Chapter 1

Introduction to Platform Manageability

There are two kinds of people, those who finish what they start and so on.
—Robert Byrne

Too much coffee, premature loss of hair, late hours, and excessive stress are often symptoms of a network administrator facing a increasingly large network and difficult troubles. It's often after facing an endless stream of support issues that network administrators start asking: Isn't there another way to solve this? Computer software issues, hardware failures, software patches, network viruses, stolen hardware, and bad settings are just a few of the major headaches facing network administrators today and it's only getting worse as computers and operating systems become more complicated.

A long time ago, turning a computer off and on would solve just about any problem, but those days are long gone. With the interconnection of computers and the increasing complexity of software, the only solution is to deal with problems using increasingly smart network manageability software and hardware. On top of all of this, administrators are facing a scaling and cost problem. Organizations have thousands of computers that must run properly at all times and this with an increasingly reduced budget.

One could ask: if a computer is so smart, why can't it help trouble shoot problems, isolate viruses, and alert the administrator if something is going wrong and help in its own management tasks? This is where platform manageability comes into play.

In this book, we look at how a computer can best be managed; that is, the role of software manageability solutions and their limitations. Then we look at the Intel® vPro™ technology solution and how it can help with secure manageability features built right into the computer's hardware.

Platform Manageability

In this book, a platform is a computer system and all of its hardware components: motherboard, disk storage, network interface, and attached devices, as shown in Figure 1.1. In other words, it's everything that makes up the computer's hardware.

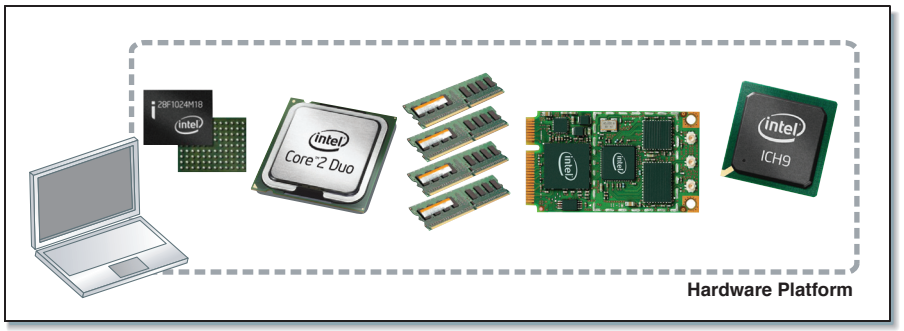

Figure 1.1 Hardware of a Modern Computer Platform

It is worth noting that the platform also includes the BIOS that boots up the computer. So if a BIOS setting is incorrect, and as a result the computer does not start up correctly, we can consider this to be a platform issue. Platforms have gotten significantly more powerful in the last few years, as illustrated in Figure 1.2. They can boot remote operating systems from the network, boot on RAID arrays, they have built-in security locks, and much more.

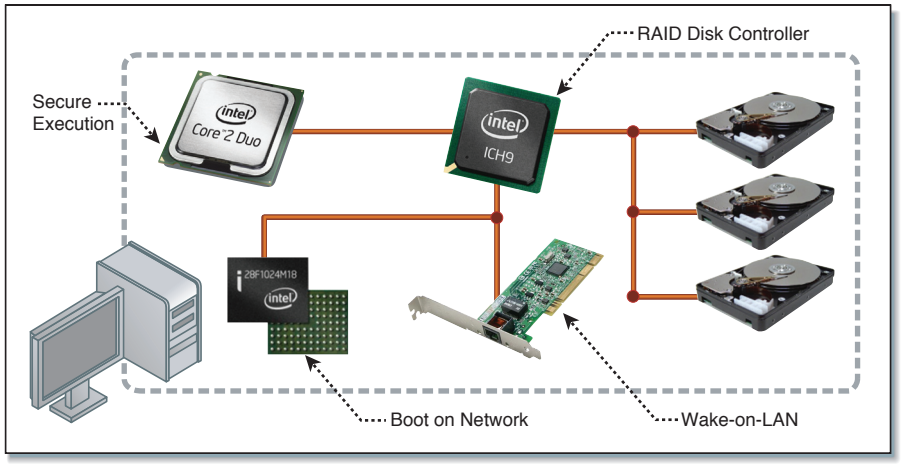

Figure 1.2 Advanced Features on Today's Computer Platforms

Platforms are much more powerful today; most platforms have limited manageability built in them. A buzzer may sound when the temperature is too high, or an error code is displayed when a disk fails. As we will see in this book, Intel vPro technology adds powerful new management features to the platform itself.

System Manageability

System manageability is broader; it includes both the software and hardware portions of a computer. The aim of system manageability is to take into account all of the components of a computer and ensure that they function correctly, as shown in Figure 1.3.

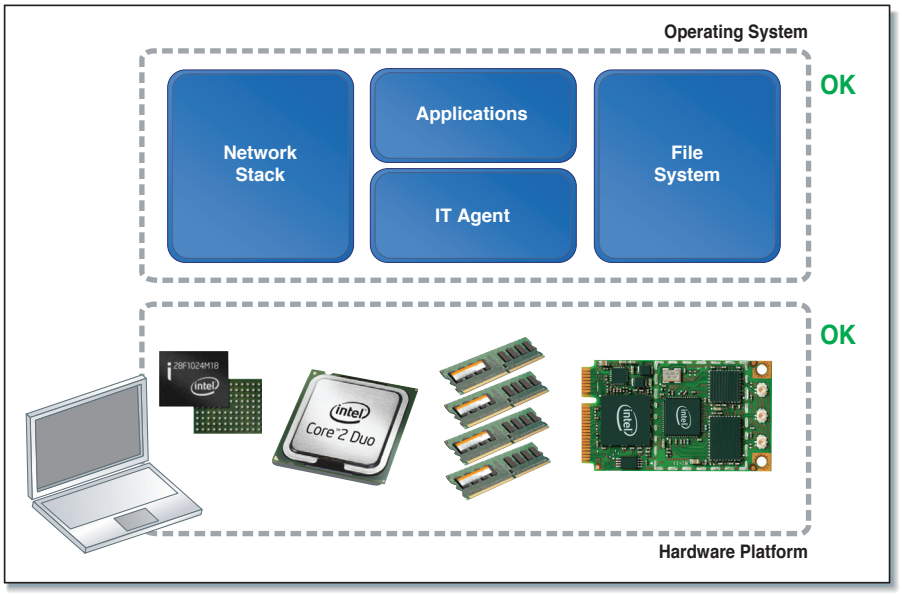

Figure 1.3 Both Platform and OS Software Running Correctly

One way to rate how effective a manageability solution works is to look at how much of the system is covered by the solution. Firewalls, anti-virus software, and remote control software all address, manage, and secure different portions of a system. The best solutions would of course be solutions that could monitor and address the widest array of possible platform and system problems. Network administrators may sometimes focus too much on one part of the system and forget others. For example: anti-virus software prevents a virus outbreak, but a bad driver patch stops all printers from working. For a manageability solution to work well, it must cover in the best way possible all of the components that make up a computer system, both the hardware platform and the software.

Since manageability software often runs within the computer's operating system it's trying to manage, it has limitations as to what it can monitor and fix. For example, if the BIOS settings are not set properly, software solutions can't easily change the BIOS. If a platform is not booting correctly, no manageability software is running at that time to investigate the problem. Software manageability solutions that run in the OS also run only then the computer is powered on and can't react when the computer is sleeping. While

software solutions are powerful, they also have limitations because they run within the environment they are trying to manage.

Manageability Problems

In this section, we want to cover some of the problems network administrators are facing today and some of the same issues manageability solutions are trying to deal with.

Asset Inventory

Keeping tabs on the hardware and software inventory within an organization is probably the first problem administrators try to deal with. Where are the computers? Is there sufficient memory and disk space? Are hardware components being stolen? These questions are not only important, but in some organizations, computer asset tracking is required by law. Whether this information is used to understand when to upgrade computers or report theft to authorities, network administrators have to deal with this in one way or another.

Computer Repair

Keeping computers up and running is a difficult job. It can be costly if the downtime is significant or a technician has to make an on-site visit. Computers can break down because of hardware or software, and in both cases proper diagnostic is the first step to quick resolution. In some cases, repairs can be made by bringing a laptop to a repair desk for a few minutes, but in other cases, computers are critical or located in remote locations that don't allow for quick physical access.

Computer Security

Security is now a mainstream topic. Stolen disk drives, viruses, malware, and denial of service attacks sometimes get featured on the evening news. Increasingly, organizations are not only protecting their own data, but also the customer's data or patient information. Even if a computer is running correctly, it can still have severe security issues that need to be monitored and addressed quickly.

What makes security an especially difficult topic to address has to do with what software you can trust and what software you can't trust. Firewall software may be running on a computer, but other software may be able to turn it off. One could run software that would monitor the firewall, but who would monitor the monitoring software? Ultimately, what software can you trust when running in an environment where a user can run applications that are not trusted at any time?

Power Savings

Network administrators are now more and more frequently assigned the task of monitoring and finding ways to reduce power use. When computer resources are neatly arranged in server racks, this can be a simple task, but when computer resources are distributed across many sites, it is more difficult.

Many employees leave their computers on all the time resulting in a large waste of power. Network administrators can generally push operating system policies to place computers to sleep when idle, but this can have drawbacks when it's time to push urgent updates. It's also difficult to evaluate the efficiency of new power policies when there is no good way to know which computers are asleep. It may also be difficult to remotely tell if a computer is sleeping or disconnected from the network.

Possible Solutions

In most network environments, software agents and desktop remote control software are running on each computer along with a combination of anti-virus and firewall software. Since these management solutions are software running in the operating system, they are difficult to trust completely; they don't run unless the operating system is running correctly and they have various limitations in monitoring and controlling the computer and operating system on which they run.

One possible solution is to use a remote keyboard and mouse over network device (IP/KVM device) to fully control a computer remotely. These devices allow an administrator to remotely see the display and control the keyboard and mouse of a computer over the network, as shown in Figure 1.4.

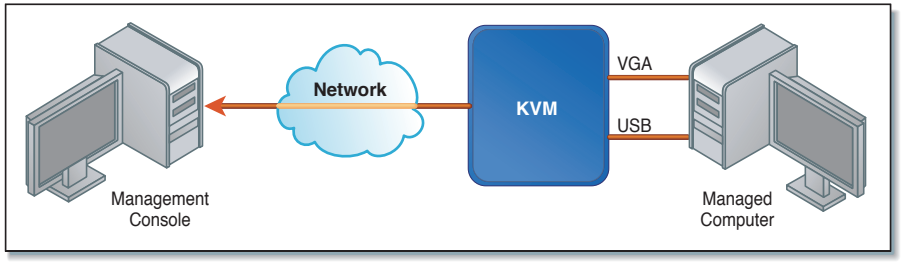

Figure 1.4 An IP/KVM Device Connected to a Managed Computer

Since this device stands on the side of the computer, it can be trusted and can't easily be compromised through the network. Such devices can't generally monitor or control the power state of a computer and are relatively expensive because they must take the video out of the computer and encode it in such a way as to be sent over the network. For mission critical computers this is an excellent option, but it is not an option that can be deployed widely. It is also impractical for large scale deployments.

For years now, large servers have had baseboard management controllers (BMC), which are small embedded controllers that monitor the larger server. Since these controllers are effectively separate from the main computer and have many connected sensors, they can be trusted and perform accurate diagnostic and monitoring of a large server, as shown in Figure 1.5.

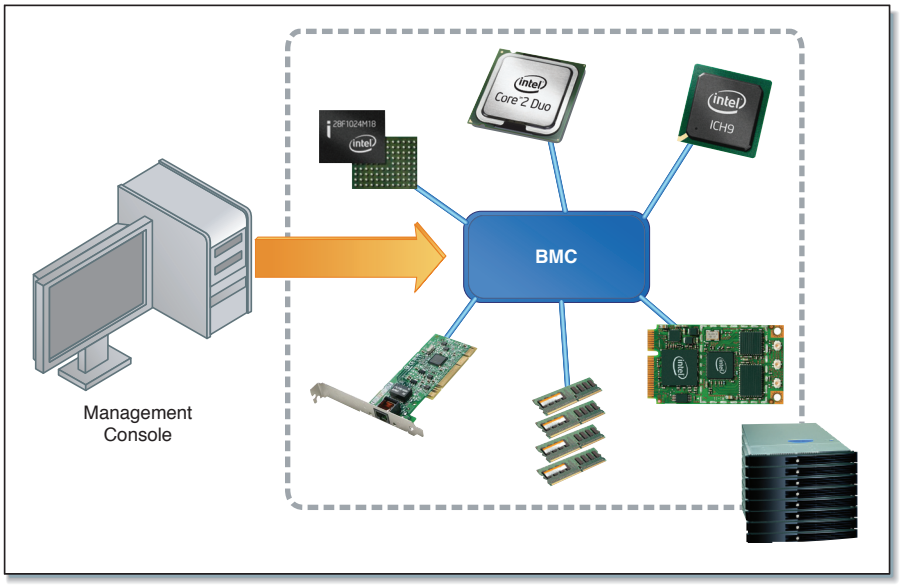

Figure 1.5 Baseboard Management Controller (BMC)

Many new BMCs also combine an IP/KVM feature making them very powerful. Administrators can turn a computer on and off remotely, take control of it and monitor system temperatures, fan controls, and much more. BMCs can be very useful, but they also add significantly to the cost of the platform and so are reserved for high end servers.

In effect, today's solutions are ether software-only or an effective but costly combination of software and hardware.

In-Band versus Out-of-Band

When looking at various management solutions, we have to look at how the management solution communicates with the management console. This is important because how a management console communicates with a managed computer affects the robustness and cost of the communication link.

In-band management solutions run within the operating system and use the operating system resources and network communication, as illustrated in Figure 1.6. For example, a corporate agent might monitor the computer and report back to a main server about the health of the computer.

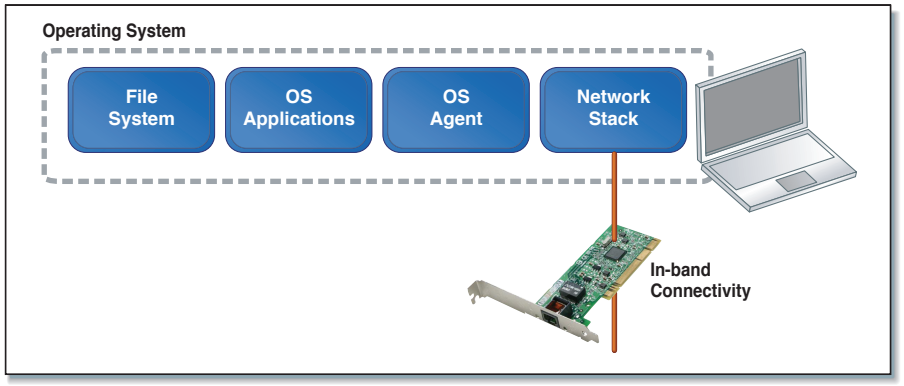

Figure 1.6 In-Band Connectivity: This Is the Usual Flow of Network Traffic from the Operating System to the Network.

Out-of-band management solutions run alongside the main operating system and use an alternate communication path that does not depend on the operating system running properly. A good example would be an IP/KVM device that runs alongside the main computer and uses a separate connection to the network. Another example involves sharing some of the hardware used by the operating system but using a separate network stack.

Out-of-band management solutions can be built within the computer itself, but they are considered out-of-band when they don't depend on the operating system. Sometimes, they can use a different communication path like a separate serial port or the same path as the operating system (such as sharing an Ethernet port), as shown in Figure 1.7.

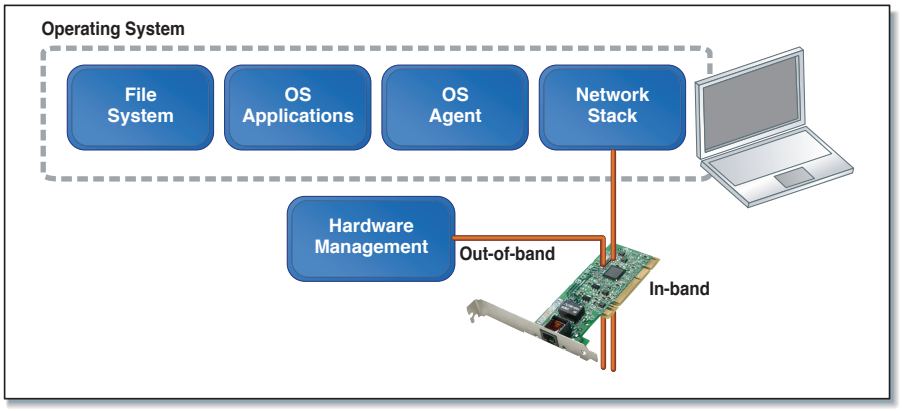

Figure 1.7 Out-of-Band Management: Both the Operating System and Hardware Management Traffic Can Use the Same Network Hardware.

Out-of-band communication is typically more reliable since it's more often available than the in-band channel. The Wake-on-LAN (WOL) feature that has been available on most computers for many years is a good example of a primitive out-of-band channel. When the computer is sleeping and the operating system is not running, the Ethernet controller on the computer is still on, waiting for a packet that will instruct the wakeup of the computer.

Wake-on-LAN is a good example of what we mean by out-of-band. It's built right into the motherboard or network card of many computers and uses the same Ethernet connection and components as the in-band channel. Yet, because it does not depend on the operating system, it is considered to be out-of-band.

The difference between in-band and out-of-band is important because as we look at how to solve today's management problems, we quickly come to the conclusion that out-of-band management has many interesting benefits: it's dependable, it can be trusted, and more interestingly, it's available more often than in-band solutions.

Management Agents

One of the staples of network management has been the management agent. In the context of computer manageability an agent refers to software running on each managed computer on the network that facilitates the task of the remote administrator. Agents come in many forms and generally run as a background task within the operating system. Agents can do many things like performing system checks, reporting when the computer is present on the network, allowing the administrator to remotely control the computer, and so on. Almost all management software vendors have agents as part of their solutions. Agents have access to many of the computer's resources and can perform many tasks, but they have key drawbacks.

Trust and reliability are two of the main problems facing agents running in the operating system. Rogue software can replace, stop, or completely remove a running agent, making it impossible to manage the computer. Even without the presence of rogue software, agents are often disabled by the users or applications that attempt to clean up the operating system startup sequence. As a result, even the best agent is limited in how reliable and trusted it can be when running on a computer.

Connectivity is another problem facing agents. Even when running properly, the user may enable a firewall or other software that will block agent network connectivity. This often happens when the user changes firewall policies or installs new network filtering software. In this case, the running agent may try to solve the problem by resetting the firewall settings, but this is not always possible.

Since agents are an undeniable part of network manageability solutions, network administrators have been seeking solutions to solve the trust, reliability, and connectivity problems. One of the best solutions is to run the agent completely outside the operating system, such as, for example, on a completely separate computer or baseboard management controller (BMC), as shown in Figure 1.8. These solutions are expensive, but the general idea is a good one.

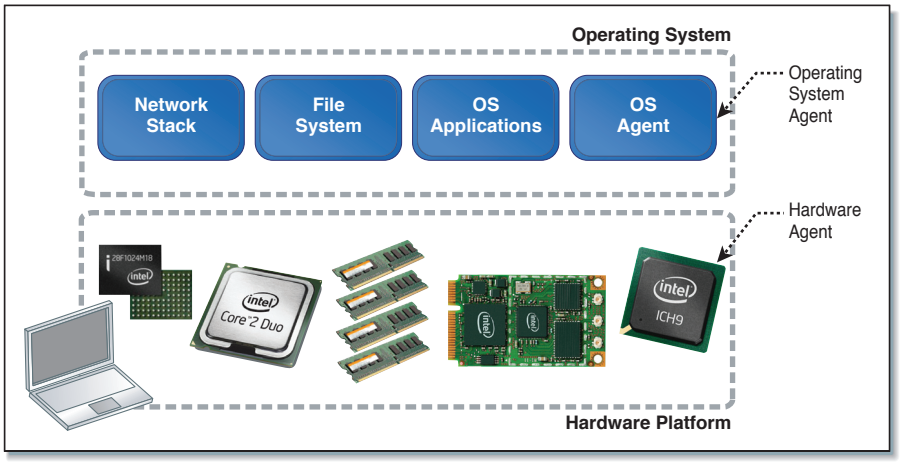

Figure 1.8 Agent within Operating System versus Agent in Hardware

If sufficient portions of the network management functionality run outside the main operating system in a separate and trusted environment, it could makes agents completely optional. Some computers would therefore run without management agents in an "agent-less" configuration.

Out-of-Band and Agent-less

Out-of-band communications and running agent features outside the operating system should be viewed as separate. However, both are logically related. It is possible for an agent running in the operating system to use an alternate means of communication such as a serial port, and it is possible for management features outside the operating system to use in-band communications.

While separate, using management features that run outside the operating system along with a connectivity path that is also outside the operating system's control provides trust, reliability, and connectivity that is desired in an ideal managed computer.

Management in Low Power States

Another management feature that is on the top of the manageability solution wish list involves being able to manage computers regardless of their power

state. This is especially important in an era of rising energy costs and heightens sensitively to waste of power. Manageability solutions based on software agents require the computer to be on for any manageability feature to be available. Software agents can work along with the Wake-on-LAN feature to allow the computer to turn off and be woken up when manageability operations need to be performed. Software agent along with Wake-on-LAN is not an ideal solution. When the computer is in low power, Wake-on-LAN cannot be queried to determine if the computer is still connected unless the computer is woken up first. Also, Wake-on-LAN may work on desktop PCs, but on mobile platforms that move from network to network, it's generally impossible to manage.

An ideal solution would offer some management features even when the computer is in low power states, making it easy to query and wake up the computer when appropriate.

Summary

In this chapter we reviewed various solutions and technologies from a historical perspective. We also defined the basic components that make a computer a manageable one. Connectivity, trust, and relativity are all factors that differentiate manageability solutions.

As we will see later in this book, running agent-like management functionality outside the main operating system along with trusted and reliable execution along with out-of-band connectivity is the basic idea behind Intel Active Management Technology (Intel AMT), a major component of Intel vPro technology platforms.

In the next chapter we look at the history of manageability.