

Computer Power Management for Enterprises

A Practical Guide for Saving up to \$100 per Seat Annually in Electricity

David Korn & Robert Huang
The Cadmus Group, Inc.
Watertown, MA United States
dkorn@cadmusgroup.com
rhuang@cadmusgroup.com

Thomas Bolioli
Terra Novum
Watertown, MA United States
tbolioli@terranovum.com

Mike Walker
Beacon Consultants Network Inc.
Boston, MA United States
mwalker@beaconconsultants.com

Abstract— While the use of monitor power management features has become fairly widespread in the United States, relatively few enterprises utilize computer power management (CPM) features—also known as computer “sleep settings.” Since activating CPM features in desktop and notebook operating systems can save up to \$50 per computer annually (and up to \$100 per computer where monitor sleep settings aren’t already in use), we set out to understand the most common barriers to the use CPM features in enterprise IT environments. Our goal was to develop a set of practical instructions for overcoming technical and other hurdles that stand in the way of their widespread adoption. We first confirmed that the core challenge lay in making CPM compatible with regular computer maintenance tasks – specifically, the periodic delivery of software updates and security patches. IT administrators were concerned that sleeping computers might interfere with these important maintenance events. We subsequently focused our research on developing a set of solutions for maintaining sleep-enabled computers. This paper offers practical guidance for IT managers who want to realize the full energy savings potential of CPM features, without compromising a well-maintained and secure IT environment.

Keywords- energy conservation, computer power management, WOL, EPA ENERGY STAR

I. INTRODUCTION

Traditionally, IT administrators considered power consumption an unavoidable cost of doing business -- something only facilities managers worried about. But power consumption is increasingly becoming IT’s problem. According to AFCOM’s 2005 survey of its members, data center power requirements are increasing an average of 8% per year. Power requirements of the top 10% of data centers are growing at over 20% [1]. Rising energy costs aren’t limited to data centers. Enterprises are increasingly leaving desktop computers powered 24 hours a day so that network administrators can access them immediately with software updates and security patches. In extensive interviews, we have confirmed that at least half (and most likely a far higher percentage) of PCs used by enterprises are left on continuously. Compounding the problem is the fact that new computers typically consume twice the energy of older models, thanks to faster processors and video cards. For example, a Dell Optiplex PC from 3 years ago used 35 watts compared to 70 watts today [2].

So what are IT managers to do? Many of the reasons IT power demands are increasing -- more powerful processors,

higher densities of servers and switches, rising cooling demands – are difficult to address in the short-term. But there are two often-overlooked energy-saving tools already hanging on the IT manager’s tool belt: computer and monitor power management features. Standard in Windows 95, 98, ME, 2000, and XP as well as Mac OS and Linux, these features allow computers (hard drive, CPU, etc.) and monitors to enter a low-power “sleep” mode when inactive to save energy and money. A simple touch of the mouse or keyboard “wakes” the computer and/or monitor within seconds. Since computers use 60 to 90 watts when active and only 2 to 3 watts in sleep mode, activating computer power management (CPM) features can save up to \$50 per computer annually – and up to \$100 per computer where monitor sleep settings aren’t already in use.

A. Problem Addressed

For years, EPA’s ENERGY STAR® program has successfully promoted the activation of monitor sleep features, and their use has become widespread. However, power management of the computer has lagged far behind that of the monitor. In fact, relatively few enterprises have activated CPM features. The primary reasons were documented in our May 2004 paper entitled “Power Management of Computers: \$ 1.5 Billion in Potential Energy Savings Annually,” presented at the 2004 IEEE International Symposium on Electronics and the Environment in Scottsdale, AZ. These reasons include:

- No convenient way to centrally manage power management settings on groups of desktops and notebooks
- Issues with CPM in networked environments, including potential conflicts with regular software updates and security patches
- Past reliability issues associated with CPM features
- Compatibility problems with certain software
- Lack of awareness and misconceptions about CPM among end-users.

This paper will describe how enterprises have made substantial progress in addressing these barriers in just a few short years. Their motivation is easy to understand. EPA estimates that the nationwide savings available if all computers had power management activated is approximately 25 billion kWh, equivalent to:

- \$1.8 billion in energy bills
- Enough electricity to light all the homes in CA and NY
- Preventing 18 million tons of greenhouse gas emissions.

B. *Prior Work in this Area*

While IT industry leaders are very much focused on how CPM might be improved in future hardware and software releases, it will take many years for these improvements to reach critical mass. We were interested in understanding how computer sleep might be made to work in today's enterprise IT environments. One of our conclusions – confirmed through numerous conversations with IT industry leaders – was that no one had systematically investigated and documented how these obstacles to CPM might be addressed by IT managers in the field.

C. *Project Undertaken*

With \$1.8 billion in potential energy savings at stake, we set out to understand how IT managers are overcoming the obstacles to enterprise CPM. Our goal was to develop specific tools and guidelines for successfully utilizing CPM features in common enterprise IT environments. We hoped to eventually hand IT managers a set of keys for unlocking \$10-100 in annual energy savings per computer.

II. RESEARCH METHODS

Our research began with a national search for organizations that had attempted to implement computer sleep features. Through subsequent interviews and site visits with corporate, government, and nonprofit IT managers, we documented the various ways that CPM was or was not working. To help expand the number of organizations utilizing computer sleep settings, we developed a simple, convenient software tool (called EZ GPO) that allowed IT managers in certain environments to activate and manage computer sleep features on groups of computers. By early fall, 2005, we were armed with case studies from a variety of IT environments, each documenting technical challenges to power management implementation. One of the biggest barriers to the widespread use of computer sleep features in enterprises could be summed up by the following question: How can sleeping computers become available to receive urgent software updates and security patches? In general, sleeping computers are not available for software updates and security patches until a user wakes them up.

In October 2005, we set up a test network with the goal of better understanding common barriers to computer power management in enterprises, and to develop a set of practical instructions for working around them. Since an exhaustive examination of computer sleep settings on the universe of available computer hardware, software, and network environments would be impractical, we focused our research on the most common computing platforms and environments seen in today's enterprises. First, we examined how several of the most commonly utilized desktop management tools might be used to activate sleep settings. Next, we tested a variety of

methods for delivering urgent software patches to sleeping computers. Finally, we examined common difficulties or bugs we had observed in the field, in hopes of developing solutions or workarounds.

III. FINDINGS

This paper offers practical guidance for IT managers, a basic “how to” primer to help enterprises realize the full power saving potential of CPM features. For the purposes of this paper, CPM includes activating the existing Windows capabilities of system standby and/or hibernation, but not “turn off hard disks,” a feature that saves only a modest amount of power. For a complete overview of CPM, please go to www.energystar.gov/powermanagement.

A. *Central Management of Power Management Settings*

CPM features cannot be centrally managed via common methods such as registry pushes and group policy. This served as a major barrier to their use in enterprises – until recently. Several tools now fill this gap, some open source and some commercial, allowing network administrators to centrally manage computer sleep settings. They are:

- Apple's OS X Tiger and Remote Desktop 2
- Desktop Standard's Policy Maker
- ENERGY STAR EZ GPO
- Verdiem's Surveyor

For complete instructions on the use of these and other tools, please visit www.energystar.gov/powermanagement.

B. *Computer Power Management: Avoiding Conflicts with Regular Software Updates and Security Patches*

A computer can't run software patches and security updates while in sleep mode. Consequently, enterprises need to ensure that activating CPM does not interfere with updating and maintaining their networks. Overcoming this challenge is the foremost concern of most network administrators and, consequently, the primary thrust of this paper.

In general, network administrators update, or “patch,” client PC software using one of three basic network management scenarios – opportunistic, scheduled, or on-demand. Opportunistic updates occur whenever the machine becomes available (e.g., logs onto the network). Scheduled updates automatically occur at a pre-set time. On-demand updates are network administrator-initiated and, by definition, take place immediately. Described below are instructions and tips for using Systems Management Server (SMS) and Windows Server Update Services (WSUS) to keep PCs maintained and secure in a CPM-enabled environment – under each of these three patching scenarios. This guidance should hold true for most other managed IT environments as well.

1) *Opportunistic Patching and Maintenance – Ideal for CPM*

Opportunistic maintenance refers to patching and updating that occurs as soon as a computer becomes available on the network. A sleeping computer, like an “off” computer, is not

available for updates. In a CPM-enabled environment, patches and maintenance are not guaranteed to occur at a particular time but rather occur when the computer wakes. Therefore, opportunistic patching does not require ANY additional configuration and management to run effectively in a CPM-enabled environment. When services such as WSUS, Norton Anti Virus and other client driven update services are running in conjunction with a sleeping, network disconnected, or “off” computer, the next time the machine is turned on or connected to a network, these services will force a check-in and catch-up to where they should be with software updates.

However, CPM can potentially impact the network load balancing features of SMS, WSUS and other network services. In automated software delivery, there are three generic steps in a successful installation – advertisement, distribution and installation/restart – and there are randomly generated waiting periods (or “offset periods”) associated with these steps. (SMS has two waiting periods, but in WSUS and most others the distribution and installation steps are combined, so only one offset period exists). These offset periods help distribute the network traffic associated with software delivery over time, thereby balancing network loads. If the offsets are short (e.g., less than 2 hours) then all three delivery steps typically occur when the end user wakes a computer, since the offset periods have usually been exceeded. Assuming a 9-5 work day, a network administrator should expect to see a shift in network loads towards the morning (when machines would be awakened or powered up by users) and away from uniform distribution throughout the day.

Since offset times are configurable in SMS, WSUS, and others, network administrators may want to set them sufficiently high if network traffic issues are a concern. This will ensure that load balancing is preserved and the impact on client installations is not as pronounced. For example, consider setting the SMS offset periods to 22 hours (the installed default) instead of 2 hours. This will ensure that the offset feature continues to help balance network loads, even if a client computer is asleep for 12+ hours over night.

2) *Scheduled Updates – Use Scheduled Wake-ups to Make Them CPM-Compatible*

Windows Task Scheduler (set through the OS) can awaken sleeping computers for updates. Relatively easy to deploy and manage, scheduled tasks are a middle ground between on-demand updates, which generally require 24/7 availability of client computers, and opportunistic updates, which allow end users to turn off machines and receive updates at check-in. Scheduled tasks use the real time clock (RTC) and power management events (PMEs) provided by the Advanced Configuration and Power Interface (ACPI) to raise the machine out of system standby or hibernation. At the settings tab of a scheduled task, an option labeled “Wake the machine to run this task” will set a PME inside the RTC for the time when the task is scheduled to run. (See Figure 1.)



Figure 1. Windows Task Scheduler

While scheduling a wake-up on an individual PC is fairly simple, creating and enabling scheduled wake-ups across a network requires the use of a third-party desktop management tool or Active Directory managed and distributed scripts, even in Windows Server 2003. Dameware Utilities, Desktop Standard’s Policy Maker, and Verdiem’s Surveyor are three such third party network management tools.

- Dameware Utilities can remotely install and manage scheduled tasks through remote procedure call (RPC) and remote administration of client machines. See www.dameware.com/products/dntu/.
- Desktop Standard’s Policy Maker can distribute and update tasks via Group Policy. It uses scheduled tasks to wake up the machine at a predetermined time, force a Group Policy object that turns off standby or hibernate, conduct automatic updates/patches, and force another Group Policy object to re-establish standby or hibernate. See www.desktopstandard.com/quickguides/power.aspx.
- Verdiem’s Surveyor provides a simplified, network-level management interface for the power functions of networked PCs. It can ensure that every PC is awake and ready for after-hours remote back-up jobs or software upgrades, and it also details your energy and cost savings with built-in reporting. See www.verdiem.com/.

Alternatively, network administrators can centrally manage scheduled tasks via a scheduled task file (*.job located in the windows\tasks directory). This involves the following steps:

- 1) Develop a batch file to actually run in this scheduled task. For SMS, as an example, the batch file could contain the following command “WUAUCLT /detectnow” to force a check-in and start the process for any unprocessed

automated installs. In theory though, any number of maintenance tasks can be run from within the batch file, either individually or one after the other.

- 2) Create a scheduled task with the batch file by copying the scheduled task, created on one machine, into the %WINDOWS%\tasks directory on each of the clients on the network.
- 3) Modify the scheduled task file through a batch file in order to gain authentication credentials. The scheduled task file loses its authentication credentials and will run under the SYSTEM ac-count, instead of under a particular user account. In order to correct this, new credentials must be placed into the file. An example batch file to accomplish this is:

```
@echo off
copy \\machine\share\wake.job c:\windows\tasks
schtasks /change /RU domain\UserName /RP
PasswordHere /TN wake [3]
```

3) *On-demand Updates – Use Wake-On-LAN to Make Them CPM-Compatible*

Wake on LAN (WOL) is a Layer 2-based means for waking up machines from sleep states such as system standby, hibernate and shutdown – and for remote access to them [4]. With WOL activated, a network administrator can wake up sleeping machines at any time in order to perform on-demand patches or updates. The WOL setting, tied to the network interface card (NIC) driver, is activated by selecting the appropriate options on the network adapter power management properties located in the device manager. On the power management tab select “Allow this device to bring the computer out of standby” and “Allow only management workstations.” These settings enable WOL but limit the packet types to those that are intended specifically for this machine. These so called “magic packets” have the Media Access Control (MAC) address embedded in them.

a) *Activating WOL Across the Network*

WOL activation across all computers on the network requires careful planning and preparation. WOL is typically not activated by default on PCs. In addition, WOL is not easily activated organization-wide because one cannot use Group Policy, or related techniques, to centrally enable WOL on machines that have already been deployed unless the client machines are clones of each other. Ideally, network administrators should activate the WOL function before deployment by making WOL part of their template client software image.

Post deployment activation of WOL can be difficult because NIC cards cannot be identified in the registry beyond just a general location. This situation is mitigated where the client machines are built from a master image(s). In such cases, the network administrator must: 1) have the machines organized into groups based on a series of standardized hardware configurations, each with its own hardware specific image; 2) examine the NIC cards for each group and determine the appropriate registry entries for activating WOL. If these

prerequisites can be met, one could either push out a registry key or enable WOL via Symantec Ghost.

b) *WOL at the Registry Level*

The registry value labeled PNPCapabilities is set to a particular DWord value in the settings hive for the network adaptor. (Disabled is decimal 38 while both WOL options on is decimal 288.) This is located at...

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl
Set\Control\Class\{4D36E972-E325-11CE-BFC1-
08002bE10318}\000x]
```

...where x represents the network adaptor device number. Typically x is 0 or 1 but it could be any number. This is where the use of hardware specific images greatly eases management headaches. With a hardware specific image, this device number will be standard across an entire population of computers. The following instructions provide one example for pushing out a registry key in order to activate WOL:

- 1) Create a registry key in the registry of your local machine
- 2) Enter all of the values needed
- 3) Export the registry key to a reg file, editing paths/content if necessary
- 4) Place the exported reg file on a server share that is accessible by the users and/or machine accounts you plan on having this reg file applied to.
- 5) Create a batch or vbs file, to be used as a startup/login script, with at least the following command: regedit /s \\server\path to reg file\file.reg
- 6) Place this batch file on the same share created earlier.
- 7) Open or create a group policy on an OU that contains the users/computers you want to apply the registry settings to.
- 8) Edit the Policy and go to either “Computer Configuration” or “User Configuration” depending on where the registry file will be applied to.
- 9) Then edit Windows\Scripts (this is labeled Startup/Shutdown for computers and Login/Logout for users).
- 10) Add the new script to the list by navigating to the script using its UNC name (\\Server\path-to-script).
- 11) Say OK. Close out and test it by restarting or logging in.

For additional information see:

- <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kmag01/html/DistributingRegistryChanges.asp>
- <http://support.microsoft.com/?kbid=310516>
- <http://techsupt.winbatch.com/TS/T000001048F90.html>
- <http://www.windowsitlibrary.com/Content/314/1.html>

On more complex networks, routers and firewalls must be reconfigured to ensure that the broadcast packets can travel from one subnet to another while simultaneously ensuring that only authorized entities can send those packets. Although not Internet Protocol (IP) based per se, WOL is capable of using IP broadcast User Datagram Protocol (UDP) packets that encapsulate “magic packets”. This makes writing a WOL tool to wake up machines easy and portable.

c) *Utilizing Symantec Ghost Solution Suite to enable WOL*

Symantec Ghost Solution Suite is an enterprise level client imaging solution that can centrally manage WOL settings on client machines. Ghost re-images machines and allows for small post-deployment tweaks of machines loaded with that image. Armed with the registry key information detailed above, network administrators can use AI Builder to distribute a registry modification. For example:

- 1) Open AIBuilder and navigate to the Registry entry of the SYSTEM CHANGES menu.
- 2) Enter:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\000x
```

in the Key Name section where x represents the network adaptor device number as found in the master machine for that group of machines.
- 3) Choose new as the action.
- 4) Choose “Add Value” and edit it to replace a DWORD labeled “PNPCapabilities” with a data value of 288.
- 5) Save this and run it using Enterprise Manager as a task.

Ghost can do more than simply enable WOL. Because Ghost has integrated WOL capabilities into everyday functions, any Ghost task can utilize WOL to wake the machine, thereby ensuring that the task runs at the proscribed time.

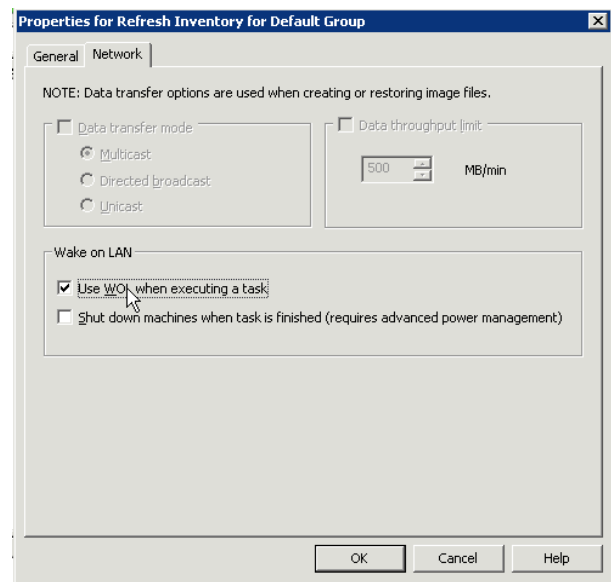


Figure 2. Utilizing WOL within Symantec Ghost

d) *Waking Up Machines Once WOL Is Activated*

To wake up a machine, a packet, commonly referred to as a “magic packet,” is sent to the broadcast port on an Ethernet based network. Remote wakeup can be initiated by a variety of packets. Magic packets are Ethernet based (using IP broadcast): client machines look for packets with their NIC’s specific Media Access Control (MAC) address, and ignore anything that does not resemble a known wakeup packet. The packet data tells each properly configured Network Interface Card (NIC) to fire off a PME through the Peripheral Component Interconnect (PCI) bus in order to bring the machine out of its sleep state. Two options for waking up machines are described below.

Scripts for Sending WOL Packets. Any number of network management or stand-alone programs can send WOL packets, and many are available for free on the Internet. Network administrators can then write a simple script or download one from the internet in order to build a solution for waking up remote machines either on a timer or on demand [5]. The data obtained by SMS in its asset discovery can be used to build a list of computer MAC addresses. This information is stored in Active Directory and can be retrieved via LDAP from within vb script or other means.

SMS Wakeup. Although SMS 2003 lacks a means for waking up machines, a plug-in from IE, Inc., called SMSWakeup, provides this functionality. SMSWakeup integrates with SMS and uses data from the SMS asset collection to obtain MAC addresses for each client computer. Once SMS posts an advertisement, SMSWakeup wakes the targeted computers, which then check in and act accordingly. For a small, single-subnet network, the default settings on SMS Wakeup are adequate. For more complex networks, SMSWakeup provides slave agents which will act as proxies for the server and wake up machines from the subnet, eliminating the need for broadcast address routing and firewall rules.

C. Other Barriers to CPM

1) Past Reliability Issues

Compatibility issues between hardware and software led to reliability problems in early versions of Windows CPM. This occasionally resulted in Windows 95 and 98 computers failing to wake properly from sleep, for instance. Unfortunately, some IT administrators remain reluctant to implement CPM to this day, based on their initial experience with CPM five to ten years ago. In reality, CPM works very consistently and reliably on recent hardware (Pentium 4 and higher) running Windows 2000 and XP. The experiences of GE, numerous colleges, and other leading organizations underscore this point. To date, EPA technical contractors have worked with dozens of organizations to implement CPM on more than 140,000 computers. They have encountered no significant reliability issues.

2) Lack of Awareness and Misconceptions Among End-users

Reliability issues aside, end-users did not appreciate the 10-30 second wait associated with waking a sleeping PC in the “early days” of CPM (e.g., Windows 95 and 98). Some implementations added an additional delay by requiring users to log back into their network.

Today, however, CPM features resume far more quickly from sleep mode. Because waking the computer takes only a few seconds, CPM no longer adversely affects the user experience. In fact, many users prefer it to booting up the machine each morning. Network connections typically re-establish themselves automatically, but network administrators can add an additional level of security by requiring a user-password upon resume. Whereas end users once viewed such measures as bothersome, the vast majority have come to appreciate the importance of client-level security.

Our experience indicates that users typically embrace power management when they understand that they are saving money and preventing pollution by using these features. We recommend that you inform employees about power management settings prior to activating them. Including information on the economic and environmental benefits can secure their full support. To calculate these benefits, please visit the ENERGY STAR program’s online calculator at www.energystar.gov/powermanagement.

3) Compatibility Problems with Certain Software

Windows certification requires software to handle sleep transitions appropriately. However, some hardware drivers and software applications (particularly older, proprietary applications commonly found in state and local government) do not handle CPM well. In some instances this can result in lost data; in other cases it simply prevents PCs from sleeping. Certain types of screensavers, for example, keep the CPU at a high level of activity, preventing the PC Box from entering sleep mode and needlessly burning energy. Fortunately such cases are increasingly rare, as the rise of mobile computing has demanded that applications perform flawlessly on power-managed platforms. While compatibility problems are not common in typical office environments, CPM should be thoroughly tested on each image prior to rollout.

IV. CONCLUSIONS

We are pleased to conclude that CPM features can work quite well in many common IT settings — saving energy, money, and helping to protect the environment. US EPA offers free technical assistance to organizations interested in activating CPM features. For more information, see www.energystar.gov/powermanagement.

- [1] Matt Stansbuerry, IT Energy Crisis Reaching Critical Mass, SearchDataCenter.com, 24 Oct 2005.
- [2] Lab testing, The Cadmus Group, 2005.
- [3] Notice on the last line that the password for the username is required to properly authenticate the scheduled task. This can be implemented relatively securely by: 1) ensuring that the batch file share is readable only by the Computer OU (as opposed to the Users OU); 2) making the batch file readable only by the members of that OU; 3) having the computer account, as opposed to the users, run the batch file. In addition an administrator could create a specific account for scheduled tasks and limit the types of logins to that account to ensure that if the tasks account is compromised, an attacker will not be able to utilize the login credentials for remote access to the network.
- [4] Layer 2, also known as the physical layer, is most typically Ethernet but could be token ring, etc.
- [5] See a list at <http://pages.towson.edu/aczech/magicpkt>.