UPLOGIX

UPLOGIX WHITE PAPER

REMOTE CONTROL:

How to Reduce the Cost, Complexity and Risk of Managing Your Distributed IT Infrastructure

APRIL 2008

WWW.UPLOGIX.COM

Contents

Executive Summary

If money were no object, companies could station a trained IT administrator in front of every router, switch, firewall and server in their distributed network that needed to be managed. However, competent IT staff is becoming both harder to find and harder to hold on to.

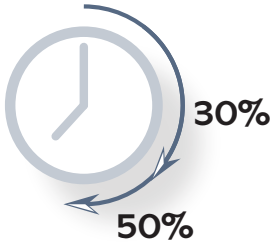
Unfortunately, traditional network and systems management approaches cannot address the cost and complexity challenges of managing a widely distributed IT infrastructure. Due to their legacy design and architectural limitations, they are slow to detect and diagnose issues and usually cannot take action to fix the problem themselves. This forces IT staff to get involved in routine and burdensome actions, driving up costs and increasing the risks of error and non-compliance.

New secure remote management solutions can drastically reduce the cost, complexity and risk of managing remote locations, while also improving the service levels that IT delivers in the process.

A new active and integrated approach to remote management is needed that can augment limited and overworked IT staff. This white paper outlines the requirements of managing a highly distributed IT environment and examines how new secure remote management solutions can drastically reduce the cost, complexity and risk of managing remote locations, while also improving the service levels that IT delivers in the process. Finally, it provides a specific business case and customer examples that illustrate why it makes sense to take action with this fresh approach now.

The Costs and Challenges of Remote Management

The greatest challenge to providing high service levels at remote locations, whether it be the data center across campus or a far-flung branch office, 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.



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. First, IT departments usually have to do more with less at remote locations where technical resources are often scarce. Second, remote users frequently experience poor application and network performance due to WAN (wide area network) performance constraints. However, IT staff is 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. Finally, during network outages and disruptions the centralized IT staff faces 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 to hard-to-reach locations on the network.

Limitations of Traditional Approaches to 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 or remote access tools are able to reliably diagnose and fix problems, or automate ongoing operations, which forces IT staff to spend more time and expense doing routine administration and recovery tasks at remote locations.

Network and Systems Management Solutions

Most network and systems management systems, such as Tivoli NetView, HP OpenView, NetCool, or EMC Smarts, were designed when systems were connected by a LAN (local area network) 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" of on-site technicians to perform what are often simple recovery actions.

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

Remote Access Technologies

Remote access technologies such as KVM (keyboard, video, mouse) and console/terminal servers, on the other hand, provide an alternative path to access remote devices, overcoming the network dependency issue of software-based network monitoring tools. These technologies give administrators the same kind of control they would have if they were sitting in front of the device. However, they too lack the intelligence and automation capabilities to identify and resolve problems, or execute routine tasks, leaving it up to an IT administrator's best guess to fix critical issues and make changes manually.

According to Forrester Research, US companies spent in excess of $25 billion on network support personnel in 2006 alone and this figure is set to grow as networks expand across time zones and geographic boundaries.

Internal and Outsourced IT Staff

As a result of the limitations of existing management tools, IT staff is still too often called upon to perform routine system maintenance, configuration and recovery tasks at remote locations. According to Forrester Research, US companies spent in excess of $25 billion on network support personnel in 2006 alone, and this figure

is set to grow as networks expand across time zones and geographic boundaries. Throwing more personnel at the problem is an expensive and inefficient solution for what legacy management tools cannot address. Often it's the only viable alternative to avoid costly outages and downtime that can severely impact business operations.

To counter the difficulty of hiring and retaining technical staff to manage the network, many enterprises are turning to outsourcing as an alternative. The rational to shift the problem into somebody else's lap may well fix a short-term issue, but does not solve the fundamental process weakness in the management of the network—that routine maintenance and break/fix tasks are still being performed manually. As a result, remote management of the network and the distributed IT infrastructure remains a mundane, costly, and error-prone task.

Secure Remote Management from Uplogix

To effectively, efficiently and securely manage remote locations, a new management approach and architecture is required. Solutions need to be deployed where they are needed most—at the edge of your network—becoming an integrated component of the IT infrastructure that they are designed to manage.

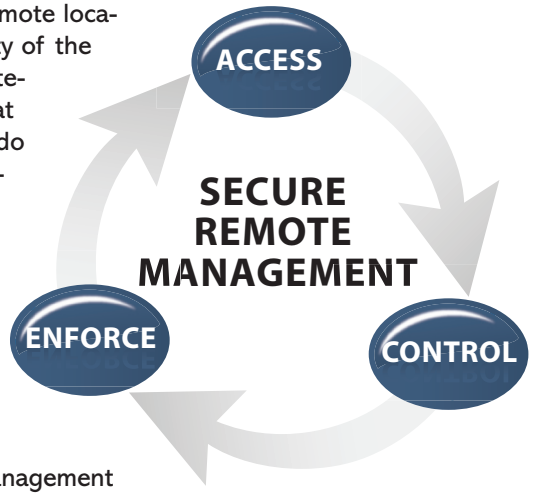
Uplogix has introduced an innovative approach to remote management that not only fulfills the remote management checklist (at the end of this paper), but also overcomes the shortcomings of existing management tools to address the long-standing costs and challenges of managing a geographically distributed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

Instead of having to hire and dispatch an army of technicians in the field to sit in front of routers, switches, servers and firewalls, watching them for problems, and taking action if something goes wrong or needs changing, Uplogix provides an intelligent remote management solution that essentially performs the same functions, but faster, error-free and at a fraction of the cost. Deploying Uplogix is like putting the power of a competent, trusted IT administrator everywhere they're needed, all the time.

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 network devices, servers and communications equipment, Uplogix delivers uninterrupted connectivity, access, monitoring and control over remote devices—regardless of the state of the network.

- **Control** | With the Uplogix remote management solution on-site at a remote location, it can perform a majority of the routine administration, maintenance and recovery tasks that an on-site technician would do today. By diagnosing and fixing problems locally as well as automating routine maintenance tasks, the Uplogix solution minimizes costly tech support calls and on-site 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.

Access

Uplogix provides secure, always-available access to the distributed devices you need to manage, and continuously monitors devices locally.

Secure Access & Connectivity

One of the biggest challenges to managing remote locations is being able to securely connect to and access remote devices to perform maintenance tasks or troubleshoot and fix problems.

Traditional remote access solutions typically use network-based protocols, such as SNMP or Telnet, which can render them both unreliable in the case of a network outage and insecure due to a lack of encryption and authorization controls.

Uplogix solutions don't rely on the network to manage the network. Uplogix SRM appliances are collocated and directly connects to devices and servers to deliver persistent connectivity, as well as localized management services—regardless

of the state of the network or device. This means that you always have secure access to the distributed devices you need to manage.

When the network is functioning properly, Uplogix appliances uses an Ethernet-based connection to connect to the centralized management server, the Uplogix Control Center. But when it's not, appliances immediately establish remote connectivity via a secure out-of-band path using a variety of backup communication options including dial-up modem, cellular network, or satellite communications. This enables the appliances to deliver secure, always-on access and connectivity to remote devices.

In-depth, Local Monitoring

IT staff not only need to be able to constantly and securely access remote devices, but also need to be able to effectively monitor the distributed infrastructure in order to ensure its health and performance. Traditionally administrators have relied on network monitoring tools to provide this visibility. However, SNMP-based monitoring 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.

Uplogix solutions can gather much more granular diagnostic data and more frequently than SNMP-based systems without affecting the performance of the devices or the network. Uplogix appliances leverage a serial connection to managed devices and servers to collect data, either in-band or out-of-band, on hundreds of network performance variables, every 5 to 30 seconds. More importantly, this rich diagnostic data feeds a rules-based policy engine which can determine if a parameter is in or out of specification. Uplogix can then either automatically resolve the incident based on pre-approved guidelines, or communicate the problem and recommended recovery steps back to centralized IT staff for resolution.

Control

Uplogix provides local, assisted automation and control of routine maintenance, configuration, recovery, and service level management tasks.

Proactive Maintenance

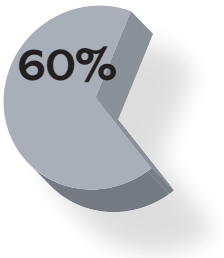
The majority of an enterprise IT staff's time is spent maintaining and making changes to the network and its underlying IT infrastructure. Routine tasks like OS

upgrades, patches, password resets, and configuration changes are ripe for automation, but remain largely manual, time-consuming and costly. IT staff often puts off necessary changes like OS upgrades because of the fear and certainty that some percentage of changes will fail, leading to costly system downtime while someone tries to figure out which change failed, why, and how to restore service.

The Uplogix Remote Management Operating System (RMOS) provides the intelligence for proactive maintenance capabilities that customers can control to speed changes, dramatically reduce the labor resources required, and minimize the risks of manual errors. Uplogix allows customers to selectively choose which maintenance activities to automate and to what degree—and provides a built-in safety net to quickly recover from failed changes.

Configuration Management & Recovery

According to market research firm Enterprise Management Associates, 60% of network downtime is caused by human error during device configuration. There are just too many devices to manage and too many changes to make to those devices on a regular basis in enterprise environments to rely on manual, error-prone, one-at-a-time processes. Uplogix offers significant time and cost savings by providing the capability to automate common configuration management tasks, and reduces downtime by eliminating common errors introduced by the manual execution of these tasks. In fact, the Uplogix platform has been designed to give the option of automating more than 60% of normal change management tasks—like OS upgrades, password updates, and all-important device configuration changes.



60% of network downtime is caused by human error during device configuration
—Enterprise Management Associates

If a configuration change fails, Uplogix immediately rolls the device back to the last known good configuration using its unique SurgicalRollback™ feature, minimizing downtime that is impossible to avoid using in-band only software solutions.

This process restores the device to working order without affecting other device operations. The Uplogix appliance locally stores multiple configurations for each device under management to enable this powerful feature. This capability alone has prevented many hours of downtime and a number of headaches for our customers.

Automated Problem Resolution

Finding and fixing IT problems at remote sites remains a time-consuming, labor-intensive and expensive process. Existing management tools are good at monitoring devices and identifying problems, but lack the intelligence and local control to actively fix problems when they occur, forcing IT staff to go on-site to perform routine fault diagnosis and recovery tasks.

Uplogix can address and resolve 95% of the issues that commonly impact distributed networks

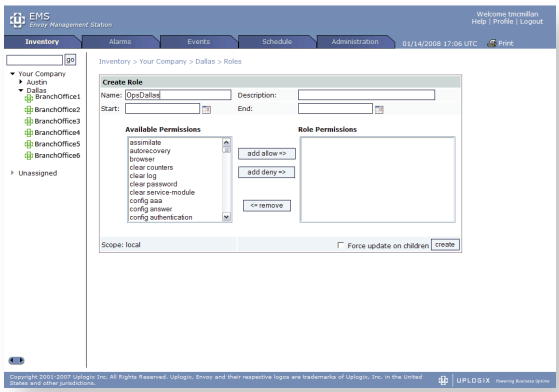
Uplogix lowers the cost and complexity of remote management by proactively finding and automatically fixing common problems throughout your infrastructure. In fact, Uplogix can address and resolve 95% of the issues that commonly impact distributed networks such as configuration errors, nonresponsive devices and telecom hardware failures. Using device manufacturers' best practices, the Uplogix RMOS has hundreds of built-in management procedures that enable the appliances to take action when certain conditions occur. For example, Uplogix can automatically recover devices from ROMmon state or power cycle a frozen console. Uplogix' ability to automatically fix problems locally, quickly and consistently reduces downtime incidents and lowers your support burden by eliminating the need for manual intervention.

Remote Power Management

Complex IT infrastructure devices such as servers, networking and telecom equipment are prone to entering states that are not recoverable through normal remote administrative commands—even at the BIOS level. This often leads to the inevitable step of a hard reboot, which requires an administrator to physically power cycle the device. This is not only an inconvenience (especially if it is remotely located or if it happens in the middle of the night), but it can lengthen downtime, disrupt business continuity and increase support costs.

Not only can Uplogix securely access and control power to non-responsive remote devices, but by using a best-in-class automation engine, more complex recovery actions can be executed such as recovering from a failed configuration change. For example, Uplogix can power cycle a remote server, break into the reboot sequence at just the precise moment, and restore the last known good configuration file for the device—all within seconds and without ever having to dispatch a support technician on-site.

Using the Uplogix remote power management feature allows monitoring, management and control of power to nearly every device in a distributed IT infrastructure—regardless of network availability.



The Uplogix Control Center enables secure remote management through a centralized point of control for all Uplogix appliances and managed devices deployed throughout a distributed IT environment.

Service Level Management

One of the biggest challenges in managing remote locations is ensuring the same high levels of IT service are being delivered to a remote workforce as the employees at headquarters receive. Centralized IT staff has not traditionally had enough visibility and control at the network's edge to accurately measure and manage network and application performance. Existing service level monitoring and management tools have been designed to measure performance from a central location, not the end user's perspective. Additionally, these tools usually depend on the network to perform and lack the automation to proactively find and fix service-related problems.

Uplogix solutions are designed to meet these challenges by monitoring, measuring and managing the performance of critical network services and applications from the end-user's perspective. Using synthetic transactions, the advanced version of the Uplogix RMOS regularly collects network- and application-specific performance data from each remote management appliance.

> Administrators can quickly and easily establish acceptable thresholds for all monitored services and receive alerts via email when service-level events occur that violate these thresholds.

This data is uploaded to the Uplogix Control Center—Uplogix' web-based central management console—where it is available for operators to view and analyze. Administrators can quickly and easily establish acceptable thresholds for all monitored services and receive alerts via email when service-level events occur that violate these thresholds. Service-level data is also stored and archived for up to one year to facilitate trend analysis, and can be easily exported for custom reporting or integration into other management systems.

Most importantly, Uplogix can proactively improve service levels by quickly pinpointing the root cause of a service-related issue and automatically correcting it if desired, drastically shortening the mean-time-to-recover and avoiding costly downtime.

Enforcement

Uplogix provides consistent IT security and policy enforcement, even during network outages, and logs all actions to ensure complete compliance reporting.

IT Policy Enforcement

Uplogix helps customers eliminate security threats before they impact the network, overcoming the security risks of traditional management protocols used today, such as SNMP and Telnet, and setting a new standard for enforcing IT policies. The SRM appliances operate on a secure management platform that supports the industry's most stringent AAA requirements, ensuring that security and management policies are always enforced, even during a network outage. Additionally, Uplogix utilizes the strongest security, encryption and authentication standards on the market such as SSHv2 to access and communicate with managed devices.

Uplogix solutions ensure that only the right users have the right access to devices and systems by providing very granular and customizable authorization controls, as well as role-based permissions.

Uplogix solutions ensure that only the right users have the right access to devices and systems by providing very granular and customizable authorization controls as well as role-based permissions. Uplogix appliances can even be setup to accommodate additional security precautions, such as restricting access to specific IP addresses and encrypting passwords stored in the database, or automating management functions related to security enforcement, like updating the access passwords on hundreds of managed devices at once.

Audit & Compliance Reporting

Enterprises need complete reporting data to pass today's stringent compliance audits. companies are often penalized as a result of incomplete information, especially when outages have occurred. During the network's most vulnerable moments, reporting data on who has accessed devices and what was done to those devices often goes uncaptured and unrecorded.

Leveraging dedicated serial connections with managed devices and servers, Uplogix appliances log all changes made by users and the results of these changes. This information is saved locally and then transmitted to a central location for analysis and long-term storage. Logging, recording and reporting are unaffected by the state of the network—Uplogix appliances continue to satisfy compliance requirements even during downtime. Uplogix can also inspect the log files in real-time for problems and can proactively take automated recovery actions based on log patterns—a feature unique to Uplogix that can put an end to the laborious, and time-consuming process of manually sifting through log data trying to find the proverbial "needle in the haystack."

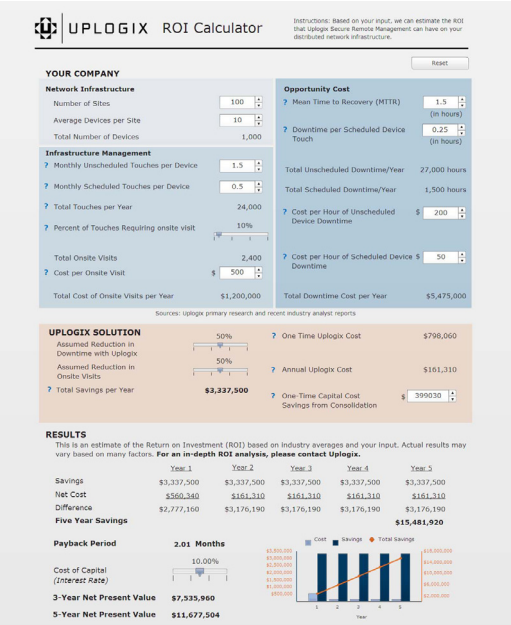
The Business Case for Remote Control

The business case for implementing remote control is a compelling one demonstrated by the many enterprises that have successfully deployed the Uplogix secure remote management platform across a wide variety of industries (see Case Studies). Deploying Uplogix solutions can significantly reduce the cost, complexity and risk of managing a distributed IT infrastructure, while improving IT service levels in the process.

Reduced Costs

Uplogix solutions can reduce 25-50 percent of remote IT support costs by automating a majority of the routine maintenance and recovery tasks that an IT administrator has to manually perform today, but faster, error-free and at a fraction of the cost—resulting in lower ongoing operational costs and increased uptime. Uplogix proactively finds and fixes problems at remote sites within minutes, often before other management tools even know there is a problem, reducing the mean-time-to-repair from hours or days down to minutes. Additionally, the built-in safety net feature called SurgicalRollback™ helps to quickly recover from failed changes, minimizing costly unplanned outages caused by human error.

Capital costs per location can also be greatly reduced by replacing myriad point solutions with the Uplogix single, integrated remote management platform that is the first to incorporate the critical functionalities of access, control and enforcement that IT administrators need to successfully and cost-effectively manage a widely distributed IT infrastructure.



The Cost Savings Calculator at www.uplogix.com/ROI provides a way to explore the full financial impact of IT support and how Uplogix solutions can reduce the cost, complexity and risk of managing your distributed IT infrastructure.

Reduced Complexity

The number of tools and personnel needed to manage a distributed IT infrastructure can be greatly reduced with Uplogix solutions as they combine the local access and control of remote access technologies such as KVM or a console server, the in-depth monitoring and diagnostics of systems management software, and the competence and capabilities of an on-site technician into one integrated remote management appliance.

Instead of having to piece together a mix of disjointed technologies and point products to manage a distributed infrastructure, Uplogix has taken a best of breed approach and incorporated a number of critical remote management capabilities, including remote access and network/system monitoring, as well as configuration, fault and service level management into a single management appliance that is simple to deploy, use and manage.

Uplogix appliances are deployed locally where they are needed most, becoming an integral part of the network infrastructure that they are designed to manage—acting as a local, trusted, 24/7 IT administrator in locations that are too costly or difficult to support with on-site technicians. Although deployed locally, Uplogix appliances can be managed centrally via the web-based management portal of the Uplogix Control Center, where IT management tasks can be scheduled and consistently executed system-wide, or on a one-off basis. And, there is no need to "rip and replace" as Uplogix solutions integrate seamlessly with existing enterprise monitoring and management systems, complementing the investment already made by providing a level of local control and automation not previously available.

There is no need to "rip and replace" as Uplogix solutions integrate seamlessly with existing enterprise monitoring and management systems,

Reduced Risks

According to the FBI, two of the top four types of security attacks are related to insider abuse or unauthorized access to systems. Uplogix solutions reduce this risk by ensuring that management security policies are always enforced, even during an outage. They make certain that only the right users have the right access to the right systems at the right time, unlike network-based solutions that fail to enforce security, access and audit controls during network outages. They don't rely on the network to manage the network, instead Uplogix uses the most reliable and most secure management channel—the console port—for constant access and connectivity to remote devices, and utilizes the strongest security, encryption and authentication standards on the market to access and communicate with managed devices. Additionally, a number of management tasks related to security enforcement can be automated, such as automatically updating the access passwords on hundreds of managed devices at once.

A recent survey of Fortune 1000 companies conducted by the Yankee Group, found that over 50 percent of respondents reported unauthorized network changes in a 12 month period. What's worse is that the majority of these respondents said they couldn't account for nearly half of those unauthorized changes. Detailed audit and logging information is a must to become compliant with new federal and industry

regulatory standards such as Sarbanes-Oxley, PCI DSS, HIPAA and ITIL. Uplogix captures, logs and archives every user keystroke and output, unlike SNMP-based tools that fail to capture changes during a network outage. Uplogix solutions enable policy compliance by monitoring, measuring and reporting on all changes made to the managed IT infrastructure to satisfy internal and regulatory security standards.

Improved Service Levels

Uplogix can proactively improve network and application service levels for remote users, ensuring increased productivity and reduced downtime. Unlike centralized, software-based service level monitoring solutions, the advanaced version of RMOS can monitor, measure and manage the performance of critical IT services and applications, including TCP/IP communications, web-based transactions and IP telephony, from the end-user's perspective to provide a true representation of what remote users are experiencing. And go a step further by pinpointing the root cause of a service-related issue and automatically correcting it if possible in order to keep key systems and applications available and performing well, reducing the mean-time-to-repair a problem and associated downtime. Furthermore, Uplogix protects SLAs by providing detailed reports and metrics required to hold both internal IT staff and third party service providers accountable.

Case Study #1:

RigNet Relies on Secure Remote Management to Significantly Reduce IT Support Costs

RigNet delivers managed remote communications and networking solutions for offshore drilling platforms and remote locations worldwide. RigNet's solutions are available to drillers, operators, and service companies on over a quarter of the world's mobile offshore platforms.

Remote Management Challenges

The primary responsibility of RigNet's operational team is to ensure that a customer's communications network is always available and delivering a high quality of service. However, this is especially challenging to control in an industry where customers have remote sites located in inhospitable and often hazardous places.

When communications go "off-line" due to an outage or service disruption, it usually means dispatching a RigNet technician via plane or helicopter to fix the problem—a

costly, time consuming, and sometimes dangerous proposition. The same holds true when extensive maintenance has to be performed at a remote site, such as upgrading communications equipment to the latest software revision.

Key Benefits:

- Automates over 75% of routine network support and maintenance tasks
- Remotely monitors and manages customers' hybrid satellite and terrestrial networks
- Out-of-band capabilities enable "always up"network availability

Secure Remote Management in Action

RigNet's executive team selected the Uplogix management appliance and the Uplogix Control Center to meet their rigorous network support and automation requirements. Uplogix appliances serve as an on-site, virtual network assistants and are deployed at RigNet's teleport and POP locations to manage their internal infrastructure, as well as at end-customer locations to automate problem diagnosis and recovery, perform routine network maintenance and configuration, and ensure network availability, even when the primary connection is down.

If a customer's main broadband satellite link goes down due to a failed configuration change or other unforeseen circumstances, the Uplogix appliance at the remote disconnected location automatically dials out to a low earth orbit (LEO) satellite via an integrated external modem to re-establish an alternate, out-of-band network connection to ensure constant management connectivity and availability.

The Uplogix Control Center is used by RigNet's staff to centrally manage all satellite and terrestrial network equipment from a single screen via the web-based portal. From the Control Center, administrators can schedule and coordinate all network maintenance and management operations. In addition, the Uplogix Control Center serves as the central repository and reporting interface for all data collection and audit logs provided by the Uplogix appliances deployed at RigNet's customer locations.

Case Study #2:

Global Bank Protects Infrastructure from Insider Abuse to Reduce Risk

One of the world's largest financial institutions faced the challenge of managing a highly distributed and complex global infrastructure, while ensuring compliance with strict security and compliance standards. The bank's IT staff found themselves consistently failing internal security audits as a result of vulnerabilities introduced by the legacy terminal servers that were widely deployed throughout their environment to provide remote access to Solaris servers and networking equipment.

After a competitive selection process, the bank chose Uplogix as a solution to improve security and compliance standards. Key criteria were the delivery of out-of-the-box support for Secure Shell Version 2 (SSHv2), which leverages powerful encryption technologies to protect management communication with the bank's Solaris servers. Unlike other remote access products, the Uplogix appliances provide encrypted access both in-band and out-of-band.

When the network is functioning properly, Uplogix appliances use an in-band Ethernet-based connection to connect to the centralized management server, the Uplogix Control Center. If this primary management link becomes unavailable, the appliance immediately establishes remote connectivity using a dial-up modem, cellular network, or satellite communications; this secondary link offers the bank the same secure, encrypted access as the in-band connection.

Granular Control

Uplogix satisfied the bank's need to protect root passwords by providing command-level access control and simple role-based permissions to ensure that the right users get the right access to the right devices. While traditional console servers only provide port-level control over permissions, the Uplogix

Key Benefits:

- Encrypted management access to Solaris servers, both in- and out-of-band
- Granular, role-based permissioning with port- and command-level authorization controls
- Logging and compliance reporting of all user interactions, keystrokes, and changes
- Session management, such as ensuring the proper termination of user sessions to prevent unauthorized "piggybacking" sessions
- Centralized management of the appliances

appliance can control every command inside the system on a per-user or per-group basis, giving the bank the ability to appropriately delegate responsibilities between the operations, engineering, and security teams in accordance with their management policies. Uplogix also integrates with remote authentication mechanisms, such as TACACS and Radius; if connectivity is lost, the appliances rely on cached authorization data to maintain permissions even during downtime.

Logging and Compliance Reporting

To ensure compliance with internal audits, the bank relies on the robust logging and reporting capabilities of Uplogix. The appliance logs three sets of data, including console data from the Solaris servers and other networking devices, session data detailing user interactions with servers and devices, and change data that records any configuration modifications. Uplogix collects this data at all times—even during outages—to provide complete reporting.

Additionally, Uplogix delivers powerful real-time log inspection capabilities. This enables the appliance to generate alarms or take automated actions when specific patterns are identified in the log data. For example, the Uplogix appliance might generate an alert when a user starts or stops a critical network service on a server or when a potentially detrimental procedure is run on a router.

Conclusion

The role of IT has never been more important or challenging. Successful enterprises are increasingly turning to technology to gain a competitive edge in the global marketplace. However, managing technology has grown increasingly more difficult as the 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.

However, new solutions have emerged that overcome the limitations of legacy management tools to enable IT staff to remotely control IT infrastructure at distributed locations. The Uplogix secure remote management platform takes the headaches and hassles out of managing remote locations, greatly reducing the costs and risks that have saddled enterprise IT staff for years. To learn how to solve your toughest remote management challenges, visit uplogix.com or contact Uplogix today.

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.

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**.

www.uplogix.com | Headquarters: 7600B N. Capital of Texas Hwy. Suite 220, Austin, Texas 78731 | US Sales 877.857.7077, International Sales +44(0)207 193 2798

UPLOGIX