HP Compaq dc7800p Business PC with Intel vPro Processor Technology and Virtual Appliances

Introduction

Intel vPro Processor Technology* is designed to improve management of PC systems and provide proactive security. It is a combination of Intel AMT (Active Management Technology) and Intel VT (Virtualization Technology).

Intel AMT provides several defense mechanisms against malicious software attacks:

- System Defense to monitor and control network traffic.
- Network Outbreak Containment to isolate a compromised system.
- Agent Presence to detect malfunctioning software.

In addition to the system protection Intel AMT provides, the hardware virtualization capabilities of Intel VT allows for a "virtualized layer" of protection. This virtualized layer protection is accomplished by what is known as a Virtual Appliance (VA).

The HP Compaq dc7800p Business PC is Intel vPro Processor Technology compliant.

The HP Compaq dc7700p Business PC is fully Intel vPro Processor Technology compliant and readily supports Virtual Appliances with the appropriate BIOS update. See **"BIOS Requirements" on page 3** for *details.

*The HP dc7800p and dc7700p PCs are enabled for Intel vPro Processor Technology. Some functionality of this technology, such as Intel Active Management Technology and Intel Virtualization Technology, requires additional 3rd party software to run. Availability of future "virtual appliance" applications for Intel vPro Processor Technology is dependant on 3rd party software providers. Compatibility of this generation of Intel vPro Processor Technology-based hardware with future "virtual appliances" and Microsoft Windows Vista operating system is yet to be determined.

What is Virtualization?

Virtualization is an abstraction layer that separates physical system resources from an operating system. It allows a single processor to run multiple operating systems simultaneously and independently through the use of a Virtual Machine Monitor (VMM). A VMM is also known as a hypervisor and is software that handles the sharing of system resources between different operating systems running beneath it.

Intel Virtualization Technology (VT) provides hardware support for virtualization. This simplifies the need for complex VMM software. A Light-weight Virtual Machine Monitor (LVMM) can be used instead of a full VMM.

What is a Virtual Appliance?

A Virtual Appliance is a virtualized environment that runs independently yet concurrently with the Client Operating System (COS). It is transparent to the COS and the user. The purpose of a VA is to protect the COS from malicious software attacks and provide automatic security updates without user intervention.

A VA is composed of several components: an LVMM, a Service OS (SOS), and embedded applications. The LVMM, along with Intel VT, virtualizes the VA from the COS. The SOS executes the embedded applications within the VA. Using a management console, IT personnel can control a VA. VA packages are available through third party vendors such as Symantec or Altiris.

Virtual Appliance Generations

Virtual Appliance 2.0 features include:

- SOS based on Windows CE 5.0
- COS is Windows XP 32-bit
- Supports AMT 2.1 and later

The HP Compaq dc7700p Business PC shipped in 2006 and will have a VA 2.0 compliant BIOS available in September 2007 (see **"BIOS Requirements" on page 3**).

The version of VA 2.0 on the HP Compaq dc7700p is VA 2.0.1, which is VA 2.0 with an Intel LVMM hotfix. For the purposes of this white paper, VA 2.0 is listed to avoid confusion. See **"Known Limitations" on page 11**.

Virtual Appliance 2.6 features include:

- All features of VA 2.0
- Support for AMT 3.0

VA 2.6 is backwards compatible with VA 2.0 and supports both HP Compaq dc7700p and dc7800p Business PCs. The HP Compaq dc7800p Business PC shipped in 2007.

BIOS Requirements

The HP Compaq dc7800p Business PC uses the 786F1 BIOS family. Use BIOS version 1.04 or later for best compatibility and performance with VA 2.6.

The HP Compaq dc7700p Business PC uses the 786E1 BIOS family. Use BIOS version 3.03 or later for best compatibility and performance with VA 2.0 and VA 2.6.

Intel Virtualization Technology must be enabled in F10 Setup before a VA can be launched. VT is disabled by default in F10 Setup.

A VA can be installed with VT enabled or disabled, although some VA installers may warn users that VT is disabled during installation. If VT is disabled during installation, enter F10 Setup and enable VT after the installation is complete.

There are two kinds of Intel Virtualization Technology: VTx and VTd.

Intel Virtualization Technology for IA-32 processors (VTx) deals with virtualization at the processor level. This must be enabled for a VA to function.

Virtualization Technology Directed I/O (VTd) is an extension of VTx and deals with virtualization at the chipset level. VTd provides the capability to control DMA accesses and direct them to specific domains which are regions in physical memory.

All Core 2 Duo processors support VTx. More advanced versions of Core 2 Duo also support VTd in addition to VTx. Depending on which VT is supported by the processor, one or both options may appear in F10 Setup.

The VT options are located in the **Security** tab in F10 Setup.

For the HP Compaq dc7700p Business PC, go to:

- **Security > OS Security > Virtualization Technology (VTx)**

For the HP Compaq dc7800p Business PC, go to:

- **Security > System Security > Virtualization Technology (VTx)**
- **Security > System Security > Virtualization Technology Directed I/O (VTd)**

If the processor supports Intel Trusted Execution Technology (TxT), then that option will also appear under **System Security** below the VT options on a HP Compaq dc7800p Business PC. TxT is a processor feature that protects data on the system and verifies that the system is loading from a known safe state. TxT is not required for VA2.0 or VA2.6.

BIOS Recommendation

HP recommends that administrators set an F10 Setup password and a MEBx password when deploying Virtual Appliances. HP also recommends that IT administrators disable **Removable Media Boot** in F10 Setup, located at: **Storage > Storage Options > Removable Media Boo**t

This prevents malicious users from bypassing the SOS boot.

Hardware Requirements

An Intel vPro processor technology capable system is required to use a VA.

VA 2.0 requires the following hardware:

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

A TPM is needed for VA 2.0 is to hash the VA boot record. It has to be unhidden, but does not have to be enabled.

VA 2.6 must have the following hardware:

- Intel Core 2 Duo processor (E6x50)
- Intel Q35 with ICH9-DO chipset
- Intel 82566DM Network Interface Controller
- 1.2 TCP compliant TPM

The HP Compaq dc7700p Business PC is an Intel vPro processor technology branded system that meets all Intel vPro processor technology hardware requirements and supports VA 2.0 and VA 2.6 with the appropriate BIOS update.

The HP Compaq dc7800p Business PC is an Intel vPro processor technology branded system that meets all Intel vPro processor technology hardware requirements and supports VA 2.6.

In addition to the hardware requirements, HP recommends that the system has a minimum of 1-GB RAM.

Virtual Appliance Installation

Currently, VA 2.0 and VA 2.6 must be installed on a system with Windows XP 32-bit. The system must meet or exceed the hardware and BIOS requirements mentioned in the previous sections.

The following provides an example of a VA 2.6 appliance installation:

1. Run the VA Setup file.
2. Follow the directions from the installer.
3. Reboot the system.
4. If necessary, enable VT in F10 Setup, and then reboot.
5. Go into the MEBx by pressing **Ctrl+P** during POST.
6. Type the MEBx password.
7. Select **Intel AMT Configuration**.

The VA Configuration option will now be available at the bottom of the AMT Configuration list.

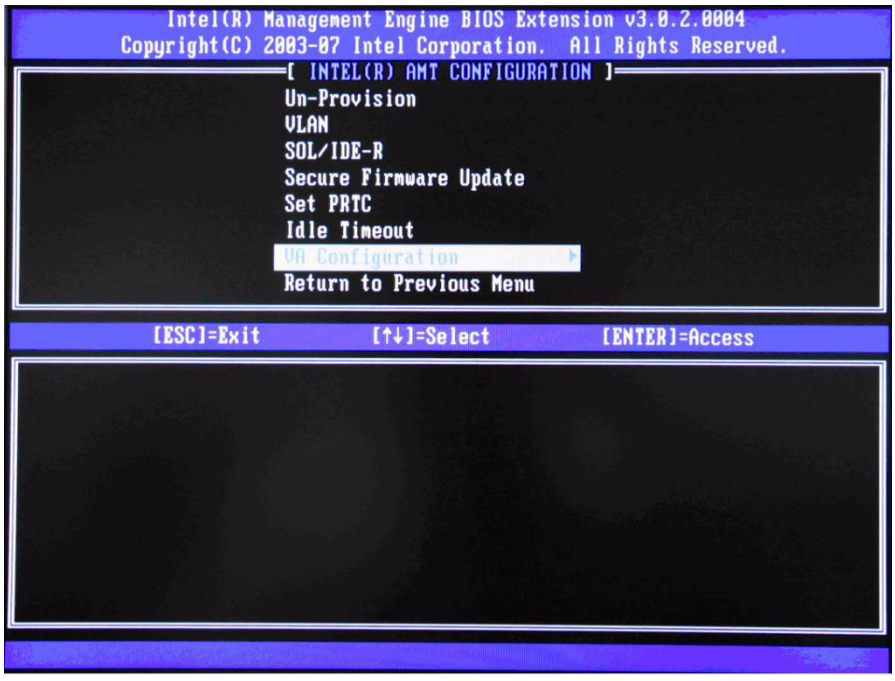

Figure 1 VA Configuration option in the MEBx

8. Enable VA Support.

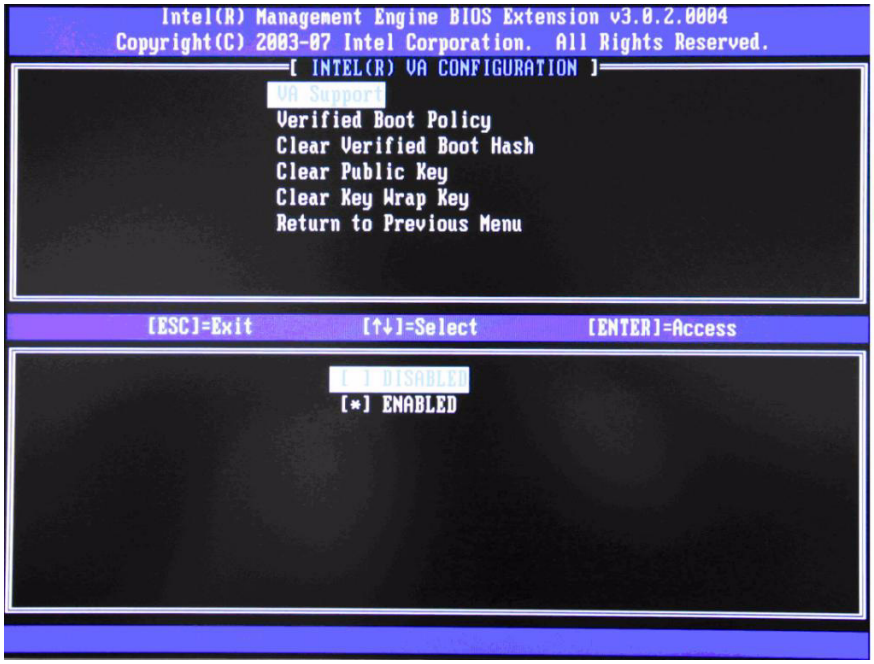

Figure 2 VA Support Enabled

9. Set **Verified Boot Policy** to **Verified Boot and Halt**.

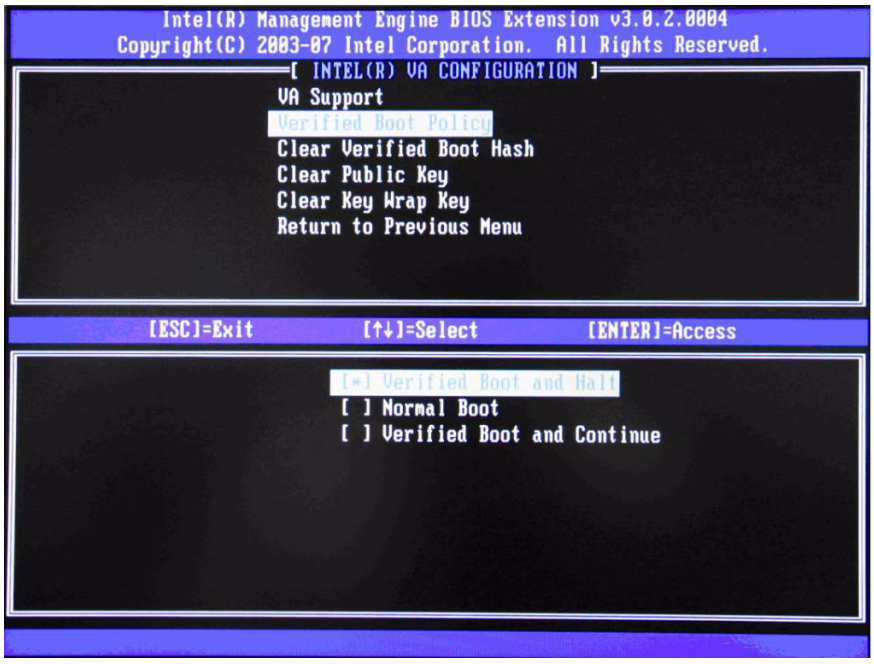

Figure 3 Verified Boot Policy set to Verified Boot and Halt

10. Exit MEBx and boot into the operating system.

A VA can be uninstalled. This can be because a VA is no longer needed or the user wants to install a different VA. Only one VA can be installed at any given time.

The following provides an example of a VA 2.6 appliance uninstallation:

1. Run the VA uninstallation file.
2. Reboot the system.

   The ME firmware will display an error stating that VA has been uninstalled with the VA boot policy set to Verified Boot and Halt. You will then see the 2221 POST error message (see **"Appendix A: POST Error Messages" on page 13**).
3. Cycle power to the system and go into the MEBx by pressing **Ctrl+P** during POST.
4. Enter the MEBx password.
5. Select **Intel AMT Configuration**.
6. Select **VA Configuration** at the bottom of the list and change the **VA Boot Policy** to **Normal Boot**.

   Depending on the BIOS version, the system may reboot and then display the 2228 POST message (see **"Appendix A: POST Error Messages" on page 13**). This is an informational message that lets the user know that VTx has automatically been disabled. Press **F1** to continue the boot process.

The system boots normally to Windows XP.

Network Modifications

The installation of a VA causes the onboard network controller to be virtualized. The COS is no longer in control of the physical network device. Instead, the COS is in control of a virtual version of the network device and the SOS is in control of the physical network device.

The network device virtualization will cause the Device ID and name string of the Intel 82566DM network adapter to change. This should result in "new hardware found" message and the installation of Intel virtual network drivers.

All other network devices will be virtualized away. This means:

- Vendor and Device ID will be changed to 8086h / 10B8h.
- Moved to System Devices as an Unsupported Virtual Network Device.
- No driver is installed for unsupported devices.
- Although device is non-operational, system resources will be used.

The purpose of this network device virtualization is for security reasons. Network traffic can be monitored and filtered through the Intel 82566DM network controller, but this cannot be done with any other network devices. Therefore, no other network devices can be functional when a VA is installed.

The virtualization of the network adapter will cause network packets to be redirected to the SOS in the SOS partition, which can impact network traffic performance. If additional network packet monitoring and filtering are applied, network performance may be impacted.

The following is an example of a system with two network devices, the Intel 82566DM and a Broadcom, before a VA is installed.

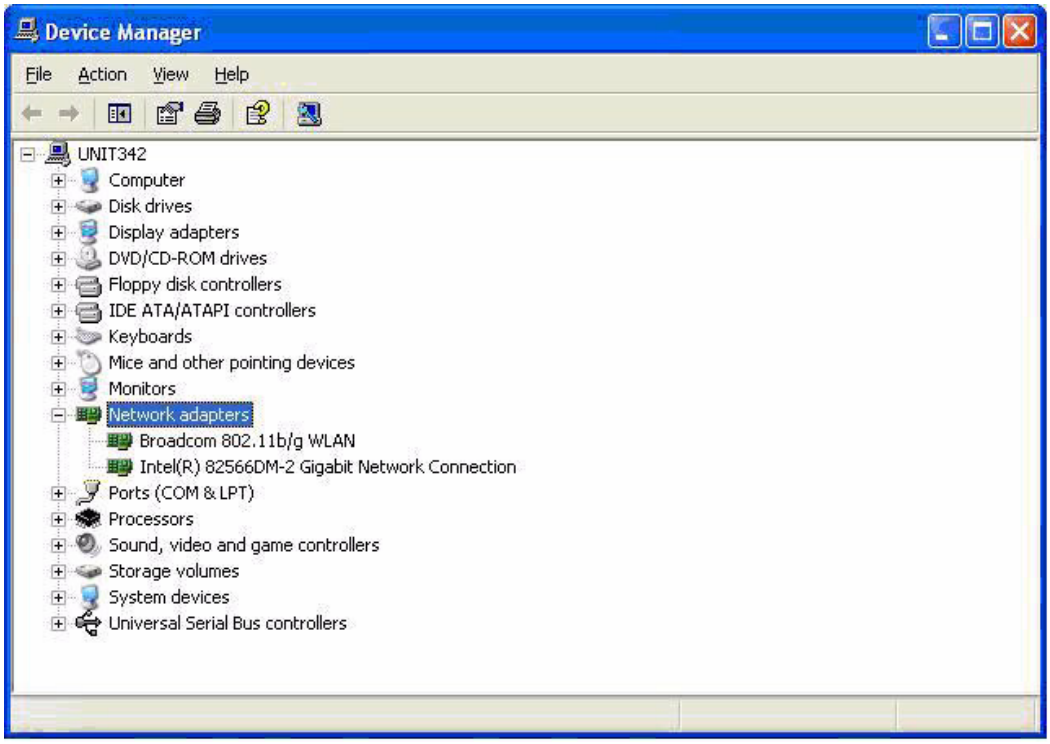

Figure 4 Two Network Devices - Intel 82566DM and Broadcom

After the VA is installed, the Intel 82566DM NIC is renamed `Intel Virtual 82555 Gigabit Network Connection`.

Notice that the Broadcom network device is no longer under **Network Adapter**s in Device Manager.

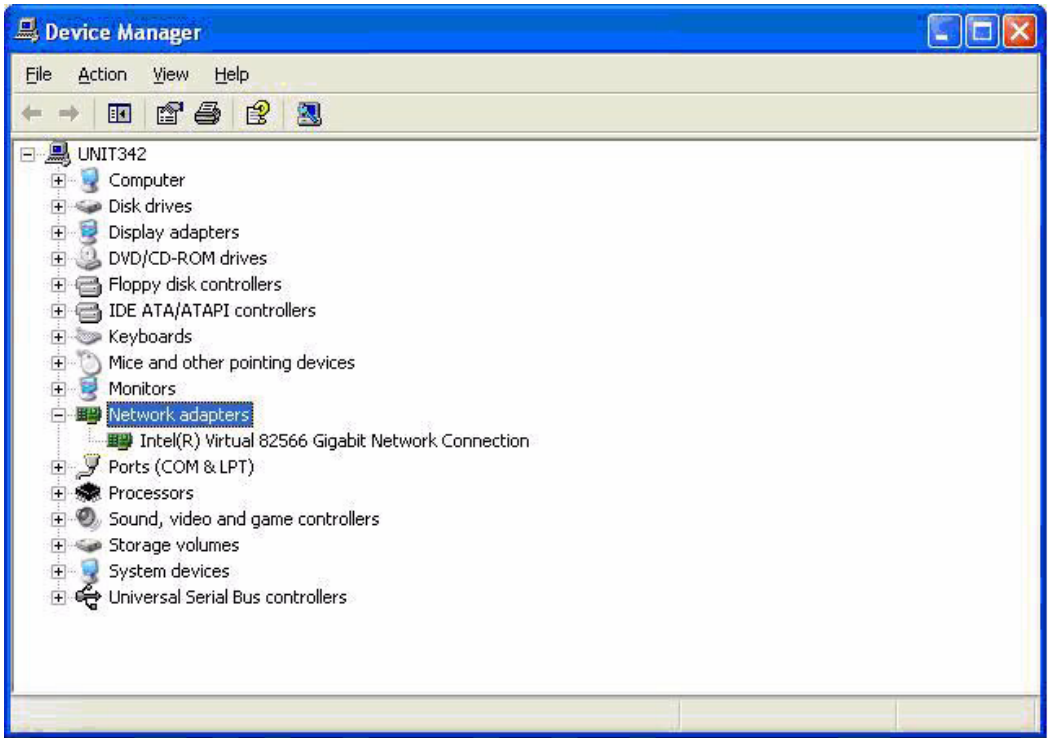

Figure 5 Virtualized Intel 82566DM Network Controller

After the VA is installed, the Broadcom network device is renamed `Unsupported Virtual Network Device` and moved to **System Devices** in Device Manager.

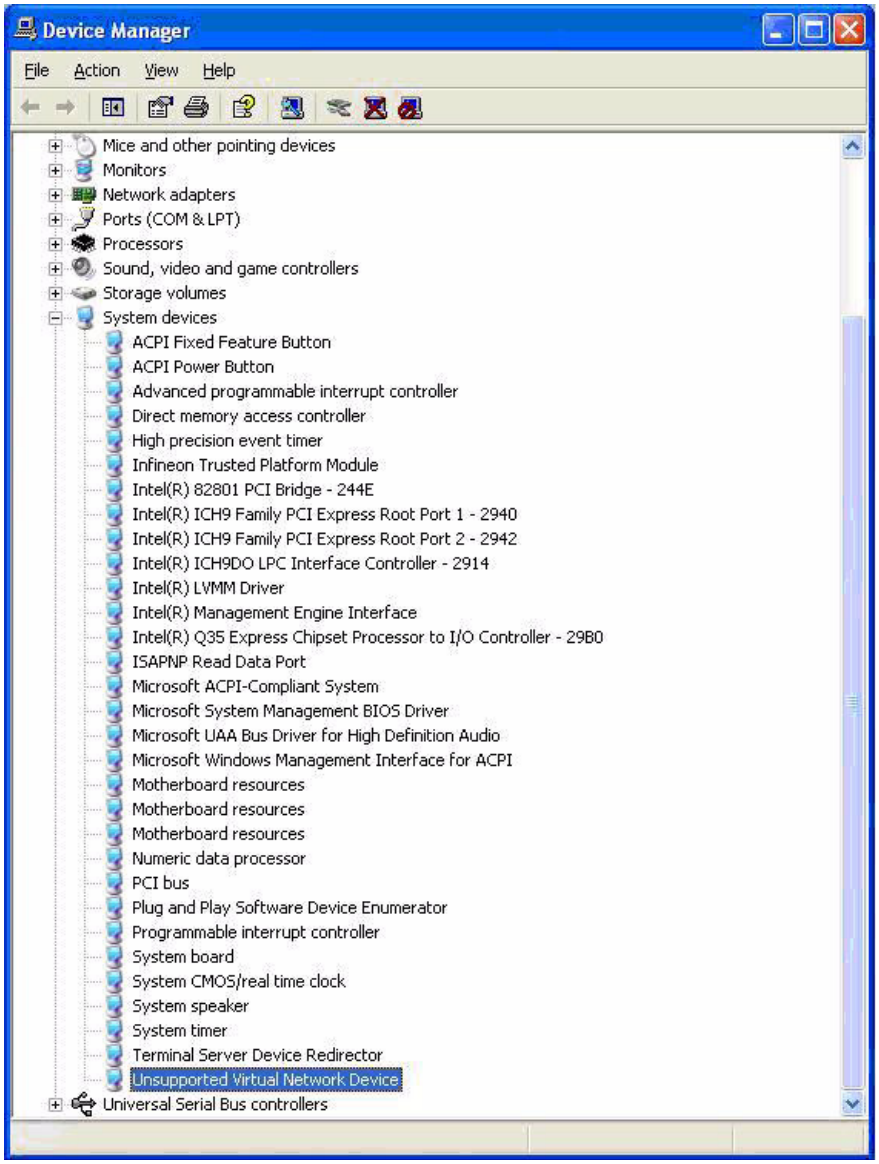

Figure 6 Unsupported Virtual Network Device

Hard Drive Layout

A VA is located on its own hard drive partition, called the Service OS partition, to isolate it from the Client operating system. Since the VA is an isolated entity that does not require COS interaction, it is much more resistant to malicious software.

HP Compaq dc7700p and dc7800p Business PCs have a 102MB SOS partition at the end of the hard drive. This partition is empty and is of type 72h. Once a VA is installed, the partition will become type 71h. The VA loaded in the SOS partition will be in a single binary image.

The SOS partition is not formatted or given a hard drive letter. It does not have a file system and is not accessible through normal means.

The HP Backup and Recovery partition is located in between the COS partition and the SOS partition.

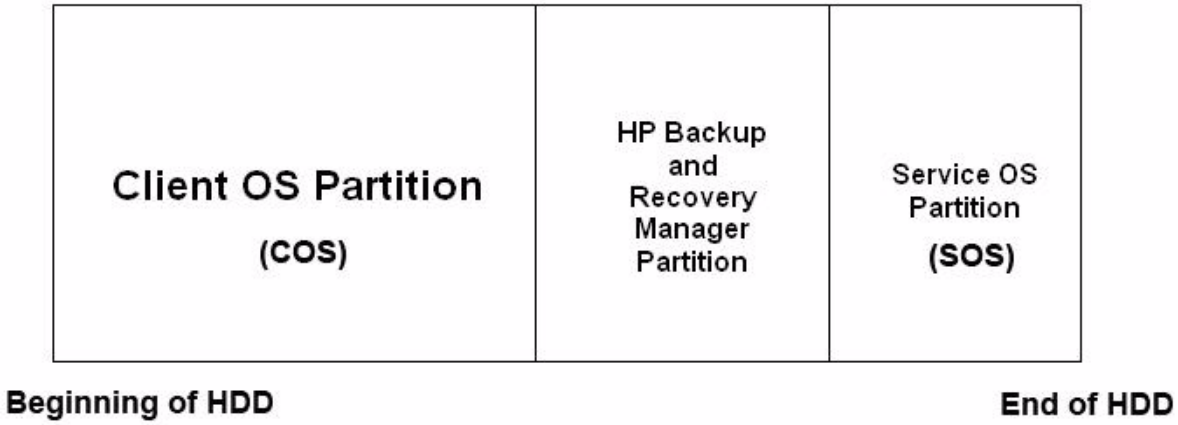

Figure 7 HP Compaq dc7700p and dc7800p hard drive layout

Known Limitations

- Intel vPro technology currently supports only a single VA. You will need to select the right VA to suit your needs.
- VA 2.6 is available at time of launch of the HP Compaq dc7800p Business PC but will only support Windows XP as the COS. There is no Vista support for VA 2.6.
- VAs do not support RAID configurations at this time.
- VAs do not support more than two processor cores at this time. Therefore, quad core processors such as the Intel Q6xxx are not supported.
- VAs do not support AMT 1.0. The system must be in AMT 2.x or AMT 3.0 mode.
- VAs do not support any other network cards besides the onboard Intel 82566DM network controller.
- Installation of a VA to a system with multiple hard drives might encounter complications. This is due to the Windows XP plug n' play (PnP) algorithms using an in-place reorder mechanism for PnP enumeration.

More details on this issue can be found in the Microsoft Knowledge Base Article at: **http://support.microsoft.com/kb/825668/en-us**

To work around this issue, the IDE-R controller in Device Manager must be disabled and the system rebooted before installing the VA. Once this is done, Windows XP will only see one IDE controller and enumerate the hard drives properly. The IDE-R controller appears as a standard dual channel PCI IDE controller.

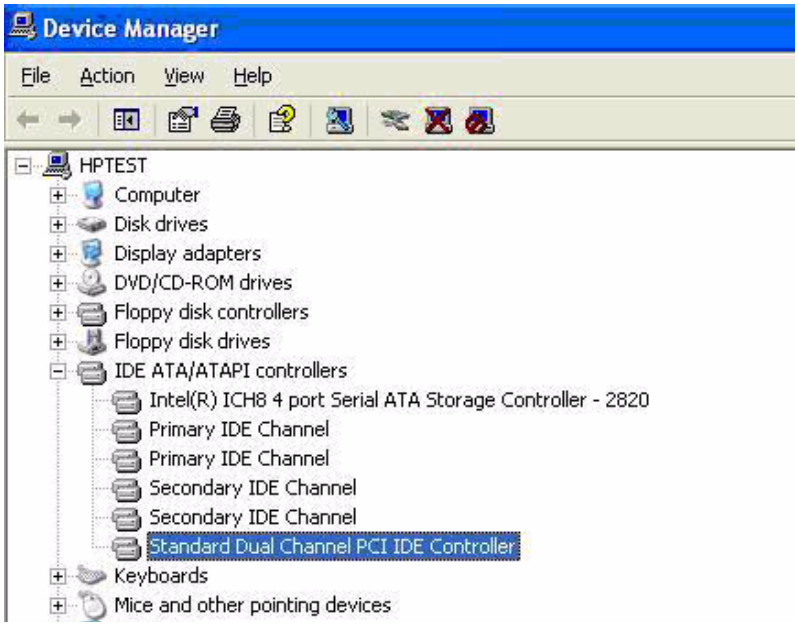

Figure 8 IDE-R controller in Device Manager

- There are restrictions in the way hard drives can be duplicated using duplication software, such as Symantec Ghost, once a virtual appliance is installed. Hard drive cloning through software means is only possible for same sized hard drives. This is because of the LVMM and the way it boots.
- A system with a VA installation cannot swap out its booting hard drive with another hard drive. The hash check will fail and the system will not boot.
- VA 2.0 appliances on the dc7700p systems require the 2.0.1 LVMM hotfix from Intel. Without this hotfix, the following symptoms may be seen:
  - Failure to load LVMM with error code of 0x81.
  - Failure to load Windows XP with the KB909095 Microsoft patch applied (or other patches that update NTOSKRNL.EXE to a version greater than 5.1.2600.2774). This patch is included in the preinstall image shipping with the dc7700p.
  - Failure to resume from S3.

Appendix A: POST Error Messages

The following are POST error messages related to VA problems during system boot.

Post Error	Message	Suggested Action	VA Version Applicable
2213-EIT Failure	Hardware for VA support not present.	Ensure Intel AMT is enabled and a VT-capable processor is installed.	2.x
2214-EIT Failure	VA partition corrupt or missing.	Ensure drive with VA image is installed correctly.	3.x
2215-EIT Failure	VA boot record read failure.	Ensure drive with VA image is installed correctly.	2.x
2221-EIT Failure	VA partition corrupt or missing.	Enter MEBx setup and change Verified Boot Policy to continue normal boot.	2.x
2222-EIT Failure	Unknown boot policy returned from MEBx.	Upgrade ME firmware. Re-flash BIOS.	2.x
2223-EIT Failure	VT must be enabled to launch VA.	Enter F10 Setup and enable Intel Virtualization Technology.	2.x and 3.x
2224-EIT Failure	Embedded Security must be available to launch VA.	Enter F10 Setup and set Embedded Security Device to Device Available.	2.x
2225-EIT Failure	VT-d must be enabled to launch VA.	Enter F10 Setup and enable Intel Virtualization Technology Directed I/O.	3.x
2226-EIT Failure	TXT must be enabled to launch VA.	Enter F10 Setup and enable Trusted Execution Technology.	3.x
2227-EIT Failure	Embedded Security must be enabled to launch VA.	Enter F10 Setup and set Embedded Security Device support to Enable.	3.x
2228	EIT uninstall has automatically disabled VT.	No action required. For some BIOS versions, VT is disabled after uninstalling a VA. Virtualization Technology should be turned off when not in use for security reasons. This is done to protect your system from malicious attacks. To re-enable VT, enter F10 Setup and set Virtualization Technology to Enable.	2.x
2229-EIT Failure	VA does not support processors with more than two cores.	Replace processor with a single or dual core processor.	2.x

Additional Information

To learn more about HP Compaq Business PC and Intel vPro Processor Technology, go to **www.hp.com** and read the following white papers.

- *vPro Prerequisites and Trade-offs for the dc7800 Business PC with Intel vPro Technology*
- *vPro Setup and Configuration for the dc7800 Business PC with Intel vPro Technology*

461594-001, 10/2007