Remote Power Management:

The Key to Maximizing Network and Server Uptime

Contents

Introduction

Many businesses and service providers rely heavily on distributed LAN/WAN internetworking equipment. The revenue stream from internetworking equipment is jeopardized with the long list of problems caused by a failed network. Potential disasters include lost revenue, customer dissatisfaction, decreased productivity and service level agreement penalties.

When a device "locks-up" or fails, the options for recovery are limited. The most proven method is to cycle power or reboot. If the internetworking device is at a remote POP site, Telco central office, co-location facility or even an equipment room, gaining access to perform the reboot on the device can present a challenge.

In addition, a majority of enterprises use uninterruptible power supplies (UPS) to keep their equipment operational. Multiple internetworking devices are connected via a single UPS to power outlets, which poses its own dilemma. If an individual router fails, for example, the UPS does not have the ability to power cycle an individual power outlet. There are typically two recovery choices. One option is a radical approach whereby an operator can command the UPS to simultaneously power cycle both itself and all its attached devices. The second choice is to dispatch a technician to power cycle the problem router at the remote location. Both options have their definite drawbacks in time and expense.

The realities in dealing with internetworking problems are:

- Most third party technician service calls to locked-up network equipment are solved with a reboot operation
- A third party service call averages about $500
- The average downtime from locked-up equipment averages 1.5 hours
- Service level penalties and lost revenue go up exponentially by the size of the enterprise

Significance of Intelligent Power Distribution

A critical factor that defines what equipment can be installed is the available power. Service providers and other businesses whose revenue is dependent upon the quantity of internetworking devices they manage need to know the maximum number of devices the available power resource will support. Yet, configuring the maximum number of devices for a power supply is not a straightforward process.

With the expectation of an always on, always working Internet economy, installation of new equipment is needed to handle the exploding data loads. Adding more equipment, however, is constrained by the availability of power resources and complicated by the manufacturer's nameplate specification, which is generally inaccurate and cannot be used for power planning.

The solution for adding new equipment to existing power supplies is to perform power measurement verification. If, however, equipment units are co-located at multiple sites, then performing on-site measurement verifications becomes costly and time-consuming. There is also the consideration that technicians with the skills to perform power verification are very limited. Remote Power Management devices can expedite this process, performing the needed verification remotely.

The Need for Remote Power Management

Maintaining maximum 99.99% uptime of devices in the data center is imperative for today's distributed networks. There is a solution to quickly return a network to operational status after a failure or a system reconfiguration. A Remote Power Management solution provides maximum uptime by isolating individual locked-up components and independently rebooting that device. Remote Power Management Devices provide a logical, software-controlled interface to individual power modules. Remote Power Management combines intelligent power distribution, management and measurement into a single device. Using this solution, network and system administrators, service providers and hosting companies are able to power On/Off and reboot attached servers or individually control the power to attached devices from a remote location. This is achieved via in-band or out-of-band communications through a Console Server, Remote KVM™ or directly over an IP network.

The Remote Power Manager provides the ability to immediately power cycle or reboot the network without interrupting all the equipment attached to the UPS. Remote Power Managers in conjunction with a console server or Remote KVM can also initiate a graceful shutdown for a wide variety of servers, and provide remote equipment monitoring to ensure that software is running correctly.

Another important function that Remote Power Managers can provide is power sequencing. During a power-up, each of the power outlets can power on sequentially, which distributes the load and eliminates the risk of a blown fuse or circuit breaker trip. Highly useful in a networked data center, power sequencing gives system administrators the option to turn on certain devices before others.

A further way Remote Power Managers help to maximize data center utilization is through environmental monitoring. Remote Power Managers should include temperature and humidity sensing allowing for the remote monitoring of critical environmental conditions.

Benefits
- Improved problem/solution response time
- Reduced field service visits and costs
- Improved network availability
- Improved facility security

How Remote Power Management Technology Works

A network control center utilizes a terminal emulation application to establish immediate asynchronous communications. This can be done via modem, console server, Remote KVM or direct TCP/IP connection. A password protected user interface allows control to each power output receptacle.
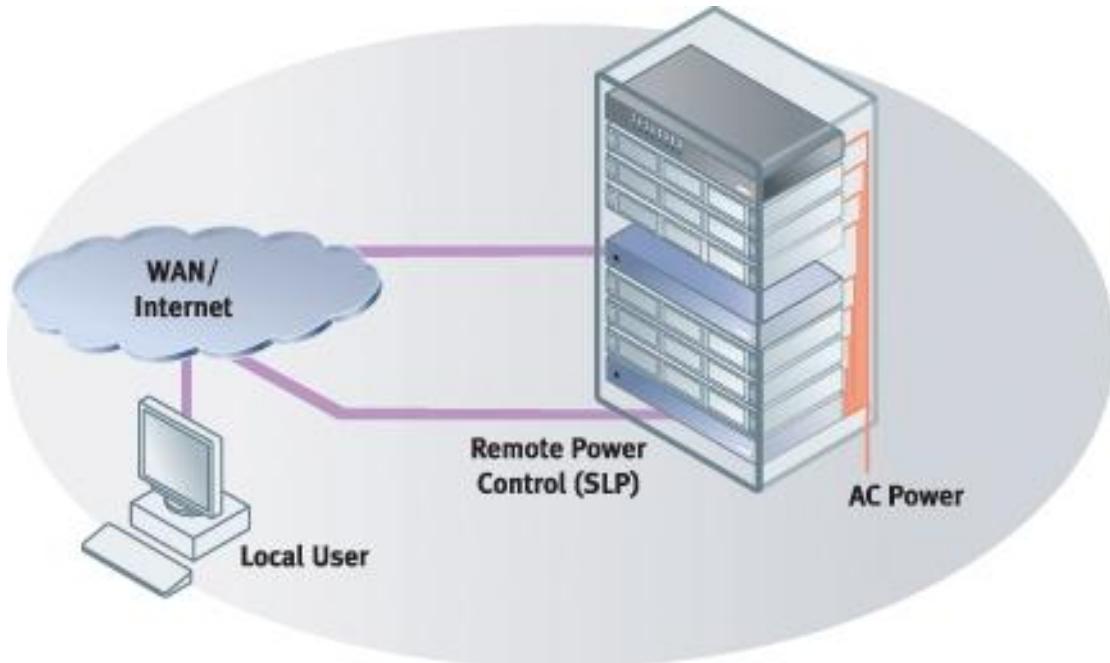
User Interface

There are typically two types of user interfaces that need to be supported. A graphical user interface (GUI) allows an operator to control individual power modules directly. The command line interface (CLI) allows script files to be constructed and sent directly for execution. Remote Power Managers execute response codes after each command.

Communications Interface Support

Network control hardware such as routers, DSU/CSU, network servers and uninterruptible power supplies require In-Band management. For remote access to critical network hardware, SNMP management, IP-based management tools and other In-Band management approaches are needed. But when the network in a remote location is not functioning, SNMP and In-Band management tools are of no use. A good alternative to sending a technician on-site is to install an Out-of-Band management system.

Out-of-Band management provides dial up access to the RS-232 console or AUX ports on network control hardware. With this access, systems administrators can communicate with routers, DSU/CSU, file servers, or any other network hardware equipped with an asynchronous RS-232 control port, with a modem and phone line.

Many internetworking devices have an RS-232 network management system ports. The ports permit users to upload new software and to update and inspect configuration tables. This conveniently allows an initial communication session to be established with the device's management port to perform a reboot. It also allows the same communications session to be switched giving the network administrator the ability to inspect or update the system's configuration table or to verify its operability.

In addition, new firmware releases or improvements can be uploaded to the device via File Transfer Protocol (FTP). This can easily be accomplished from anywhere including a remote facility with a standard web browser interface.

Furthermore, the device needs to support LAN communications with an Ethernet connection for In-Band communications. This can be accomplished with either a 10/100Base-T, TCP/IP or a SNMP connection.

Network management applications typically collect SNMP MIB information about internetworking devices including routers, hubs, bridges, concentrators, servers and switches. When an alarm is issued for a specific SNMP managed device, the network management application can send specific commands to a Remote Power Management device that is TCP/IP addressable.

Security

Direct TCP/IP access to each Remote Power Management device on the network is the fastest and most direct method to reboot an individual server or router, but also presents the greatest security risk to the network. Non-secure network traffic can be penetrated and sensitive information, such as usernames and passwords, can be intercepted.

To prevent such an attack, the Remote Power Manager solution must provide encrypted security solutions for network traffic. True access security is provided only when utilizing one of the commonly used security protocols, such as SSLv3 and SSHv2 security protocols. SSH and SSL represent the strongest security protocols available for communicating and managing a Remote Power Management device via TCP/IP network. Both of these protocols provide for the strongest encryption of the entire session.

SSL: Securing Web GUI Sessions

An SSL-secured HTTPS interface ensures sensitive information such as user accounts and passwords are protected from outside observers. 128-bit SSL key enables users to verify a device's authenticity and communicate with it securely, which protects confidential information from interception and hacking.

SSH: Secure Remote Terminal Sessions

Secure Socket Shell (SSH) is a command interface and protocol for securely accessing a remote computer. SSH provides strong encryption, robust authentication and data integrity. Use of SSH virtually eliminates the risk in remote management as all session data is encrypted using strong ciphers with keys exchanged dynamically using RSA/DSA public key algorithms. SSH is intended as a replacement for telnet among other protocols.

Secure Shell protects against:

- IP spoofing, where a remote host sends out packets, which pretend to come from another trusted host.
- IP source routing, where a host can pretend that an IP packet comes from another trusted host.
- DNS spoofing, where an attacker forges name server records.
- Interception of clear text passwords and other data by intermediate hosts.
- Manipulation of data by people in control of intermediate hosts.

Console Ports: Secure Communication through SSH

Using an SSH connection to securely connect to the serial console port of an attached data center device allows users to aggregate the serial console ports for several devices into the one SSH connection. For instance, by launching an SSH session directly to the serial console port of a Unix server through a Remote Power Manager connection, the network manager accesses the Command Line Interface (CLI) of the server itself.

Active Directory

There are many management tasks businesses face with the deployment of large numbers of internetworking equipment. These tasks include network configuration settings (e.g. IP address), assigning usernames and passwords, distribution of access rights, security architecture, SNMP configuration and device specific settings. Not only does the configuration need to be setup initially, it must be updated on a periodic basis for security reasons.

Active Directory (AD) is a component of the Windows 2000 & 2003 Server architecture and it gives organizations a directory service designed for distributed computing environments. AD acts as a central repository for information, eliminating the redundancy of management tasks. For example, instead of changing a user's password in hundreds or thousands of individual devices, or changing it in multiple devices' management software, the change need only occur in one place – the directory. Active Directory supports multiple protocols for this purpose. The most common network protocol for accessing directory services access is the Lightweight Directory Access Protocol (LDAP).

Remote Power Management Solutions from Lantronix

SecureLinx™ SLP Remote Power Management products from Lantronix allow for the fast and easy recovery of locked-up devices. With an advanced feature set, a network operations center can immediately establish a communications session with an SLP Remote Power Manager to reboot a device and quickly return it to operational status. The individual on/off/reboot outlet control of the SLP Remote Power Manager allows re-booting of attached servers and data center equipment or the cycling of power to institute configuration changes. Everything service providers, hosting companies and businesses with distributed networks need to maximize network operations.

SLP Remote Power Managers uniquely combine both In-Band Ethernet and Out-of-Band serial management. This gives system administrators multiple options for hardware and software management and in establishing communications sessions. In addition, SNMP measurement traps help to extend network management capabilities and protect a company's investment in their internetworking devices. Plus, SLP's "power-up" sequencing of outputs prevents an in-rush current overload to the main circuit. Allowing a more steady power draw, power sequencing also provides the option to turn on certain devices before others, which can be a great benefit in networked data center equipment.

Providing the ability to remotely perform power measurement verification, SecureLinx SLP Remote Power Managers allow for the safe loading of existing power circuits and capacity management to know when to additional power circuits are needed. This real-time power measurement feature also helps service providers and business determine when more equipment can be added onto existing power circuits resulting in the optimization of equipment resources.
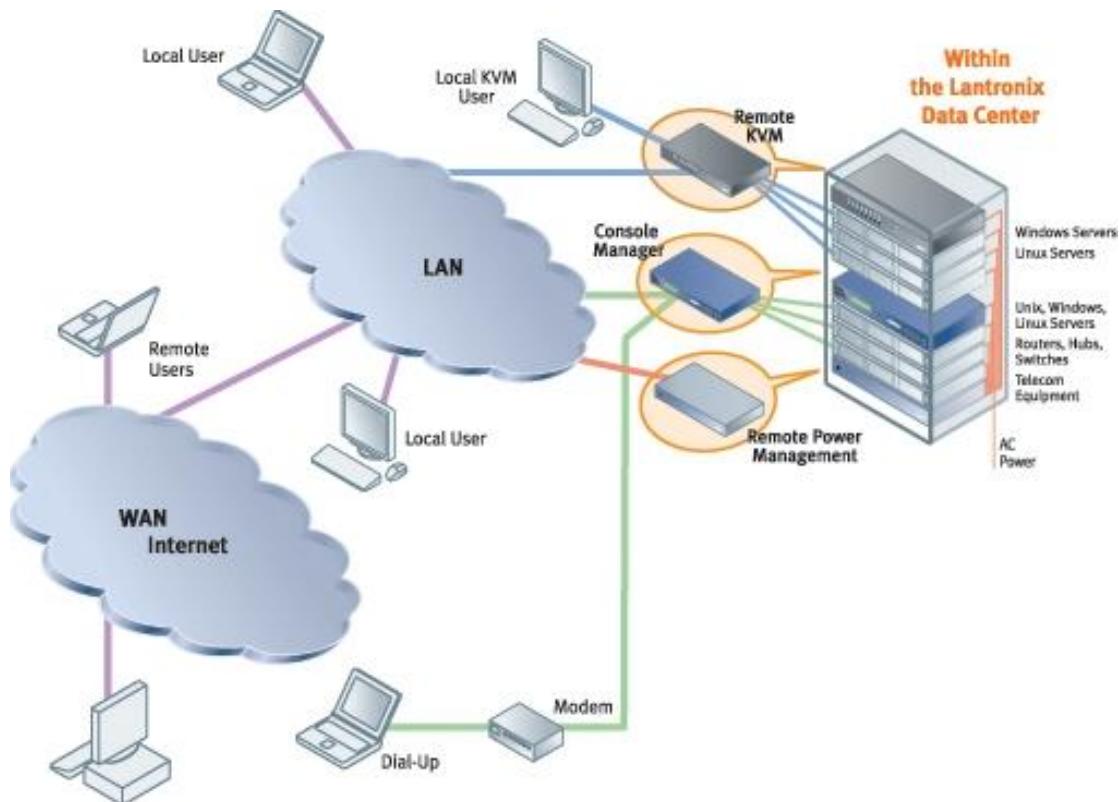
Lantronix also offers an unparalleled level of security. Utilizing both SSH for the command line interface (CLI) and SSL for web access, these security protocols provide the strongest encryption available. The products feature an SSL Certificate for device verification and a directly integrated SSH Ethernet interface. Lantronix also includes support for Active Directory in order to remotely secure user authentication, and simplify management of users.

Additional features provided by Lantronix's SLP include environmental monitoring and remote firmware upgrades. Optional temperature and humidity sensors allow remote monitoring of key environmental conditions. Plus, new firmware improvements and releases can easily be uploaded via FTP with a standard web browser interface.

Lantronix Advanced Feature Set

- Individual On/Off/Reboot and group control of receptacles
- Local access via RS-232 serial port
- Remote access via TCP/IP (web browser or SSH)

- Access control list for user authorization
- Active Directory (LDAP) for remote user authentication
- SNMP MIBs and traps supported for integration with enterprise systems
- Line current monitoring, with built-in display
- Receptacle status retained after power loss
- LED outlet status indicators
- 1U 19" rack mount or Zero-U form factors
- 100-120 VAC 30 Amp, and 208-240 VAC 20 Amp capacity

Glossary

The following table identifies the technical terms used in this paper.

Authentication	The process of identifying an individual usually based on a username and password. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.
Authorization	The process of granting or denying access to a network resource. Most computer security systems are based on a 2-step process. The first stage is authentication (described above). The second stage is authorization, which allows the user access to various resources based on the user's identity.
Lightweight Directory Access Protocol (LDAP)	A software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network.
Network Attached Storage (NAS)	A server that is dedicated to file sharing. NAS allows more hard disk storage space to be added to a network that already utilizes servers without shutting them down for maintenance and upgrades. With a NAS device, storage is not an integral part of the server. Instead, the server handles all of the processing of data but a NAS device delivers the data to the user. A NAS device does not need to be located within the server but can exist anywhere in a LAN and can be made up of multiple networked NAS devices.
SSH v1	SSH v1 is based on the V1.5 protocol and 1.3.7 F-Secure code base. It is incompatible with SSH v2, but can coexist on an SSH-capable device.
SSH v2	SSH v2 is based on the V2 protocol and the F-Secure 3.1.0 code base. SSH v2 is generally regarded to be more secure than SSH v1. It is incompatible with SSH v1, but can coexist on an SSH-capable device.

Storage Area Network (SAN)	A high-speed subnetwork of shared storage devices. A SAN's architecture works in a way that makes all storage devices available to all servers on a LAN or WAN. As more storage devices are added to a SAN, they too will be accessible from any server in the larger network. In this case, the server merely acts as a pathway between the end user and the stored data.
Telnet	A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects it to a server on the network. You can then enter commands through the Telnet program, which are executed as if you were entering them directly on the device console. This enables you to control the device and communicate with other devices on the network. To start a Telnet session, you log into a server by entering a valid username and password.