ASF: Standards-based Systems Management

Providing remote access and manageability in OS-absent environments

Contents

Executive Summary

One of the last, big pieces of the TCO (Total Cost of Ownership) puzzle is currently falling into place with the ASF (Alert Standard Format) specification. Developed by the Pre-OS Working Group under DMTF (Distributed Management Task Force), ASF helps deliver on the cost-reduction promise of systems management through capabilities such as system health monitoring, asset protection and remote control.

Even though network management solutions have been widely available and deployed for years, many IT departments are not fully utilizing these solutions because of systems management gaps in low-power and OS-absent states. Now ASF is helping to close those gaps and reduce IT costs by defining interfaces that provide access and manageability in OS-absent environments. This paper provides a detailed overview of ASF including a variety of usage scenarios.

The Promise of Systems Management

IT managers have a dream: they want to reduce the time and money spent on routine "help desk" inquiries, enabling them to spend more time on higher-level tasks and strategic planning. They want to look at the big picture – developing and providing different classes of user services instead of just putting out fires. Software management solutions, available since the 1990s, promise to bring this dream closer to reality while also ensuring maximum end-user system uptime.

These solutions give the IT manager remote access to local computing systems and provide regular health and inventory data for the remote user systems. Management console applications focused on this level of systems management facilitate tasks ranging from inventory, maintenance and troubleshooting to more complex debugging capabilities.

With such management tools, enterprise IT departments should be able to reduce the number of on-site visits to distant systems, resulting in a corresponding decrease in support staff costs and system TCO. However, a barrier to fully realizing these benefits has been the inability of these software-based solutions to provide remote management in low-power and OS-absent states such as:

- System sleeping
- System powered off
- Operating System (OS) hung
- Booting up

Previous technologies have not provided a complete solution. For example, Wake on LAN (WoL) technology is designed to bring remote systems out of sleep mode for off-hours maintenance and then allow them to go back to sleep until regular work hours. But WoL doesn't work when the OS is hung. In fact, a problem with software-based management in general is that it depends on a healthy OS and application to keep working.

When the OS or application becomes unavailable or unstable, that is when the IT manager most needs to retain access to the remote system for diagnosis and recovery. Ironically, that is precisely when the remote management solution is least likely to deliver the needed access. The Alert Standard Format specification addresses this gap.

ASF provides the missing piece of standards-based alerting and remote control, which can be implemented on mobile, desktop and workstation systems, or server platforms. Both the "send" (alerting) and "receive" (remote control) capabilities of the ASF technology are hardware-based and local to the networking solution on managed systems. This allows these solutions true CPU and OS independence, providing a much more persistent connection with the management console.

Historical Perspective

The history of this technology begins with Alert on LAN (AoL), developed by IBM and Intel in 1997. The original AoL was uni-directional, enabling reporting from clients to consoles only. Intel added bi-directionality with AoL2 in 1999, providing additional remote control and acknowledgement capabilities. This allowed connection-based, bi-directional communication between the management console and the managed client.

The technology was subsequently standardized by the Pre-OS working group of DMTF in June 2001 as the ASF Specification (now v1.03). A revised specification that adds security to the remote-control operations, ASF v2.0, is expected to be released the summer of 2002.

ASF Technology Overview

From a technological standpoint, ASF lives primarily in the Ethernet controller and then extends to various motherboard and system elements. The controller sits on the motherboard or a plug-in network adapter card (NIC) in the local system. It collects information from various components in the system – including the CPU, chipset, BIOS and sensors on the motherboard – and sends this information to a remote server running a management console (see Figure 1).

The controller also accepts commands back from the management console, and drives the execution of those commands on the local system. ASF defines specifications for the various interfaces required – for example, to and from the console and the controller on the NIC, or to and from the controller and the motherboard.

ASF is different from the myriad of other system management solutions on the market today because it does not require significant additional hardware outside the Ethernet controller in order to provide the majority of potential benefits. In addition, the standards-based set of interfaces for alerting system components provides a Plug and Play environment in which multiple vendors for each solution element can be found in the market. These attributes enable systems manufacturers to bring management-enabled systems to market for a low cost, thus reducing the initial investment IT must make in a new managed system.

ASF alerting capabilities include system health information such as BIOS messages, POST alerts, OS failure notifications, and heartbeat signals to indicate the system is up and running on the network. Also included are environmental notifications such as thermal, voltage and fan alerts, which send proactive warnings that something is wrong with the hardware. In addition, asset security is provided by messages such as “cover tamper” and “CPU missing” that notify an IT manager of potential system break-ins and even processor or memory theft.

Remote-control capabilities allow an IT manager to remotely power up, power down, power cycle, reset or reboot. If necessary, the managed system can be commanded to reboot to multiple boot paths – for example, to reboot the system and change the boot device from the hard drive to a diagnostics routine on a CD-ROM, Floppy or Boot ROM. A manager can also ping remote systems to ensure that they are on the network and running smoothly.

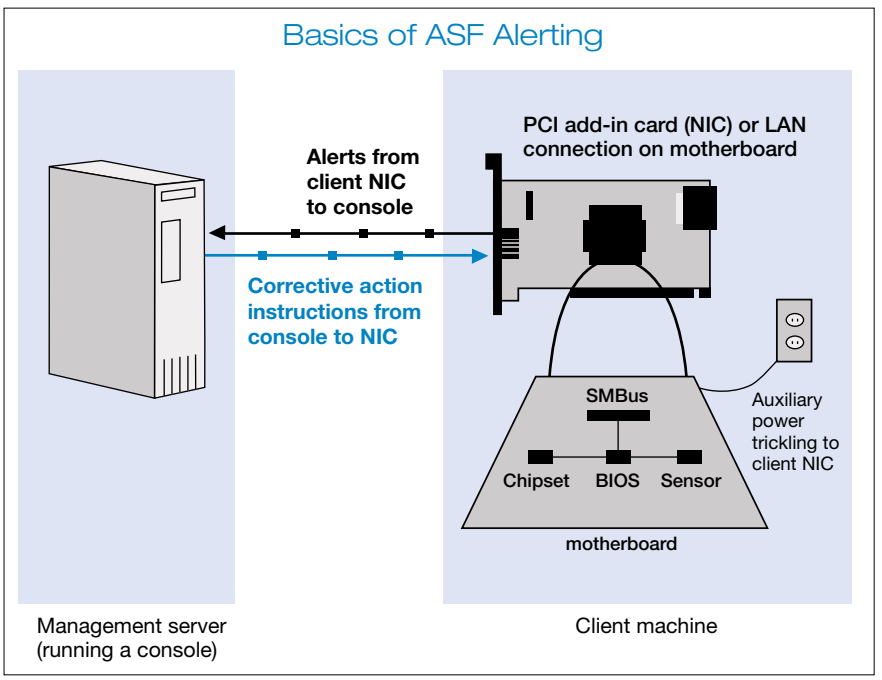

Figure 1.

Usage Scenarios

The following scenarios demonstrate how network managers can realize the three principal benefits of ASF-enabled alerting: system health monitoring, asset management and remote control.

System Health Monitoring

In this scenario, users arrive for the day and systems boot. Two alerts are received at the management console:

- BIOS Alert – Hard-Disk Controller Failure
- BIOS Alert – Video Controller Failure

The IT manager now knows what the problem is, even before an end-user calls for help, and thus can focus on fixing the problem versus diagnosing it.

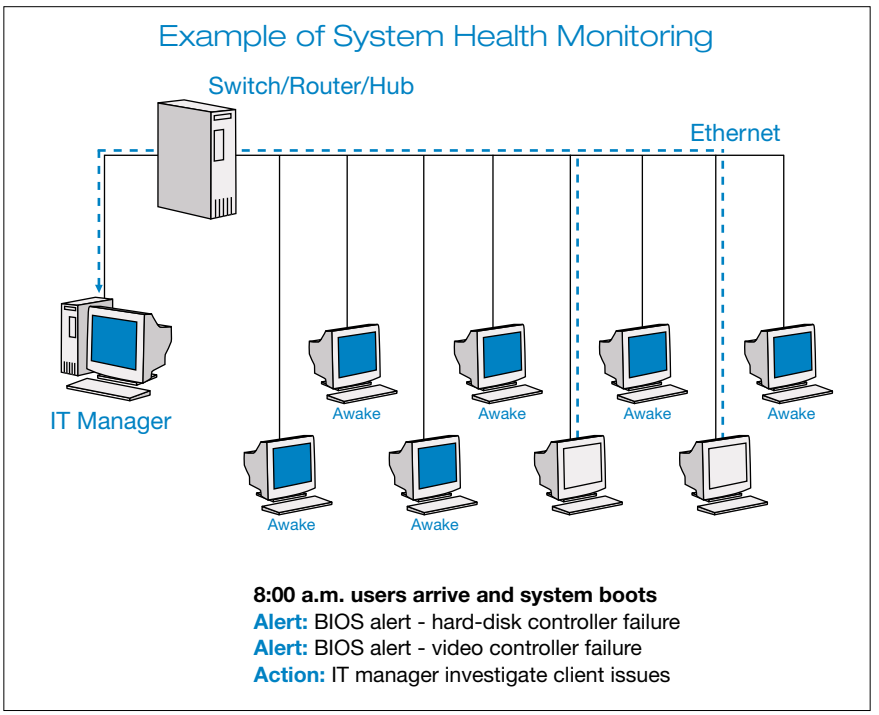

Figure 2.

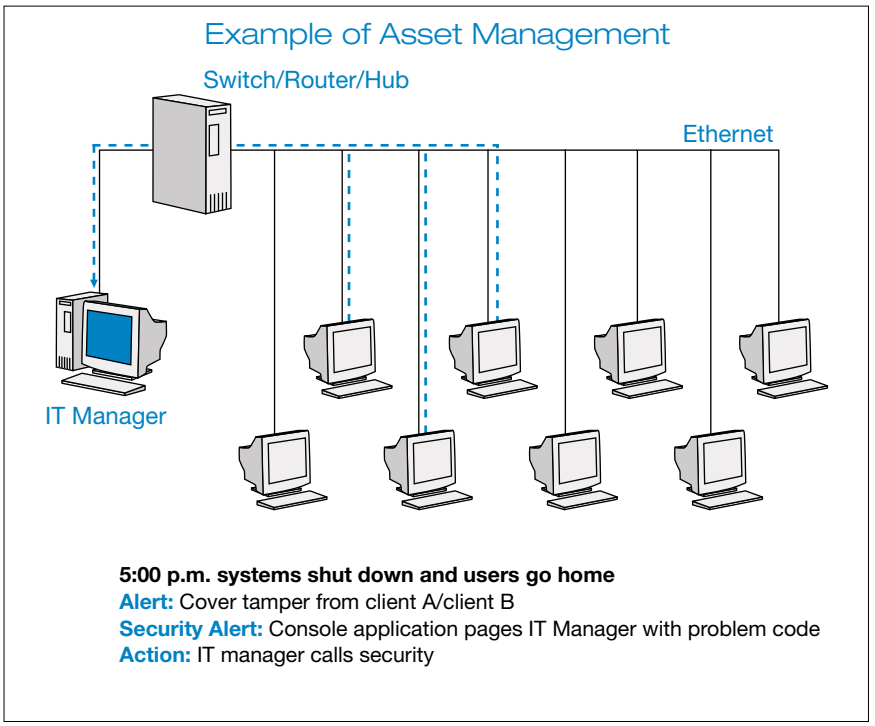

Figure 3.

Asset Management

At 5:00 p.m., systems shut down and users go home for the day. Later, alerts are generated and received at the management console:

- Alert – Cover tamper from client A/client B

The console application pages the IT manager and provides a specific problem code. The IT manager calls security.

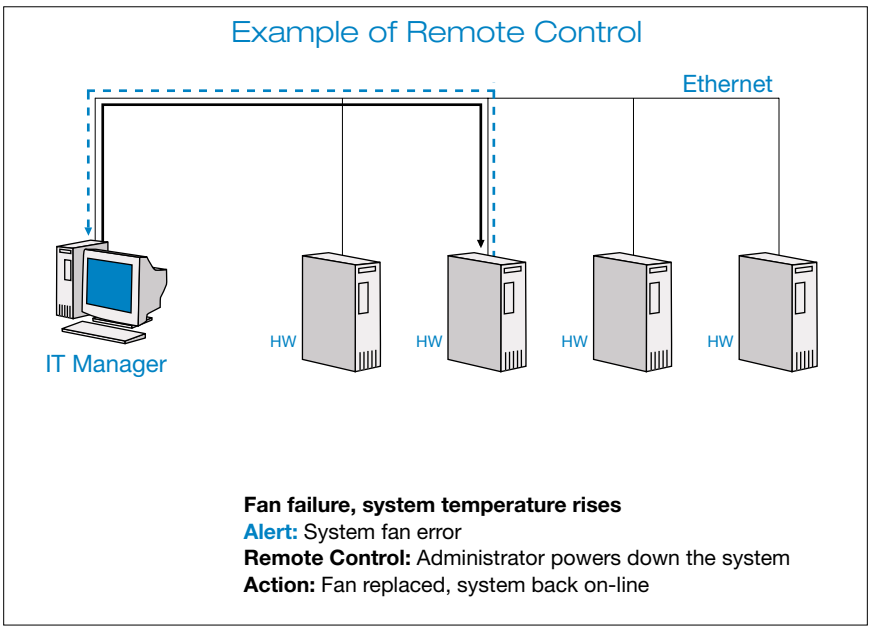

Figure 4.

Remote Control

During the workday, a fan failure occurs and system temperature rises. An alert is triggered to the management console:

- Alert – System Fan Failure

In response, the administrator remotely powers down the affected system to prevent potential heat damage to the CPU and memory. A technician is scheduled to replace the fan and bring the system back on line.

Clearly, this gives IT the ability to move from purely reactive measures to proactive problem resolution. By exercising control from a central location to avoid catastrophic failures, IT managers can generate huge savings and begin realizing the true potential of systems management.

Importance of Standardization

The DMTF is the industry organization leading the development, adoption and unification of systems management standards and initiatives for desktop, enterprise and Internet environments. Working with key technology vendors and affiliated standards groups, the DMTF is enabling a more integrated, cost effective and less crisis-driven approach to systems management through interoperable management solutions such as ASF.

In the case of ASF, there are several reasons why a standard is very appealing. For example, ASF will enable a company that is using add-in NICs to interchange these cards regardless of the brand. It ensures that different vendors are producing ASF-compliant cards, so that swapping them causes virtually no change to the systems alerting configuration, software or BIOS. Additionally, deploying a standard technology across the enterprise assures reduced training costs for IT administrators by avoiding the headaches of supporting multiple proprietary implementations.

Value to Users and IT

Perhaps the most important benefit of ASF is to the user – the overall service level provided to the user is improved, maximum system uptime is assured and, consequently, general workplace productivity can be expected to increase.

A wide variety of benefits is also realized by a company's IT department. Alerting reduces overall TCO by:

- Reducing support time and visits to the PC or user
- Helping to protect assets
- Simplifying the task of managing desktops and low-end servers
- Increasing the productivity of IT support personnel
- Enabling proactive cost avoidance (such as shutting down a system to avoid heat damage when a fan failure alert is received)
- Allowing increased specialization in the IT department

This last benefit is especially important to understand because it can revolutionize the personnel profile in an IT department and provide consistent, long-term cost reductions. With ASF-enabled alerting in place, most troubleshooting can be performed remotely from the management console by the IT administrator, who typically has the most extensive training and experience. Specialized personnel who have less training, and are therefore less costly to staff, can be dispatched to handle on-site visits for system recovery instead of the more experienced (and costly) network/systems experts.

For example, suppose that an administrator is remotely rebooting a system. Assume that as part of the process, specific ROMs must be run for video and SCSI add-in cards, in that order. The console shows that the video card has been brought up successfully, but then the system locks up in BIOS. Another reboot is tried and the same thing happens. The IT administrator watching the console can conclude from this information that the SCSI card is the problem.

As a result, only the IT person specializing in this area needs to be sent on-site, taking far fewer tools than would have been needed for system troubleshooting. Not everyone on the IT staff needs to know everything. Only the top administrators require broad knowledge and training. This is a powerful and heretofore unavailable model for IT support which is directly enabled by alerting technologies.

Conclusion

ASF-enabled alerting provides a solution in many areas critical to delivering customer support for IT departments. The management capabilities that the IT department delivers through its service level agreements are dependent on several discrete IT tools. A fair portion of these tools, including inventory, remote management and event/fault management are directly delivered by ASF. This makes it a key element in the IT environment both today and in the future.

Ultimately, the goal is to apply Plug and Play principles to the entire IT environment, with available consoles, systems and NICs all supporting the same standard technologies. ASF fundamentally supports the Plug and Play paradigm. The IT administrator ideally should be able to order an Ethernet NIC or LoM (LAN on Motherboard) and automatically get ASF technology along with all the existing Wired for Management baseline technologies – without having to specify it in the order. Toward that end, alerting is now available in all Intel® DT chipsets and all of Intel's latest generation of network controllers.

For More Information

For more information about ASF and the DMTF, see: http://www.dmtf.org

For more information about Intel desktop chipsets, see: http://developer.intel.com/design/chipsets/linecard.htm

For more information about Ethernet controllers, see: http://developer.intel.com/design/network/products/ethernet/linecard_ec.htm

0402/OC/EW/PP/2K

Please Recycle NP2127