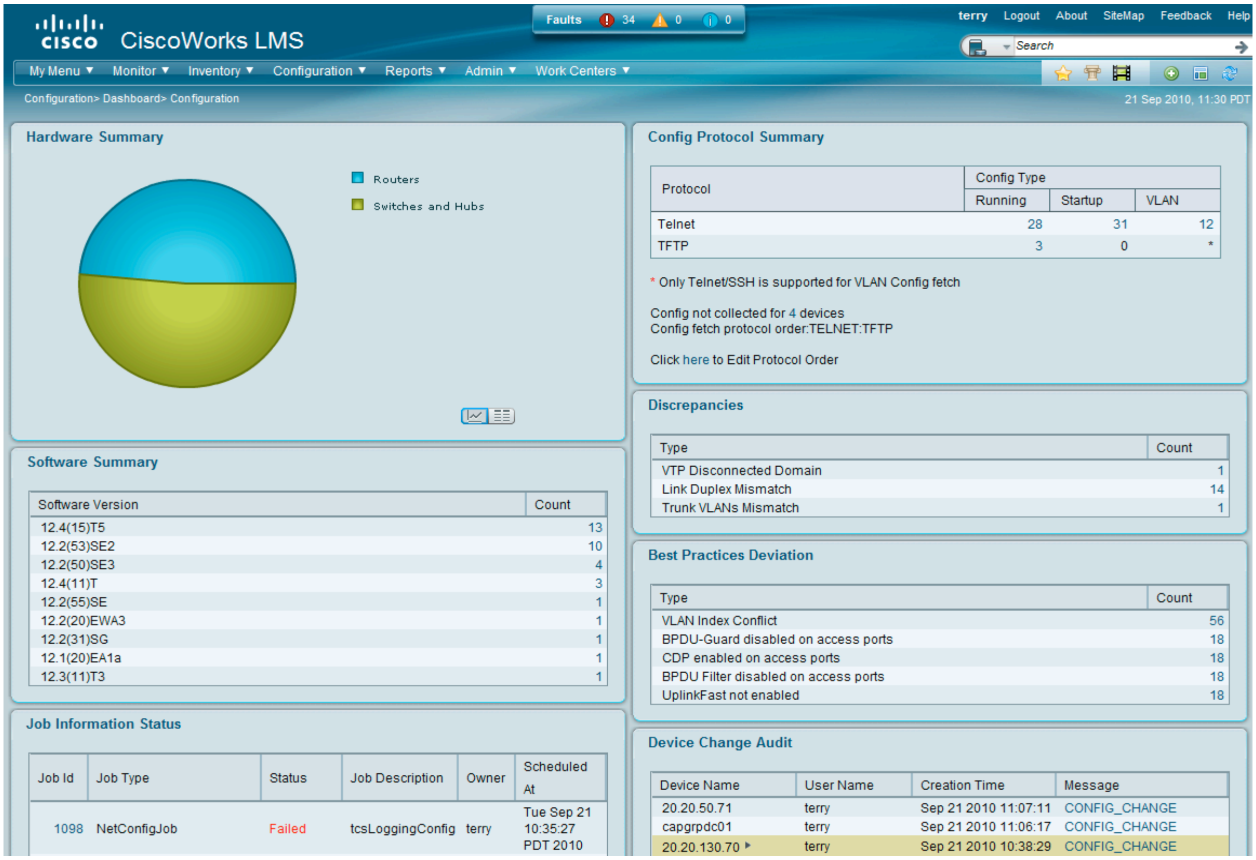
Network Change and Configuration Management

We believe that configuration management is the most critical function of a network management system, because of the large percentage of network failures that are due to configuration errors. Industry studies indicate that forty percent or more of network outages are due to configuration mistakes, so configuration management tools can be extremely useful for making networks more stable.
(See http://www.networkworld.com/newsletters/frame/2004/1025wan1.html)

While a configuration management system does not prevent errors, it allows the network staff to validate planned changes against a design template, to manage and automate the process of rolling out changes, and to perform rapid rollback if a failure occurs.

Configuration Dashboard

The LMS Configuration Dashboard, shown in the next figure, is a fully customizable display of several key functions regarding the configuration of network devices. The dashboard elements, called portlets, can be moved, added, or deleted to prominently show important information.


CiscoWorks LMS
Faults 34 0 0
terry Logout About SiteMap Feedback Help
Search
My Menu ▼ Monitor ▼ Inventory ▼ Configuration ▼ Reports ▼ Admin ▼ Work Centers ▼
Configuration> Dashboard> Configuration
21 Sep 2010, 11:30 PDT
Routers
Switches and Hubs

Hardware Summary

Config Protocol Summary

Protocol	Config Type		
	Running	Startup	VLAN
Telnet	28	31	12
TFTP	3	0	*

* Only Telnet/SSH is supported for VLAN Config fetch

Config not collected for 4 devices
Config fetch protocol order:TELNET:TFTP

Click here to Edit Protocol Order

Software Summary

Software Version	Count
12.4(15)T5	13
12.2(53)SE2	10
12.2(50)SE3	4
12.4(11)T	3
12.2(55)SE	1
12.2(20)EWA3	1
12.2(31)SG	1
12.1(20)EA1a	1
12.3(11)T3	1

Discrepancies

Type	Count
VTP Disconnected Domain	1
Link Duplex Mismatch	14
Trunk VLANs Mismatch	1

Best Practices Deviation

Type	Count
VLAN Index Conflict	56
BPDU-Guard disabled on access ports	18
CDP enabled on access ports	18
BPDU Filter disabled on access ports	18
UplinkFast not enabled	18

Job Information Status

Job Id	Job Type	Status	Job Description	Owner	Scheduled At
1098	NetConfigJob	Failed	tcsLoggingConfig	terry	Tue Sep 21 10:35:27 PDT 2010

Device Change Audit

Device Name	User Name	Creation Time	Message
20.20.50.71	terry	Sep 21 2010 11:07:11	CONFIG_CHANGE
capgrpdc01	terry	Sep 21 2010 11:06:17	CONFIG_CHANGE
20.20.130.70 ▸	terry	Sep 21 2010 10:38:29	CONFIG_CHANGE

Figure 2: LMS Configuration Dashboard

LMS automatically performs analysis of the collected data, as evidenced in the Discrepancies and the Best Practices Deviations functions. The analysis rules for these sections are currently predefined. We hope the analysis rule API will be published in the near future to allow LMS customers to customize the built-in rules as well as design their own, which we believe will significantly increase the utility of LMS.

The Software Summary function is useful for tracking software versions deployed on the network. A small improvement would be to include the device types for each OS version and provide a way to sort by either device type or software version.

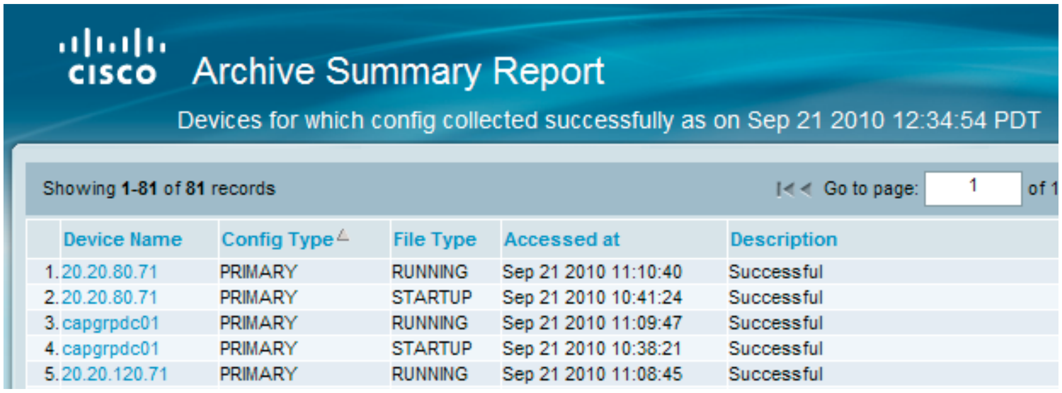
The Device Change Audit and the Job Information Status portlets identify who performed what operations on specific devices or groups of devices. Since configuration changes are the most common source of network problems, examining the Device Change Audit function for modifications made at the time that a problem started can help reduce the time to diagnose a problem.

Device Grouping

Configuration and data access in LMS is performed by selecting either individual devices or groups of devices. Device groups typically correspond to logical operating groups within the network, taking into account the function of devices, such as core, distribution, and access layers, or the location of devices, such as DataCenter1. A variety of criteria can be used to create a device group, including device names, IP addresses, or whether the devices support a specific technology, such as EnergyWise or Smart Ports. Devices can belong to multiple device groups, which increases efficiency for managing device configurations and monitoring performance.

Configuration Archive

LMS can archive device configurations, providing a safety net for when a device completely dies or when a major configuration mistake is made and you need to go back to the prior version. The configuration archive *shadow directory* is an image of the most recent configurations gathered by the configuration archive. We recommend enabling the shadow directory option under the Archive Settings of Archive Management under Configuration Management, storing the configurations in this secondary directory, and mapping that directory to an external file system on another server. With this practice, even if the LMS server is unavailable, you will have a backup of all the device configurations. A useful archive search capability exists for performing configuration searches, but we also like to use Unix tools such as *grep, sort, uniq,* and *wc* to search the configurations in the shadow directory.



Archive Summary Report

Devices for which config collected successfully as on Sep 21 2010 12:34:54 PDT

Showing **1-81** of **81** records

Go to page: 1 of 1

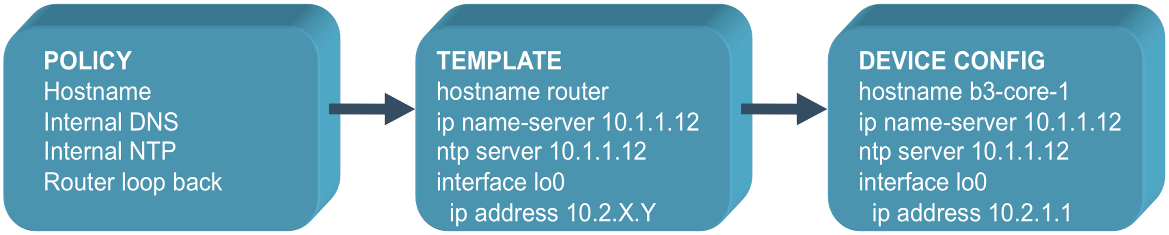
	Device Name	Config Type	File Type	Accessed at	Description
1.	20.20.80.71	PRIMARY	RUNNING	Sep 21 2010 11:10:40	Successful
2.	20.20.80.71	PRIMARY	STARTUP	Sep 21 2010 10:41:24	Successful
3.	capgrpdc01	PRIMARY	RUNNING	Sep 21 2010 11:09:47	Successful
4.	capgrpdc01	PRIMARY	STARTUP	Sep 21 2010 10:38:21	Successful
5.	20.20.120.71	PRIMARY	RUNNING	Sep 21 2010 11:08:45	Successful

Figure 3: LMS Archive Summary Report

We did encounter a minor problem with the *Search Archive* function; our MacBook Pro running Firefox is not a supported platform and the menu did not work correctly. Switching to Internet Explorer or Firefox on a Windows VM solved the problem. We hope that additional standard business platforms will be supported in future LMS releases.

Configuration Compliance

The function that probably provides the greatest benefit after archiving configurations is the ability to check them against network policies. A typical policy definition starts with written requirements, followed by a configuration template that can be used for deploying new devices or that can be used to validate existing device configurations for compliance with the policy. For example, a policy might reflect the desired TACACS+ Authentication, Authorization, and Accounting (AAA) configuration in Cisco network equipment. The process is shown in the following figure.



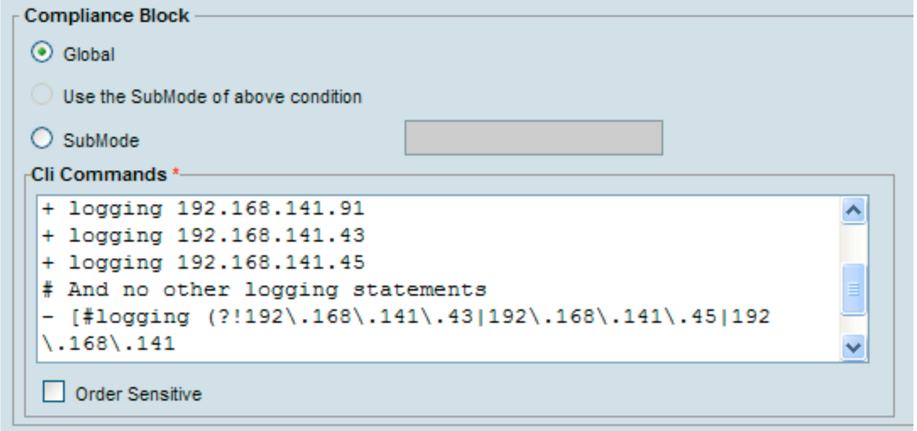
POLICY
Hostname
Internal DNS
Internal NTP
Router loop back

TEMPLATE
```
hostname router
ip name-server 10.1.1.12
ntp server 10.1.1.12
interface lo0
 ip address 10.2.X.Y
```

DEVICE CONFIG
```
hostname b3-core-1
ip name-server 10.1.1.12
ntp server 10.1.1.12
interface lo0
 ip address 10.2.1.1
```

Figure 4: Typical Configuration Compliance Process

The Configuration Compliance Template allowed us to configure a policy:



Compliance Block

● Global

○ Use the SubMode of above condition

○ SubMode

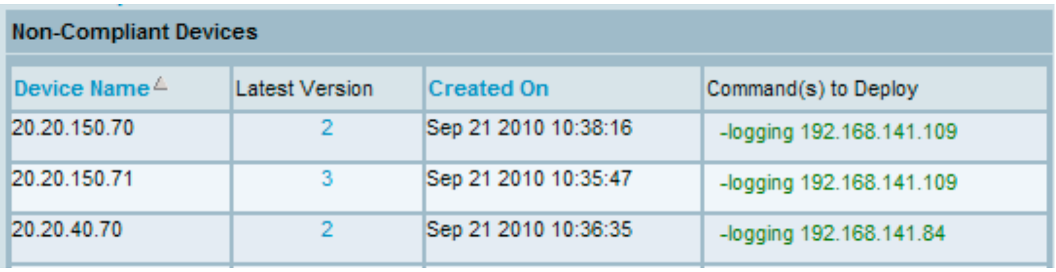
Cli Commands *

```
+ logging 192.168.141.91
+ logging 192.168.141.43
+ logging 192.168.141.45
# And no other logging statements
- [#logging (?!192\.168\.141\.43|192\.168\.141\.45|192
\.168\.141
```

□ Order Sensitive

Figure 5: Creating a Policy Using the Configuration Compliance Template

The LMS compliance policy definition is quite flexible. It can depend on other configuration blocks, it can require commands within a sub-mode, and it can require that the commands appear in a specific order. Policy templates are built using regular expression syntax, which is a powerful pattern matching mechanism, thus the seemingly strange syntax in the example above. Our test checked the logging configuration of the lab devices. Of course, there were initially many exceptions when we ran the policy:

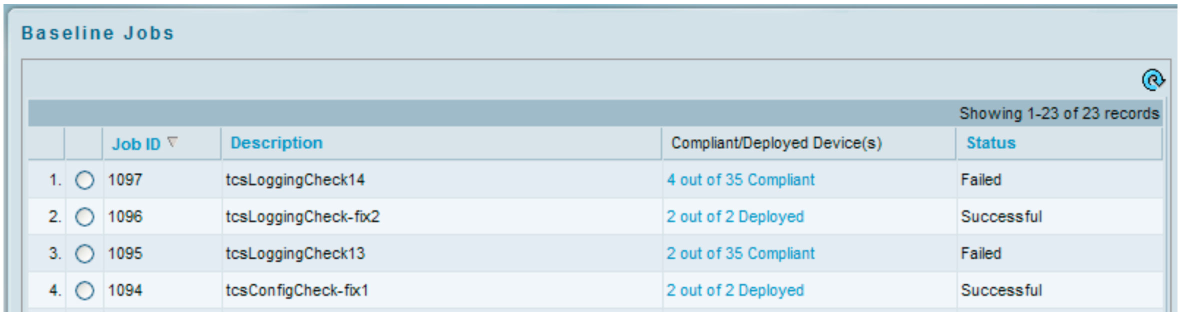


Non-Compliant Devices

Device Name	Latest Version	Created On	Command(s) to Deploy
20.20.150.70	2	Sep 21 2010 10:38:16	-logging 192.168.141.109
20.20.150.71	3	Sep 21 2010 10:35:47	-logging 192.168.141.109
20.20.40.70	2	Sep 21 2010 10:36:35	-logging 192.168.141.84

Figure 6: Summary of Initially Non-Compliant Devices

Deploying configuration changes to remediate the exceptions took a number of steps, but was not difficult and it worked quickly. The job monitoring system clearly showed devices being remediated, and the resulting compliance checks listed the correct number of devices that complied with the policy.



Baseline Jobs

Showing 1-23 of 23 records

		Job ID ▽	Description	Compliant/Deployed Device(s)	Status
1.	○	1097	tcsLoggingCheck14	4 out of 35 Compliant	Failed
2.	○	1096	tcsLoggingCheck-fix2	2 out of 2 Deployed	Successful
3.	○	1095	tcsLoggingCheck13	2 out of 35 Compliant	Failed
4.	○	1094	tcsConfigCheck-fix1	2 out of 2 Deployed	Successful

Figure 7: Baseline Jobs from the Job Monitoring System

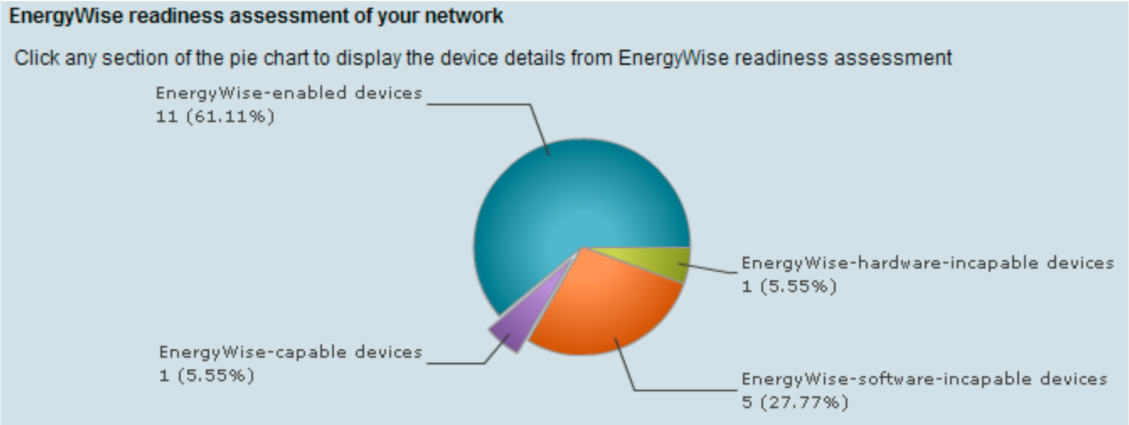
There is a file import function to read configuration commands from a file for those changes that require per-device parameters, such as IP addresses or device names.

Configuration Management Summary

The configuration archiving and management functionality is useful, allowing us to build policies to check configuration consistency and to correct the configurations where they did not match the policy template. The released product will include videos that augment the written documentation to help new users get started and be successful. Like any good network management system that has a lot of power, it will require dedicated time to learn it and be productive.

Work Centers to Simplify Deployments

A Work Center is a set of functions that automate the lifecycle management of deploying and managing a particular technology. The lifecycle begins with assessing whether your network can support the new technologies, making it easier to know when and where you can deploy these new technologies. In addition, LMS 4.0 can help facilitate the deployment of the IOS software versions and configurations that are required for the supported technologies. For example, the Work Center readiness assessment summary for EnergyWise, shown in the following diagram, shows the devices that support it, do not support it, and why they do not support it (software or hardware incapable). Manually performing a readiness assessment in a large network would be time consuming and would likely never be finished. LMS automates the assessment, making this information readily accessible.



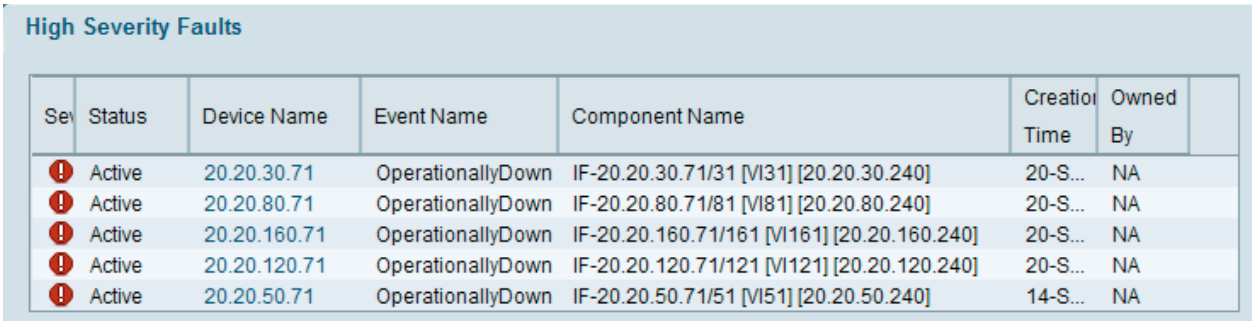
EnergyWise readiness assessment of your network

Click any section of the pie chart to display the device details from EnergyWise readiness assessment

Figure 8: Work Center Readiness Assessment Summary for EnergyWise

Performance and Monitoring

As with most network management products, there are dashboard elements for monitoring faults, performance, and events. Faults are typically due to interface or device failures and appear in a dedicated window in the Monitoring dashboard. In the picture below, a set of operationally down interfaces are identified. Any router interface or link between network infrastructure devices that is in up/down state should be investigated, particularly in highly redundant networks. This practice implies that the network administrators need to shutdown any links that are not used to aid in the identification of redundant link failures. (Setting the interface description to 'unused' also helps.)

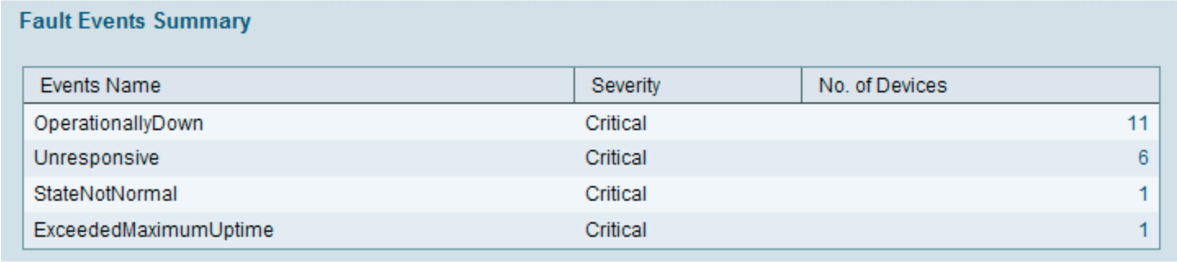


High Severity Faults

Sev	Status	Device Name	Event Name	Component Name	Creatio Time	Owned By	
❗	Active	20.20.30.71	OperationallyDown	IF-20.20.30.71/31 [Vl31] [20.20.30.240]	20-S...	NA	
❗	Active	20.20.80.71	OperationallyDown	IF-20.20.80.71/81 [Vl81] [20.20.80.240]	20-S...	NA	
❗	Active	20.20.160.71	OperationallyDown	IF-20.20.160.71/161 [Vl161] [20.20.160.240]	20-S...	NA	
❗	Active	20.20.120.71	OperationallyDown	IF-20.20.120.71/121 [Vl121] [20.20.120.240]	20-S...	NA	
❗	Active	20.20.50.71	OperationallyDown	IF-20.20.50.71/51 [Vl51] [20.20.50.240]	14-S...	NA	

Figure 9: High Severity Faults from the Monitoring Dashboard

In addition to the specific faults shown above, LMS includes an events summary that shows exceptions, sorted by severity (see the following diagram). The summary includes events such as devices that are no longer responding, perhaps because they are unreachable or because they have crashed. Abnormal events are also logged, such as power supply failures and high temperature (StateNotNormal) and backup or dial interfaces that are up for long times (ExceededMaximumUptime). The *No. of Devices* column contains links to view the devices with each fault.



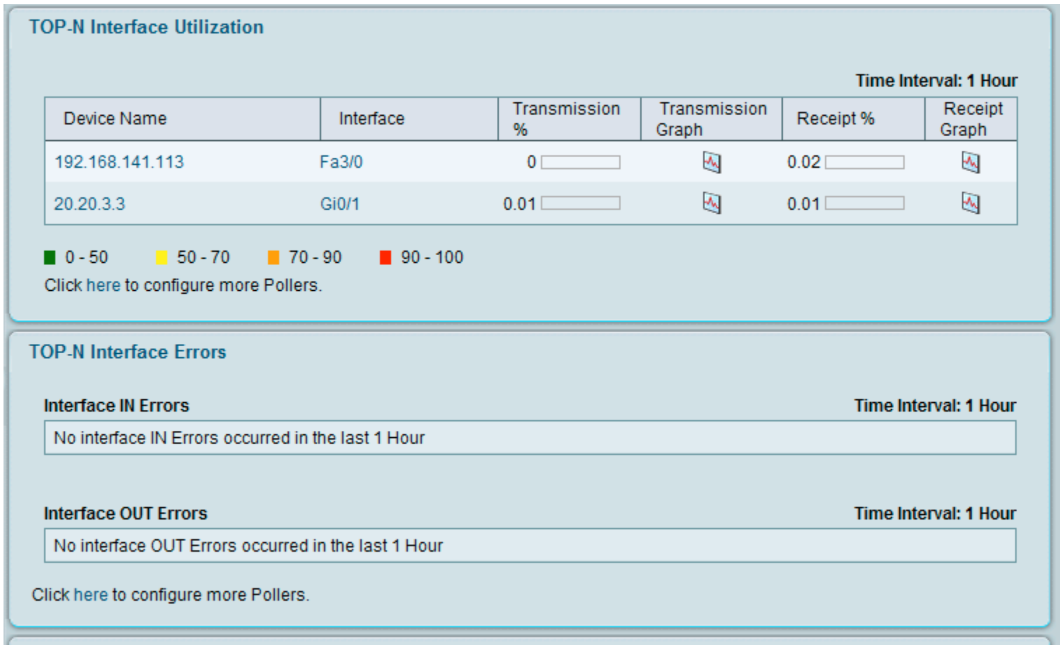
Fault Events Summary

Events Name	Severity	No. of Devices
OperationallyDown	Critical	11
Unresponsive	Critical	6
StateNotNormal	Critical	1
ExceededMaximumUptime	Critical	1

Figure 10: LMS Fault Events Summary

After fault and event handling, performance information is probably the most requested capability in a network management system. (Configuration management is the next most frequently requested capability, due to the number of network outages that result from lack of configuration management, but most managers focus on performance before configuration management.) The LMS monitoring dashboard includes the standard displays of device CPU and memory utilization.

LMS also has interface reporting that includes metrics such as utilization, errors, and discards, shown in the following diagrams:



TOP-N Interface Utilization

Time Interval: 1 Hour

Device Name	Interface	Transmission %	Transmission Graph	Receipt %	Receipt Graph
192.168.141.113	Fa3/0	0	📈	0.02	📈
20.20.3.3	Gi0/1	0.01	📈	0.01	📈

🟩 0 - 50 🟨 50 - 70 🟧 70 - 90 🟥 90 - 100

Click here to configure more Pollers.

TOP-N Interface Errors

Interface IN Errors — Time Interval: 1 Hour

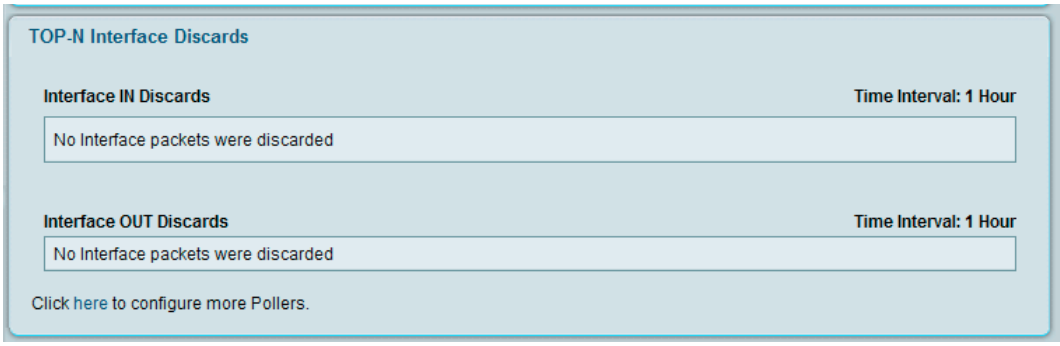
No interface IN Errors occurred in the last 1 Hour

Interface OUT Errors — Time Interval: 1 Hour

No interface OUT Errors occurred in the last 1 Hour

Click here to configure more Pollers.

Figure 11: LMS Interface Reporting for Utilization and Errors



TOP-N Interface Discards

Interface IN Discards — Time Interval: 1 Hour

No Interface packets were discarded

Interface OUT Discards — Time Interval: 1 Hour

No Interface packets were discarded

Click here to configure more Pollers.

Figure 12: LMS Interface Reporting for Discards

Topology

Topology diagrams are indispensible when troubleshooting, and LMS provides a topology display and editor. It relies on the CDP and other data collected during its normal polling process to identify the interconnections between devices. Hovering the cursor over a device or a link shows detailed information about that element. We prefer topology displays that include logical and physical information, such as IP addresses, VLAN names/numbers, and interface identifiers, but that would make the diagram difficult to read. The topology display uses a java web-start application to provide basic editing and layout capability. By adjusting the topology map, we were able to take a topology diagram that was initially unreadable and easily tweak it into a drawing that shows the hierarchical connectivity that exists.

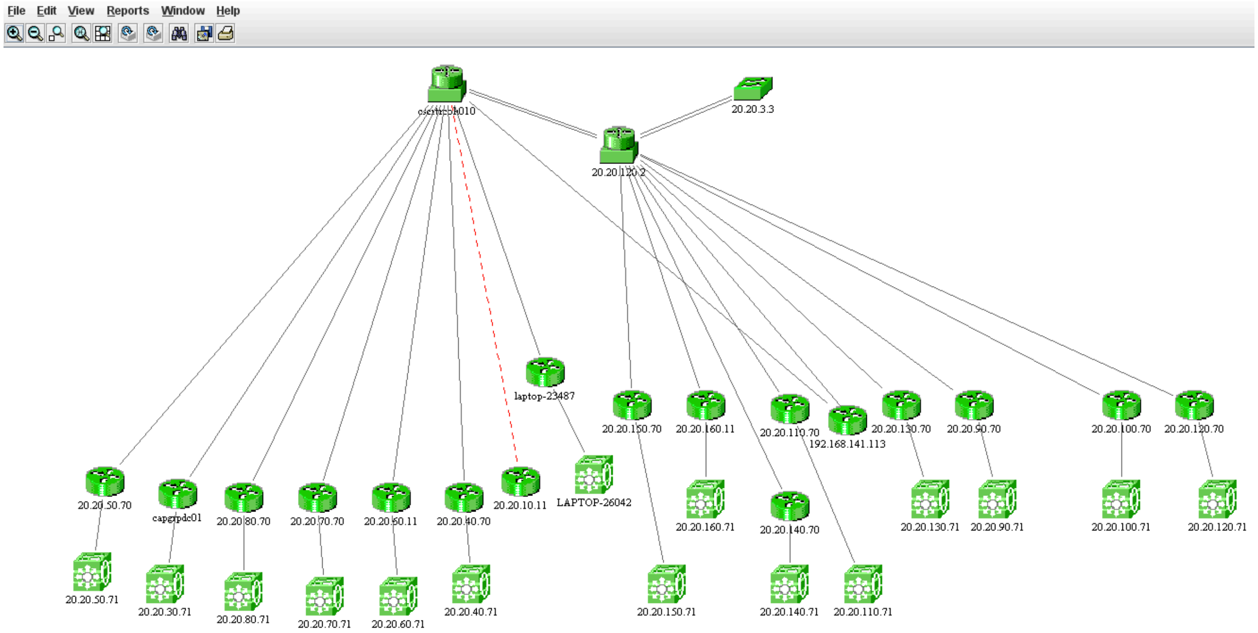


Figure 13: Example LMS Topology Map

Published Database Schema

The LMS 4.0 database schema is published, and APIs for various methods of database access are provided. (Note that LMS 3.2 also published its schema.) This is a huge benefit because it gives the network staff the ability to perform data searching and queries that would have previously not been possible. There are also per-device user-defined fields that can contain additional data about the device, such as its specific location. For example, in other products we have seen custom database fields used to store latitude and longitude, which are then used with Google Maps or Google Earth to create a display of device locations. Other organizations use these fields to store maintenance contract information or lease renewal dates, keeping the data with the device’s management information.

Summary

Key Benefits and Strengths

The updated UI is more web-friendly. The different modules that made up prior versions of LMS have been merged together in 4.0, making it easier to use. Data no longer needs to be imported and exported between modules. Portlets allow customization of individual pages to match an organization's monitoring requirements. Configuration management is more advanced, with configuration policy compliance, configuration update, and change management functions. Support for deploying new technologies such as EnergyWise and Auto Smart Ports have been enhanced. Event processing helps reduce the number of events that must be individually handled, and performance management still provides visibility into network health. Access to the database schema and per-device custom data fields allows network managers and developers to add new functionality that was previously impossible.

Areas for Improvement

Of course, LMS 4.0 is not perfect. The top enhancements we would like to see include:

- Optimize workflows by grouping of functions to make it easy to accomplish common tasks. For example, the information page about a device contains a section labeled "Configuration," which surprisingly does not have a link to the configuration archive for that device. Since all the configuration data is available in LMS, this enhancement could improve the efficiency of the UI.
- Add de-duplication and correlation to event management, as is found in other event management products.
- Significantly improve the written documentation, focusing on network management tasks instead of the emphasis on what each button and dialog box does. Fortunately, there is good online help and short videos on how to accomplish tasks. Until you get accustomed to the menu layout, you will likely spend some time looking for key functions. This is where My Menu will be useful – you can put your frequently used functions in a private or public menu.
- Improve scalability and performance by optimizing the data collection engine. This enhancement will scale LMS to support larger networks and provide better overall performance when LMS is running in smaller networks.
- Support the ability to save/load files from the system on which the web browser is running and not require access to the LMS server file system. This would optimize the operations that save or load files from the LMS server's file system and require LMS users to have access to the file system.

Overall Thoughts on LMS 4.0

LMS 4.0 is a significant improvement over prior versions of LMS. The integration of the different tools into one product that uses a common underlying database provides a much-needed improvement in the usability of the system. Importing data between the internal components is no longer needed, making the network administrators more productive.

The configuration management functionality is exactly what is needed. It has the ability to verify that configurations match network and corporate policies, including the often-overlooked ability to check that the configurations do not include undesirable commands.

About Chesapeake NetCraftsmen

Chesapeake NetCraftsmen, LLC is an advanced network consulting firm that specializes in high-profile and challenging network consulting jobs. A third of the company are CCIEs across the spectrum of specializations. NetCraftsmen is a Premier Cisco Partner, with a large number of Cisco specializations.

Terry Slattery is a Principal Consultant at Chesapeake NetCraftsmen. He previously founded Netcordia and Chesapeake Computer Consultants, invented NetMRI, a network management appliance, and the v-Lab hands-on training system. Terry co-authored the successful McGraw-Hill text Advanced IP Routing in Cisco Networks, and is the second Cisco Certified Internetwork Expert (CCIE #1026) awarded. He focuses on route/switch and network management technologies.

Carole Warner Reece is a Senior Consultant at Chesapeake NetCraftsmen. She is certified by Cisco as CCIE #5168 and also a certified instructor (CCSI #31564). Three of her current interests are course development, network design and operations, and exploring data center solutions for our customers.

Chesapeake NETCRAFTSMEN

Chesapeake NetCraftsmen, LLC.
1290 Bay Dale Drive, Suite #312
Arnold, MD 21012
1-888-804-1717
www.NetCraftsmen.net