Understanding Cisco IOS Software Embedded Self-Management Capabilities

Attaining Optimal Value from Existing Cisco Infrastructures

Using What You Paid For

As a service provider, are you optimizing your ability to fulfill service requests, validate service-level agreements (SLAs), monitor network activity, and detect and isolate faults? Do you know how to fully exploit the Cisco IOS® Software already deployed in your network to speed service delivery, attain and maintain service-level objectives, reduce downtime, and aid troubleshooting?

Cisco IOS Software pervades service provider networks worldwide. Its extensive features and intelligence enable granular visibility and control over packets traversing the thousands of Cisco® routers, switches, and gateways in a typical service provider infrastructure. Cisco IOS Software includes an extensive list of self-management features. These embedded capabilities allow Cisco devices to monitor their own system resources and status, report alerts to the network operations center (NOC), and take preconfigured actions to address element faults and failures.

Embedded self-management describes software subsystems within Cisco IOS Software that help manage, monitor, and automate actions within a router or switch running Cisco IOS Software. It complements external management systems, which play a significant role in fault management, configuration management, capacity planning, provisioning, and data collection. Embedded self-management adds a dimension to the management infrastructure by enabling devices to manage themselves according to policies. It allows devices to automatically take action and collect data, improving service providers' ability to better manage devices and the network.

Cisco increases device-level intelligence through advanced instrumentation to enhance management efficiencies for zero-touch deployments and SLA compliance, along with fault, performance, and configuration management. Its open application programming interfaces (APIs) assist integration with operations support systems (OSSs) and customized or off-the-shelf network management platforms. Devices can be configured to monitor themselves and provide management applications with focused, pro-active information, allowing these applications to perform more directed and efficient status polls for retrieving summary data.

To help service providers evaluate the embedded self-management capabilities of Cisco IOS Software, Cisco Systems® offers a detailed scenario that demonstrates how operational teams would interact with these features during service fulfillment and service assurance activities. The following scenario offers a perspective designed to encourage service providers to take the necessary steps to attain the greatest benefits from their Cisco infrastructures.

Service Fulfillment

After careful review of technical and budgetary requirements, UpscaleTheme is ready to deploy a VPN service from its headquarters in Paris to its 200 retail stores throughout Europe. It needs this VPN to carry data, voice, and video traffic to support its mission-critical applications that operate cash registers, manage inventory, assist customer service, and support enterprise resource planning (ERP) applications. The VPN will also support corporate IP telephony services and a new

IP broadcast and interactive video service for training of store employees and marketing to customers.

Working closely with MediaProvider.com, its service provider, UpscaleTheme has already estimated its WAN bandwidth requirements to each location and provisioned its links accordingly. Now it needs to deploy and configure the customer premises equipment (CPE) to its stores, its primary data center in Paris, and its secondary/backup data center in Amsterdam.

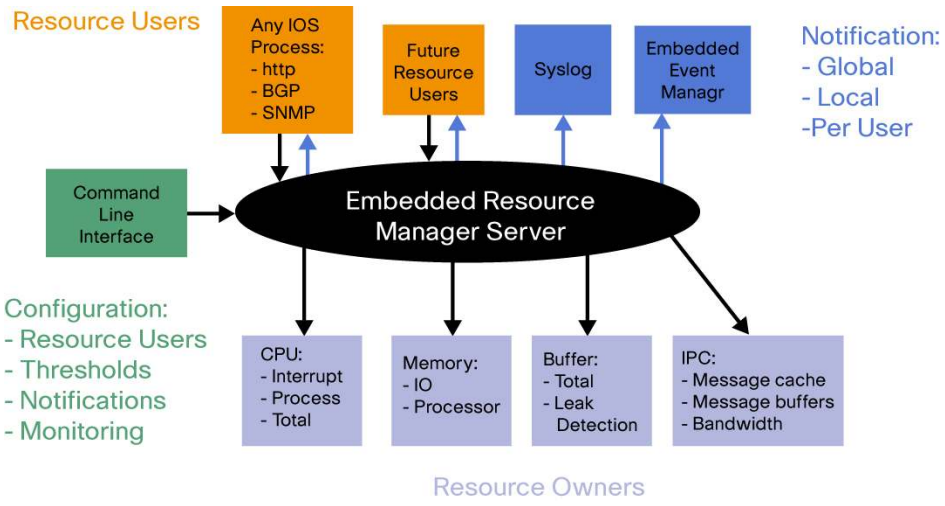
Because it is a retailer and not a network operator, UpscaleTheme has decided to buy a managed service from MediaProvider. Its requirements include:

- Installation completed within three weeks.
- Quality guarantees (maximum round-trip time and jitter) to assure consistent voice and video services.
- Availability guarantees of 99 percent at stores and 99.99 percent at headquarters and data centers.
- Security guarantees to comply with its internal security policy. For example: all phone conversations and data will be encrypted; device configuration files will not travel the Internet in cleartext over telnet or e-mail, but will be encrypted through a VPN tunnel.
- Joint service validation period and change management process to make sure the service operates as expected.

Having signed the contract, MediaProvider initiates service fulfillment in parallel along two project management tracks. Stores receive CPE using a standardized process, while the larger data center, backup data center, and headquarters CPE will be deployed using a combination of standard and customized processes.

Before deployment, MediaProvider needs to verify that its network infrastructure has the capacity to handle 202 new sites and meet the customer's strict SLAs. Are enough ports and line cards available? Do network elements have enough processing power and memory? Is there enough bandwidth? Cisco IOS Software Embedded Resource Manager (ERM) in its Cisco aggregation devices at relevant points of presence (POPs) captures resource allocation information to help MediaProvider network planners address these questions. Cisco IOS Software ERM monitors system resource usage to better understand scalability needs (Figure 1).

Figure 1. Cisco IOS Software Embedded Resource Manager Architecture



The ERM infrastructure tracks resource depletion and resource dependencies across processes and within a network element to handle various error conditions. The error conditions are handled by providing an equitable sharing of information between various applications. The ERM framework provides a communication mechanism for resource entities and allows communication between these resource entities. The ERM framework also helps in debugging the CPU and memory-related issues. ERM monitors system resource usage to better understand scalability needs by allowing configuration of threshold values for resources such as CPU, buffer, and memory. The infrastructure provided by ERM can be extended to any resource that needs to be monitored. The ERM infrastructure also supports multiprocessor platforms through a distributed ERM (dERM) architecture that shares the same commands and functionality as nondistributed ERM. The ERM framework provides a mechanism to send notifications whenever a resource user breaches specified threshold values. This notification makes operators aware of issues regarding CPU, buffer, and memory utilization.

Starting with ERM data, network planners can make adjustments to the infrastructure to prevent any negative effect of new services on existing ones for other customers. When they give the go-ahead date to the project manager, MediaProvider can begin shipping CPE to each UpscaleTheme site.

The initial ERM data indicates that MediaProvider needs to expand its core Multiprotocol Label Switching (MPLS) network to accommodate more ports and higher throughput. It can use Cisco IOS Software MPLS Embedded Management features to facilitate and validate its expansion. Cisco IOS Software MPLS Embedded Management is a set of standards and value-added services that facilitate the deployment, operation, administration, and management (OAM) of MPLS networks in line with the fault, configuration, accounting, performance, and security (FCAPS) model.

In stores, Network-Based Application Recognition (NBAR) enables precise traffic classification and guaranteed minimum available bandwidth within the MediaProvider network for individual applications such as UpscaleTheme's voice-over-IP (VoIP) phone calls, its broadcast video streams, and its time-sensitive ERP application transactions. NBAR is a Cisco IOS Software Quality of Service (QoS) mechanism that can recognize a wide variety of applications, including Web-based applications and client/server applications that dynamically assign TCP or User Datagram Protocol (UDP) port numbers and heuristic application recognition. After application recognition, the network can invoke specific services for that particular application. NBAR works with other Cisco IOS Software QoS features to help ensure optimal bandwidth utilization to meet

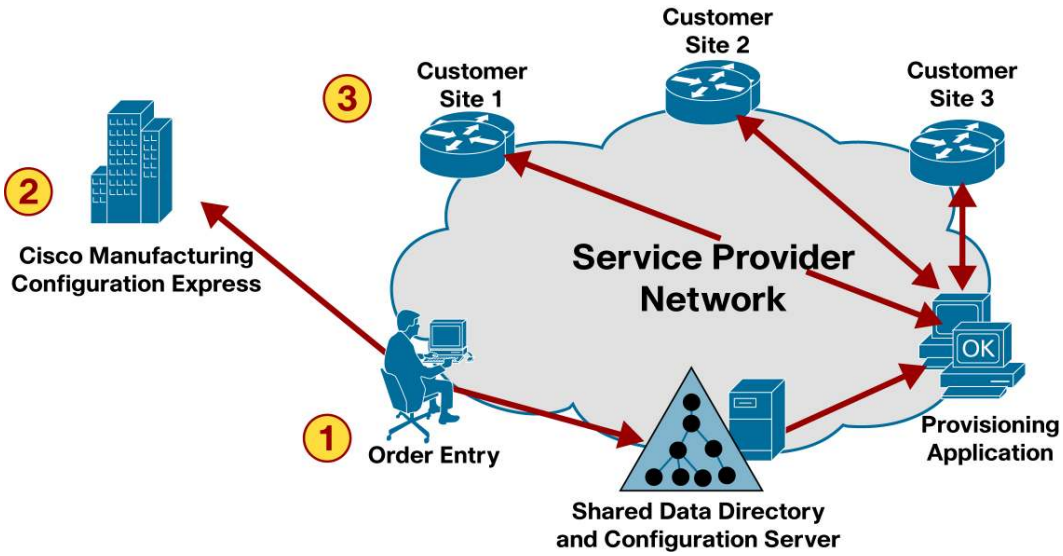
SLA guidelines. NBAR adds classification to the network to deliver more granular identification and control over multiple Internet-based and client/server applications, which other QoS mechanisms cannot differentiate.

MPLS OAM is pivotal for enabling MediaProvider to assure SLA guarantees, service assurance, QoS assurance, and overall service management. Network operators need the ability to reliably conduct SLA testing, detect MPLS control- and user-plane defects, and check MPLS forwarding path integrity in a real-time environment. After configuring new label switched paths (LSPs) for every UpscaleTheme source and destination node, the LSP tree trace feature allows MediaProvider to discover all equal-cost multiple pathways (ECMPs) through its MPLS core, to assist with load balancing, traffic engineering, and possible path reroutes. It discovers and lists multiple “branches” for each LSP or each subnet that UpscaleTheme traffic will use. The MPLS OAM toolkit combines the following capabilities: Cisco MPLS ping and traceroute, Cisco Virtual Circuit Connectivity Verification (VCCV), Cisco MPLS Traffic Engineering AutoTunnel and AutoMesh, and Cisco IP SLA. Operators can use the command-line interface (CLI) to access and manage these Cisco IOS Software capabilities, or they can use Cisco MPLS Diagnostics Expert (MDE) for automated MPLS troubleshooting and diagnosis to reduce mean time to repair (MTTR) and help operators perform their duties more effectively. In addition to MPLS OAM capabilities, MDE can diagnose more complex failure scenarios.

Stores: Deployment, Configuration, And Service Validation

MediaProvider assigns a project manager to work with a logistics partner to ship a Cisco Integrated Services Router (ISR) as CPE to each store. This partner uses the “zero-touch” Cisco Configuration Express service model, which uses Cisco IOS Software ConfigAgent and ImageAgent in each CPE router and in Cisco Configuration Engine appliances at the MediaProvider NOC (Figure 2). This scenario does not consider the alternatives required for stores located in countries where customs law prevents the use of Cisco Configuration Express.

Figure 2. Cisco Configuration Express Process Flow



1. Service rep enters customer service information.
   Network engineer enters technical information and orders routers.

2. Cisco drop ships devices to site with basic connectivity pre-configured or pre-configuration is done by provider or customer technician
3. Device boots and pulls down complete configuration.
   Device generates ‘configuration success’ event—service is on!

The Cisco IOS Software ConfigAgent and ImageAgents in conjunction with Cisco Configuration Engine provide:

- Zero-touch initial device deployment and activation using a self-registration process
- Secure high-volume, high-speed asynchronous firmware image and configuration distribution
- Open API Web services and Software Development Kit (SDK)
- Scalable device configuration and image distribution management up to 10,000 devices per engine, with clustering capabilities to support more devices
- Programmable configuration and inventory templates

The MediaProvider project manager assigns unique identifiers to the UpscaleTheme sites and associates every identifier with specific device configurations that are downloaded automatically to each CPE after installation. The unique identifiers also allow the MediaProvider OSS to identify UpscaleTheme devices and bill for services to each one after the Cisco Configuration Engine confirms successful service activation.

To simplify compliance with UpscaleTheme 's strict security policies, the logistics partner does not need access to any router configurations or credentials. It orders CPE from Cisco and arranges for router installation at every site. MediaProvider provides a generic "bootstrap" configuration to Cisco, allowing the Cisco ConfigExpress Service to pre-provision every device and then drop-ship it. The bootstrap configuration tells each Cisco CPE how to contact the Cisco Configuration Engine at MediaProvider for self-registration upon startup. The Cisco IOS Software ConfigAgent communicates with the Configuration Engine server at MediaProvider and downloads its router configuration file based on its unique identifier assigned using Cisco Configuration Express. The device completes a boot cycle and comes online using the new configuration. Based on event notifications from the Cisco Configuration Engine, MediaProvider can instantly track the status of its installation project and can notify UpscaleTheme as sites come online.

Acknowledging the security policy, the zero-touch deployment process uses device authentication and encryption to protect configuration files traversing the Internet. If a download session is interrupted, ConfigAgent continues to contact the Configuration Engine until its configuration is complete and verified. MediaProvider can use this same system to update Cisco IOS Software using the embedded Cisco IOS Software ImageAgent in each device. It can configure the CPE to call in and check for configuration and software image updates on a regular basis, perhaps once a week.

As each site comes online, MediaProvider begins the service assurance process. Manual monitoring methods are impractical given the number of retail stores. To automate this process, MediaProvider uses embedded Cisco IOS Software management features to monitor operations in each CPE router and use the Cisco IOS Software IP Service-Level Agreement (IP SLA) feature to verify SLA compliance. The Cisco IOS Software IP SLA feature augments traditional service-level monitoring with IP application awareness that measures compliance within the IP layer. It allows managers to verify service guarantees, increase network reliability by validating network performance, proactively identify network issues, and ease deployment of new IP services. It exclusively uses active monitoring to generate synthetic traffic in a continuous, reliable, and predictable manner, enabling measurement of network performance and health. It measures round-trip delay, jitter, and packet loss, allowing MediaProvider to verify that the network can support time-sensitive ERP data transactions and high-quality voice and video.

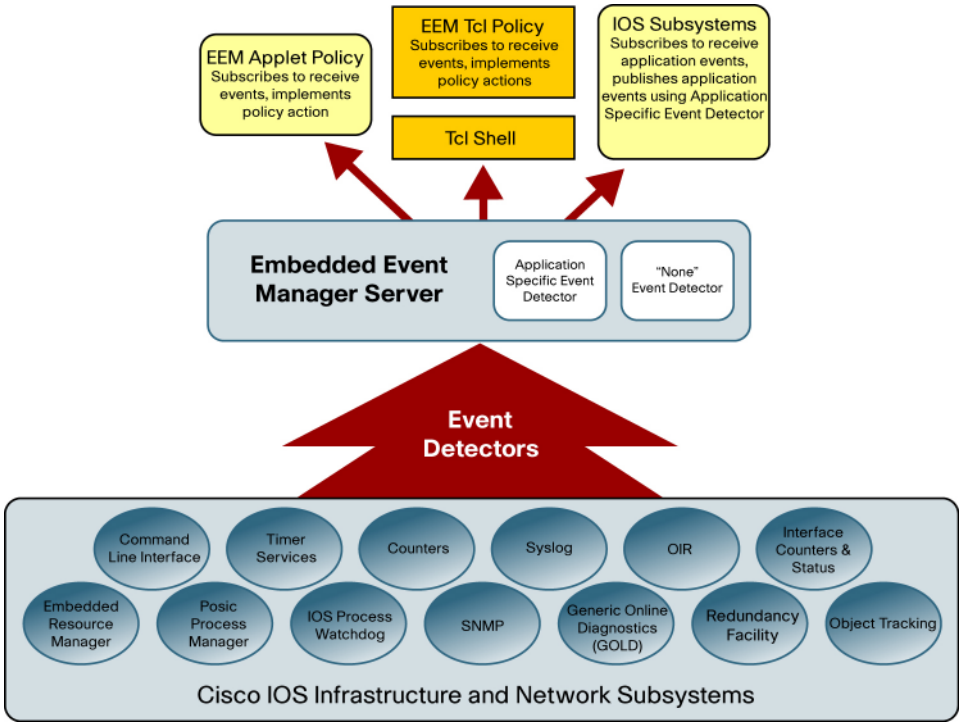
The initial configuration files downloaded to every CPE device include defined measurements to verify critical SLA metrics and policies. Threshold layers capture problems that are fixed before the customer sees them to conform to internal operation-level agreements (OLAs). In this case, the threshold is set at 3 ms delay. Delays exceeding 5 ms exceed the SLA with UpscaleTheme and are proactively reported to its IT staff.

In addition to Cisco IOS Software IP SLA, the embedded management features used for initial service validation (and later for ongoing service assurance monitoring) include Cisco IOS Software ERM (measuring the same statistics used to verify resources before deployment), Cisco IOS Software Embedded Event Manager (EEM), Cisco IOS Software Event MIB (RFC 2981), Cisco IOS Software Expression MIB (RFC 2982), and Cisco IOS Software Flexible NetFlow.

- Cisco IOS Software EEM—Makes a Cisco IOS Software router or switch an active participant in the management process, allowing service providers to define policies and customize actions in response to network events as they happen. It is a set of tools that automate many network management tasks and direct the operation of Cisco IOS Software to increase availability, collect information, and notify external management systems or personnel about critical events.

  EEM has three main components (Figure 3): event detectors, the event manager server, and the policy director, which all reside in software on the device. Event detectors notify the event manager server of events detected by the detectors, for example the Event and Expression MIBs. The policy director registers with the event manager server to receive events and implement policy actions.

Figure 3. Cisco IOS Software Embedded Event Manager 2.1 Architecture



- Cisco IOS Software Event MIB—Provides a superset of capabilities of the remote monitoring (RMON) MIB alarm and event functions. It monitors programmed events and allows alarm generation for MIB objects that are on the same or a remote network element. It sends Simple Network Management Protocol (SNMP) notifications in response to defined triggers to the network console or to Cisco EEM.
- Cisco IOS Software Expression MIB—Allows creation of new SNMP objects based on existing MIB variables and formulas, complementing the functionality of the Event MIB.
- Cisco IOS Software NetFlow and Flexible NetFlow—Perform passive monitoring of real traffic. Although NetFlow is primarily intended to help operators optimize network performance, reduce operation costs, and improve capacity planning and security incident detection, its data may be useful for import into management applications at the OSS layer. Flexible NetFlow is an enhancement to the standardized IP flow technology invented by Cisco. It allows service providers to create custom templates that extract only the

information that stakeholders are interested in. Customized traffic flow reports can include (but are not limited to): source, destination, timing, application information, and number of packets.

Data Center And Headquarters Deployment, Configuration, And Service Validation

In parallel with CPE deployment at the retail stores, MediaProvider works closely with UpscaleTheme IT staff to deploy CPE in primary and backup data centers and the headquarters campus. It uses the logistics partner to ship a Cisco Catalyst® 6500 switch to each data center site and install it. It then assigns an engineer to customize the switch configuration and perform service validation. The engineer can use the Cisco IOS Software Enhanced Device Interface (E-DI) capability for efficient, reliable implementation of custom configurations of the group of Catalyst 6500 CPE over a remote connection.

Cisco IOS Software E-DI provides:

- Command-line interface with embedded Perl scripting capabilities and built-in least-common-denominator syntax verification against CPE groups. Onscreen visual feedback changes the text to red when an invalid command is issued to a device or group of devices
- Graphical configuration editor
- Programmatic XML and IETF Netconf (draft-ietf-netconf-prot-07.txt) interface—E-DI supports both Secure Shell (SSH) Protocol and telnet transport, acting as the Netconf agent on behalf of managed devices.

Using E-DI, the MediaProvider engineer quickly groups CPE nodes with identical customization requirements (such as all Cisco Catalyst 6500 switches) together and issues the custom-designed configuration on top of the basic configuration installed by the logistics partner. She can work interactively with the group of devices, has visual confirmation about the validity of commands, and can then schedule all customizations to be downloaded in a single bulk operation.

Next, the MediaProvider engineer validates service operations according to initially defined test cases. She also makes use of Cisco IOS Software ERM and verifies that the network accommodates test cases to predefined SLA scenarios.

During the service validation phase, UpscaleTheme reports unverified complaints about intermittent network performance issues by some pilot users in branch offices and similar issues reported by pilot users in a headquarters site. MediaProvider issues and approves a change request to analyze the problems.

MediaProvider gathers NetFlow information from its POP locations to develop an initial understanding of traffic flows within the UpscaleTheme network. Although most behavior conforms to original design assumptions, there are unpredicted traffic flows between some branch offices and what turns out to be a standalone server located under a desk in a headquarters building. To complement Layer 3 and 4 information from NetFlow with protocol and application information, MediaProvider uses the Modular quality of service command-line interface (QoS CLI) to configure NBAR to obtain more detailed traffic data from one of the Cisco Catalyst 6500 CPE devices involved. The Modular QoS CLI allows users to specify a traffic class independently of QoS policies.

Here, NBAR data discovered a legacy application on the standalone server. The UpscaleTheme staff forgot to list this server's specifications to MediaProvider. The server will remain online until users migrate to a replacement application housed in the primary data center. MediaProvider and UpscaleTheme agree on an extended observation period until the transition is complete and the

old server is taken offline. MediaProvider will report future instances when excessive bandwidth usage by the legacy application causes problems with the branch offices.

To implement this requirement, MediaProvider configures NBAR and Expression MIB on the affected branch office CPE devices. It uses the thresholding capability of the NBAR MIB to detect high-activity periods in the legacy protocol. It also uses Expression MIB to detect periods of high activity in the legacy protocol that coincide with periods of excessive delays or very high bandwidth usage. The MIB Object resulting from these expressions is then used to escalate a customized SNMP trap (using Event MIB) to notify NOC personnel of high-risk situations that the legacy application causes.

Service Assurance

When all data centers and sites are online, and MediaProvider has completed its initial verification tests, it activates and hands off the service to UpscaleTheme for production traffic. Using the same Cisco IOS Software self-management features applied during service validation, MediaProvider now enters the service assurance monitoring phase of the MPLS core, customer endpoints, and its internal POP aggregation sites to verify consistent compliance with customer SLA terms.

Within the MPLS core at MediaProvider, the network monitoring team uses the LSP Health Monitor of IP SLA to periodically check all LSPs and verify their operation. The LSP Health Monitor feature enables the following:

- End-to-end LSP connectivity measurements for determining network availability or testing network connectivity in MPLS networks
- Proactive threshold violation monitoring through SNMP trap notifications and Syslog messages
- Reduced network troubleshooting time for MPLS networks
- Scalable network error detection using fast retry capability
- Creation and deletion of IP SLA LSP ping and LSP traceroute operations based on network topology
- Discovery of Border Gateway Protocol (BGP) next-hop neighbors based on local VPN routing or forwarding instances (VRFs) and global routing tables
- Multioperation scheduling of IP SLA operations

Cisco IOS Software Embedded Syslog Manager (ESM) feature extends traditional system message logging (Syslog), which allows a router or switch to report and save important error and notification messages, either locally or to a remote logging server. Cisco IOS Software ESM allows flexible logging of Syslog messages in standard format or ESM filtered format. It can send outputs to any of the traditional Syslog targets or send each output type to a different host. This flexibility allows MediaProvider to support a range of external monitoring applications with supported message formats. It allows the monitoring staff to preformat and copy a small subset of relevant Syslog messages (such as failed login attempts) to the internal security operations center (SOC) while the central NOC remains the primary target for event information.

The NOC and SOC teams at UpscaleTheme, along with its application assurance team, would also benefit from information gathered from branch and data center CPE devices. MediaProvider forwards relevant events based on Cisco IOS Software ESM and EEM. Data center CPEs use EEM to flexibly respond to monitoring requirements raised by the UpscaleTheme application assurance team. Using Cisco IOS Software EEM, MediaProvider copies relevant events to

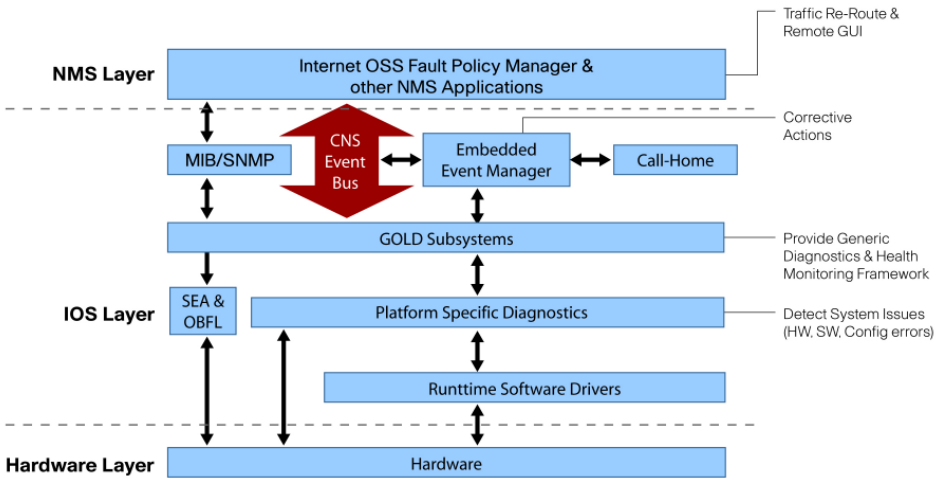
management applications in use at the UpscaleTheme NOC. These events are detected through SNMP, CLI configuration changes, and hardware online insertion and removal (OIR) events.

Service Troubleshooting

Throughout the life of the VPN service, both MediaProvider and UpscaleTheme rely on Cisco IOS Software embedded management features to assist them in troubleshooting. Features such as Syslog and NetFlow generate data that can be imported into advanced management applications that automate root-cause analysis. In addition to the capabilities already discussed, Cisco embeds powerful diagnostic capabilities within the Cisco Catalyst 6500 software to help ensure high availability and rapid troubleshooting and problem resolution.

Cisco Generic Online Diagnostics (GOLD) defines a common framework for diagnostic operations, measuring performance and operation of Catalyst 6500 switch hardware and communicating with upstream Network Management System (NMS) applications through MIBs and SNMP traps (Figure 4).

Figure 4. Cisco IOS Software Generic Online Diagnostic (GOLD) Framework



The GOLD framework specifies a proactive fault-detection architecture for centralized and distributed systems. It includes the common diagnostics CLI and fault-detection procedures for both boot-up and runtime diagnostics. Boot-up diagnostics help ensure that a failing module is not introduced into a live network. Runtime diagnostics can be either disruptive or nondisruptive. They can be run on demand, on schedule, or continually in the background. Nondisruptive health monitoring tests can run in the background and are useful for triggering switchovers (to a backup supervisor engine, for example) to maintain high availability. The GOLD runtime diagnostics can monitor system health, and programmed policies tell the system what actions to take upon detecting a fault. It can detect the following problems during boot-up or in a live environment: faults in hardware components, connectors, interfaces, or memory; inconsistencies that cause errors in the data and control paths; and software misbehaviors or failures.

MediaProvider relies on GOLD during deployment to verify that all switch modules operate correctly before they go online to help ensure proper operation, services, and high availability to UpscaleTheme. During normal maintenance, GOLD provides boot-up diagnostics to assure proper function of new or replaced modules. Unfortunately, a Cisco Catalyst 6500 module was improperly handled during installation at the UpscaleTheme data center, and now it intermittently fails. The GOLD background diagnostics detect this behavior and initiate a failover to a backup module,

simultaneously alerting the NOC by reporting events and actions to Cisco IOS Software EEM or generating a Syslog message. The entire sequence prevents an immediate service outage, and MediaProvider dispatches a logistics partner to replace the module.

The Value Of Embedded Device Management

The embedded self-management capabilities of Cisco IOS Software can greatly enhance service fulfillment, validation, assurance, and troubleshooting activities. Service providers can configure their Cisco IOS Software routers and switches to automatically take automated actions upon detecting defined events. Using both properly configured embedded management and powerful management applications, service providers attain greater visibility and control over their Cisco networks. In service provider networks scaling from a few dozen to hundreds of thousands of internal and CPE devices, Cisco IOS Software embedded self-management provides the device-level instrumentation and data for management applications to deliver more flexible services with shorter lead times. These capabilities help service providers save vast amounts of staff time during deployment, operation, and troubleshooting, leading to greater efficiencies, improved service quality, and operational cost controls. More importantly, service providers are better positioned to upsell customers to higher-grade services, increasing revenue and protecting profit margins.

Appendix A

Cisco IOS Software Embedded Management Capabilities				
Fault	**Configuration**	**Accounting**	**Performance**	**Security**
• Generic Online Diagnostics (GOLD) • Embedded Syslog Manager • Embedded Event Manager (EEM) • Event and Expression MIB • MPLS OAM tools	• Embedded Resource Manager (ERM) • Configuration Express with Configuration Engine • Enhanced Device Interface (E-DI) • ConfigAgent • ImageAgent	• NetFlow and Flexible NetFlow • NBAR	• Flexible NetFlow • IP SLA • NBAR • Event and Expression MIB	• Embedded Syslog Manager

For More Information

For more information about the embedded device management capabilities visit: http://www.cisco.com/go/instrumentation.

Cisco IOS Software ConfigAgent
Cisco IOS Software ImageAgent
Cisco IOS Software Embedded Event Manager (EEM)
Cisco IOS Software Embedded Resource Manager (ERM)
Cisco IOS Software Embedded Syslog Manager (ESM)
Cisco IOS Software Enhanced Device Interface (E-DI)
Cisco IOS Software Event MIB (RFC 2981)
Cisco IOS Software Expression MIB (RFC 2982)
Cisco IOS Software NetFlow and Flexible NetFlow
Cisco Generic Online Diagnostics (GOLD)
Cisco IOS Software IP Service-Level Agreement (IP SLA)
Cisco MPLS Operations, Administration, and Management (OAM)
Cisco MPLS Diagnostics Expert (MDE)
Cisco IOS Software Network-Based Application Recognition (NBAR)

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.**

Printed in USA

C11-378757-01 1/07