UPLOGIX

UPLOGIX WHITE PAPER

Making Cisco Stronger with Automated Remote Management

WWW.UPLOGIX.COM

CISCO PARTNER
Technology Developer

Contents

Executive Summary

As more systems and applications centralize and virtualize into the datacenter, the communications and applications infrastructure has become more important than ever. Delivering new technologies and applications such as unified communications, telepresence, security and mobility require the infrastructure to work—and business leaders expect IT to make it happen—at all points on the network at all times.

Cisco developed an architectural platform that takes advantage of a more flexible, adaptive, and feature-rich IT communications infrastructure they call Service-Oriented Network Architecture (SONA). Because today's distributed Cisco infrastructures often include multiple data centers, remote sites or branch offices, management has become increasingly costly and complex. Traditional tools for network and systems management rely on the network, meaning they are effective when the IP-based network infrastructure is operational, but limited when the production network connections or devices fail. This limitation creates business interruptions, increases in services calls and service quality issues.

Automated Remote Management solutions can drastically decrease the headaches and hassles of remote management by eliminating routine repetitive tasks, and minimizing tech support trips to remote sites.

An integrated approach to remote management augments limited and overworked IT staff, enforces internal security policies and proves compliance, and ensures dramatically faster mean-time-to-repair. This white paper outlines the requirements of managing a highly-distributed Cisco infrastructure and examines how Automated Remote Management solutions can drastically decrease the headaches and hassles of remote management by eliminating routine repetitive tasks, and minimizing tech support trips to remote sites.

Today's Challenges

Managing today's infrastructures has become increasingly costly and complex—and it's not any easier just by buying "all-Cisco." The need for continuous access to business information has increased the reliance of enterprises on the network infrastructure to run most aspects of business.

To address this, IT management teams have deployed network and systems management tools like CiscoWorks, LAN Management Solution, Tivoli NetView, HP OpenView, EMC Smarts and others which are generally used to discover, monitor and report the status of the production network using protocols such as SNMP, RMON and Telnet. These tools are effective when the IP-based network infrastructure is operational, but limited when the production network connections fail. When Cisco network devices lose their connection to the production network, an alternate or out-of-band (OOB) infrastructure is necessary to remotely access, diagnose and restore the disconnected device. Even when this is possible and actionable, there is usually still a manual, possibly tedious and time consuming process needed to return the devices and network to working order.

These tools are effective when the IP-based network infrastructure is operational, but limited when the production network connections fail.

Unfortunately, in recent years the growing dependence on networks has been accompanied by an increase in the potential for unplanned network downtime. Several factors have contributed to this risk: IT systems have become more complex and widely distributed within organizations; corporate downsizing has reduced the number of IT personnel available to service the network infrastructure; and systems management can be more complex because hardware and operating system (OS) environments have become increasingly heterogeneous.

The Headaches and Hassles of Remote Management

The greatest challenge to providing high service levels at remote locations, whether it is the data center across campus or remote branch offices, is the lack of onsite IT support staff to monitor, troubleshoot and fix network and system-related problems. According to Nemertes Research, IT staff at large enterprises spend from 30–50% of their time troubleshooting and fixing problems at remote offices. If a problem

does occur, a technician usually has to be dispatched either locally or from a distance to fix it—which can be a costly, time-consuming and sometimes risky proposition. This same scenario repeats itself when extensive maintenance has to be performed on network devices and IT systems at a remote site. For the technician, it can mean unappreciated effort. Often it takes as much as 90% of the time to discover and diagnose a problem and only 10% of the time to fix it.

IT staff at large enterprises spend from 30–50% of their time troubleshooting and fixing problems at remote offices.
—Nemertes Research

Managing remote locations presents a number of unique challenges:

- **Resources** | IT departments usually have to do more with less at remote locations where technical resources are often scarce.
- **Performance** | Remote users frequently experience poor application and network performance due to WAN (wide area network) performance constraints. However, IT staff are often unable to accurately measure end-user performance and cost-effectively resolve issues because they lack the tools that can autonomously find and fix remote problems.
- **Complexity** | During network outages and disruptions, centralized IT staff face reduced visibility, control and security at remote sites because the monitoring and management tools they rely on are themselves dependent on the network being up and functional. As a result, managing remote locations has become increasingly complex. A simple task such as reconfiguring a router can turn into a major headache and expense if it requires deploying support personnel at all hours to hard-to-reach locations on the network.

Technical Limitations of Traditional Remote Management

Unfortunately, **a critical solutions gap exists between current technologies and the management needs of today's highly distributed enterprises**. Neither software-based monitoring nor remote access tools are able to reliably diagnose AND fix problems. Even pieced together in a patchwork of systems, they are unable to respond to events and automate ongoing operations, which forces IT staff to spend more time and expense doing routine administration and recovery tasks onsite at remote locations.

Most network and systems management systems were designed when systems were connected by a local area network (LAN) instead of the wide area networks (WANs) that are becoming pervasive in enterprises today. These LAN environments had

relatively few performance problems due to their high-bandwidth and limited points of failure. They were also easier to maintain when problems did arise since fixing a "remote device" meant, at most, traveling across campus to do so. The majority of these tools rely on a network protocol, such as SNMP (simple network management protocol), to both collect and report system data, which makes them dependent on the very thing they are supposed to manage—the network. During network outages or disruptions, IT staff is left "in the dark" as these network-based tools cease to function. Administrators have no way to control remote devices, nor the ability to gather diagnostic data about the state of remote devices, leading to costly "truck rolls" to get technicians onsite to perform what are often simple recovery actions.

Existing solutions provide rich diagnostic, fault management and reporting information. However, they are not designed for active, Automated Remote Management. In other words, they're good at pointing out problems, but lack the ability to fix those problems.

Automated Remote Management (ARM) from Uplogix Makes Cisco Stronger

To effectively, efficiently and securely manage Cisco Systems network devices in remote locations, a new management approach and architecture is required. Reliable active management should be deployed where it is needed most—at the edge of your network—becoming an integrated component of the IT infrastructure that it is designed to manage.

Uplogix has introduced an innovative approach to remote management that not only fulfills the remote management checklist (see page 13), but also overcomes the shortcomings of existing management tools to address the long-standing costs and challenges of managing a geographically distributed IT infrastructure.

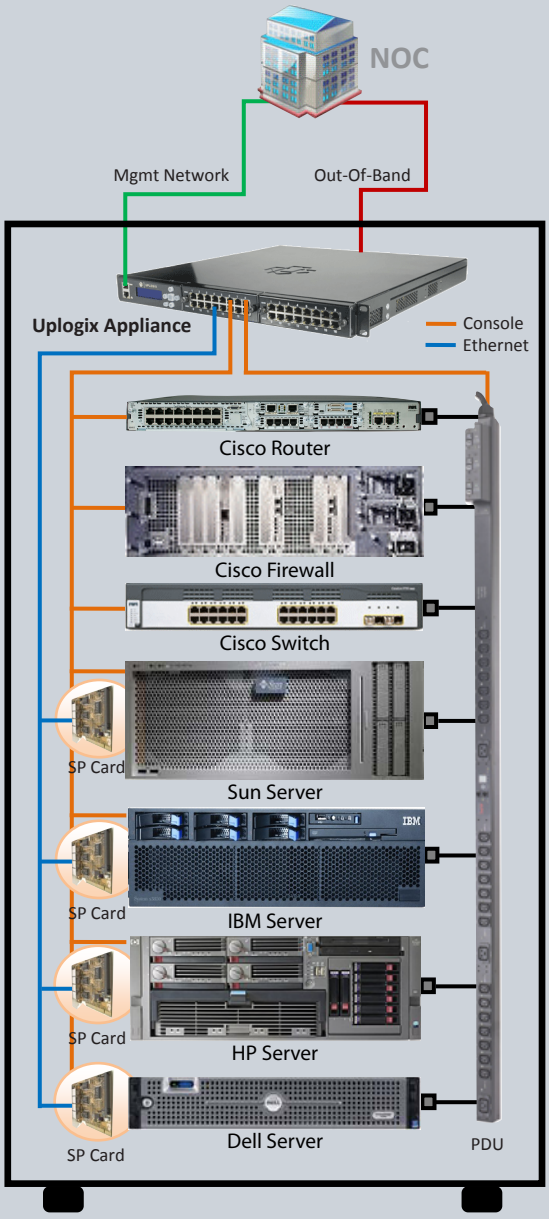
The headaches and hassles of remote management are decreased by the elimination of routine, repetitive tasks and minimized tech support trips to remote sites. Tasks such as IOS upgrades, config changes, password updates, and recovering a device from a ROMmon state can be automated, freeing up admin time for more strategic work. Robust recovery capabilities decrease risk and Uplogix simplifies remote management by reducing the number of tools needed to support remote sites, while improving end-user service levels for greater customer satisfaction.

The ARM Architecture

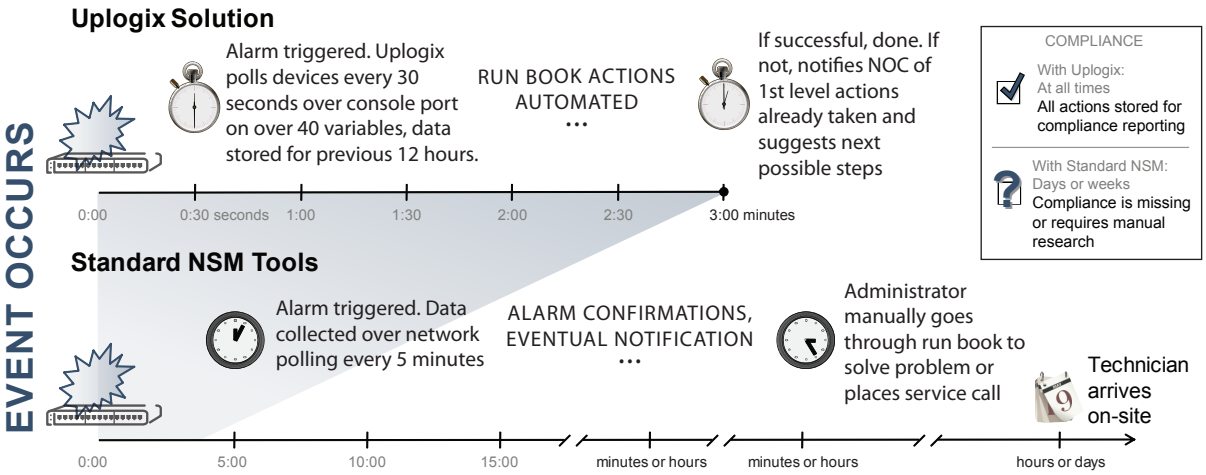
Uplogix' unique and integrated architecture uses an always-available, secure and intelligent direct connection to the remote devices it manages to deliver:

- **Access** | By collocating and directly connecting to the console ports of the Cisco Systems router, switch, firewall and/or VPN concentrator devices, Uplogix delivers uninterrupted connectivity, access, monitoring and control over remote devices—regardless of the state of the network.
- **Control** | With the Uplogix ARM appliance installed locally, it can perform a majority of the routine administration, maintenance and recovery tasks that an onsite network engineer would do today. By diagnosing and fixing problems, as well as automating routine maintenance tasks, the Uplogix platform minimizes costly support calls and visits to remote locations.
- **Enforce** | Uplogix ensures that internal security and management policies are always enforced, even during a network outage. IT staff can control who has access to devices on the network, what they are doing while accessing the devices, and accurately report on all user interactions in order to satisfy security and compliance requirements.

Uplogix decreases the headaches and hassles of managing remote locations by eliminating routine, repetitive tasks and reduces the number of tools you need to support remote sites.



Uplogix vs. Standard Network System Management Tools



Uplogix collects data through serial connections to managed devices. This rich diagnostic data feeds a rules-based policy engine to determine if a parameter is in or out of specification. Uplogix can then either automatically resolve the incident based on pre-approved automated operations, or communicate the problem and recommended recovery steps back to centralized IT staff for resolution management tools. All of this in less time than most standard management tools take to find the problem, and often before users even knew there was an issue.

Case Scenarios

Cisco Router with T-1 Loss of Frame (Primary Path Failure)

Situation

Whether the Cisco device is at a branch office or in a wiring closet at an enterprise headquarters, the need for remote access to the network devices that are unresponsive or cannot be reached over the network infrastructure is critical. The business impact might be greater at the branch office or at the enterprise headquarters, but in either case a network device failure can hamper revenue and customer satisfaction. Plus the issue might remain undiscovered until there is a need for the service, which might be too late.

Current Methods

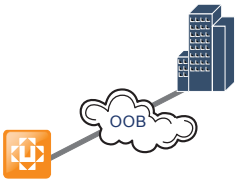
The current solution is to wait for a central network monitoring tool to alert IT staff or the problem is discovered when the remote office employees complain of lost access to company resources. The loss of connectivity and visibility further hinders IT's ability to troubleshoot. Then there is also the problem of how to access the network device remotely and securely. A network engineer or an outsourced third-party IT professional would be dispatched, each costing time and revenue.

Event Timeline

00:00 Loss of frame is detected by Uplogix appliance

00:30 Uplogix monitors the network device every 30 seconds to verify the loss of frame continues to be an issue.

02:30 After 2 minutes of monitoring and confirming the failure, Uplogix establishes a secure OOB connection back to the NOC, and forwards info to technicians and workflow management systems.



03:30 If the problem is still present, Uplogix appliance issues a command to clear the service module

If the problem persists, Uplogix cycles the T-1 interface

5:00 If the problem is still present, Upogix collects Show Tech information

6:00 Still a problem—Uplogix issues a soft reboot

7:30 T-1 interface still down or Loss of Frame is still present—Uplogix power cycles the Cisco device

After the power cycle, if the problem still exists, Uplogix recommends escalating the issue. The problem could be a hardware failure or the ISP is experiencing problems.

Uplogix Solution— Local, In-Depth Monitoring

In the same time it takes traditional network monitoring tools to just discover a problem at a remote site, the Uplogix platform can find it, fix it, and alert the NOC it has been resolved or needs escalation— dramatically reducing your Mean Time to Resolution (MTTR) by eliminating costly "truck rolls" that could add hours or days to the situation.

Image Key

Incorrect Configuration Change

Situation

A network admin makes a change that has caused an outage. Examples include typos, wrong patches and other errors that cause problems with configuration changes in the Access Control List (ACL) for a Cisco network device. This causes the network to become inaccessible for all users in an office. Another example would be when an IOS upgrade patch does not execute on the network device due to corrupted file, corrupt flash sector or not enough RAM on the network device. Situations like these create organizational downtime and an inability to complete mission critical work. In addition, the loss of connectivity and visibility hinders the ability for IT administrators to troubleshoot, prolonging the situation.

Current Methods

There isn't much you can do for this other than dispatch a network engineer to the site to access the device directly or contract with a third-party technician to visit the site. The final option would be to locate and train an onsite employee, which could mean increased risk, delay and possibly still needing to send a technician.

How it works

Connects and authenticates to Uplogix via secure connection

Connects to Cisco device via Uplogix

Initiates a terminal connection to Cisco device

During the terminal initialization to the connected device, a current running configuration is cached by the appliance

Makes changes to the connected Cisco device

Executes IOS commands for the device

If during the session the user logs out of the device or loses connection due to a configuration error, a running configuration is pulled again

Generates a list of changes made during the session and prompts the user with a confirmation to accept, reject or delay the changes made. If the user session times out due to configuration error or general inactivity after a configurable amount of time, the appliance backs out all uncommitted changes made during that session.

The default action is to rollback all uncommitted changes

Starts countdown to SurgicalRollback

If no response, Uplogix will rollback only changes made to the device

Logs event and changes for reporting purposes

Uplogix Solution—SurgicalRollback™

If a configuration change fails, Uplogix can immediately roll the device back to the last known good configuration. **It's an automated safety net to recover from configuration errors without requiring an onsite visit.**

Cisco Network Device Lost Startup Configuration

Situation

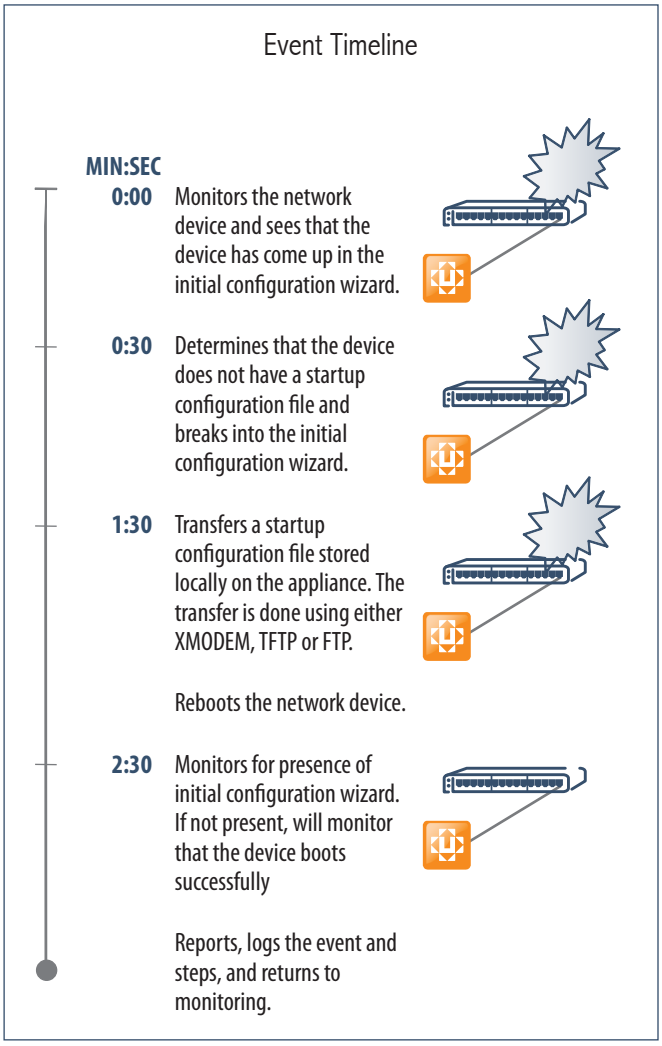
There are times when a brand new router is sent to a remote office, or a Cisco network device loses the startup configuration, or a power glitch corrupts the configuration file. The result is that the network device will boot up in the Cisco initial configuration wizard and wait for a human to input the parameters. This causes downtime in an organization resulting in inability to complete mission critical work, and possibly a mass business disruption effecting multiple sites.

Current Methods

All you can do is dispatch a technician, or call in a third-party technician to access the device directly. Both could be costly in both time and money.

Uplogix Solution—Proactive Maintenance of Remote Problems

Using device manufacturers' best practices, the Uplogix platform has hundreds of built-in management procedures that enable the appliances to take action when certain conditions occur, often fixing technical issues before they become business problems.



Cisco Router enters ROMmon mode

Situation

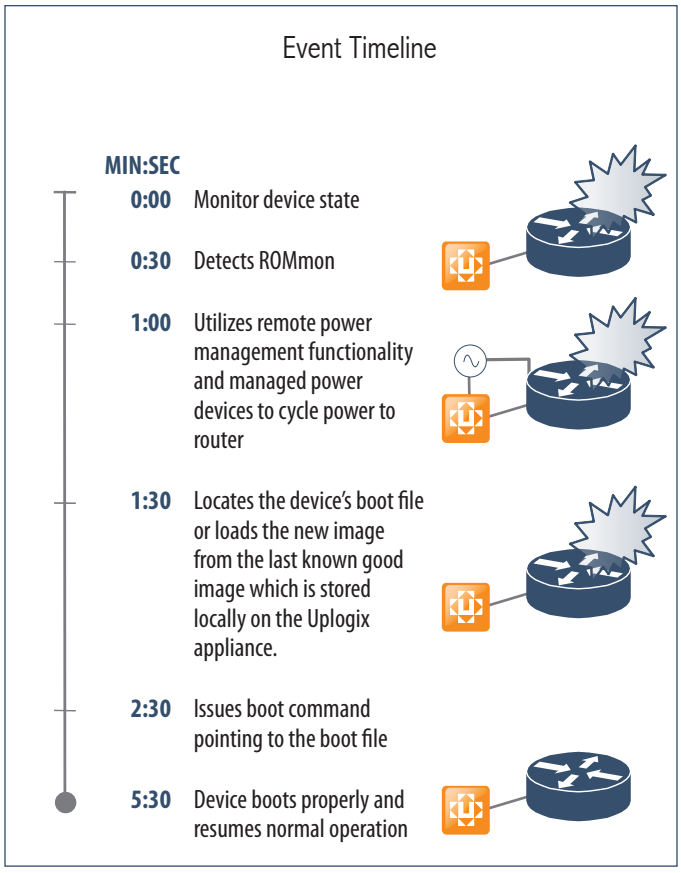
A hung or unresponsive router can enter ROMmon mode for reasons such as a boot failure, settings in the virtual configuration register that force the router to stop in ROMmon mode during the boot, or a break sequence sent to the console. Whatever the cause, the device isn't available for business use, which likely means that the site is down and business comes to a halt.

Current Methods

Send a trained technician, call in a third-party source, or grant access to the devices and try to talk onsite personnel through the repair requirements. All are slow, expensive, and possibly risky alternatives.

Uplogix Solution—Automated Problem Resolution

With built-in intelligence, Uplogix ARM appliances can automatically detect, diagnose and sequence events to restart and recover a device to a working state with the last known good configuration, keeping the network (and business) up and running and alerting IT to the issue.



Mass Configuration / Password / OS Change

Situation

Conditions arise where there is a requirement for a mass push to multiple devices. This can be a labor-intensive operation absorbing hours of manual cycles, and there are multiple opportunities for error or introduction of inconsistencies between devices.

Current Methods

In-band network management systems can perform mass changes, but risk reliance on the network enabled by the very devices undergoing the changes. The expensive alternative is sending a technician to connect to and update each device directly.

Uplogix Solution—Centralized Single Push

The Uplogix Control Center enables Automated Remote Management through a **centralized point of control for all Uplogix appliances and managed devices deployed throughout a distributed IT environment.** With its web-based graphical user interface, the Control Center gives IT administrators real-time data to easily manage, configure, and control all network devices and servers connected to Uplogix ARM appliances.

How it works

Configuration changes or IOS upgrade patches are uploaded to the Uplogix Control Center

Searches the Control Center database for a list of network devices to push the configuration changes or IOS upgrade patches using filters within the Control Center platform. For example, "list all ISR 3825 series routers."

Lists can be created according to region, functionality, location, etc.

Sets a schedule for the configuration change or IOS upgrade patch. For example, schedule the change in Europe first, then North America.

Downloads to the Uplogix appliances:
- Configuration changes or IOS upgrade patches
- Schedule to push the change or upgrade

Executes according to the schedule and configuration change

Reports back to Uplogix Control Center on status of change

Prior to any configuration changes or IOS upgrades, current configuration and IOS image archived

If during the configuration change or IOS upgrade, the procedure fails, appliance rolls back the prior configuration and/or IOS image

Reports status back to Control Center

The Control Center combines "one-click" administration of rules, policies and changes across the entire network, with robust and flexible reporting of device statistics, alarms and events, user interactions and network service levels. It scales to support even the most complex distributed networks and integrates easily with existing management systems.

Conclusion

The role of IT has never been more important or challenging, as successful enterprises expect technology to help gain a competitive edge in the global marketplace. However, managing technology has grown increasingly difficult as IT infrastructure has become more widely distributed, more complex and more susceptible to availability and security breaches. IT staff are stretched thin just trying to stay on top of everything that needs managing, and are constantly being asked to do more with less, leaving little time to focus on strategic initiatives.

Fortunately, new solutions have emerged that overcome the limitations of legacy management tools to enable IT staff to remotely control IT infrastructure at distributed locations.

Uplogix decreases the headaches and hassles of remote management by eliminating routine, repetitive tasks and minimizing tech support trips to remote sites. With the first integrated, remote management solution to provide secure remote access and local, in-depth monitoring, as well as configuration, fault and service level management, Uplogix reduces management complexity. Valuable IT staff time can be allocated to more strategic projects and development of new skills. Uplogix solutions reduce risk by ensuring that management security policies are always enforced (even during an outage), and audit all user interactions with systems to aid in compliance reporting. Uplogix can proactively improve service levels by pinpointing the root cause of a service-related issue and apply Cisco TAC or corporate runbook steps, automatically correcting the issue, reducing MTTR and downtime, which makes all customers happy.

Put Uplogix to Work for You Today

To learn how to make your Cisco implementations stronger with Automated Remote Management from Uplogix, please visit us online or contact us for a technical demo and free evaluation of the benefits of ARM in your infrastructure:

Online:

- uplogix.com/makingciscostronger
- sales@uplogix.com

By phone:

- 877.857.7077 (North America)
- 44(0)207 193 2798 (EMEA)

Appendix: The Remote Management Checklist

How can you determine if a management solution can truly and actively address the challenges of managing remote locations? With so many vendors claiming "management" capabilities, it's important to separate fact from fiction. A solution that provides active, remote control of network devices and IT systems should be able to address the following questions:

- ❑ **How can I securely access and manage a device that I can't physically touch?**
  IT staff need to be able to connect to and control remote devices even when the network is down. All access, communications and actions taken need to be done securely, and audited for reporting purposes. When the primary in-band network connection is unavailable, a secure, out-of-band path is required for accessing and managing devices.

- ❑ **How does the product perform when there is a network outage or disruption?**
  All remote management tasks, including remote access, monitoring, configuration, fault and service level management needs to be performed securely and consistently, regardless of network availability.

- ❑ **How are problems with remote devices detected and fixed?**
  This is what separates monitoring from true management solutions. When common problems arise with network devices or systems, the remote management solution should be able to quickly pinpoint the root cause of an issue and offer the capability to automatically fix it without requiring manual intervention or costly on-site repair. These automated problem diagnosis and recovery abilities should be administrator-controlled, so IT staff can determine which automated features to activate and which to keep manual control over.

- ❑ **How does the product recover when a change fails?**
  Since the majority of unplanned outages are caused by human error while making changes to IT systems, it is imperative that a remote management solution provide some sort of safety net that can quickly recover from failed changes to minimize the risk of human errors and associated downtime.

- ❑ **How does the product enforce security policies?**
  Access and communications with remote devices need to be secure, authenticated and encrypted at all times. User access controls need to be enforced and user sessions managed to ensure that only the right people have the right access to the right systems. And all IT security policies need to be not only always-enforced, but also audited for compliance reporting purposes, even during network outages.

- ❑ **How much automation is built into the product?**
  Routine system maintenance, configuration, and recovery tasks should be automated whenever and wherever possible. It's just too costly and risky to send scarce, trained IT staff, or recruit untrained local staff, to perform these time-consuming tasks. Administrators should be able to control the level of automation desired in order to reduce downtime, speed changes, reduce labor requirements and minimize the risk of unplanned outages.

- ❑ **How complete is the logging data that the product provides?**
  Enterprises need complete reporting data to pass today's stringent compliance audits. This means every user interaction with network devices and systems must be logged and securely stored to comply with data control requirements found in laws such as Sarbanes-Oxley, PCI DSS (Payment Card Industry's Data Security Standards) and HIPAA (Health Insurance Portability and Accountability Act). However, when a network outage or disruption occurs, reporting data on who has accessed devices and what was done to those devices often goes un-captured and unrecorded, which can lead to stiff financial penalties as a result of incomplete reporting information.

- ❑ **How are service levels monitored and managed?**
  Existing service level monitoring and management tools have been designed to measure performance from a central location, not the end user's perspective, so they do not accurately capture and relay the quality of service that a remote user is experiencing. Additionally, these tools usually depend on the network to perform and lack the automation to proactively find and fix service-related issues. To protect SLA's, IT staff needs better visibility and control throughout the distributed infrastructure to accurately measure and manage the application and network service levels being delivered.

- ❑ **How resource-intensive (i.e. performance impact) is the product?**
  SNMP-based tools are limited by how much data they can collect and how often it can be collected in order to minimize the performance impact of these queries on the overall network. Since these tools are network-dependent, they fail to capture diagnostic data during network outages or disruptions—literally leaving IT staff "in the dark" and unable to determine the root cause of a problem, or how to fix it. Local, in-depth monitoring of devices is needed that can gather data on hundreds of diagnostic variables every few seconds without impacting network performance, which means problems at remote sites can be identified and resolved faster before leading to costly downtime that can impact business performance.

- ❑ **How easy is the product to deploy, use and manage?**
  Managing a widely distributed IT infrastructure is hard enough. It doesn't need to be made more challenging and expensive by having to buy, deploy and manage multiple non-integrated, point management tools. An integrated remote management solution is needed that deploys quickly, begins working immediately, is simple to use and manage, and integrates seamlessly with existing IT management systems.

To learn how to make your Cisco implementations stronger with Automated Remote Management from Uplogix, please visit us online or contact us for a technical demo and free evaluation of the benefits of ARM in your infrastructure:

- **uplogix.com/makingciscostronger**
- sales@uplogix.com
- 877.857.7077 (North America)
- 44(0)207 193 2798 (EMEA)

ABOUT UPLOGIX // Uplogix provides the first fully-integrated remote management solution. Our collocated management appliances automate routine administration, maintenance and recovery tasks—securely and regardless of network availability. In comparison, traditional network and systems management requires multiple tools, relies on the network, and remains labor intensive. Uplogix puts the power of your most trusted IT administrator everywhere, all the time.

Uplogix is privately held and headquartered in Austin, Texas with European offices in London.
For more information, please visit **www.uplogix.com**.

UPLOGIX