

Intel[®] Active Management Technology (Intel[®] AMT) Platform

Montevina SW/FW OEM Bring up Guide

October 2007

Rev 0.4

Intel Confidential



INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

This document contains information on products in the design phase of development.

All products, platforms, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice. All dates specified are target dates, are provided for planning purposes only and are subject to change.

This document contains information on products in the design phase of development. Do not finalize a design with this information. Revised information will be published when the product is available. Verify with your local sales office that you have the latest datasheet before finalizing a design.

Intel® Active Management Technology requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see <http://www.intel.com/technology/manage/iamt/>

Montevina, Santa Rosa, Weybridge and other code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2007, Intel Corporation. All rights reserved.



Contents

1	Introduction	8
1.1	Document scope	8
1.1.1	Important Assumptions	8
1.1.2	Known-good system configuration	8
2	Terminology	9
3	Montevina bring up overview	11
3.1	Flash image	11
3.2	Bring-up summary	12
4	Final image generation	14
4.1	Image components	14
4.2	Flash image tool from VIP	15
4.3	Assemble the final image	15
4.3.1	Setup the flash image tool	15
4.4	Create the flash image	17
4.4.1	Descriptor region	17
4.4.2	ME region	20
4.4.3	GbE region	21
4.4.4	BIOS region	21
4.4.5	Platform Data Region	22
4.4.6	ME Parameters	22
4.4.7	Save configuration	27
4.5	Building the flash image	27
4.6	Programming the image onto the flash	29
4.7	Using a flash programmer	29
4.8	Using the flash programming tool	29
4.8.1	DOS environment	30
4.8.2	Load files onto the target platform	30
4.8.3	Query the flash devices	31
4.8.4	Program the image	31
4.8.5	Windows environment	32
4.8.6	Load files onto the target platform	33
4.8.7	Query the flash devices	33
4.8.8	Program the image	34
4.9	Installing EC Firmware	34
5	BIOS Setup	35
5.1	Set Parameters	35
5.2	iTPM Parameters on BIOS	35
6	Intel® Management Engine BIOS Extension Setup	36
6.1	Intel® Management Engine BIOS Extension screen	36
6.1.1	Enabling Intel® AMT	37
6.1.2	Enabling ASF 2.0	39



7	Installing drivers.....	41
	7.1 Driver identification	41
8	Basic Intel® AMT functional demonstration.....	43
	8.1 Ping verification	43
	8.2 Test Intel® AMT using the WebUI.....	45
9	Basic iTPM functional demonstration	47
	9.1 XP Verification	47
	9.2 Vista Verification	47
	9.2.1 Method 1	47
	9.2.2 Method 2	47
10	Intel® AMT Tools.....	48
	10.1 AMTVTL tool	48
	10.1.1 AMTVTL from VIP	49
	10.1.2 Executing AMTVTL	49
	10.2 MEInfo tool.....	50
	10.2.1 MEInfo DOS tool	50
	10.2.2 MEInfo DOS tool from VIP	50
	10.2.3 Executing MEInfo	51
	10.2.4 MEInfo Windows tool	52
	10.2.5 MEInfo Windows tool from VIP	53
	10.2.6 Executing MEInfoWin	53
	10.3 AMTVTR tool.....	54
	10.3.1 AMTVTR tool from VIP.....	55
	10.3.2 Executing AMTVTR.....	55
	10.4 System Defense Test	57
	10.4.1 Executing System Defense test with AMTVTR	57
	10.5 Testing SOL and IDE-R features	59
	10.6 Final checklist.....	61
11	Appendix A – Board rework to enable Integrated TPM 1.2	62



List of Figures

Figure 1. Flash Image Regions	11
Figure 2. Components making final image	11
Table 3. Kit Components	14
Figure 3. Flash Image Tool – Configuration Setup	16
Figure 4. Configuring Build Settings	20
Figure 5. PDR Region	22
Figure 6. ME Region	23
Table 4. Firmware Override Update Variables	23
Figure 7. AMT Region	24
Figure 8. iTPM Region	25
Table 5. iTPM Permanent Flags	26
Table 6. Dictionary Attack Flags	26
Pillar Rock CRB Rework	62
STEP A	62
STEP B	65
STEP C	65
STEP C	66
Silver Cascade CRB Rework	67
STEP A	67
STEP B	68
STEP B	69
STEP C	70



Revision History

Build Number	Description	Revision Date
0	<ul style="list-style-type: none">-Santa Rosa & Weybridge OEM Bring-up Guide used as an initial template-Removed all aspects that do not pertain to mobile, such as QST-First draft of TOC for review	7/23/2007
0.1	<p>Updated flash programming based on the updated FIT tool, based on the tools guide.</p> <p>Removed MENVN, AMTNVM sections as it is now merged into FIT through the NVAR menu, made corresponding changes on the TOC</p> <p>Included ME parameters and temporary firmware update procedures within the image building sections</p> <p>Initial release – note that there is still no hardware available so the procedures noted haven't been tested in a lab.</p> <p>Initial indexing of figures, tables and filenames are generic and should be treated as placeholders and nothing more.</p>	7/31/2007
0.2	<p>Removed non relevant material such as BL CRB info</p> <p>Tool changes reflected (FITC, AMTVTL, AMTVTR</p> <p>Added warning notes on fpt section to disable ME before flashing</p> <p>Some tools and features not working: AMTVTL, AMTVTR, system defense, SOL and IDER</p> <p>Added EC firmware installation section</p>	8/17/2007
0.3	Added TPM info	8/21/2007
0.31	Added .NET framework requirement for AMTVTL	8/29/2007



Build Number	Description	Revision Date
0.32	Added Appendix A – CRB Board rework instructions	8/31/2007
0.40	Updated for Alpha1 release Updated Pillar rock CRB TPM rework instructions Added Silver Cascade TPM rework instructions Added command line usage of FITC Updated AMTVTR usage section Updated image creation process (ROM bypass) Added link to document to get VSCC tables for different flash parts Updated corresponding sections affected by the now shared single MAC address for ME and host	10/09/2007

§



1 *Introduction*

1.1 Document scope

This document describes the OEM-ODM bring up procedure for the Montevina/ICH9M platform with Intel® AMT 4.0/ASF 2.0/iTPM firmware. This document describes how to create an integrated image from the component images (BIOS, Gigabit Ethernet and Intel® ME images) and program the integrated image onto the SPI flash devices. This document includes information on setting parameters required to enable Intel® AMT. This document also describes methods for testing the platform after Intel® AMT or iTPM is enabled to verify that Intel® AMT/iTPM is functioning.

1.1.1 Important Assumptions

- The reader has already reviewed the Readme and Release Notes documents included in the kit distribution.
- **Static IP mode only** for simplicity.
- The Intel CRB (Pillar Rock) is the system on which you are performing the bring-up process.
- Fresh operating system installed on the system after flashing the image.

1.1.2 Known-good system configuration

1. Two 512-Megabyte DDR2 667Mhz memory modules
2. Penryn 2.2 Ghz CPU, 800 Mhz Front Side Bus

§



2 Terminology

Acronym	Explanation
Intel® AMT	Intel® Active Management Technology
ASF	Alerting Standard Format
BIOS	Basic Input Output System
CRB	Customer Reference Board
DHCP	Dynamic Host Configuration Protocol
FIT	Flash Image Tool
FPT	Flash Programming Tool
FW	Firmware
G3	A system state of Mechanical OFF where all power is disconnected from the system
GbE	Gigabit Ethernet
GUI	Graphical User Interface
Intel® MEI	Intel® Management Engine Interface
HW	Hardware
ICH	I/O Controller Hub
IDER	Integrated Drive Electronics Redirection – the ability to redirect input and output of an IDE device to a remote console.
IP	Internet Protocol
iTPM	Integrated TPM—1.2 TPM Compliant
LAN	Local Area Network
LMS	Local Manageability Service
MAC	Media Access Control
MCH	Memory Controller Hub
ME	Intel® Management Engine
MEBx	Intel® Management Engine Bios Extension
NIC	Network Interface Card
NVM	Non-Volatile Memory
OEM	Original Equipment Manufacturer
SOL	Serial Over LAN
SPI Flash	Serial Peripheral Interface Flash



Acronym	Explanation
Static IP	An Internet Protocol address set manually (not by DHCP)
SUT	System Under Test
SW	Software
S0	A system state where power is applied to all Hardware devices and system is running normally.
S1, S2, S3	A system state where the host CPU is not running. However power is connected to the memory system.
S4	A system state where the host CPU and memory is not active
S5	A system state where all power to the host system is off. However the power cord is still connected.
Sx	All S states that are not S0.

§



3 Montevina bring up overview

The flash image consists of multiple regions, as shown in the figure below.

Figure 1. Flash Image Regions

Region	Content
0	Flash Descriptor
1	BIOS
2	ME
3	GbE
4	Platform Data

3.1 Flash image

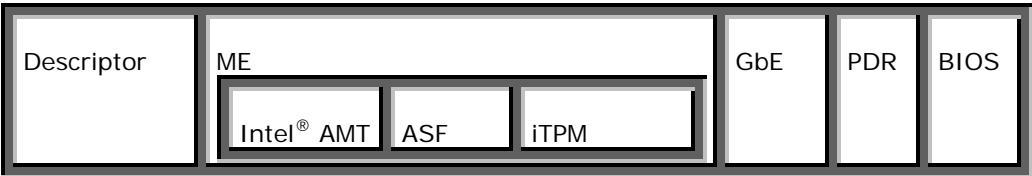
The CRB ships with a total of two SPI flash devices installed. The image created below will span both devices as a single flash memory area. Bringing up a Montevina platform with the FW/SW kit involves the following steps:

- Integrating the following images into a final, combined image:
 - Flash Descriptor
 - Intel ME image
 - BIOS image
 - GbE image
 - Platform Data Region
- Programming this final image onto the SPI flash devices.
- BIOS setup
- Activating Intel® ME BIOS Extension (MEBx) Setup to configure the Management Engine and Intel® AMT.
- Basic demonstration of Intel AMT/ASF 2.0/iTPM functionality.

Each of these steps is addressed in detail in the following pages.

The figure below shows the components of the final firmware image which is built from the component images.

Figure 2. Components making final image





3.2 Bring-up summary

This section summarizes the complete bring-up procedure, which is detailed in the remainder of the document.

Step #	Description	Input	Output
1	Download kit from VIP	N/A	The downloaded zip file containing the following folders – NVM Image, System Tools, Drivers and based on the FW supported - ASF 2.0 Tools, iTPM Tools and Intel® AMT Tools.
2	Create the Flash Image using the flash image tool, which integrates component binary images (BIOS, GbE, ME) into a single flash image.	BIOS.rom, ME.bin and GbE.bin	outimage.bin
3	Program the Flash Image onto the SPI flash devices on the target platform using the Flash Programming Tool.	outimage.bin	Flash image programmed successfully on the target platform.
4	Remove AC power cord from CRB Power supply.	N/A	N/A
5	Clear CRB CMOS settings	N/A	N/A
6	Modify the settings in the BIOS setup screen.	Select to enable settings for ME and AMT/ASF/iTPM, activate HECI link	Fields in the BIOS screen have been modified to support Intel AMT/ASF/iTPM on the target platform.
7	Modify the settings in the Intel® ME BIOS Extensions (MEBx) setup	Configure settings for ME and Intel® AMT/ASF	ME and Intel® AMT/ASF configured on the target platform.
8	Install the Chipset.INF file and then install the supported drivers.	Chipset.INF, LAN, LMS and Intel® ME Interface Setup and iTPM driver files.	Chipset.INF, LAN, LMS, iTPM and Intel® ME Interface drivers installed on the target platform.
9	Demonstrate the basic functionality of Intel® AMT.	Ping Verification and WebUI	The management console is able to connect to the Intel® AMT system and you can verify that Intel® AMT has been successfully enabled on the target platform.
10	Check the functionality of Intel® AMT locally using the AMTVTL tool	AMTVTL.exe + username and password (if Kerberos* is not used)	Checks the functionality of a local Intel® Active Management Technology (AMT) 4.0 device.
11	Verify Intel ME features in a DOS environment using MEInfo DOS Tool.	MEInfo.EXE (DOS)	Verifies Intel ME FW is alive. Returns version data about BIOS, Intel® ME, iTPM, Intel® AMT Firmware and components.
12	Verify Intel ME features in a	MEInfoWin.EXE (Windows)	Verifies Intel ME FW is alive.



Step #	Description	Input	Output
	Windows environment using MEInfo Windows Tool		Returns version data about BIOS, Intel® ME, iTPM, Intel® AMT Firmware and components.
13	Check the functionality of Intel® AMT remotely using the AMTVTR tool.	<ul style="list-style-type: none"> - Host IP address - AMT username and password (if Kerberos* is not used) -Feature select 	Returns success if Intel® AMT has been enabled successfully, otherwise returns a failure.
14	Check for the System Defense functionality using the AMTVTR tool.	<ul style="list-style-type: none"> - Host IP address - AMT username and password (only if Kerberos* is not used) -Feature select 	Successfully checks for System Defense functionality on Intel® AMT machine.
15	Verify MEI/LMS/iTPM Drivers Installed	Review Device Manager to verify HECI device, TPM device and LMS are present.	Review properties to confirm that the correct MEI and LMS versions are loaded in the OS.

§



4 Final image generation

The flash image tool is used to create the final flash image file that you will use to program the SPI flash devices on the CRB system board.

The purpose of this tool is to create and configure a flash image for the Montevina/ICH9M platform. The following binary files are provided as input to this tool:

- BIOS (.rom)
- Intel ME firmware (.bin)
- GbE (.bin)

The tool usage is explained in detail in the following sections.

4.1 Image components

The various image components can be downloaded from Validation Internet Portal (VIP - formerly known as ARMS):

(<https://platformsw.intel.com/>)

The kit will contain one component archive as shown in the table below.

Table 3. Kit Components

Archive name	Intel® AMTFirmware	Intel® TPM	ASF2.0 Firmware
iAMT_ASF2_iTPM_4.0.0.xxxx.zip	✓	✓	N/A in alpha1
iTPM_4.0.0.xxxx.zip		✓	N/A in alpha1

NOTE: The “xxxx” shown herein throughout in this text will actually be a 4-digit number corresponding to the build number. Example: iAMT_ASF2_iTPM_4.0.0.1023.zip

Download the required archive and expand it to a folder using an archive utility, such as WinZIP. (Example: E:\)

- Example: If the ‘iAMT_ASF2_iTPM_4.0.0.xxxx.zip’ archive has been downloaded, then the contents will be downloaded into the following directory structure - E:\iAMT_ASF2_iTPM_4.0.0.xxxx\
- Refer to the remainder of this document to create the proper build directory structure.



Under the root of the above directory hierarchy, the actual composite binary image files you will use to build the final image (BIOS, ME, GbE) are located under the **NVM Image** directory. (Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\NVM Image) When you configure the flash image tool to build your final image, you will set an environment variable called \$SourceDir to point to this directory for the source images. All environment variables required by the flash image tool are covered in detail in the sections below.

4.2 Flash image tool from VIP

The flash image tool can be accessed from the following directory:

- "Unzipped_folder"\Tools\System Tools\Flash Image Tool\

(Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\System Tools\Flash Image Tool\fitc.exe)

The 'Flash Image Tool' folder contains the following files:

- a. fitc.exe
- b. ftool.ini
- c. ftoolmplc.xml
- d. newfiletmpl.xml

Note:

- For details on tools usage and the files listed above, please refer to the document: 'Intel® System Tools User Guide.pdf'.
- The flash image tool main executable is 'fitc.exe'. It is required that the following files be in the same directory as ftoolc.exe:
 - ftoolmplc.xml
 - newfiletmpl.xml
- The flash image tool will NOT execute properly if the above files are missing.
- This tool runs in Windows* XP only.

4.3 Assemble the final image

4.3.1 Setup the flash image tool

Follow the steps given below to set up the flash image tool.

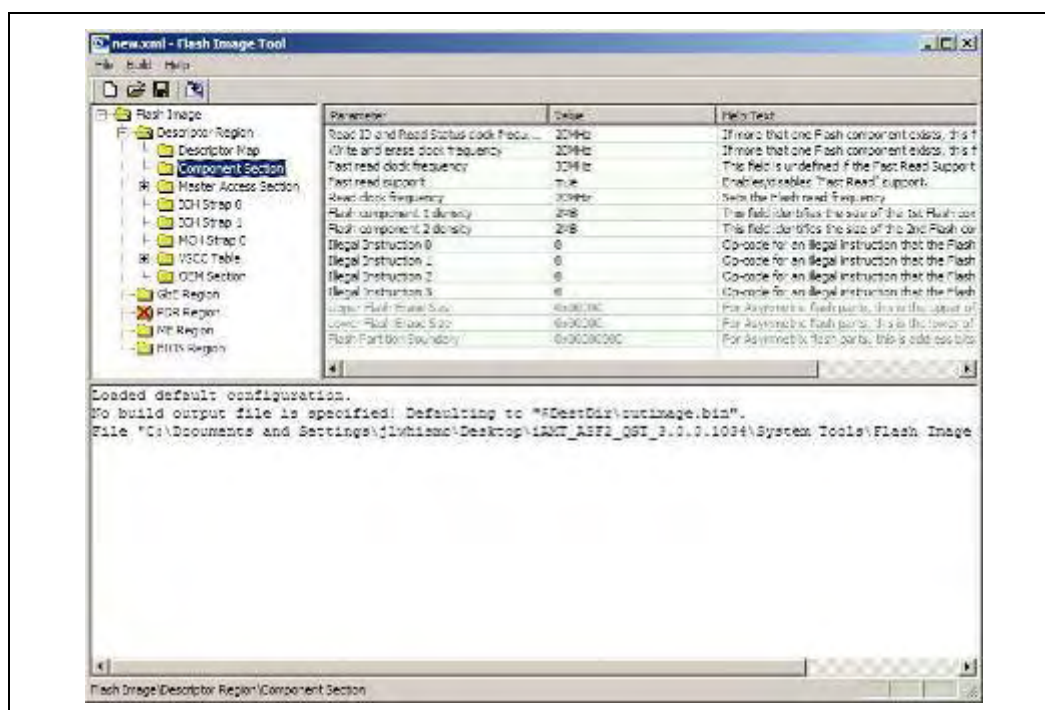
1. Go to the directory containing 'fitc.exe'.
2. Double click on 'fitc.exe'.
3. Read through the license agreement, accept it, and then click 'OK'.
4. The flash image tool opens a new configuration file entitled:

'Untitled.xml – Flash Image Tool'.
5. Click on the 'Build' menu.
6. Select 'Environment Variables...'

7. The Environment Variables window opens. Set the following values:
 - a. Set '\$WorkingDir:' to: .\Working
 - b. Set '\$SourceDir:' to: .\..\..\NVM Image (this corresponds to the directory path containing the NVM images.)
 - c. Set '\$DestDir:' to: .\Output
 - d. For '\$UserVar1:', '\$UserVar2:' and '\$UserVar3:' do not change the default values. (Retain the values as '.')
 - e. Click 'OK', and the 'Environment Variables' window will close.
8. Click on the 'Build' menu at the top of the current window.
9. Select 'Build Settings...'
10. In the new window opened, entitled 'Build Settings':
 - a. Set the 'Output path:' to include the final flash image name.

(Example: \$DestDir\outimage.bin) Note: You may opt to name your output file so it includes the build number, i.e. "\$DestDir\1023_Outimage.bin".
 - b. Leave 'Generate intermediate build files' as checked.
 - c. Leave 'Build compact image' as unchecked. (when selected creates the smallest flash image possible, by default the application uses the flash component sizes in the descriptor to determine the image length)'.
 - d. Set 'Flash Block/Sector Erase Size:' to the sector size of the target flash device. (Example: 4KB for 16 Mbit SST device with ID SST25VF016B used on the CRB)
 - e. Click 'OK', and the 'Build Settings' window will close.

Figure 3. Flash Image Tool – Configuration Setup





4.4 Create the flash image

This section details the steps required to configure the flash image tool and to set the various required parameters, before the final flash image is created from its component images, i.e. BIOS image, GbE image and the Intel ME image. The following regions are configured using the flash image tool:

4.4.1 Descriptor region

1. Expand the 'Descriptor Region' node in the left pane of the main window.
2. Click on 'Descriptor Map' node under the 'Descriptor Region' node.
 - a. All of the parameters of the 'Descriptor Map' section will appear in the list in the right pane.
 - b. Double click on 'Number of Flash Components' parameter.
 - c. A dialog box will open, entitled 'Number of Flash Components'.
 - d. Set this value to the number of flash components installed on the target board. Valid values are 1 or 2. Note: the Montevina CRB comes with 2 flash devices installed, so you would select 2 for this setting. Other platforms may have only one flash device.
 - e. Click 'OK' and the dialog box closes.
3. In the left pane, under the 'Descriptor Region' node and click to select the 'Component Section' node. (as shown in figure 3)
 - a. All of the parameters of the 'Component Section' will appear in the list in the right pane.
 - b. Double-click on 'Fast read clock frequency' parameter.
 - c. A dialog box will open, entitled 'Fast read clock frequency'.
 - d. Select '33MHz' from the drop-down list.
 - e. Click 'OK' and the dialog box closes.
 - f. Double-click the 'Fast read support' parameter.
 - g. A dialog box will open, entitled 'Fast read support'.
 - h. Select the 'true' radio-button if it is not already selected.
 - i. Click 'OK' and the dialog box closes.
 - j. Double-click the 'Flash component 1 density' parameter.
 - k. A dialog box will open, entitled 'Flash component 1 density'.
 - l. Select the correct component size from the drop-down list and set it to the size of the flash part being used, according to the following criteria:

Flash component density:

- If the value for 'Number of Flash Components' is set to 1, then 'Flash Component 1 density' should be set to 4MB or whatever the case is.
- If the value for 'Number of Flash Components' is set to 2, then 'Flash Component 1 density' should be set to the proper size value. (i.e 2MB)
- If you are using the Intel Montevina Pillar Rock CRB (it has two flash components) or another platform that has two 2MB flash components, set each component to 2MB. Examine the target system board to determine the proper settings.

Note: The below steps m, n and o are applicable only if the 'Number of Flash Components' is set as 2.



- m. Double-click on 'Flash component 2 density' parameter.
 - n. A dialog box will open, entitled 'Flash component 2 density'.
 - o. Select the correct component density from the drop-down list (Example: 2MB).
 - p. All the remaining parameters for the 'Component section' are retained as default values.
4. Expand the 'Descriptor Region' node and then expand the 'Master Access Section' node in the left pane.
- a. Click to select the 'CPU/BIOS' node under the 'Master Access Section' node.
 - i. All the parameters of the 'CPU/BIOS' section are displayed in the right pane.
 - ii. Double-click the 'Read access' parameter.
 - iii. A dialog box opens, entitled 'Read access'
 - iv. **Enter the value '0xFF' here.
 - v. Click 'OK' and the dialog box closes.
 - vi. Double-click on 'Write access' parameter.
 - vii. A dialog box opens, entitled 'Write access'
 - viii. **Enter the value '0xFF' here. (**Important:** the value 0xFF - full read/write access - is for engineering purposes only – for production, you will need to change this to WRITE access permission only.)
 - ix. Click 'OK' and the dialog box closes.
 - b. In the left pane, open the 'Master Access Section' node and click to select the 'Manageability Engine (ME)' node.
 - i. All the parameters of the 'Manageability Engine (ME)' section are displayed in the right pane.
 - ii. Double-click the 'Read access' parameter.
 - iii. A dialog box opens, entitled 'Read access'
 - iv. **Enter the value '0xFF' here.
 - v. Click 'OK' and the dialog box closes.
 - vi. Double-click the 'Write access' parameter.
 - vii. A dialog box opens, entitled 'Write access'
 - viii. **Enter the value '0xFF' here.
 - ix. Click 'OK' and the dialog box closes.
 - c. In the left pane, open the 'Master Access Section' node and click to select the 'GbE LAN' node.
 - i. All the parameters of the 'GbE LAN' section are displayed in the right pane.
 - ii. Double-click the 'Read access' parameter.
 - iii. A dialog box opens, entitled 'Read access'
 - iv. **Enter the value '0xFF' here.
 - v. Click 'OK' and the dialog box closes.
 - vi. Double-click the 'Write access' parameter.
 - vii. A dialog box opens, entitled 'Write access'
 - viii. **Enter the value '0xFF' here.
 - ix. Click 'OK' and the dialog box closes.

Note:

- All the above steps are necessary and must be followed. If any of the steps are missed, there may be chances of locking down the flash chip, in which case further updating will not be possible and an SPI flash part replacement will be required.
- ** - The value '0xFF' gives all the regions (Example: Intel ME, GbE and BIOS regions) complete read/write access to a particular region (Example: BIOS region). This value set is only for the engineers/developers.



- For more details on the read/write access and how to determine the values for each permission setting, please refer to the document – ‘Intel® flash image tool.pdf’.
5. Click to select the ‘ICH Strap 0’ node in the tree in the left pane.
 - a. In the ‘ICH Strap 0’ section, the default value of the parameter ‘SmBus address (7-bit)’ is 0x64. Before building the image, make sure the value of the parameter ‘SmBus address (7-bit)’ is set to 0x64. This is the default value, but you should always verify it.
 6. Click to select the ‘MCH Strap 0’ node in the tree on the left side of the main window.
 - a. All the parameters of the ‘MCH Strap 0’ section are displayed in the right pane.
 - b. Double-click on ‘ME boot from Flash’ parameter.
 - c. A dialog box opens, entitled ‘ME boot from Flash’.
 - d. Select the ‘true’ radio button if it is not already selected. (When this option is set to true firmware will begin to read from the ROM bypass section of code and the firmware loaded must contain a ROM bypass section) If not possible to select ‘true’ go to step 4.4.2 and then come back and the ‘true’ option will be available.
 - e. Click ‘OK’ and the dialog box closes.

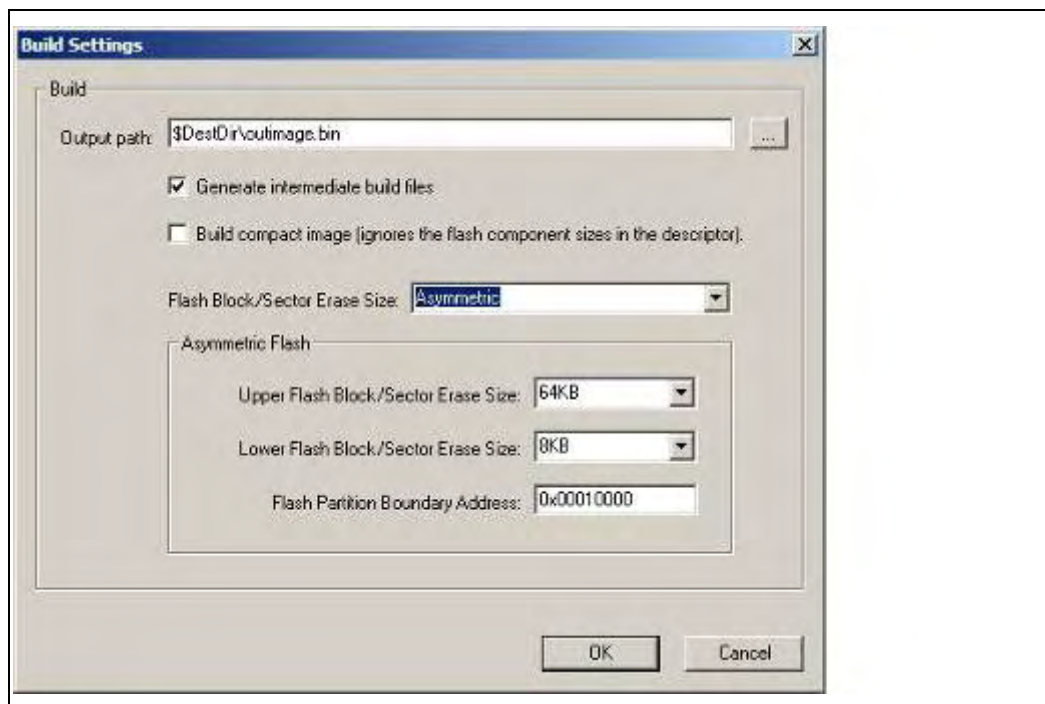
Note:

- Step 7 is to enable ‘ROM By-pass mode’. A ROM by-pass image has been provided in this kit (Firmware image).
 - For more details on the ROM by-pass mode, please refer to the document ‘ReleaseNote.pdf’ (which can be downloaded from the same web page where you obtained the kit)
7. Click to select the VSCC Table node in the tree on the left side of the main window.
 - a. Add the SPI flash component to your VSCC table:

(Example for SST SPI flash)

- i. Right click on VSCC Table to add entry name: SST 25VF016B
 - ii. Left Click to select the entry name created
 - iii. Configure Vendor ID: 0xBF
 - iv. Configure Device ID 0: 0x25
 - v. Configure Device ID 1: 0x41
 - vi. Configure VSCC register value: 0x00002009
- a. Configure ‘Flash Block/Sector Erase Size:’ to Asymmetric
 - b. Make sure that the ‘Upper Flash Block/Sector Erase Size:’ is set to 64KB
 - c. Make sure that the ‘Lower Flash Block/Sector Erase Size:’ is set to 8KB.

Figure 4. Configuring Build Settings



Note: For values to be entered for the above setup, please refer to the *Intel® I/O Controller Hub 9 (ICH9M) Family EDS* and the SPI flash's datasheet. Vendor ID, Device ID 0 and Device ID 1 are all derived from the output of the JEDEC ID command which can be found in the flash's datasheet. In the ICH9M EDS, 22.2.8.2 VSCC0—Vendor Specific Component Capabilities 0 describes the 32 bit VSCC register value.

8. No modifications to the 'OEM Section' are needed – it should be left to default.

4.4.2 ME region

1. Click to select the 'ME Region' node in the left pane of the main window.
2. All the parameters of the 'ME Region' section are displayed in the right pane.
3. Double-click the 'Binary file' parameter.
4. A dialog box opens, entitled 'Binary file'.
5. Click the browse button (...) and open the directory where the Intel ME image is located (Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\NVM Image\Firmware).

Note:

- There will be several Intel ME images present in this directory.
- The image (CA_ICH9M_REL_IAMT_BY_P_ME_PreProduction.BIN) is the Intel ME image to be selected for creating the flash image for Pre-Production Silicon using the flash image tool.



- The second image (CA_ICH9M_REL_IAMT_ME_Production.BIN) is the Intel ME image to be selected for creating the flash image for Production Silicon using the flash image tool. (no ROM bypass)
 - Bypass image files (Example: CA_ICH9M_REL_IAMT_BYP_ME_PreProduction.BIN) are needed on early pre-production A3/B0 silicon like on the initial CRB boards (i.e 1023 build)
 - Remaining images (Example: CA_ICH9M_REL_IAMT_BYP_ME_UPD_PreProduction.BIN) are Intel ME image files to be used [only with the Firmware Update Tool](#) (FWUpdate Tool). For more details on this tool, please refer to the document – 'Intel® AMT Tools User Guide.pdf', located in the folder: "Unzipped_folder"\iAMT Tools\ (Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\iAMT Tools\Intel® AMT Tools User Guide.pdf)
1. Select the Intel ME image (Example: CA_ICH9M_REL_IAMT_BYP_ME_PreProduction.BIN) from this location, and click 'Open'.
 2. Click 'OK' and the dialog box closes.
 3. The remaining parameters are left with default values.

4.4.3 GbE region

1. Click the 'GbE Region' node in the left pane of the main window.
2. All the parameters of the 'GbE Region' are displayed in the right pane.
3. Double-click the 'Binary input file' parameter.
4. A dialog box will appear, entitled 'Binary input file'.
5. Click the Browse (...) button and open the directory where the GbE image is located. (Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\NVM Image\GbE).
6. Select the BOAZ GbE image file (NAHUM2_BOAZ_A0.bin) from this location and click on 'Open'.
7. Click 'OK' and the dialog box closes.
8. Double-click the 'MAC address' parameter.
9. A dialog box will appear, entitled, 'MAC address'.
10. Enter the 48-bit MAC address (Physical Address) for the host adapter on the target platform. (Example: 00 12 34 56 78 91)
11. Click 'OK' and the dialog box closes.

Note:

- The GbE MAC Address set in the steps above must be unique for all systems on a network.
12. The remaining parameters are left with default values.

4.4.4 BIOS region

- 1) Click to select the 'BIOS Region' node in the left pane.
- 2) All the parameters of the 'BIOS Region' are displayed in the right pane.
- 3) Double-click the 'Binary input file' parameter.
- 4) A dialog box will appear, entitled 'Binary input file'.
- 5) Click to select the Browse (...) button and open the directory where the BIOS image (Intel Reference BIOS) is located. (Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\NVM Image\BIOS).



- 6) Select the BIOS image file from this location and click **OPEN** (Example: "CAMPGOXX.ROM" for the Montevina CRB).
- 7) Click 'OK' and the dialog box closes.
- 8) The remaining parameters are left with default values.

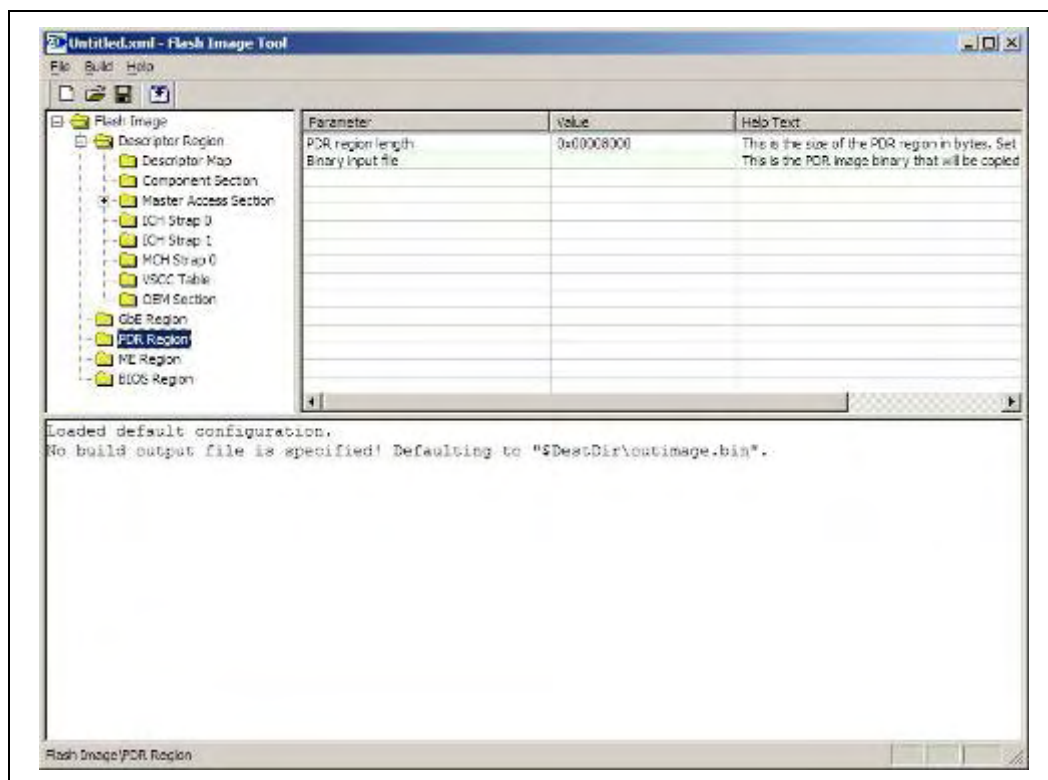
4.4.5 Platform Data Region

Ensure that the Platform Data Region is enabled. This option is disabled by default in Fitc.

- 1) Right Click on the PDR Region and select the Enable Region option.
- 2) As the system supports VA, the PDR region length must be set to 0x8000

Note: This region is reserved for VA 4.0 and is not to be used for OEM storage.

Figure 5. PDR Region



4.4.6 ME Parameters

The ME section allows the user to specify the manageability features. The parameters values can be found in the help text next to the parameter value.



Figure 6. ME Region

	<table> <tr> <th>Parameter</th><th>Value</th></tr> <tr> <td>Manageability Mode</td><td>1</td></tr> <tr> <td>Manageability Mode Lock</td><td>false</td></tr> <tr> <td>Local Firmware Update Enabled</td><td>false</td></tr> <tr> <td>Local FWU Override Counter</td><td>-1</td></tr> <tr> <td>Local FWU Override Qualifier</td><td>2</td></tr> <tr> <td>BIOS Reflash Capable</td><td>false</td></tr> <tr> <td>MEManuf Test Counter</td><td>8</td></tr> <tr> <td>ME Visual LED Indicator Enabled</td><td>false</td></tr> <tr> <td>LAN Power Well</td><td>2</td></tr> </table>	Parameter	Value	Manageability Mode	1	Manageability Mode Lock	false	Local Firmware Update Enabled	false	Local FWU Override Counter	-1	Local FWU Override Qualifier	2	BIOS Reflash Capable	false	MEManuf Test Counter	8	ME Visual LED Indicator Enabled	false	LAN Power Well	2
Parameter	Value																				
Manageability Mode	1																				
Manageability Mode Lock	false																				
Local Firmware Update Enabled	false																				
Local FWU Override Counter	-1																				
Local FWU Override Qualifier	2																				
BIOS Reflash Capable	false																				
MEManuf Test Counter	8																				
ME Visual LED Indicator Enabled	false																				
LAN Power Well	2																				

4.4.6.1 Temporary Firmware Update parameters

When **Local FWU Override Counter** has a value between 1 and 255, firmware updates are allowed even if updates are disabled in the ME BIOS Extension settings. After the flash is programmed, each time the machine restarts it causes **Local FWU Override Counter** to be decremented. When **Local FWU Override Counter** reaches 0, firmware updates are no longer allowed if they are not enabled by the ME BIOS Extension settings.

Note: The restart that takes place after the flash memory has been programmed also causes **Local FWU Override Counter** to be decremented. Therefore if you want to enable updating the firmware **N** times, you need to assign **Local FWU Override Counter** the initial value **N+1**.

If **Local FWU Override Counter** is set to -1 and **Local Firmware Override Qualifier** is set to 0, firmware updates are always allowed regardless of the settings in the ME BIOS extension

The following table shows the possible value combinations for the two variables. To enable local firmware updates, make sure both variables are assigned the correct values.

Table 4. Firmware Override Update Variables

	Local FWU Override Qualifier = 0 (zero)	Local FWU Override Qualifier = 1 (one)	Local FWU Override Qualifier = 2 (two)
Local FWU Override counter = 0 (zero)	Local Firmware Updates <u>NOT</u> Allowed	Local Firmware Updates <u>NOT</u> Allowed	Local Firmware Updates <u>NOT</u> Allowed
Local FWU Override Counter = -1 (minus one)	Local Firmware Updates Allowed	Local Firmware Updates <u>NOT</u> Allowed	Local Firmware Updates Allowed only until ME is configured
Local FWU Override Counter = 0 < n < 255	Local Firmware Updates Allowed	Local Firmware Updates Allowed	Local Firmware Updates Allowed



4.4.6.2 AMT Section

The AMT section allows the user to specify the default AMT parameters. After the Intel® AMT system is Un-provisioned (full or partial) the values specified in this section will be used.

Figure 7. AMT Region

Parameter	Value
Configuration Server Port	0
Configuration Server Name	ProvisionServer
Configuration Server IP	0.0.0.0
AMT Host Name	IntelAMT
AMT Domain Name	amt.intel.com
DHCP Enabled	false
AMT Ping Response Enabled	true
AMT Static IP Address	192.168.0.15
AMT Static IP Subnet Mask	0.0.0.0
AMT Static IP Default Gateway Address	0.0.0.0
AMT Static IP Primary DNS Address	
AMT Static IP Secondary DNS Address	
VLAN	0
IDER Boot Capable	true
SOL Boot Capable	true
Boot into BIOS Setup Capable	true
Pause during BIOS Boot Capable	true
HostIF IDER Enabled	true
HostIF SOL Enabled	true
Idle Timeout - Manageability Engine	1
MEManuf Test Counter	8

Enter values for the following fields (Example values have been given):

- AMT Host Name (Example: IntelAMT)
- AMT Domain Name (Example: amt.intel.com)
- AMT Static IP Address (Example: 192.168.0.15)

Leave all other values in the file as they are.

NOTE:

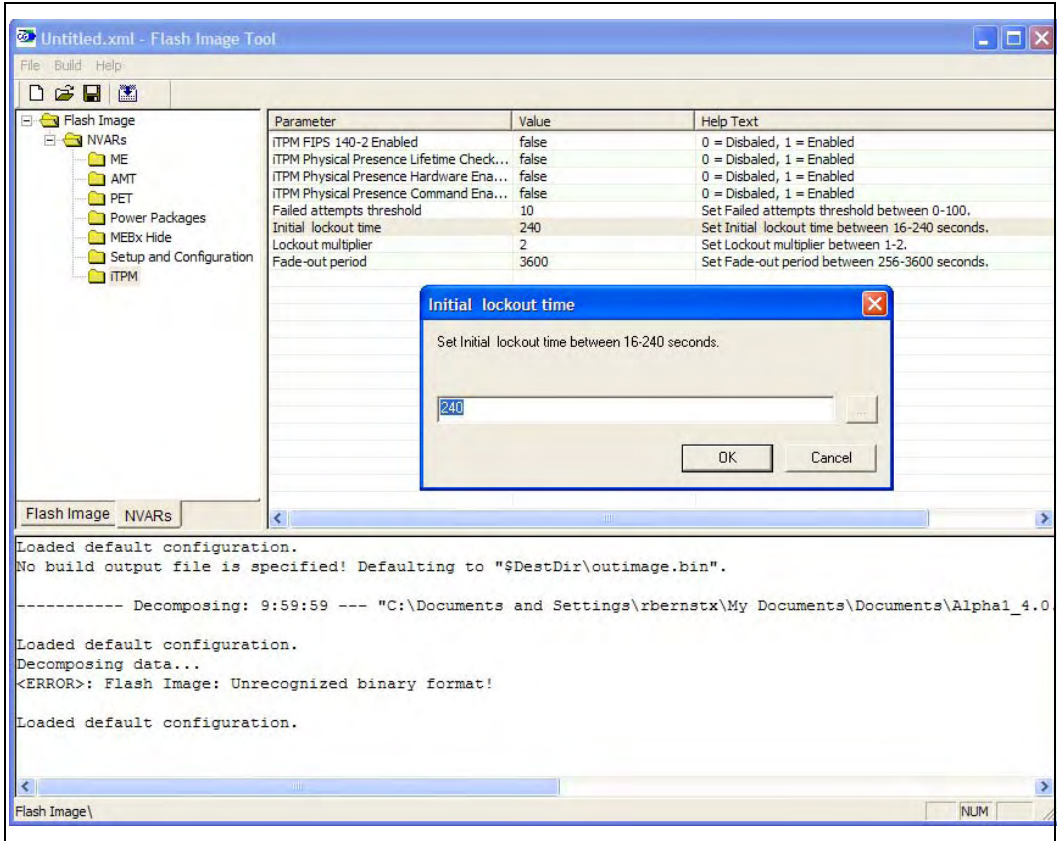
- The 'AMT Dedicated MAC', also known as the Intel ME MAC address (or MNGMAC address) is now the same MAC address set on the GbE region, this has changed from the initial pre-alpha release where two different MAC addresses were required.

Idle Timeout specifies the amount of time (in minutes) before the system goes into an M-off state if ME-WOL is enabled. This value can be modified by the end user in the MEBX. To reduce the amount of end user configuration time, this value should be set to a reasonable value.



4.4.6.3 iTPM Section

Figure 8. iTPM Region





The following is a list of the iTPM parameters along with their defaults that can be modified.

Table 5. iTPM Permanent Flags

Bit	Flag	Description	Default
0	FIPS	TRUE: This TPM operates in FIPS mode FALSE: This TPM does NOT operate in FIPS mode	FALSE
1	Physical Presence Lifetime Lock	FALSE: The state of either physicalPresenceHwEnable or physicalPresenceCmdEnable MAY be changed TRUE: The state of either physicalPresenceHwEnable or physicalPresenceCmdEnable MUST NOT be changed for the life of the TPM	FALSE
2	Physical Presence HW Enable	FALSE: Disable the hardware signal indicating physical presence TRUE: Enables the hardware signal indicating physical presence	FALSE
3	Physical Presence CMD Enable	FALSE: Disable the command indicating physical presence TRUE: Enables the command indicating physical presence	TRUE

Table 6. Dictionary Attack Flags

Bit	Field	Description	Default	Min	Max
0	Auth Fail Threshold	Number of failed auth attempts which will trigger lockout	10	1	100
1	Initial Lockout Time	Duration in seconds of first lockout period	240	16	0xFFFF
2	Lockout Increase Factor	Factor by which lockout period is multiplied with every additional failed auth	2	1	0xFFFF



Bit	Field	Description	Default	Min	Max
3	Fade Out Time	Every time this period (in seconds) passes with no auth failures, lockout time will be reduced (divided by Lockout Increase Factor)	3600	256	0xFFFF

4.4.7 Save configuration

The following steps are used to save the configuration settings you made in the previous sections:

- 1) Click 'File' on the top menu of the window, and then click 'Save'.
- 2) A dialog box will open which will take as input the name of the file under which the present configuration will be saved.
- 3) Use the pull-down to choose the folder where you want to place the file (Example "Unzipped_folder", and enter the file name (Example: config.xml) and click the 'Save' button.
- 4) Close the main window.

The configuration settings are now saved under the filename (and the path) you specified earlier (Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\config.xml)

Note:

- The purpose of saving your configuration to an .xml configuration file (as described above) is so that image layouts need not be recreated each time.

4.5 Building the flash image

An image can be created in two ways:

- 1) **GUI:** To create an image from a previously-saved configuration file:
 - Double-click on 'fitc.exe'.
 - Click on 'File' in the top menu of the window and then click on 'Open'.
 - Select the configuration file, (Example: config.xml), and then click the 'Open' button. This will load the configuration file.
 - Click on 'Build' in the top menu of the window and then click on 'Build Image'. (Pressing <F5> after opening a stored configuration file will also execute the build process.)

To create an image without a previously-saved configuration file:

- Double-click on 'fitc.exe' and perform all steps as described in section 4.1.
- Click 'Build' in the top menu of the window and then click 'Build Image' (or press <F5>) after you have configured all the various sections.



- 2) **Command Line:** The flash image tool is also supported on the Windows XP command line interface. The following syntax is used to execute the flash image tool on the command line:

- `fitc.exe [xml_file] [/o <file>] /b`

Where:

<xml_file> : The XML configuration file saved when configuring using the flash image tool.

/o <file> : The path and filename where the image will be saved. This command overrides the 'Output path' in the XML file.

/b : Automatically builds the flash image.

The UI will not be shown if this flag is specified. This causes the program to run in auto-build mode. If there is an error, an error message will be displayed and the build will not occur.

(Example: `fitc.exe config.xml /o outimage.bin /b`)

The 'config.xml' file used in the command above is created and saved using the GUI as explained in previous sections.

Is it possible as well to override the binaries from the xml file, example using the command line:

```
fitc config.xml /o ./outimage.bin /b /gbe NAHUM2_BOAZ_A0.bin /bios  
CAMPG028.ROM /me CA_ICH9M_REL_IAMT_BYP_ME_PreProduction.BIN
```

- The output of the build (a binary file) will be created in directory specified by the '\$DestDir' environment variable, which you set during the initial setup of flash image tool earlier in this document. This directory will contain the image map (Example: `outimage_Map.txt`), the flash image created (Example: `outimage.bin`) and a folder named 'Int' containing four intermediate build binaries (Example: `BIOS Region.bin`, `Descriptor Region.bin`, `GbE Region.bin` and `Intel ME Region.bin`). The final flash image (Example: `outimage.bin`) is the file which will be programmed into the flash devices as explained later.
- Note: when 2 SPI parts are specified in the flash image tool (as with the Montevina Pillar Rock CRB), the output directory will also contain 2 additional binary files (example: `outimage(1).bin` and `outimage(2).bin`). These files are for use with an external flash programmer, and will not be used in this process. They can be ignored.
- For more information on the flash image tool, please refer to the document - 'Intel® flash image tool.pdf', located in the folder:

"Unzipped_folder"\Tools\System Tools\flash image tool\

(Example: `E:\IAMT_ASF2_iTPM_4.0.0.xxxx\Tools\System Tools\flash image tool\Intel® flash image tool.pdf`)

**Result:**

The result of using the flash image tool is the flash image file (Example: outimage.bin) created by integrating the component images, namely, the BIOS image, the GbE image and the Intel ME image. The flash image file will be located in the directory defined by the \$DestDir environment variable, as mentioned above. For Montevina, this image binary file will be 4MB in size.

4.6 Programming the image onto the flash

Prior to manufacturing, there are two ways to load the flash image file (Example: outimage.bin) onto the flash. These are described in the following two sections (4.7 and 4.8):

Note: If you are re-flashing a full image onto an AMT platform previously programmed you must make sure to clear the CMOS to ensure that the platform reloads the default parameters and to ensure that there are no erroneous settings remaining.

4.7 Using a flash programmer

An external Flash Programmer/Burner can be used to write the flash image file onto the flash. When you use the flash image tool (FITC) to generate a flash image, in addition to the final output binary (outimage.bin), the tool also creates two separate binary images, named "outimage(1).bin" and "outimage(2).bin".

These two binary images are generated for the purpose of using an external flash programmer to program the SPI devices without having them installed on the system board. Each of the two binary image files mentioned above corresponds to a separate SPI device in the case that two parts are implemented on the board (as with the Pillar Rock CRB). If the system has only one part you must use the complete binary file.

Multiple commercial flash burners are available. The description of the use of these is beyond the scope of this document.

4.8 Using the flash programming tool

The flash programming tool is supported on the following operating systems - DOS, Free DOS, DRMK DOS, Windows XP SP2 and Windows PE. If you are using a DOS environment to program the image in to the flash, follow the steps in section 4.8.1. If you are using the Windows environment to program the image in to the flash, follow the steps in section 4.8.5.



Note: Make sure the ME (management engine) is disabled before flashing a full image. This can be done by removing the memory module installed on Bank 0, or by using a special jumper. If ME is running there may be a risk of corrupting the new image while flashing it, rendering the system unusable and requiring to re-program the flash chip by a stand alone programmer.

4.8.1 DOS environment

4.8.1.1 Flash programming tool from VIP

The DOS flash programming tool can be accessed under the following directory:

"Unzipped_folder"\Tools\System Tools\Flash Programming Tool\DOS\

(Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\System Tools\Flash Programming Tool\DOS \fpt.exe)

The files in the 'Flash Programming Tool\DOS\' folder are:

1. **fpt.exe:** This is the executable to write the flash image file into the flash.
2. **License.rtf:** This contains the Intel® Software License Agreement.
3. **System Tools User Guide.pdf:** This document gives more details on the flash programming tool and others.
4. **readme.txt:** This file contains the description and usage of the 'fpt.exe' tool.

IMPORTANT: DOS4GW.exe is necessary to use the flash programming tool. DOS4GW can be downloaded from the following URL:
<http://www.scene.org/file.php?file=%2Fresources%2Fdos4gw.exe&fileinfo>.

Download the 'dos4gw.exe' file and save this file to the same directory as 'fpt.exe':

"Unzipped_folder"\Tools\System Tools\Flash Programming Tool\DOS\

(Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\System Tools\Flash Programming Tool\DOS\)

4.8.2 Load files onto the target platform

The Flash Programming Tool files are loaded onto the target platform as follows:

1. Create the final flash image file (Example: outimage.bin) and copy all the files along with the Flash Programming Tool (fpt.exe, fparts.txt and DOS4GW.exe) to a medium that is accessible to the target platform (for example, using a USB pen drive or other media that can be made accessible to DOS on the target platform).
2. Boot the target platform to DOS.
3. Change to the directory where the Flash Programming Tool and the flash image file (outimage.bin) are stored.



4.8.3 Query the flash devices

To ensure that the flash programming tool recognizes the SPI flash devices on the target platform before programming the flash image file onto the flash, execute the following at the DOS prompt:

- `fpt /i`

Under 'Flash Devices Found' in the output, all flash devices on the target platform should be listed.

Example: The following will be displayed:

--- Flash Devices Found ---

SST25VF016B ID: 0xBF2541 Size: 2048KB (16384Kb)

SST25VF016B ID: 0xBF2541 Size: 2048KB (16384Kb)

NOTE:

- Initially, if no descriptor is present on the SPI flash, only the first flash part is listed (even if two flash parts are present on the target platform). Once the flash descriptor is loaded, both the flash parts will be listed upon subsequent execution of the above-referenced command.
- If no flash parts enumerate, please verify that the SPI part you are using is listed in the `fparts.txt` file and that your BIOS is correctly setting up the VSCC register as defined by the latest Intel® I/O Controller Hub (ICH9M) BIOS specification.

4.8.4 Program the image

To program the final flash image file (Example: `outimage.bin`) onto the SPI flash, execute the following command at the DOS prompt. *(remember to disable ME)*

- `fpt /f: <filename>`

(Example: `fpt /f outimage.bin`)

After having successfully programmed the flash image (Example: `outimage.bin`) onto the SPI flash devices, the following message will be displayed: **'Write Complete.'**

Unplug the power cord and the network cable (G3 reset), and then reattach them after 10 seconds. This ensures all capacitors on the board are fully discharged before the system starts up again.

Result:

- The flash image file (Example: `outimage.bin`) has now been successfully programmed onto the SPI device.



NOTE:

- For more details on this tool, please refer to the document - 'Intel® Flash Programming Tool.pdf', located in the folder:

"Unzipped_folder"\Tools\System Tools\Flash Programming Tool\

(Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\System Tools\Flash Programming Tool\Intel® Flash Programming Tool.pdf)

4.8.5 Windows environment

The Windows version of the flash programming tool is a command line tool designed for use within the Windows command shell environment (cmd.exe).

4.8.5.1 Flash programming tool from VIP

The Windows Flash Programming Tool can be accessed under the following directory:

- "Unzipped_folder"\Tools\System Tools\Flash Programming Tool\Windows\
- (Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\System Tools\Flash Programming Tool \Windows\fptw.exe)

The files in the '\Flash Programming Tool\Windows\' folder are:

1. **fparts.txt:** This file contains a comma separated list of attributes for supported flash devices. The text in the file explains each field. An additional entry may be required in this file (to be added) to describe the flash part which is on the target system. Examine the target board before adding in the appropriate attribute values. Default values are already entered for SPI devices used with Intel Customer Reference Boards (CRBs).
2. **fptw.exe:** This is the executable to write the flash image file to the SPI flash devices.
3. **sseIdrv.dll32e.dll:** Supported library file.
4. **ssePmxdll32e.dll:** Supported library file.
5. **ssepmxdrv.sys:** Supported system file.



4.8.6 Load files onto the target platform

Use the flash programming tool to load the files onto the target platform as follows:

1. Create the final flash image file (Example: outimage.bin) and copy all the files along with the Flash Programming Tool (fptw.exe, fparts.txt, sseldrvidl32e.dll, ssePmxdll32e.dll and ssepmdrv.sys) to a medium that can be made accessible to the target platform (for example, use a USB pen drive or other media that can be made accessible to Windows on the target platform).
2. Boot the target platform to Windows and open a command prompt window.
3. Change to the directory where the flash programming tool and the flash image file (outimage.bin) are located.

4.8.7 Query the flash devices

To ensure that the flash programming tool recognizes the SPI flash devices on the target platform before programming the flash image file onto the flash, execute the following at the command prompt:

- `fptw /i`

Under 'Flash Devices Found' in the output, all flash devices on the target platform should be listed.

Example: The following will be displayed:

--- Flash Devices Found ---

SST25VF016B ID: 0xBF2541 Size: 2048KB (16384Kb)

SST25VF016B ID: 0xBF2541 Size: 2048KB (16384Kb)

NOTE:

- Initially, if no descriptor is present on the SPI flash, only the first flash part is listed (even if two flash parts are present on the target platform). Once the flash descriptor is loaded, both the flash parts will be listed upon subsequent execution of the above-referenced command.
- If no flash parts enumerate, please verify that the SPI part you are using is listed in the fparts.txt file and that your BIOS is correctly setting up the VSCC register as defined by the latest Intel® I/O Controller Hub (ICH9M) BIOS specification.



4.8.8 Program the image

To program the final flash image file (Example: outimage.bin) onto the flash devices, execute the following command at the command prompt. *(remember to disable ME)*

- `fptw /f <filename>`

(Example: `fptw /f outimage.bin`)

After having successfully programmed the flash image onto the SPI flash devices, the following message will be displayed: **'Write Complete.'**

Unplug the power cord and the network cable, and then reattach them after 10 seconds. This ensures all capacitors on the board are fully discharged before the system starts up again.

Result:

- The flash image file (Example: outimage.bin) has now been successfully programmed onto the SPI flash device.

NOTE:

- For more details on this tool, please refer to the document - 'Intel® Flash Programming Tool.pdf', located in the folder:
 - "Unzipped_folder"\Tools\System Tools\Flash Programming Tool\
 - (Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\System Tools\Flash Programming Tool\Intel® Flash Programming Tool.pdf)

4.9 Installing EC Firmware

- Extract all files ("Unzipped_folder"\NVM Image\EC). Keep all files in the same folder to a single directory of your choice on the host machine or on a floppy disk (recommended).
- Boot host in DOS mode.
- From the host directory where you extracted the files, run the following command line: **KSCFlash ksc.bin**
- This file will flash KSC firmware

After installing the KSC FW make sure system is shutdown and G3 operation is performed before rebooting back to make sure update was successful.



5 BIOS Setup

5.1 Set Parameters

The following steps are used for setting up parameters in the BIOS setup screen on the target platform (CRB) after you have programmed the image onto the flash devices. **Remember to always start with a fresh OS install on the platform any time you are enabling a new FW image.**

1. Press 'Del' during Setup message display at power-on to enter the BIOS Setup screen.
2. Once you are in BIOS Setup, load the default BIOS settings.
3. Update the time and date if it is incorrect.
4. Go to the "Advanced" Menu -> "AMT configuration" -> and Enable "Intel AMT"
5. Save changes and exit BIOS setup. Disconnect the power cord for at least 10 seconds and then restart the system (G3 power cycle).

NOTE: It is recommended to use a PS/2 keyboard instead of USB for preliminary releases.

5.2 iTPM Parameters on BIOS

NOTE: If you are using the Pillar Rock CRB FAB2, a board rework is needed as described on appendix A.

To modify the iTPM BIOS parameters:

Press **Del** during **Setup** message display at power-on to enter the BIOS Setup screen.

Load optimal setting, press **F3**

Select **Advanced**.

Select **TPM**.

The following options are available:

TPM Device (Disabled/Enabled) → Enabled (Enable/Disable the TPM Device)

TPM State (Deactivate/Activate) → Activate (Activate/Deactivate the TPM Device)

TPM Force Clear (Disabled/Enabled) → Disabled (Force Clear TPM data)

Press **F4** to save changes and exit BIOS setup.



6 *Intel® Management Engine BIOS Extension Setup*

6.1 Intel® Management Engine BIOS Extension screen

NOTE:

- The default power policy is M0ff during Sx. To allow Intel ME Firmware to go to M1 with network during Sx, the power policy settings as described in this section must be done.

The Intel Management Engine BIOS Extension screen is used to enable Intel® AMT or ASF 2.0 on the target platform (CRB). Follow the below steps:

1. On rebooting the system (as mentioned in the previous section), after the initial boot screen, the following message will be displayed:

'Press <Ctrl-P> to enter Intel ME Setup'. Press 'Ctrl-P'

NOTE:

- Should press <Ctrl-P> as soon as the above message is displayed, as this message will be displayed for only a few seconds.
2. You will be prompted for the password if you enabled MEBx Password in BIOS Setup. If you left MEBx Password disabled in BIOS Setup, skip to step 5.
 3. Enter 'admin' under 'Intel ME Password' (you will change this later). Press Enter.
 4. The Intel Management Engine BIOS Extension screen will be displayed.

NOTE:

- The Intel ME BIOS Extension screen can be used to enable either Intel® AMT or ASF 2.0, not both. If Intel® AMT is to be enabled on the target platform, then follow the steps in section 10.0.1. If ASF 2.0 is to be enabled on the target platform, then follow the steps in section 10.0.2.



6.1.1 Enabling Intel® AMT

This section describes how to enable Intel® AMT using the Intel ME BIOS Extension screen. This section describes how to set the Intel® AMT system in static mode only (for simplicity). The below steps are followed:

1. Select 'Change Intel ME Password'. Press Enter.

Enter a new password under 'Intel ME Password' and then press Enter.

The new password must be strong 7-bit ASCII characters **excluding** ':', ',', and '' characters.

String length is limited to 32 characters.

Limitations:

Password Length: Passwords must comprise of at least 8 characters.

Password Complexity: Password must include:

- a. At least one Digit character ('0', '1',... '9')
- b. At least one 7-bit ASCII non alpha-numeric character, above 0x20, (e.g. '!', '\$', ';').
- c. Both lower-case Latin ('a', 'b',..., 'z') and upper case Latin ('A', 'B',..., 'Z').

Note: '_' (underscore) and ' ' (space) are valid password characters but are **not** used in determination of complexity.

2. 'Verify password' will be displayed. Enter the new password just entered in the previous step. Press Enter.
3. Select 'Intel ME Configuration'. Press Enter.
4. The following message will be displayed:

'System resets after configuration changes. Continue: (Y/N)'.

5. Press 'Y'.
6. The following message will be displayed: 'Acquiring Intel ME Configurations...'
7. Select 'Intel ME State Control'. Press Enter.
8. Select 'Enabled'. Press Enter.
9. Select 'Intel ME Firmware Local Update'. Press Enter.
10. Select 'Enabled'. Press Enter.
11. Select 'Intel® ME Features Control'. Press Enter.
12. Select 'Manageability Feature Selection'. Press Enter.
13. Select 'Intel® AMT'. Press Enter.
14. Select 'Return to Previous Menu'. Press Enter.
15. Select 'Intel® ME Power Control'. Press Enter.
16. Select the desired power policy radio button.
17. Select 'Return to Previous Menu'. Press Enter.
18. Select 'Return to Previous Menu'. Press Enter.
19. The system shuts down. Pull out the power cord and reconnect after 5 seconds. Then, turn on the system.



20. After the initial boot screen, the following message will be displayed:

'Press <Ctrl-P> to enter Intel® ME Setup'

21. Press 'Ctrl-P'.

NOTE:

- Should press <Ctrl-P> as soon as the above message is displayed, as this message will be displayed for only a few seconds.

22. The user will be prompted for the password.

23. Enter the new Intel® ME password (strong password required – see step 2 above). Press Enter.

24. Select 'Intel® AMT Configuration'. Press Enter.

25. The following message will be displayed: 'Connecting to Intel® AMT Client...'

26. The Intel® AMT Configuration screen is displayed.

27. Select 'Host Name'. Press Enter.

28. Type in: IntelAMT. Press Enter.

29. Select 'TCP/IP'. Press Enter.

30. The following message will be displayed:

'Disable Network Interface: (Y/N)'.

31. Press 'N'.

32. The following message will be displayed:

'[DHCP Enabled] Disable DHCP: (Y/N)'.

33. Press 'Y'.

34. The following is displayed: 'IP address:'

35. Enter a static IP address. (Example: 192.168.0.15). Press Enter.

NOTE:

- If more than one Intel® AMT machine is being configured in static IP mode and all these Intel® AMT machines are on a single Local Area Network (LAN), then it should be ensured that each of the static IP addresses are unique. If more than one Intel® AMT device has the same static IP address, then a collision of IP addresses will occur on the network and the Intel® AMT machines will not respond correctly on the network.

36. The following is displayed: 'Subnet mask:'

37. Enter the subnet mask. (Example: 255.255.255.0). Press Enter.

38. The following is displayed: 'Default Gateway address:'

39. Press Enter. (Leave as default value).

40. The following is displayed: 'Preferred DNS address:'

41. Press Enter. (Leave as default value).

42. The following is displayed: 'Alternate DNS address:'

43. Press Enter. (Leave as default value).

44. The following is displayed: 'Domain name:'

45. Enter the domain name. (Example: amt.intel.com). Press Enter.

46. Select 'Provision Model' from the menu. Press Enter.

47. The following message is displayed: '[Enterprise] Change to Small Business: (Y/N)'. Press 'Y'.

48. Select 'SOL/IDER'. Press Enter.

49. The following message is displayed: '[Caution] System resets after configuration changes. Continue (Y/N)'. Press 'Y'.

50. The following message is displayed: 'Username & Password'.

51. Select 'Enabled'. Press Enter.

52. The following message is displayed: 'Serial Over LAN'.



53. Select 'Enabled'. Press Enter.
54. The following message is displayed: 'IDE Redirection'.
55. Select 'Enabled'. Press Enter.
56. Select 'Return to Previous Menu'. Press Enter.
57. Select 'Exit'. Press Enter.
58. The following message will be displayed:

'Are you sure you want to exit? (Y/N):'

59. Press 'Y'.
60. The system will boot to OS.

6.1.2 Enabling ASF 2.0

This section describes how to enable ASF 2.0 using the Intel® ME BIOS Extension screen. The below steps are followed:

1. Select 'Change Intel® ME Password'. Press Enter.

Enter a new password under 'Intel ME Password' and then press Enter.

The new password must be strong 7-bit ASCII characters **excluding ':' , ',' and '''' characters.**

String length is limited to 32 characters.

Limitations:

Password Length: Passwords must comprise of at least 8 characters.

Password Complexity: Password must include:

- a. At least one Digit character ('0', '1',...'9')
- b. At least one 7-bit ASCII non alpha-numeric character, above 0x20, (e.g. '!', '\$', ';').
- c. Both lower-case Latin ('a', 'b',..., 'z') and upper case Latin ('A', 'B',...'Z').

Note: '_' (underscore) and ' ' (space) are valid password characters but are **not** used in determination of complexity.

2. 'Verify password' will be displayed. Enter the new password just entered in the previous step. Press Enter.
3. The following message will be displayed:

'System resets after configuration changes. Continue: (Y/N).'

4. Press 'Y'.
5. The following message will be displayed: 'Acquiring Intel® ME Configurations...'.
 6. Select 'Intel® ME State Control'. Press Enter.
 7. Select 'Enabled'. Press Enter.
 8. Select 'Intel® ME Features Control'. Press Enter.
 9. Select 'Manageability Feature Selection'. Press Enter.
 10. Select 'ASF'. Press Enter.



11. Select 'Return to Previous Menu'. Press Enter.
12. Select 'Intel® ME Power Control'. Press Enter.
13. Select 'Intel® ME State upon Initial Power-On'. Press Enter.
14. Select 'ON'. Press Enter.
15. Select 'Intel® ME ON in Host Sleep States'. Press Enter.
16. Select 'ALWAYS'. Press Enter.
17. Select 'Return to Previous Menu'. Press Enter.
18. Select 'Return to Previous Menu'. Press Enter.
19. The system shuts down. Pull out the power cord and reconnect after 10 seconds.
20. Turn on the system and boot to the OS.

§



7 Installing drivers

7.1 Driver identification

NOTE: Before the drivers mentioned in this section are installed, make sure to install the chipset INF (This is required for proper installation of the Intel® ME Interface and LMS/SOL drivers). It is also recommended to install the graphics drivers.

The following drivers must be installed on the target platform before continuing. Some of the Montevina/ICH9M tools used will require these drivers to be installed.

The drivers to be installed are:

1. Intel® ME Interface driver - The setup file for installing the Intel® ME Interface driver can be accessed from under the following directory:
 - "Unzipped_folder"\Drivers\MEI\
 - (Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Drivers\MEI\Setup.exe)
2. GbE driver -Copy the GbE driver onto the target platform (CRB) from the following location:
 - "Pro_Lan_Driver\Montevina_LAN_xx.zip"

And update the GbE driver on the target platform.

NOTE: The above zip component can be downloaded from the same web page where you obtained the kit.

3. LMS_SOL driver - The setup file for installing the LMS_SOL driver can be accessed from under the following directory:
 - "Unzipped_folder"\Drivers\LMS_SOL\
 - (Example: E:\iAMT_ASF2_i_4.0.0.xxxx\Drivers\LMS_SOL\Setup.exe)

NOTE:

- The LMS_SOL driver is to be installed only if the downloaded kit contains firmware for Intel® AMT.



NOTE:

- Section 7 is only applicable if the downloaded kit has firmware for Intel® AMT and Intel® AMT has been enabled as described in section 6.1.1
- If the downloaded kit has firmware for ASF 2.0, and if ASF has been enabled as described in section 6.1.2, then for further details on configuring the client system, please refer to the documents under the following directory:

`"Unzipped_folder"\Tools\ASF 2.0 Tools\ASF Agent\DOCS\GUIDE\`

(Example: `E:\iAMT_ASF2_XXX_4.0.0.xxxx\Tools\ASF 2.0 Tools\ASF Agent\DOCS\WS03XP2K`)

- For details on the ASF Tools and their installation instructions, please refer to: 'readme.txt' document, which can be downloaded from the same web page where you downloaded the kit.
- Please note that the Linux section under these documents is not relevant for Montevina/ICH9M, as Montevina/ICH9M does not provide ASF Linux support. Only old Intel® NICs, like Tabor, Tekoa, Ophir, ESB2, etc, support ASF on Linux.

4. TPM Driver installation

The setup file and documentation for installing the Intel® iTPM driver can be accessed from under the following directory:

`"Unzipped_folder"\Drivers\iTPM\`

Instructions for installing the iTPM driver can be found in the **iTPM Driver Installation Guide** document included on this folder

§



8 Basic Intel® AMT functional demonstration

8.1 Ping verification

Ping verification tests the network connection between the target platform (CRB/Intel® AMT device) and other systems on the network. This is done as follows:

- 1) Connect the system under test (client system/Intel® AMT machine) to the management console (any other system on the network) through a Local Area Network. This connection can be done in two ways:
 - Connect an Ethernet cross cable between the client system and the management console.
 - Or, use a hub/switch to connect the client system and the management console.

NOTE:

- When connecting the Intel® AMT system to a Local Area Network (LAN) with multiple Intel® AMT machines on the LAN (all configured in static IP mode), ensure that each of the machines have a unique static IP address (set in the 'Intel® AMT Configuration Screen' as described in section 6.1.1)
- If Intel® AMT device is configured in static IP mode, then the host machine (OS) of the Intel® AMT machine must also be configured in static IP mode. The host static IP address must be different from the Intel® AMT static IP address (set up in the 'Intel® AMT Configuration screen' as described in section 6.1.1). Also, the host static IP address must be unique across the LAN when multiple Intel® AMT systems are connected to the LAN.
- To configure the host machine of the Intel® AMT system in static IP mode, follow the below steps:
 - Boot the host system through Windows operating system.
 - Click on 'Start' on the windows tool bar, and select 'Control Panel'.
 - The 'Control Panel' window is displayed. Select 'Network Connections' and double click on it.
 - Right-Click on 'Local Area Connection' and select 'Properties'.
 - In the 'General' tab, select 'Internet Protocol (TCP/IP)' and click on 'Properties'.
 - Select the option 'Use the following IP address'.
 - Enter a static IP address under 'IP address'. Example: 192.168.0.20

NOTE: This IP address must be different from the static IP address set in the 'Intel® AMT Configuration Screen'.



- Enter the subnet mask (255.255.255.0) under 'Subnet mask'.
- Click 'OK' and then on 'Close' to save the parameters entered as above.

- 2) Boot the Management Console system into Windows.
- 3) Ensure that the Management Console is configured in static IP mode:
 - a) On the host system, click on 'Start' on the windows tool bar, and select 'Control Panel'.
 - b) The 'Control Panel' window is displayed. Select 'Network Connections' and double click on it.
 - c) Right-Click on 'Local Area Connection' and select 'Properties'.
 - d) In the 'General' tab, select 'Internet Protocol (TCP/IP)' and click on 'Properties'.
 - e) Select the option 'Use the following IP address'.
 - f) Enter a static IP address under 'IP address'. Example: 192.168.0.10

NOTE: This IP address must be different from the static IP address set on the Intel® AMT machine (in the 'Intel® AMT Configuration Screen') and the host IP address of the Intel® AMT machine.

Also make sure any firewall software is disabled under Windows in both the host machine and the console machine

- g) Enter the subnet mask (255.255.255.0) under 'Subnet mask'.
- h) Click 'OK' and then on 'Close' to save the parameters entered as above.

- 4) Open the Windows command line interface on the management console.
- 5) Ping the Intel® AMT device (target platform).

ping <IP-address of Intel® AMT machine> (Example: ping 192.168.0.15)

- 6) Ping the host operating system from the management console.

ping <IP-address of the host OS> (Example: ping 192.168.0.20)

- 7) Ping the management console from the host operating system.

ping <IP-address of the management console> (Example: ping 192.168.0.10)

- If the client machine is connected to the management console through the network, then the ping is successful and returns the bytes of data transferred.
- If the ping returns: 'Request timed out', then either one of the following might be the cause:
 - a) The system under test (client machine) is not connected to the network properly, or
 - b) The user has not set the IP parameters of the Intel® AMT system (target platform/CRB) correctly.



- **Troubleshooting:** If the 'ping verification' is not working, then try the following:
 - Make sure Windows Firewall or any other firewall software is turned off on both machines
 - Ping <IP-address of Intel® AMT host OS>, i.e., 192.168.0.20 from the management console. Ping the management console from the host OS of the client machine, i.e., ping 192.168.0.10. This will help verify network connectivity. If this fails check your network setup.
 - Reboot both the systems, client machine (Intel® AMT system) and the management console, and try again.
 - Configure the network driver with static IP. This IP address must be different from the Intel® AMT Static IP address (configured in the 'Intel® AMT Configuration screen' as described in section 6.1.1). But must be configured on the same subnet.
 - Verify all IP address configurations and try again.

NOTE: When pinging the Intel® AMT device, make sure the management console and the system under test (client machine/target platform operating system) are operating in the same segment, i.e., the management console, Intel® AMT device and the host OS of the Intel® AMT device should be configured in static IP mode or all the three of them should be configured in DHCP mode.

8.2 Test Intel® AMT using the WebUI

To ensure that Intel® AMT is enabled on the host system (client system), the user should try to access Intel® AMT via the WebUI application. This may be done from any system on the network with one of the following browsers installed:

- Microsoft* Internet Explorer 6 SP1 or newer
- Netscape* Navigator 7.1 or newer.
- Mozilla* Firefox* 1.0 or newer.
- Mozilla 1.7 or newer.

NOTE: Other browsers may or may not work as they have not been officially tested.

The Web UI cannot be accessed locally (from the host operating system of the Intel® AMT machine). You can access AMT remotely from another machine.

To access Intel® AMT via the WebUI, follow the steps given sequentially:

- 1) Open a web browser (any of above listed, and supported on the management console), and in the address box, enter one of the following:
 - If the network can resolve the client computer name to an IP address (i.e., a DNS server is installed or the name is listed in the hosts file), then: `http://host_name:16992` (Example: <http://clientname1:16992>).
 - If the client system has a static IP address, then:

`http://host_name:16992` (Example: <http://192.168.0.15:16992>).



- 2) A Login web page will be displayed. Click to select the 'Log On...' button, and a login dialog box is displayed.
- 3) In the 'User name' box enter 'admin', and in the 'Password' box enter the same password as changed in the 'Intel® Management Engine BIOS Extension' screen setup.

Once the username and password have been successfully entered, the web browser opens the Intel® AMT Web User Interface page and the web interface can be used for browsing through the various options present.

§



9 Basic iTPM functional demonstration

Prior to testing the iTPM, the iTPM driver must be installed. Refer to the iTPM Windows XP Driver Installation Guide.

Note: If you are using the Pillar Rock CRB FAB2, a board rework is needed as described on appendix A.

9.1 XP Verification

To verify that the iTPM has been recognized under Windows XP:

Click **Start**, then **Control Panel**.

Click **System**, then **Hardware** and select **Device Manager**.

Click on **System Devices** and verify that **Trusted Platform Module** is listed.

9.2 Vista Verification

There are two methods to verify that the iTPM has been recognized under Windows Vista:

9.2.1 Method 1

Click **Start**, then **Run**.

Type **tpm.msc** and press **ENTER**.

The **TPM Management on Local Computer** window will be displayed. This will indicate whether the iTPM has been recognized and its state (enabled, active, owned).

9.2.2 Method 2

Click **Start**, then **Settings**, then **Control Panel**.

Click **System and** select **Device Manager**.

Click on **Security Devices** and verify that **Trusted Platform Module 1.2** is listed.



10 Intel® AMT Tools

This section describes the various tools you can use to test and verify AMT functionality, configuration and behavior. These tools are typically included in the kit or available separately from VIP. Any tool included in a kit release should supersede any version available from any other source. Always consider the tools and documentation supplied with the kit as the latest revision above all others.

System Requirements for the AMT tools:

These tools are supported by the following operating systems:

- Windows* Server 2003
- Windows* XP SP1 or SP2
- Windows Vista*

10.1 AMTVTL tool

NOTE: For Alpha1 release this tool requires .NET Framework to be installed on the local OS.

The AMTVTL tool is used to check the functionality of a local Intel® AMT system. It is a command line executable and must be run locally on an Intel® AMT machine. AMTVTL tool needs the following services to be installed:

- Intel® AMT Local Manageability Service (LMS)
- Intel ME Interface driver.

The tool checks that the following components are working:

- LMS
- Intel ME Interface driver
- Firmware Intel ME Interface network interface (LME)
- Storage Manager in firmware.



10.1.1 AMTVTL from VIP

The AMTVTL tool can be accessed from under the following directory:

"Unzipped_folder"\Tools\iAMT Tools\iAMTVTL\

(Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\iAMT Tools\iAMTVTL\AMTVTL.exe)

10.1.2 Executing AMTVTL

On the command line interface (in the local Intel® AMT system), execute the following command:

- `AMTVTL.exe -user<username> -pass <password> -tls -cert <certificate> -host <IPAddress>`

Here:

<username> : Username used to access the Intel® AMT machine.
<password> : Password used to access the Intel® AMT machine.
-tls : To be used in TLS work mode
<certificate>: User certificate for mutual authentication (must be in TLS mode). This value should be the client certificate common name (CN).
<IPAddress> : Although a local tool, it requires the actual IP of the AMT to be entered.

- If Kerberos* is used username & password must not be given as input.
- Here, since we are configuring in non-TLS mode, [TLS] and [<certificate>] options are not required.
- On successful execution of the command, the following is displayed:
'AMT Features local ended successfully'.
- On failure, an output message (error message) is printed.



NOTE:

- For more details on this tool, please refer to the document - 'Intel® AMT Tools User Guide.pdf', located in the folder:
"Unzipped_folder"\Tools\iAMT Tools\

(Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\iAMT Tools\Intel® AMT Tools User Guide.pdf)

10.2 MEInfo tool

The MEInfo Tool provides simple aliveness test of the Intel® ME firmware, returns data about Intel® ME and also compares the value of a feature given as input with the Intel® ME actual features value.

10.2.1 MEInfo DOS tool

10.2.2 MEInfo DOS tool from VIP

The MEInfo DOS tool can be accessed from under the following directory:

"Unzipped_folder"\Tools\System Tools\MEInfo\DOS\

(Example: E:\iAMT_ASF2_XXX_4.0.0.xxxx\Tools\System Tools\MEInfo\DOS\MEInfo.exe)



10.2.3 Executing MEInfo

Execute the following command on the DOS prompt:

- MEInfo.exe [feat <feature name> <value>]

Here:

feat : To be used if only one feature is requested.

<feature name> : The feature name.

<value> : The feature value.

The following are examples of executing MEInfo.

1) Execute MEInfo without any optional parameters:

- Example: MEInfo
- Following is a sample of what MEInfo will display after executing the above command successfully:

Intel® MEInfo Version: 4.0.0.1035

BIOS Version: CAMPG0XX.86P

Intel® AMT code versions:

Flash:	4.0.0
Netstack:	4.0.0
AMTApps:	4.0.0
AMT:	4.0.0
SKU:	IAMT
Vendor ID:	8086
Build Number:	1035
Legacy mode:	False
Link status:	Link up
Hardware SKU:	AMT
Cryptography fuse:	Enabled
Flash Protection:	Enabled



Last reset reason:	Firmware Reset
Setup and Configuration:	Completed
AMT mode:	4.0
Bios Mode:	Post Boot
Mac Address:	00-11-22-33-44-55

- On error, an error message is printed and a non-zero error level is returned.

2) Execute MEInfo with the optional parameters specified – Here a definite feature should be requested

- a) Example: MEInfo feat "MAC Address" 00-11-22-33-44-55
- The output displayed is: Success. The values are identical.
- b) Example: MEInfo feat "Mac Address" 00-aa-22-33-44-55

- The output displayed is:
Failed. The values are not identical.
Mac Address: 00-11-22-33-44-55

NOTE:

- The MEInfo DOS tool is supported on the following operating systems: MS-DOS 6.22, Windows 98 DOS, Free DOS, DRMK DOS.
- For more details on this tool, please refer to the document - 'Intel® AMT Tools User Guide.pdf', located in the folder: "Unzipped_folder"\Tools\System Tools\

(Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\iAMT Tools\Intel® AMT Tools User Guide.pdf)

10.2.4 MEInfo Windows tool

The MEInfo Windows tool requires that the following be installed on the Intel® AMT system:

Intel® AMT Local Manageability Service (LMS) and Intel ME Interface driver



10.2.5 MEInfo Windows tool from VIP

The MEInfo Windows tool can be accessed from under the following directory:

"Unzipped_folder"\Tools\System Tools\MEInfo\Windows\

(Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\System Tools\MEInfo\Windows\MEInfoWin.exe)

10.2.6 Executing MEInfoWin

Execute the below on the Windows command line:

- MEInfoWin.exe [feat <feature name> <value>]

Here:

feat : To be used if only one feature is requested.
<feature name> : The feature name.
<value> : The feature value.

The following are examples of executing MEInfo.

1) Execute MEInfo without any optional parameters:

- Example: MEInfo
- Following is a sample of what MEInfo will display after executing the above command successfully:

Intel® MEInfo Win Version: 4.0.0.1023

BIOS Version: CAMPGOXX.86P

Intel® AMT code versions:

Flash:	4.0.0
Netstack:	4.0.0
AMTApps:	4.0.0
AMT:	4.0.0
Sku:	0



Vendor ID:	8086
Build Number:	1023
Recover Version:	4.0.0
Recovery Build Num:	1023
Legacy mode:	False
Link status:	Link up
Hardware SKU:	AMT
Cryptography fuse:	Enabled
Flash Protection:	Enabled
Last reset reason:	Firmware Reset
Setup and Configuration:	Completed
AMT mode:	4.0
Bios Mode:	Post Boot
Mac Address:	00-11-22-33-44-55
LMS version:	4.0.0.1034
HECI version:	4.0.0.1034

- On error, an error message is printed and a non-zero error level is returned.
-

NOTE:

- The MEInfo Windows tool is a command line executable and is supported on the following operating systems: Windows 2000 SP4, Windows XP SP 1/2.
- This tool should be run on Windows OS using Administrator privileges.
- Before running this tool Intel ME Interface driver must be installed.
- For more details on this tool, please refer to the document - 'Intel® AMT Tools User Guide.pdf', located in the folder:
"Unzipped_folder"\Tools\System Tools\

(Example: E:\iAMT_ASF2_XXX_4.0.0.xxxx\Tools\System Tools\Intel® AMT Tools User Guide.pdf)

10.3 AMTVTR tool

NOTE: For Alpha1 release this tool requires .NET framework installed on the machine where is being run.

The AMTVTR tool is a command line tool used to check the functionality of a remote Intel® AMT system (target platform/CRB). It tests the remote SOAP API to the Intel® AMT device. And it also tests various components in the Intel® AMT device (like, storage, hardware assets, System Defense, event manager, agent presence, remote control, etc). It is a command line executable and should be executed on the management console (any other system on the network).



10.3.1 AMTVTR tool from VIP

The AMTVTR tool can be accessed from under the following directory:

"Unzipped_folder"\Tools\iAMT Tools\iAMTVTR\

(Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\iAMT Tools\iAMTVTR\AMTVTR.exe)

10.3.2 Executing AMTVTR

On the command line interface (in the management console), execute the following command:

- `AMTVTR.exe -host <hostname> -pass <password> -tls -cert <certificate> -feat <opt>`

Here,

<hostname> : Host name/IP address of the Intel® AMT device.

(Note: In TLS mode hostname must be used.)

<username> : Username used to access the Intel® AMT machine

<password> : Password used to access the Intel® AMT machine.

-tls : To be used in TLS work mode

<certificate>: User certificate for mutual authentication (must be in TLS mode). This value should be the client certificate common name (CN).

<opt> : can be one of the following:

all : all features

sto : storage and storage admin features

hwinv : hardware asset

rc : remote control

sd : System Defense (circuit breaker)



em : event manager
na : network admin
sa : security admin
ap : agent presence
[<boot>] : to use in case rc or all were chosen, in order to boot the Intel®
AMT machine.

- If Kerberos* is used username & password must not be given as input.
- Here, since we are configuring in non-TLS mode, [TLS] and [<certificate>] options are not required.

(Example: AMTVTR.exe –host 192.168.0.15 –user username –pass password -feat na)

- The above example is checking for 'na' or network admin, i.e., get TCP/IP parameters.
- On successful execution of the above command, below is a sample of what will be displayed:

Current TCP/IP parameters:

DhcpMode = 1 (Disabled)
LocalAddress = 192.168.0.15
SubnetMask = 255.255.255.0
DefaultGatewayAddress = 0.0.0.0
PrimaryDnsAddress = 0.0.0.0
SecondaryDnsAddress = 0.0.0.0
DomainName = amt.intel.com

NOTE:

- The AMTVTR tool is supported on the following operating systems: Windows 2000 SP4, Windows XP SP 1/2, Windows Server 2003.
- On error, an error message is printed and a non-zero value is returned.
- On a successful run, the tests run are enumerated.



- For more details on this tool, please refer to the document - 'Intel® AMT Tools User Guide.pdf', located in the folder:

"Unzipped_folder"\Tools\iAMT Tools\

(Example: E:\iAMT_ASF2_XXX_4.0.0.xxxx\Tools\iAMT Tools\Intel® AMT Tools User Guide.pdf)

10.4 System Defense Test

NOTE: For alpha release this tool requires .NET framework to be installed

The system defense option on AMTVTR tool tests the remote System Defense feature of Intel® AMT. The System Defense feature is designed to help protect the system and the network from viruses, worms and other malicious code.

10.4.1 Executing System Defense test with AMTVTR

On the command line interface (in the management console), execute the following command:

- `AMTVTR -host <IPAddress> -user <username> -pass <password> -tls -cert <certificate> -feat sd`

Where:

hostname : Host name/IP address of the AMT server

(Note: In TLS mode hostname must be used.)

username : Username used to access the Intel® AMT device.

password : Password used to access the Intel® AMT device.

TLS : To be used in TLS work mode

certificate : User certificate for mutual authentication

Note: Must be in TLS mode for <certificate>. This value should be the client certificate common name (CN).

- If Kerberos* is used username & password must not be given as input.
- Here, since we are configuring in non-TLS mode, [TLS] and [<certificate>] options are not required.



- Follow the steps in the below example for testing System Defense functionality:

- a) Open a command prompt window (first) on the management console. At the command prompt, execute the following command:

```
AMTVTR -host 192.168.0.15 -user <username> -pass  
<password> -feat sd
```

where "username" and "password" are actually the username and password you previously configured.

- b) The following message will be displayed:

'press any key to activate the system defense...'

- c) Press Enter.

- d) The following message will be displayed:

'System Defense is active.'

Press any key to deactivate the system defense...'

- e) Open a second command prompt window on the management console, and ping the host machine, not the Intel® AMT machine.

(Example: ping 192.168.0.10)

Where, 192.168.0.10 is the static IP address of the host machine.

- f) The ping will return the following output: 'Request timed out'.

- g) On the first command prompt window on the management console, press Enter.

- h) The following message will be displayed:

'System Defense was deactivated.'

- i) In the second command prompt window, ping the host machine.

(Ex: ping 192.168.0.10)

- j) The ping will be successful and will return the number of bytes transferred.

**NOTE:**

- In case the test stopped in the middle and the System Defense remains active then the cleanup option should be used in order to deactivate System Defense.
- For more details on this tool, please refer to the document – ‘Intel® AMT Tools User Guide.pdf’, located in the folder:

“Unzipped_folder”\Tools\iAMT Tools\

(Example: E:\iAMT_ASF2_iTPM_4.0.0.xxxx\Tools\iAMT Tools\Intel® AMT Tools User Guide.pdf)

10.5 Testing SOL and IDE-R features

- Follow the steps in the below example for testing SOL and IDE-R functionality:
 - Open a command prompt window (first) on the management console. At the command prompt, execute the following command:

```
AMTVTR.exe -host <IP address of ME> -username <login> -pass <password> -tls -cert <certificate> -redirect
```

This command will give you the options to select to run SOL and IDE-R:

The following message will be displayed:

- a: Open SOL Session
- b: Close SOL Session
- c: Open IDER Session
- d: Close IDER Session
- e: Regular boot
- f: SOL boot
- g: SOL boot to BIOS setup
- h: IDER Floppy boot
- i: IDER CD boot
- j: SOL + IDER Floppy boot
- k: SOL + IDER CD boot.
- m: enable Redirection listener
- n: disable Redirection listener
- l: Display Menu Option
- x: Exit



SOL

- Press m to enable listener
- Press a to open a SOL session
- Open Telnet terminal window with serial port at COM3 in host S0
- Type commands in Telnet terminal screen and you should see them on the Management Console.

IDE-R

- Press m to enable listener
- Use c, h for IDER floppy boot
- Use c, l for IDER CD boot
- Open device manager on host in S0 and "REFRESH" the device manager, you will see a "Intel virtual floppy or CDROM"
- Go to my computer and you can access the CDROM or floppy connected to the Management Console.



10.6 Final checklist

This section provides a summarized checklist of the principal steps required to bring up an Intel® AMT firmware release on the CRB platform, arranged in the sequence that they should be performed. Please use this checklist to ensure no steps were missed as you went through the detailed procedures outlined herein above.

	Build FW Image using FitC (Flash image tool)
	Set optimal defaults in system BIOS
	Shut down and disable ME by closing the Manufacturing Mode jumper or removing all memory modules from Bank 0
	Program the image onto the SPI Flash using the fpt tool
	Verify the image (fpt /v)
	Shut down, do a clear CMOS using jumper J5H2
	Restart the system to boot BIOS from the Flash
	Enter BIOS setup and enable iTPM and AMT (through Chipset menu -> ME subsystem)
	Do a full G3 reset (disconnect power cable for 10 seconds)
	Restart the system and use CTRL-P to enter MEBx
	Set desired ME and AMT settings
	Restart the system and begin AMT & iTPM testing
	Install OS

§



11 *Appendix A – Board rework to enable Integrated TPM 1.2*

The rework for the Intel Integrated TPM 1.2 is required to activate the TPM. This will require the addition of resistors and a Jumper to easily activate and deactivate the TPM functionality.

This rework will activate the Integrated TPM enable straps on both the MCH and ICH, and will set the Physical Presence pin on the ICH.

The motherboard must be removed from the chassis to do the rework. There are three areas on the board that need to be changed. This appendix includes the rework for the Pillar Rock CRB (DDR2) and the Silver Cascade CRB (DDR3)

Pillar Rock CRB Rework

Step A: Populate a 2.2k ohm resistor to R1T7 on the bottom of the board.

Step B: add 1k ohm to R7U10 (bottom of the board). A 1x2 jumper can be connected to this topology to easily enable and disable the integrated TPM. When the Integrated TPM is disabled, TPM commands to be sent down to the LPC header on the platform.

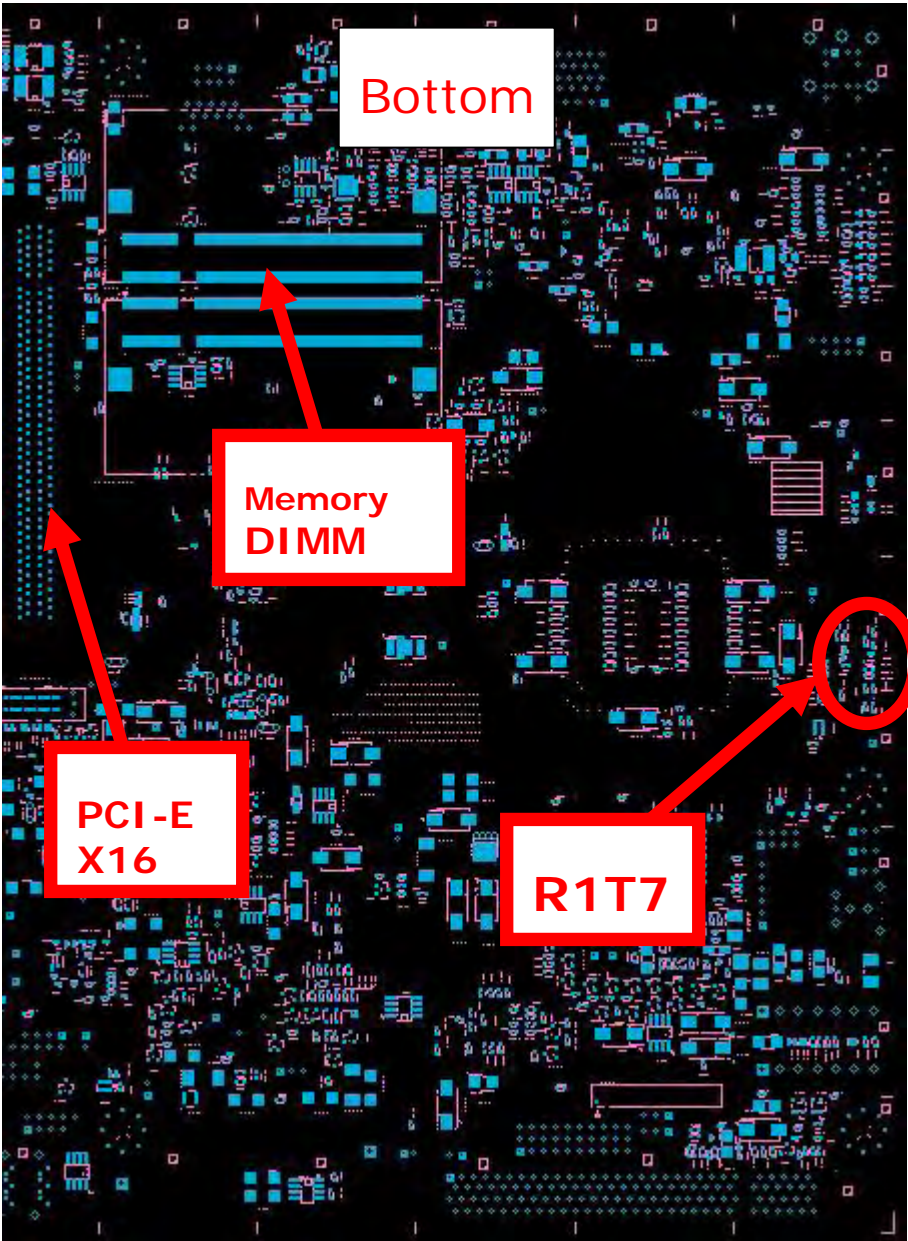
Step C: Connect the 2pin Jumper on J7H2

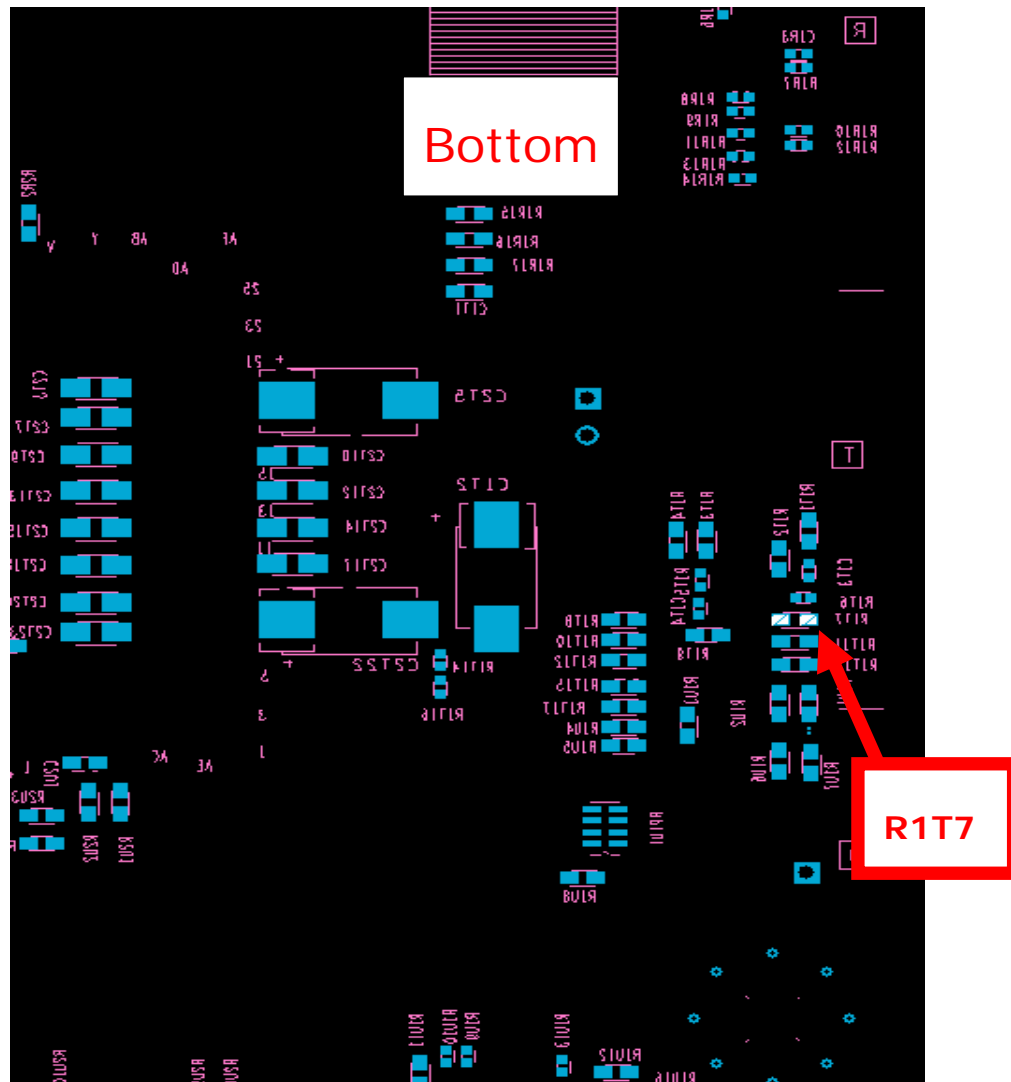
NOTE: The pictures shown are looking from the top down into the board, they are a mirror image of what is seen when physically looking at the board.

STEP A

R1T7 is located on the bottom of the board, the first picture shows the general location of the part, where the second picture shows the exact location. This is to enable Integrated TPM 1.2 the on the Cantiga MCH.

The following pictures in Step A are a mirror image of the physical board



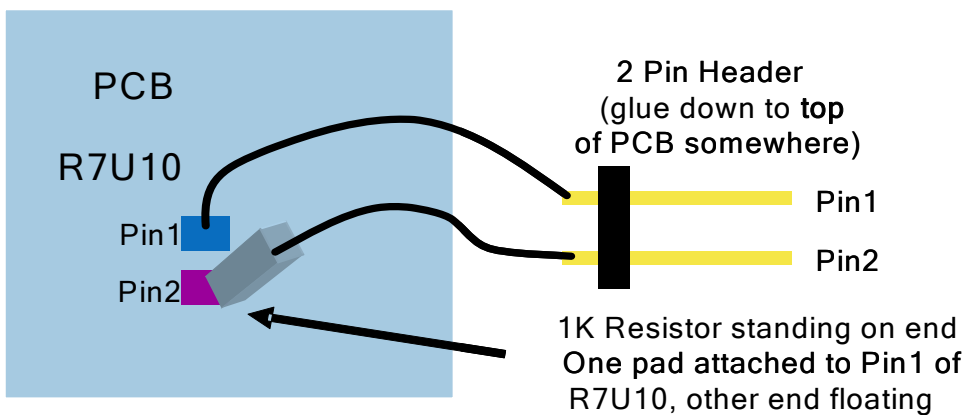




STEP B

R7U10 is located near the ICH9M device on the bottom of the board. Place a 1K ohm resistor at this location. This is to enable Integrated TPM 1.2 the on the ICH9M

Optional rework: Add 2 pin jumper to top of the board. For easy enable/disable.

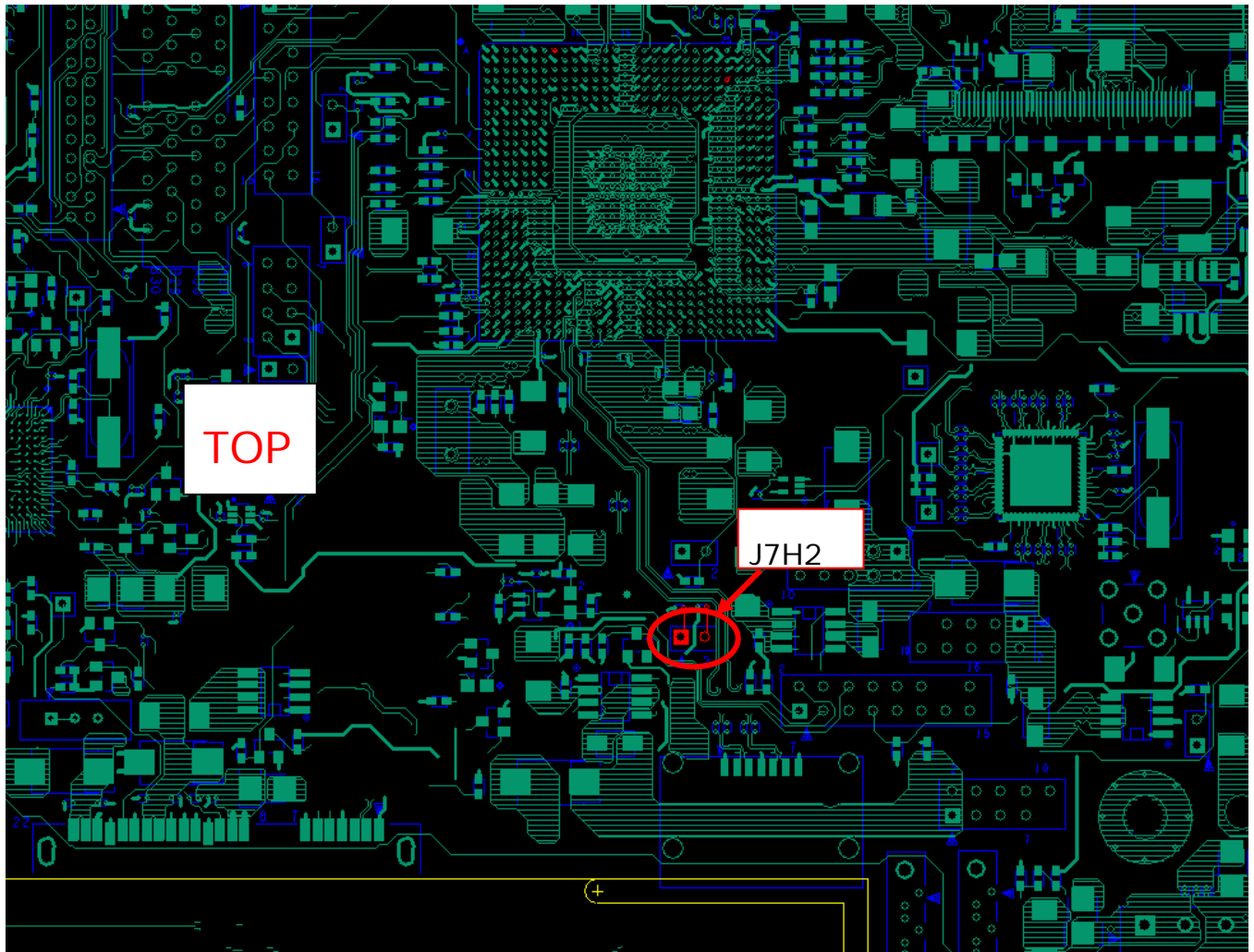




STEP C

Connect the 2pin Jumper on J7H2 on the top side of the motherboard. This is to assert the Integrated TPM Physical Presence on the platform.

The picture below is as shown at the top of the board, and is not a mirror image





Silver Cascade CRB Rework

Step A: Populate a 2.2k ohm resistor to R1T8 on the bottom of the board.

Step B: add 1k ohm to R7U9 (bottom of the board). A 1x2 jumper can be connected to this topology to easily enable and disable the integrated TPM. When the Integrated TPM is disabled, TPM commands to be sent down to the LPC header on the platform.

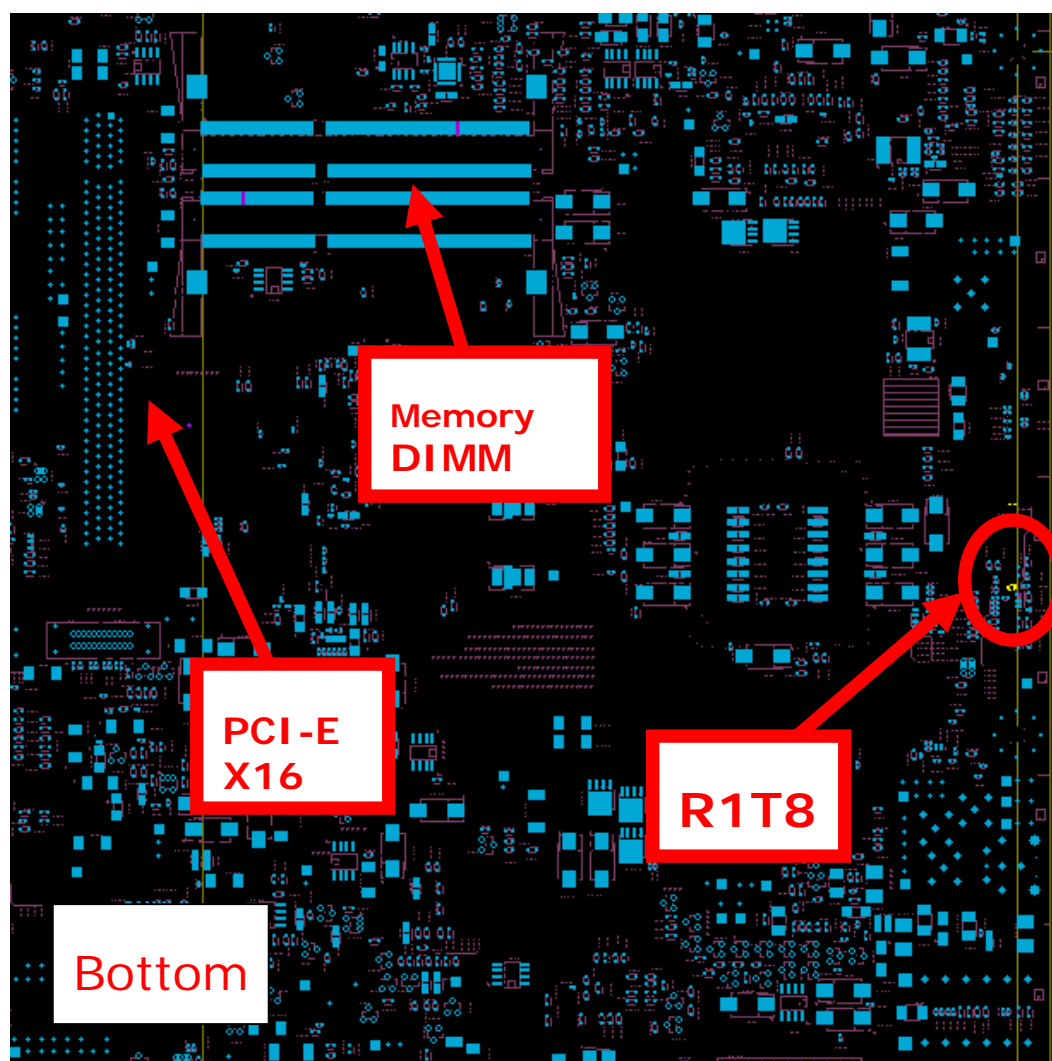
Step C: Connect the 2pin Jumper on J7H2

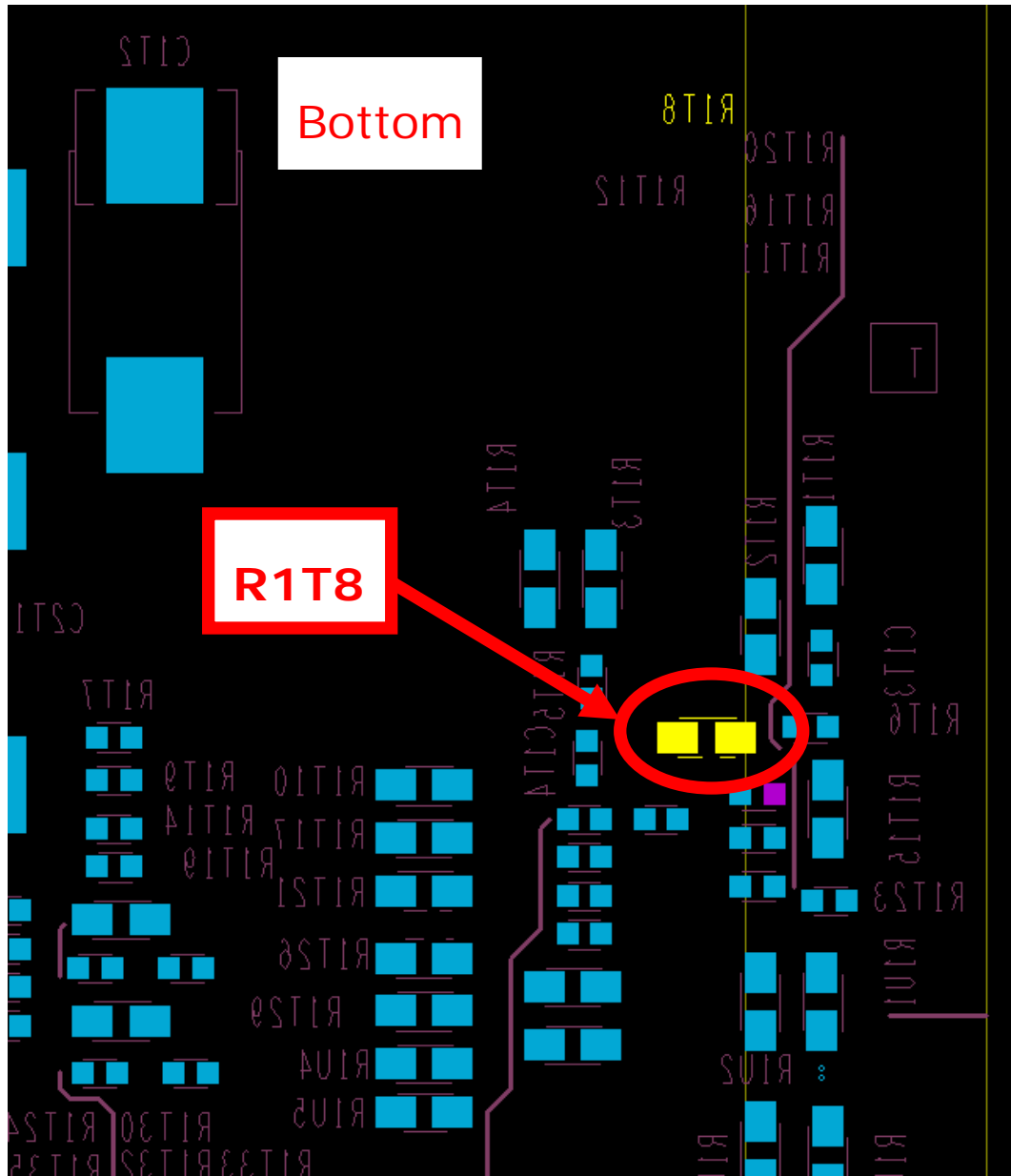
NOTE: The pictures shown are looking from the top down into the board, they are a mirror image of what is seen when physically looking at the board.

STEP A

R1T8 is located on the bottom of the board, the first picture shows the general location of the part, where the second picture shows the exact location. This is to enable Integrated TPM 1.2 the on the Cantiga MCH.

The following pictures in Step A are a mirror image of the physical board

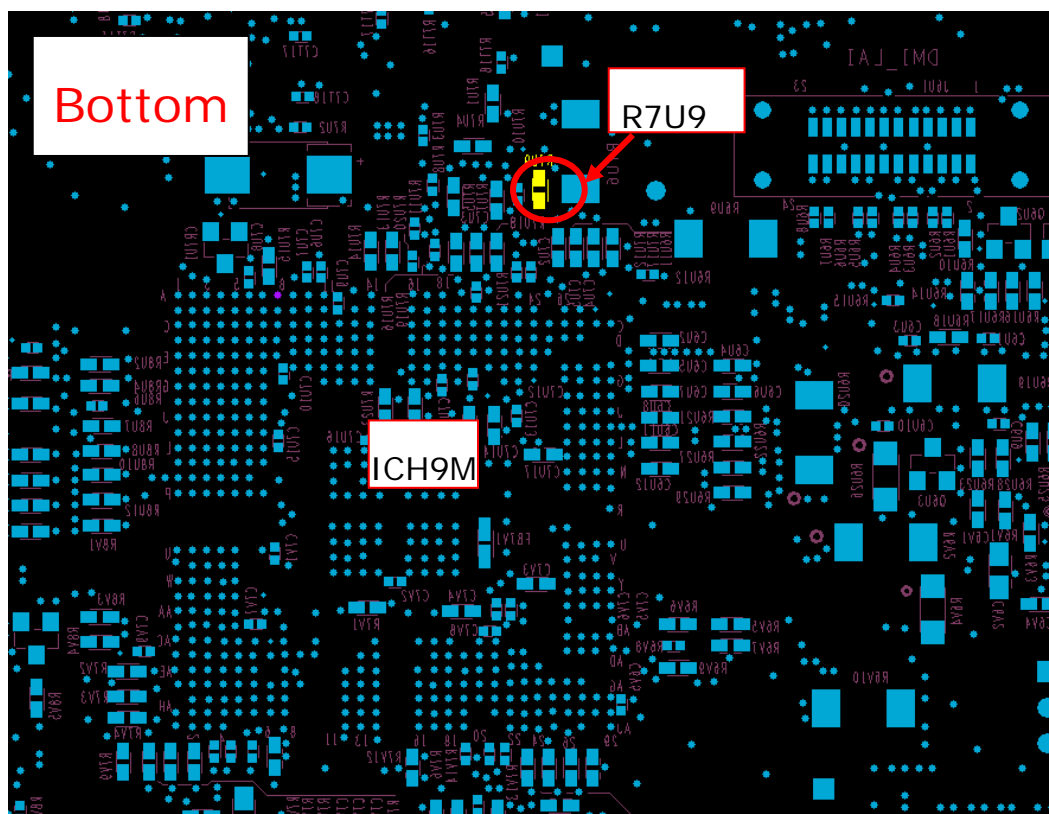
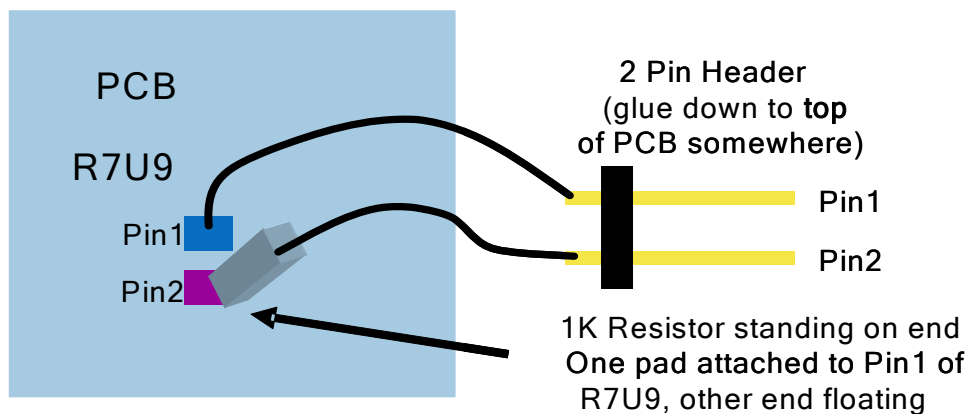




**STEP B**

R7U9 is located near the ICH9M device on the bottom of the board. Place a 1K ohm resistor at this location. This is to enable Integrated TPM 1.2 the on the ICH9M

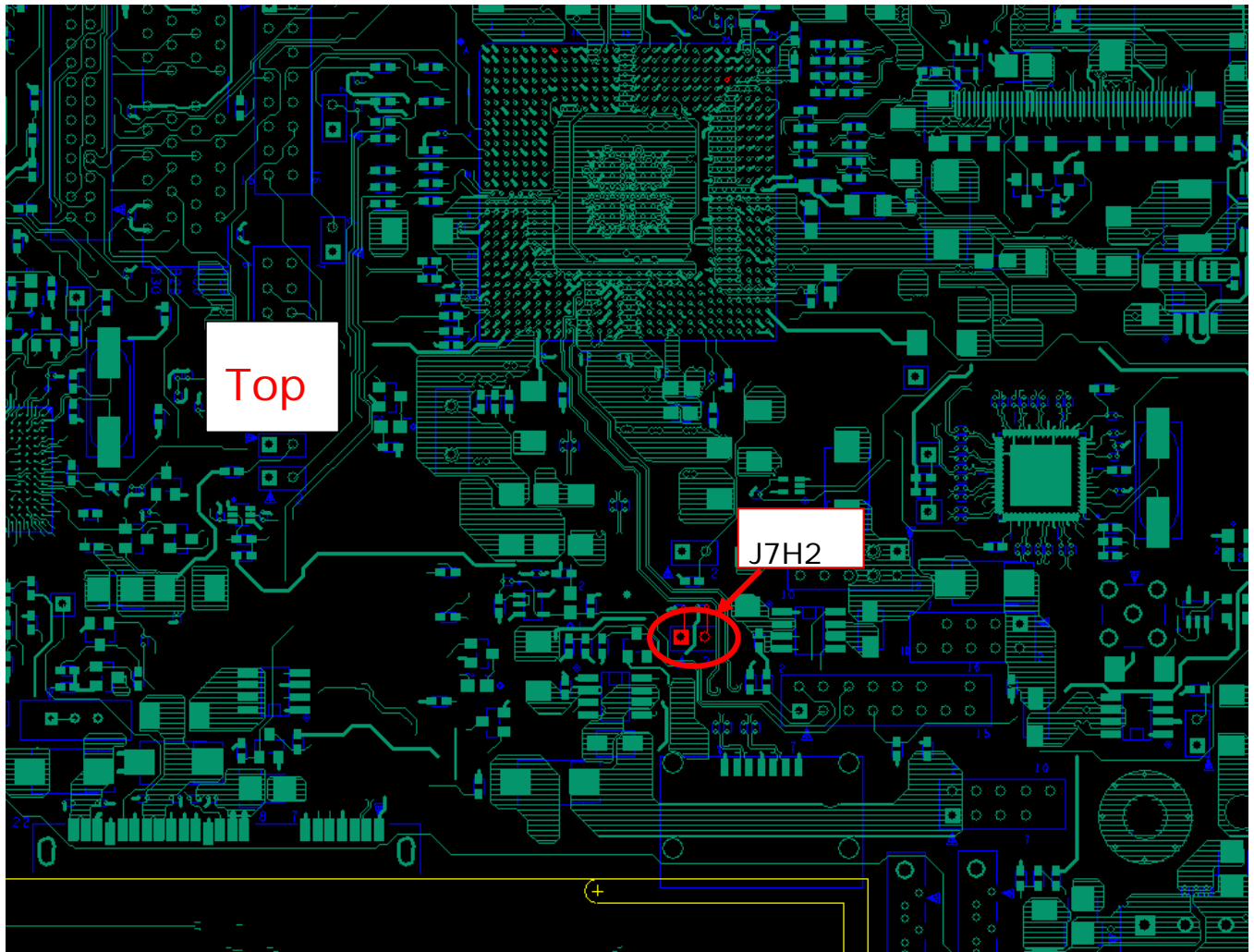
Optional rework: Add 2 pin jumper to top of the board. For easy enable/disable.





STEP C

Connect the 2pin Jumper on J7H2 on the top side of the motherboard. This is to assert the Integrated TPM Physical Presence on the platform.



§