

Supporting the Alert Standards Format (ASF) 2.0 Specification

Preserve Your Investment... Stick with the Standard



September 2005



Executive Summary

Today's IT manager is under pressure to reduce the costs of maintaining the network and computing infrastructure. The typical enterprise employs a manageability software suite to facilitate this effort. However, software alone cannot solve all manageability challenges. In some cases, hardware-based manageability technology can provide additional capabilities. PCs based on a technology called Alert Standard Format (ASF) 2.0 can provide such functionality to the IT manager. ASF offers the following benefits:

- Reduces new PC provisioning time from 4.5 hours to 25 minutes (sample: 20 PCs)
- Makes software patching more secure and reliable
- Reduces costly desk-side visits by fixing common PC problems online
- Protects PCs from physical threats: theft, misplacement, and malfunction

Leading PC manufacturers such as Dell, HP, and Fujitsu-Siemens have already shipped nearly 75 million ASF-enabled PCs, and will continue offering ASF 2.0 in upcoming PC lines. These systems can be enabled and controlled using any manageability console that supports ASF 2.0.

What is ASF?

ASF is a standard created by the Distributed Management Task Force (DMTF). It is implemented in the PC's hardware and firmware, and is managed from a remote console. ASF provides robust management features that function while the PC does not have an operating system (OS) present.

When the OS is present in a client PC, much of its remote functionality is available using various tools. However, the client PC is often in an OS-absent state – either because the PC is turned off, has gone into a low power mode, or has hung during operation. As a result, the ability to remotely interact with a PC is severely limited. This is why ASF was created: to provide a suite of features that can be accessed remotely and while the PC does not have an OS present. These features fall into two categories:

- Alerting: a PC can alert a remote management console with - "I have a problem"
- Remote Control: a remote management console can control an OS-absent PC.

ASF serves as the conduit for a manageability infrastructure. The IT manager interacts directly with the management console, perhaps unaware of the underlying technology, or "plumbing", which enables the employed features (see Figure 1). Other options for the plumbing may exist, but ASF is the only one that is standards-based and widely deployed.

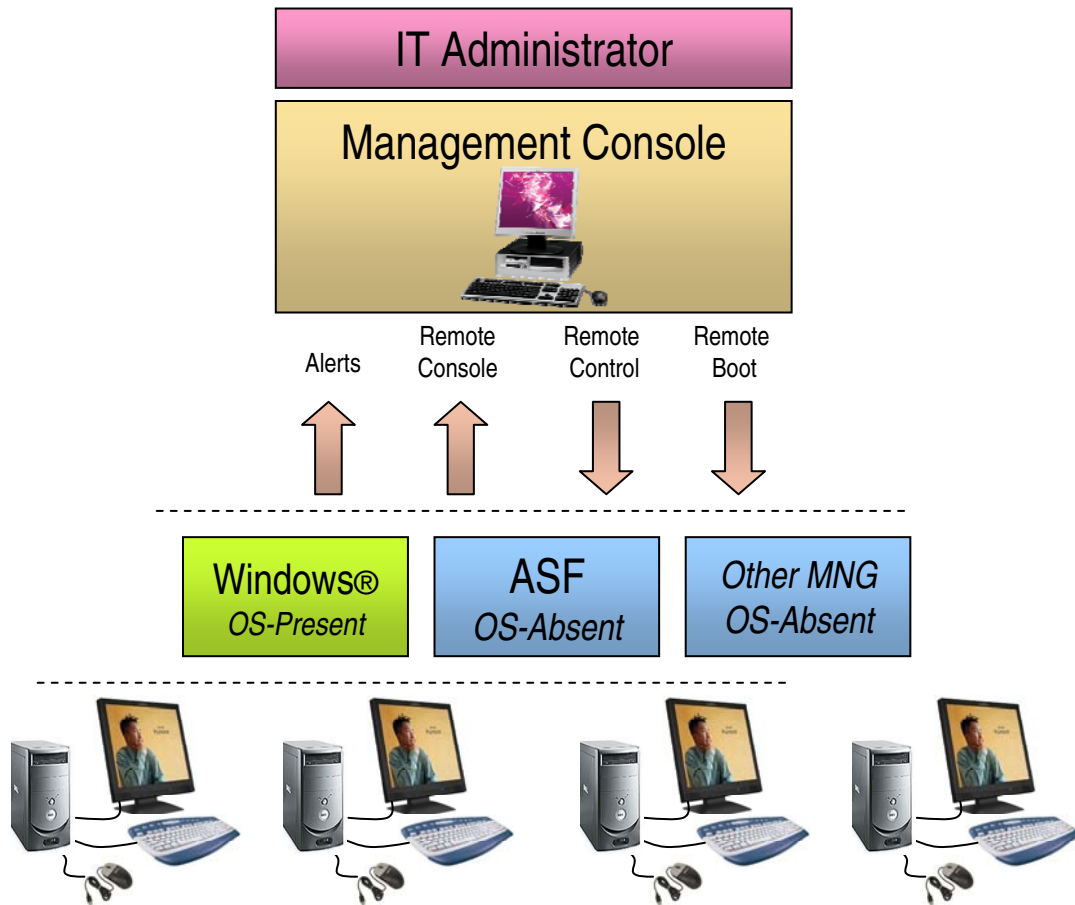


Figure 1: Client Management Components

The ASF Standard

The industry has long recognized the requirement for some type of OS-absent functionality. In the early 1990's, the first of several proprietary client manageability technologies was developed. Ultimately, the PC industry demanded a standards-based approach, thus giving rise to ASF.

The fact that ASF is standards-based is highly significant. Standards are the only way to ensure the key technology traits that IT demands.

They also provide the following benefits:

- **Interoperability:** most enterprise environments are heterogeneous – supporting PCs from multiple vendors, and using different manageability consoles. The only way to ensure out-of-the-box interoperability is for the technology to be based on a management standard that all vendors understand and test uniformly.
- **Security:** A truly effective security system follows a comprehensible paradigm and is open to industry scrutiny. Proprietary security solutions represent only one company's methodology to ensuring network integrity.
- **Choice:** IT managers want to base their hardware purchases on price-performance criteria; they do not want to be restricted by compliance with a proprietary or outdated scheme. Standards eliminate this problem.
- **Stability:** A standard is industry-driven, and modifications are typically subject to an open process that provides a buffer against arbitrary change. Proprietary systems can be altered subjectively by the owning company. This condition can only benefit the provider as the customer is then required to purchase an upgrade to take advantage of new changes and features.

ASF Installed Base

For IT to be willing to activate any manageability technology, a significant portion of the installed hardware infrastructure must support it. IT simply won't change their workflows to accommodate the new technology until it can be rolled out onto 50-75 percent of the enterprise's PCs. ASF solves this problem for IT because the vast majority of PCs sold by Tier 1 PC OEMs over the last three years contain ASF-enabled hardware. By the end of 2005, nearly 100 million PCs with ASF-enabled hardware will have been deployed. And this run rate is expected to continue through 2007 (see Figure 2).

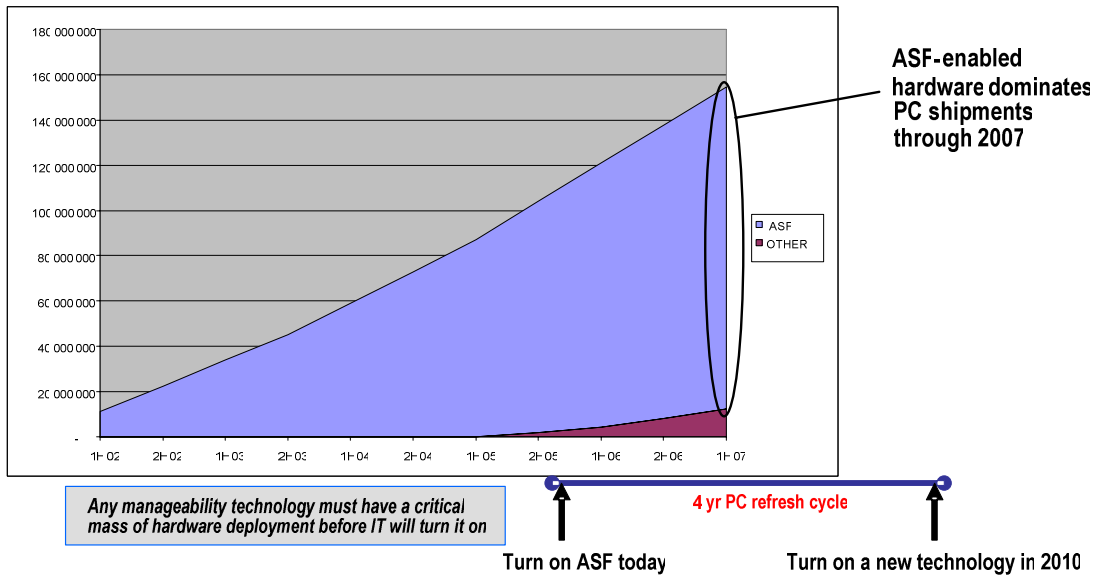


Figure 2: ASF Installed Base and Projected Shipments

Any new manageability technology would not enjoy the benefits of an installed base. Because the typical PC refresh cycle within the enterprise is four years, IT would not be able to turn it on until 2010. That is the benefit of ASF – it can be turned on today.

What Drives the Cost of the PC Infrastructure?

IT organizations have historically been reluctant to manage clients directly. This is surprising, given that the industry has long known the 'rule of thumb' for PC costs: 80 percent goes to managing the PC, while only 20 percent constitutes the cost of the hardware. However, using conventional IT tools, cost-effective management of client PCs is still difficult. Most enterprises simply rely on users to perform a reset (Ctrl-Alt-Del) or hard re-boot to solve typical problems.

With a perpetual focus on cost reduction, IT organizations need to scrutinize the true costs of managing PCs. PC management costs not only include resolving client issues (e.g. hung PCs, "blue screens", and boot problems) but also consist of deployment and regular maintenance costs. The following are recognized as key cost drivers in the computing infrastructure:

- Provisioning a new PC is a time consuming, manual process that can become highly serialized when large numbers of systems are involved. The critical nature of this manual task requires a skilled technician.
- Software patching can be unreliable due to limitations with Wake on LAN (WoL), a key technology used to push patches overnight to PCs that are off or in a sleep state.
- Desk-side visits are expensive since skilled IT technicians must be dispatched to the client site, even for easily diagnosed issues. User downtime is an added cost of desk-side visits as it often takes time for the technician to arrive and fix the problem.
- Physical threats to PCs can adversely impact users and increase IT support costs. Examples include stolen PCs, changed hardware configurations, and malfunctioning hardware.

Client Manageability Use Cases

The following sections detail typical use cases and demonstrate how IT managers can take advantage of their ASF-capable systems.

Use Case 1: Shortening PC Provisioning

When provisioning new systems, personnel typically must download a standard corporate image to the hard drive.

This work is performed by an IT technician on a provisioning bench. With the current methods, this is the process:

- All I/O (keyboard, mouse, and monitor) must be plugged into the new machine. Not only is this very time consuming, but the technician is also limited by space and the number of I/O peripherals available. The process is serialized.
- The PC is manually turned on by pressing the power button.
- The IT manager physically sits in front of the PC, monitors the boot process, and presses the "F8" key to prompt the boot option screen.
- The technician then boots to PXE and downloads the corporate image.
- PC is then manually shut down, and all I/O is manually detached.

This process can take up to 25 minutes per PC, assuming a typical image size. In contrast, ASF removes many of these manual steps:

- Plug in the LAN cable
- Use the management console to run the provisioning script. Using the power of ASF, the PC will automatically power on, change to a PXE boot option, download the image, and shut down. This occurs with no intervention by the technician.
- Unplug the LAN cable

Since ASF only requires a network connection to the new PC (no I/O connections), the process is run completely in parallel fashion (see Figure 3).

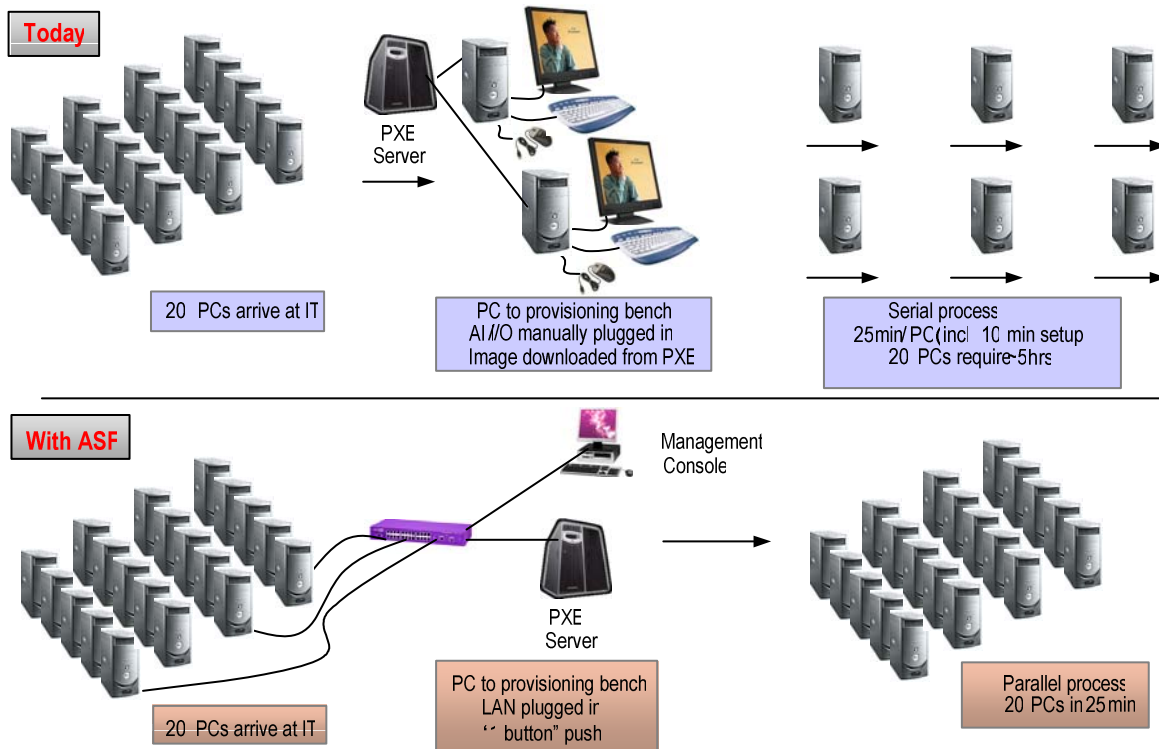


Figure 3: PC Provisioning

Table 1 summarizes the provisioning steps and times for the processes illustrated in Figure 3.

Table 1: Provisioning Time Comparison

	<u>Today</u>	<u>ASF</u>
New Machines (to be provisioned)	20	20
IT bench capacity	2	-
<i>(Note: bench capacity refers to limitation in space and I/O devices)</i>		
Unpack, connect power + LAN (minutes)	8	8
Connect power + LAN (minutes)	1	2
Connect I/O (minutes)	1	-
Total setup time (minutes)	10	10
Power on PC, wait to press F8	2	-
Download one image (minutes)	15	15
Total provisioning time, one PC	27	25
Number of times to repeat (if serialized)	10	-
Total Time (hours)	4.5	0.4
Time Savings (hours)		4.1

Use Case 2: Improving Software Patching

An essential IT challenge is that of defending the network against viruses and other malicious attacks that cripple the network and impact business. Based on a recent survey conducted by *Information Week* magazine, 21 percent of businesses had a minor financial loss due to a cyberattack¹.

The ability to securely and reliably patch the software image on the enterprise's PCs is fundamental to protecting against these attacks. Often, these patches are pushed to client PCs overnight using WoL (Wake on LAN). WoL technology resides in a PC's managed network adapter and motherboard. It is used to turn on PCs remotely, but has several limitations which ASF solves. Table 2 compares both methods and illustrates the advantages of ASF Remote Management and Control Protocol (RMCP).

Table 2: WoL Compared to ASF

Category	Problem Description	WoL	ASF
Security	IT requires a secure communication channel between management console and client.	No	Yes: HMAC/SHA-1 based authentication
Feedback	IT requires confirmation that the client is responding and identification/notification of issues.	No	Yes: Two-way communication
Cross subnets	IT requires capability to deploy S/W patches across complex networks (large enterprises).	No	Yes: Can cross subnets
Reset hung PC	IT requires a method to power cycle a PC if problem encountered during patch procedure.	No	Yes: Remote power reset

Use Case 3: Repairing a Hung PC

One of the most costly aspects of PC maintenance is a desk-side visit by a technician to diagnose and repair a PC that is hung and will not boot. Because the PC cannot reach an OS-present state, most of the over-the-wire tools that IT would normally use are not available.

The typical types of problems which can cause a PC to hang fall into two categories (see Figure 4):

Phase 1: typically associated with hardware and BIOS problems

Phase 2: those caused by file problems.

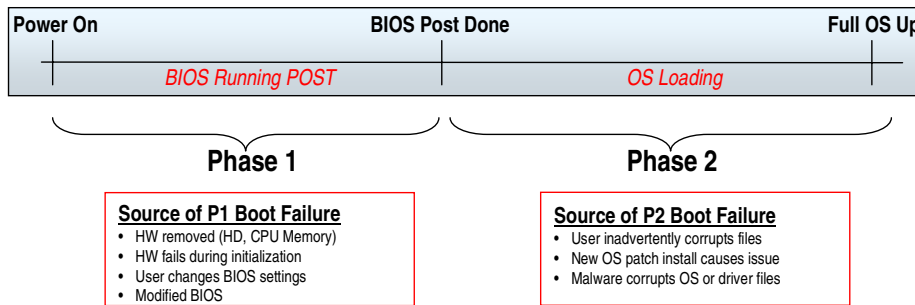


Figure 4: Typical Boot Issues

When problems such as these occur, a Level 2 or above technician will need to be sent to the user’s desk to determine what is wrong and to repair the problem. In some cases multiple visits are required. In addition, there is an implicit cost attached to user downtime. It is easy to see that the total cost of a hung PC rapidly becomes significant (see Figure 5).

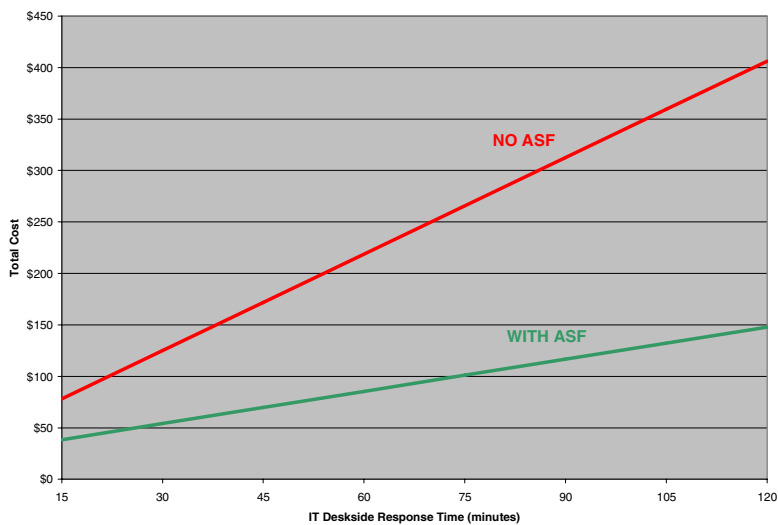


Figure 5: Total Cost for Repairing a Hung PC

ASF delivers an effective method to reduce these costs by providing tools for IT to diagnose and repair common PC problems over-the-wire, even if the PC OS is absent.

In so doing, ASF allows IT to address more issues with Level 1 technicians, rather than higher skill Level 2 or 3 specialists who are much more costly. Overall user down time is decreased as the user no longer has to wait for a skilled technician to physically arrive at the desk.

Figure 6 shows an example of how ASF can help diagnose and repair common PC problems, and how IT would react to a help desk call with a complaint about a hung PC.

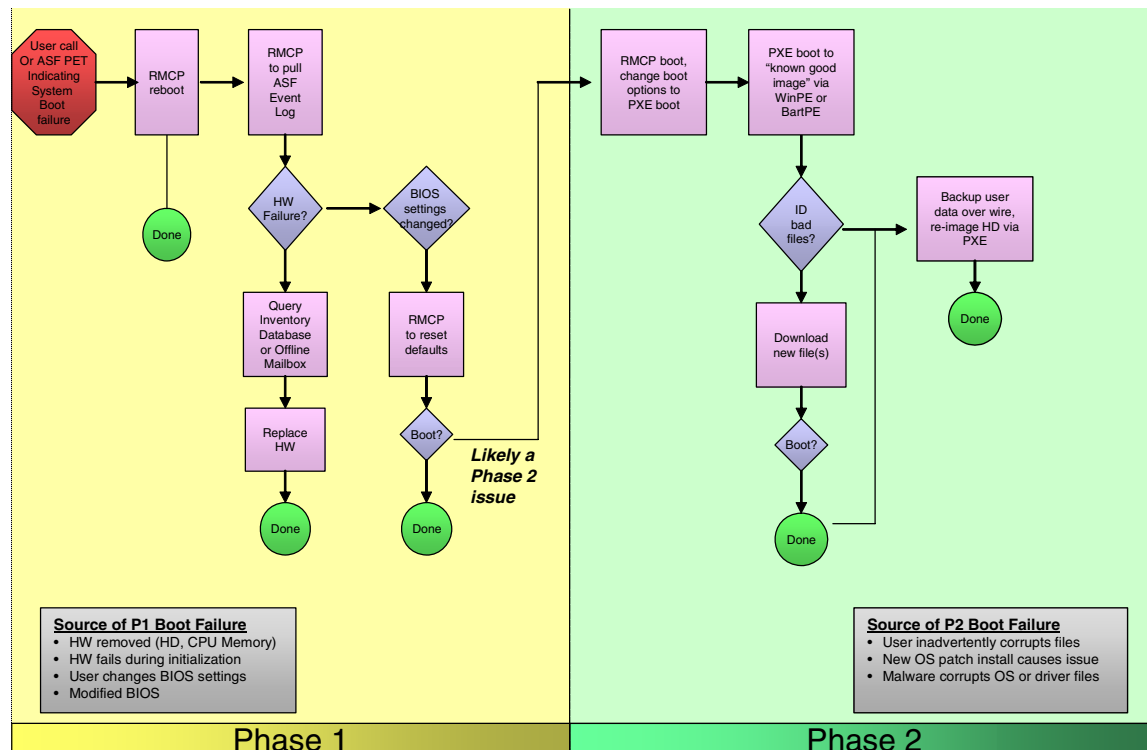


Figure 6: Procedures to Repair a Hung PC using ASF

The following procedural steps are typical:

- User calls IT help desk to report a problem
- Technician uses the ASF power cycle feature to reboot the PC. If successful, the problem is solved.
- If the basic re-boot does not solve the problem, the technician remotely retrieves the ASF Event Log. The log shows boot progress and helps the technician pinpoint common hardware problems. If a hardware problem is identified, the technician queries the company’s hardware database to identify the type of hardware installed in the PC, secures the component from inventory, and walks to the user’s desk to replace the faulty hardware.

- If no hardware problem is detected, the ASF Event Log can then be used to check for evidence of unintended changes to or corruption of the BIOS. For example, if the problem initiates because the user has inadvertently changed the BIOS settings, an ASF command can be issued to reset the BIOS settings to default.
- If no hardware or BIOS issues are detected, then it is likely that the cause of the hang is not a Phase 1 issue, but instead a Phase 2 issue.
- The PC is rebooted again and the ASF is used to remotely change the boot options to allow a PXE boot. A “known good image” can be loaded onto the PC to allow it to be brought to an OS-present state. At this point, the file system can be accessed and the file problem possibly repaired. If the technician cannot repair the problem, he can use PXE or iSCSI to re-image the system.

Use Case 4: Defending Against Physical Threats

As a company grows larger, physical asset management becomes increasingly more difficult. Protection of valuable assets is essential to controlling costs. This can be a very difficult task. In 2003 alone, 600,000 computers were stolen, ² which equates to a loss of approximately \$0.5 billion (based on a unit cost of \$800). In addition to stolen PCs, other threats exist that inhibit the ability to use or maintain the PC:

- Theft of components: PC memory or CPU are commonly stolen items
- Misplacement of PCs: Large enterprises grow via acquisitions and cannot always account for all assets
- Unauthorized change of PC configuration: Users add unauthorized hardware
- Malfunctioning hardware: Fan failure is a common example

ASF has pre-defined alerts that signal any of these physical threats. For example, an IT administrator is warned via the management console that a physical threat occurred. Since ASF supports OS-absent manageability, these threats can also be signaled even if PCs are off or hung.

Conclusion

Remote client manageability that functions in an OS-absent environment can save IT departments a significant amount of money. This important capability simplifies PC provisioning, improves software patching, reduces desk-side visits, and protects the enterprise against physical PC threats. All of these factors help reduce IT support costs and user downtime, therefore reducing the total support cost.



To enable client manageability in today's enterprise, ASF is the hardware "plumbing" of choice. It is standards-based, and thus more secure, interoperable, and widely supported than a proprietary scheme. It also boasts a massive installed base of 75 million PCs with ASF-enabled hardware. Today, this allows IT to turn on ASF on a majority of the PCs in their enterprise.

References

- 1 *InformationWeek* Research's U.S. Information Security Survey 2005
- 2 Microsoft (<http://www.microsoft.com/atwork/stayconnected/protectpcdata.mspx>)



Phone: 949-450-8700
Fax: 949-450-8710
E-mail: info@broadcom.com
Web: www.broadcom.com

Broadcom®, the pulse logo, Connecting everything®, the Connecting everything logo, BroadSAFE™, BroadVoice™ and BroadVoice32™ are trademarks of Broadcom Corporation and/or its affiliates in the United States, certain other countries and/or the EU. Any other trademarks or trade names mentioned are the property of their respective owners.

BROADCOM CORPORATION
16215 Alton Parkway, P.O. Box 57013
Irvine, California 92619-7013
© 2005 by BROADCOM CORPORATION. All rights reserved.

ASF-WP102-R 10/10/05