Policy-Based Network Management for Services Automation

White Paper

Contents

Executive Summary

This document is written for network managers, network engineers, and business executives responsible for managing business-critical networks. It discusses how policies, in the form of rules, can be used to automate various services provided by Cisco.

Introduction

Cisco offers a number of services that augment the corporation's other network management applications to provide actionable, analyzed network data for network managers and executives to use during the network development phases suggested by Information Technology Infrastructure Library (ITIL) Version 3: service stratgey, service design, service implemention, service operate, and continious service improvement. The ITIL phases are equivalent to the Cisco prepare, plan, design, implement, operate, and optimize (PPDIOO) phases.

The services offered by Cisco incorporate collection of customer network data and analysis of this data in comparision to custom (customer specific) or Cisco® Advanced Services recommended policies for configurations (best practices) and syslogs. Data is matched against Cisco's databases of inventory-specific information such as product end-of-life bulletins, field notices, and security alerts, as well as software feature and image analysis, to facilitate accurate software risk analysis. Network assessments collect command-line interface (CLI) and Simple Network Management Protocol (SNMP) MIB data to analyze performance, capacity, protocols, faults, configuration, security, and other aspects of devices and the network. Assessments can also be used to create baselines and benchmarks and analyze compliance such as for security compliance to regulatory standards.

For more than a decade, Cisco has provided services for customers that include the collection and analysis of network inventory and other network device information and the application of policies for analysis of various aspects of the devices in the network. These capabilities have been improved over the years and expanded to include additional capabilities. Customers who do not have these services or who have other vendors' applications or services that do not include Cisco's capabilities may have to perform this analysis manually, which is time consuming and often requires a skilled networking engineer to interpret the results.

Business Needs

Network managers and executives need to know what devices the network includes, how the network is performing, and whether any specific changes would improve the network on which their business relies. The network inventory for matching against bulletins required to perform accurate analysis is notoriously difficult to identify, whether it involves determining which products are reaching the end of their life and should be replaced or updated because of rising support costs or network improvement requirements, products with field notices against them, or software planning required as a result of software bulletins.

Understanding the entire network topology and the relationships among the devices as well as the protocols and solutions running on the network is a complex task and requires well-trained and knowledgeable engineers. Retention of this knowledge by encoding it into policies helps ensure that if the engineer is no longer available, this knowledge is not lost.

In addition, network engineers can examine the data for a device and provide analysis based on their expertise, but they may not benefit from the knowledge of other experts. By using services automation tools, the user gains the expert analysis of many engineers, and the system can automatically analyze millions of devices daily in a 24-hour period, rather than having to rely on local staff to manually analyze the data.

Target Market

Cisco service automation and policy-based analysis service offers are targeted at enterprises and service providers as well as the commercial market and include most customers of most sizes. Some of these offers are provided directly by Cisco, and others are provided through Cisco partners.

The services are limited only by the ability to collect accurate data from a product and the policies created for use with those products as well as the availability of common databases. Some acquired products may take a longer time to be integrated into the services automation solution.

Technology

Policies - what Cisco calls rules-based intellectual capital (RBIC) - allows consistent analysis across multiple devices in the network. The policy knowledge may be provided by Cisco network consulting engineers and other Cisco experts, or it may be provided in customer-specific custom policies that have been developed in conjunction with a CCIE® certification.

Cisco uses both custom analysis engines and industry-standard analysis engines and languages to create the analysis environment to provide various types of analysis for services automation.

The Cisco Solution

Cisco has created a suite of applications and methodologies to capture intellectual capital. This intellectual capital can be used by engineers within Cisco to share knowledge; it can also be automated in RBIC policies so that vast numbers of customer devices can be matched against this knowledge and reports generated to inform engineers and customers about issues seen in the device or network. RBIC can be used to match the following to customer network inventory:

- End-of-life bulletins
- Hardware field notices
- Security advisories
- Configuration best-practice exceptions and software features in configurations
- Assessments of performance, capacity, faults, security, design, and other aspects of the network and devices in the network

What Is Policy-Based Network Management?

Inventory is the basic building block of policy-based management solutions. After the inventory data is collected, it can be processed by policy-based applications to help ensure data integrity; then policies can be applied to analyze the devices and the network. In deploying services automation, policies should be applied only if the inventory is correct; otherwise, false or inaccurate information may be passed to the customer regarding the customer's network, and the customer will lose satisfaction with Cisco services. Uses of the inventory data include providing accurate data to Cisco account teams regarding equipment that is reaching the end of its life. This information helps sales staff; it also helps customers keep up-to-date and provide more stable and reliable networks to meet their business needs. Accurate inventory also helps ensure that customers retain service contracts with Cisco or Cisco partners and that Cisco is supporting devices under contract. By bringing the inventory data back to Cisco, the data can be compared against Cisco databases, and contracts can be updated to help ensure that customers get the support they need. Accurate inventory also allows Cisco to help the customer plan for capacity in the network and software upgrades and take other proactive actions.

In an ideal situation, a device can be interrogated electronically, and network management can occur automatically. The data is summarized and consolidated so that sound decisions can be made regarding the management of the device. Unfortunately, many devices fall short of the ideal, and various workarounds may be necessary to collect and analyze the data from a device. Policies may be created to collect additional information not traditionally collected by a network management system to complete the inventory of some devices. The application of policies or rules to determine the correctness of the data is called explicit or low-level knowledge. This information is usually readily available, but a lot of effort is needed to look up one device at a time. To meet this challenge, Cisco has created hierarchical model rules to determine what to collect in very specific cases. Cisco also offers collection rules that are conditional, with which some data is collected and parsed and then used as input for another collection operation. In addition, collection can be limited based on rules that act on the inventory so that if certain inventory values are identified, the collection skips specified items that are known to cause problems in a device running specified versions of an operating system.

The workarounds are policies put into place based on criteria for organizing device inventories. These policies allow users to sort and report on only the devices in which they are interested at any particular time. The policies that define the device inventory can be organized hierarchically to optimize the performance of the management application and reduce the amount of code required. This process implies inheritance of attributes based on the policies. After the device inventory data is collected, other policies can be applied to the data to specify actions to take based on criteria determined by the policies. Policies based on inventory can be created that identify defective printed circuit board assemblies, software security vulnerabilities, obsolete components and devices, and other attributes. Policies can also be written to determine future requirements based on the inventory such as capacity planning and software upgrade planning.

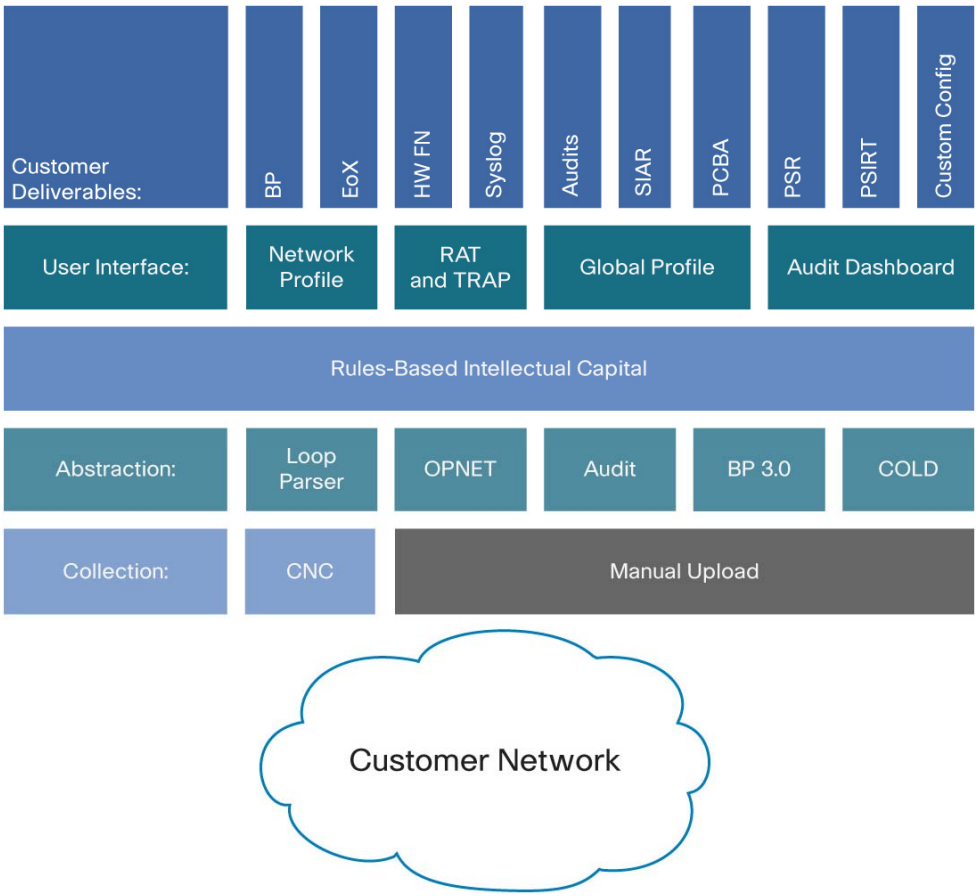
Some of the uses of accurate inventory are end-of-life analysis, field notice application, security advisory (software) matching, and the application of particular policies based on the inventory of the device. In this last application, the inventory analysis becomes part of the logic of the policy being applied since the policy requires that it be applied only to a particular subsegment of the inventory or even just one particular device name or group of devices performing a particular role in the network such as the core, distribution, or access role.

Beyond Device Management to Network Management: Services Automation

Inventory and the identification of a device is only the beginning of services automation. Just as each customer needs to know what devices it has purchased and how they are performing, so does Cisco. When Cisco has information about a customer’s network devices, Cisco can offer additional services. Some services can be included in a hardware or software support contract. In addition, Cisco can offer proactive services that can help optimize the performance of the customer network as well as assessments to determine what the network can support now in terms of business benefits, and what changes are needed to support additional capabilities that the business desires.

Figure 1 shows a conceptualized diagram of some policy-based analysis and the architecture to enable the services automation.

Figure 1. Knowledge-Focused Architecture



The Need for Data Integrity

It is important to know that the collected data is accurate. It is not enough to collect the data and simply trust it. The data must constantly be evaluated and tested based on the experience of knowledgeable engineers to help ensure data integrity. Incorrect data may be the result of software faults in which the instrumentation of a device has a problem. When this fault is identified and fixed, a software upgrade should resolve the data integrity problem. Sometimes a device does not support instrumentation to display certain desired parameters. In these situations, often a workaround can be created to collect the desired data. With the continual development of new devices and software, Cisco has made new SNMP MIB support and instrumentation a very high priority to make network management easier.

One aspect of data integrity that may not always be available directly to the customer but which can be implemented by Cisco as a service is a check of inventory data against what was manufactured or sold. By collecting inventory data and then comparing that data with manufacturing and contract data, the inventory can be validated and a result returned to the customer with the corrected data. After the data is validated, it can be used to enhance service-level agreements (SLAs) and help ensure that the customer receives the service to which the customer is entitled. For services automation, accurate data is essential.

Basic Network Management Model

Using the International Telecommunications Union's Telecommunication Standardization Sector (ITU-T) Telecommunications Management Network (TMN) fault, configuration, accounting, performance, and security (FCAPS) network management model, the types of analysis can be categorized and policies written for each area of the model. These categories can be further divided into subcategories depending on the vocabulary needed to

identify and organize the data returned. For example, the security area may include protocol-related policies of interest, such as policies for Border Gateway Protocol (BGP) authentication. The taxonomy used to identify policies needs to be standardized to allow both internal and external users of the system to understand what is being analyzed. An industry-standard taxonomy is best, but if none exists, then a vendor-specific one that most constituents understand can be used. These constituents include marketing, engineering, technical support, and consulting personnel; partners; and customers. Standardizing the taxonomy enables policies to be reused between applications, saving engineering and development resources. This type of knowledge applied in policies is called implicit, or high-level, knowledge. This knowledge is based on experience and in-depth research to determine operational parameters (thresholds) and solutions to problems that have been encountered before.

Fault Management

After the device inventory has been identified, policies can be applied to collected data from a device and various types of faults determined. These faults may be hardware or software failures or failures of specific functions running on a device such as protocols and data transiting the network device. Fault management concept policies are applied to networks, but they can also be applied to any system requiring management.

In general, all faults are either hardware or software failures, but these two categories can be subdivided into smaller components. For instance, a networking protocol is defined in software, and any faults detected in the way it functions will be considered software faults. Some faults may refer to capacity problems and others to configuration problems, so it is important to organize the results of any policies so that they can be effectively interpreted to identify the actions to take to correct the situation. Using the Open Systems Interconnection (OSI) seven-layer network model, a policy can be created that identifies a fault at the physical layer, and this policy can be applied to a network-based policy that identifies problems at Layers 3 or higher.

It is not always adequate to identify a physical or even a software problem on a single device. Often the operations staff needs to identify how a problem affects applications and users throughout the network. Many customers need to identify the extent of a network outage for SLAs between themselves and vendors. These could be the suppliers of equipment or services to the network. It is also important to determine when a problem is detected and when it is corrected to determine mean time to resolution (MTTR) and mean time between faults (MTBF) for both software and hardware. By building into any network management system a means to track the health of devices and the network and to trend the data, decisions can be made regarding the severity of problems and how quickly certain failures should be repaired. With limited resources, this type of determination can be invaluable to IT managers.

Exception Example: Interface Alignment Errors

Description: Alignment errors received count is greater than 0.1 percent of input packets. The count indicates the number of received error frames not ending with an even number of octets and having a bad cyclic redundancy check (CRC) result. This result is representative of alignment errors relative to received frames.

Recommendation: Monitor these errors closely to determine the possible cause. These errors are typically related to a cabling problem and sometimes increase after initial attachment of a cable to a port. They may also be evident in conjunction with frame check sequence (FCS) errors and may indicate port and speed mismatch between the switch port and end host.

Configuration Management

Configuration management usually refers to management of configuration changes and making sure that a backup of the device configuration is available in case a problem occurs and the configuration needs to be restored. Management also requires knowing who made changes in a device configuration and when the changes were made. In addition to these management processes, Cisco analyzes the configuration of a device to determine how the device is configured. Rule-Based Markup Language (RBML) rules are created to determine which software features are configured and how they are configured. (Other representations of the rules are also used in some applications.)

Cisco knowledge is added to the rules in the form of best practices, which are policies that tell the customer whether a device is not configured optimally according to Cisco. Consistency of configuration between devices is also examined to determine whether a group of devices in the network is configured according to a policy. Counts of configuration items are also identified and policies applied to help optimize performance.

As part of configuration analysis, the software features are identified. This information is added to the inventory to identify which software features are active on a device.

Another aspect of device and network configuration management is analysis to identify how the network is configured in order to apply additional policies for performance optimization. Many of the assessments that Cisco performs examine the configuration as well as other CLI and SNMP data to determine how the devices and the network are configured.

It is not enough to determine that there is an exception to a policy, but the RBIC also includes a recommendation and proposed corrective action as wells a additional references for more information.

Exception Example: Multicast Source Discovery Protocol Without the Originator ID Configured

Description: Many networks use Multicast Source Discovery Protocol (MSDP) in conjunction with Anycast Rendevous Point (RP) Protocol. The originator ID must be used in this case, referencing an interface with a unique IP address (usually **Loopback0**). For other environments, the originator ID is recommended.

Recommendation: Specify the interface to use as the MSDP originator ID.

Corrective Action: Configure **ip msdp originator-id Loopback0.**

Accounting Management
Network accounting management examines who is doing what in the network. In some ways, accounting management is associated with security, but generally it assesses which users are using the network and how much of the network resources each user and business unit in the organization is using. This information can be used for billing back to individuals or departments, etc. Often the collection process is implemented by deploying software agents or hardware probes on the network to monitor the data flowing through the network; an application then uses this information to create reports for management.

Performance Management
Performance management involves the collection of performance-related data from a device. This data can be information about CPU utilization, memory utilization, interface utilization, protocol utilization in the form of number of packets transmitted or received, etc.

Another part of performance management is capacity planning. For devices and the network to perform properly, the network design and the device hardware and software must be able to handle the capacity of the traffic passing through the network. Capacity planning involves collecting and monitoring some of the performance data. It also includes assessing the number of ports, number of slots, memory size, amount of bandwidth, etc. This information can be used for spares planning, failover planning, upgrade planning, the addition of traffic or applications on the device or network, etc.

Exception Example: Ternary Content Addressable Memory Overutilized on Cisco Catalyst 6500 and 7600 Series Switches

Description: If ternary content addressable memory (TCAM) is nearly full, the supervisor turns on aggressive aging, when the table size reaches almost 90 percent capacity. The supervisor checks every 30 seconds to see how full the NetFlow table is. The concept of aggressive aging is that if the table is nearly full, new active flows may not be able to be created; hence, the less active (or inactive) flows in the table are aggressively aged out to make space for more active flows in the table. Cisco Catalyst® Supervisor Engines 720 and 32 use Multilayer Switching (MLS) entries for

traffic accounting and features such as reflexive access control list (ACL), Network Address Translation (NAT), Cisco IOS® Software server load balancing (SLB), and microflow policing.

Recommendation: Reducing the granularity of the NetFlow mask or tuning NetFlow timers to aggressively age out unused entries are two methods of lowering TCAM utilization. Upgrading to newer policy feature cards or supervisors with increased NetFlow capacity is also recommended.

Security Management

Security management involves monitoring the policies for access to the devices in the network and the policies specifying who has access to the network to pass traffic across it. Part of this management involves monitoring device configurations, and part involves monitoring the traffic and device logs to determine whether policies are being breached or the network is being attacked.

Exception Example: Enable Password Not Adequately Protected

Description: The **enable password** command is used to access privileged mode on a device. The device should be protected with the command **enable secret**. The **enable secret** command implements a stronger encryption algorithm than the **enable password** command and should be used. If both commands are configured on a device, Cisco IOS Software will use **enable secret**.

Recommendation: Use **enable secret** to protect the privileged-mode password.

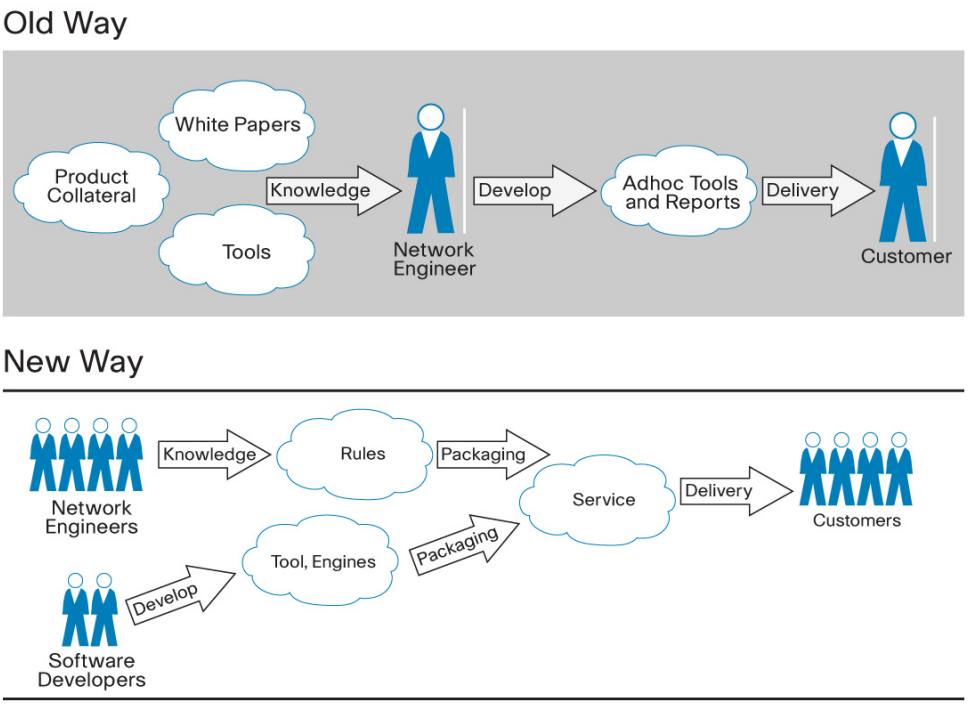
Corrective Action: Configure **enable secret**.

Why Use Policy-Based Network Management and RBML?

Policies are based on knowledge. This knowledge is based on many sources of data including common practices, experience, white papers, conversations, and laboratory work. Some of this knowledge may be published as part of software discrepancy reports (bugs) or hardware and software field notices, Cisco Technical Assistance Center (TAC) cases, network design documents, troubleshooting guides, etc.

The problem with much of this knowledge is that it is held in individual's minds or in papers and websites. The knowledge can be transferred to other individuals who read the information available, or it can be learned by experience. The problem with this approach is that each individual has different experiences and abilities and may resolve problems differently. The knowledge may be documented differently in different locations and sometimes may be incorrect, or the knowledge may change over time. With the knowledge contained in many locations, it is difficult or impossible to keep it updated. It is also not possible to apply the knowledge to large numbers of devices or networks since the knowledge must be brought to the device or network by the engineer using a "stare and compare" method of detecting and troubleshooting a problem. A solution to these challenges is to embed the knowledge in a document that can be interpreted by an application. Figure 2 illustrates the differences between the older and newer approaches.

Figure 2. Changing Approach to Services Automation



With the new approach, the knowledge becomes portable and reusable. To make it even more reusable, the knowledge can be divided into individual policies. These can then be mixed and matched depending on needs and incorporated into many applications rather than just one. For example, a policy that identifies a threshold of CPU utilization on a device can be used for general capacity planning or fault identification, or it can be used to determine whether a device can support additional applications in the network. This same policy can be used to monitor a network on a regular basis, or it can be applied in an assessment of the network prior to upgrade planning or as part of network optimization analysis.

Some knowledge may be considered common knowledge and is needed to operate a network in general. Other knowledge is considered intellectual capital or intellectual property knowledge and must be protected against disclosure because it has inherent value and can be charged for or provide competitive advantage. This type of knowledge is often time sensitive and not possessed by many, or any, other organizations. Over time, it may become common knowledge and lose its inherent value. It may still be needed for managing a network and can be applied through automation, but users may be less likely to want to pay a premium for it.

Another aspect of policy-based management, helping provide modularity, is keeping the policies free of embedded code. In this way, policies can be ported to many different formats for consumption by various applications, regardless of the language in which the application is written. If policies include embedded code, they become dependent on the version of the code in which they are written. Many analysis systems are written in a particular language such as Perl, Python, or Maven and embed knowledge in an application. These systems are not portable or easily reusable. If a revision to the knowledge is required, then the application requires revision. If the policies are maintained outside the application, then each policy can be updated or maintained without regard to the consuming application.

Cisco uses an XML-based schema called RBML to capture knowledge in the form of policies, or rules. The rules can be used individually, hierarchically, or in groups to collect, parse, analyze, and present information about devices and networks to the customer. Different kinds of rules are used for different purposes. Some are used for collection of inventory and have built-in mapping and analysis to collect accurate inventory data. This mapping and analysis can be considered knowledge since there is no automated way of performing this mapping or applying the analysis

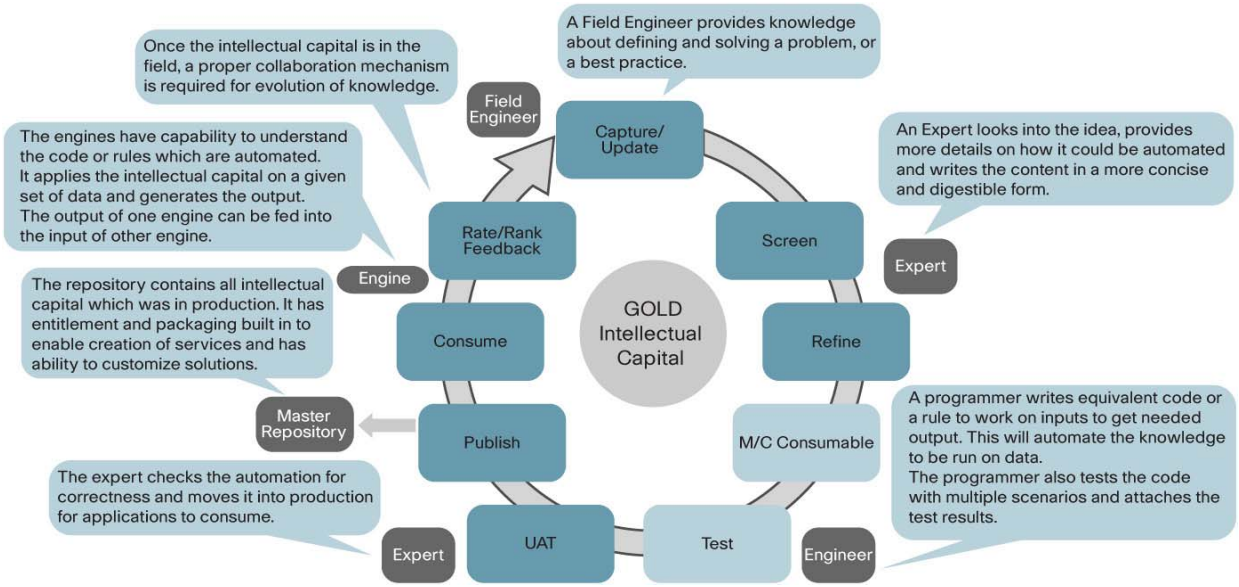
without the use of the policy or rule. If the knowledge to be applied were the same for all uses of a rule, then the rule could be a function embedded in an application. But since each device, network, protocol, threshold, etc. is different, putting this knowledge into a rule makes it reusable and allows it to be changed without having to change the consuming application.

This behavior holds true for the use of rules on various devices. One policy may apply to one device, but not another. By identifying in the rule certain attributes of a device to which to apply the rule, more accuracy can be attained in the results. If rules are applied inappropriately, then exceptions may be reported, and more work and analysis will be needed to determine that there is not a problem with that device. Also, by applying rules only as needed, the application can be optimized for performance.

Knowledge can be captured in many ways such as in the form of white papers, web pages, case management systems, Tcl scripts, etc., or within RBML rules or other rule languages. A simple text editor is all that is needed to write XML, but the script writer must understand the format and syntax and schema of the language. Many users of knowledge do not want to know the details of how the knowledge is applied; they just want to be able to submit knowledge for a white paper or system and let it be shared in any way possible that the document can be distributed.

Cisco has created a knowledge management system to organize, control, update, and otherwise maintain the knowledge. Often knowledge in the form of policies or white papers may need to be updated, or deprecated when it is no longer needed. An organization's managers may also want metrics identifying what knowledge is in the system, where gaps exist in the knowledge, who is creating or updating knowledge, etc. The knowledge management system also provides a workflow that allows one individual or many individuals or groups to work on a piece of knowledge at various stages while maintaining control of the knowledge. After the knowledge is captured in a rule, it is stored in a location that allows it to be consumed by an application or many applications or viewed as an individual document of knowledge. This knowledge can be reused many times. The knowledge contained in the individual rules can also be compiled into a white paper or other document that can be posted or distributed or otherwise reused. Figure 3 shows the management cycle for this intellectual capital.

Figure 3. Intellectual Capital Management



Conclusion

Policy-based management for services automation is a very powerful approach. It provides the methodology to retain and apply network consulting engineer's knowledge to vast numbers of devices in a network to identify weaknesses in design, software, capacity, supportability, and many other areas important for a stable and reliable network. Policies are reusable between applications and customers, saving engineering time and providing consistent analysis for various problem types in networks. Maintenance of the knowledge base is improved by the use of a single source for each policy that can be used by various applications and organizations within Cisco.

For More Information

The following references are links to some of the services offered by Cisco that use Policies and Cisco intellectual capital:

- Cisco Advanced Services - Network Optimization Service: http://www.cisco.com/en/US/services/ps2961/ps6897/Network_Optimization_Service_AAG.pdf
- Smart Care: http://www.cisco.com/en/US/products/ps7343/serv_group_home.html
- Smart Call Home: http://www.cisco.com/en/US/products/ps7334/serv_home.html
- Output Interpeter: https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl
- Cisco Advanced Services - Security Services: http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html
- Cisco Advanced Services - Wireless LAN Services: http://www.cisco.com/en/US/products/ps8306/serv_home.html
- Cisco Advanced Services - IP Communications Services: http://www.cisco.com/en/US/products/svcs/ps2961/ps2664/serv_group_home.html

Appendix

A Sample Configuration Best-Practice Rule

Table 1 provides an example of the configuration best-practice rule.

Table 1. Sample Configuration Best-Practice Rule

Exception	
Description Router interfaces may allow directed broadcasts to be used as amplifiers in smurf denial-of-service (DoS) attacks. In Cisco IOS Software releases earlier than Release 12.1, the default behavior was to permit directed broadcasts.	
Category	Security
Risk	High
Recommendation Make sure that **ip directed-broadcast** is not enabled on any interface.	
Corrective Action Enable **no ip directed broadcast** on all interfaces.	
Note If wake-on-LAN (WOL) is being used in the network, **ip directed-broadcast** must be enabled on the end-user LAN interface. In these cases, the **directed-broadcast** command should be used in conjunction with an extended ACL that permits only the User Datagram Protocol (UDP) port number (typically the discard port) that is being used by WOL. Although this restriction still leaves the network exposed to attacks based on directed broadcasts, the risk is much lower because of the use of the extended ACL.	
Devices Affected See Table 2.	
Reference URLs Additional Information http://www.cisco.com/en/US/docs/ios/12_1/iproute/configuration/guide/1cdipadr.html	

Table 2. Devices Affected

Device Name	Chassis	OS Version
la2501.ca.xyz.com	cisco2502	Cisco IOS Software Release 11.1(16)
ro4503.nj.xyz.com	cisco4500	Cisco IOS Software Release 11.1(16)
ro4504.nj.xyz.com	cisco4500	Cisco IOS Software Release 11.1(16)
sa4500.ca.xyz.com	cisco4500	Cisco IOS Software Release 11.1(16)
wi2501.pa.xyz.com	cisco2502	Cisco IOS Software Release 11.1(16)
wo2501.tx.xyz.com	cisco2502	Cisco IOS Software Release 11.1(16)

B Sample Audit Table and Rules

The following is the top text of a table in the audit which gives information about what the table is about:

Catalyst 6500 and Cisco 7600 Series High Availability(HA) - System Audit

The Cisco Catalyst 6500 and Cisco 7600 Series rules assume that each multilayer switch feature card (MSFC) routing module running Cisco IOS Software can be correlated with a supervisor running the Cisco Catalyst OS in the same chassis. The purpose of this table is to identify the switches that cannot be presented and analyzed further in the audit because collection was not possible from either a supervisor or MSFC in the same chassis. The audit performs the correlation by matching serial numbers from the results of the **show version** command on the MSFC and the **show module** command on the supervisor. The audit cannot take the approach of a typical user and session internally from the supervisor to the MSFC because the audit collector associates each login and **enable password** command with a specific hostname or IP address; in addition, the login passwords for MSFCs and supervisors may be different.

Also care must be taken to help ensure that the MSFCs are scheduled for the audit collection since they are viewed as separate devices from the switch in hybrid mode.

There may be three management IP addresses per switch chassis with redundancy features. The switch has a single management IP address even when dual or redundant supervisors are deployed because of the use of the active-standby redundancy model. However, each supervisor can have a separate MSFC in one of two modes: an active-active MSFC redundancy model called the dual-router mode (DRM), in which each MSFC has its own management IP address, and an active-standby MSFC redundancy model called the single-router mode (SRM), in which the MSFCs share a single IP address, similar to the approach in the supervisor redundancy model. High availability was introduced in Cisco Catalyst OS Release 5.4(1). SRM MSFC redundancy was introduced in Cisco IOS Software Release 12.1(8a)E2 for MSFC2 devices and in Cisco IOS Software Release 12.1(8a)E4 for MSFCs and requires Cisco Catalyst OS Release 6.3(1) on the supervisor. Configuration synchronization (config-sync) is automatically enabled when SRM in enabled. Enhanced supervisor high availability and MSFC SRM support for multicast traffic with Supervisor 2 engines and MSFC 2 devices was introduced in Cisco Catalyst OS Release 7.1(1). Enhancements were also added in Cisco Catalyst OS Release 7.5(1) for IEEE 802.1x and port security. Manual mode MSFC redundancy, in which one MSFC is left in remon mode, was deprecated from Cisco TAC support in December 2002; SRM is recommended instead.

The initial high-availability audit table (Table 3) is the system audit table and presents the fundamental high-availability features. This table presents the results of basic availability features such as redundancy hardware features (dual supervisors and dual power supplies), system power redundancy settings, and health system checks (module status, module diagnostic, and environmental checks). This table presents findings from all Cisco Catalyst 6500 and 7600 Series systems included in the audit and should be used to investigate systems found to be deficient in fundamental high-availability areas.

Note that the results captured in this table determine whether or not additional high-availability auditing is conducted on systems and subsequent tables populated. For the highlighted exceptions, please consult Cisco NetInfo and NetAdvice for corrective actions.

Table 3. Cisco Catalyst 6500 and 7600 Series High-Availability System Audit

Catalyst 6500 and Cisco 7600 Series High Availability(HA)-System Audit											
Host Name	Cisco IOS Software Mode	Supervisor Slot (Primary/Secondary)	Supervisor Hardware (Primary/Secondary)	Supervisor Software (Primary/Secondary)	Redundant Supervisor Hardware and Software Check	Redun - dant Power Supply Check	Power Redundancy Operational Mode	Module Status Check	Module Diag - nostic Check	Fan and Cooling Status	Net Rule Excep - tion Points
DR-CHN-6509-APP-02	Native	5/6	WS-SUP720-3B/WS-SUP720-3B	12.2(33)SXH5/12.2(33)SXH5	**No**	OK	Redundant	OK	OK	OK	1

Hostname	
Description	Name of the device
Cisco IOS Software Mode	
Description	Cisco IOS Software mode
Supervisor Slot Primary/Secondary	
Description	Supervisor Slot Primary and Secondary: MSFC mode
Supervisor Hardware Primary/Secondary	
Description	Supervisor hardware primary and secondary
Supervisor Software Primary/Secondary	
Description	Supervisor software primary and secondary
Redundant Supervisor Hardware and Software Check	
Description	This field appears if dual supervisors are present, are of the same hardware type, and are running identical software.
Net Rule	If only one row is present in the supervisor slot, populate the field as No and **highlight yellow**. If two rows are present in the supervisor slot, then compare the supervisor hardware. If values are identical, continue processing the field; otherwise, populate the field as Error Hardware and **boldface red**. If two rows are present in the supervisor slot, then compare the supervisor software. If values are identical, continue processing the field; otherwise, populate the field as Error Software and **boldface red**.
Redundant Power Supply Check	
Description	This field displays the results of the presence of a dual power supply, of identical type (wattage), and operating in a normal, healthy state.
Net Rule	Highly available chassis based systems should always contain dual power supplies operating in a healthy state, of equal type, and providing equal power to the system. If only one power supply is installed, then **highlight yellow**. If the wattage of the power supplies is not equal, then **highlight yellow**. If the system does not recognize the power supplies, then **boldface red**, If either power supply is unknown or failed, then **boldface red**.
Power Redundancy Operational Mode	
Description	This field describes the configured state of the power redundancy mode of systems operating with dual power supplies.
Net Rule	Compare the output of the previous column, Redundant Power Supply Check. If the value is No or No/Error-Status, populate the field as N/A and stop processing the field. Otherwise the system must have two power supplies present in some state populated with the power redundancy mode; continue processing. If the value is Combined, **highlight yellow** and stop processing.
Module Status Check	
Description	This field provides a status check if modules in the chassis are found in any state other than OK.
Net Rule	If a module status other than OK is observed, it will be indicated as an error; populate the column with Error and **boldface red**.

Module Diagnostic Check	
Description	This field provides a status check if modules in the chassis have failed the previous diagnostic check.
Net Rule	Check (Native: show mod). Check the status of Online Diag Status. If any value other than pass is found in the system, populate the column with Error and **boldface red**; otherwise, the column is populated with OK.
Fan and Cooling Status	
Description	This test verifies the fan tray operation and cooling status through three voltage termination modules (VTT 1, VTT2, and VTT3) located on the rear of the unit. The information is obtained through the Cisco IOS Software **exec** command. The operational status of the three VTT sensors as well as the outlet temperatures they are recording are checked. The temperature checks are determined by using the default temperature thresholds. If all values test successfully, the column is populated with OK; otherwise, it is populated with Error with a minor or major warning in **yellow** or **red**, respectively.
Net Rule	No alarm condition: If the fan status has a value of Fan-fail: = OK print OK. If the fan status has a value of Fan-fail is not equal to OK, print Error and **boldface red**. No alarm: If the operating status values of VTT 1 OK:, VTT2 OK:, and VTT3 OK: are equal to OK and the VTT 1, VTT2, and VTT3 outlet temperatures are less than or equal to 100°C, print OK. Minor alarm: If the operating status values of VTT 1 OK:, VTT2 OK:, and VTT3 OK: all are not equal to OK, or if any VTT1, VTT2, or VTT3 outlet temperature measurement is greater than 100°C but less than or equal to 150°C, print Error and **highlight yellow**. Major alarm: If the operating status values of VTT 1 OK:, VTT2 OK:, and VTT3 OK: all are not equal to OK, or if any VTT1, VTT2, or VTT3 outlet temperature measurement is greater than 150°C, print Error and **boldface red**.
Net Rule Exception Points	
Description	Net rule exception points (NREPs)

C Sample Syslog Problem Analysis

Table 4 presents a syslog problem analysis example.

Table 4. Sample Syslog Problem Analysis

New Problems Encountered from 2004 09 13 00:00:00 to 2004 09 14 00:00:00				
Problem Name	LINK-3-UPDOWN_problem			
Problem Description	A physical link on a Cisco IOS Software device has changed state three or more times in a 5-minute period. This behavior most likely indicates some type of link, carrier, or cabling problem. Excessive link-state changes lead to protocol rerouting, excessive resource consumption, and potential network instability, at least for short periods of time. The impact may depend on whether the device is a core, distribution, or access device. Link-state changes are relatively normal on asynchronous connections. This message may also be associated with a corresponding line protocol message.			
Recommended Action	Investigate the link information using the **show interface** command, looking for potential errors. Enable logging and look at all potential link problems. If cabling is suspect, replace the path or test the path by eliminating suspect path components. If flaps are continuing and no root cause can be determined, contact the Cisco TAC.			
Supporting Links	http://www.cisco.com/en/US/products/sw/cscowork/ps5431/products_user_guide_chapter09186a00801c1bfc.html#wp998857			
Problem Start Time	2004 09 13 06:42:36	**Problem End Time**	2004 09 13 10:28:00	
Number of Problem Occurrences	9			
Devices and Scope of Problem				
Node	**Interface**	**Neighbor**	**Message Type**	**Time Stamp**
s-b3	POS6/0	N/A	LINK-3-UPDOWN	2004 09 13 06:42:36
s-b3	POS6/0	N/A	LINK-3-UPDOWN	2004 09 13 07:09:35
s-b3	POS6/0	N/A	LINK-3-UPDOWN	2004 09 13 07:09:56
prs-th2-i1	Serial4/1/1	N/A	LINK-3-UPDOWN	2004 09 13 09:46:08
prs-th2-i1	Serial4/1/1	N/A	LINK-3-UPDOWN	2004 09 13 09:55:27
prs-th2-i1	Serial4/1/1	N/A	LINK-3-UPDOWN	2004 09 13 09:55:41
win-tal-i1	Serial3/2	N/A	LINK-3-UPDOWN	2004 09 13 10:26:22

New Problems Encountered from 2004 09 13 00:00:00 to 2004 09 14 00:00:00				
win-tal-i1	Serial3/2	N/A	LINK-3-UPDOWN	2004 09 13 10:26:40
win-tal-i1	Serial3/2	N/A	LINK-3-UPDOWN	2004 09 13 10:28:00

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA C11-642029-00 02/11