

# Preventing Data Corruption in the Event of an Extended Power Outage

By Ted Ives

**White Paper #10**

**APC**<sup>®</sup>  
Legendary Reliability<sup>®</sup>

**Revision 1**

## **Executive Summary**

**Despite advances in computer technology, power outages continue to be a major cause of PC and server downtime. Protecting computer systems with Uninterruptible Power Supply (UPS) hardware is part of a total solution, but power management software is also necessary to prevent data corruption after extended power outages. Various software configurations are discussed, and best practices aimed at ensuring uptime are presented.**

## Background

An extended power outage, which can strike at any time, can prevent unprotected computers from initiating their required shutdown procedure. PC and Server operating systems are not designed to support abrupt losses of power known as “hard” shutdowns, but rather rely on a set of built-in processes that prepare a computer for shut down such as saving memory, stopping applications and services, etc. Shutting down in this manner is often referred to a “graceful” shutdown. Hard shutdowns, on the other hand can result in lost or corrupted data and a lengthier time-to-recovery after power returns.

An Uninterruptible Power Supply (UPS) can protect the system from damaging power problems and improve server availability by allowing users to continue working without interruption during a short power outage. During an extended power outage, defined as any outage that might outlast the UPSs runtime, if the system is equipped with UPS shutdown software, it can communicate with the UPS and perform a graceful, unattended system shutdown before the UPS battery is exhausted.

## Introduction

There are many reasons for the occurrence of extended power outages, ranging from a local transformer failure due to lightning, or a regional power grid going offline. Steps must be taken to protect computer systems and the data they store from the corrupting effects of a hard shutdown. One cause of potential data corruption in the event of an extended power outage is abnormal termination of applications or the operating system while manipulating data. This can affect documents, critical file system structures (such as File Allocation Tables), or dynamic application data, and in many cases can also lead to increased “time-to-recovery” when power returns, as the operating system or application attempts to rebuild corrupted tables, etc.

Another cause of concern is with a computers hard drive. While progress has certainly been made in the industry over the last decade in hard drive technology to prevent “head crashes” (where the read/write head of the hard drive could actually damage the surface of the disk if not properly “parked”), another advance in hard drive technology has actually contributed to the likelihood of data corruption. To achieve high levels of performance, hard disk controllers are often designed to take advantage of caching techniques, which involve temporarily writing information to memory and then writing the data out to the actual disk later. In the event of a power loss, information in the cache is lost, leading to potential data file or data corruption.

One does not have to search extensively in business and government publications to see that, despite technological advances, data corruption due to power loss is still a widely recognized problem in the IT industry. This is **emphasized** in the industry quotes below:

“Even a moment’s disruption can have devastating effects on power sensitive customers such as internet service providers, data centers, wireless telecommunication networks, on-line traders, computer chip

manufacturers and medical research centers. For these customers, **power disruptions can result in data corruption**, burned circuit boards, component damage, file corruption and lost customers.

- "Electrical Power Interruption Cost Estimates for Individual Industries", Sectors, and U.S. Economy February 2002, U.S. Dept. of Energy Office of Power Technologies

**"Failure to boot after a power failure is generally caused by corrupted files** or a damaged hard disk

- neither of which Last Known Good Configuration is capable of repairing."

- "MCSE Microsoft® Windows® XP Professional Readiness Review

Exam 70-270, Section 70-270.04.03.002, 11/28/2001

"Total failures, or blackouts, constitute a complete loss of electrical power to the networking or computing equipment...these failures can cause system and network crashes, PC lockups, and **corruption or loss of valuable data** from servers and workstations."

- "Power Protection Basics", March 2002, Contingency Planning Management Magazine

**"The system and its data can become corrupt as a result of a power failure....a UPS can protect the system if power is lost. A UPS usually provides ...temporary power which may be enough to permit a graceful shutdown."**

- Special Publication 800-34 Contingency Planning Guide for Information Technology Systems

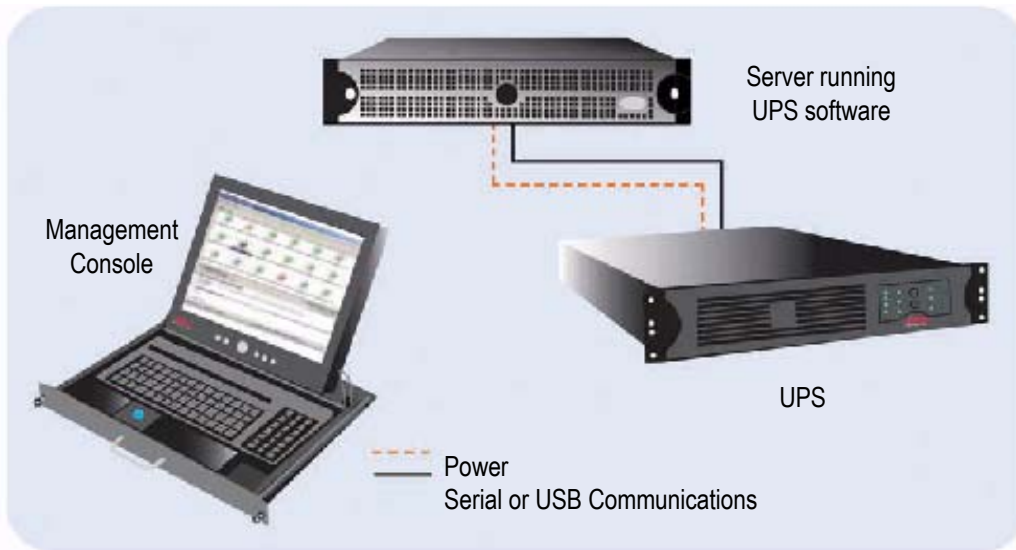
National Institute of Standards and Technology, June 2002

## Recommended Configurations for UPS Software

### Configuration 1: Protecting a single computer with a single UPS

In this configuration, each computer is backed up by its own UPS, and the UPS communicates with the computer over a serial or USB cable. UPS software is installed on the computer to provide graceful, unattended shutdown in the event of an extended power outage. In this case the UPS is managed locally by the connected computer. This is the simplest configuration and is widespread for both server and workstation deployments.

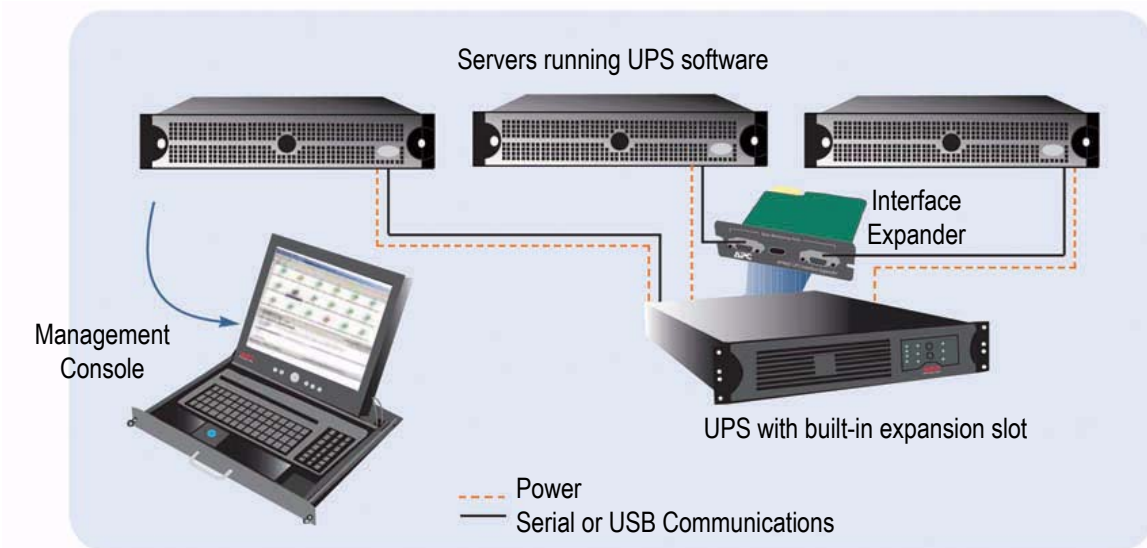
**Figure 1 – Protecting a single computer with a single UPS**



### Configuration 2: Protecting two to three computers with a single UPS

In this configuration, several computers are plugged into a larger UPS (typically one rated at 1500VA or higher). One computer will be connected directly to the serial port on the UPS, while the other two are connected to an expansion card installed in the UPS that provides two additional serial ports. In this situation, all three computers will have graceful shutdown capability, but management of the UPS is handled via the computer connected directly to the UPS. *Note that since the USB standard addresses communication with a single system only, USB connections cannot be used in this configuration.* Although this scheme can be extended to handle up to 24 computers (via daisy-chaining), APC does not recommend such an approach due to the additional cabling required.

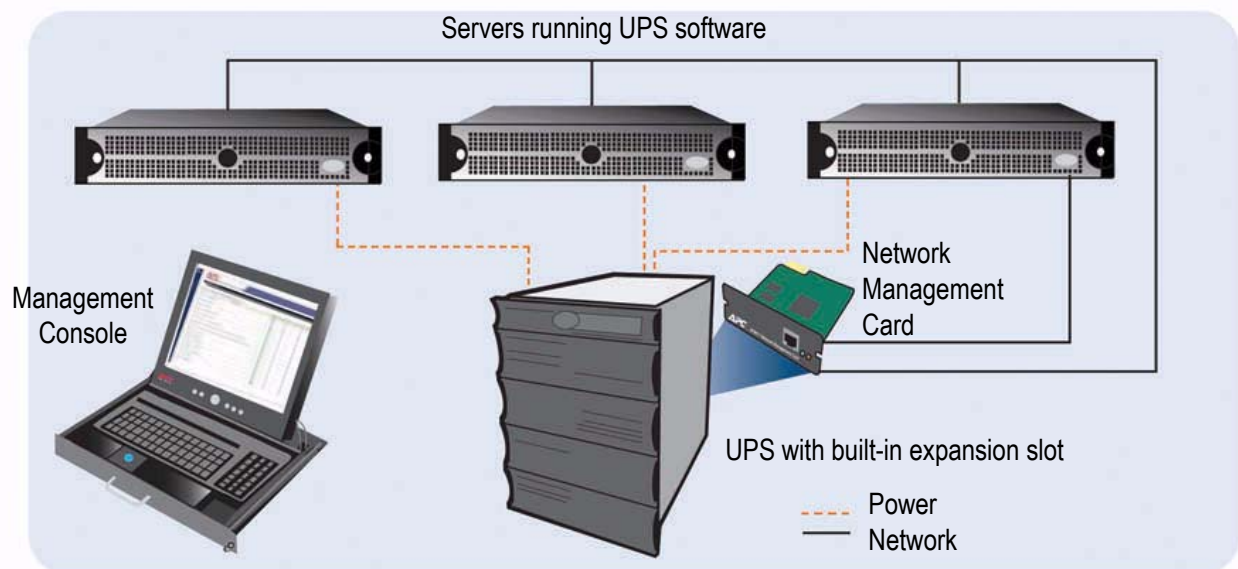
**Figure 2 – Protecting two to three computers with a single UPS**



### Configuration 3: Protecting three or more computers with a single UPS

An increasingly popular approach involves managing the UPS directly over an Ethernet network. A network management card (with a real-time operating system and hardware watchdog chip) installed in the UPS eliminates the requirement for server-based management. One example of such a configuration is the InfraStruXure architecture from APC which utilizes this approach. Software installed on the computers in this configuration need only encompass shutdown functionality since management capabilities are embedded in the UPS itself.

*Figure 3 – Protecting three or more computers with a single UP*



## Different Types of Operating System Shutdown

Modern operating systems such as Microsoft Windows® are increasingly including more advanced approaches to power management, including new methods of shutting down. Although these advances have largely been driven by laptop user requirements, selecting the right one for use with UPS software can decrease time-to-recovery after an extended power outage.

### Shutdown

This is the traditional method where the computers' Operating System receives a shutdown command from the UPS shutdown software and goes through a sequence of killing active processes before exiting. On a Windows® system for instance, this would bring the computer to the state where a message "You may now turn off your computer" appears.

## Shutdown and “off”

This is similar to the method above, but at the end of the process, the Operating System actually commands the Computer to turn off and it goes into a state where it no longer draws power. This can be a useful approach for Configuration 2 above - one computer can be shut down and turned off to lengthen the runtime of the remaining computers (this approach is sometimes referred to as “load shedding”). Shutdown and “off” capability sometimes requires a BIOS setting change to enable the “off” portion to occur.

## Hibernation

A Hibernation process (for instance, as found in Microsoft’s latest Windows® operating systems) is similar to the methods above, but some highly valuable additional steps are taken

1. First the computer’s desktop state including all open files and documents is saved. It does this by saving all of RAM to a large file on the hard disk.
2. Then the system is shutdown and powered off.
3. When power returns and the operating system boots up, the RAM is reloaded from the hard disk.
4. The desktop and all open files and applications are then presented as they appeared before the hibernation occurred.

This has a major advantage over the other methods of preserving both work in progress and the state of the machine before the shutdown occurred. For these reasons, APC strongly recommends customers consider selecting this method of shutdown for their UPS software.

## Standby

When a computer goes into “standby” mode, it is not turned completely off, but is placed into a low power state where certain components (monitor, I/O chips, etc.) are powered down. DRAM continues to be refreshed etc., and when the computer is taken out of “standby” mode, it typically reverts to the previous state very quickly. If you select a standby setting for your computer, it is important to make sure that the UPS you select can “wake” the system in the event of an extended power outage so a graceful shutdown can be initiated – otherwise the system may stay in standby state until the UPS is completely drained and then power to the system will be dropped (a “hard” shutdown).

# Best practices

## √ Purchase a UPS with extended runtime capability and/or a generator

The amount of standardized data on AC power reliability is limited. However, there are two significant surveys related to AC power reliability in the USA which have been done, one by AT&T Bell Labs and one by IBM. In addition, American Power Conversion has some experience by having approximately 8 million UPS systems installed, many of which are capable of logging power problems. In the USA, the data from surveys agrees with the experience of APC and shows the following essential points:

The average number of outages sufficient to cause IT system malfunction per year at a typical site is approximately 15:

- 90% of the outages are less than 5 minutes in duration (conversely, 10% are greater than 5 minutes)
- 99% of the outages are less than 1 hour in duration (conversely, 1% are greater than 1 hour)
- Total cumulative outage duration is approximately 100 minutes per year

This information is highly variable from site to site and in some geographic locations in the USA such as Florida the outage rate is an order of magnitude higher. Building specific problems can also raise the outage rate by as much as 3 orders of magnitude. This data is also believed to be representative of Japan and Western Europe.

Since 10% of outages are greater than 5 minutes and 1% are greater than one hour, purchasing a UPS with extended runtime capability and/or a generator merits serious consideration when the cost of downtime is high.

### √ **Protect the network equipment with UPSs**

Applications are only as available as the network that they are accessed through. Power Protection for Hubs, Routers, and Switches is an essential but sometimes overlooked ingredient in ensuring availability of applications. Additionally, if computers are running UPS shutdown software as in Configuration 3 above, the UPS shutdown software requires the network to be up during the power outage in order to communicate properly. If the network is unprotected, graceful shutdown of the computer will not be accomplished.

### √ **Accommodate each server's individual time requirement for shutdown**

The time required to properly shut down the operating system varies from system to system - some email servers with many accounts have been known to take upwards of 20 minutes to shut down for instance. Make sure the UPS software's settings take each of your computers' specific requirements into account and are set properly.

## **Conclusion**

Without shutdown software installed on the protected computer, the net effect of the UPS is simply to delay the inevitable. Regardless of which configuration, which best practices, and which particular UPS software is utilized, APC highly recommends customers not overlook this requirement – the small effort involved in installing and configuring such software can be well worth it in the event of an extended power outage that exceeds the runtime of the UPS.

## References

Monitoring of Computer Installations for power line disturbances, Allen and Segall, IBM, IEEE PES Winter conference, 1974.

*A study conducted from 1969 to 1970 using 38 monitor-months of data*

The Quality of US Commercial AC Power, Goldstein and Speranza, ATT Bell Labs, Intellec conference, 1982

*A study conducted from 1977 to 1979 at 24 sites around the US*

Power Quality Site Surveys: Facts, Fiction, and Fallacies, Martzloff, IEEE Transactions on Industry Applications, Vol 24, No 6

### About the Author:

**Ted Ives** is the Product Line Manager for Device Management at APC in West Kingston and is responsible for APC's Network Management Cards and PowerChute software products.