Chapter 12

Internet Platform Management

The Internet is like alcohol in some sense. It accentuates what you would do anyway. If you want to be a loner, you can be more alone. If you want to connect, it makes it easier to connect.

— Esther Dyson, Interview in *Time Magazine*, October 2005

We have covered a wide array of Intel® Active Management Technology (Intel AMT) features, but until now all of the benefits of Intel AMT where only available to computers connected on a managed network. In this chapter we cover a new feature available starting with Intel AMT 4.0 called Client Initiated Remote Access (Fast Call for Help). Fast Call for Help is a secure VPN-like connection initiated from Intel AMT to a management server. Once the Fast Call for Help connection is established, this tunnel can be used to communicate with Intel AMT. Fast Call for Help opens a new world of possibilities for remote computer management since, for the first time on commonly available computers, the platform itself can securely connect back to a management server over the Internet. This is especially important with laptops that are often moved and connected to random networks and behind NAT routers. Having laptops move around is no longer an obstacle to using hardware-based network manageability.

This chapter first covers the environment detection feature of Intel AMT, which is important to understand and use Fast Call for Help. After that, we will talk about the Fast Call for Help protocol, how the Fast Call for Help connection is configured, triggered, and authenticated.

Environment Detection

Before going into Fast Call for Help itself, we must first review a feature that was first introduced with Intel AMT 2.5. At the time, having Intel AMT TCP ports open for connection, even if authentication was securely checked, was still a security issue. Imagine someone connecting a laptop with Intel AMT to a hotel room network and having someone in a different room scanning, finding, and attempting to attack the Intel AMT ports on the computer.

To counter the possibility of such an attack, the environment detection feature was added. It is configured with up to four home DNS suffixes and when the computer performs a DNS request, if the response indicates that the computer is in one of the home networks, the Intel AMT ports are open. Otherwise they are closed. Figure 12.1 shows how this works.

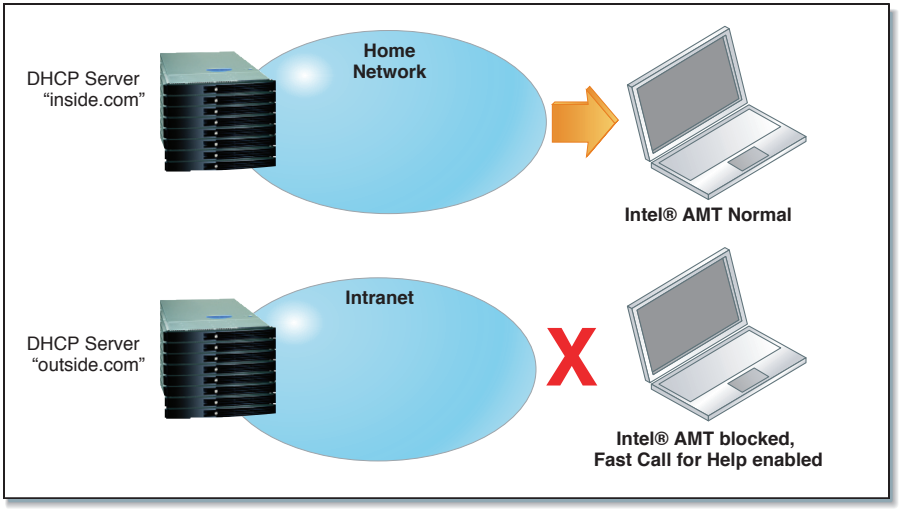

Figure 12.1 Environment Detection Turned On and Off. When On, Blocks All Intel® AMT Traffic.

Starting with Intel AMT 4.0, the same environment detection exists with a new twist. Instead of just blocking the inbound Intel AMT ports, the new Intel Fast Call for Help feature is enabled and the platform can now call home when policy requires. Figure 12.2 shows how the computer calls home and the administrator can access Intel AMT capabilities through a common server.

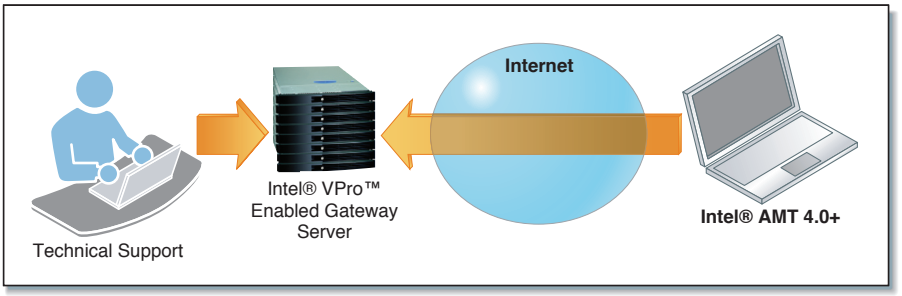

Figure 12.2 Intel® Fast Call for Help Used Over the Internet to Contact the Corporate Server

It is important to understand that Intel AMT 4.0 works exactly like previous versions of Intel AMT when the computer is connected to the native corporate network, the network of the organization to which the computer belongs.. This chapter covers Fast Call for Help, which is only active when the computer is detected to be outside the native corporate network. It's important because many people just starting out will forget to setup the environment detection feature correctly.

Manageability Commander, part of the Manageability DTK, can be used to set up the environment detection policies for a given computer. When trying this for the first time, it may be a good idea to first prepare two simple home routers with two different DHCP network names, one could be "inside.net" and the other "outside.net". Intel AMT would then be configured with "inside.net" as being part of the home network. With this setup ready, the Intel AMT computer can be moved from one network to the other.

Intel® Fast Call for Help Protocol

Intel Fast Call for Help is a TCP-based connection to a known and trusted administration server. The connection is always secured using TLS; this is true even if the computer with Intel AMT is configured in small business mode. Inside this TLS session is a binary protocol that is inspired but not compatible with the well known SSH port forwarding protocol.

As shown in Figure 12.3, the Intel AMT TCP ports (16992 to 16995) are forwarded through this tunneling connection but otherwise are used just like they would be used if Fast Call for Help connection was not in use. In addition, the same SNMP trap network alerts and WS-Management event notifications coming from Intel AMT are also forwarded through this tunnel connection.

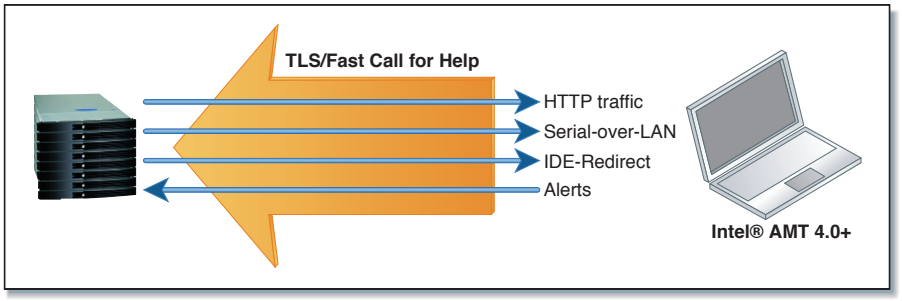

Figure 12.3 HTTP, SOL, IDE-R, and Network Alerts through the TLS Secured Fast Call for Help Tunnel

If the computer with Intel AMT is configured in enterprise mode with TLS enabled, the tunnel will then have two levels of TLS security. Figure 12.4 shows how the Fast Call for Help tunnel will be protected by TLS and will carry TLS secured HTTP, Serial-over-LAN, and IDE redirect traffic. The double security may seem a bit much, but since both levels of TLS authenticate different things, they are both useful. The TLS secured tunnel session authenticates the computers with Intel AMT and Intel vPro Technology enabled gateway. The inner TLS secured sessions authenticate individual Intel AMT users.

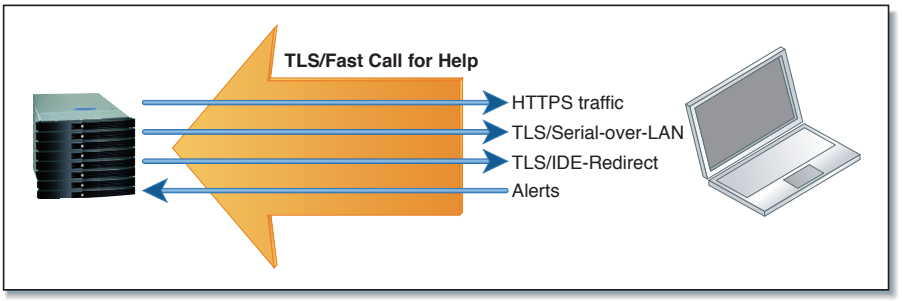

Figure 12.4 TLS Is also Used within the TLS Secured Intel Fast Call For Help Tunnel. TLS Is Applied Twice.

Intel Fast Call for Help connections are always outgoing connections and connect what is called an Intel vPro Technology enabled gateway. An Intel vPro Technology enabled gateway is a server or router that receives and processes Fast Call for Help connections. The Intel AMT SDK provides such software as reference, but for real deployments organizations should contact one of many vendors that have a product quality version of an Intel vPro Technology enabled gateway. In the Intel AMT SDK, the reference gateway software is called the Management Presence Server (MPS). Regardless of the version of the gateway that is used, in large organizations should be installed in the network DMZ, between the firewalls that separate a corporate network from the Internet. Figure 12.5 shows the reference MP Server installed in the corporate DMZ.

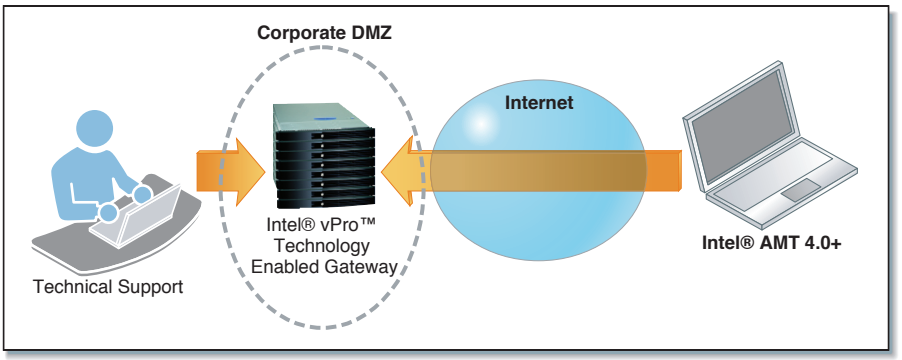

Figure 12.5 Intel® vPro™ Technology Enabled Gateway within the Corporate DMZ

An Intel vPro Technology enabled gateway acts as an intermediary between the management console and computers enabled with Intel AMT that are outside the intranet, routing management traffic within the Intel Fast Call for Help connection.

Intel® Fast Call for Help Policies

Since an Intel Fast Call for Help connection requires a new layer of authentication to verify both that the computer is managed by this server and that the management server is in fact the real one and not a fake. Fast Call for Help connections are also initiated by the computer with Intel AMT. Both the new authentication and connection triggers need to be configured by configuring the Fast Call for Help policies. In this section, we look at how the tunnel connection is triggered and authenticated and how to set up a computer with Intel AMT to use this feature.

Connection Triggers

A Fast Call for Help connection can be initiated in one of three ways. As shown in Figure 12.6, these three ways are: user initiated, periodic timer, or network alert. The policy can be set up to use any combination of these three connection triggers.

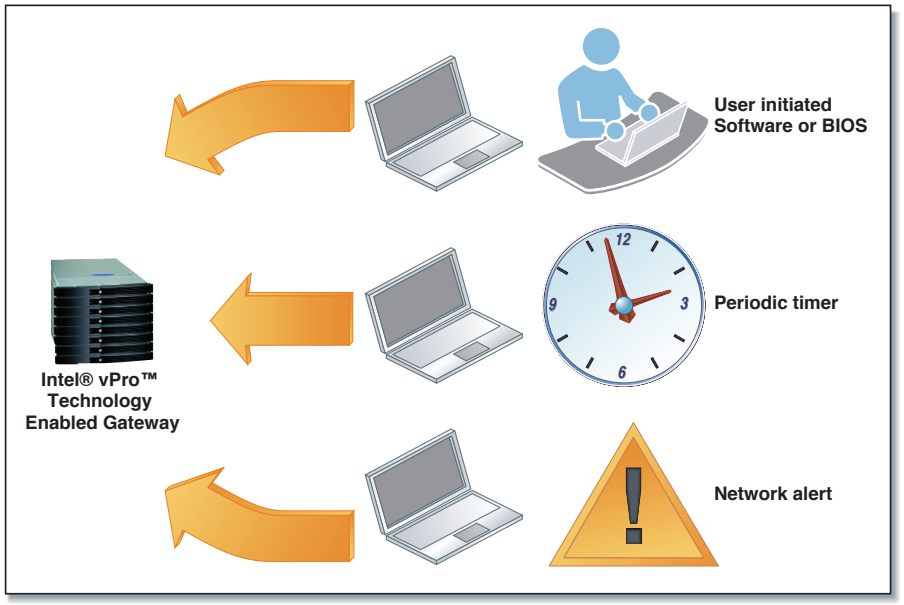

Figure 12.6 Three Connection Trigger Types

Using software like Manageability Commander or Intel SCS, an administrator can change policies. In Manageability Commander shown in Figure 12.7, we can connect to the computer with Intel AMT in the Management Engine tab and hit the Configuration button next to the Remote Management line. This will bring up the Fast Call for Help policy configuration dialog.

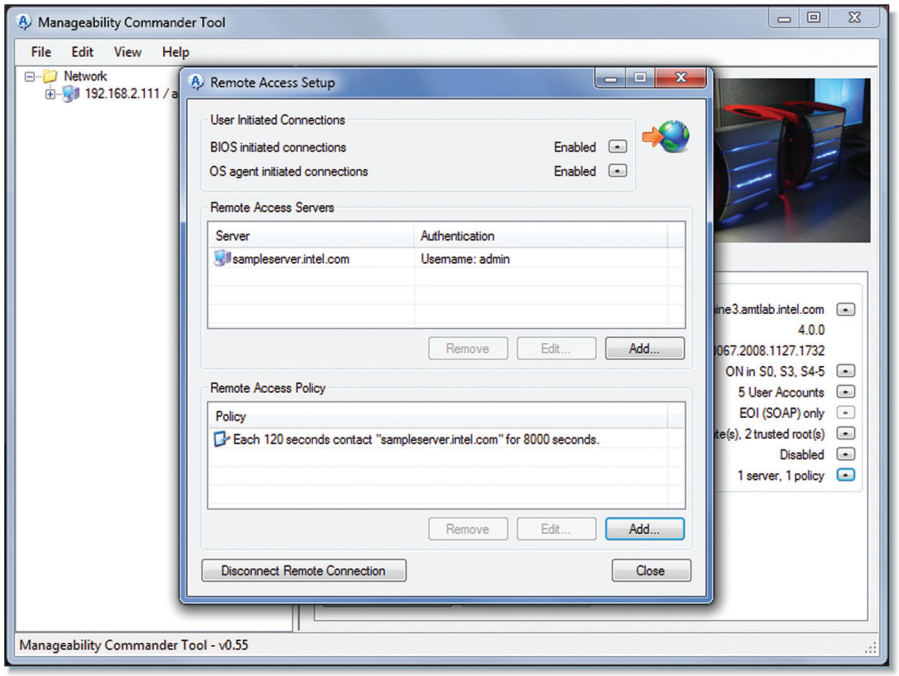

Figure 12.7 Fast Call for Help Policy in Manageability Commander

At the top of the screen, the administrator can control if the BIOS or OS tunnel connection initiation is allowed. In the middle of the screen is the configuration of the Intel vPro Technology enabled gateways, the servers that receive the Fast Call for Help connections. Lastly at the bottom of the screen is the connection action to perform for each of the three possible types of connection trigger. You can specify for each of the possible triggers to what server to connection to and specify a backup server if the primary one is not available.

The user initiated trigger can take one of two forms: the user can initiate Fast Call for Help from the BIOS or from the OS. The administrator has policy control to allow the user to initiate Fast Call for Help and allow or deny Fast Call for Help connections initiated by the BIOS or OS. Depending on the computer with Intel AMT, Fast Call for Help could also be user triggered using a combination of keyboard keys or a hardware button. Regardless of

how the user actually opts to trigger the Fast Call for Help connection, the way this works is that BIOS-initiated Fast Call for Help connections are connections that are initiated before the operating system is booted. Once the operating system is allowed to boot, any user triggered Fast Call for Help connection is considered to be initiated by the OS.

When looking at what Fast Call for Help policies are possible, we can also take note that Fast Call for Help is useful for both taking care of user problems and for passive monitoring of platforms. The main focus is often on the repair aspect of Fast Call for Help—a user gets into trouble and initiates a Fast Call for Help connection to ask for help. However, in most cases Fast Call for Help can be initiated every day using a periodic timer policy so that administrators have an opportunity to monitor the platforms' state and location from time to time.

Fast Call for Help Network Routing

Because Fast Call for Help connections are always initiated by the computer with Intel AMT, the management connection can work even if the computer is connected behind a network address translator (NAT). Figure 12.8 shows how the connection passes through standard routers.

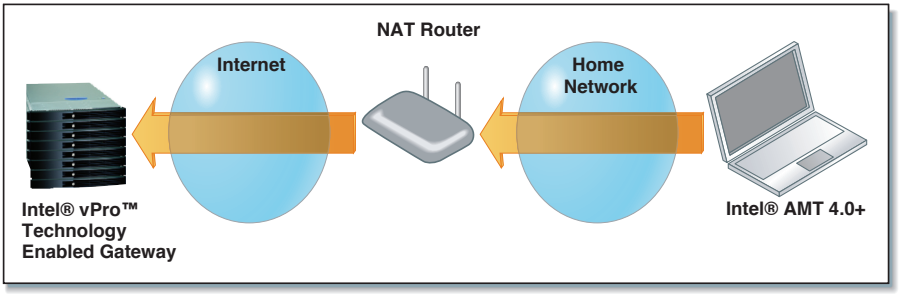

Figure 12.8 Intel® AMT behind a NAT Router

This setup is very common in home networks where the home is only assigned a single IP address and the home router translates private home addresses into global addresses. In such a setup outbound connections work, but

inbound connections are difficult or sometimes impossible. By using Fast Call for Help, Intel AMT gets around the NAT problems and so connecting the computer to most networks and launching a Fast Call for Help connection will work.

There are, however, limitations to Fast Call for Help. Outgoing Fast Call for Help connections can only be made on network interfaces that are connected to Intel AMT. So, like the rest of the Intel AMT features, adding a new USB network interface will not work. Also with Intel AMT 4.0, Fast Call for Help is only available on the wired interface and not wireless. So even if Intel AMT is correctly configured to work over wireless, Fast Call for Help will not work unless the wired Ethernet adapter is connected. Lastly, if the network has some type of access control on it, such as a redirected Web page that requires the user to accept a license agreement, PPPoE, PPPoA, 802.1x or any other authentication limitation, Intel AMT will not be able to use the network.

If a policy causes a Fast Call for Help connection be initiated but the network is not available, Intel AMT will try to connect three times before failing.

If for any reason the Fast Call for Help tunnel is unexpectedly disconnected, Intel AMT will attempt to reconnect automatically. This is why the Intel vPro Technology enabled gateway will not simply close the Fast Call for Help connection once it's done. To properly close a Fast Call for Help connection, a management console must call the "`CloseRemoteAccessConnection`" method on the RemoteAccessAdmin SOAP service. Calling this method causes Intel AMT to correctly disconnect the Fast Call for Help connection on its end.

Fast Call for Help Security and Authentication

Since Fast Call for Help is mostly used for connections over the Internet, security is a prime concern. Because Fast Call for Help is only enabled when outside the managed network and when Intel AMT inbound ports are all closed, Intel AMT itself is much less vulnerable to attack. In Figure 12.9, we review the authentication process. When a Fast Call for Help connection is established, TLS protocol negotiation starts first. This is exactly like the often used HTTPS protocol. TLS will first request and validate the Intel vPro Technology enabled gateway certificate. The MP Server certificate must be signed by a trusted root certificate, so setting up Fast Call for Help will require placing a valid trusted root certificate in the Intel AMT trusted certificate store.

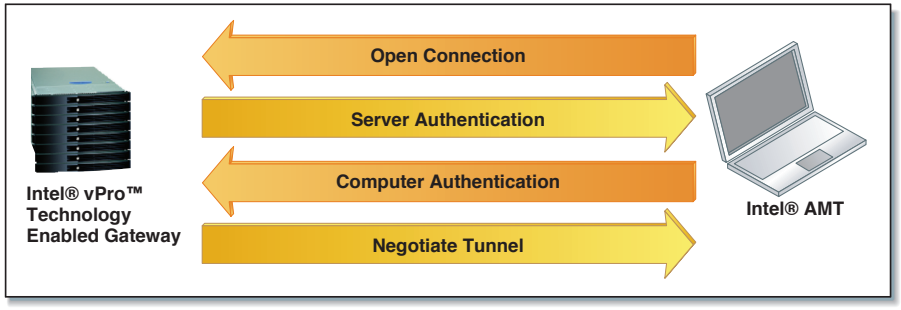

Figure 12.9 Overview of the Authentication Process

Once the Intel vPro Technology enabled gateway is connected, Intel AMT must now authenticate to the gateway. Figure 12.10 shows the two authentication systems supported by Intel AMT, either a certificate of its own or a username and password. It's important not to confuse the username and password used to authenticate Fast Call for Help with the Intel AMT user accounts. They are completely different. The Fast Call for Help uses a completely different set of credentials to authenticate the Fast Call for Help tunnel. Once established, the management console must authenticate through the tunnel to Intel AMT using a standard user account.

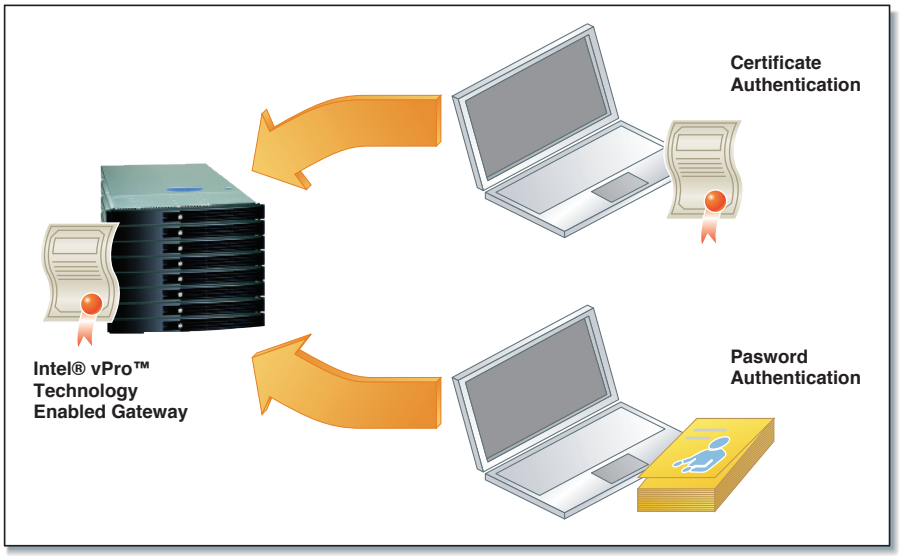

Figure 12.10 Intel® AMT Supports Both Certificate and Username/Password **Authentication**[1].

Fast Call for Help Connection

Once a Fast Call for Help connection is established between Intel AMT and the Intel vPro Technology enabled gateway, the management console must get to work. It would be very interesting for the management console to know why the Fast Call for Help connection was established in the first place, what trigger (User/Timer/Alert) caused the Fast Call for Help connection to be initiated. This information would be useful because if the user initiated the Fast Call for Help connection, help is probably required. On the other hand, if a network alert or periodic timer initiated the Fast Call for Help tunnel, the management console can probably just gather information about the platform or take action depending on the severity of the event.

1 The reference Intel® vPro™ enabled gateway included in the Intel AMT SDK only supports authenticating using certificates.

As it stands with Intel AMT 4.0, there is no easy way for the Intel vPro Technology enabled gateway or the management console to know exactly why an Intel AMT computer as established the Fast Call for Help connection, but this section will examine this question.

As of Intel AMT 4.0, Fast Call for Help policies allow up to four Intel vPro Technology enabled gateways to be configured and each trigger policy (User/Timer/Alert) allows each trigger to specify a primary and a backup Intel vPro Technology enabled gateway. Once connected, Intel AMT will not communicate with the MPS server until one of the three triggers causes the connection to be established. Figure 12.11 shows a sample policy. If a policy were set up where each trigger connects to a different MPS server, we would know which trigger caused the connection. Of course, this would require setting up a minimum of three Intel vPro Technology enabled gateways. We also know that if a Fast Call for Help connection is established because of a network alert or timer and the user causes Fast Call for Help to initiate a connection, the current Fast Call for Help session is closed and will be reconnected on the MPS server that is set for user initiated Fast Call for Help sessions.

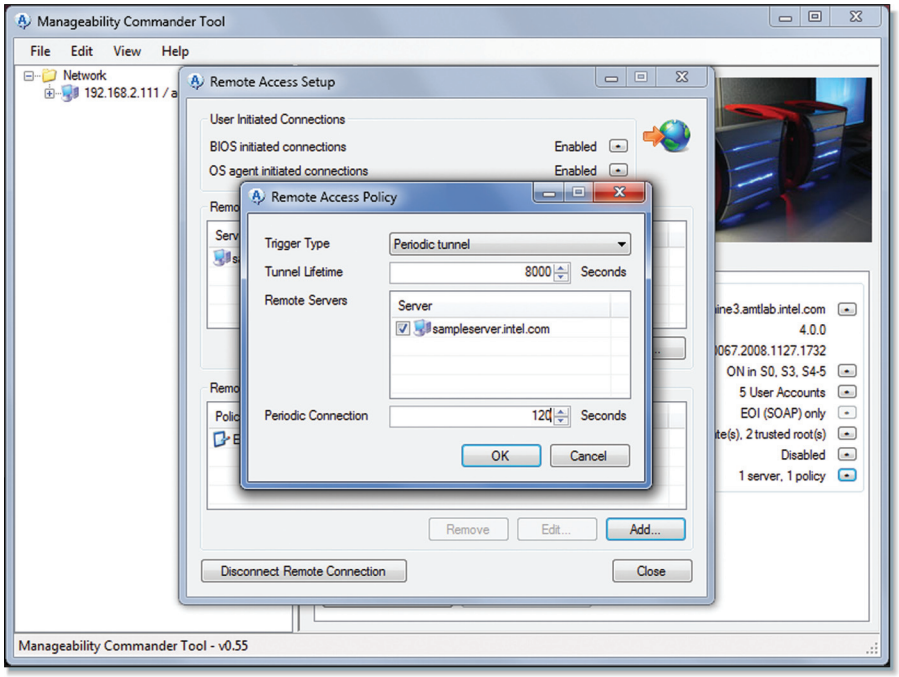

Figure 12.11 Typical Fast Call for Help Policy in Manageability Commander

Even if all the Fast Call for Help trigger policies are set to connect to the same Intel vPro Technology enabled gateway, you can still determine what caused the Fast Call for Help connection to be established in the first place. If the user manually initiates the Fast Call for Help connection, an event is also stored in the event log. A management console can read the event log and see that this event was placed in the log a short time ago and conclude that the user needs help.

If a network alert initiated the Fast Call for Help connection, that network alert will immediately be sent through the Fast Call for Help tunnel to the management console upon Fast Call for Help connection.

If the connection is due to the Fast Call for Help periodic timer policy, the event log will be clear of user help request events and no network alerts will be sent through the Fast Call for Help tunnel.

Intel® vPro™ Technology Enabled Gateway

The Intel vPro Technology enabled gateway that is included in the Intel AMT SDK is certainly not the only one; it is only provided as a reference. Vendors are encouraged to build their own to best suit their own product needs.

This section will take a quick look at the Intel vPro Technology enabled gateway that is included in the Intel AMT SDK, called MPS for Management Presence Server. It's important to understand its overall architecture before attempting to install it. Figure 12.12 shows the basic components once installed.

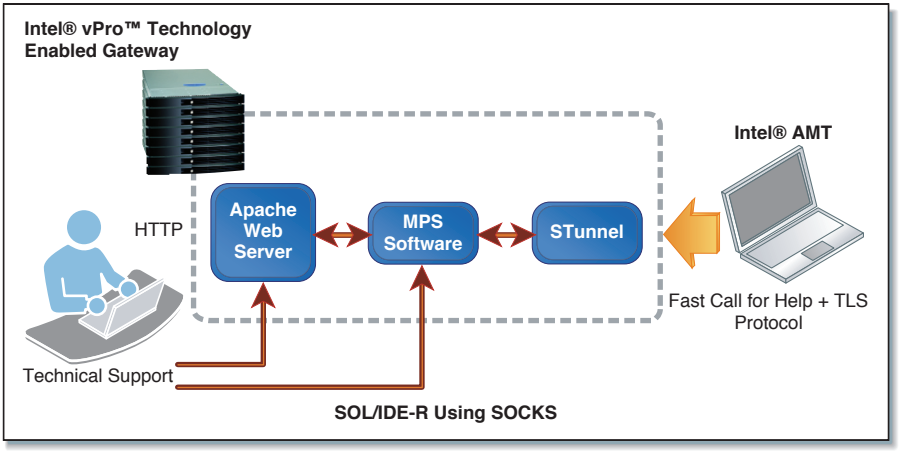

Figure 12.12 The Three Components of the Reference MPS Server Included in the Intel ®AMT SDK

The Intel vPro Technology enabled gateway included in the Intel AMT SDK is really three parts. First, an open source application called STunnel[2] receives the connection, performs certificate-related authentication, and forwards a non-secured connection to the MP Server proper. Second, MPS performs a conversion of Fast Call for Help traffic into the SOCKS protocol. Lastly, the Apache[3] web server acts as the middleman between HTTP requests made by the management console and SOCKS protocol required by the MP Server.

2 Stunnel is available at http://www.stunnel.org/

3 Apache web server is available at http://www.apache.org/

In order to perform serial-over-LAN and IDE redirect sessions, the console must be able to communicate using the SOCKS protocol directly. Figure 12.13 shows both HTTP and SOCKS protocols being used towards the server.

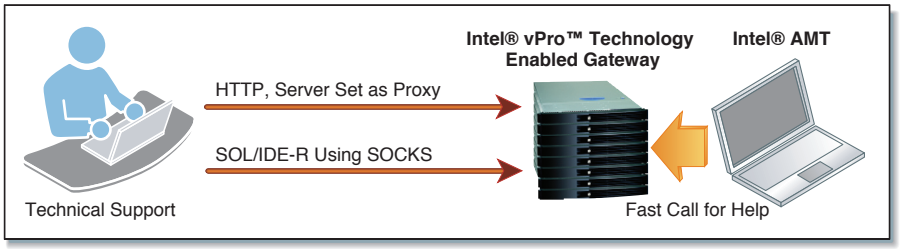

Figure 12.13 HTTP/SOL/IDER Used with Intel® vPro™ Technology Enabled Gateway

In order to simplify the task of adding SOCKS support to management consoles, SOCKS support was added to the IMRSDK.dll library. Management consoles will have to be slightly modified to support the new SOCKS support in this library.

Management consoles must also be modified to support sending HTTP management traffic to the Apache server just as if it were a proxy.

The Intel AMT SDK MPS can also be set up to send WS-Eventing alerts what a Fast Call for Help connection is established or dropped. Configuration to receive such events involves modifying the MPS configuration file. Figure 12.14 shows the server relaying network alerts to the administrator.

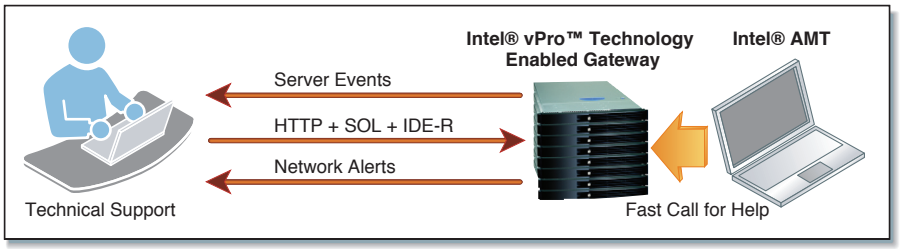

Figure 12.14 Intel® vPro™ Technology Enabled Gateway Events Inform the Console of Newly Connected and Disconnected Fast Call for Help Connections

There is currently no way to change the MPS event subscriber list on the fly or order to add or remove subscribers and no way to query MPS to list all existing connections. Of course, this is only a limitation of the reference Intel vPro Technology enabled gateway that is provided with the Intel AMT SDK. A different vendor's implementation can be made with much more functionality.

Manageability DTK and Fast Call for Help

The Manageability Developer Tool Kit (DTK) includes tools and features to help users test Fast Call for Help. Manageability Connector shown in Figure 12.15 is a simple tool that runs on the computer with Intel AMT and shows the current state of the platform environment detection, the Fast Call for Help connection and allows a user to trigger and disconnect the Fast Call for Help tunnel.

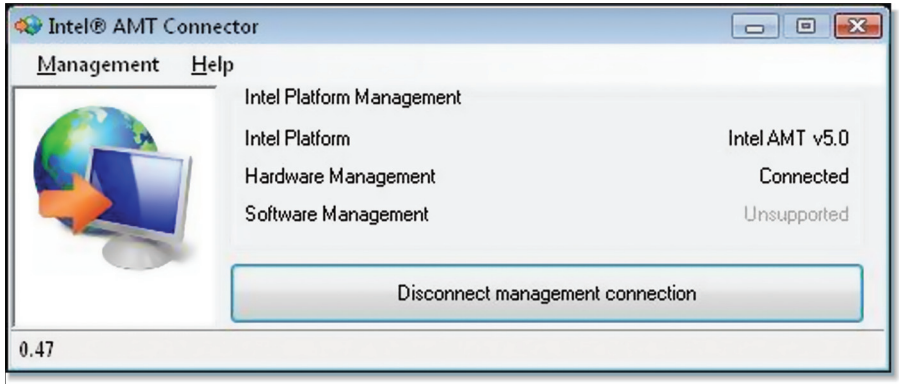

Figure 12.15 Manageability Connector

Users can also mix SDK and DTK tools, using Manageability Commander and Connector with the Intel AMT SDK's Intel vPro Technology enabled gateway. This is ideal when developing, installing, or testing the Fast Call for Help feature.

Fast Call for Help Network Speed

Management consoles will find that management operations through a Fast Call for Help tunnel and over the Internet are considerably slower than when performed on a fast local network without Fast Call for Help. Even if the Internet network connection used is relatively fast, the added latency, added processing work, and addition of an MP Server middleman will slow things down.

This slowdown will especially be felt when many network round trips are required and IDE redirect is going to feel this slowdown the most. The IDE redirect protocol relays data that is commonly transported over short and very fast wires inside a computer. Since IDE redirect makes many round trips; network administrators may opt to attempt to minimize the use of IDE-R over Fast Call for Help. One way to do this is to provide a recovery OS on the computer's hard disk or on a CD-ROM or flash drive.

Another consideration is that management consoles don't always use the HTTP protocol efficiently. Management software that open and close a HTTP session for each SOAP or WS-Management call may see a significant impact on performance. In the next section we explore exactly such a situation.

Fast Call for Help Considerations

Management consoles will be increasingly using WS-Management as the management protocol of choice for communicating with Intel AMT. For developers working on Microsoft Windows, an often used solution for quickly building WS-Management–compatible software is to use Microsoft WinRM[4] (Windows Remote Management). This is an ActiveX object that performs WS-Management operations on the network. Using WinRM works fine normally but developers will run into a problem when using WinRM with the Intel vPro Technology-enabled gateway provided in the SDK. Since the Intel AMT SDK Intel vPro Technology-enabled gateway acts like an HTTP proxy, developers will have to instruct WinRM to use the Intel vPro Technology-enabled gateway as an HTTP proxy. One way to do this is to use the "ProxyConfig" command line, but this is a global setting and will change how all applications using WinRM behave.

4 Microsoft† Windows XP requires a download. Look for "WS-Management v1.1" on the download section of the Microsoft Web site.

A possible solution for developers is not to use WinRM and instead try Openwsman[5] or use the C# WS-Management library that is built into the Manageability DTK[6]. Both these libraries will allow developers to target each WS-Management requests to a specific proxy or no proxy at all depending on what needs to be done.

Another benefit of using either OpenWSMAN or the Manageability DTK WS-Management stacks is speed. Both of these stacks support HTTP/1.1 pipelining that allows many requests and responses to be performed on a single HTTP connection. Microsoft WinRM will open and close an HTTP session for each WS-Management call that is performed resulting in many more network round trips and significantly reduced speeds.

Summary

In a world of increasingly mobile computing, being able to use the features offered by Intel AMT over the Internet on mobile devices is very valuable. All of the value of Intel AMT we have seen in previous chapters from monitoring and asset tracking to remote repair is not available over the Internet. Some companies are working on removing the notion of a trusted network altogether, and assuming that all computers are always connected on an un-trusted network. In such an organization, all computers, both desktops and laptops, would use Fast Call for Help all the time.

Moving forward, Fast Call for Help makes Intel AMT not only a great hardware-based manageability solution but is sometimes the only one that can be deployed and truly work.

5 Openwsman is available at: http://www.openwsman.org

6 Look for the WsManDIrectClient.cs file in the Intel® AMT DTK