vPro Prerequisites and Trade-offs for the dc7700 Business PC with Intel vPro Technology

Introduction

Intel vPro is a new technology designed to revolutionize the digital office. Intel vPro Technology allows for remote management of a PC regardless of system power state or operating system condition, as long as the system is attached to AC power and a network. Intel vPro also improves system security against malicious software attacks. Intel vPro's goal is to simplify back-office management and reduce IT-related expenditures.

As with any substantial new technology, questions arise about the requirements to utilize Intel vPro's benefits. There are certain prerequisites to use the features, and certain trade-offs that the IT professional should understand before deploying Intel vPro technology branded systems.

This white paper assumes some basic knowledge of AMT (Active Management Technology) and Intel Virtualization Technology compatible with Intel vPro technology.

HP Compaq dc7700p Business PCs initially shipped with AMT 2.0. AMT 2.1 is an important update that provides support for the Microsoft Vista operating system as well as power efficiencies. HP has updated this white paper to include the new features of AMT 2.1.

Prerequisites

An Intel vPro technology branded system has hardware, software, and firmware prerequisites.

Hardware

An Intel vPro technology system requires the following hardware:

- Intel Core 2 Duo processor (E6x00)
- Intel Q965 with ICH8-DO chipset
- Intel 82566DM Network Interface Controller

The HP Compaq dc7700p Business PC is an Intel vPro technology branded system that meets all Intel vPro technology hardware requirements.

The Intel Q965 chipset includes several devices that support AMT functions:

- Intel Management Engine (ME) Interface
- Serial-over-LAN
- IDE-Redirect

Some of these internal devices need drivers to function. See the Software section for more details.

Software

Required Operating System

Windows XP Pro with Service Pack 2 (32-bit version).

A Windows XP Pro software images require three deliverables:

- Intel ME Interface driver
- SOL driver
- LMS

Go to **www.hp.com** to check for the latest versions of these deliverables. AMT 2.1 support requires a new LMS deliverable.

Intel ME Interface (Intel Management Engine Interface)

The Intel ME Interface driver allows third party agents in the user operating system to communicate with the ME for out-of-band access to the non-volatile data store. All third party software products supporting Intel vPro technology may not utilize these operating system services.

The Intel ME Interface driver controls the management engine that enumerates under System Devices in Windows XP Device Manager.

SOL (Serial-over-LAN)

The SOL driver allows a management system to remotely display the keyboard interface of a managed client. The display is typically shown through a management console, and it emulates serial communication over standard network connection. This allows a management system to remotely control a client system. SOL is also known as KT (Keyboard and Text redirection).

The SOL driver comes as an INF file and contains the strings for device identification. The driver uses the SERIAL.SYS and SERNUM.SYS driver from Windows XP, and appears as a COM device.

LMS (Local Manageability Service)

LMS is a service that enables local applications running on AMT capable systems to use the same SOAP (Simple Object Access Protocol) functionality available to remote applications. LMS routes all traffic to the ME firmware through the ME interface.

LMS includes two components - the service and the system status. An AMT dialog box also displays at XP boot up, informing you that AMT is active. The dialog box contains a check box that allows you to prevent the dialog box from appearing in subsequent boots. This check box displays for each profile; therefore, if a new profile is created, the AMT dialog box displays for the new profile until it is disabled.

IDE-R (Integrated Drive Electronics Redirect)

The IDE-R is a function that allows a client system to access the ATA, ATAPI, and floppy devices on the management system. When booting through IDE-R, the client system ATA/ATAPI commands are forwarded to the management system and it will respond back to the client as if it issued the command.

The remote capabilities of IDE-R allow for client systems to load operating system or diagnostic images from a management system. The IDE-R interface is fully compliant with the ATA/ATAPI-6 specification.

At this time, IDE-R does not need a driver file. It is displayed as a real IDE controller during normal operation. When a remote IDE-R session is established, the Intel virtual driver string and device are shown. The

ME FW has the strings for device identification. IDE-R devices use the same mechanism as real IDE devices in Windows XP.

There may be a driver file associated with IDE-R in the future to assist with enumeration issues when in Compatibility mode for SATA hard drives.

Other Operating System Support

A firmware update will be made available sometime after the HP Compaq dc7700p Business PC launches that will include Vista AMT support. The HP dc7700p PC is enabled for Intel vPro Technology.

There are no plans for Intel vPro technology to support Vista Virtual Appliances. There is no support or Windows XP Pro x64 or older Microsoft operating systems.

Network Management Console Software

Providers of Network Management Console Software will need to update their current products to take advantage of new Intel vPro Technology, including AMT and future Virtual Appliances. Customers using network management console software should consult with the ISV they use regarding availability of updated software.

Firmware

To support future updates, the system BIOS may require an upgrade. Initial units shipped may not have full system BIOS support for the Vista operating system and XP-based virtual appliances. ME firmware may require an upgrade as well. Please check the HP support site for updated system BIOS, and work with your management console vendor for required ME firmware updates.

Initial HP dc7700p systems were shipped with the second generation Active Management Technology: AMT 2.0.

To take advantage of AMT 2.1 features, upgrade the system BIOS to at least BIOS 2.09 and ME firmware to at least ME firmware 2.1.0.1031. See the *HP Compaq Business PC with vPro Technology AMT 2.1 Firmware Update* white paper at **www.hp.com** for more information about updating the system BIOS and ME firmware.

VT is disabled by default in F10 Setup. You must enable it before you can use a third party Virtual Appliance. The VT option is located in F10 Setup under the following selections:

Security > OS Security > Intel Virtualization Technology

Setup and Configuration

All Intel vPro technology branded systems should be set up before deployment to enable AMT. AMT setup and configuration is also known as **Provisioning**.

There are several ways to set up a system:

- Purchase configured (pre-provisioned) systems from HP.
- Use a USB key in conjunction with a setup and configuration server console for one-touch deployment.
- Manually enter the data into the MEBx (Management Engine BIOS Extension) setup module.

Enterprise provisioning of AMT requires networking infrastructure, including DHCP, DNS, a Setup and Configuration console, and a management console. To utilize recommended security, Transport Layer Security (TLS) is required. Without TLS, AMT uses HTTP digest for security.

You can find more details about provisioning in the HP white paper, "vPro Setup and Configuration for the dc7700 Business PC with Intel vPro Technology" at **http://www.hp.com**.

AMT-capable systems that you deploy without being provisioning are vulnerable to attack, which can lead to full hijacked control of the system. This may require costly manual provisioning at a later time to use the AMT system again.

The IT administrator must keep pre-shared keys used in provisioning a secret. Stolen keys can be used in rogue provisioning servers to take control of systems.

HP will provide a fee-based customized service that will configure (pre-provision) AMT systems in the factory and securely provide pre-shared keys to the customer. HP offers a secured service that will eliminate manual setup/configuration (provisioning) of each unit at the customer site. Please contact HP for more information about this valuable service.

Hard Drive Layout

Intel vPro technology requires a separate hard drive partition for a future XP Pro based Virtual Appliances. This partition is known as the SOS (Service Operating System) partition. The Virtual Appliance in the SOS partition is a single binary image, and includes:

- Intel LVMM (Light-weight Virtual Machine Monitor)
- Virtual operating system
- Third party Virtual Appliance (if any)

The SOS partition is a 102MB partition of type 72h. It is not formatted or given a drive letter, has no file system, and cannot be directly accessed through Windows XP. It does not show up in Windows Explorer. However, the SOS partition is visible in Disk Management, so care must be taken to insure that it is not accidentally or maliciously deleted.

NOTE: Once a Virtual Appliance is installed in the SOS partition, its type will become 71h.

NOTE: Not all third party software products supporting Intel vPro technology offer Virtual Appliances.

At launch, HP Compaq dc7700p Business PC configurations will have a blank SOS partition. This partition is located at the end of the hard drive and is inaccessible. The main client operating system partition (COS) housing Windows XP is at the front of the hard drive, and the HP Backup and Recovery Manager partition is located behind the COS.

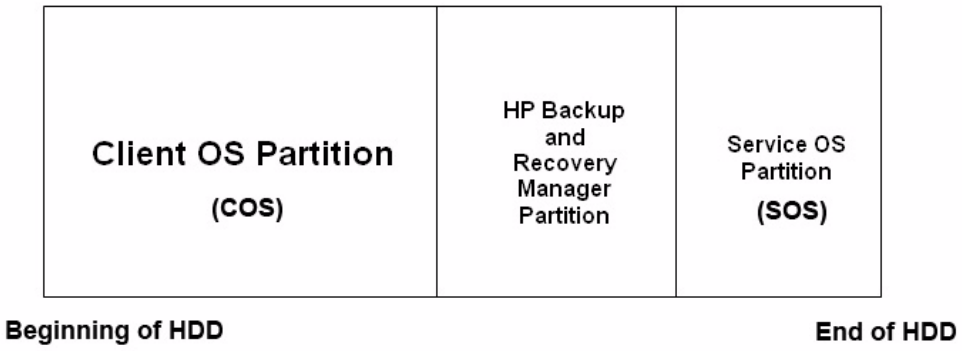

Figure 1 HDD partition layout

Customers who build their own images should be aware of the partition layout requirements for Intel vPro technology. The SOS partition must be exactly 102MB, be type 72h, not formatted, not enumerated, and located at the end of the hard drive.

Network Changes

Intel vPro technology requires usage of the embedded Intel 82566DM Network Interface Controller (NIC).

After a future Virtual Appliance is installed, PCI and PCI-e add-in NICs will no longer function. This is a security feature to prevent network traffic from add-in NICs bypassing the SOS. This may be a limitation for customers that require multiple NICs. However, USB NICs are not virtualized by the Intel LVMM, and therefore may circumvent installed Intel vPro technology compatible management and security appliances.

Memory Changes

The management engine requires that memory is populated in channel A. If memory is not populated in channel A, the ME cannot function and all AMT or ASF features are lost. A POST error message displays if memory is not populated in channel A. If this occurs, power off and unplug the system so memory can be reconfigured.

The POST error is as follows:

2211-Memory not configured correctly for proper MEBx execution.

Make sure there is a memory module in the black DIMM socket.

The DIMM slots for the Compaq dc7700 Business PC are color coded. The first DIMM slot in channel A is black and all other DIMM slots are white. Populating a DIMM in the black slot insures memory is in channel A.

For more information, see **"Memory Subsystem Changes" on page 7**.

MAC (Media Access Control) Address

The HP Compaq dc7700 Business PC has two MAC addresses, one for the NIC and another for the ME. This is a change from previous HP Business PCs, which had only one MAC address for the NIC.

Trade-offs

Intel vPro technology delivers many benefits for IT professionals and everyday users. However, as with many new technologies, these benefits are not without trade-offs.

Memory Subsystem Changes

The management engine uses system memory, much like UGA graphics. It can take up to 16MB from the operating system, not including any installed software running under the operating system or LVMM.

Virtualized appliances consume additional system memory, resulting in less usable memory for Windows XP. The amount of memory depends on the application, but can be as high as 100-200MB. The IT administrator might want to consider a minimum of 1GB system memory for use with future virtual appliances.

Since the ME requires power in all sleep states, the memory slots remain powered at all times. The only safe way to add or remove memory modules is to first unplug the unit from A/C power. Failing to do so can cause damage to the system, memory module, and possibly the person changing the memory.

CAUTON: Unplug the system before removing or inserting memory modules.

Refer to HP service and support documentation before installing or removing memory modules.

Power Consumption

Once a system is set up and configured (provisioned), the ME and system memory require power even in the sleep states (S3 Standby, S4 Hibernate, and S5 Off). Because of this, an AMT-enabled system consumes more power than a non-AMT system.

The additional power consumption is minimized with the Wake-On-ME feature implemented in AMT 2.1. Wake-On-ME allows the ME to be in an off state while the system is in the S3-S5 sleep states except when there are pending management functions. The user can set the time out value for the ME to go to sleep in the MEBx.

You can find more details on Wake-On-ME in the *vPro Setup and Configuration for the dc7700 Business PC with Intel vPro Technology* white paper, located at the HP Web site at: **www.hp.com**.

AMT vs. ASF

The HP Compaq dc7700p Business PC can support both AMT and ASF (Alert Standard Format). Once AMT is provisioned, ASF is no longer available (and vice-versa). AMT provides equivalent or better alerting and remote control capabilities with supporting management console software. Customers and IT professionals must determine which management standard is right for them.

Comparison of AMT vs ASF Capabilities

Capabilities	AMT	ASF
OOB (Out Of Band) Management	Yes - From any power state (S0, S3, S4, S5)	Limited - System must be in S0, needs to be remotely woken first
Remote Control	Yes - SOL, IDE-R, reboot, wake, shutdown, and more	Limited - Remote reboot and wake only
Event Alerting	Yes - Preset (restrictive)	Yes - Policy based (flexible)
Non-Volatile Storage	Yes - Third Party Data Store (3PDS)	No
Event Logging	Yes	No
Remote Boot	Yes - PXE or IDE-R	Yes - PXE
Asset Information	Yes - HW and SW	No
Remote ME FW Update	Yes	No
Secure Communication	TLS / HTTP Digest	Simple Authentication
Connection Protocol	HTTP (Accessible by Web browser)	RMCP
Layer 4 Stack	TCP (Preferred routing protocol)	UDP (Often blocked by routers)
Broad Enterprise ISV Support	Yes	No

Network Performance Impact

The installation of a virtualized appliance causes the NIC device to dynamically change device IDs. This should result in "New hardware found" messages and the installation of different virtual drivers.

Intel NIC Vendor ID, Device ID, and description string:

- Physical - 8086 / 104A "Intel 82566DM Gigabit Network Connection"
- Virtualized - 8086 / 10B7 "Intel Pro/1000 vVE Network Connection"

This causes redirection of user networking I/O to the virtual partition, which can impact network traffic performance. Third party appliances that inspect network packets will impact this further.

Third Party Appliances

Intel vPro technology only supports a single virtual appliance for now. The customer will need to select the right VA to suit their needs.

There could be some minor impact to runtime power consumption and suspend/resume latencies due to virtualization of processor registers required for these features.

Hard Drive Capacity Loss

Intel vPro technology branded HP Compaq dc7700p Business PC configurations include an SOS partition. This partition uses 102MB of hard drive space even with no virtual appliance installed.

If Intel vPro technology is not longer desired, the hard drive space used by the SOS partition cannot be reclaimed into the COS partition with the hard drive layout in the shipping configuration. The SOS partition is separated from the COS partition by the HP Backup and Recovery Manager partition. To reclaim the SOS partition into the COS partition, the HP Backup and Recovery Manager partition must also be reclaimed for one contiguous drive space. See **"Hard Drive Layout" on page 5** for partition placement.

Hard Drive Duplication

There are limitations in the way you can duplicate hard drives using duplication software (for example Symantec Ghost), once a virtual appliance is installed. Because of the LVMM and the way it boots, hard drive cloning through software means is only possible for same sized hard drives.

Corporate customers planning on image deployment over systems with different hard drives must be aware of this limitation. You can properly duplicate only hard drives of the same size once a VA is installed.

HP Backup and Recovery Manager Behavior

HP Backup and Recovery Manager is a backup and restore application designed to make backup images of the hard drive and restore them if needed. The SOS partition is not backed up or restored by HP Backup and Recovery Manager.

Driver and Service Verification

To verify AMT drivers and services are loading properly, look for them in Device Manager or Services.

Intel Management Engine Interface

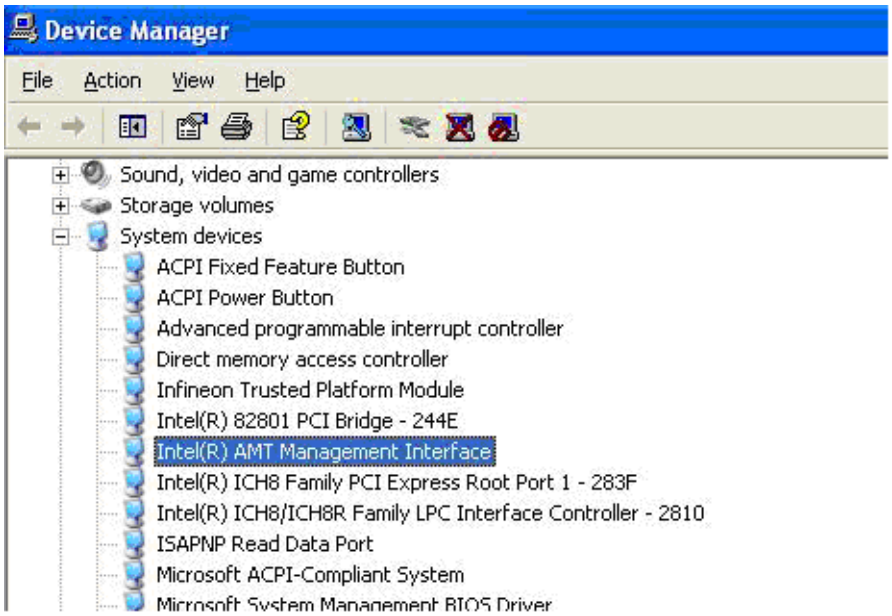

Figure 2 Intel ME Interface in Device Manager

Serial-over-LAN

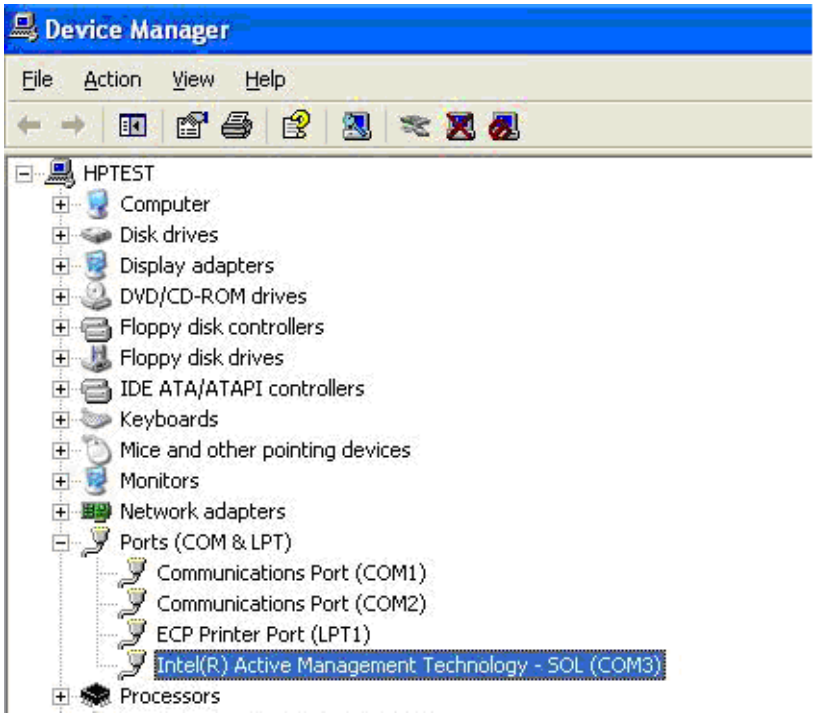

Figure 3 SOL in Device Manager

The COM port assigned to SOL can vary. It does not have to be COM3.

Local Manageability Service

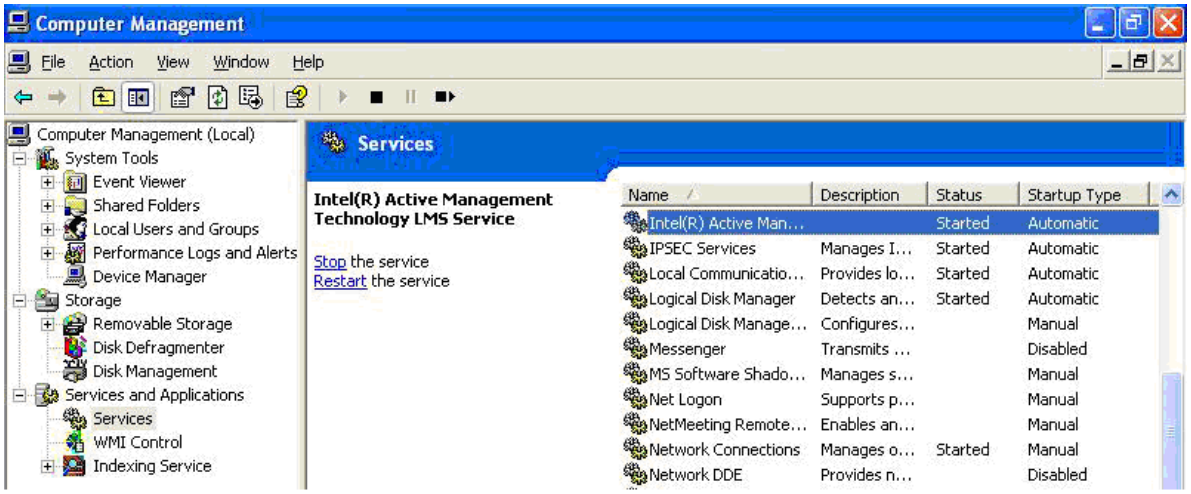

Figure 4 LMS in Services

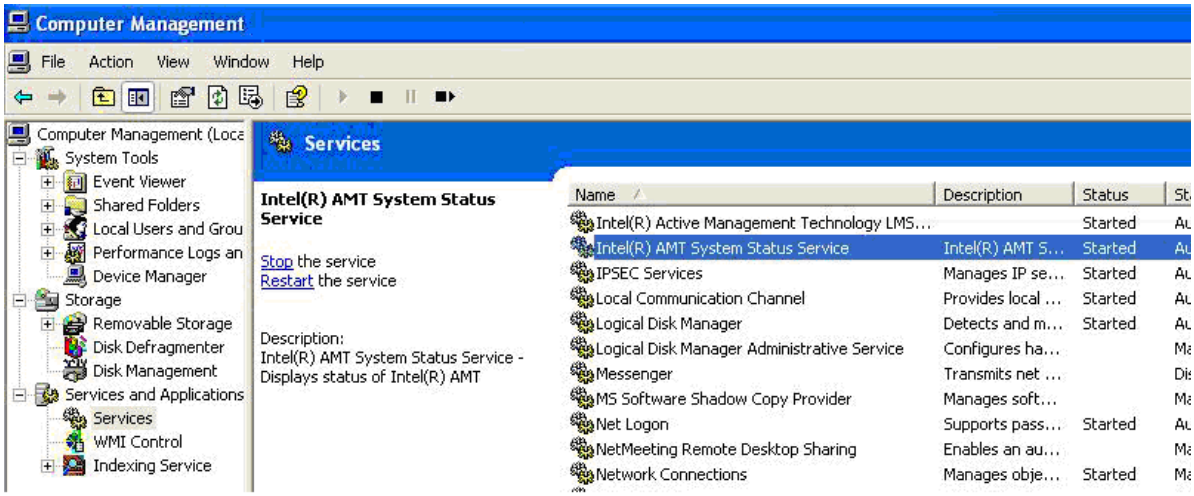

Figure 5 AMT System Status Service in Services

Figure 6 AMT Status check box

IDE-Redirect

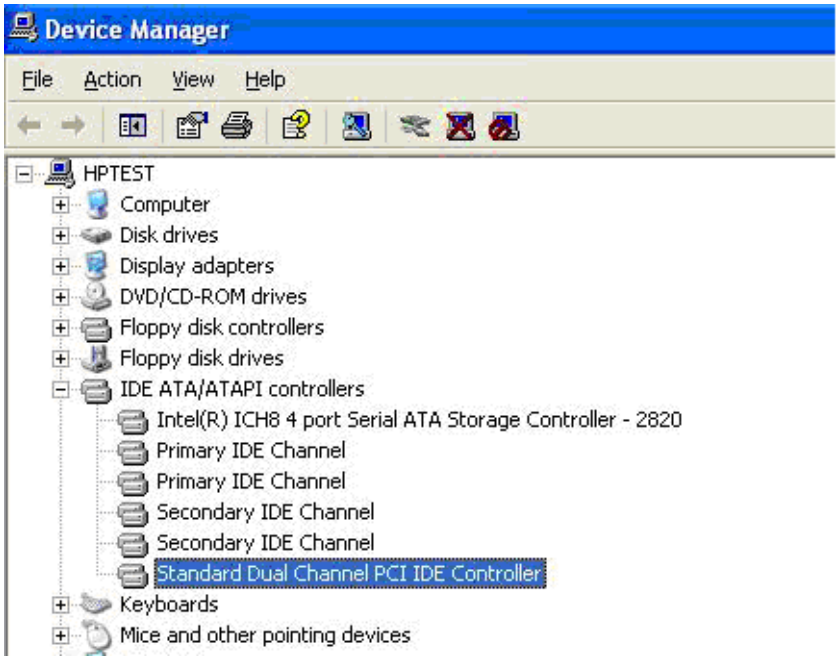

Figure 7 IDE-R during normal session in Device Manager

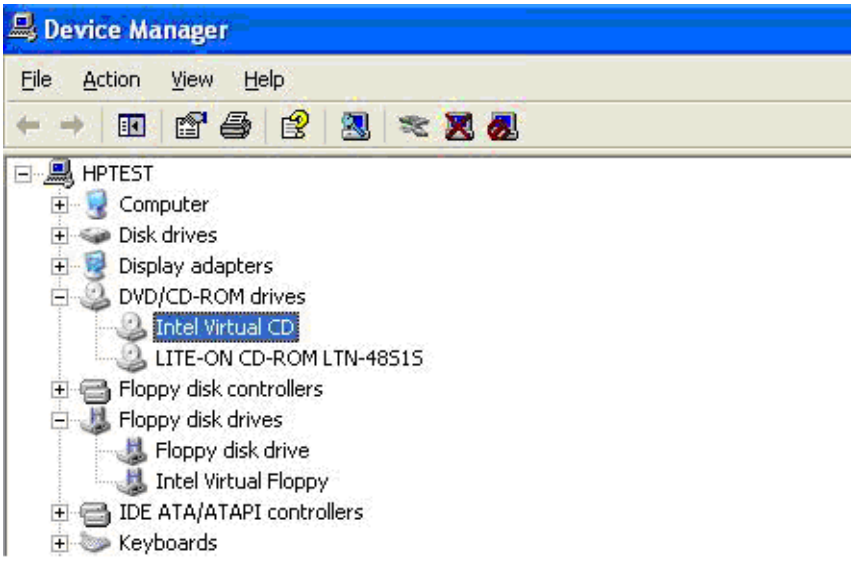

Figure 8 IDE-R (CD-ROM and Floppy) during redirected session in Device Manager

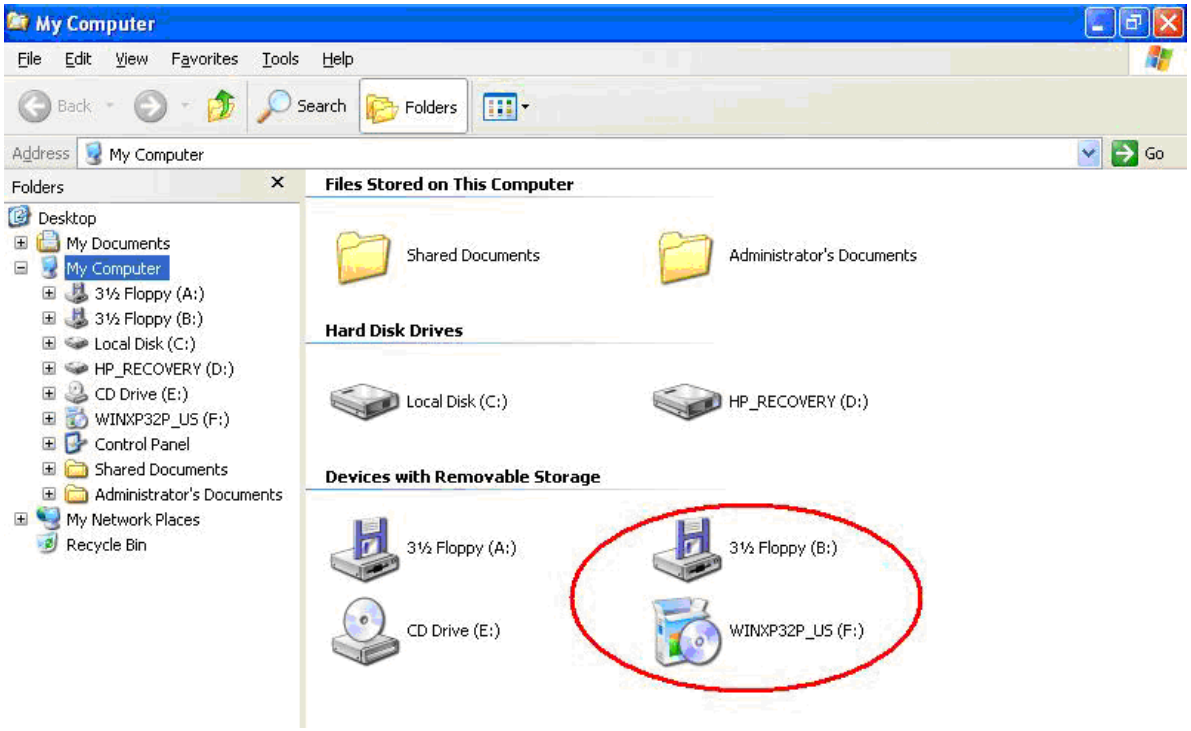

Figure 9 Explorer showing IDE-R floppy and CD-ROM drive

The virtual drives and any media within them will show up in Windows Explorer. A system can be directed to boot from the virtual drive and media.

434478-002, 2/2007