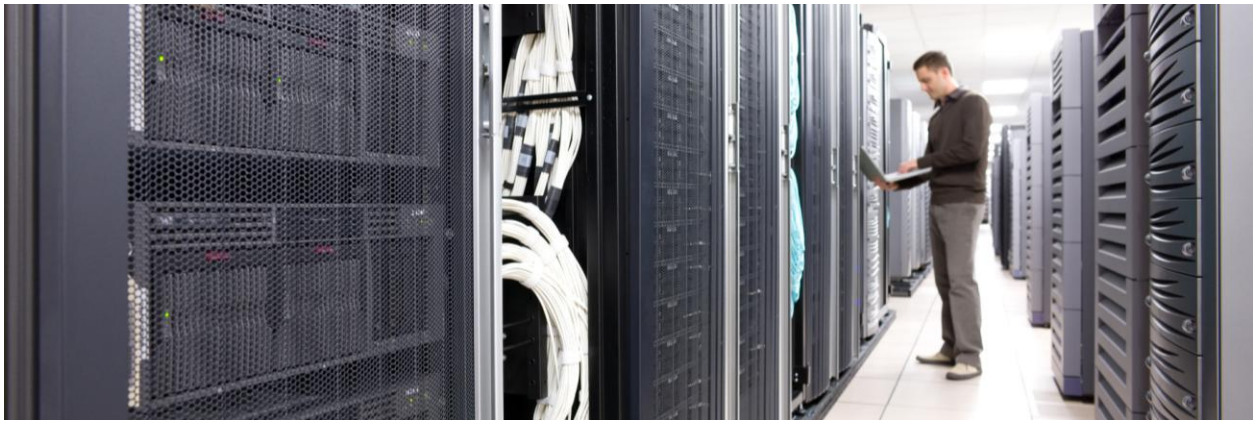
Accelerating Network Health with Smart Call Home



Introduction

Typically, network operators use various network management tools to monitor and manage their network to reduce downtime through proactive notification of issues. With extensive fine-tuning and customization by highly skilled staff, these tools also provide the capability to implement pre-emptive services at the device level.

This white paper discusses the challenges and values of providing pre-emptive Network Health services, and examines the approach of using Cisco Smart Call Home™ to accelerate network health while also helping operators understand how Smart Call Home complements their current network management systems.

If you have ever tried to manage a network, you are probably familiar with the challenges of managing different devices, device types and knowing what problems to look for. Certain issues, such as reaching a device, port up/down status, CPU and memory utilization are universal.

While these may be common attributes to monitor across device types, different device types can present unique challenges when trying to do this.

Before we go into the details of how this problem can be simplified, let's take a look at how a network is managed. Typically, network operators manage their infrastructure using a network management system, which uses various protocols to check the status/health of the devices depending on the instrumentation available in the devices and the capabilities available with the network management systems. The management of the network is both proactive and reactive, and the protocols used for managing and detecting issues could be:

- SNMP
- ICMP Ping/Traceroute
- Syslog
- XML/Soap
- Netflow
- Traps
- Telnet
- SSH
- IPSLA

The challenge that most network administrators face is to know what to monitor for each and every device since the characteristics and usage tends to be different. This is a time consuming exercise, but it helps one determine which problems to address and resolve, and which ones to ignore. It can be done by fine-tuning your network management systems, but it takes time, which can be months or even years.

The situation above is analogous to the case of a doctor. Doctors undergo years of medical practice to determine which symptoms are serious for the body and are indicating a critical health problem that needs to be addressed versus issues, which are probably temporary and will go away with time. Knowing the difference between the two is quite important, and can be the difference between a good diagnosis and catastrophe. The situation in the case of devices is certainly similar, and failure to remediate critical situations can impact your network operations, resulting in impact to the business.

As a result, a fine tuned management system is one where the system has been tuned over a period of time to setup the right thresholds for devices, know the right MIB objects to monitor, have the ability to process syslogs and traps, and take appropriate automated actions on those alarms. This work can extend to months and years of analysis.

SNMP, Syslogs, Traps, IPSLA, and EEM are immensely valuable instrumentation capabilities that help you effectively monitor and manage your network. However, to be able to effectively leverage them, a user needs to know which MIB OIDs to monitor, which asynchronous events to look for, and what remediation actions, if any, need to be taken. This optimization and generation of intellectual property within a network requires considerable time and effort.

So how does an operator manage their network, and what are the different types of management systems? We will use the FCAPS model to illustrate the different aspects of management, and later in the paper, explain how Device Diagnostics fits in the model. FCAPS stands for:

Fault Management
Fault management detects, logs, notifies and, in some cases, remediates problems on the network to improve availability without degradation of the services being offered by the network.

Configuration Management
Configuration management provides the ability to gather and store configuration from network devices, track changes being made on the network and provision any updates/changes on network devices

Accounting Management
Accounting management gathers data related to network utilization and usage statistics by various groups. This information is used for billing purposes.

Performance Management
Performance management monitors the performance of the network, which can be used for planning purposes and optimization. Information collected can include network throughput, utilization, response times and the like.

Security Management
Security management is the capability to control access to devices in the network and enforcing authorization and authentication mechanisms for enabling proper privileges for those accessing the network.

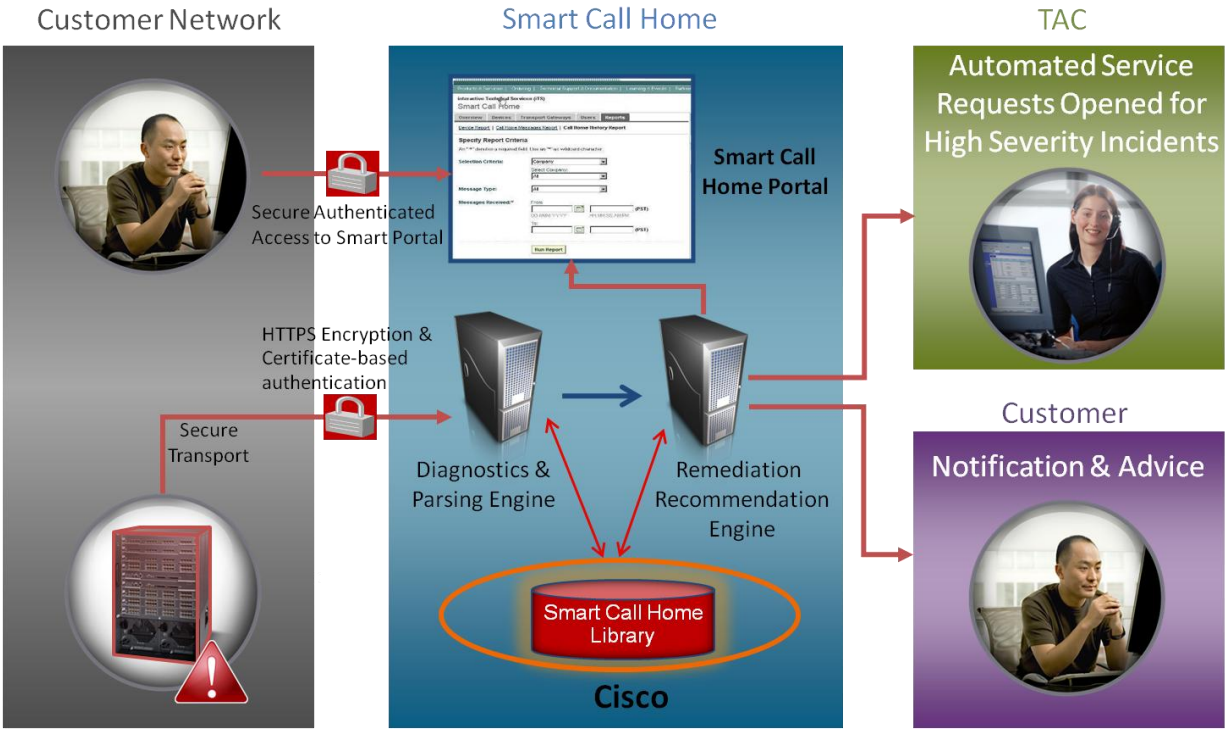
Typically, the most commonly deployed management systems are the element management systems. There is now a solution that can complement your element/network management systems and simplify your life. That solution is Cisco Smart Call Home.

What is Smart Call Home?

Smart Call Home, as shown in Figure 1, is an embedded solution that enables devices and the Smart Call Home backend to:

- Perform proactive diagnostics on their own components
- Provide real-time alerts
- Automate service requests
- Provide web-based reporting and
- Offer remediation advice

Figure 1. Cisco Smart Call Home



Let's take a look at Cisco Smart Call Home, its components, and how it leverages Cisco's Intellectual Property to simplify and notify customers of alerts that matter, along with remediations that should be implemented and automation of service requests with relevant debugging information. Smart Call Home also uses Cisco Intellectual Property to compose emails to the customer when critical issues arise, as well as provide appropriate information to the Cisco TAC for troubleshooting the problem (or RMA in the case of some hardware issues).

Smart Call Home leverages the capabilities of Generic Online Diagnostics (GOLD), Embedded Event Manager (EEM) and beyond. We will also look at the capabilities that Smart Call Home leverages and the value it delivers to a network operator who is concerned about adding proactive diagnostic capabilities to the network.

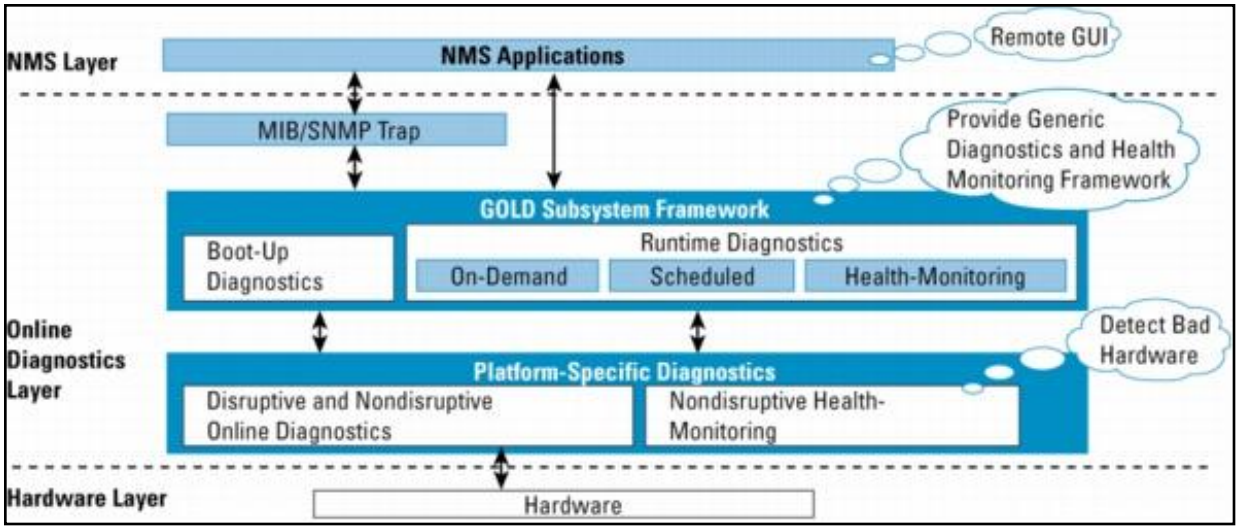
Generic Online Diagnostics (GOLD)

GOLD is a "platform independent," distributed framework that provides common CLI and scheduling for runtime diagnostics. GOLD includes the common diagnostics CLI and platform-independent fault-detection procedures for

boot-up and runtime diagnostics. The platform-specific diagnostics provide hardware-specific fault-detection tests and take appropriate corrective action in response to diagnostics test results. GOLD provides the following diagnostics:

- Boot up diagnostics during boot up and Online Insertion & Removal (OIR)
- Health monitoring diagnostics while the system is in operation
- On-demand diagnostics
- Schedule diagnostics

Figure 2. GOLD Framework



GOLD can also be used proactively to provide high availability triggers in the event of a hardware failure. GOLD can be used as part of the troubleshooting process to pinpoint a specific functional area of the hardware that is at risk of failing.

These diagnostic tests can be enabled via CLI and provide users the ability to be notified of hardware issues and, in some cases, software issues. GOLD can generate syslog messages to which management systems can subscribe. The information collected by GOLD tests can also be viewed via a CLI. Overall, GOLD capabilities enable the detection of whether the fault is hardware or software related, resulting in a lower mean time to resolution (MTTR).

To leverage GOLD, a network administrator needs to know the types of commands to configure on devices, and select the types of commands, along with options, that would provide them the information they seek.

Since GOLD is an embedded capability, it is able to accurately and quickly detect hardware and certain hardware problems which are not necessarily determined by other protocols, such as SNMP.

Embedded Event Manager (EEM)

Cisco IOS Embedded Event Manager (EEM) is a powerful and flexible subsystem that provides real-time network event detection and onboard automation. It provides the ability to adapt the behavior of the network devices to align with business needs. Cisco EEM is available on a wide range of Cisco platforms.

EEM is a flexible, policy-driven framework that supports in-box monitoring of different components of the system with the help of software agents known as event detectors. Figure 3 shows the relationship between the EEM server, core event publishers (event detectors), and the event subscribers (policies). Basically, event publishers screen events and publish them when there is a match on an event specification that is provided by the event subscriber. Event detectors notify the EEM server when an event of interest occurs. The EEM policies that are configured using the

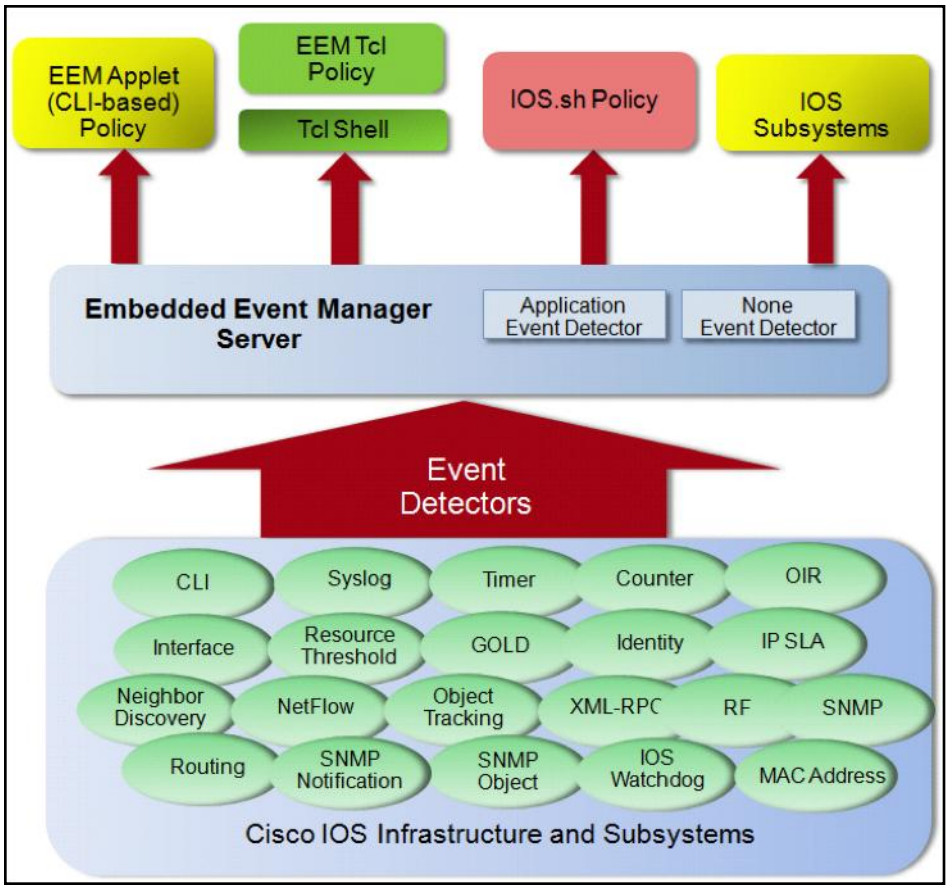
Cisco IOS command-line interface (CLI) then implement recovery on the basis of the current state of the system and the actions specified in the policy for the given event.

IOS Embedded Event Manager supports more than 20 event detectors that trigger actions or scripts in response to network events or device events. Business logic can be injected into network operations using IOS Embedded Event Manager policies. These policies are programmed using either simple command-line interface (CLI), using the Tool Command Language (Tcl) scripting language, or the bash-like IOS.sh scripting language.

Event tracking and management has traditionally been performed by external network entities. Embedded Event Manager (EEM) has been designed to offer event management capability directly in Cisco IOS devices. The on-device, proactive event management capabilities of EEM are useful, since not all event management can be done externally because some problems compromise communication between the device and the external network manager. Capturing the state of the device during such situations can be invaluable in taking immediate recovery actions and gathering information to perform root-cause analysis. Network availability can be improved if automatic recovery actions are performed without the need to fully reboot the device.

EEM offers the ability to monitor events and take informational or corrective action when the monitored events occur or when a threshold is reached. An EEM policy is an entity that defines an event and the actions to be taken when that event occurs. There are two types of EEM policies: an applet or a script. An applet is a simple form of policy that is defined within the CLI configuration. A script is a form of policy written in Tool Command Language (Tcl) or IOS.sh.

Figure 3. Embedded Event Manager Core Event Detectors



A network administrator can leverage the policy detectors and EEM applets and scripts to allow SNMP objects to be monitored and appropriate actions taken. Syslog messages and SNMP traps can be generated based on policies. Similarly, Cisco IOS CLI commands can be executed based on policies to send an email.

Based on the appropriate policy for an event that is detected, appropriate actions can be taken and include options such as:

- Executing CLI commands
- Generating a prioritized syslog message
- Generating SNMP traps

Again, to be able to leverage the power of the embedded capabilities of EEM, a network administrator needs to determine which kind of event detectors to enable, what policies to define, and then take appropriate actions based on the events.

Smart Call Home – Simplifying Network Health

Smart Call Home service provides proactive service by capturing and processing Call Home diagnostics and inventory alarms. The Call Home feature on the Cisco devices provides the capability for a customer to configure profiles that define:

- Events of interest
- Destination addresses
- Transport methods
- Message formats

To leverage the extensive capabilities of embedded technologies such EEM and GOLD, a user needs to know what to look for and configure it across the devices with the relevant profiles. However, Smart Call Home simplifies this task considerably for the user. It can be enabled on devices with a few commands, effectively enabling the relevant subset of GOLD and EEM capabilities that are relevant for that particular device.

Users can create multiple profiles, and within a profile the customer can select events of interest by subscribing to specific alert groups, which define specific actions to take when certain events occur. Within each alert group, users can customize the type of events that would trigger an alarm of a given severity. Using the Smart Call Home capability of the device, an individual can be notified of issues via email, paging, or have the syslog messages delivered to a management system.

Additionally, all Smart Call Home messages can be sent to the Smart Call Home portal via HTTPS or email. In case of critical issues, the relevant show commands and additional relevant info is sent to Smart Call Home backend. The message sent to the backend includes all the relevant information Cisco TAC needs to generate a service request. Smart Call Home provides a mechanism for Cisco hardware to send the following information to the backend:

- Periodic system messages such as inventory and configuration updates
- Real time system event messages such as Syslog and GOLD

Leveraging this information, a customer can easily monitor their network, with critical issues being reported in a proactive manner. A customer also gets visibility into their network issues via various mechanisms, such as device diagnostic portal, email or syslog messages sent to a management system. This information can be used to view trends within the network, which enables proactive embedded device monitoring.

Fault Management and Troubleshooting

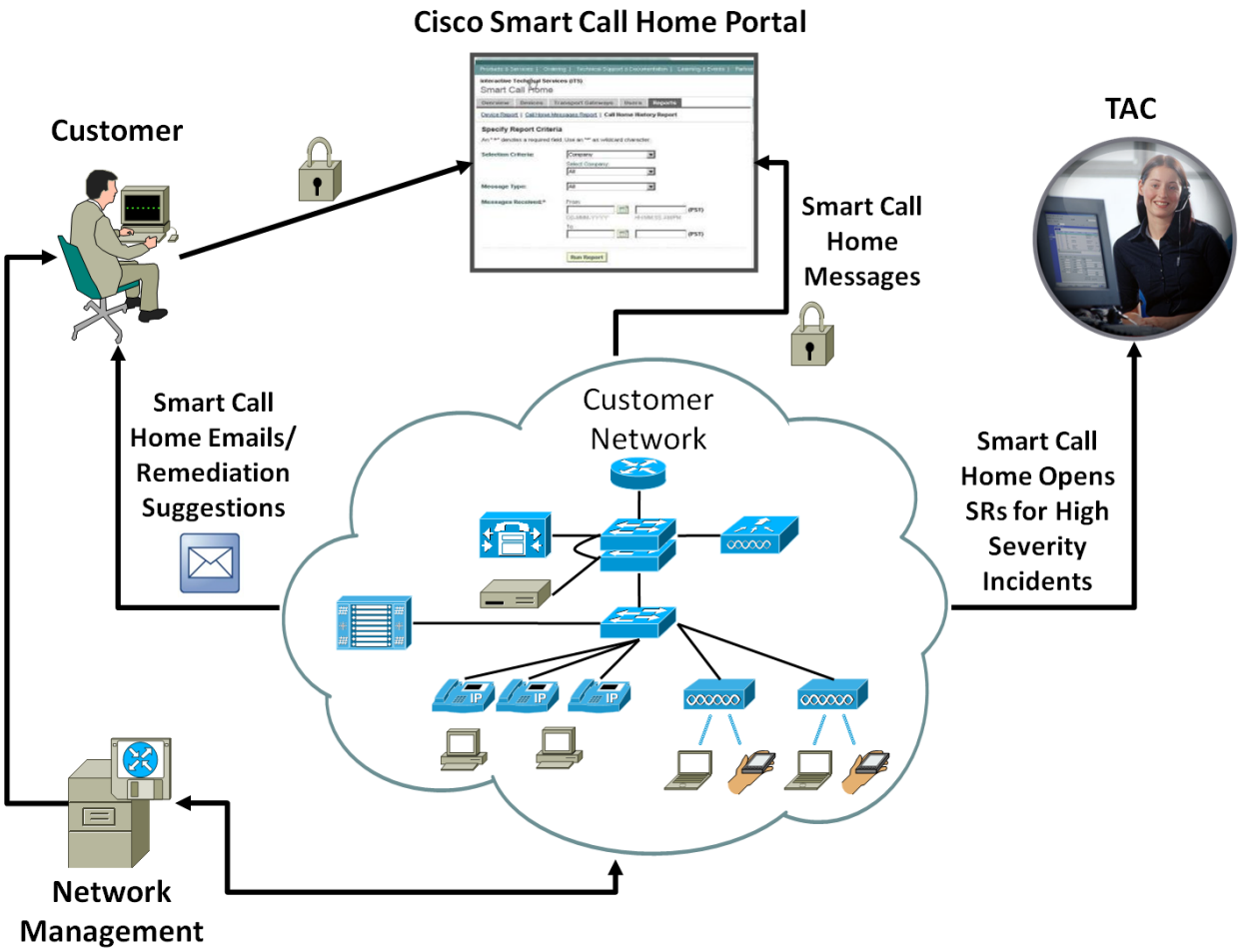
An element management system can deal with one or multiple aspects of the FCAPS model. As such it can provide extensive management capabilities for your network including a comprehensive view of the problems in the network

and the source of the issue(s) via correlation capabilities. Within the FCAPS model, Smart Call Home falls within fault management, and complements the element management systems customers might have.

Once a problem is detected in the network, generally a trouble ticket is opened and the appropriate workflow is followed to help resolve the issue. Using Smart Call Home, customers can choose to be notified by their management systems via email, which can in turn open up a trouble ticket manually or in an automated manner by populating the content of the ticket with relevant information including remediation advice based on Cisco Intellectual Capital which can be leveraged by Cisco TAC. If the problem is critical, an automated service request (SR) is opened up with Cisco TAC, which can result in a quicker resolution of the problem.

In the workflow mentioned, a customer can leverage the capabilities of Smart Call Home to complement the fault management systems that are currently managing the network, thereby helping proactively reduce disruptive impacts to the network, which can result in cost savings and reduced time and effort to resolve the problem.

Figure 4. Cisco Smart Call Home Message Flow



Conclusion

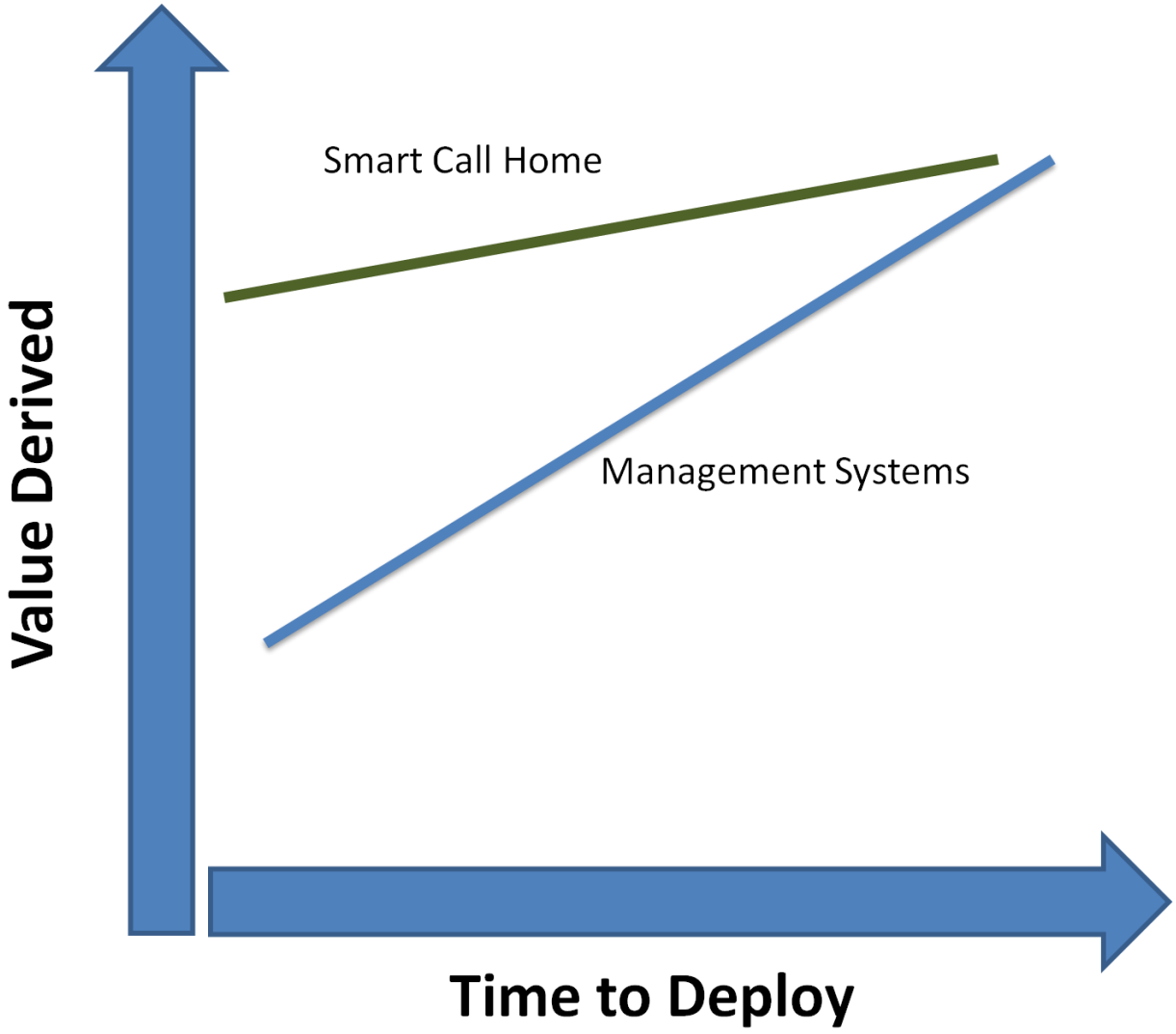
Cisco Smart Call Home is simple and easy to enable. All the relevant error information is transmitted and—based on the analysis and Cisco intellectual property—remediations are suggested. In case of major errors, the customer can leverage the available information to open a service request within their own ticketing systems and resolve the problem. In case of a need for Cisco TAC expertise, customers can leverage the information collected to provide Cisco TAC all relevant device information, helping reduce the mean time to resolution (MTTR).

The embedded capabilities leveraged within Device Diagnostics and the ability to customize profiles provide a powerful tool for network operators to be proactively notified of hardware or software issues on the network while complementing the fault management systems that continue to monitor and manage the network.

As mentioned earlier, management systems are critical in efficiently managing a network. However, configuring and fine tuning those systems and building intellectual capital around remediations requires considerable time and effort.

Figure 5. depicts the potential cost savings, benefits and usefulness of leveraging Cisco Intellectual Capital.

Figure 5. Advantages of Leveraging Cisco Intellectual Capital



For More Information

- Smart Call Home internet home page
- Smart Call Home configuration video
- Smart Call Home Blog Post

Use the Cisco Support Community for Technical Questions

Join the Cisco Support Community to learn more about Smart Call Home by interacting with networking peers and experts worldwide. The community offers a variety of resources that help you:

Connect with peers

Ask questions, get answers and share insights in the discussion forums (such as the Network Infrastructure forum).

Learn from Cisco experts

Learn about specific networking topics via online Ask the Expert discussions, interactive webinars and archived sessions; or explore expert blogs and videos.

Share knowledge

Collaborate with peers to post wiki content, and share documents through social media outlets like Facebook or Twitter.

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 04/11