Chapter 13

Intel® Active Management Technology in Small and Medium-sized Business

I do not fear computers. I fear the lack of them.

— Isaac Asimov (1920–1992)

If you have a computer enabled with Intel® Active Management Technology (Intel AMT) and want to just get started, you can "get your hands dirty" with this chapter and start using Intel AMT features with the freely available Manageability Developer Tool Kit (DTK). First, go to the following Web site, download and install the tools.

```
http://www.intel.com/software/amt-dtk
```

These tools are available freely with source code. For this chapter, only the binary versions of the tools are needed. Before starting, Intel AMT will need to be set up since new computers come with Intel AMT turned off. Appendix A demonstrates how to get into the BIOS or Intel MEBX screen at boot time and set up Intel AMT for the first time. Additionally, one should check that Intel AMT can be accessed using the built-in web server. To do this, use any web browser on a different computer and type in the following URL:

```
http://computername:16992/
```

Here "computername" must be replaced with the name or IP address of the computer with Intel AMT. It's important to note that this must be done from a different computer on the same network. Attempting to access the Intel AMT Web page from the same computer will not work. Figure 13.1 shows a sample network setup for Intel AMT and management console.

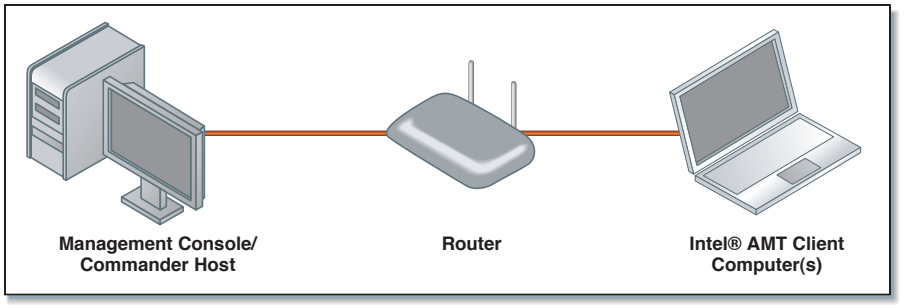

Figure 13.1 Simple Intel® AMT Network Setup

The computer that will serve as the management console does not have to support Intel AMT, but if the console does support Intel AMT, it will not be able to manage itself, only others. Once we have one or more computers with Intel AMT set up and ready to go, it's time to install the Intel Manageability Developer Tool Kit (DTK).

Installation

The DTK must be installed on Microsoft Windows XP or Microsoft Windows Vista; both 32-bit and 64-bit platforms are supported. The DTK also requires Microsoft .NET; make sure you have the latest version. It includes console and agent software so it's useful to install the DTK on both the console computer and all computers with Intel AMT. Start by launching the installer and accepting the user license. The installer file will generally have the name:

```
Manageability_Developer_Tool_Kit_<version>.msi
```

During the installation you will be prompted to install management tools, remote agents and other tools, as shown in Figure 13.2. In general, if installing on a computer that supports Intel AMT, select remote agents; otherwise, this option need not be selected since remote agents only work on computers with Intel AMT.

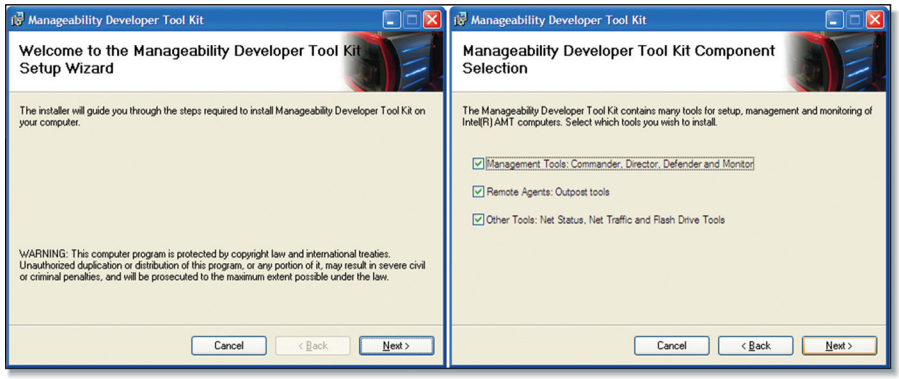

Figure 13.2 Intel Manageability DTK Installation Screens

Once completed, a set of new tools will be installed on the Start menu, under All Programs and Manageability Developer Tool Kit. Depending on the options selected in the installation, up to four main applications will be installed, which are described in the following sections.

Manageability Commander Tool

This is a sample Intel AMT management console and probably the most useful tool of this software package. Commander is built to make use of all major Intel AMT features and so serves as a great demonstration and development tool.

Manageability Network Defense Tool

This is a simplified version of the Commander tool. It's more limited, but resembles more closely what an easy-to-use Intel AMT tool would look like.

Manageability Director Tool

This is a simple setup and configuration tool. It can be used by advanced users to set up Intel AMT with full certificate security and reset Intel AMT to factory defaults.

Manageability Outpost Tool

This is an Intel AMT agent that can only run correctly on computers with Intel AMT enabled. It will log into Intel AMT using the local Intel Management Engine Interface (Intel MEI) and provide most of the functions that are available through this interface. Generally, Outpost should always run in the background and provides the console with many more management features if it's running.

Manageability Commander

Let's get started by running Intel Manageability Commander (Commander). Again, this console application can't run on the computer that's being managed; it must run on a different computer running on the same network. When entering Commander for the first time, no managed computers are listed. We need to add computers we are going to manage. To do this, we can manually add them or scan the network for computers that support Intel AMT.

To add a known computer, click File→Add→Add Intel AMT Computer…. The dialog box shown in Figure 13.3 prompts you for the address, username, and password of the Intel AMT computer.

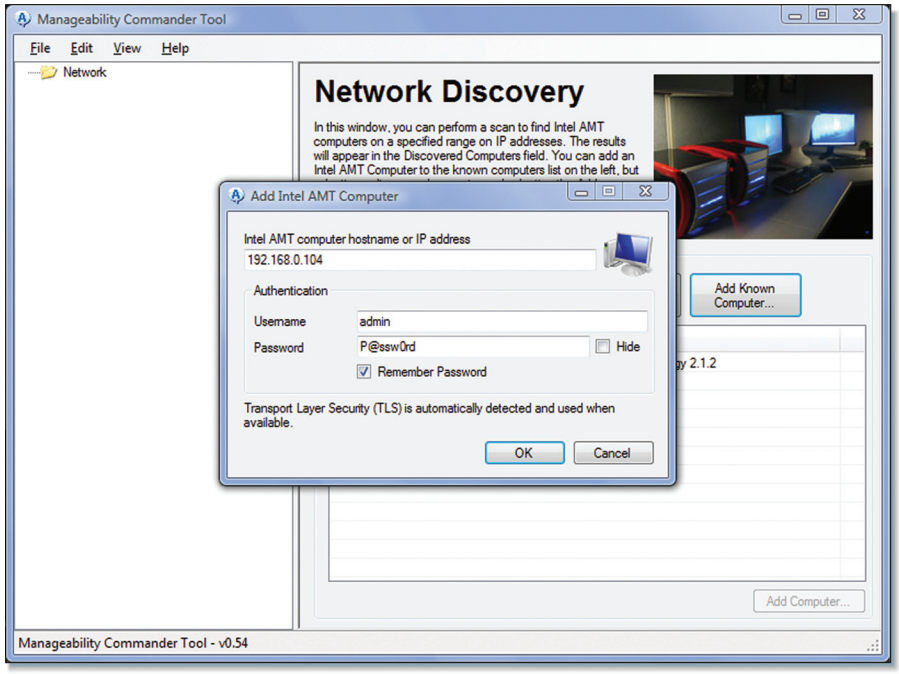

Figure 13.3 Manageability Commander Prompting for a New Intel® AMT Computer

Additionally, Commander can scan the network for Intel AMT computers. While in the Network Discovery screen, enter the starting and ending IP address and press the Start button. As shown in Figure 13.4, as each computer is found, it will be added to the Discovered Computers list.

When possible, Commander tries to gather data about the computer that was found. Without knowing the username and password to log into Intel AMT, Commander can only discover whether transport layer security (TLS) is being used, and when TLS is not in use, which version of Intel AMT is supported. When a computer is discovered, it must still be added to the list of managed computers. To do this, select a discovered computer and click Add Computer. A dialog box will prompt you for a username and password.

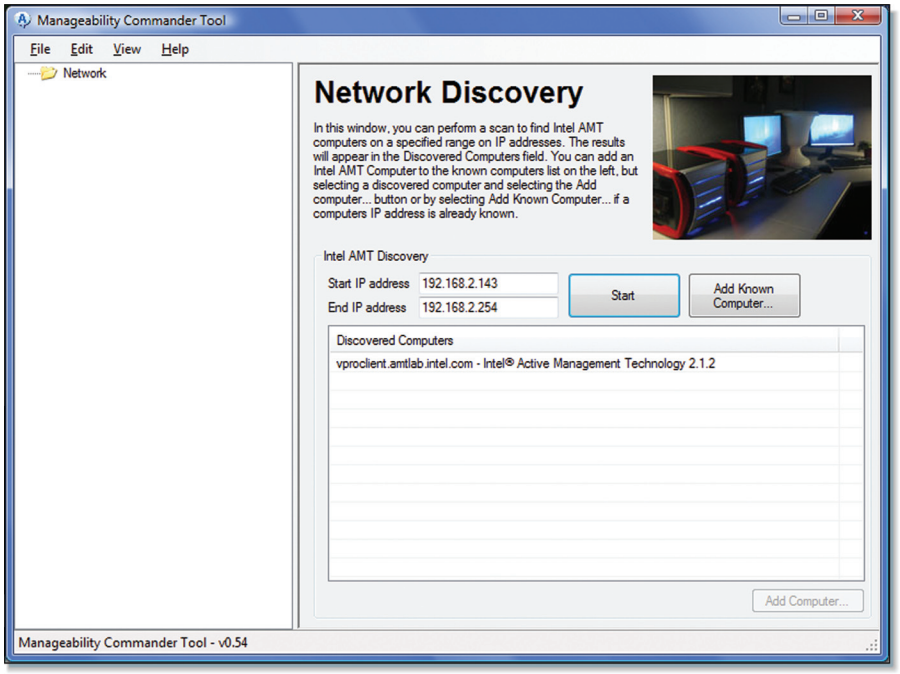

Figure 13.4 Manageability Commander Finds One Computer After Performing a Limited Network Scan

For each computer that is discovered, repeat the process of selecting it and adding it to the list of managed computers on the left tree view. It's possible to add the same computer more than once. This is especially useful if Intel AMT is configured with more than one user account. For now, only the administrator account with the username "admin" can be used.

Connecting

Once one or more computers have been added to the left side of the Commander tool, its time to connect to them and start performing management operations. As shown in Figure 13.5, select a computer on the left side tree view and press the connect button.

Tip You can also connect to a computer by right-clicking on its name and selecting the Connect option, or by double-clicking the computer's name in the left side tree view.

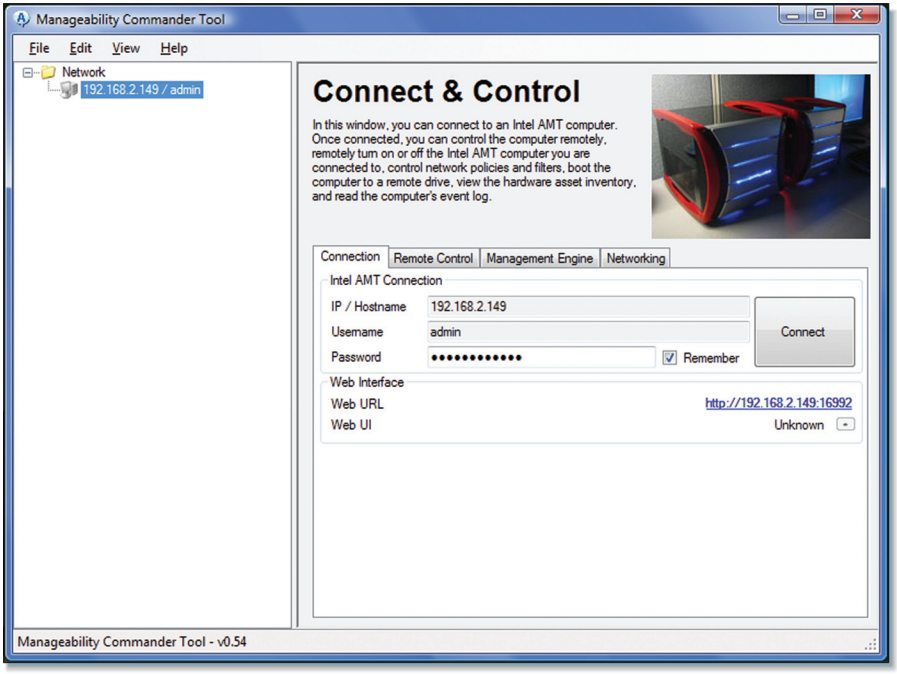

Figure 13.5 Selecting and Connecting to an Intel® AMT Computer

When Commander connects to an Intel AMT computer, it will immediately acquire most of the state information from Intel AMT. For the first few seconds, Commander will fill up the tree view with information as it arrives. By acquiring most of the state when first connecting, the user interface is much faster, but may contain stale information. The "Clear Web Service Cache" and "Fetch Web Service Cache" options on the File menu can be used to force Commander to reload its state cache, but using these is rarely needed. Many management consoles can connect to Intel AMT at any given time and the changes made by one management console may not be reflected in the other consoles unless the cache is cleared.

If there is any problem connecting to the Intel AMT computer, remove the computer and add it again, double-checking the hostname, username, and password. Also make sure that the Intel AMT Web page is accessible and Intel AMT setup as been completed as described in Appendix A.

Now that we have connected Manageability Commander to Intel AMT, we can start management operations. Feel free to open and browse the connected computer and explore the tree view on the left side of the screen.

Remote Display

Now it's time to remotely manage the computer using the Serial-over-LAN feature of Intel AMT. Select the computer on the left side and go to the Remote Control tab as shown in Figure 13.6.

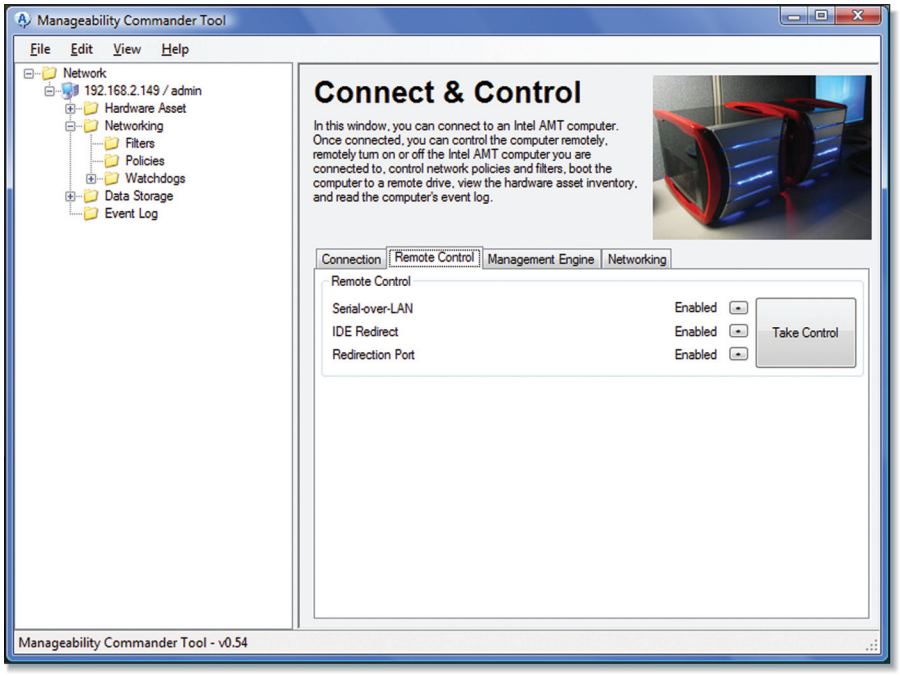

Figure 13.6 Manageability Commander Redirection and Control Screen

Here, we can make sure that the Serial-over-LAN, IDE-Redirect, and redirection ports are all enabled. The redirection port is 16994 without TLS and 16995 with TLS security. If the redirection port is disabled, management consoles can't use the Serial-over-LAN or IDE-Redirect features. Now we click Take Control to open the terminal window.

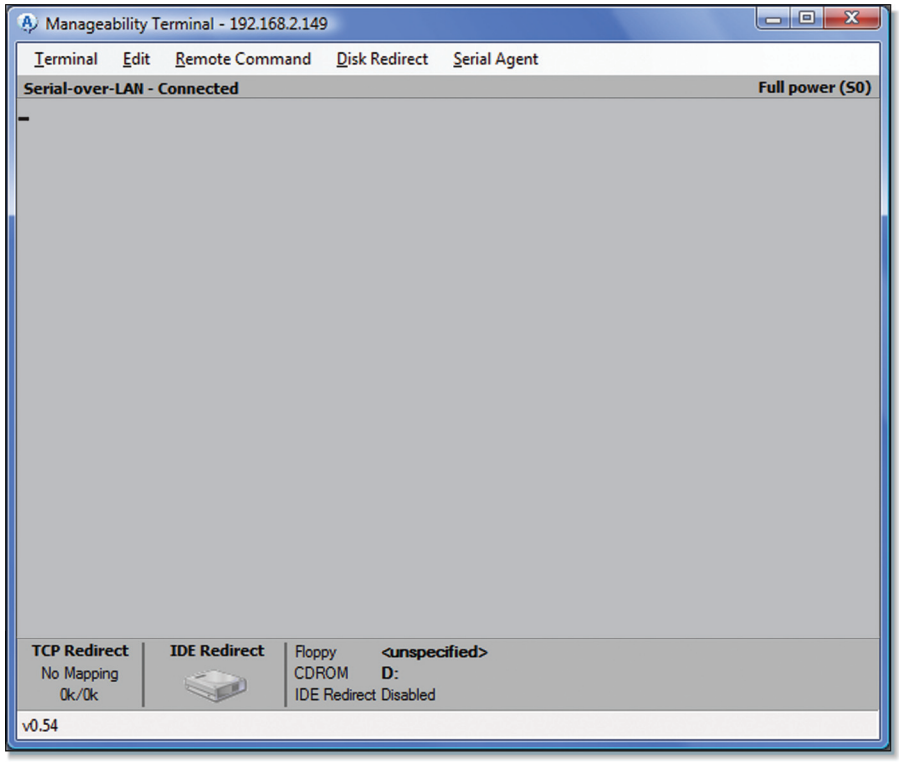

Figure 13.7 Manageability Commander VT100 Terminal Window

Figure 13.7 shows the VT100 terminal window. This terminal is just like the terminals used years ago with modems. It has a fixed number of 25 text lines and an 80-character width. This terminal view was built from the ground up for use with Intel AMT. On the top status bar, we see the terminal connection state of the upper left and the computer's power state on the upper right. The power state is polled every few seconds, but this polling can be turned off by clicking on the power state indicator. The bottom status bar

is mostly dedicated to displaying IDE-Redirect state. To use IDE-Redirect, select the Disk Direct menu at the top of the terminal.

From this screen, we can use the Remote Control menu to perform remote power control on the Intel AMT computer. Let's select Remote Reboot to BIOS setup in the remote control menu.

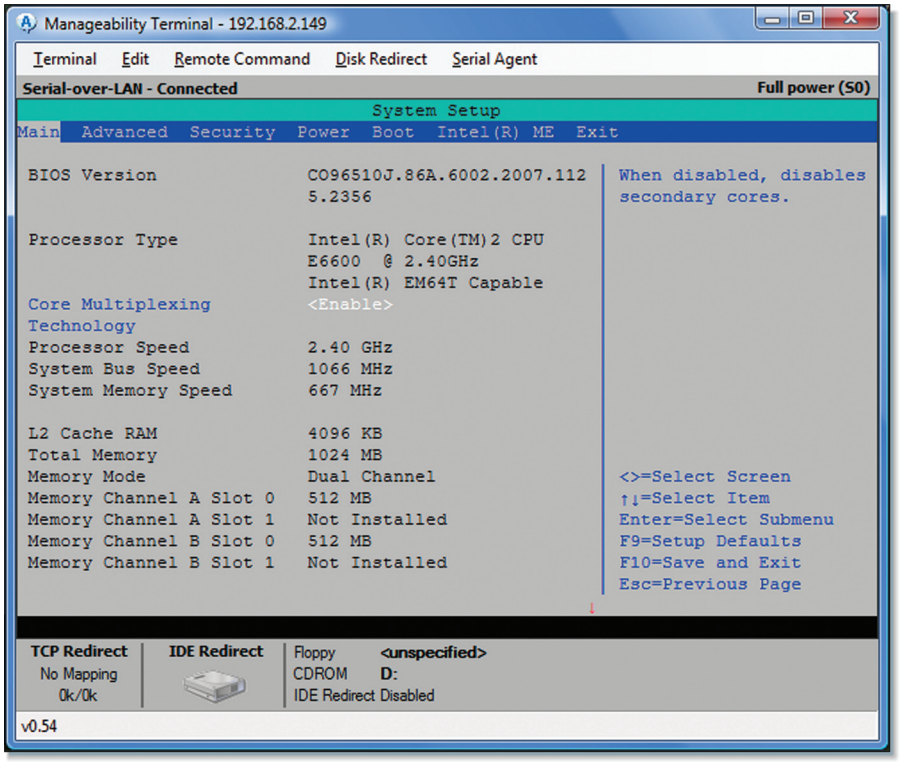

Figure 13.8 Remote BIOS Management Using Manageability Commander

The managed computer will abruptly reboot and after a few seconds, the computer's BIOS screen will show up on the terminal window as shown in Figure 13.8. At this point, the administrator can remotely navigate the BIOS screens and change the necessary settings. The F1 to F12 keys have different values depending on the BIOS, if the function keys don't work correctly, try going into the Terminal menu and select a different key translation from the Special Key Translation sub-menu. There are three possible translations and one of them will usually work.

The remote control menu allows easy access to most of the commonly used remote control operations, but the Custom Command option at the bottom of the remote control menu allows for all possible remote operations a computer can support. For example, on some computers, it's possible to enter the BIOS and lock the local user's keyboard.

Now, let's perform a normal reboot and have the managed computer boot into Microsoft Windows. Since the computer is now in graphics mode, the terminal will be blank and remote management operations are normally not possible using Serial-over-LAN when the operation system is running, but there is a way around this problem.

On the Intel AMT computer, install and run Manageability Outpost. This is an agent tool that usually runs as a background service, but can also run as an application. Once Outpost is running, select the Serial Agent tab and make sure the checkbox is enabled as shown in Figure 13.9.

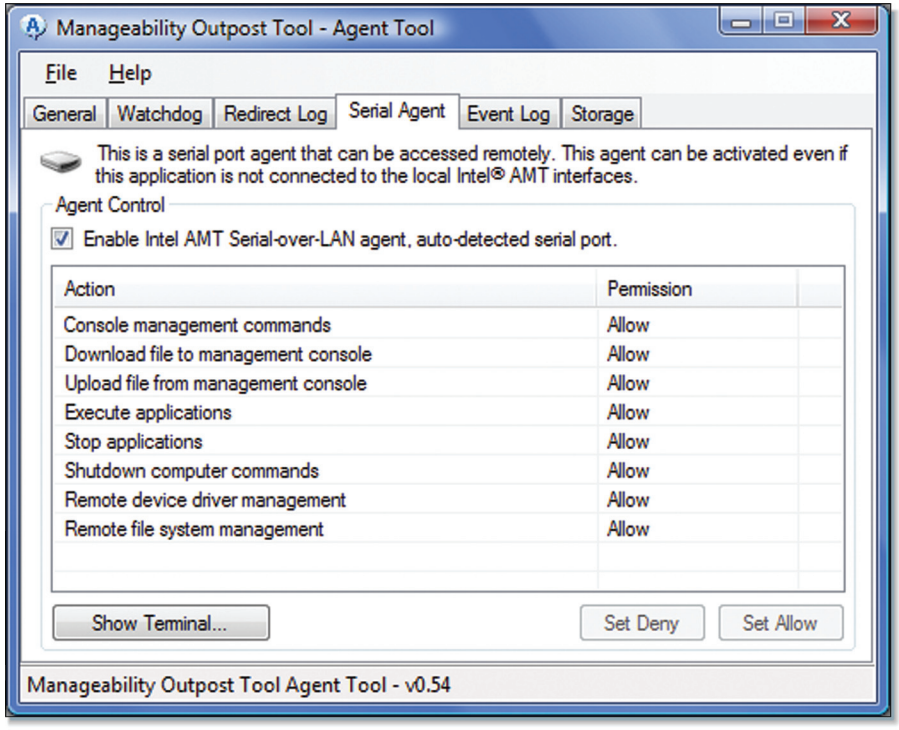

Figure 13.9 Manageability Outpost Serial Agent Is Enabled

When enabled, Outpost automatically finds the Intel AMT serial port and offers a remote management command prompt. The privacy controls in Figure 13.9 allow the local user to block some remote management operations.

As soon as Outpost is started, it will display a welcome screen to the remote administrator as shown in Figure 13.10. If the remote terminal is connected after Outpost runs, the administrator can cause the welcome screen to reappear at any time using the reverse apostrophe key (`). It's the key located above the TAB and left of the 1 key on US-English keyboards.

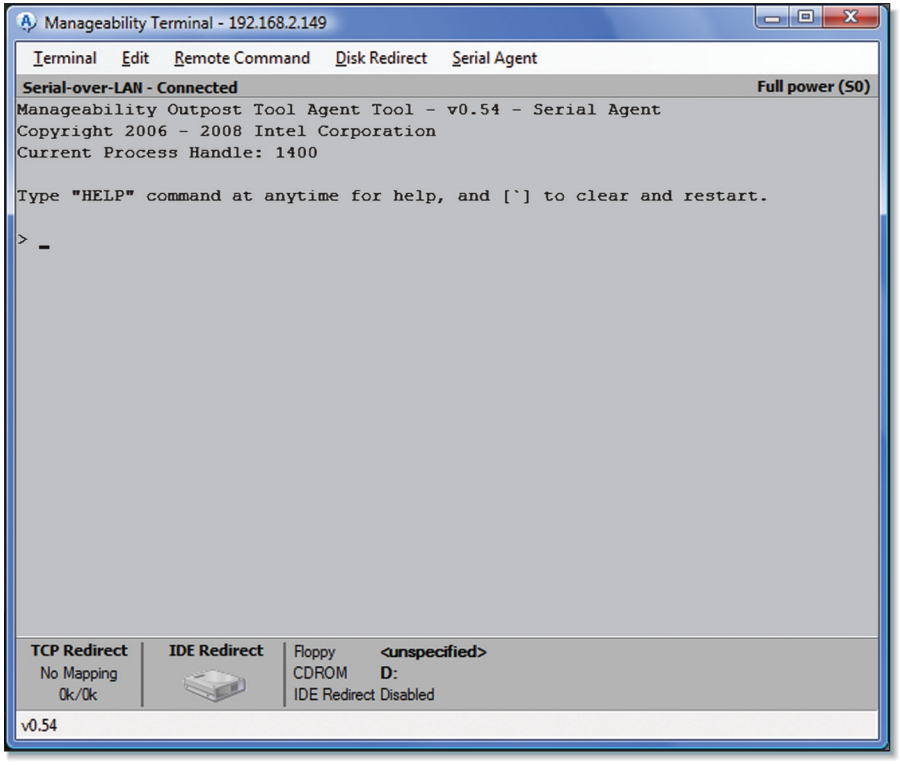

Figure 13.10 Manageability Outpost Command Prompt on the Administrator's Terminal

At this point, the administrator can type the `help` command and start remotely managing the computer. Commander and Outpost are also built

to talk to each other in a special way. When both Commander and Outpost are running, all the options in the Serial Agent menu above the terminal become active. Instead of enumerating, starting, and stopping processes using the command prompt, the Serial Agent menu includes a Process Monitor window that is much easier to use.

Now that we can remotely manage a computer using Commander and Outpost, we go on to the managed computer and disable all of the network drivers. Open a command prompt on the managed computer and type `ipconfig` to confirm that the Intel AMT computer has no IP address. Then, notice that Commander and Outpost still work. This is because Intel AMT has its own connectivity via an embedded network stack, separate from the operating system.

It's also possible to redirect TCP connections over Serial-over-LAN using the TCP Port Redirector in the Serial Agent menu. One good usage of this feature is to perform a VNC connection to a computer that has no working network stack. For instructions on how to do this, consult the tutorial video and user guide on the Manageability Developer Tool Kit Web site[1].

Intel® System Defense

Starting with Intel AMT 2.0, the administrator can manage a set of hardware network filters on each Intel AMT computer; this feature is called Intel® System Defense. Commander allows the administrator to add, remove, view, and activate network policies and filters. First, let's run the Manageability Net Status tool on the Intel AMT computer. This is a normal PING tool, no different from the PING command, but was built to be more user- and camera-friendly for onstage demonstrations.

In Figure 13.11, we elected to ping our own local router and the progress bars are moving to the right as traffic is being sent and received correctly. We will now attempt to use Commander to add a hardware filter to block this stream of packets. In Figure 13.12, we select the Policies folder and click Create New Policy.

1 http://www.intel.com/software/amt-dtk

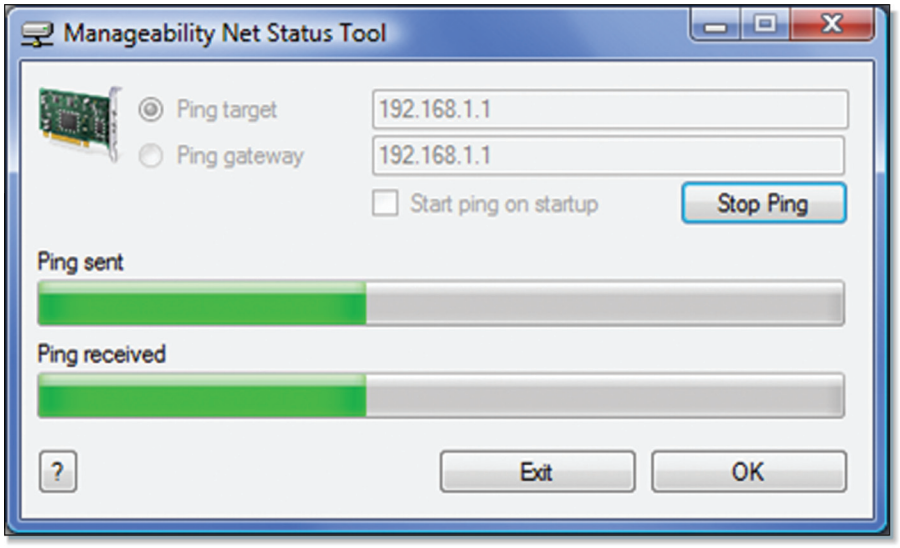

Figure 13.11 Manageability Net Status Tool Sending and Receiving Ping Packets

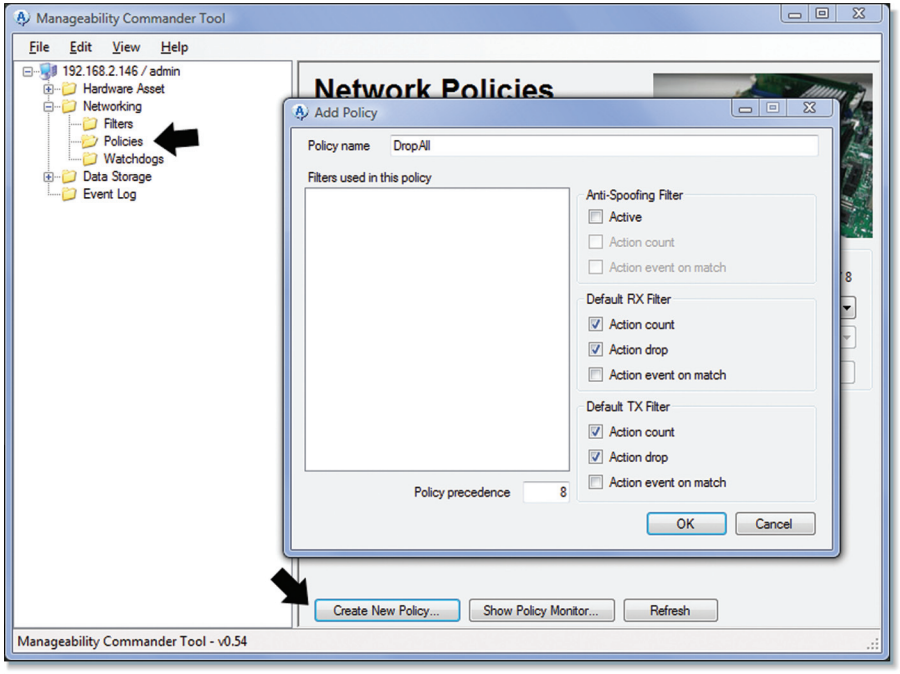

Figure 13.12 Adding a Network Policy with Commander

With Intel AMT, the administrator can create network filters and none, one, or many filters can be part of a network policy. Only one network policy can be active at any give time. In this first example, we create a policy with no filters. Packets are compared against all filters in the policy and if none of them match, the default action is performed. In our case, we will simply select drop and count defaults for both transmit and receive, we will call this policy "DropAll". Press OK to add this new policy to Intel AMT. At this point, the newly created policy is present in Intel AMT but not active.

To activate a network policy, select it in the tree view and press the activation button on the lower right of the screen, as shown in Figure 13.13. The preferred way to enable and disable a policy is to right-click the policy in the tree view and select it to enable or disable it. Once the policy is enabled, all traffic to and from the operating system will be dropped. The Net Status tool we started earlier will show that PING traffic is no longer getting a response. Right-clicking the policy and disabling it will cause the traffic to resume normally.

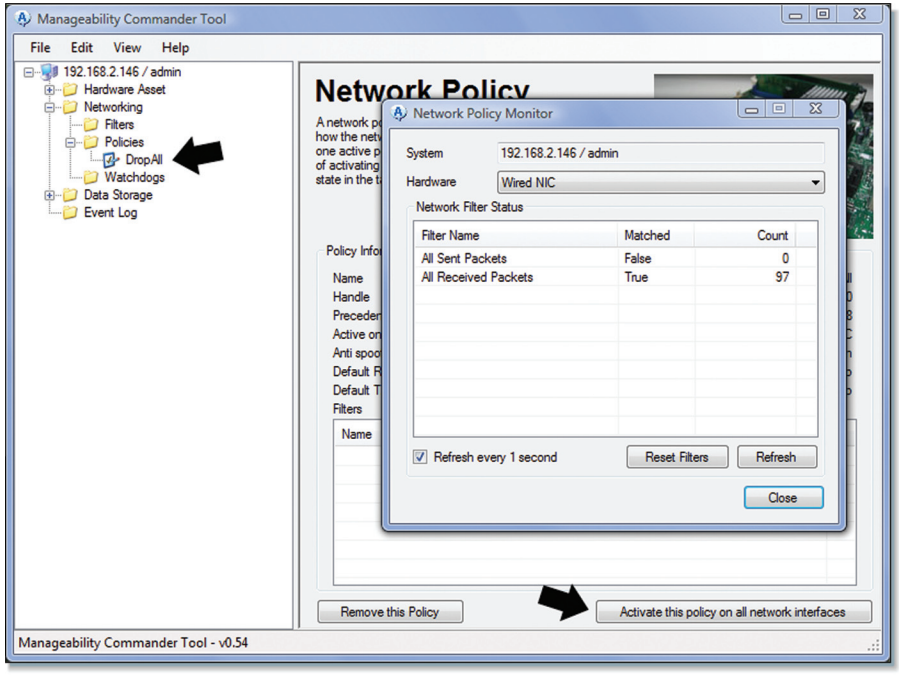

Figure 13.13 Activating a Network Policy and Viewing the Results

In Commander, we can also right-click a policy and select "Show Policy Monitor…" to display a window that will poll the Intel AMT network policy state and hardware counters. We can use this to see how much traffic is being dropped.

Once we understand how network policies work, we can add network filters to our policies. Select the Filters folder in Commander and click Create New Filter. In Figure 13.14, we have an example of a filter that will only count and drop inbound PING traffic.

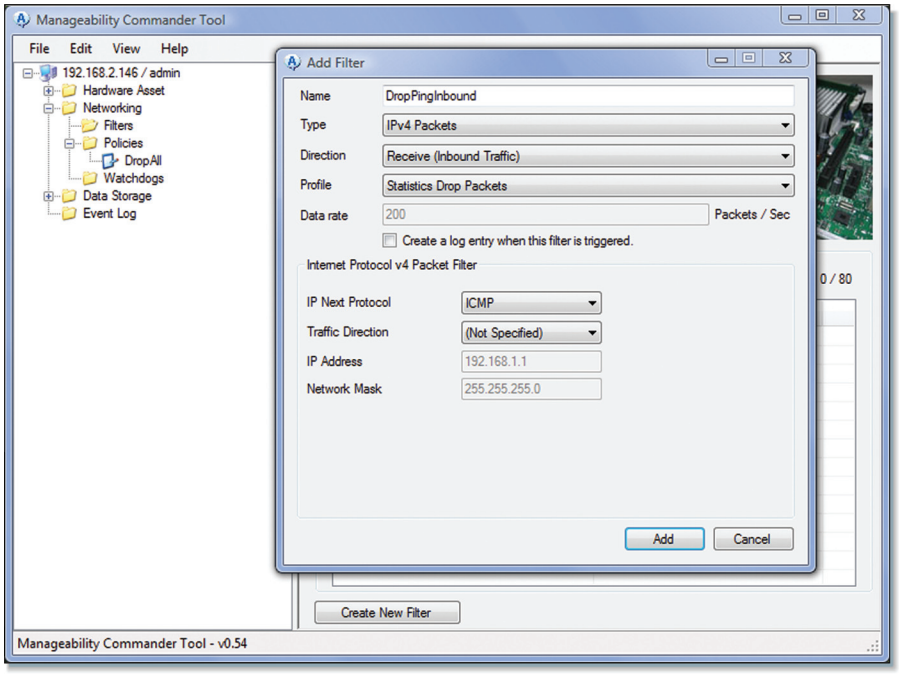

Figure 13.14 Adding a Filter to Block Only Inbound PING Traffic

Once we have created this filter, we can create a new policy that includes this new filter. Figure 13.15 shows how to do this. In this new policy, we will also select to count packets that don't match any filter as our default action. This allows us to see more counters in the policy monitor window.

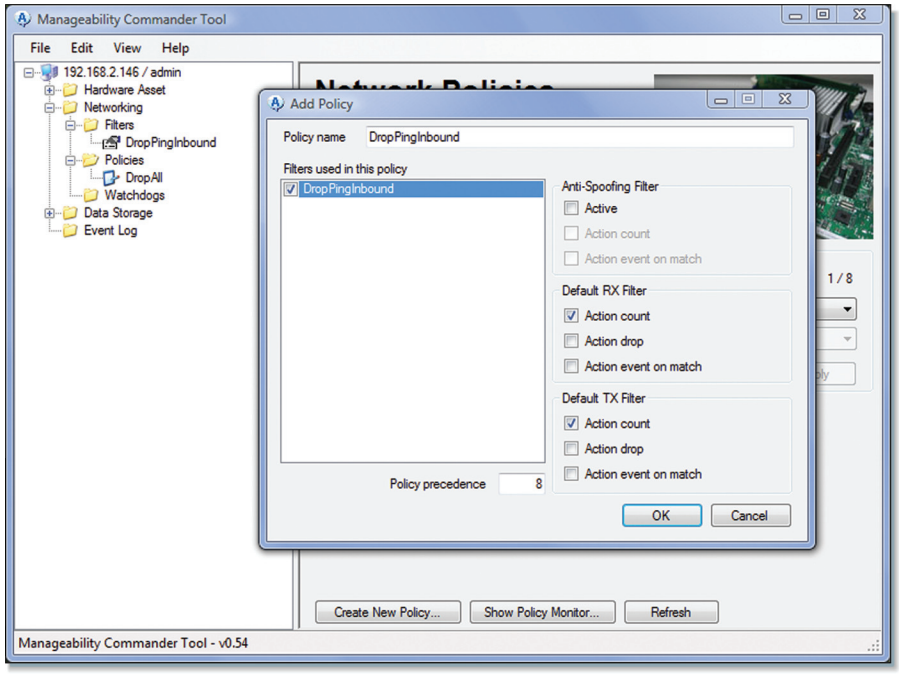

Figure 13.15 A Policy That Drops Only Inbound PING Packets

Summary

In this chapter we got hands-on experience with Intel AMT for the first time covering two of the main features of Intel AMT: Serial-over-LAN and Intel System Defense. The Manageability Developer Tool Kit (DTK) is a good starting point for people experimenting with Intel AMT for the first time or wanting to check the state of Intel AMT in the field. Users are encouraged to play around with Commander and Outpost. An extended user's guide and many tutorial videos are available on the Manageability Developer Tool Kit Web site, the same site where these tools can be downloaded.