Intel® HM57, and HM55 Express Chipsets — Intel® ME 4MB Firmware

Bring Up Guide

November 2009

Revision 6.0.3.1195

Intel Confidential

Locate Firmware Kit Contents and Tools

Assemble Firmware Image

Platform Bring Up

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.

I2C is a two-wire communications bus/protocol developed by Philips. SMBus is a subset of the I2C bus/protocol and was developed by Intel. Implementations of the I2C bus/protocol may require licenses from various entities, including Philips Electronics N.V. and North American Philips Corporation.

Intel® High Definition Audio requires a system with an appropriate Intel chipset and a motherboard with an appropriate codec and the necessary drivers installed. System sound quality will vary depending on actual implementation, controller, codec, drivers and speakers. For more information about Intel® HD audio, refer to http://www.intel.com/

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see http://www.intel.com/technology/security

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group and specific software for some uses. For more information, see http://www.intel.com/technology/security

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. See www.intel.com/products/processor_number for details.

Intel® Active Management Technology requires the computer system to have an Intel(R) 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 www.intel.com/technology/platform-technology/intel-amt/

Warning: Altering clock frequency and/or voltage may (i) reduce system stability and useful life of the system and processor; (ii) cause the processor and other system components to fail; (iii) cause reductions in system performance; (iv) cause additional heat or other damage; and (v) affect system data integrity. Intel has not tested, and does not warranty, the operation of the processor beyond its specifications.

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, Intel vPro, Intel Core, 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 © 2008-2009, Intel Corporation. All rights reserved.

Table of Contents

1 Introduction 7
1.1 Intel® ME FW Features 7
1.2 Prerequisites 9
1.2.1 System Power States 9
1.3 Reference Documentation 10
1.4 Format and Notation 11
1.5 ME FW Kit Contents 11
1.6 External Hardware Requirements for Bring Up 14

2 Image Creation: Config Wizard (FICW) 17
2.1 Flash Image Configuration Wizard (FICW) Requirements 17
2.1.1 OS Support 17
2.2 Installation Instructions 17
2.3 Use Configuration Wizard to Build SPI Flash Binary Image 19

3 Image Creation: Flash Image Tool (FITC) 33
3.1 Quick Start for Intel CRBs 33
3.2 Start FITC and Load the Default Settings XML File 34
3.3 Set Up The Build Environment 34
3.4 Configure PCH Silicon Stepping 36
3.5 Set Up Descriptor and SPI Flash Device(s) 36
3.5.1 Set Up Soft-Straps (Ibex Peak B-stepping Only) 41
3.6 Set Up SPI Flash Regions 46
3.7 Configure PCH Silicon SKU 49
3.8 ME FW Feature Configuration 49
3.8.1 Clock Control Parameters 49
3.9 Build SPI Flash Binary Image 54
3.9.1 Build SPI Flash Binary Image 54
3.9.2 Save Your Settings 55

4 Burn the SPI Flash Binary Image 57
4.1 Flash Burner/Programmer 57
4.2 Flash Programming Tool (DOS Version) 57
4.2.1 Flash Programming Tool (Windows* Version) 58

5 Intel® ME Firmware Feature Bring Up 59
5.1 Manufacturing Mode (GPIO33) 59
5.2 Intel Wired LAN Settings and Driver 61
5.3 Thermal Reporting 61

6 System Tools 67
6.1 Overview 67
6.2 Image Editing Tools 67
6.3 Manufacturing Line Tool 67
6.4 ME Setting Checking Tool 67
6.5 Operating System Support 68

Intel Confidential

6.6 Flash Image Tool (FITC) 68
6.6.1 System Requirements 69
6.7 Flash Image Configuration Wizard (FICW) 69
6.8 Flash Programming Tool (FPT) 69
6.8.1 System Requirements 69
6.8.2 Flash Image Details 69
6.8.3 Windows* Required Files 70
6.8.4 DOS Required Files 70
6.8.5 Usage 71
6.8.6 Fparts.txt File 75
6.9 MEmanuf and MEmanufwin 76
6.9.1 Usage 76
6.10 MEinfo 78
6.10.1 Usage 78

A Appendix — Ibex Peak Clock Configuration 79
A.1 Functional Blocks 80
A.2 ME FW Clock Control Parameters 81
A.2.1 FCSS – Flex Clock Source Select 81
A.2.2 PLLEN* – PLL Enable 82
A.2.3 OCKEN – Output Clock Enable 83
A.2.4 OBEN – Output Buffer Enable 85
A.2.5 IBEN – Input Buffer Enable 85
A.2.6 DIVEN* – Divider Enable 86
A.2.7 PM1 – Power Management 87
A.2.8 PM2 – Power Management 87
A.2.9 SEBP1 – Single Ended Buffer Parameters 88
A.2.10 SEBP2 – Single Ended Buffer Parameters 89
A.2.11 SSCCTL* – SSC Control 91
A.2.12 PMSRCCLK1 – SRC Power Management 91
A.2.13 PMSRCCLK2 – SRC Power Management 94

B Appendix — Flash Configurations 971Introduction11
1.1 Prerequisites 11
1.2 ME FW Kit Contents 11
1.3 External Hardware Requirements for Bring Up 15

2 Image Creation: Config Wizard (FICW) 17
2.1 Flash Image Configuration Wizard (FICW) Requirements 17
2.1.1 OS Support 17
2.2 Installation Instructions 17
2.3 Use Configuration Wizard to Build SPI Flash Binary Image 19

3 Image Creation: Flash Image Tool (FITC) 37
3.1 Start FITC and Load the Default Settings XML File 37
3.2 Set Up The Build Environment 37
3.3 Configure PCH Silicon Stepping 39
3.4 Set Up Descriptor and SPI Flash Device(s) 39
3.4.1 Set Up Soft-Straps (Ibex Peak B-stepping Only) 44

3.5 Set Up SPI Flash Regions 49
3.6 Configure PCH Silicon SKU 52
3.7 ME FW Feature Configuration 52
3.7.1 Clock Control Parameters 52
3.7.2 Firmware Features and Capabilities 57
3.8 Build SPI Flash Binary Image 61
3.8.1 Build SPI Flash Binary Image 61
3.8.2 Save Your Settings 62
3.8.3 Protect Saved Configuration Files 62

4 Burn the SPI Flash Binary Image 65
4.1 Flash Burner/Programmer 65
4.2 Flash Programming Tool (DOS Version) 65
4.2.1 Flash Programming Tool (Windows* Version) 66

5 Intel® ME Firmware Feature Bring Up 67
5.1 Manufacturing Mode (GPIO33) 67
5.2 Intel Wired LAN Settings and Driver 69
5.3 Thermal Reporting 69

A Appendix — Ibex Peak Clock Configuration 75
A.1 Functional Blocks 76
A.2 ME FW Clock Control Parameters 77
A.2.1 FCSS – Flex Clock Source Select 77
A.2.2 PLLEN* – PLL Enable 78
A.2.3 OCKEN – Output Clock Enable 79
A.2.4 OBEN – Output Buffer Enable 81
A.2.5 IBEN – Input Buffer Enable 81
A.2.6 DIVEN* – Divider Enable 82
A.2.7 PM1 – Power Management 83
A.2.8 PM2 – Power Management 83
A.2.9 SEBP1 – Single Ended Buffer Parameters 84
A.2.10 SEBP2 – Single Ended Buffer Parameters 85
A.2.11 SSCCTL* – SSC Control 87
A.2.12 PMSRCCLK1 – SRC Power Management 87
A.2.13 PMSRCCLK2 – SRC Power Management 90

B Appendix — Flash Configurations 93

Figures

1-1 Clock Initialization Process (Simplified) 8
1-2 Thermal Reporting 9
3-1 Saving PDF Attachments 33
3-2 Build | Build Image 34
3-3 Build | Environment Variables... 35
3-4 Build | Build Settings... 35
3-5 PCH Silicon Stepping Combo Box 36
3-6 SKU Manager Combo Box 49
3-7 Build | Build Image 55
5-1 Desktop CRB Manufacturing Mode Jumper Location 60

5-2 Mobile CRB Manufacturing Mode Jumper Location 60
5-3 Flash Descriptor Security Override (GPIO33) Rework for Redfort 60
5-4 MPG BIOS: Enable TR (Step 1 of 3) 62
5-5 MPG BIOS: Enable TR (Step 2 of 3) 63
5-6 MPG BIOS: Enable TR (Step 3 of 3) 64
5-7 CCG BIOS: Enable TR (Step 1 of 2) 65
5-8 CCG BIOS: Enable TR (Step 2 of 2) 66
A-1 Ibex Peak Buffer Through Mode Architecture 79
A-2 Ibex Peak Display Clock Integration Architecture 80
B-1 Configuration "A" — Desktop/Server/Workstation or Mobile 97
B-2 Configuration "B" — Mobile only 98
B-3 Configuration "C" — Desktop/Server/Workstation only 98
B-4 Configuration "D" — Mobile only .....993-1Build | Environment Variables...38
3-2 Build | Build Settings... 38
3-3 PCH Silicon Stepping Combo Box 39
3-4 SKU Manager Combo Box 52
3-5 Build | Build Image 61
3-6 Protecting FITC Configuration XML and ConfigParams TXT Files 63
5-1 Desktop CRB Manufacturing Mode Jumper Location 68
5-2 Mobile CRB Manufacturing Mode Jumper Location 68
5-3 Flash Descriptor Security Override (GPIO33) Rework for Redfort 68
5-4 MPG BIOS: Enable TR (Step 1 of 3) 70
5-5 MPG BIOS: Enable TR (Step 2 of 3) 71
5-6 MPG BIOS: Enable TR (Step 3 of 3) 72
5-7 CCG BIOS: Enable TR (Step 1 of 2) 73
5-8 CCG BIOS: Enable TR (Step 2 of 2) 74
A-1 Ibex Peak Buffer Through Mode Architecture 75
A-2 Ibex Peak Display Clock Integration Architecture 76
B-1 Configuration "A" — Desktop or Mobile 93
B-2 Configuration "B" — Mobile only 94
B-3 Configuration "C" — Desktop only 94
B-4 Configuration "D" — Mobile only 95

Tables

1-1 System States and Power Management (Sheet 1 of 5) 10
1-2 Reference Documentation 10
1-3 Number Format Notation 11
1-4 Data Format Notation 11
1-5 ME FW Kit Contents 11
1-6 ME FW Kit Tools 13
2-1 FICW In FITC Directory 17
2-2 Configuration Wizard: Choose Configuration File 19
2-3 Configuration Wizard: Choose Configuration File 20
2-4 Configuration Wizard: Image Source Files (1 of 2) 21
2-5 Configuration Wizard: Image Source Files (2 of 2) 22
2-6 Configuration Wizard: Intel Integrated Wired LAN Configuration 23

2-7 Configuration Wizard: DMI/PCIe* configuration 24
2-8 Configuration Wizard: Thermal Reporting Configuration 25
2-9 Configuration Wizard: Boot Configuration options..... 26
2-10 Configuration Wizard: Production/nonproduction configuration..... 27
2-11 Configuration Wizard: Integrated Clocking Configuration..... 28
2-12 Configuration Wizard: OEM Request Record — Single-Ended Clocks (1 of 2) 29
2-13 Configuration Wizard: OEM Request Record — Single-Ended Clocks (2 of 2) 30
2-14 Configuration Wizard: OEM Request Record — Differential Clocks..... 31
2-15 Configuration Wizard: Save and Build..... 32
3-1 Flash Image | Descriptor Region 36
3-2 Flash Image | Descriptor Region | Descriptor Map 36
3-3 Flash Image | Descriptor Region | Component Section..... 37
3-4 Flash Image | Descriptor Region | Master Access Section | CPU/BIOS 38
3-5 Flash Image | Descriptor Region | Master Access Section | Manageability Engine (ME) 38
3-6 Flash Image | Descriptor Region | Master Access Section | GbE LAN 39
3-7 Flash Image |Descriptor Region | ME VSCC Table | Add Table Entry 39
3-8 Flash Image | Descriptor Region | ME VSCC Table | AT26DF321..... 40
3-9 Flash Image | Descriptor Region | OEM Section 40
3-10 Flash Image | Descriptor Region | PCH Straps | PCH Strap 0 41
3-11 Flash Image | Descriptor Region | PCH Straps | PCH Strap 2 42
3-12 Flash Image | Descriptor Region | PCH Straps | PCH Strap 4 42
3-13 Flash Image | Descriptor Region | PCH Straps | PCH Strap 7 43
3-14 Flash Image | Descriptor Region | PCH Straps | PCH Strap 9 43
3-15 Flash Image | Descriptor Region | PCH Straps | PCH Strap 10 44
3-16 Flash Image | Descriptor Region | PCH Straps | PCH Strap 11 45
3-17 Flash Image | Descriptor Region | PCH Straps | PCH Strap 14 45
3-18 Flash Image | Descriptor Region | PCH Straps | PCH Strap 15 46
3-19 Flash Image | PDR Region 46
3-20 Flash Image | GbE Region..... 47
3-21 Flash Image | ME Region 48
3-22 Flash Image | BIOS Region 48
3-23 Flash Image | Configuration | ICC Data 50
3-24 Flash Image | Configuration | ICC Data | OEM Request Record 0 | Static Registers Section 51
3-25 Flash Image | Configuration | ICC Data | OEM Request Record 0 | Dynamic Registers Section 52
3-26 High Impact Clock Control Parameters..... 53
5-1 Thermal Reporting Options in MPG BIOS 64
6-1 Operating System Support..... 68
6-2 Flash Programming Tool Windows Contents..... 70
6-3 Flash Programming Tool DOS Contents..... 71
A-1 SSC Blocks 80
A-2 Clock Dividers 80
A-3 Flex Clock Source Select Parameters 81
A-4 PLL Enable Parameters 82
A-5 Output Clock Enable Parameters..... 84
A-6 Input Buffer Enable Parameters 86

A-7 Divider Enable Parameters 86
A-8 Power Management Parameters 87
A-9 Power Management Parameters 88
A-10 Single Ended Buffer Parameters 88
A-11 Single Ended Buffer Parameters 90
A-12 SSC Control Parameters 91
A-13 SRC Power Management 92
A-14 SRC Power Management .....951-1ME FW Kit Contents11
1-2 ME FW Kit Tools 13
2-1 FICW In FITC Directory 17
2-2 Configuration Wizard: Choose Configuration File 19
2-3 Configuration Wizard: Choose Configuration File 20
2-4 Configuration Wizard: Image Source Files (1 of 2) 21
2-5 Configuration Wizard: Image Source Files (2 of 2) 22
2-6 Configuration Wizard: Intel ME VSCC Table Configuration 23
2-7 Configuration Wizard: Intel ME Configuration Parameters Screen 24
2-8 Configuration Wizard: Intel Integrated Wired LAN Configuration 25
2-9 Configuration Wizard: DMI/PCIe* configuration 26
2-10 Configuration Wizard: Thermal Reporting Configuration 27
2-11 Configuration Wizard: Boot Configuration options 28
2-12 Configuration Wizard: Production/nonproduction configuration 29
2-13 Configuration Wizard: Integrated Clocking Configuration 30
2-14 Configuration Wizard: OEM Request Record — Single-Ended Clocks (1 of 2) 31
2-15 Configuration Wizard: OEM Request Record — Single-Ended Clocks (2 of 2) 32
2-16 Configuration Wizard: OEM Request Record — Differential Clocks 33
2-17 Configuration Wizard: Braidwood Configuration 34
2-18 Configuration Wizard: Save and Build 35
3-1 Flash Image | Descriptor Region 39
3-2 Flash Image | Descriptor Region | Descriptor Map 39
3-3 Flash Image | Descriptor Region | Component Section 40
3-4 Flash Image | Descriptor Region | Master Access Section | CPU/BIOS 41
3-5 Flash Image | Descriptor Region | Master Access Section | Manageability Engine (ME) 41
3-6 Flash Image | Descriptor Region | Master Access Section | GbE LAN 42
3-7 Flash Image |Descriptor Region | ME VSCC Table | Add Table Entry 42
3-8 Flash Image | Descriptor Region | ME VSCC Table | AT26DF321 43
3-9 Flash Image | Descriptor Region | OEM Section 43
3-10 Flash Image | Descriptor Region | PCH Straps | PCH Strap 0 44
3-11 Flash Image | Descriptor Region | PCH Straps | PCH Strap 2 45
3-12 Flash Image | Descriptor Region | PCH Straps | PCH Strap 4 45
3-13 Flash Image | Descriptor Region | PCH Straps | PCH Strap 7 46
3-14 Flash Image | Descriptor Region | PCH Straps | PCH Strap 9 46
3-15 Flash Image | Descriptor Region | PCH Straps | PCH Strap 10 47
3-16 Flash Image | Descriptor Region | PCH Straps | PCH Strap 11 48
3-17 Flash Image | Descriptor Region | PCH Straps | PCH Strap 14 48
3-18 Flash Image | Descriptor Region | PCH Straps | PCH Strap 15 49
3-19 Flash Image | PDR Region 49
3-20 Flash Image | GbE Region 50

3-21 Flash Image | ME Region 51
3-22 Flash Image | BIOS Region 51
3-23 Flash Image | Configuration | ICC Data 53
3-24 Flash Image | Configuration | ICC Data | OEM Request Record 0 | Static Registers Section 54
3-25 Flash Image | Configuration | ICC Data | OEM Request Record 0 | Dynamic Registers Section 55
3-26 High Impact Clock Control Parameters 56
3-27 Flash Image | Configuration | ME 58
3-28 Flash Image | Configuration | Power Packages 59
3-29 Flash Image | Configuration | Features Supported 59
3-30 Flash Image | Configuration | Features Supported (HM57) 60
3-31 Flash Image | Configuration | Features Supported (HM55) 61
5-1 Thermal Reporting Options in MPG BIOS 72
A-1 SSC Blocks 76
A-2 Clock Dividers 76
A-3 Flex Clock Source Select Parameters 77
A-4 PLL Enable Parameters 78
A-5 Output Clock Enable Parameters 80
A-6 Input Buffer Enable Parameters 82
A-7 Divider Enable Parameters 82
A-8 Power Management Parameters 83
A-9 Power Management Parameters 84
A-10 Single Ended Buffer Parameters 84
A-11 Single Ended Buffer Parameters 86
A-12 SSC Control Parameters 87
A-13 SRC Power Management 88
A-14 SRC Power Management 91

§

1 Introduction

This document covers the ME FW bring up procedure. Intel® Management Engine is tied to essential platform functionality — this dependency cannot be avoided for engineering reasons.

The bring up procedure primarily involves building an SPI flash image that will contain:

- **[required]** Descriptor region — Contains sizing information for all other SPI flash image regions, SPI settings (including Vendor Specific Configuration - or VSCC - tables, SPI device parameters), and region access permissions.
- **[required]** BIOS region — Contains firmware for the processor (or host) and/or Embedded Controller (EC)
- **[required]** ME FW region — Contains firmware for the Intel® Management Engine.
- **[optional]** GbE region — Contains firmware for Intel LAN solution

See *SPI Flash Programming Guide* and Appendix B (page 93) for more details on SPI Flash layout. Once the SPI flash image is built, it will be programmed to the target Ibex Peak based platform, and the platform will be booted. This document also covers any tests and checks required to ensure that this boot process is successful, and that ME FW is operating as expected.

1.1 Prerequisites

Before this document is read and utilized, it is essential that the reader first review the Release Notes (included with this ME FW kit).

This document is constructed so that the reader can run through the bring up steps as given for the Intel CRB. However, in the case that bring up is being performed on a different Ibex Peak based platform, this document will highlight any changes that must be imposed onto the bring up steps accordingly.

This document makes only the following assumptions for hardware:

- The platform is Ibex Peak based.
- The platform is equipped with one or more SPI flash devices with a total capacity large enough to contain the generated SPI flash image.

1.2 ME FW Kit Contents

The ME FW kit can be downloaded from VIP (http://platformsw.intel.com/). The contents of this kit are provided in this section. The contents are organized within the example framework shown below

Table 1-1. ME FW Kit Contents

File or [Directory]	Content Description
[root]	Root directory.
FW Bring Up Guide.pdf	This document.
Release Notes.pdf	List of open, ongoing, and closed sightings for this Intel® ME FW kit release.

Intel Confidential

Table 1-1. ME FW Kit Contents

File or [Directory]	Content Description
SPI Programming Guide.pdf	How to program SPI device parameters, VSCC tables, descriptor region details. This document's contents are integrated with *FW Bring Up Guide*. Also contains a complete SPI Flash soft-strap reference.
[NVM Image]	
[BIOS]	
CGIBX1xx.ROM	CG BIOS firmware binary. **Can only be used with the Intel Desktop CRB.** For other Ibex Peak based platforms, a custom BIOS firmware binary will be required.
MPGxxx.ROM	MPG BIOS firmware binary. Can only be used with the Intel Mobile CRB. For other Ibex Peak based platforms, a custom BIOS firmware binary will be required.
EPIBX146.ROM	For the Palomar Server CRB the required BIOS image is **EPIBX146.ROM** from the Palomar_BIOS_0146 release. This BIOS image should be retrieved based on the respective BIOS release e-mail announcement and stored in the **NVM Image\BIOS** subdirectory (along with the other BIOS images available in the kit) before starting the SPI flash image creation process.
[Firmware]	
PCH_4M_PreProduction.BIN	ME firmware binary. To be used on an Ibex Peak based platform.
PCH_4M_PreProduction_UPD.BIN	ME firmware update binary. To be used with FWUpdLcl.exe for data-safe ME FW update.
[root]	Root directory.
[NVM Image]	
[GbE]	
[82577 (Mobile)]	
[LAN Switch]	Intel LAN PHY firmware binary. Use with mobile Ibex Peak based platforms that support docking and uses a LAN switch.
[82577LC (Consumer)]	
82577LC_A3_IBEXPEAK_B1B2_LAN_SWITCH_VER0PTA4.bin	
82577LC_A3_IBEXPEAK_B1B2_LAN_SWITCH_VER0PTA4.txt	
[82577LM (Corporate)]	
82577LM_A3_IBEXPEAK_B1B2_LAN_SWITCH_VER0PTA1.bin	
82577LM_A3_IBEXPEAK_B1B2_LAN_SWITCH_VER0PTA1.txt	
[Non LAN Switch]	Intel LAN PHY firmware binary. Use with mobile Ibex Peak based platforms that support docking and does not use a LAN switch. If IEEE conformance does not meet requirements, then _LAN_SWITCH_ version may need to be used.
[82577LC (Consumer)]	
82577LC_A3_IBEXPEAK_B1B2_NON_LAN_SWITCH_VER0PTA6.bin	
82577LC_A3_IBEXPEAK_B1B2_NON_LAN_SWITCH_VER0PTA6.txt	
[82577LM (Corporate)]	

Table 1-1. ME FW Kit Contents

File or [Directory]	Content Description
82577LM_A3_IBEXPEAK_B1B2_NON_LAN_SWITCH_VER0PTA3.bin	
82577LM_A3_IBEXPEAK_B1B2_NON_LAN_SWITCH_VER0PTA3.txt	
[82578 (Desktop)]	Intel LAN device firmware binary. Use with desktop, server, or workstation Ibex Peak based platforms.
[82578DC (Consumer)]	
82578DC_C0_IBEXPEAK_B1B2_VER0PTA5.bin	
82578DC_C0_IBEXPEAK_B1B2_VER0PTA5.txt	
[82578DM (Corporate)]	
82578DM_C0_IBEXPEAK_B1B2_VER0PTA2.bin	
82578DM_C0_IBEXPEAK_B1B2_VER0PTA2.txt	

Table 1-2. ME FW Kit Tools

File or [Directory]	Content Description
[root]	Root directory.
[Tools]	
[System Tools]	
Tools_Version.txt	This file provides the tool versions for manufacturing tools contained in the kits
[Flash Image Tool]	Flash Image Tool (FIT) will be used to assemble the SPI flash image binary. This tool will program the binary image with all settings, including clock control parameters.
fitc.exe	Flash Image Tool executable.
fitc.ini	Initialization file that stores working and decomposition directory locations.
fitctmpl.xml	
newfiletmpl.xml	Default FIT configuration XML file.
vsccommn.bin	
ConfigWizard.exe	Flash Image Configuration Wizard executable.
[ConfigWizard]	Sub directory used for FICW help and default configuration
Wizard.help	Text file contains FICW help text
WizardDefault.conf	Sets default settings in FICW . Do not edit this.
[Flash Programming Tool]	Flash Programming Tool (FPT) will program the SPI flash binary image into the SPI flash device.
License.rtf	FPT license.
[DOS]	Copy this entire directory for FPT for DOS to function properly.
fparts.txt	Database of supported SPI flash devices.
fpt.exe	Flash Programming Tool binary for DOS.
fptcfg.ini	
vsccommn.bin	
[Windows]	Copy this entire directory for FPT for Windows* to function properly.

Intel Confidential

Table 1-2. ME FW Kit Tools

File or [Directory]	Content Description
fparts.txt	Database of supported SPI flash devices.
fptcfg.ini	
fptw.exe	Flash Programming Tool binary for 32-bit Windows operating systems.
idrvdll.dll	Supporting library file.
pmxdll.dll	Supporting library file.
vsccommn.bin	
[MEInfo]	MEInfo can be used to check and debug the platform in the R&D lab and by system integrators.
[DOS]	Copy this entire directory for FPT for DOS to function properly.
MEInfo.exe	MEInfo binary for DOS.
[Windows]	Copy this entire directory for FPT for DOS to function properly.
MEInfoWin.exe	MEInfo binary for 32-bit Windows operating systems.
sseidrv.DLL	
ssepmx.DLL	
[MEManuf]	MEManuf can be used to check and debug the platform in the R&D lab and on the manufacturing line.
[DOS]	Copy this entire directory for MEManuf for DOS to function properly.
MEManuf.exe	MEManuf binary for DOS.
vsccommn.bin	
[Windows]	Copy this entire directory for MEInfo for DOS to function properly.
MEManufWin.exe	MEManuf binary for 32-bit Windows operating systems.
sseidrv.DLL	
ssepmx.DLL	
vsccommn.bin	
[QST Tools]	
QstCfg.exe	• Windows* command line tool • OS support – Windows XP, Windows 2000 and Windows* Preinstallation Environment (Windows PE) • Used for configuring and tuning the Intel® QST subsystems, taking an INI file as input
QstCfgATXIP.ini	
QstCfgD.exe	• DOS tool • Used for configuring and tuning the Intel® QST subsystems, taking an INI file as input
QstComm.dll	
QstComm.lib	
QstConfigurationWizard.msi	
QstCply.exe	• DOS tool • Used for running compliance tests on an Intel® QST-enabled platform
QSTCT_GUI.exe	

Table 1-2. ME FW Kit Tools

File or [Directory]	Content Description
QstCtrl.exe	
QstINI.exe	
QstINID.exe	
QstInst.dll	
QstInst.lib	
QstLog.exe	
QstStat.exe	
QstStatD.exe	
QstTuningWizard.msi	
[Include]	
QstCfg.h	
QstCmd.h	
QstComm.h	
QstInst.h	
typedef.h	
[Braidwood Tools]	
NANDUtil.exe	• DOS based command line tool • Provides support for following commands: • NAND configuration commands such as create, destroy and erase for NVMHCI (cache) and/or SSD regions • NAND quality check using test command • Compliance command to check platform, BIOS and NAND subsystem compliancy • Firmware status and NAND region query command

1.3 External Hardware Requirements for Bring Up

Acquire the following hardware tools beforing moving on to the next step.

Window OS System	Flash Burner	DOS Bootable USB Key
 Example Picture	 Example Picture	 Example Picture
Equipment: • A latop or desktop that supports win32 applications **Purpose:** • Will run image assembly and build process software on the equipment	**Equipment:** • A Flash Chip Burner/ Programmer **Purpose:** • Will be used to burn firmware image onto SPI Flash (equipment normally used for bringing up a system that has not booted previously)	**Equipment:** • A DOS Bootable USB Key (Size > 512 MB) **Purpose:** • Will be used to transfer image created onto a flash burner • Or acting as a bootable device and will be used to run Flash Programming Tool (fpt.exe) directly on the system that is undergoing Bring Up process

§

2 Image Creation: Config Wizard (FICW)

Flash Image Configuration Wizard (FICW) will be used to generate a full SPI flash binary image with Descriptor, GbE, BIOS, and Intel® ME Regions. Use the steps shown in following sections.

This chapter will also cover how this image can be burned onto the target platform's SPI Flash part(s).

2.1 Flash Image Configuration Wizard (FICW) Requirements

FICW will not load without the Microsoft* .NET 2.0 Framework. Download a copy of this software from this location:

http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en

2.1.1 OS Support

- Microsoft Windows XP* with Service Pack2
- Microsoft Windows Vista*

2.2 Installation Instructions

After insuring that Microsoft* .NET 2.0 Framework is installed, be sure to copy all the FICW distribution files into the Flash Image Tool directory.

The FICW executable must be in the same directory as fitc.exe and vsccomn.bin for proper operation.

Table 2-1. FICW In FITC Directory

File or [Directory]	Content Description
[root]	Root directory.
[Tools]	
[System Tools]	
[Flash Image Tool]	Flash Image Tool (FIT) will be used to assemble the SPI flash image binary.
fitc.exe	Flash Image Tool executable.
fitc.ini	Initialization file that stores working and decomposition directory locations.
fitctmpl.xml	
newfiletmpl.xml	Default FITC configuration XML file.
vsccommn.bin	
ConfigWizard.exe	Flash Image Configuration Wizard executable.

Intel Confidential

Table 2-1. FICW In FITC Directory

File or [Directory]		Content Description
	[ConfigWizard]	Sub directory used for FICW help and default configuration
	Wizard.help	Text file contains FICW help text
	WizardDefault.conf	Sets default settings in FICW . Do not edit this.

2.3 Use Configuration Wizard to Build SPI Flash Binary Image

Table 2-2. Configuration Wizard: Choose Configuration File

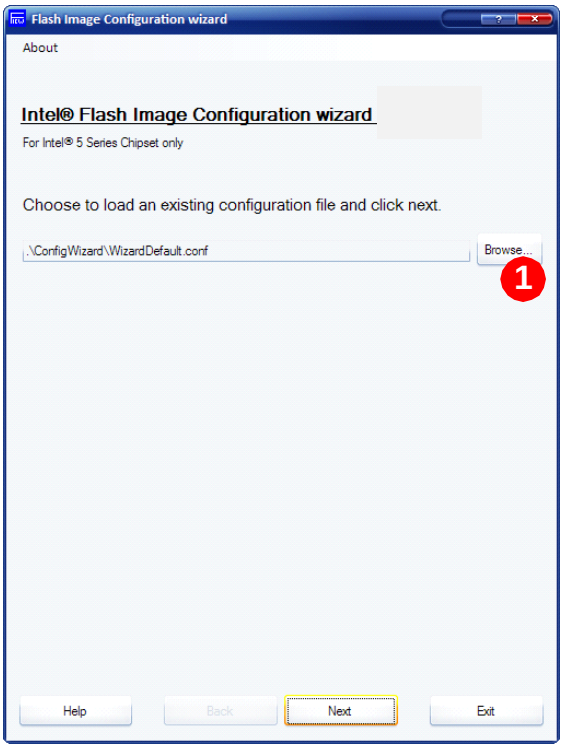
Screen	#	CRB Setting	Setting for All Platforms
	1	.\ConfigWizard\WizardDefault.conf	For first time start with **CRB Setting**. Load a custom **.conf** file if one is available.
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-3. Configuration Wizard: Choose Configuration File

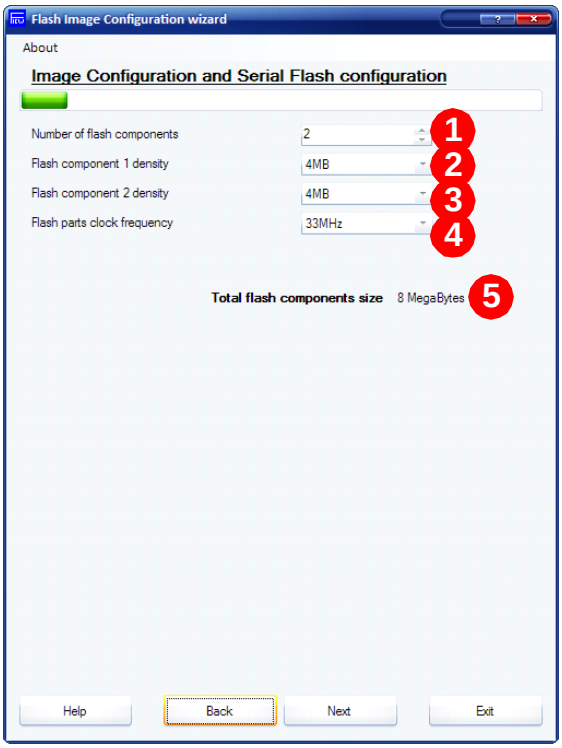
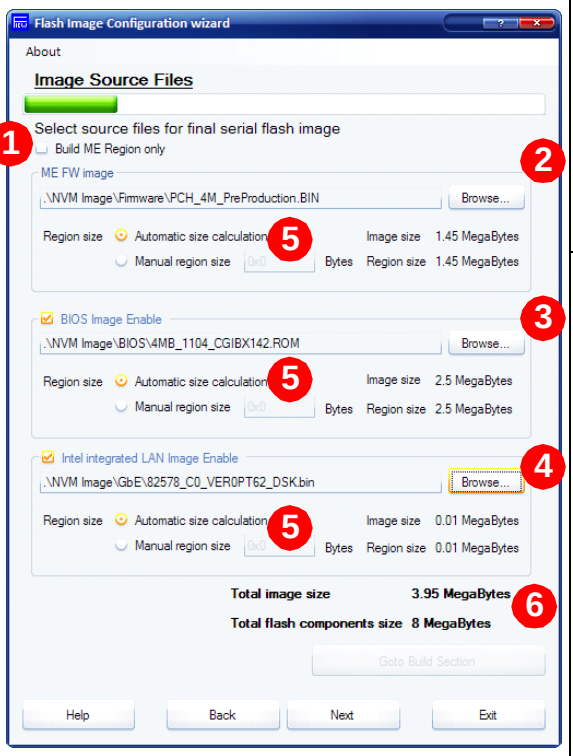
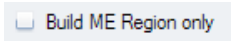
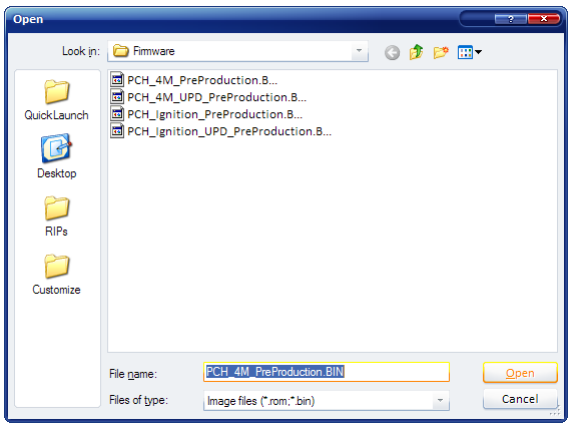
Screen	#	CRB Set To	Settings for Any Platform
	1	2	Number of SPI flash devices on the platform **1** or **2** = Total SPI flash devices Default is **2**
	2 3	**4MB** for both flash devices	Size of first and second SPI flash parts on the platform.
	4	33 MHz	Set to lowest common frequency of all SPI flash parts on the platform. **50MHz** support is only available in Ibex Peak B- or later stepping. Sets the following: • Read ID and Read Status clock frequency • Write and erase clock frequency • Fast read clock frequency
	5	Reports the total flash component size. Updated in realtime.	
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-4. Configuration Wizard: Image Source Files (1 of 2)

Screen	#	CRB Setting	Setting for All Platforms
	1		
		Unchecked	Building the ME Region separately can be useful if updating the ME region only in a pre-production or debug environment. • For all other scenarios leave this option unchecked.
	2	Click **Browse** and choose ME FW binary image: 	

#	CRB Setting	Setting for All Platforms
3	**BIOS Image Enable** checked + CCG or MPG BIOS	Check the **BIOS Image Enable** if BIOS is stored in the same SPI flash as ME FW and GbE FW. This will enable the **Browse** button to the right. Click **Browse** and choose BIOS binary image: If BIOS is stored in a separate SPI Flash device or in FWH (see Configurations "B", "C", and "D" in Appendix B (page 93) then uncheck **BIOS Image Enable**.
Do not click **Next** yet. Check the next table in this document.		

Table 2-5. Configuration Wizard: Image Source Files (2 of 2)

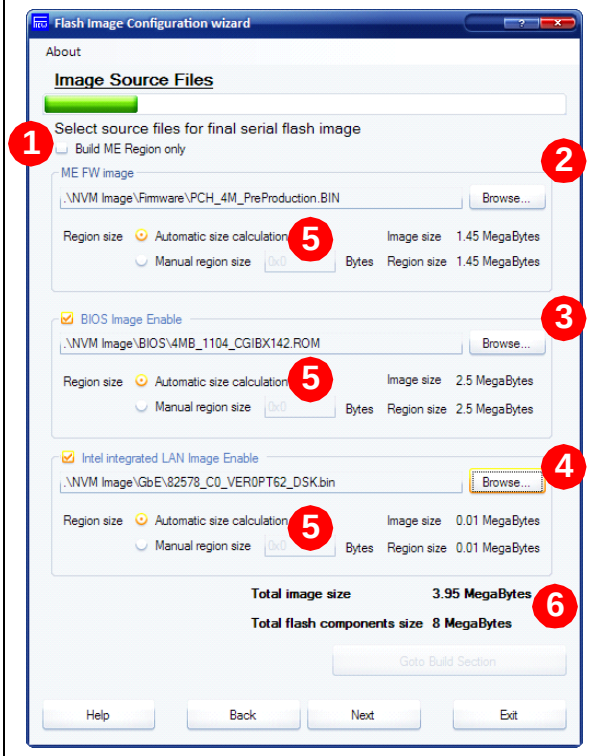
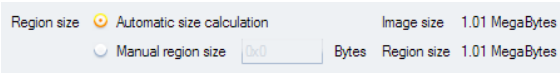
Screen	#	CRB Setting	Setting for All Platforms
	4	**Intel Intg LAN Image Enable** checked + Desktop/ Server CRB uses **xxxxx_DSK** image Mobile CRB uses **LAN_SWITCH** image	Check the **Intel Integrated LAN Enable** checkbox if using Intel LAN. This will enable the **Browse** button to the right. Click **Browse** and choose BIOS binary image: Choose the Intel GbE LAN FW image as follows: • Desktop platforms should use the xxxxx_DSK image • Mobile platforms that support docking and uses a LAN switch should use the _LAN_SWITCH_ image • Mobile platforms that support docking and does not use a LAN switch should use the _NON_LAN_SWITCH_ image. If IEEE conformance does not meet requirements, then _LAN_SWITCH_ version may need to be used. • See the documents in the **GbE** subdirectory for more information If not using Intel LAN then uncheck **Intel Integrated LAN Enable**.
5	**Automatic Size Calculation** for all SPI Flash Regions	 **Automatic Size Calculation** assumes that SPI Flash Regions can be sized as per default guidelines: • Place Descriptor at the lowest SPI Flash address • Place GbE FW at the next available SPI Flash address. The size of this region will be as large as the GbE FW binary itself, grown to the nearest 4 kByte (to adhere to SPI Flash sector size requirements). • Place ME FW at the next available SPI Flash address. The size of this region will be grown to contain all the remaining (blank) space in SPI Flash. • Place BIOS at the next available SPI Flash address. The size of this region will be as large as the BIOS binary itself, grown to the nearest 4 kByte. **Manual Region Size** will specify the SPI Flash Region size. Each **0x400** worth of hexadecimal bytes is equivalent to 1 kByte. The total region size is reported here, updated in realtime.	
6	Reports the total image size. Updated in realtime.		
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-6. Configuration Wizard: Intel ME VSCC Table Configuration

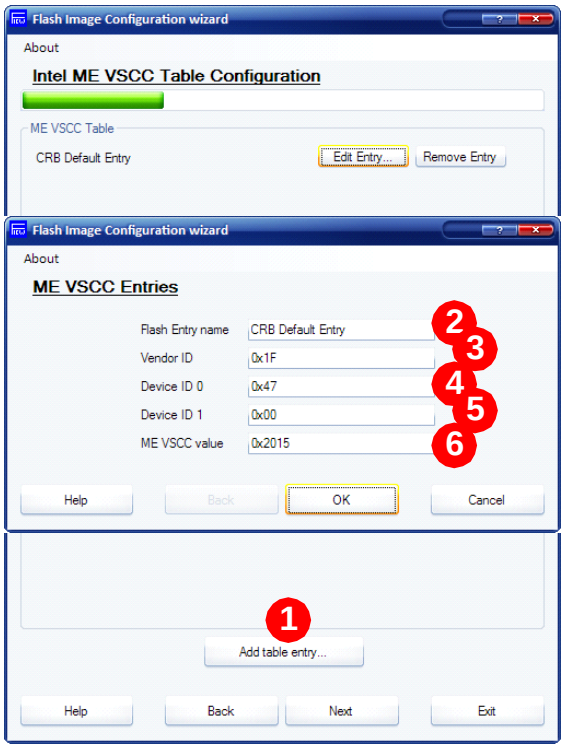
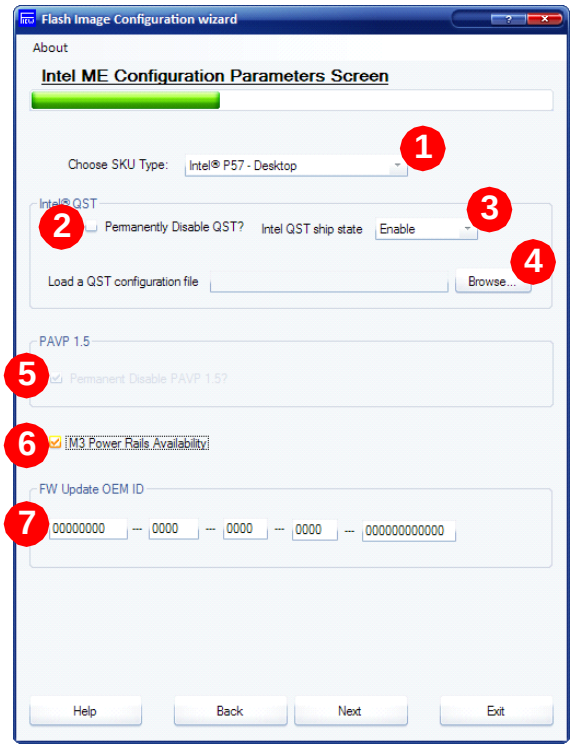
Screen	#	CRB Setting	Setting for All Platforms
	1	Add table entry... Click this button to add an SPI Flash device as a VSCC Entry for ME FW.	
	2	Desktop and Mobile CRBs use **AT26DF321**	Enter the part name of the SPI Flash device for which this VSCC Entry for ME FW is being created.
	3	Desktop and Mobile CRBs use **0x1F**	Enter Vendor ID. This information can be found in the specific SPI Flash device datasheet.
	4	Desktop and Mobile CRBs use **0x47**	Enter Device ID 0. This information can be found in the specific SPI Flash device datasheet.
	5	**0x00**	Enter Device ID 1 only if needed according to the SPI datasheet. This information can be found in the specific SPI Flash device datasheet.
	6	Desktop and Mobile CRBs use **0x2015**	Enter VSCC Table architecture. This information can be found in the specific SPI Flash device datasheet.
Add additional VSCC entries, or... Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-7. Configuration Wizard: Intel ME Configuration Parameters Screen

Screen	#	CRB Setting	Setting for All Platforms
	1	**Intel® P57** = Desktop **Intel® HM57**, **Intel® HM55**, = Mobile See Section 3.6 (page 52) for more information on SKU Manager.	
	2	**Unchecked** for desktop CRB **Unchecked (greyed out)** for mobile CRB	**Checked** = Intel® P57 platform's Intel® QST enable/disable will be determined by ship state setting **Unchecked** = Intel® P57 platform has Intel® QST permanently disabled **Unchecked (greyed out)** = Intel® HM57, Intel® HM55, have Intel® QST permanently disabled
	3	**Enable** for desktop CRB **Disable (greyed out)** for mobile CRB	**Enable** = Intel® QST is enabled **Disable** = Intel® QST is disabled ***Note:*** This setting can be later changed through available interfaces such as MEBx, USB key provisioning, manageability agents, remote management consoles, etc. ***Note:*** **Intel QST Ship State** option is only available when **Permanently Disable QST?** is **Unchecked** (and not greyed out).
	4	**Load a QST configuration file** is only used when Intel® QST is enabled and there is a pre-existing configuration file.	
	5	**Unchecked** for desktop CRB **Unchecked (greyed out)** for mobile CRB	**Checked** = Intel® HM55 or HM57 platform has PAVP 1.5 enabled **Unchecked** = Intel® HM55 or HM57 platform has PAVP 1.5 permanently disabled **Checked (greyed out)** = PAVP 1.5 permanently disabled

#	CRB Setting	Setting for All Platforms
6	**M3 Rail Present** checked	This parameter must reflect physical platform topology. **Checked =** Target platform power rail topology is such that the ME and SPI wells are powered from standby. MEPWROK and PCH_PWROK are two separate signals. This is true for platforms that are capable of supporting Out Of Band (OOB) functionality with Intel® ME 8MB Firmware and appropriate Power Package selected. A platform whose core and ME power rails are bifurcated, as described, but does not use OOB functionality, but still select **checked** for this parameter. **Unchecked** = Target platform power rail topology is such that the ME and SPI wells are powered from core (S0 only). MEPWROK and PCH_PWROK are shorted.
7	00000000-0000-0000-0000-000000000000	This field provides the ability to target FWUpdate (FWUpdLcl.exe) by Platform OEM. This ID will make sure that customers can only update a platform with an image coming from the platform OEM. The string entered aftIf set to an all zeros, then any input is valid when doing a firmware update.
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.		

Table 2-8. Configuration Wizard: Intel Integrated Wired LAN Configuration

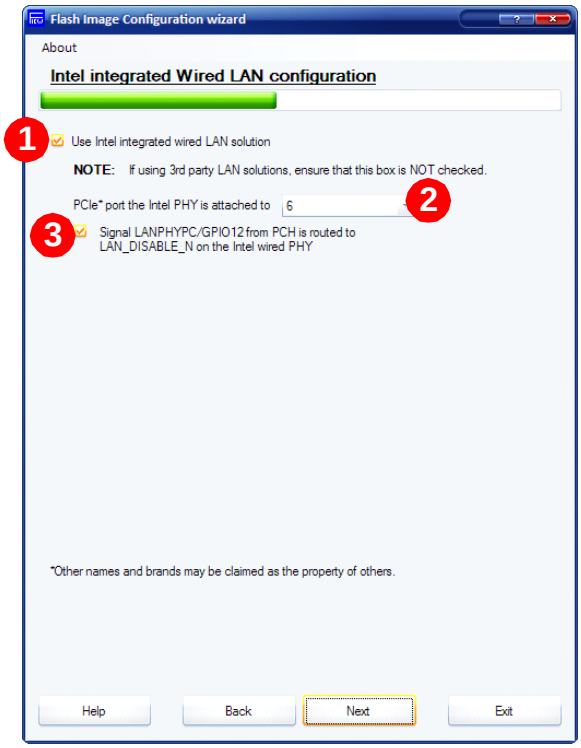
Screen	#	CRB Setting	Setting for All Platforms
	1 2	**Checked** and select **Port 6**	**Checked** = Intel LAN is present. Select PCH PCI Express* port utilized for GbE LAN PHY. **Unchecked** = Third-party LAN is present. The port selection parameter will be grayed out.
	3	Checked	**Checked** = Only required if target platform has Intel wired LAN and PCH GP12 is used as LAN_PHYPC for Intel LAN. **Unchecked** = PCH GP12 is used as General Purpose Input/Output (GPIO) pin. Must be **Unchecked** if Third-party LAN is present.
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-9. Configuration Wizard: DMI/PCIe* configuration

Screen	#	CRB Setting	Setting for All Platforms
	1	Unchecked	**DMI and FDI Lanes Reversed** option must reflect platform topology.
	2	**4x1** **PCIe* lane 1 reversed** unchecked	**PCIe* Lanes 1-4 configuration** panel must reflect platform topology. ***Note:*** **PCIe* lane 1 reversed** option is available only when **1x4 - one four lane PCIe* port** is selected.
	3	Desktop CRB uses **4x1** Mobile CRB uses **2x1, 2x1** **PCIe* lane 5 reversed** unchecked for Desktop and Mobile CRBs	**PCIe* Lanes 5-8 configuration** panel must reflect platform topology. ***Note:*** **PCIe* lane 5 reversed** option is available only when **1x4 - one four lane PCIe* port** is selected.
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-10. Configuration Wizard: Thermal Reporting Configuration

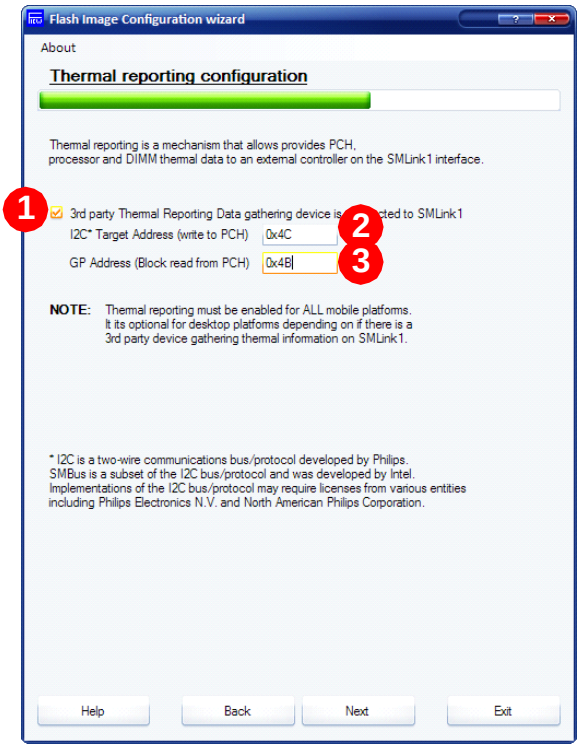
Screen	#	CRB Setting	Setting for All Platforms
	1	3rd party Thermal Reporting Data gathering device is connected to SMLink1	
		Unchecked for desktop CRB. **Checked** for mobile CRB	**Checked** = Set for all desktop platforms which are experiencing power flow issues or are having Intel® QST enabled. For mobile platforms, check this for EC/SIO/BMC to interact Thermal Reporting feature over SMLink1 **Unchecked** = Platform has no EC/SIO/BMC on SMLink1 Enables **I2C* Target Address** and **GP Address** fields. This field is **checked** by default for mobile platforms and cannot be unchecked.
	2	Mobile CRB uses **0x4C**	Denotes EC/SIO/BMC SMBus write address over SMLink1. This field cannot be blank or **0x0**, otherwise the **Next** button will be disabled.
	3	Mobile CRB uses **0x4B**	Denotes EC/SIO/BMC SMBus read address over SMLink1. This field cannot be blank or **0x0**, otherwise the **Next** button will be disabled.
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-11. Configuration Wizard: Boot Configuration options

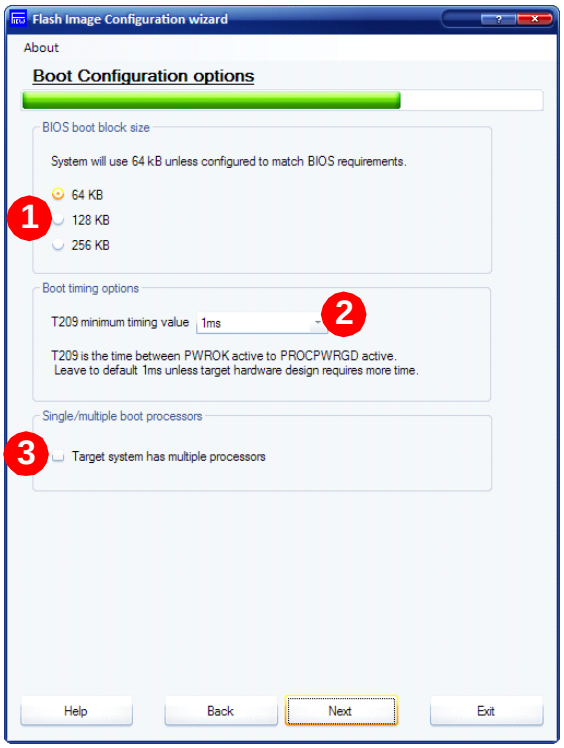
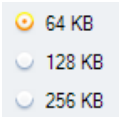
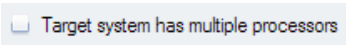
Screen	#	CRB Setting	Setting for All Platforms
	1	64 KB	 BIOS Boot Block is bare minimum BIOS code required to boot a platform. The soft-strap allows for proper address bit to be inverted as required by BIOS Boot Block Size. **64KB** = Invert A16 if Top Swap is enabled **128KB** = Invert A17 if Top Swap is enabled **256KB** = Invert A18 if Top Swap is enabled If BIOS is stored in a separate SPI Flash device or in FWH (see Configurations "B", "C", and "D" in Appendix B (page 93) then leave this parameter at **64KB**. ***Note:*** This field will be disabled when **BIOS Image Enable** is not checked
	2	1 ms	Minimum timing between PWROK assert and CPUPWRGD assert. Change to reflect optimal timing for your platform. Can also be set to **50ms**, **5ms**, and **100ms**.
	3		
		Unchecked	Indicates if RequesterID checking during DMI accesses is disabled. This parameter is only applicable for server platforms that contain multiple PCHs. **Unchecked** = single PCH on the same platform **Checked** = multiple PCHs in the same platform
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-12. Configuration Wizard: Production / nonproduction configuration

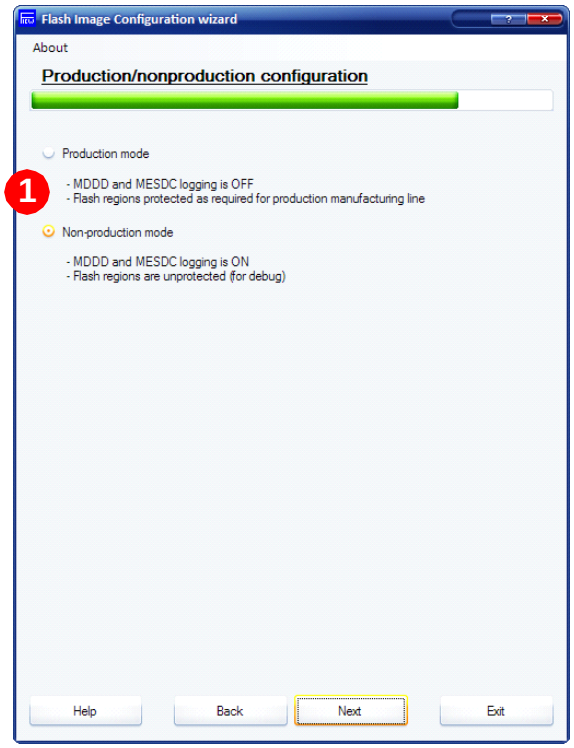
Screen	#	CRB Setting	Setting for All Platforms
	1	Non-production mode	Selecting **Production Mode** sets the following: • BIOS Region Master Access Permissions set to **0x0B** for read access and **0x0A** for write access • ME FW Region Master Access Permissions set to to **0x0D** for read access and **0x0C** for write access • GbE FW Region Master Access Permissions set to to **0x08** for both read and write access • ME SMBus Diagnostic Console capability is disabled • MDDD capability is disabled Selecting **Non-production Mode** sets the following: • Master Access Permissions for all SPI Flash Regions set to **0xFF** for both read and write access • ME SMBus Diagnostic Console capability is disabled • MDDD capability is disabled **Production Mode** is for a system as it would be shipped. **Non-production Mode** is for debug and simplifies flashing new images onto SPI Flash.
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-13. Configuration Wizard: Integrated Clocking Configuration

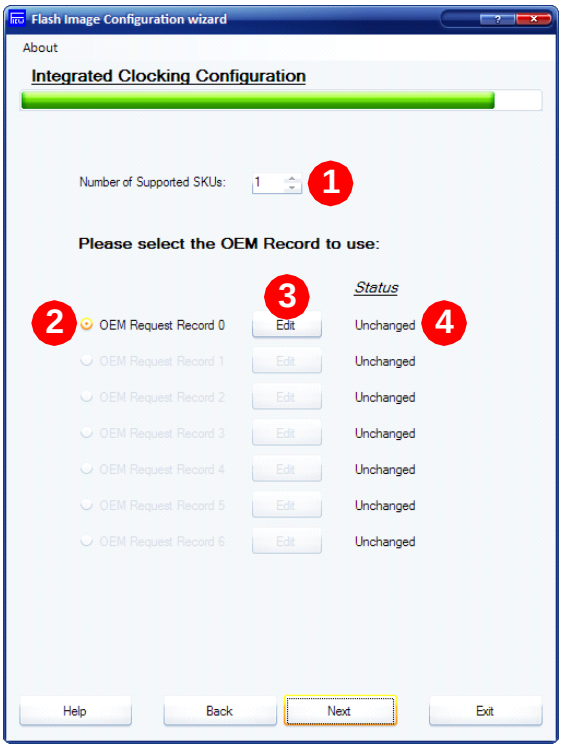
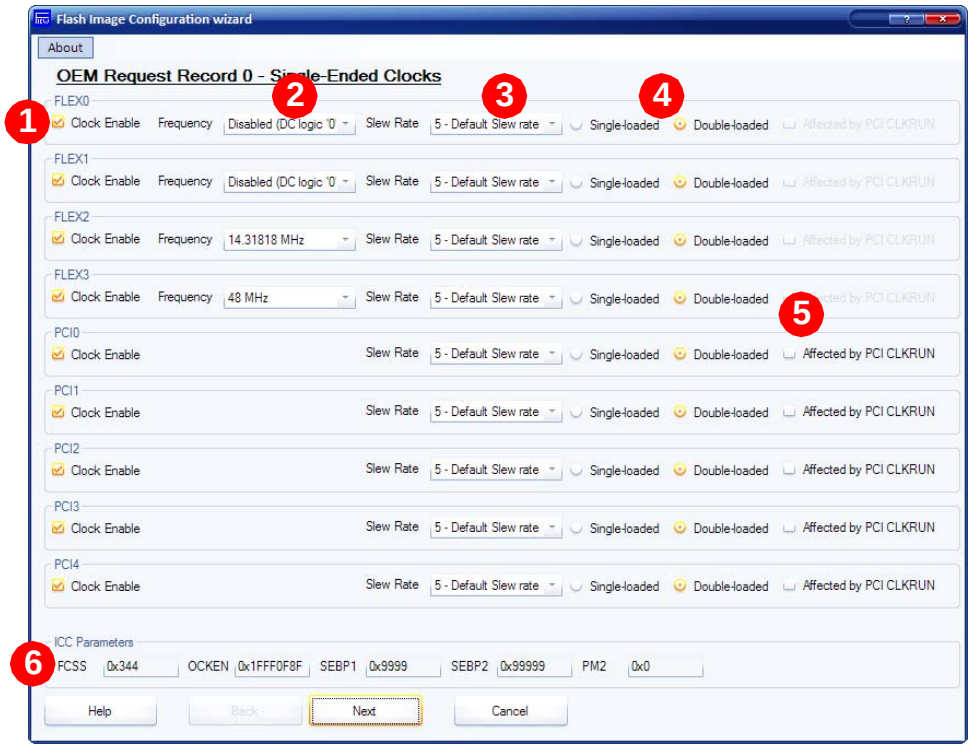
Screen	#	CRB Setting	Setting for All Platforms
	1	1	SPI flash binary images across multiple board designs can contain the same block of Clock Control Parameters (OEM Request Records), up to 7 sets total. This parameter selects how many total OEM Request Records will be built into the image.
	2	OEM Request Record 0	Specifies which clock control parameter set is to be used by the final generated SPI flash binary image by the target platform at boot time.
	3	Clicking **Edit** will open a new dialog box with Clock Control Parameters belonging to the associated OEM Request Record.	
	4	**Unchanged** indicates that all FITC default settings will be used to configure the associated OEM Request Record. What these FITC defaults are can be found in Appendix A (page 75). **Changed** indicates that Clock Control Parameters in the associated OEM Request Record have been changed from their default values.	
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-14. Configuration Wizard: OEM Request Record — Single-Ended Clocks (1 of 2)

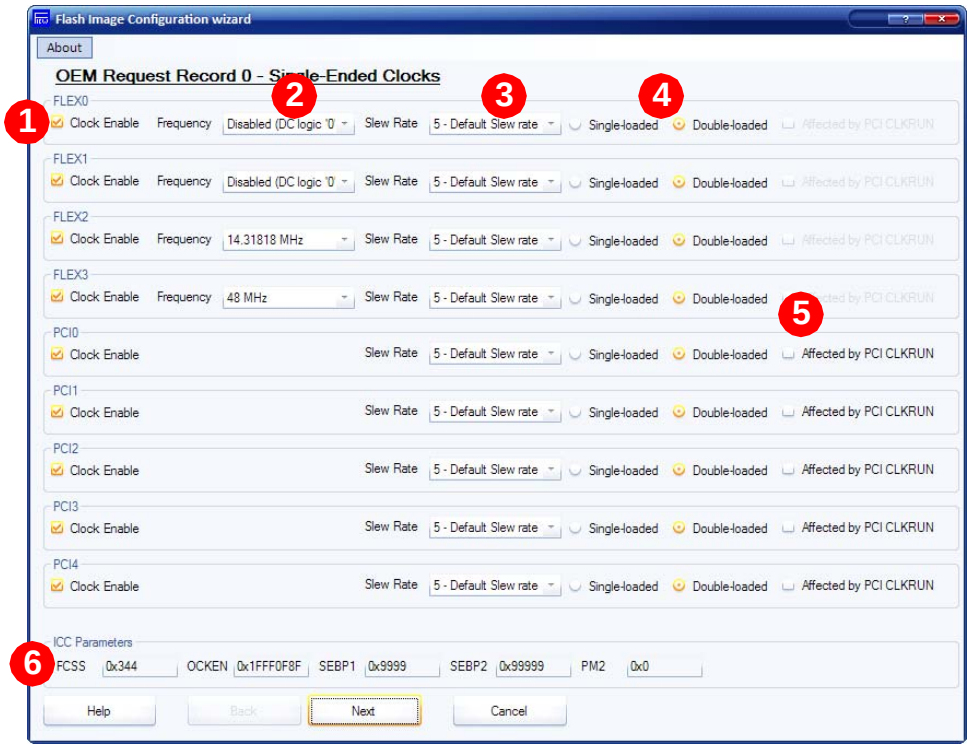
Screen	#	CRB Setting	Setting for All Platforms



#	CRB Setting	Setting for All Platforms
1	**Checked** for all PCI and FLEX clocks	**Unchecked** = Output clock is gated to low state **Checked** = Output buffer is enabled to toggle once its clock source has been initialized
2	**Disabled (DC Logic '0')** for FLEX0, FLEX1 **14.31818 MHz** for FLEX2 **48 MHz** for FLEX3	Controls muxing to select sources for FLEX clock outputs. ***Note:*** PCI clock outputs are fixed at 33 MHz, but FLEX clock outputs may be configured to act as PCI outputs. ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the Ibex Peak EDS for configuration of GPIO vs. native usage.
3	**5-Default Slew Rate** for all PCI and Flex clocks	Controls slew rate for PCI and FLEX clocks. PCI Specifications 2.4 and 3.0 allow for an acceptable slew rate range of 1 to 4 V/ns. ME FW programmability allows for slew rate to be specified between 0.6 to 2 V/ns for two reasons: • Slew rates exceeding 2 V/ns can have adverse effects on platform EMI • Slew rates lower than 1 V/ns can be specified for EMI benefits, at the risk of violating PCI specification
Do not click **Next** yet. Check the next table in this document.		

Table 2-15. Configuration Wizard: OEM Request Record — Single-Ended Clocks (2 of 2)

Screen	#	CRB Setting	Setting for All Platforms



#	CRB Setting	Setting for All Platforms
4	**Double-loaded** for all PCI and FLEX clocks	Sets programmable series resistance for PCI and FLEX clocks.
5	**Unchecked** for all PCI clocks	Enables support for CLKRUN protocol for PCI 33 MHz clocks muxed out to CLKOUTFLEX[3:0] and CLKOUT_PCI[4:0]. **Checked** = Corresponding CLKOUTFLEX PCI clock is free-running, unaffected by CLKRUN protocol **Unchecked** = Corresponding CLKOUTFLEX PCI clock is shut off when CLKRUN protocol turns off PCI clocks ***Note:*** When the corresponding CLKOUTFLEX pins are not configured for PCI 33Mhz clock, this option is disabled and **unchecked**.
6	Reports the dword values of FCSS, OCKEN, SEBP1, SEBP2, and PM2 Clock Control Parameters, as they are affected by the settings on this screen. See Appendix A (page 75) for more information on Clock Control Parameters.	

Click **Next** to advance to the next screen, or **Back** to return to the previous screen.

Table 2-16. Configuration Wizard: OEM Request Record — Differential Clocks

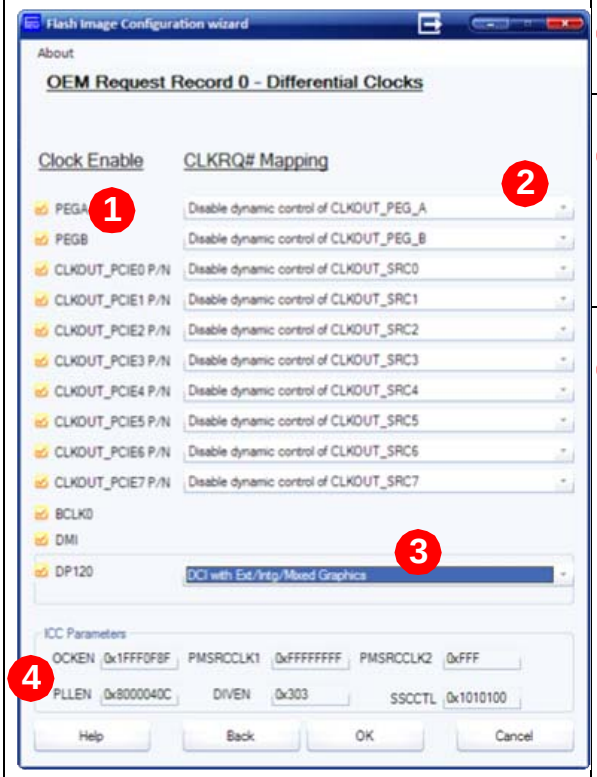
Screen	#	CRB Setting	Setting for All Platforms
	1	**Checked** for all differential clock outputs	**Unchecked** = Output clock is gated to low state **Checked** = Output buffer is enabled to toggle once its clock source has been initialized
	2	**Disable dynamic control** for all PCI Express* clocks	Assigns dynamic CLKRQ# control of SRC clocks. Each PCI Express* clock may be assigned to a muxed CLKRQ#/GPIO PCH pin. ***Note:*** These CLKRQ# settings only take effect when this muxed CLKRQ#/GPIO pin is configured for CLKRQ# native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.
	3	DCI with Ext/ Intg/Mixed Graphics	**DCI with Ext/Intg/Mixed Graphics** = Display Clock Intergration (DCI) Mode clock generation for Display Clock (PCH generation from 25-MHz crystal). • For the CRB, use this with MPG BIOS 072 or CG BIOS 154 or later. • Non-CRB BIOS requires VBIOS that supports DCI. • Use in OS requires Intel® Graphics Accelerator Driver support for DCI. **External Graphics only** = Use this setting if platform supports external graphics only **BTM with Ext/Intg Graphics** = Buffer Through Mode clock generation for Display Clock (CK505 generation from 14-MHz crystal). • This option may be used if the platform supports only LVDS and/or VGA displays For the CRB, use this with BIOSes earlier than MP072 or CG154.
	4	Reports the dword values of OCKEN, PMSRCCLK1, and PMSRCCLK2 Clock Control Parameters, as they are affected by the settings on this screen. See Appendix A (page 75) for more information on Clock Control Parameters.	
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-17. Configuration Wizard: Braidwood Configuration

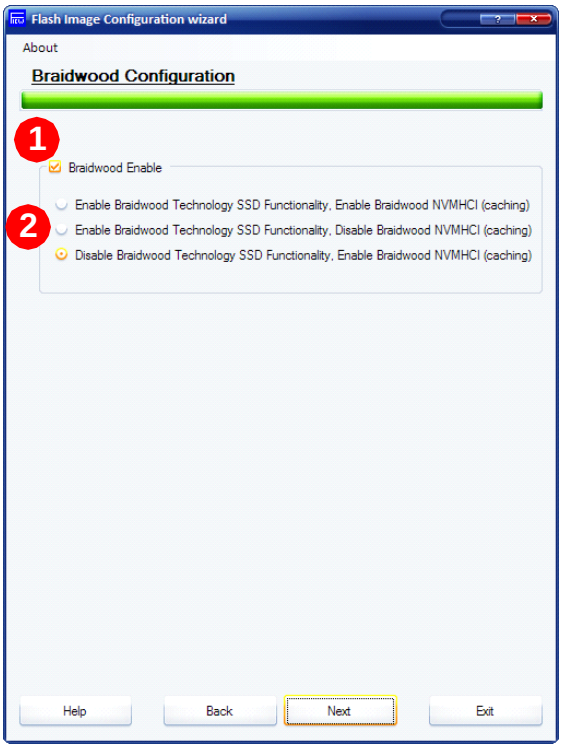
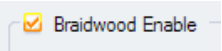
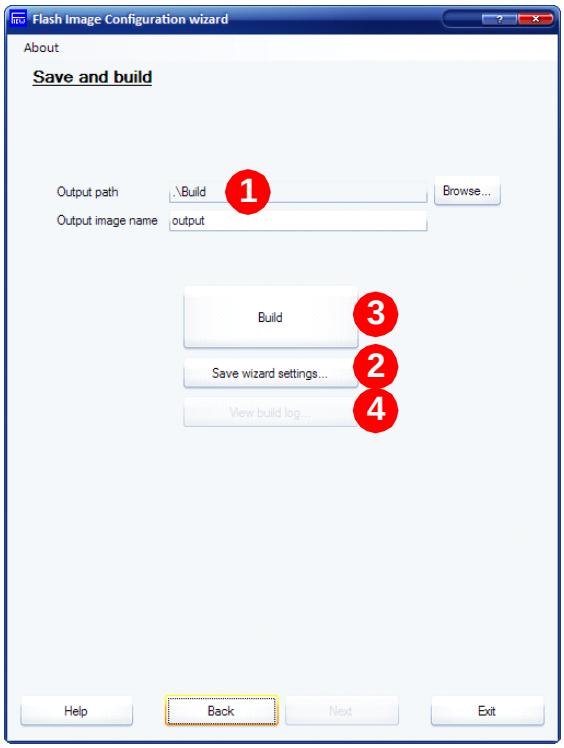
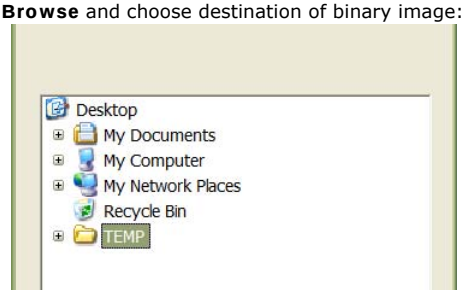
Screen	#	CRB Setting	Setting for All Platforms
	1	Checked	Check the **Braidwood Enable** option to enable Braidwood Technology. 
	2	Disable Braidwood Technology SSD Functionality, Enable Braidwood NVMHCI (caching)	SSD capability is not currently available for Braidwood Technology. Use the CRB setting for all platforms.
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

Table 2-18. Configuration Wizard: Save and Build

Screen	#	CRB Setting	Setting for All Platforms
	1	Click **Browse** and choose destination of binary image:  Put desired image name in **Output image name:**	
	2	Click **Save Wizard Settings** and choose the name of the configuration file of your choice	
	3	Click **Build** to create the flash image	
	4	Click on **View Build Log** to view errors, if Image Failed to build. Common errors are: • Missing or incorrect ME VSCC values. This only is necessary if using a Intel ME 4MB FW SKU binary for ME region. • Using _UPD.bin files as the source for ME region	
Click **Next** to advance to the next screen, or **Back** to return to the previous screen.			

§

3 Image Creation: Flash Image Tool (FITC)

Flash Image Tool (FITC) will be used to generate a full SPI flash binary image with Descriptor, GbE, BIOS, and Intel® ME Regions. Use the steps shown in following sections.

This chapter will also cover how this image can be burned onto the target platform's SPI Flash part(s).

3.1 Start FITC and Load the Default Settings XML File

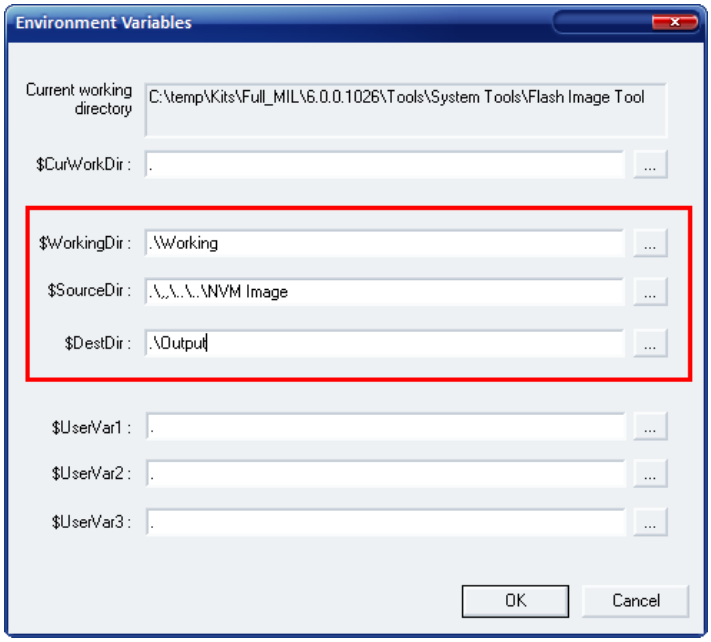
1. Invoke Flash Image Tool. Using Explorer*, navigate to **[root]\Tools\System Tools\Flash Image Tool**. Ensure that FIT's directory contents are intact (Section , page 37). Double-click **fitc.exe**.
2. In the main menu select **File | Open…**. In the Open dialog that appears navigate to **[root]\Tools\System Tools\Flash Image Tool**. Click on **newfiletmpl.xml** and click **OK**.

3.2 Set Up The Build Environment

1. In the main menu select **Build | Environment Variables…**. Edit your configuration as shown below. Note that in the example, **[root]** is **".**". **Source Directory** is where FIT will look to find binary images during the image creation process. **Destination Directory** is where FIT will save the SPI flash binary image. Click **OK** to apply your changes.

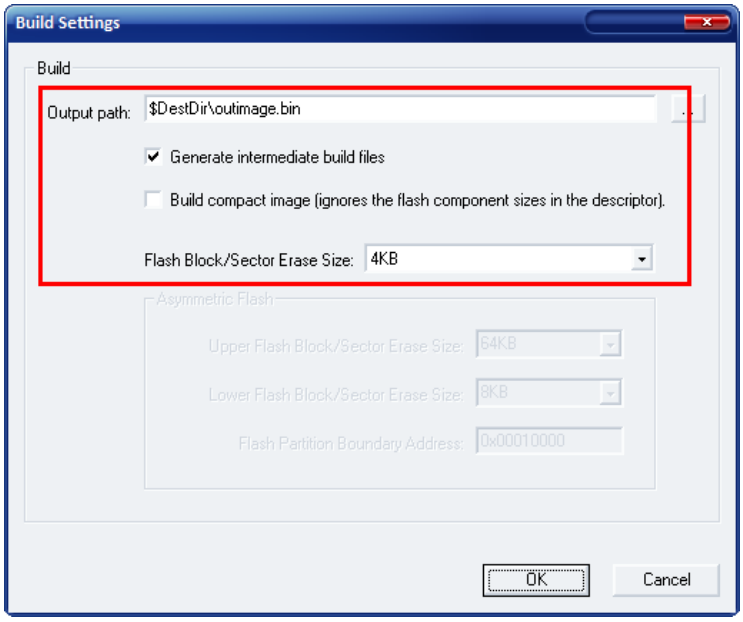
Intel Confidential

Figure 3-1. Build | Environment Variables...



2. In the main menu select **Build | Build Settings...**. Leave the defaults for **Output Path**, **Generate intermediate build files**, and **Build compact image** as shown. Change the **Flash Block/Sector Erase Size** as appropriate for your SPI flash part(s).

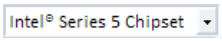
Figure 3-2. Build | Build Settings...



3.3 Configure PCH Silicon Stepping

Leave the **PCH Silicon Stepping Combo Box** at its default value of **Intel® 5 Series Chipset**.

Figure 3-3. PCH Silicon Stepping Combo Box



3.4 Set Up Descriptor and SPI Flash Device(s)

Table 3-1. Flash Image | Descriptor Region

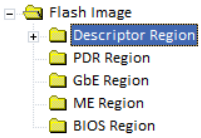
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab. Select **Flash Image | Descriptor Region** • Set the parameters in the **Descriptor Region** section as shown  	Descriptor region length	0h	Leave this at zero. Allows FITC to auto-size the descriptor region length.

Table 3-2. Flash Image | Descriptor Region | Descriptor Map

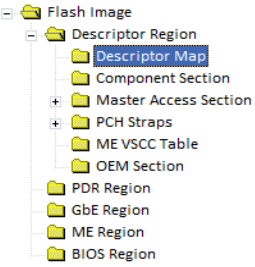
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Descriptor Map** • Set the parameters in the **Descriptor Map** section as shown  	**Yellow means custom settings may be required, otherwise use CRB setting.**		
	Region base address	0x00000004	Flash region base address (FRBA)
	Number of flash components	2	Number of SPI flash devices on the platform **1** or **2** = Total SPI flash devices **0** = Build ME region only
	Component base address	0x00000002	Unless severely constrained in Descriptor for free flash space, do not change this
	Number of PCH straps	16	
	PCH straps base address	0x00000010	Unless severely constrained in Descriptor for free flash space, do not change this
	Number of Masters	2	
	Master base address	0x00000006	Unless severely constrained in Descriptor for free flash space, do not change this
	Number of PROC straps	0	
	PROC straps base address	0x00000020	

Table 3-3. Flash Image | Descriptor Region | Component Section

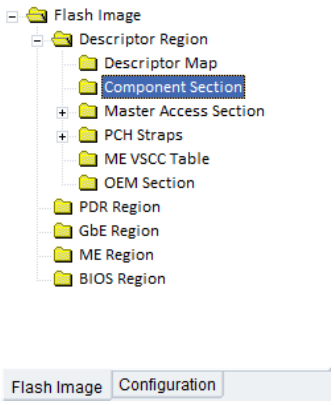
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab. Select **Flash Image | Descriptor Region | Component Section** • Set the parameters in the Component Section section as shown 	**Yellow means custom settings may be required, otherwise use CRB setting.**		
	Read ID and Read Status clock frequency	33MHz	Lowest common frequency of all SPI flash parts on the platform. **50MHz** support is only available in Ibex Peak B- or later stepping.
	Write and erase clock frequency	33MHz	Lowest common frequency of all SPI flash parts on the platform. **50MHz** support is only available in Ibex Peak B- or later stepping.
	Fast read clock frequency	33MHz	In order for PCH HW to override its own internal default value (20 MHz), **Fast Read Support** must be CRB Set To **true**. **50MHz** support is only available in Ibex Peak B- or later stepping.
	Fast read support	true	
	Read clock frequency	20MHz	
	Flash component 2 density	4MB	Size of second SPI Flash part on the platform.
	Flash component 1 density	4MB	Size of first SPI Flash part on the platform.
	Invalid instruction 3	0	Illegal instruction op-code. Check flash part datasheet. **0** = no instruction is specified
	Invalid instruction 2	0	Illegal instruction op-code. Check flash part datasheet. **0** = no instruction is specified
	Invalid instruction 1	0	Illegal instruction op-code. Check flash part datasheet. **0** = no instruction is specified
	Invalid instruction 0	0	Illegal instruction op-code. Check flash part datasheet. **0** = no instruction is specified
	Flash Partition Boundary	0x00000000	FPBA. Only applies to SPI flash parts with asymmetric block/sector erase sizes. Configured in main menu option **Build | Build Settings** (see Section 3.2, page 37).

Table 3-4. Flash Image | Descriptor Region | Master Access Section | CPU/BIOS

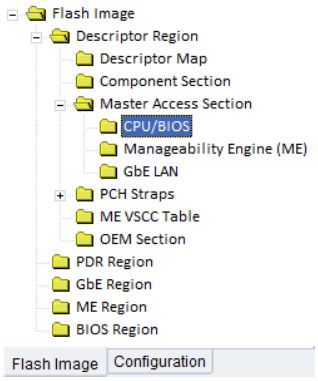
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Master Access Section | CPU/BIOS** • Set the parameters in the **CPU/BIOS** section as shown  	**Yellow means custom settings may be required.**		
	PCI Bus ID	0	
	PCI Device ID	0	
	PCI Function ID	0	
	Read Access	0xFF	Controls read access by BIOS to: • Bit 0: Descriptor (region 0) • Bit 1: BIOS region (region 1) • Bit 2: ME FW region (region 2) • Bit 3: GbE FW region (region 3) • Bit 4-7: Regions 4 through 7 **0x0B** = Production platform **0xFF (default)** = Non-production/debug platform
	Write Access	0xFF	Controls write access by BIOS. Structure is identical to **Read access** parameter. **0x0A** = Production platform **0xFF (default)** = Non-production/debug platform

Table 3-5. Flash Image | Descriptor Region | Master Access Section | Manageability Engine (ME)

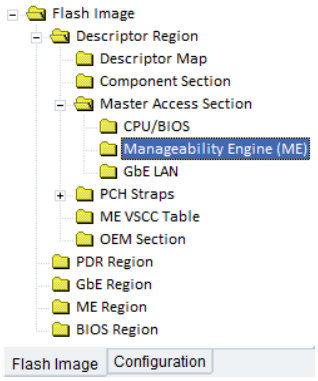
Location	Parameter	CRB Set To	Settings for target platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Master Access Section | Manageability Engine (ME)** • Set the parameters in the **Manageability Engine (ME)** section as shown  	**Yellow means custom settings may be required.**		
	PCI Bus ID	0	
	PCI Device ID	0	
	PCI Function ID	0	
	Read access	0xFF	Controls read access by ME FW to: • Bit 0: Descriptor (region 0) • Bit 1: BIOS region (region 1) • Bit 2: ME FW region (region 2) • Bit 3: GbE FW region (region 3) • Bit 4-7: Regions 4 through 7 **0x0D** = Production platform **0xFF (default)** = Non-production/debug platform
	Write access	0xFF	Controls write access by ME FW. Structure is identical to **Read access** parameter. **0x0C** = Production platform **0xFF (default)** = Non-production/debug platform

Table 3-6. Flash Image | Descriptor Region | Master Access Section | GbE LAN

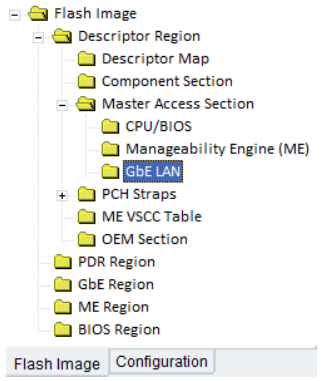
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | Master Access Section | GbE LAN** • Set the parameters in the **GbE LAN** section as shown  	**Yellow means custom settings may be required.**		
	PCI Bus ID	1	1
	PCI Device ID	3	3
	PCI Function ID	0	0
	Read access	0xFF	Controls read access by GbE FW to: • Bit 0: Descriptor (region 0) • Bit 1: BIOS region (region 1) • Bit 2: ME FW region (region 2) • Bit 3: GbE FW region (region 3) • Bit 4-7: Regions 4 through 7 **0x08** = Production platform **0xFF (default)** = Non-production/debug platform
	Write access	0xFF	Controls write access by GbE FW. Structure is identical to **Read access** parameter. **0x08** = Production platform **0xFF (default)** = Non-production/debug platform

Table 3-7. Flash Image |Descriptor Region | ME VSCC Table | Add Table Entry

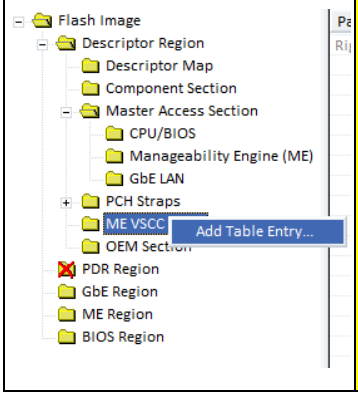
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | ME VSCC Table** • Right click on **ME VSCC Table** to add entry name  	ADD Table Entry Value	For Mobile and Desktop CRBs use **AT26DF321**	Set this to the name of the SPI Flash device on the target platform. ***Note:*** The **AT26DF321** entry may already be created as part of the default FITC template.

Table 3-8. Flash Image | Descriptor Region | ME VSCC Table | AT26DF321

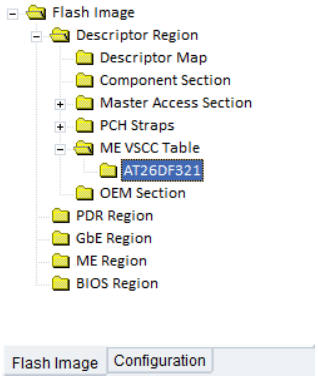
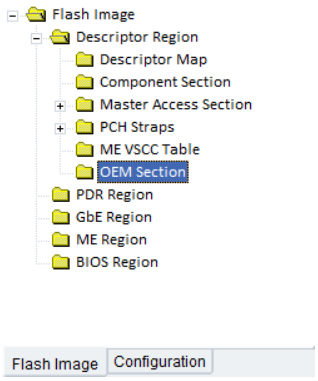
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | Descriptor Region | ME VSCC Table | AT26DF321** • Set the parameters for the Atmel 4-MB SPI part in the **AT26DF321** section as shown  	**Yellow means custom settings may be required.**		
	VendorID	For Mobile and Desktop CRBs use **0x1F**	For information on values that need to be entered in this section, refer to the *Intel® Ibex Peak Chipset Family EDS* and the SPI Flash device 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 vendor datasheet for the specific SPI Flash part. In *Ibex Peak EDS*, Section **VSCC0 — Vendor Specific Component Capabilities 0** describes the 32-bit VSCC register value. Default is **0x00**.
	Device ID 0	For Mobile and Desktop CRBs use **0x47**	Default is **0x00**.
	Device ID 1	0x00	
	VSCC register value	For Mobile and Desktop CRBs use **0x20152015**	Default is **0x00000000**.

Table 3-9. Flash Image | Descriptor Region | OEM Section

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **Flash Image | Descriptor Region | OEM Section** • Set the parameters in the **OEM Section** section as shown  	Binary input file	(leave blank)	This is an optional field and input depends on Customer Design and features support.

3.4.1 Set Up Soft-Straps (Ibex Peak B-stepping Only)

Table 3-10. Flash Image | Descriptor Region | PCH Straps | PCH Strap 0

Ibex Peak B-Stepping

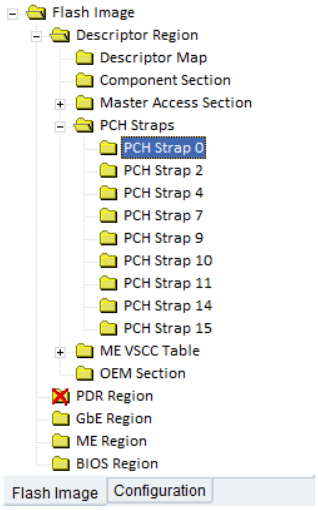
Location	Parameter	CRB Set To	Settings for Any Platform
Ibex Peak B-stepping only. Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 0** • Set the parameters in the **PCH Strap 0** section as shown 	**Yellow means custom settings may be required.**		
	BIOS Boot Block Size	64KB	BIOS Boot Block (BBB) is bare minimum BIOS code required to boot a platform. This soft-strap allows for proper address bit to be inverted as required by BBB Size. **64KB (default)** = Invert A16 if Top Swap is enabled **128KB** = Invert A17 if Top Swap is enabled **256KB** = Invert A18 if Top Swap is enabled If BIOS is stored in a separate SPI Flash device or in FWH (see Configurations "B", "C", and "D" in Appendix B (page 93) then leave this parameter at **64KB**.
	Intel® Anti-Theft Technology Data Protection Disable	true	**true** = Set for all platforms
	DMI RequesterID Security Check Disable	false	Indicates if RequesterID checking during DMI accesses is disabled. This parameter is only applicable for server platforms that contain multiple PCHs. **false (default)** = Set for all platforms
	LANPHYPC_GP12_SEL	1	**1** = Only required if target platform has Intel wired LAN and PCH GP12 is used as LAN_PHYPC for Intel LAN. **0 (default)** = PCH GP12 is used as General Purpose Input/Output (GPIO) pin. Must be **0** if Third-party LAN is present.
	Intel® ME SMBus Enable	true	**true** = Set for all platforms
	Intel® ME SMBus Frequency	**100kHz** for B-stepping	
	SMLink0 Enable	true	**true (default)** = Intel LAN is present **false** = Third-party LAN is present
	SMLink0 Frequency	**100kHz** for B-stepping	
	SMLink1 Enable	Mobile CRB uses **true** Desktop CRB uses **true**	**true (default)** = SMLink1 is being used by EC/SIO/BMC for Thermal Reporting. **false** = Set for all other platforms ***Note:*** Must be set to true for desktop platforms even if an EC/SIO/BMC is not using SMLink1 for Thermal Reporting. Otherwise there may be issues with: • Intel® QST • Power flows
	SMLink1 Frequency	**100kHz** for B-stepping	
	Chipset Config	01b	

Table 3-11. Flash Image | Descriptor Region | PCH Straps | PCH Strap 2

Ibex Peak B-Stepping

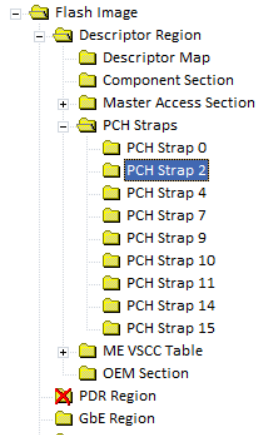
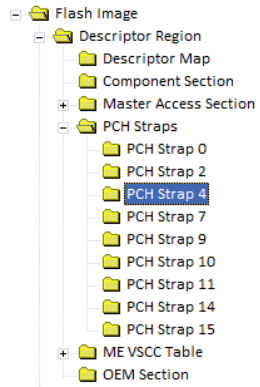
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 2** • Set the parameters in the **PCH Strap 2** section as shown 	**Yellow means custom settings may be required.**		
	Intel® ME SMBus I2C Address Enable (SMBI2CEN)	false	Refers to device-to-PCH write address over Intel® ME SMBus. **false (default) =** Set for all platforms
	Intel® ME SMBus I2C Address (SMBI2CA)	0x00	Refers to device-to-PCH write address over Intel® ME SMBus. **0x00 (default) =** Set for all platforms
	Intel® ME SMBus ASD Address Enable (MESMASDEN)	false	
	Intel® ME SMBus ASD Address (MESMASDA)	0x00	
	Intel® ME SMBus GP Address Enable	false	Refers to device-to-PCH read address over Intel® ME SMBus.
	Intel® ME SMBus GP Address	0x00	Refers to device-to-PCH read address over Intel ME SMBus.

Table 3-12. Flash Image | Descriptor Region | PCH Straps | PCH Strap 4

Ibex Peak B-Stepping

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 4** • Set the parameters in the **PCH Strap 4** section as shown 	**Yellow means custom settings may be required.**		
	GbE PHY SMBus Address	0x64	Intel wired LAN PHY SMBus address. No change required for this soft-strap value.
	GbE MAC SMBus Address	0x70	Intel wired LAN MAC SMBus address. No change required for this soft-strap value.
	GbE MAC SMBus Address Enable	true	**true** = Intel LAN is present **false** = Third-party LAN is present
	PHY Connectivity	10: PHY Connectivity	**10: PHY Connectivity** = Intel LAN is present **00: No PHY Connected (default)** = Third-party LAN is present

Intel Confidential

Table 3-13. Flash Image | Descriptor Region | PCH Straps | PCH Strap 7

Ibex Peak B-Stepping

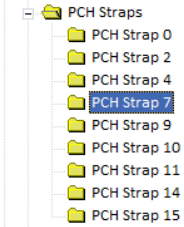
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab. • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 7** • Set the parameters in the **PCH Strap 7** section as shown in the table below 	Intel® ME SMBus Subsystem Vendor & Device ID for ASF2	0x00000000	0x00000000

Table 3-14. Flash Image | Descriptor Region | PCH Straps | PCH Strap 9

Ibex Peak B-Stepping

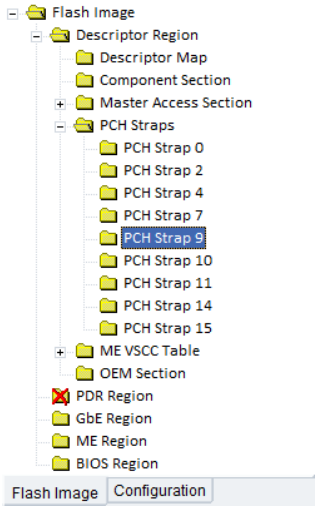
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 9** • Set the parameters in the **PCH Strap 9** section as shown 	**Yellow means custom settings may be required.**		
	Intel® PHY Over PCI Express Enable (PHY_PCIE_EN)	true	**true (default)** = Intel LAN is present **false** = Third-party LAN is present
	Intel® PHY PCIe Port Select (PHY_PCIEPORTSEL)	101	Only necessary if Intel LAN is present. **101** = Third-party LAN is present (don't care setting) **000** = Port 1 **001** = Port 2 **010** = Port 3 **011** = Port 4 **100** = Port 5 **101** = Port 6 **110** = Port 7 **111** = Port 8 Default is **101**.
	DMI Lane Reversal	false	This parameter must reflect platform topology.
	PCIe Lane Reversal 2	false	This parameter must reflect platform topology. ***Note:*** This parameter can only be set to true if **PCIe Port configuration 2** is set to **1x4**.
	PCIe Lane Reversal 1	false	This parameter must reflect platform topology. ***Note:*** This parameter can only be set to true if **PCIe Port configuration 1** is set to **1x4**.
	PCIe Port Configuration 2	Desktop CRB uses **00: 4x1 Ports 5-8 (x1)** Mobile CRB uses **10: 2x2 Port 5 (x2), Port 7 (x2), Ports 6, 8 (disabled)**	This parameter must reflect platform topology.
	PCIe Port Configuration 1	4x1 Ports 1-4 (x1)	This parameter must reflect platform topology.

Table 3-15. Flash Image | Descriptor Region | PCH Straps | PCH Strap 10

Ibex Peak B-Stepping

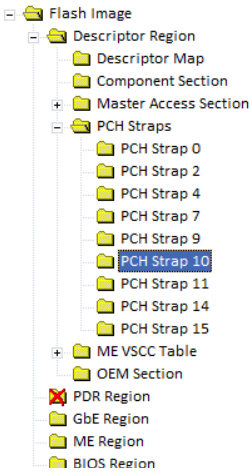
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 10** • Set the parameters in the **PCH Strap 10** section as shown  	ME boot from flash	false	Also see Table 3-21, (page 51). **true** = ME ROM bypass image is included in the ME Region binary. Instead of using ME ROM code hard-coded in the PCH, Intel® ME will use bypass code in SPI instead. **false (default)** = No ME Region binary loaded, or ME Region binary does not contain ME ROM bypass image
	ME MDDD Enable	true	**true** = Enable MDDD logging. Set for non-production/debug platforms. **false (default)** = Set for production platforms
	ME MDDD Address	0x38	**0x38** = Enable MDDD logging. Set for non-production/debug platforms. **0x00** = Set for production platforms.
	ICC OEM Config Select	0	Specifies which clock control parameter set is to be used by the final generated SPI flash binary image by the target platform at boot time. SPI flash binary images across multiple board designs are expected to contain the same block of clock control parameters, up to 7 sets total. The 'Record #' refers to records created under the Configuration Tab, **Flash Image | Configuration | ICC Data**. Default is **0**.

Table 3-16. Flash Image | Descriptor Region | PCH Straps | PCH Strap 11

Ibex Peak B-Stepping

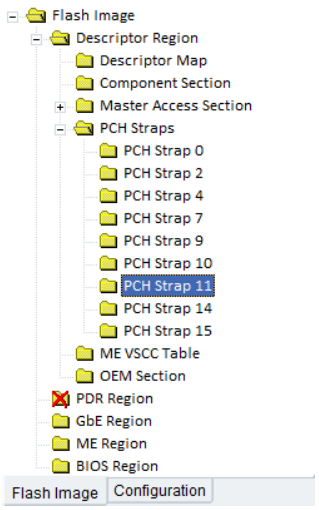
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the **Flash Image** tab • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 11** • Set the parameters in the **PCH Strap 11** section as shown 	SMLink1 I2C Address Enable	Mobile CRB uses **true** Desktop CRB uses **false**	**true (default)** = Enable EC/SIO/BMC to interact Thermal Reporting feature over SMLink1 **false** = Platform has no EC/SIO/BMC on SMLink1
	SMLink1 I2C Address	Mobile CRB uses **0x4C** Desktop CRB uses **0x00**	This parameter defines a write address for PCH over SMLink1. Set this to an address supported by EC/SIO/BMC hardware. Note that PCH/Intel® ME acts as slave on SMLink and EC/SIO/BMC acts as master. **0x4C (default)** = PCH SMBus write address for EC on mobile CRB **0x00** = Platform has no EC/SIO/BMC on SMLink1
	SMLink1 GP Address Enable	Mobile CRB uses **true** Desktop CRB uses **false**	**true (default)** = Enable EC/SIO/BMC to interact Thermal Reporting feature over SMLink1 **false** = Platform has no EC/SIO/BMC on SMLink1
	SMLink1 GP Address	Mobile CRB uses **0x4B** Desktop CRB uses **0x00**	This parameter defines a read address for PCH over SMLink1. Set this to an address supported by EC/SIO/BMC hardware. Note that PCH/Intel® ME acts as slave on SMLink and EC/SIO/BMC acts as master. **0x4B (default)** = PCH SMBus read address for EC on mobile CRB **0x00** = Platform has no EC/SIO/BMC on SMLink1

Table 3-17. Flash Image | Descriptor Region | PCH Straps | PCH Strap 14

Ibex Peak B-Stepping

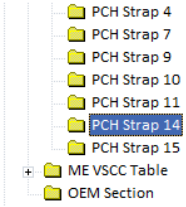
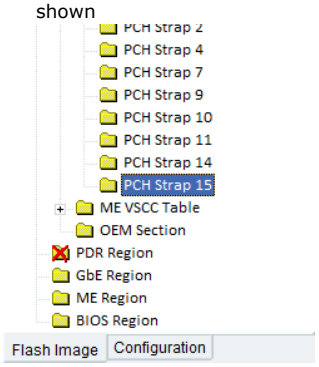
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select **FlashImage | Descriptor Region | PCH Straps | PCH Strap 14** • Set the parameters in the **PCH Strap 14** section as shown in the table below 	**Yellow means custom settings may be required.**		
	VE Enable	true	This option is always read-only. **true** = Target platform supports Braidwood **false** = Braidwood support disabled
	VE Boot from Flash	false	This option is always read-only. See Table 3-21, (page 51). **true** = VE ROM bypass image is included in the ME Region binary. Instead of using VE ROM code hard-coded in the PCH, VE will use bypass code in SPI instead. **false (default)** = No ME Region binary loaded, or ME Region binary does not contain VE ROM bypass image
	Braidwood Technology SSD enabled	true	**false** =Set for all platforms
	Braidwood Technology NVMHCI enable	true	**true** = Enable NVMHCI support for Braidwood **false** =NVMHCI support for Braidwood is disabledSet for all platforms

Table 3-18. Flash Image | Descriptor Region | PCH Straps | PCH Strap 15

Location	Parameter	CRB Set To	Settings for Any Platform
Ibex Peak B-Stepping Follow navigation tree below: • Select **Flash Image | Descriptor Region | PCH Straps | PCH Strap 15** • Set the parameters in the **PCH Strap 15** section as shown 	t209 Timing	1ms	Minimum timing between PWROK assert and CPUPWRGD assert. Change to reflect optimal timing for your platform. Can also be set to **50ms**, **5ms**, and **100ms**. Leave at default value of **1ms** unless experiencing power sequencing issues.
	Intel®Integrated LAN Enable	true	**true** = Intel LAN is enabled **false** = Intel LAN is disabled

3.5 Set Up SPI Flash Regions

Table 3-19. Flash Image | PDR Region

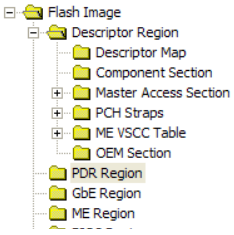
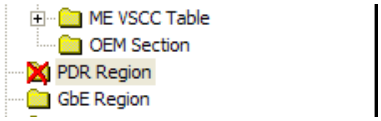
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image • Select **Flash Image | PDR Region** • Set the parameters in the **PDR Region** section as shown 	PDR Region Length	PDR Region is disabled	Displays Region size information when **Binary input file** is specified.
	Binary Input File	PDR Region is disabled	Load a Platform Data Region binary if required and available.
...or if NOT using Platform Data Region (PDR)			
A red "X" will indicate whether this Region is disabled. If this Region is not disabled, disable it by right-clicking on **Flash Image | PDR Region** and selecting **Disable Region**.			

Table 3-20. Flash Image | GbE Region

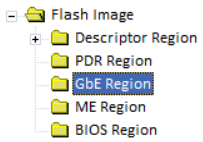
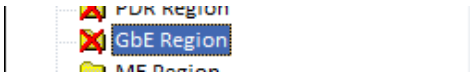
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image • Select **Flash Image | GbE Region** • Set the parameters in the **GbE Region** section as shown 	**Yellow means custom settings may be required.**		
	GbE LAN region length	0h	
	Binary input file	Desktop/Server CRB uses **xxxxx_DSK** image Mobile CRB uses **LAN_SWITCH** image	**Recommendation** If Using Intel LAN then Navigate to your **Source Directory** (as specified in Section 3.1, page 37) and switch to the **GbE** subdirectory. Choose the Intel GbE LAN FW image as follows: • Desktop platforms should use the xxxxx_DSK image • Mobile platforms that support docking and uses a LAN switch should use the _LAN_SWITCH_ image • Mobile platforms that support docking and does not use a LAN switch should use the _NON_LAN_SWITCH_ image. If IEEE conformance does not meet requirements, then _LAN_SWITCH_ version may need to be used. • See the documents in the **GbE** subdirectory for more information If not using Intel LAN then leave this parameter blank.
	Major Version	0	Displays major revision value for Intel LAN GbE FW version when **Binary input file** is specified.
	Minor Version	0	Displays minor revision value for Intel LAN GbE FW version when **Binary input file** is specified.
	Image ID	0	Displays image ID value for Intel LAN GbE FW version when **Binary input file** is specified.
...or if not using Intel wired LAN device			
A red "X" will indicate whether this Region is disabled. If this Region is not disabled, disable it by right-clicking on **Flash Image | GbE Region** and selecting **Disable Region**.			

Table 3-21. Flash Image | ME Region

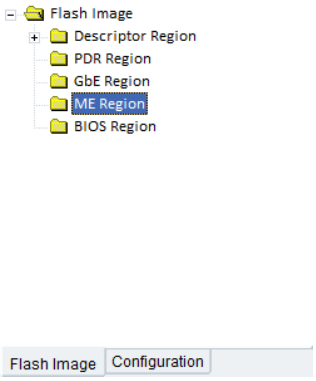
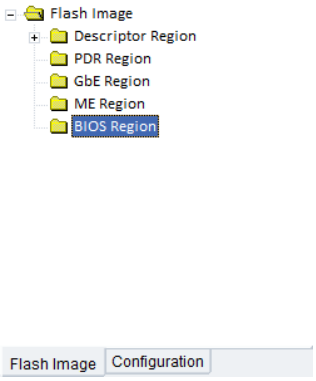
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image tab • Select **Flash Image | ME Region** • Set the parameters in the **ME Region** section as shown • **Note:** Loading an ME FW binary image that contains ME ROM Bypass unlocks the **ME Boot from Flash** parameter in **Flash Image | Descriptor Region | PCH Straps | PCH Strap 10**  	Binary input file	Navigate to your **Source Directory** (as specified in Section 3.1, page 37) and switch to the **Firmware** subdirectory. Choose the ME FW binary image. • ***Note:*** You may choose to build the ME Region only. To do so, **Flash Image | Descriptor Region | Descriptor Map** parameter **Number of flash components** must be set to **0**. • ***Note:*** Loading an ME FW binary image that contains ME ROM Bypass unlocks the **ME Boot from Flash** parameter in **Flash Image | Descriptor Region | PCH Straps | PCH Strap 10**.	
	Intel® QST config file	**Load a QST configuration file** is only used when Intel® QST is enabled and there is a pre-existing configuration file.	
	Permit file		
	* Partition Rom Bypass Enabled		Not technically a parameter. This information panel appears when an ME FW image enables ME boot directly from flash.
	Major Version	0	Displays major revision value for ME FW version when **Binary input file** is specified.
	Minor Version	0	Displays minor revision value for ME FW version when **Binary input file** is specified.
	Hotfix Version	0	Displays hotfix value for ME FW version when **Binary input file** is specified.
	Build Version	0	Displays build value for ME FW version when **Binary input file** is specified.

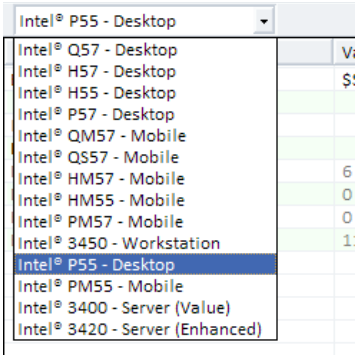
Table 3-22. Flash Image | BIOS Region

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image tab • Select **Flash Image | BIOS Region** • Set the parameters in the **BIOS Region** section as shown  	BIOS Revision		Displays BIOS revision information when **Binary input file** is specified.
	BIOS region length	0h	Displays Region size information when **Binary input file** is specified.
	Binary input file	For the Intel CRB navigate to your **Source Directory** (as specified in Section 3.1, page 37) and switch to the **BIOS** subdirectory. Choose the desktop or mobile BIOS binary image.	For all other platforms point this parameter to the appropriate BIOS image. If BIOS is stored in a separate SPI Flash device or in FWH (see Configurations "B", "C", and "D" in Appendix B (page 93) then leave this parameter blank.

3.6 Configure PCH Silicon SKU

Use the **SKU Manager Combo Box** to select the appropriate platform type for your specific chipset. For Intel® ME 4MB Firmware Alpha 2, the only valid choices are Intel® HM57, and HM55.

Figure 3-4. SKU Manager Combo Box



When a SKU is selected in FITC, Non-SKU PCH silicon will then behave as if it were the selected Production SKU PCH silicon from ME FW perspective. The SKU Manager selection option has no effect on Production SKU PCH silicon. Features cannot be enabled on such SKUs that do not support them. For example, Braidwood Technology cannot be enabled on HM55.

Note: For more information see Table 3-29 (page 59), Table 3-30 (page 60), and Table 3-31 (page 61) for ME FW features listed by Production SKU PCH silicon using Intel® ME 4MB Firmware Alpha 2.

Note: Sections of FITC other than the **Features Supported** folder under **Flash Image | Configuration** will not reflect what is disabled for the selected PCH silicon SKU and/or ME FW binary.

3.7 ME FW Feature Configuration

Note: Do not load or change any parameters in the Configuration tab until you load an ME Region binary.

3.7.1 Clock Control Parameters

Table 3-23. Flash Image | Configuration | ICC Data

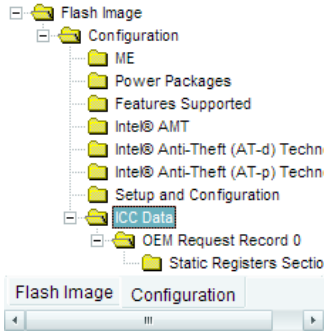
Location	Parameter	CRB Set To	Settings for Any Platform
On the navigation tree to the left, • Select the **Configuration** tab. • Select **Flash Image | Configuration | ICC Data**. • Set the parameters in the **ICC Data** section as shown in the table below. 	Number of Supported SKUs	1	Specify the maximum number of sets of clock configuration parameters need to be specified. It is possible that a clock control parameter set is required for each separate board design. Set to **1** unless multiple platform in single image support is desired.

Table 3-24. Flash Image | Configuration | ICC Data | OEM Request Record 0 | Static Registers Section

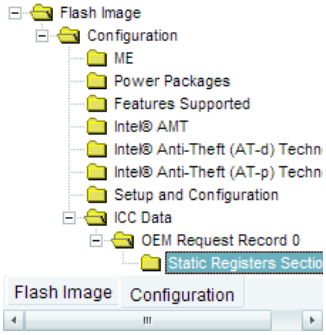
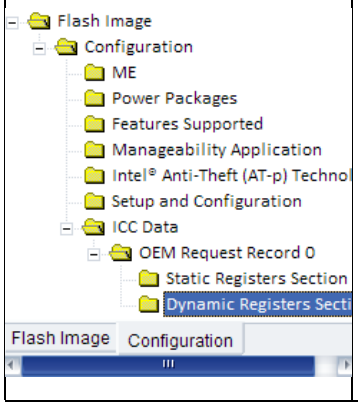
Location	Parameter	CRB Set To	Settings for Any Platform
On the navigation tree to the left: • Select the **Configuration** tab. • Select **Flash Image | Configuration | ICC Data| OEM Request Record 0 | Static Registers Section** • Set the parameters in the **Static Registers Section** section as shown • Each dword parameter shown below is further broken down bit by bit in Flash Image Tool. Reference these bits in Section A.2 (page 77) 	FCSS	Set to **0x00004322**: • F3SS = **100b = Disabled** • F2SS = **011b = 14 MHz** • F1SS = **010b = 33.3 MHz** • F0SS = **010b = 33.3 MHz**	This parameter controls muxing to select sources for Flex Clock outputs. See Section A.2.1, page 77. Default is **0x00000344**.
	PLLEN	0x8000040C	This parameter controls PLL enables. See Section A.2.2, page 78. **0x8000040C** = Display Clock Intergration (DCI) Mode clock generation for Display Clock (PCH generation from 25-MHz crystal). • For the CRB, use this with MPG BIOS 072 or CG BIOS 154 or later. • Non-CRB BIOS requires VBIOS that supports DCI. • Use in OS requires Intel® Graphics Accelerator Driver support for DCI. **0x8000041B** = Use this setting if platform supports external graphics only **0x8000041C** = Buffer Through Mode clock generation for Display Clock (CK505 generation from 14-MHz crystal). • This option may be used if the platform supports only LVDS and/or VGA displays • For the CRB, use this with BIOSes earlier than MP072 or CG154. Default is **0x8000040C**.
	OCKEN	0x1FFF0F8F	This parameter controls enabling of output buffers. See Section A.2.3, page 79. Default is **0x1FFF0F8F.**
	IBEN	0x00000000	This parameter controls enabling of input buffers. See Section A.2.4, page 81. Default is **0x00000000**.
	DIVEN	0x00000303	This parameter controls PLL enables. See Section A.2.6, page 82. **0x00000303 = Display Clock Intergration (DCI) Mode clock generation for Display Clock.** **0x00000100 = Use this setting if platform supports external graphics only** **0x00000003 = Buffer Through Mode clock generation for Display Clock.** Default is **0x8000040C**.
	PM1	0x00000013	Allows VBIOS and Integrated Graphics Device driver to power manage DIV1S (see Figure A-1, page 75). This seting is also safe for processors without Integrated Graphics. See Section A.2.7, page 83. Default is **0x00000013**.
	PM2	0x00000000	This parameter controls power management features of clocks. See Section A.2.8, page 83. Default is **0x00000000**.

Table 3-24. Flash Image | Configuration | ICC Data | OEM Request Record 0 | Static Registers Section

Location	Parameter	CRB Set To	Settings for Any Platform
	SEBP1	0x00009999	This parameter controls double/single load series resistance and slew rate for FLEX clocks. See Section A.2.9, page 84. Default is **0x00009999**.
	SEBP2	0x00099999	This parameter controls double/single load series resistance and slew rate for PCI clocks. See Section A.2.10, page 85. Default is **0x00099999**.
	PMSRCCLK1	0xFFFFFFFF	This parameter controls which CLKRQ# pins on Ibex Peak are assigned to which PCI Express* clocks. CLKRQ# pins may also be completely deassigned with this parameter. See Section A.2.11, page 87. Default is **0xFFFFFFFF**.
	PMSRCCLK2	0x00000FFF	This parameter controls which CLKRQ# pins on Ibex Peak are assigned to which PCI Express* clocks. CLKRQ# pins may also be completely deassigned with this parameter. See Section A.2.13, page 90. Default is **0x00000FFF**.

Table 3-25. Flash Image | Configuration | ICC Data | OEM Request Record 0 | Dynamic Registers Section

Location	Parameter	CRB Set To	Settings for Any Platform
On the navigation tree to the left: • Select the **Configuration** tab. • Select **Flash Image | Configuration | ICC Data| OEM Request Record 0 | Static Registers Section** • Set the parameters in the **Dynamic Registers Section** section as shown • Each dword parameter shown below is further broken down bit by bit in Flash Image Tool. Reference these bits in Section A.2 (page 77)  	SSCCTL	0x1010100	This parameter controls spread spectrum modulation capability of SSC blocks. See Section A.2.2, page 78. **0x1010100** = Display Clock Intergration (DCI) Mode clock generation for Display Clock. **0x1010101** = Use this setting if platform supports external graphics only **0x1010101** = Buffer Through Mode clock generation for Display Clock. Default is **0x1010100**.

Intel Confidential

Table 3-26. High Impact Clock Control Parameters

Clock Output Pin	XML Symbol and Bit Offsets	Default	Description
CLKOUT_FLEX3	FCSS[14:12]	000b	**FLEXCLK3 Source Select (F3SS):** Selects the source of clock to be driven out on CLKOUTFLEX3. **000b** = 48 MHz **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/ GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.
CLKOUT_FLEX3	SEBP1[12]	1b	**FLEXCLK3 Single / Double Load Series Resistance (F3SDLSR):** Sets programmable series resistance for CLKOUTFLEX3. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
CLKOUT_FLEX2	FCSS[10:8]	000b	**FLEXCLK2 Source Select (F2SS):** Selects the source of clock to be driven out on CLKOUTFLEX2. **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/ GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.
CLKOUT_FLEX2	SEBP1[8]	1b	**FLEXCLK2 Single / Double Load Series Resistance (F2SDLSR):** Sets programmable series resistance for CLKOUTFLEX2. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
CLKOUT_FLEX1	FCSS[6:4]	011b	**FLEXCLK1 Source Select (F1SS):** Selects the source of clock to be driven out on CLKOUTFLEX1. **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/ GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.
CLKOUT_FLEX1	SEBP1[4]	1b	**FLEXCLK1 Single / Double Load Series Resistance (F1SDLSR):** Sets programmable series resistance for CLKOUTFLEX1. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage

Table 3-26. High Impact Clock Control Parameters

Clock Output Pin	XML Symbol and Bit Offsets	Default	Description
CLKOUT_FLEX0	FCSS[2:0]	100b	**FLEXCLK0 Source Select (F0SS):** Selects the source of clock to be driven out on CLKOUTFLEX0. **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/ GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.
CLKOUT_FLEX0	SEBP1[0]	1b	**FLEXCLK0 Single/Double Load Series Resistance (F0SDLSR):** Sets programmable series resistance for CLKOUTFLEX0. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
CLKOUT_PCI4	SEBP2[16]	1b	**PCI4 Single/Double Load Series Resistance (PCI4SDLSR):** Sets programmable series resistance for CLKOUT_PCI4. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
CLKOUT_PCI3	SEBP2[12]	1b	**PCI3 Single/Double Load Series Resistance (PCI3SDLSR):** Sets programmable series resistance for CLKOUT_PCI3. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
CLKOUT_PCI2	SEBP2[8]	1b	**PCI2 Single/Double Load Series Resistance (PCI2SDLSR):** Sets programmable series resistance for CLKOUT_PCI2. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
CLKOUT_PCI1	SEBP2[4]	1b	**PCI1 Single/Double Load Series Resistance (PCI1SDLSR):** Sets programmable series resistance for CLKOUT_PCI1. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
CLKOUT_PCI0	SEBP2[0]	1b	**PCI0 Single/Double Load Series Resistance (PCI0SDLSR):** Sets programmable series resistance for CLKOUT_PCI0. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage

The complete clock control parameter reference is provided in Appendix A (page 75). Use it to complete any necessary clock configuration.

3.7.2 Firmware Features and Capabilities

Table 3-27. Flash Image | Configuration | ME

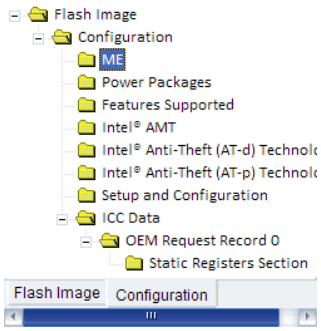
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Configuration Tab • Select **Flash Image | Configuration | ME** • Set the parameters in the **ME** section as shown 	Local FWU Override Counter	0	**-1** = FW Update Counter disabled
	Local FWU Overide Qualifier	0	**0** = Set for all platforms
	FW Update OEM ID	00000000-0000-0000-0000-000000000000	This field provides the ability to target FWUpdate (FWUpdLcl.exe) by Platform OEM. This ID will make sure that customers can only update a platform with an image coming from the platform OEM. The string entered aftIf set to an all zeros, then any input is valid when doing a firmware update.
	ME State on Flash Desc OVR	false	**0 (false)** = FW Update Strap is enabled **1 (true)** = FW Update Strap is blocked
	BIOS Reflash Capable	false	**false** = Disable this capability **true** = Enable this capability
	LAN Power Well Config	3	Intel LAN power configuration selection: **0** = Core Well (SLP_S3#) **1** = Sus Well (RSMRST#) **2** = ME Well (SLP_M#) **3 (recommended)** = SLP_LAN# (MPGIO3)
	WLAN Power Well Config	0x80	**0x80 (recommended)** = Disabled **0x81** = Core Well **0x82** = Sus Well **0x83** = ME Well **0x84** = WLAN Power Controlled via SLP_M# || SPDA
	M3 Power Rails Availability	True	**true** = M3 power rails designed on platform (ME is powered by standby) **false** = M3 power rails not designed on platform (ME is powered by core)
	HECI ME Region Unlockable	true	**false** = Disable HMFPRO LOCK and HMFPRO ENABLE Intel® MEI messages for BIOS-based FW Update **true** = Enable this capability
	Sub System Vendor ID	0x0000	This ID allows OEMs the ability to test boards using Manufacturing Test Permits. Recommend **0x0000**.
	Debug Si Features	0x00000000	Allows OEM Control to enable FW features to assist with the debug of the platform. This control has no effect if used on production silicon.
	Prod Si Features	0x00000000	Allow OEM Control to enable FW features to assist with the production platform.

Table 3-28. Flash Image | Configuration | Power Packages

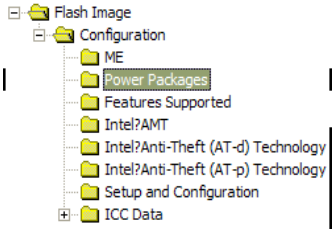
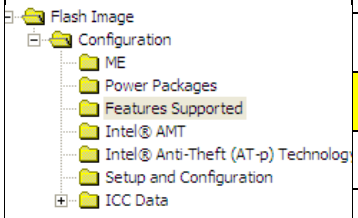
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image • Select **Flash Image | Configuration | Power Packages** • Set the parameters in the **Power Packages** section as shown 	Power Pkg 1 Supported (Desktop: ON in S0)	true	**true** = Set for all platforms
	Power Pkg 2 Supported (Desktop: ON in S0, ME Wake in S3, S4-5)	false	**true** = Set for all platforms
	Default Power Package	1	Select the default Power Package from the avialable packages. Set to **1** for all platforms.

Table 3-29. Flash Image | Configuration | Features Supported

Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image • Select **Flash Image | Configuration | Features Supported** • Set the parameters in the **Features Supported** section as shown 	Enable Intel® Standard Manageability; Disable Intel® AMT	This setting has no effect	
	Intel® Manageability Application Permanently Disabled?	No	**No**
	PAVP 1.5 Permanently Disabled	This setting has no effect	
	Intel® QST Permanently Disabled?	This setting has no effect	
	Sentry Peak Permanently Disabled?	No	**No**
	Intel Remote Wake Technology Supported	This setting has no effect	
	KVM Permanently Disabled?	This setting has no effect	
	Braidwood Technology Permanently Disabled?	No	**No** = Braidwood Technology enable/ disable will be determined by ship state setting **Yes** = Braidwood Technology is permanently disabled
	TLS Permanently Disabled?	No	**No**
	Intel® Manageability Application Enable/ Disable	Enabled	**Enabled**
	PAVP 1.5 Enable/Disabled	This setting has no effect	
	Intel®QST Enable/Disable	This setting has no effect	
	Sentry Peak Enable/ Disable	Enabled	**Enabled**
	Intel Remote Wake Technology Supported Enable/Disable	This setting has no effect	

Intel Confidential

Table 3-30. Flash Image | Configuration | Features Supported (HM57)

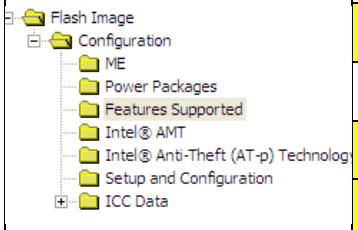
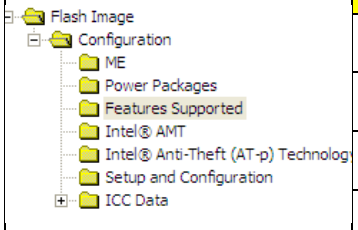
Location	Parameter	CRB Set To	Settings for Any Platform
Depending on which SKU selected, there will be different feature sets shown. Follow navigation tree • Select the Flash Image • Select **Flash Image | Configuration | Features Supported** • Set the parameters in the **Features Supported** section as shown 	Enable Intel® Standard Manageability; Disable Intel® AMT	This setting has no effect for Intel® HM57	
	Intel® Manageability Application Permanently Disabled?	No	**No** = Set for all Intel® HM57 platforms
	PAVP 1.5 Permanently Disabled	No	**No** = Set for all Intel® HM57 platforms
	Intel® QST Permanently Disabled?	This setting has no effect for Intel® HM57	
	Sentry Peak Permanently Disabled?	No	**No** = Set for all Intel® HM57 platforms
	Intel Remote Wake Technology Supported	This setting has no effect for Intel® HM57	
	KVM Permanently Disabled?	No	**No** = Set for all Intel® HM57 platforms
	Braidwood Technology Permanently Disabled?	No	**Recommendation is set based on whether Braidwood is supported on platform**
	TLS Permanently Disabled?	No	**No** = Set for all Intel® HM57 platforms
	Intel® Manageability Application Enable/ Disable	Enabled	**Enabled** = Set for all Intel® HM57 platforms
	PAVP 1.5 Enable/Disabled	Enabled	**Enabled** = Set for all Intel® HM57 platforms
	Intel®QST Enable/Disable	This setting has no effect for Intel® HM57	
	Sentry Peak Enable/ Disable	Enabled	**Enabled** = Set for all Intel® HM57 platforms
	Intel Remote Wake Technology Supported Enable/Disable	This setting has no effect for Intel® HM57	

Table 3-31. Flash Image | Configuration | Features Supported (HM55)

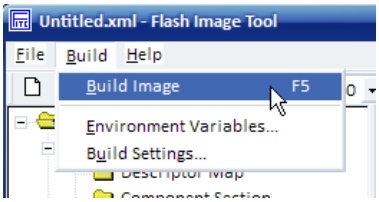
Location	Parameter	CRB Set To	Settings for Any Platform
Follow navigation tree below: • Select the Flash Image • Select **Flash Image | Configuration | Features Supported** • Set the parameters in the **Features Supported** section as shown  	Enable Intel® Standard Manageability; Disable Intel® AMT	This setting has no effect for Intel® HM55	
	Intel® Manageability Application Permanently Disabled?	This setting has no effect for Intel® HM55	
	PAVP 1.5 Permanently Disabled	No	**No** = Set for all Intel® HM55 platforms
	Intel® QST Permanently Disabled?	This setting has no effect for Intel® HM55	
	Sentry Peak Permanently Disabled?	This setting has no effect for Intel® HM55	
	Intel Remote Wake Technology Supported	This setting has no effect for Intel® HM55	
	KVM Permanently Disabled?	This setting has no effect for Intel® HM55	
	Braidwood Technology Permanently Disabled?	This setting has no effect for Intel® HM55	
	TLS Permanently Disabled?	This setting has no effect for Intel® HM55	
	Intel® Manageability Application Enable/ Disable	This setting has no effect for Intel® HM55	
	PAVP 1.5 Enable/Disabled	Enabled	**Enabled** = Set for all Intel® HM55 platforms
	Intel®QST Enable/Disable	This setting has no effect for Intel® HM55	
	Sentry Peak Enable/ Disable	This setting has no effect for Intel® HM55	
	Intel Remote Wake Technology Supported Enable/Disable	This setting has no effect for Intel® HM55	

3.8 Build SPI Flash Binary Image

3.8.1 Build SPI Flash Binary Image

In the main menu select **Build | Build Image**. The image will be saved in the directory specified by **$DestDir** parameter and will be named **outimage.bin**, unless the default **Output Directory** in **Build | Build Settings** was changed (see Section 3.2, page 37).

Figure 3-5. Build | Build Image



3.8.2 Save Your Settings

In the main menu select **File | Save As...**. Select a name and location for the XML file that contains all the settings configured thus far. It is recommended that you save this file in your **[root]** directory for easy access.

Assuming that the custom settings file was saved as **my_settings.xml** to the FIT directory (**[root)]\Tools\System Tools\Flash Image Tool**), then these settings could be loaded in the FIT GUI itself using the main menu option **File | Load...**.

This custom settings file could also be used to generate an SPI flash binary image using the commandline, with a command of the form:

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

where:

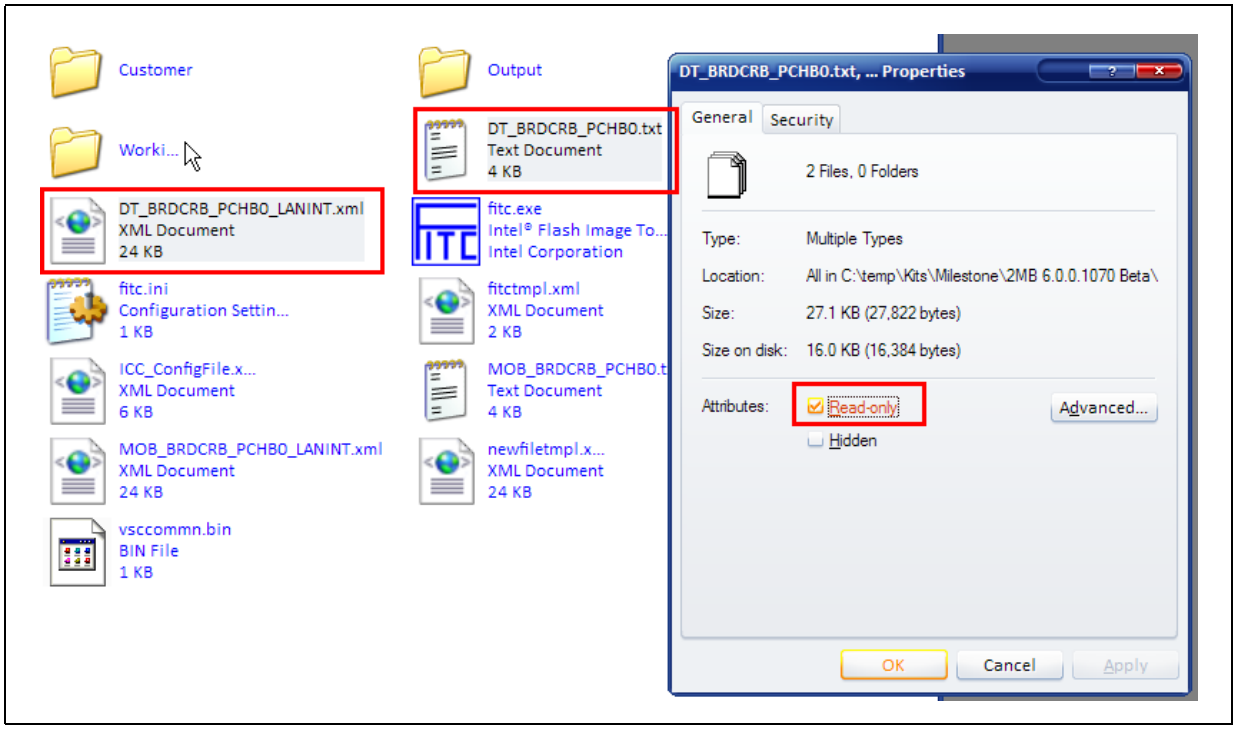
- **<xml_file>** — The XML configuration file saved when configuring using the flash image tool.
- **/o <file>** — The path and filename where the image will be saved. This command overrides the 'Output path' in the XML file.
- **/b** — Automatically builds the flash image. The FIT GUI will not be displayed when this flag is set, since FIT will run in auto-build mode. Error messages will be displayed by FIT, if necessary.

3.8.3 Protect Saved Configuration Files

To avoid custom-configured values from ever overwritten when loading new binaries files (ie: when loading binaries into BIOS, GbE and ME regions in FITC) do the following (see Figure 3-6, page 63):

- After building the SPI Flash binary image and saving your configuration, close Flash Image Tool
- Right-click on the saved FITC configuration XML and ConfigParams TXT files and select **Properties**
- Check the **Read-Only** checkbox and click **OK**

Figure 3-6. Protecting FITC Configuration XML and ConfigParams TXT Files



§

4 Burn the SPI Flash Binary Image

Now that the SPI Flash binary image file has been created, it can be programmed into the SPI flash device of the target machine. Either a flash programmer/burner or Flash Programming Tool can be used.

4.1 Flash Burner/Programmer

The specific use of a flash burner/programmer is beyond the scope of this document. However, the following general steps may be followed:

1. Navigate to your **Output Directory** (as specified in Section 2.3, page 19 or Section 3.8, page 61) where your generated SPI flash binary images are saved. It is assumed that this image file is named **outimage.bin**.

   If two total SPI flash devices were specified during the build process, then additional image files will be saved, one for each SPI flash device. These files are assumed to be named **outimage(1).bin** and **outimage(2).bin**.
2. Utilize a flash burner/programmer to program the image or images. For multiple SPI flash devices, the images are numbered sequentially to correspond to the first and second SPI flash device accordingly.

4.2 Flash Programming Tool (DOS Version)

Flash Programming Tool (FPT) can be used to substitute for a flash burner/programmer, provided the system is capable of booting to an Operating System (OS).

The DOS version of FPT is supported on the following operating systems: DOS, Free DOS, and DRMK DOS.

1. Check DOS FPT directory contents. Using Explorer*, navigate to (root)\Tools\System Tools\Flash Programming Tool\DOS. Ensure that FPT DOS' directory contents are intact (see Section 1.2, page 11).
2. Copy the contents of DOS FPT directory to the root directory of a bootable USB drive.
3. Navigate to your **Output Directory** (as specified in Section 2.3, page 19 or Section 3.8, page 61) where your generated SPI flash binary images are saved. It is assumed that this image file is named **outimage.bin**. Copy this file to the root directory of the same USB drive.
4. Inventory the SPI flash devices on the target system. Boot the target system, change directory to the root directory of the bootable USB drive, and at the DOS prompt type:

```
fpt.exe /i
```

5. The system should respond with the number of SPI flash devices available. For example:

```
--- Flash Devices Found ---
SST25VF016B ID: 0x00BF41 Size: 2048KB (16384Kb)
SST25VF016B ID: 0x00BF41 Size: 2048KB (16384Kb)
```

Note: If the SPI flash device does not currently contain a descriptor it may report only a single device.

6. Program the SPI flash binary image. Change directory to the root directory of the bootable USB drive, and at the DOS prompt type:

```
fpt.exe /f outimage.bin
```

4.2.1 Flash Programming Tool (Windows* Version)

Flash Programming Tool (FPT) can be used to substitute for a flash burner/programmer, provided the system is capable of booting to an Operating System (OS).

The Windows* version of FPT is supported on the following operating systems: Windows XP, Windows PE, Windows Vista, and Windows 7.

1. Check Windows* FPT directory contents. Using Explorer*, navigate to (root)\Tools\System Tools\Flash Programming Tool\Windows. Ensure that FPT Windows*' directory contents are intact (see Section 1.2, page 11).
2. Copy the contents of Windows* FPT directory to the root directory of a standard USB drive.
3. Navigate to your **Output Directory** (as specified in Section 2.3, page 19 or Section 3.8, page 61) where your generated SPI flash binary images are saved. It is assumed that this image file is named **outimage.bin**. Copy this file to the root directory of the same USB drive.
4. 9.Inventory the SPI flash devices on the target system. Boot the target system to Windows*, change directory (using Command Prompt) to the root directory of the bootable USB drive, and at the command line prompt type:

```
fpt.exe /i
```

5. The system should respond with the number of SPI flash devices available. For example:

```
--- Flash Devices Found ---
SST25VF016B ID: 0x00BF41 Size: 2048KB (16384Kb)
SST25VF016B ID: 0x00BF41 Size: 2048KB (16384Kb)
```

Note: If the SPI flash device does not currently contain a descriptor it may report only a single device.

6. Program the SPI flash binary image. Change directory (using Command Prompt) to the root directory of the bootable USB drive, and at the command line prompt type:

```
fpt.exe /f outimage.bin
```

§

5 Intel® ME Firmware Feature Bring Up

5.1 Manufacturing Mode (GPIO33)

When GPIO33 is driven low (through a 1-kΩ resistor) during PCH PWROK transition from low to high, then hardware-based SPI Flash protection (Flash Region Access Permissions, or FRAPs) is disabled. This allows any agent (processor, Intel® ME, or GbE) to read or write to any SPI Flash Region (Descriptor, ME, GbE, or BIOS). GPIO33 is guaranteed to override FRAPs, but it may not override other types of protections, specifically:

- BIOS-based Flash Protection Ranges. These permissions can only be overridden if FLOCKDN is not set (1b) by BIOS:
  - In OS use an application that can read or write to platform and memory registers.
  - Check PCI Config Space, Bus 0, Device 1Fh, Function 0, Offset F0h. This address is called RCBA.
  - Read the dword and zero-out the least significant byte (XXXX XX00)
  - Check Physical Memory, location RCBA + 3878h. Clear bits 31 and 15 of this dword.
  - Do the same for RCBA + 3874h, 387Ch, 3884h, 3880h
- SPI Flash device write-only protection mechanisms. Check the SPI Flash datasheet for details on overriding this hardware-based protection mechanism.

The use of GPIO33 is intended to be used in the debug or manufacturing environment, as a means to reflash part or all of the SPI Flash. GPIO33 is not a FW update mechanism, and reflashing the SPI does not preserve any data in the ME Region. Also note:

- For Intel® ME 4MB FW and Intel® ME 8MB FW (Consumer), ME is halted with GPIO33 assert until a cold reset or Global Reset is issued. This is done to ensure zero ME writes to SPI Flash during a reflash operation.
- For For Intel® ME 8MB FW (Corporate), ME is also halted as described but only recovers:
  - With a Global Reset (if Power Package 3 M0-M3 support is enabled)
  - With a cold reset or Global Reset if Power Package 1 M0-only support is enabled

Figure 5-1. Desktop CRB Manufacturing Mode Jumper Location

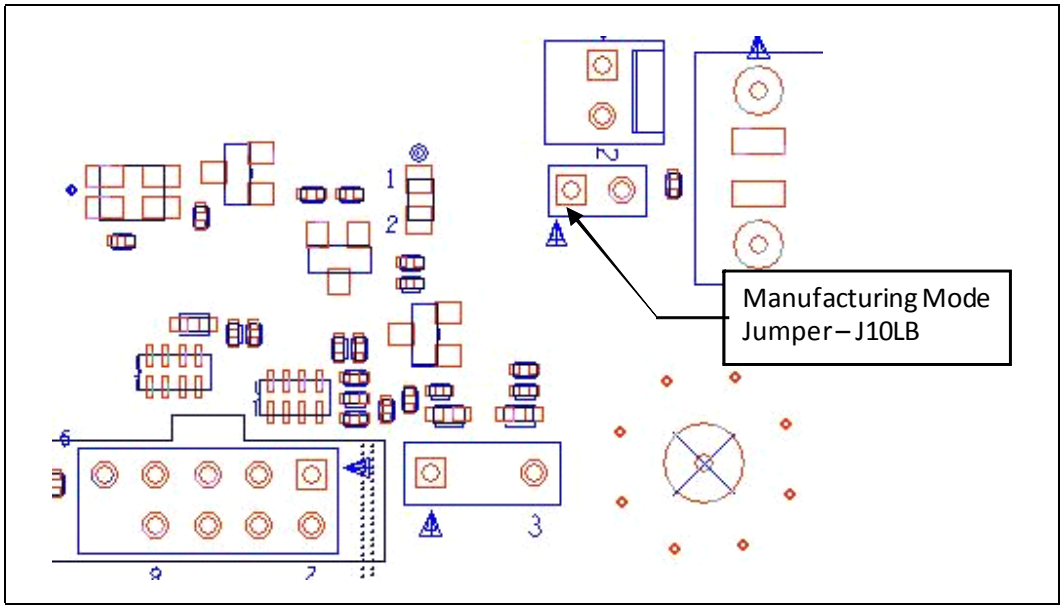
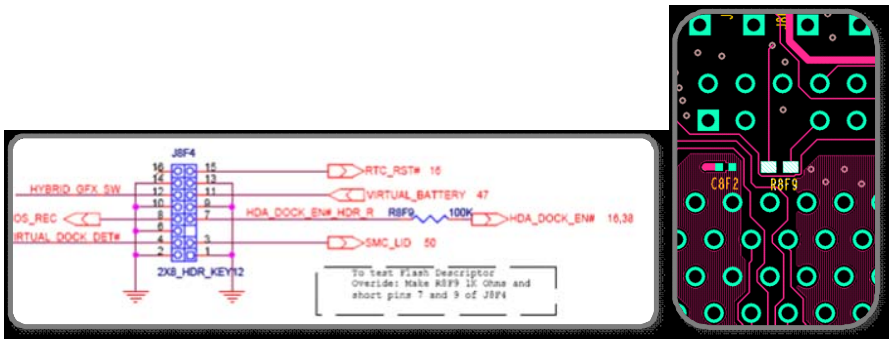


Figure 5-2. Mobile CRB Manufacturing Mode Jumper Location

For proper operation of GPIO33 as Manufacturing Mode, rework is required for Redforts PBA#E32053-211/212/203/204, PBA#E32054-201/202, and PBA#E32053-301.

- PCH HDA_DOCK_EN# has ~10 kΩ internal pull-up
- 100k external pull-down is too weak will not work
- Change R8F9 to 1 kΩ ((RESD,0603,5%,1K)
- Short the pin 7 & 9 of J8F4 with jumper pins

Figure 5-3. Flash Descriptor Security Override (GPIO33) Rework for Redfort



5.2 Intel Wired LAN Settings and Driver

The 82577(Hanksville-M)/8578(Hanksville-D) NVM, Windows drivers, tools (EEUPDATE, Lanconf, CELO) and Intel Boot Agent utilities are available in the following locations:

- 82577 (Hanksville-M)
  - CDI: http://www.intel.com/cd/edesign/library/asmo-na/eng/402854.htm
  - Document ID:-402854
  - Title:-Intel® 82577 Gigabit Ethernet PHY - (Hanksville-M -Beta1 Update SVK) Silicon Sample Kit - 27-Feb-2009
  - Abstract:-LAN Access Division (LAD) - Update to Beta1 kit that has updated NVM versions for use with Ibex Peak B0 and 82577 A2, ES2 samples. Has an updated version of Intel Boot Agent. Version V1.0C0073 TIC 180648,
  - VIP: 16954 - Intel® 82577 Gigabit Ethernet Controller (Hanksville-M SVK) - Beta1 Update - TIC 180648
- 82578 (Hanksville-D)
  - CDI: http://www.intel.com/cd/edesign/library/asmo-na/eng/402853.htm
  - Document ID:-402853
  - Title:-Intel® 82578 Gigabit Ethernet PHY - (Hanksville-D Beta1 Update SVK) Silicon Sample Kit - 27-Feb-2009
  - Abstract:-LAN Access Division (LAD) - Update to Beta1 kit that has updated NVM versions for use with Ibex Peak B0 and 82578 C0, ES2 samples. Contains an updated version of Intel Boot Agent. Version V1.0C0073 TIC 180643.
  - VIP: 16955 - Intel® 82578 Gigabit Ethernet Controller (Hanksville-D SVK) - Beta1 Update - TIC 180643

5.3 Thermal Reporting

This section is only applicable if Thermal Reporting is to be configured on the target platform. If not, skip this section. Thermal Reporting is required for all mobile platforms. To enable Thermal Reporting on the desktop and mobile CRBs follow the diagrams below.

Note: Northbridge related settings are not available for Lynnfield or Clarksfield processors.

Figure 5-4. MPG BIOS: Enable TR (Step 1 of 3)

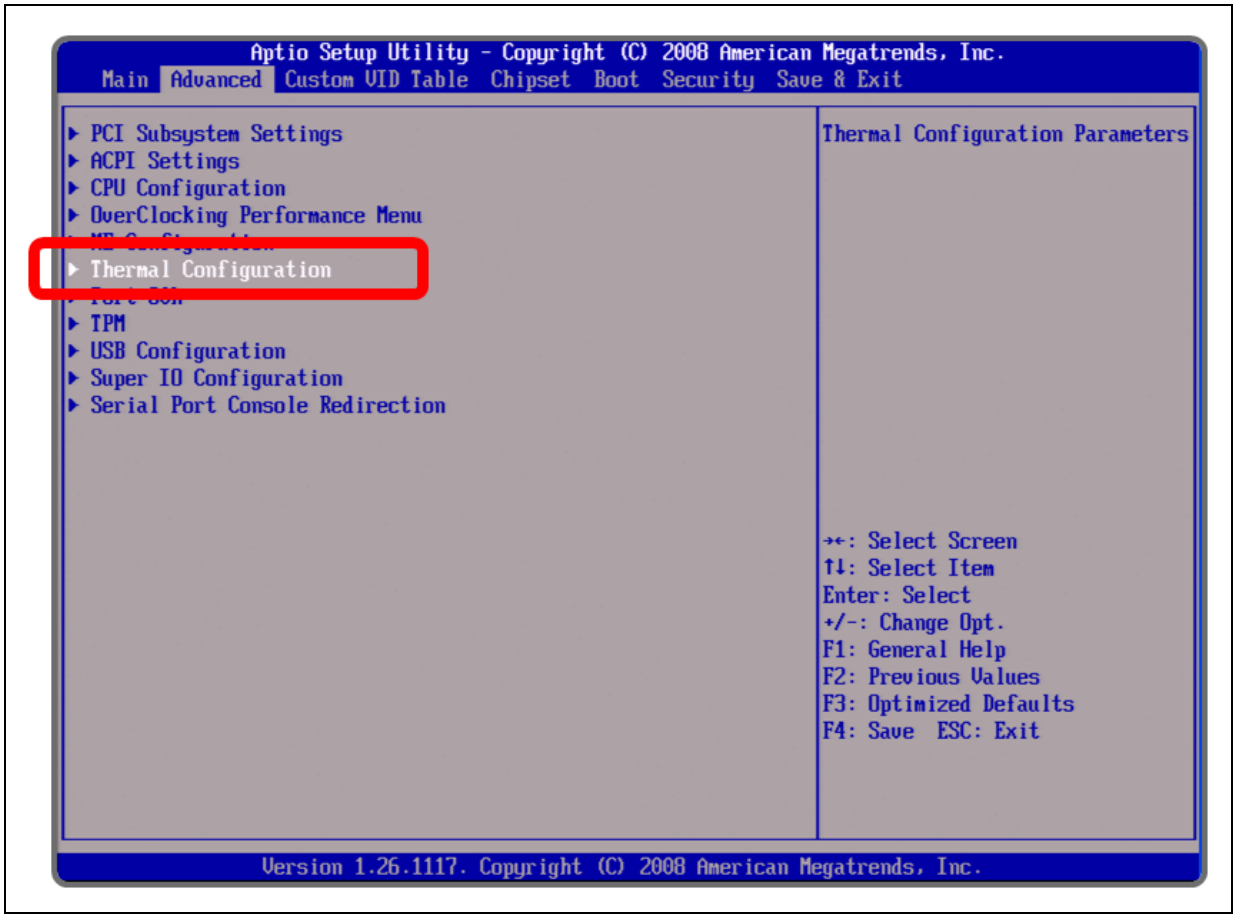


Figure 5-5. MPG BIOS: Enable TR (Step 2 of 3)

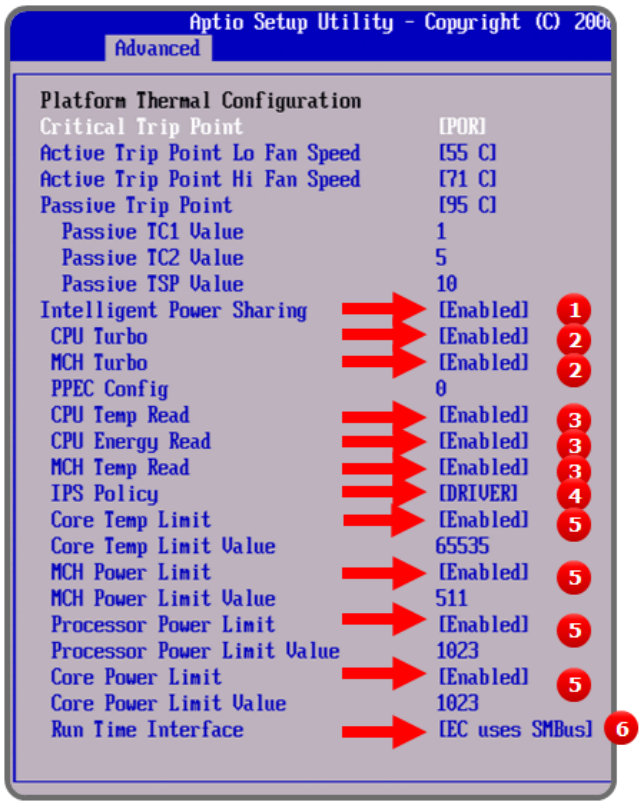


Figure 5-6. MPG BIOS: Enable TR (Step 3 of 3)

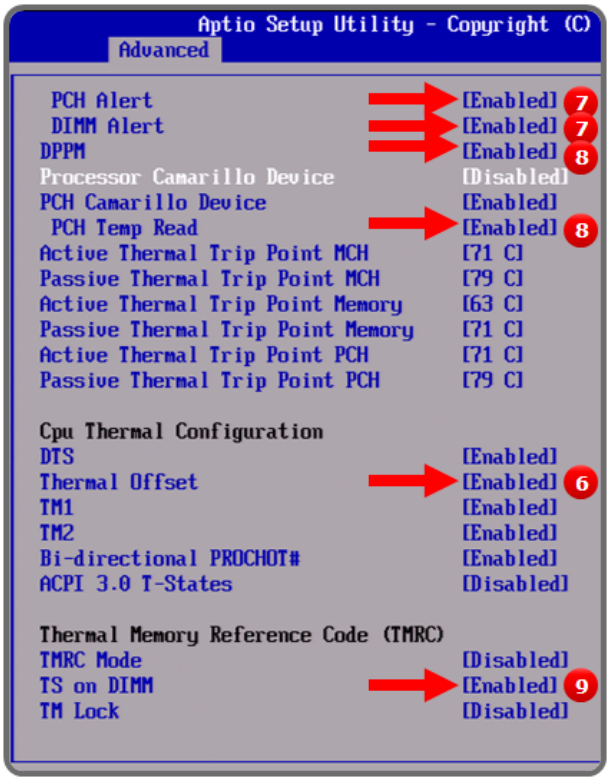


Table 5-1. Thermal Reporting Options in MPG BIOS

Step	Action
1	Enables B0:D31:F6 PCI Thermal Sensor Device
2	Enabled by default with IPS
3	Enabled by default with IPS. Sets TRC register bits 7, 6, and 4
4	Enabled by default with IPS
5	Enables Temp Limits for EC access. Does not work without step #6
6	Enables interaction with EC over SMBus (also requires Thermal Offset enabled)
7	Enables Thermal Alerting (AE registers)
8	Enable DPPM to get access to PCH Temp Read Enable. Sets TRC register bit 5
9	Enables DIMM Temp Read. Sets TRC register bits 3:0

Figure 5-7. CCG BIOS: Enable TR (Step 1 of 2)

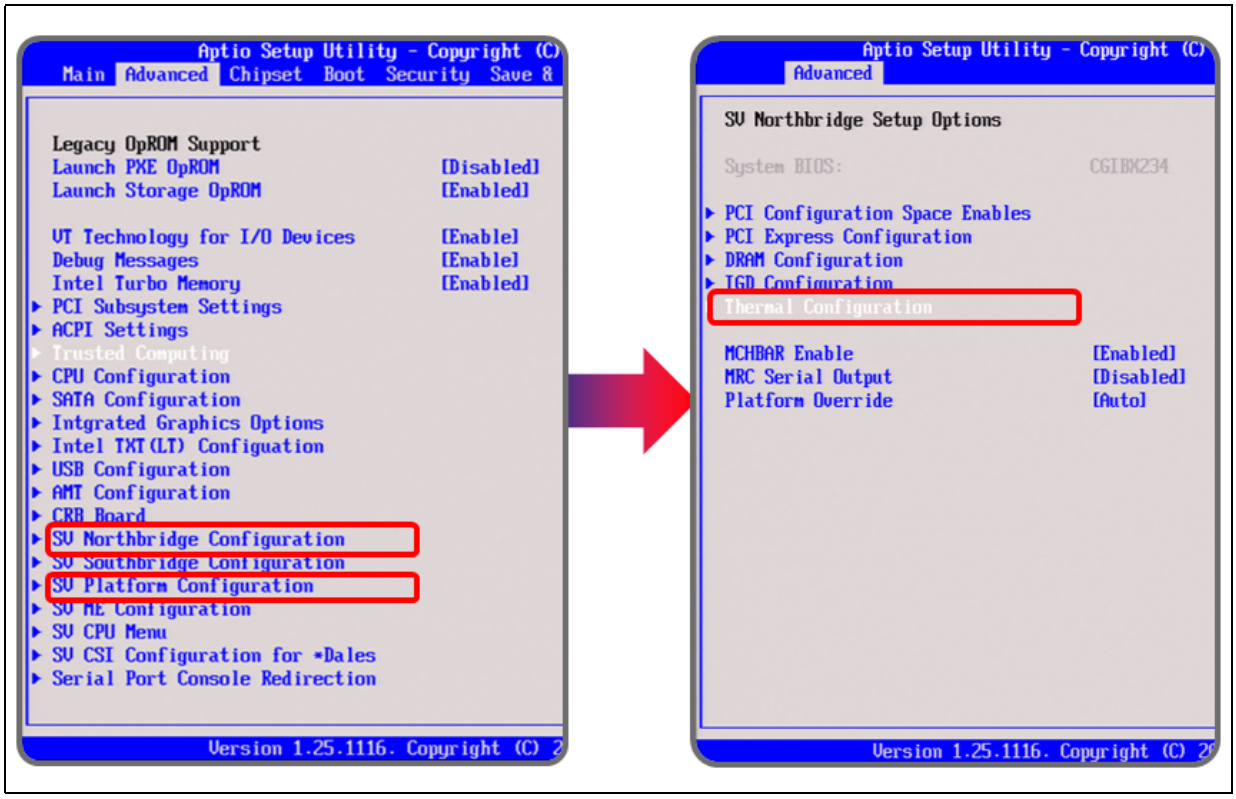
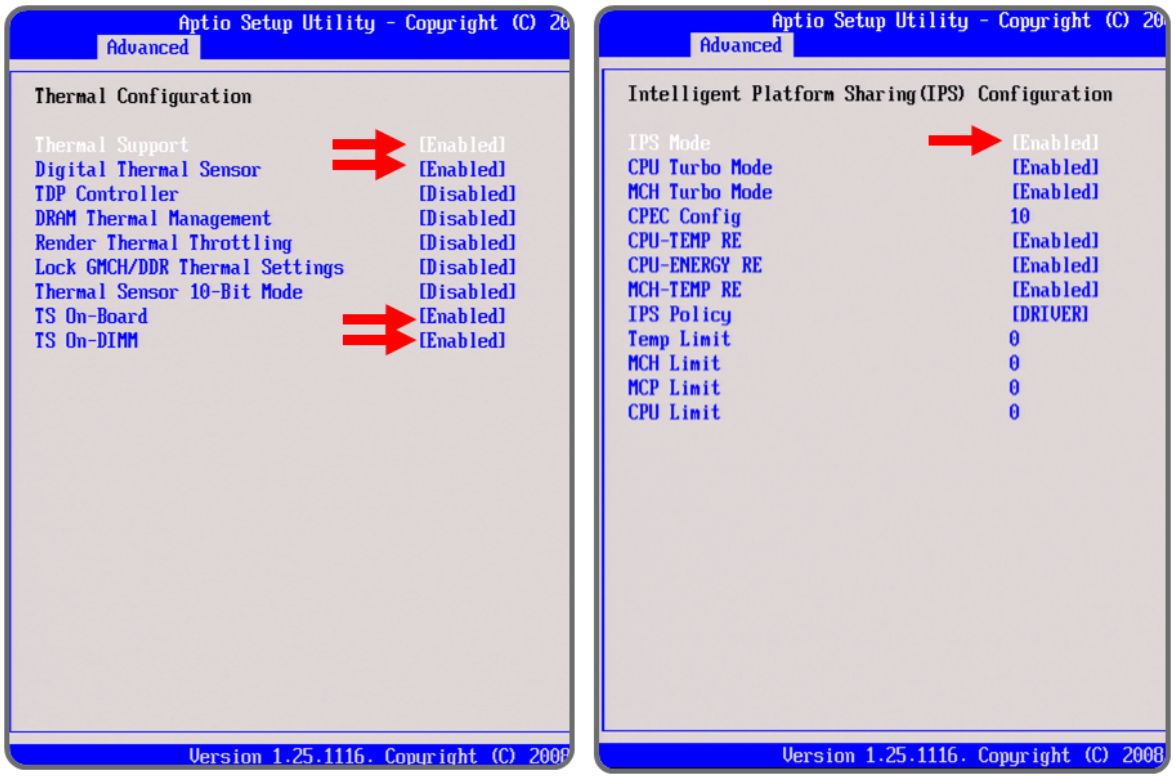


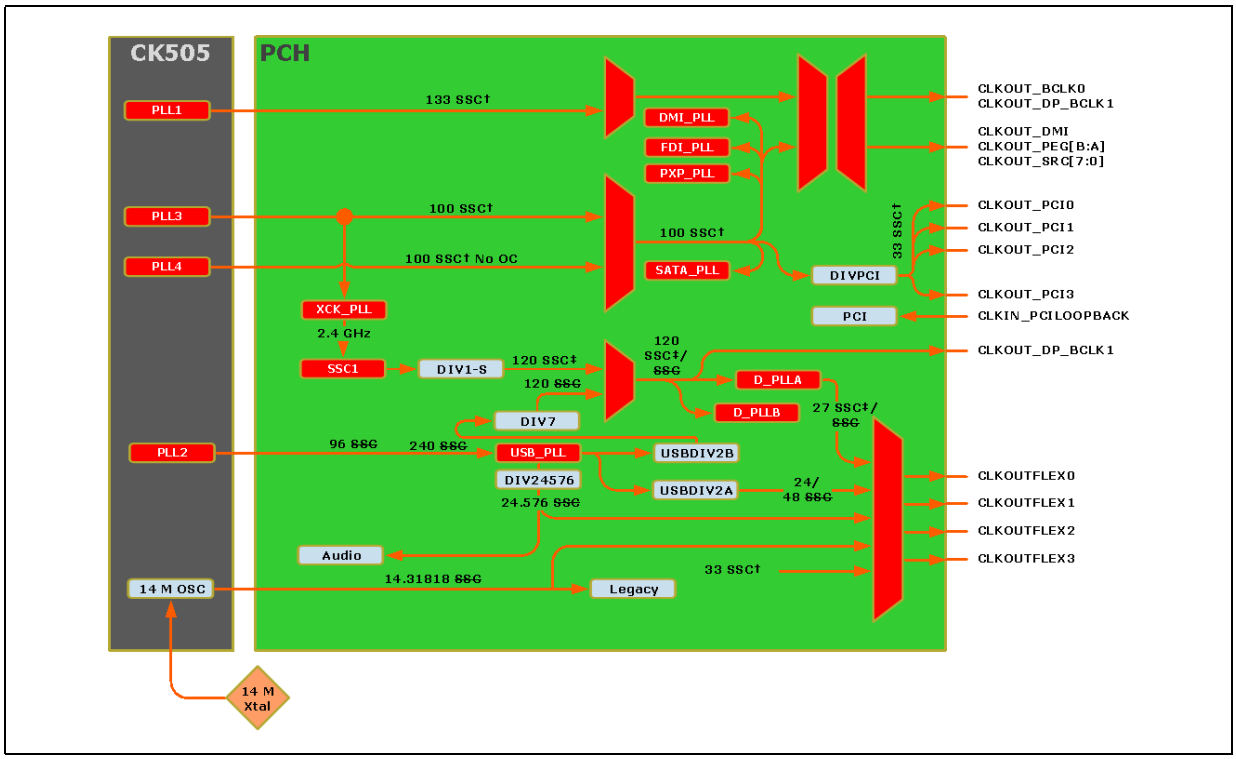
Figure 5-8. CCG BIOS: Enable TR (Step 2 of 2)



A Appendix — Ibex Peak Clock Configuration

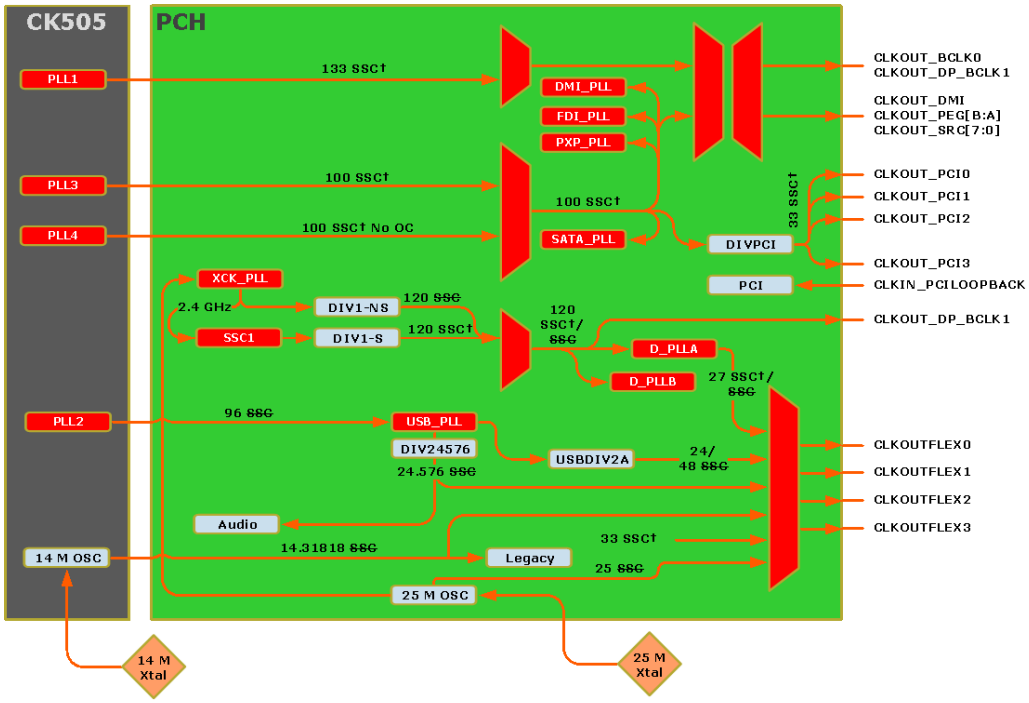
This chapter covers only the basic information needed for clock control parameter programming. For a more detailed treatment of PCH clocks, see *Ibex Peak Platform Clocks and Intel® Management Engine — Platform Compliancy Guide.*

Figure A-1. Ibex Peak Buffer Through Mode Architecture



Note: Only 14.31818 MHz and 48 MHz outputs from CLKOUTFLEX[3:0] are guaranteed. All other output frequencies are available in PCH hardware, but not extensively tested or recommended for use.

Figure A-2. Ibex Peak Display Clock Integration Architecture



A.1 Functional Blocks

There is 1 spread modulator in the Ibexpeak, labeled as follows:

Table A-1. SSC Blocks

Modulator	Description
SSC1	Generates single phase 2.4-GHz output with spread for 120-MHz clock with spread generation by DIV1-S. Uses 2.4-GHz output of XCK PLL. Supplies CLKOUT_DP.

There are various clock dividers in the Ibexpeak, labeled as follows:

Table A-2. Clock Dividers

Modulator	Description
DIV1-S	Generates 120-MHz clock with spread. Uses output of SSC1. Can be no spread if SSC1 is disabled. Supplies CLKOUT_DP.
DIV7	Generates 120-MHz clock with no spread. Uses output of USBDIV2B. Supplies CLKOUT_DP.
USBDIV1	Generates 96-MHz clock with no spread. Uses output of DIV5A. Supplies USB PLL.
USBDIV2A	Generates 24-MHz clock with no spread. Uses 96-MHz output of DIV5B or USBDIV1 (not shown). Supplies CLKOUTFLEX3.
USBDIV2B	Generates 240-MHz clock with no spread. Uses USB PLL's 1.92 GHz clock output. Supplies DIV7.
DIVPCI	Generates 33-MHz clock with spread. Uses output of either DIV2-S, DIV2-NS, or DIV4. Can be no spread if DIV2-NS is used or SSC4 is disabled. Supplies CLKOUT_PCI[4:0] and CLKOUTFLEX[3:0].

A.2 ME FW Clock Control Parameters

The following parameters can be specified for ME FW programming. For more details on how to configure an SPI flash image with these clock control parameters see the Bring Up Process chapter in the *Firmware Bring Up Guide* included in the ME FW kit.

Note: Clock control parameter specifications may be different between Buffer Through Mode, Display Clock Integration. The specification for each mode is listed separately. For those parameters that are mode-agnostic, only a single specification is given.

A.2.1 FCSS – Flex Clock Source Select

BTM/DCI Default: 0000 0304h
ME FW Default: No changes from BTM/DCI defaults
Flash Image Tool and Config Wizard Default: 0000 0344h
Recommended Defaults:

- **Desktop CRB:** 0000 4444h
- **Mobile CRB DCI with Ext/Intg/Mixed Graphics:** 0000 4422h
- **Mobile CRB External Graphics Only or BTM with Ext/Intg Graphics:** 0000 4322h

Description: This parameter controls muxing to select sources for Flex Clock outputs
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-3. Flex Clock Source Select Parameters

Bits	Default	Description
31:15	0h	**Reserved (RSVD)**
14:12	000b	**FLEXCLK3 Source Select (F3SS):** Selects the source of clock to be driven out on CLKOUTFLEX3. **000b** = 48 MHz **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.
11:11	0h	Reserved (RSVD)
10:8	011b	**FLEXCLK2 Source Select (F2SS):** Selects the source of clock to be driven out on CLKOUTFLEX2. **DCI/BTM** **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.
7:7	0h	**Reserved (RSVD)**

Table A-3. Flex Clock Source Select Parameters

Bits	Default	Description
6:4	000b	**FLEXCLK1 Source Select (F1SS):** Selects the source of clock to be driven out on CLKOUTFLEX1. **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.
3:3	0h	**Reserved (RSVD)**
2:0	100b	**FLEXCLK0 Source Select (F0SS):** Selects the source of clock to be driven out on CLKOUTFLEX0. **000b** = Reserved **001b** = Reserved **010b** = 33.3 MHz **011b** = 14.31818 MHz **100b** = Disabled (DC logic '0') **101b** = Disabled (DC logic '0') **110b** = Disabled (DC logic '0') **111b** = Reserved ***Note:*** These clock select settings only take effect when this muxed FLEXCLK/GPIO pin is configured for FLEXCLK native usage. Refer to the *Ibex Peak EDS* for configuration of GPIO vs. native usage.

A.2.2 PLLEN* – PLL Enable

BTM/DCI Default: 00000404h (before PCH_PWROK), 8000040Ch (after PCH_PWROK)
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults
Recommended Defaults:

- **DCI with Ext/Intg/Mixed Graphics:** 8000 040Ch
- **External Graphics Only:** 8000 041Bh
- **BTM with Ext/Intg Graphics:** 8000 041Ch

Description: This parameter controls PLL enables.
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-4. PLL Enable Parameters

Bits	Default	Description
31	1b	**Chipset Configuration (PCHCFG):** Must be set to **1b**.
30:11	0h	**Reserved (RSVD)**
10	1b	**Chipset Configuration (PCHCFG):** Must be set to **1b**.
9	0b	**DPLLA/DPLLB/SSC1 Ownership (DPLLSSC1OWN):** Controls the owner of DPLLA, DPLLB, and SSC1. **0b** = Display Driver register set controls DPLLA, DPLLB, and SSC1 **1b** = ME FW controls DPLLA, DPLLB, and SSC1. Note that ME FW only provides a subset of controls, to enable/disable the DPLLs and configure it for 27MHz spread or non-spread

Table A-4. PLL Enable Parameters

Bits	Default	Description
8	0b	**DP120/BCLK1 Output Buffer Ownership (DPBCLK1OBOWN):** Controls the owner of CLKOUT_DP_BCLK1 output buffer. **0b** = Display Driver register controls CLKOUT_DP_BCLK1 output buffer. In this case, this output pin usage is to provide reference clock to the DPLL associated with the CPU embedded display. **1b** = ME FW controls CLKOUT_DP_BCLK1 output buffer. In this case, this output usage is to provide BCLK reference clock to the CPU. The default is display owned. ***Note:*** Specifically this field determines whether the display side control logic owns the gating/un-gating of the output clock source to the CLKOUT_DP_BCLK1 output pin, or whether the clock module side owns this gating / un-gating. This field does not have any effect at the output buffer tri-state/ driven control.
7:5	0h	**Reserved (RSVD)**
4	0b	**Crystal Oscillator Disable (OSCDIS):** Disables the crystal oscillator when it is not used as a reference clock source to the XCK PLL. **0b** = Enable oscillator **1b** = Disable oscillator to save power ***Note:*** The crystal oscillator should be disabled when integrated graphics (or any other consumer of 120 MHz clock internal and external to Ibex Peak) is not utilized. The output frequency for PCH pin CLKOUT_DP_BCLK1 is controlled by parameter field "DP120/BCLK1 Clock Source Select" at CSS[9:8].
3	Strap (FITC/FICW assumes this value to be 1b)	**XCK VRM Bypass (XCKVRMBYP):** This read-only field reports the state of the VRM bypass hardstrap pin GPIO[27]/MGPIO[6]. Software reads this field to determine whether the VRM powers the XCKPLL circuitries. ME FW writes to "XCK VRM Disable" parameter field at 1230Ch[1] to disable power consuming circuitries in the VRM when it is not used. **0b** = Board powers XCK PLL circuitry **1b** = Integrated VRM powers XCK PLL circuitry ***Note:*** The true value of the hard strap, which resides in the suspend power well, is not reflected in this core well register field until Ibex Peak has received its PCH_PWROK indication. Software read of this register field prior to PCH_PWROK assertion will return zero because of power well crossing isolation.
2	1b	**XCK Voltage Divider Enable (XCKVDIVEN):** Enables the shared voltage divider associated with biasing current generation for the crystal oscillator and the PI blocks. The voltage divider should be disabled to save power when the crystal oscillator and none of the PI blocks are used. **0b** = Disable the voltage divider to save power **1b** = Enable the voltage divider ***Note:*** The XCK voltage divider should be disabled when integrated graphics (or any other consumer of 120 MHz clock internal and external to Ibex Peak) is not utilized. The output frequency for PCH pin CLKOUT_DP_BCLK1 is controlled by parameter field "DP120/BCLK1 Clock Source Select" at CSS[9:8].
1	0b	**XCK VRM Disable (XCKVRMDIS):** Disables the integrated VRM when it is not used to power XCK PLL circuitry. 0b = Enable VRM 1b = Disable VRM to save power ***Note:*** The XCK VRM should be disabled when integrated graphics (or any other consumer of 120 MHz clock internal and external to Ibex Peak) is not utilized. The output frequency for PCH pin CLKOUT_DP_BCLK1 is controlled by parameter field "DP120/BCLK1 Clock Source Select" at CSS[9:8].
0	0b	**XCK_PLL Disable (XCKDIS):** Disables the XCK PLL. **0b** = Enable XCK PLL **1b** = Disable XCK PLL ***Note:*** The XCK PLL should be disabled when integrated graphics (or any other consumer of 120 MHz clock internal and external to Ibex Peak) is not utilized. The output frequency for PCH pin CLKOUT_DP_BCLK1 is controlled by parameter field "DP120/BCLK1 Clock Source Select" at CSS[9:8].

A.2.3 OCKEN – Output Clock Enable

BTM/DCI Default: 1FFF 0F8Fh
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter controls enabling of output buffers

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-5. Output Clock Enable Parameters

Bits	Default	Description
31:29	0h	**Reserved (RSVD)**
28	1b	**DMI Output Clock Enable (DMIOCKEN):** Controls the enabling of DMI clock toggling. When this clock output is not used, it should be gated to low state to save power. **0b** = Output clock is gated to low state **1b** = Output buffer is enabled to toggle once its clock source has been initialized
27	1b	**PEG_B Output Clock Enable (PBOCKEN):** Controls the enabling of PEG_B clock toggling. When this clock output is not used, it should be gated to low state to save power. **0b** = Output clock is gated to low state **1b** = Output buffer is enabled to toggle once its clock source has been initialized
26	1b	**PEG_A Output Clock Enable (PAOCKEN):** Controls the enabling of PEG_A clock toggling. When this clock output is not used, it should be gated to low state to save power. **0b** = Output clock is gated to low state **1b** = Output buffer is enabled to toggle once its clock source has been initialized
25	1b	**DP120/BCLK1 Output Clock Enable (DPBCLK1OCKEN):** Controls the enabling of CLKOUT_DP_BCLK1 clock toggling. When this clock output is not used, it should be gated to low state to save power. **0b** = Output clock is gated to low state **1b** = Output buffer is enabled to toggle once its clock source has been initialized ***Note:*** Note that in order for this parameter field to take effect, the ownership of the muxed output clock pin CLKOUT_DP_BCLK1 must be configured to be clock-module-owned, via "BCLK/DP120 Output Buffer Ownership" parameter field at PLLEN[8]. When the ownership is under display control, the display logic side (not ME FW) determines whether the output clock pin CLKOUT_DP_BCLK1 toggles or gated to low state.
24	1b	**BCLK0 Output Clock Enable (BCLK0OCKEN):** Controls the enabling of CLKOUT_BCLK0 clock toggling. When this clock output is not used, it should be gated to low state to save power. **0b** = Output clock is gated to low state **1b** = Output clock is enabled to toggle once its clock source has been initialized
23:16	FFh	**SRC 7:0 Output Clock Enable (SRC70OCKEN):** Controls the enabling of SRC clock toggling. Each bit position controls the corresponding SRC output clock, e.g. bit 0 controls SRC0. When any clock output is not used, it should be gated to low state to save power. **0b** = Corresponding output clock is gated to low state **1b** = Corresponding output clock is enabled to toggle once its clock source has been initialized (hot plug capable)
15:12	0h	**Reserved (RSVD)**

Table A-5. Output Clock Enable Parameters

Bits	Default	Description
11:7	1Fh	**PCICLK 4:0 Output Clock Enable (PCI40OCKEN):** Controls the enabling of PCI clock toggling. Each bit position controls the corresponding PCI output clock, e.g. bit 7 controls CLKOUT_PCI0. When any clock output is not used, it should be gated to low state to save power. **0b** = Corresponding output clock is gated to low state **1b** = Corresponding output clock is enabled to toggle once its clock source has been initialized ***A-stepping Note:*** This parameter has no effect and clock output is always enabled. ***B-stepping Note:*** Parameter behaves normally.
6:4	0h	**Reserved (RSVD)**
3:0	Fh	***A-stepping Implementation:*** **FLEXCLK 3:0 Output Buffer Enable (F30OBEN):** Controls the enabling of CLKOUTFLEX[3:0] output buffers. Each bit position controls the corresponding FLEXCLK output buffer, e.g. LSB (bit 0) controls CLKOUTFLEX0. **0b** = Corresponding output clock is tri-stated (not driven) **1b** = Corresponding output clock is driven ***Note:*** Actual driven logic state is a function of clock module state (such as during initialization, normal operation, dynamic clock management if supported, and preparation for system powering down). These bits also control the weak pull down of the FLEX input pad. Each bit position controls the corresponding FLEX weak pull down, e.g. LSB (bit 0) controls FLEX0. When the FLEX output buffer is tristated, the corresponding internal weak pull down should be enabled to avoid reliability issue due to floating input pad. ***B-stepping Implementation:*** **FLEXCLK 3:0 Output Clock Enable (PCI40OCKEN):** Controls the enabling of FLEXCLK toggling. Each bit position controls the corresponding FLEXCLK output clock, e.g. LSB (bit 0) controls CLKOUTFLEX0. When any clock output is not used, it should be gated to low state to save power. **0b** = Corresponding output clock is gated to low state **1b** = Corresponding output clock is enabled to toggle once its clock source has been initialized ***General Note Not Stepping Dependent:*** CLKOUTFLEX[3:0] is muxed with GPIOs. Clock module logic should only enable the weak pull down when the muxed pin is configured for FLEXCLK usage (not DC logic '0') and FLEXCLK is tri-stated. FLEXCLK values can be set in the "Flex Clock Source Select" parameter at FCSS[31:0].

A.2.4 OBEN – Output Buffer Enable

BTM/DCI Default: 0F1F F1FFh
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter has been deprecated. All functionality previously specified for this parameter is now available in OCKEN parameter.
Flash Image Tool Configuration: Not present in Flash Image Tool

A.2.5 IBEN – Input Buffer Enable

BTM/DCI Default: 0000 0000h
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter controls enabling of input buffers
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-6. Input Buffer Enable Parameters

Bits	Default	Description
31:2	0h	**Reserved (RSVD)**
1	0b	**CLKIN_DOT96 Input Buffer Disable (CKIN96InBufDis):** Controls the differential input buffer for CLKIN_DOT96. When CLKIN_DOT96 is not used, its input buffer should be turned off for power saving. **0b** = Input buffer is enabled **1b** = Input buffer is disabled for power saving ***A-stepping Note:*** This parameter has no effect and the CLKIN_DOT96 input is always enabled. ***B-stepping Note:*** Parameter behaves normally.
0	0b	**BCLK Input Clock Buffer Disable (BCLKInClkBufDis)**: Controls the differential input buffer for CLKIN_BCLK. **0b** = Input buffer is enabled **1b** = Input buffer is disabled for power saving. A weak pulldown ensures output nodes are not floating.

A.2.6 DIVEN* – Divider Enable

BTM/DCI Default: 0000 08C3h
ME FW/Flash Image Tool and Config Wizard Default: 0000 0303h
Recommended Defaults:

- **DCI with Ext/Intg/Mixed Graphics:** 0000 0303h
- **External Graphics Only:** 0000 0100h
- BTM with Ext/Intg Graphics: 0000 0003h

Description: This parameter controls enabling of divider blocks.
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-7. Divider Enable Parameters

Bits	Default	Description
31:12	0h	**Reserved (RSVD)**
11	HW: 1b ME FW: 1b FITC: 0b	**24.576Mhz Fractional Divisor Enable (24FDEN):** Enables fractional divisor for 24.576-Mhz clock generation (see Figure A-1, page 75, Figure A-2, page 76,). When not used, the fractional divisor can be disabled for power saving. **0b** = Divider is disabled **1b** = Divider is enabled
10	**0b**	**Reserved (RSVD)**
9	**BTM** 0b **DCI** 1b	**XCK Reference Clock Select (XCKRS):** Selects the source of reference clock for XCK PLL. **0b** = CLKIN_DMI **1b** = 25-Mhz crystal oscillator
10:9	0b	**Reserved (RSVD)**
8	0b	**DIV7 Enable (DIV7EN):** Enables DIV7 clock divider (see Figure A-1, page 75, Figure A-2, page 76,). **0b** = Divider is enabled (120 Mhz generated from USB PLL) **1b** = Divider is disabled (120Mhz generated by XCK PLL)
7:6	HW: 3h ME FW: 3h FITC: 0h	**Chipset Configuration (PCHCFG):**Set to **3h** by hardware default, but recommended to be **0h**.

Table A-7. Divider Enable Parameters

Bits	Default	Description
5:2	0h	**Reserved (RSVD)**
1	1b	**DIV1-S Enable (DIV1SEN):** Enables DIV1-S clock divider (see Figure A-1, page 75, Figure A-2, page 76,). **0b** = Divider is disabled **1b** = Divider is enabled
0	1b	**DIV1-NS Enable (DIV1NSEN):** Enables DIV1-NS clock divider (see Figure A-1, page 75, Figure A-2, page 76,). **0b** = Divider is disabled **1b** = Divider is enabled ***Note:*** In BTM, 120-MHz non-spread will be enabled through USB PLL and DIV7. In PCIM, 120-MHz non-spread will be enabled through XCK PLL and DIV7.

A.2.7 PM1 – Power Management

BTM/DCI Default: 0000 0000h
ME FW Default: No changes from BTM/DCI defaults
Flash Image Tool and Config Wizard Default: 0000 0013h

Description: This parameter controls power management features of clocks
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-8. Power Management Parameters

Bits	Default	Description
31:4	0h	**Reserved (RSVD)**
4	HW: 0b ME FW: 0b FITC: 1b	**Dynamic ~~DIV~~SSC1 Shutdown Enable (~~DIV~~SSC1DSEN):** Enables dynamic power management of DIV1-S (see Figure A-1, page 75, Figure A-2, page 76,). Integrated graphics display may dynamically power manage SSC1 and DIV1-S when it is assigned ownership of SSC1 ("DPLLA/DPLLB/SSC1 Ownership" parameter field at PLLEN[9] is **0b**). This bit has no effect, (no dynamic power management of DIV1-S), when ME has ownership (PLLEN[9] is **1b**). The following are logical combinations of this parameter field (MSB) and "Dynamic DIV1S Shutdown Enable" parameter field at PM1[0] (LSB). **00b** = Disable dynamic management of DIV1-S and SSC1 **01b** = Dynamic management of DIV1-S only. SSC1 stays up and maintains current state for lower clock recovery latency at the expense of power. **10b** = Reserved **11b** = Dynamic management of both DIV1-S and SSC1. Longer clock recovery latency but more power savings. ***A-stepping Note:*** This parameter has no effect and the divider output is always enabled. ***B-stepping Note:*** Parameter behaves normally.
3:2	0h	**Reserved (RSVD)**
1	HW: 0b ME FW: 0b FITC: 1b	**Dynamic DIV1-NS Shutdown Enable (DIV1NSDSEN):** Enables dynamic power management of DIV1-NS (see Figure A-1, page 75, Figure A-2, page 76,). **0b** = Disable dynamic power management of DIV1-S **1b** = Enable dynamic power management of DIV1-S ***A-stepping Note:*** This parameter has no effect and the divider output is always enabled. ***B-stepping Note:*** Parameter behaves normally.
0	HW: 0b ME FW: 0b FITC: 1b	**Dynamic DIV1-S Shutdown Enable (DIV1SDSEN):** Enables dynamic power management of DIV1-S (see Figure A-1, page 75, Figure A-2, page 76,). **Do not configure this parameter field on its own. See "DIV1 Shutdown Enable" parameter field at PM1[4].**

A.2.8 PM2 – Power Management

BTM/DCI Default: 0000 0000h
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter controls power management features of clocks
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-9. Power Management Parameters

Bits	Default	Description
31:9	0h	**Reserved (RSVD)**
8:5	0000b	**CLKRUN Control Enable for PCI 33 Mhz on CLKOUTFLEX (CLKRUNCEN_FLEX):** Enables support for CLKRUN protocol for PCI 33 MHz clocks muxed out to CLKOUTFLEX[3:0]. **0b** = Corresponding CLKOUTFLEX PCI clock is free-running, unaffected by CLKRUN protocol **1b** = Corresponding CLKOUTFLEX PCI clock is shut off when CLKRUN protocol turns off PCI clocks ***Note:*** These bits must be clear (**0b**) when the corresponding CLKOUTFLEX pins are not configured for PCI 33Mhz clock. ***A-stepping Note:*** This parameter has no effect and the outputs are unaffected when CLKRUN protocol turns off PCI clocks. ***B-stepping Note:*** Parameter behaves normally.
4:0	0 0000b	**CLKRUN Control Enable (CLKRUNCEN):** Enables support for CLKRUN protocol for CLKOUT_PCI[4:0]. **0b** = Corresponding CLKOUT_PCI is free-running, unaffected by CLKRUN protocol **1b** = Corresponding CLKOUT_PCI is shut off when CLKRUN protocol turns off PCI clocks ***Note:*** This parameter does not enable CLKRUN protocol support for CLKOUTFLEX[3:0]. ***A-stepping Note:*** This parameter has no effect and the outputs are always disabled when CLKRUN protocol turns off PCI clocks. ***B-stepping Note:*** Parameter behaves normally.

A.2.9 SEBP1 – Single Ended Buffer Parameters

BTM/DCI Default: 0000 9999h
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter controls double/single load series resistance and slew rate for FLEX clocks
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-10. Single Ended Buffer Parameters

Bits	Default	Description
31:16	0h	**Reserved (RSVD)**
15:13	100b	**FLEXCLK3 Slew Rate Control (F3SLC):** Controls slew rate for CLKOUTFLEX3. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
12	1b	**FLEXCLK3 Single/Double Load Series Resistance (F3SDLSR):** Sets programmable series resistance for CLKOUTFLEX3. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage

Table A-10. Single Ended Buffer Parameters

Bits	Default	Description
11:9	100b	**FLEXCLK2 Slew Rate Control (F2SLC):** Controls slew rate for CLKOUTFLEX2. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
8	1b	**FLEXCLK2 Single/Double Load Series Resistance (F2SDLSR):** Sets programmable series resistance for CLKOUTFLEX2. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
7:5	100b	**FLEXCLK1 Slew Rate Control (F1SLC):** Controls slew rate for CLKOUTFLEX1. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
4	1b	**FLEXCLK1 Single/Double Load Series Resistance (F1SDLSR):** Sets programmable series resistance for CLKOUTFLEX1. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
3:1	100b	**FLEXCLK0 Slew Rate Control (F2SLC):** Controls slew rate for CLKOUTFLEX2. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
0	1b	**FLEXCLK0 Single/Double Load Series Resistance (F0SDLSR):** Sets programmable series resistance for CLKOUTFLEX0. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage

A.2.10 SEBP2 – Single Ended Buffer Parameters

BTM/DCI Default: 0009 9999h
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults

Description: This parameter controls double/single load series resistance and slew rate for PCI clocks. PCI Specifications 2.4 and 3.0 allow for an acceptable slew rate range of 1 to 4 V/ns. ME FW programmability allows for slew rate to be specified between 0.6 to 2 V/ns for two reasons:

1. Slew rates exceeding 2 V/ns can have adverse effects on platform EMI
2. Slew rates lower than 1 V/ns can be specified for EMI benefits, at the risk of violating PCI specification

Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-11. Single Ended Buffer Parameters

Bits	Default	Description
31:16	0h	**Reserved (RSVD)**
19:17	100b	**PCI4 Slew Rate Control (PCI4SLC):** Controls slew rate for CLKOUTPCI4. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
16	1b	**PCI4 Single/Double Load Series Resistance (PCI4SDLSR):** Sets programmable series resistance for CLKOUT_PCI4. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
15:13	100b	**PCI3 Slew Rate Control (PCI3SLC):** Controls slew rate for CLKOUT_PCI3. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
12	1b	**PCI3 Single/Double Load Series Resistance (PCI3SDLSR):** Sets programmable series resistance for CLKOUT_PCI3. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
11:9	100b	**PCI2 Slew Rate Control (PCI2SLC):** Controls slew rate for CLKOUT_PCI2. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
8	1b	**PCI2 Single/Double Load Series Resistance (PCI2SDLSR):** Sets programmable series resistance for CLKOUT_PCI2. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
7:5	100b	**PCI1 Slew Rate Control (PCI1SLC):** Controls slew rate for CLKOUT_PCI1. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)

Table A-11. Single Ended Buffer Parameters

Bits	Default	Description
4	1b	**PCI1 Single/Double Load Series Resistance (PCI1SDLSR):** Sets programmable series resistance for CLKOUT_PCI1. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage
3:1	100b	**PCI0 Slew Rate Control (PCI0SLC):** Controls slew rate for CLKOUT_PCI0. **000b** = Weakest slew rate setting (~0.6 V/ns for a TBD inch trace at double load) **001b** **010b** **011b** **100b** = Default Slew rate setting (~1.4V/ns for a TBD inch trace at double load) **101b** **110b** **111b** = Strongest slew rate setting (~2 V/ns for a TBD inch trace at double load)
0	1b	**PCI0 Single/Double Load Series Resistance (PCI0SDLSR):** Sets programmable series resistance for CLKOUT_PCI0. **0b** = 25 Ohms for single load usage **1b** = 17 Ohms for double load usage

A.2.11 SSCCTL* – SSC Control

BTM/DCI Default: Default: 00000000h
ME FW/Flash Image Tool and Config Wizard Default: No changes from BTM/DCI defaults
Recommended Defaults:

- **DCI with Ext/Integrated/Mixed Graphics Default:** 0101 0100h
- **External Graphics Only Default:** 0101 0101h

Description: This parameter controls spread spectrum modulation capability of SSC blocks.
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Dynamic Registers Section

Table A-12. SSC Control Parameters

Bits	Default	Description
31:3	0h	**Chipset Configuration (PCHCFG):** Must be set to **20 20 20h**
2:1	0b	**SSC1 Spread Mode (SSC1_SprdMd):** Select the spread mode for SSC1. **00b** = Down spread **01b** = Center spread **10b** = Reserved **11b** = Reserved
0	0b	**SSC1 Enable, Active Low (SSC1_EnB):** Determines whether SSC1 (see Figure A-1, page 75, Figure A-2, page 76,) is enabled. **0b** = Enable SSC1 **1b** = Power off SSC1 and select bypass path to SSC1 output. SSC1 output will thus be non-spread.

A.2.12 PMSRCCLK1 – SRC Power Management

BTM/DCI Default: 7654 3210h
ME FW/Flash Image Tool and Config Wizard Default: FFFF FFFFh

Description: This parameter as signs dynamic CLKRQ# control of SRC clocks
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-13. SRC Power Management

Bits	Default	Description
31:28	HW: 0111b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC7 (CRQSELSRC7):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC7 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC7 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC7 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC7 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC7 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC7 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC7 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC7 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC7 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC7 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC7 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC7 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC7 output. ***B-stepping Note:*** Parameter behaves normally.
27:24	HW: 0110b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC6 (CRQSELSRC6):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC6 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC6 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC6 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC6 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC6 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC6 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC6 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC6 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC6 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC6 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC6 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC6 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC6 output. ***B-stepping Note:*** Parameter behaves normally.
23:20	HW: 0101b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC5 (CRQSELSRC5):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC5 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC5 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC5 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC5 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC5 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC5 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC5 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC5 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC5 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC5 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC5 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC5 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC5 output. ***B-stepping Note:*** Parameter behaves normally.

Table A-13. SRC Power Management

Bits	Default	Description
19:16	HW: 0100b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC4 (CRQSELSRC4):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC4 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC4 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC4 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC4 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC4 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC4 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC4 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC4 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC4 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC4 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC4 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC4 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC4 output. ***B-stepping Note:*** Parameter behaves normally.
15:12	HW: 0011b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC3 (CRQSELSRC3):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC3 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC3 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC3 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC3 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC3 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC3 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC3 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC3 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC3 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC3 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC3 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC3 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC3 output. ***B-stepping Note:*** Parameter behaves normally.

Table A-13. SRC Power Management

Bits	Default	Description
11:8	HW: 0010b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC2 (CRQSELSRC2):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC2 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC2 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC2 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC2 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC2 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC2 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC2 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC2 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC2 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC2 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC2 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC2 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC2 output. ***B-stepping Note:*** Parameter behaves normally.
7:4	HW: 0001b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC1 (CRQSELSRC1):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC1 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC1 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC1 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC1 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC1 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC1 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC1 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC1 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC1 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC1 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC1 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC1 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC1 output. ***B-stepping Note:*** Parameter behaves normally.
3:0	HW: 0000b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_SRC0 (CRQSELSRC0):** Select external input CLKRQ# pin for dynamical control of CLKOUT_SRC0 output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_SRC0 **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_SRC0 **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_SRC0 **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_SRC0 **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_SRC0 **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_SRC0 **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_SRC0 **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_SRC0 **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_SRC0 **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_SRC0 **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_SRC0 ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_SRC0 output. ***B-stepping Note:*** Parameter behaves normally.

A.2.13 PMSRCCLK2 – SRC Power Management

BTM/DCI Default: 0000 0F98h
ME FW/Flash Image Tool and Config Wizard Default: FFFF FFFFh
0000 0FFFh

Description: This parameter assigns dynamic CLKRQ# control of SRC clocks
Flash Image Tool Configuration: Flash Image | Configuration | ICC Data | OEM Request Record [6:0] | Static Registers Section

Table A-14. SRC Power Management

Bits	Default	Description
31:12	0h	**Reserved (RSVD)**
11:8	HW: 1001b ME FW: 1111b FITC: 1111b	**Chipset Configuration (PCHCFG):** Must be set to **1111b**.
7:4	HW: 1000b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_PEG_B (CRQSELPEGB):** Select external input CLKRQ# pin for dynamical control of CLKOUT_PEG_B output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_PEG_B **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_PEG_B **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_PEG_B **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_PEG_B **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_PEG_B **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_PEG_B **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_PEG_B **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_PEG_B **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_PEG_B **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_PEG_B **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_PEG_B ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_PEG_B output. ***B-stepping Note:*** Parameter behaves normally.
3:0	HW: 1000b ME FW: 1111b FITC: 1111b	**CLKRQ# Select for CLKOUT_PEG_A (CRQSELPEGA):** Select external input CLKRQ# pin for dynamical control of CLKOUT_PEG_A output. **0000b =** SRC0CLKRQ#/GPIO73 controls CLKOUT_PEG_A **0001b =** SRC1CLKRQ#/GPIO18 controls CLKOUT_PEG_A **0010b =** SRC2CLKRQ#/GPIO20 controls CLKOUT_PEG_A **0011b =** SRC3CLKRQ#/GPIO25 controls CLKOUT_PEG_A **0100b =** SRC4CLKRQ#/GPIO26 controls CLKOUT_PEG_A **0101b =** SRC5CLKRQ#/GPIO44 controls CLKOUT_PEG_A **0110b =** SRC6CLKRQ#/GPIO45 controls CLKOUT_PEG_A **0111b** = SRC7CLKRQ#/GPIO46 controls CLKOUT_PEG_A **1000b** = SRC8CLKRQ#/PEG_A_CLKRQ#/GPIO47 controls CLKOUT_PEG_A **1001b =** SRC9CLKRQ#/PEG_B_CLKRQ#/GPIO56 controls CLKOUT_PEG_A **101xb =** Reserved **1110b =** Reserved **1111b =** Disable dynamic control of CLKOUT_PEG_A ***A-stepping Note:*** This parameter has no effect and the dynamic control CLKOUT_PEG_A output. ***B-stepping Note:*** Parameter behaves normally.

§

B Appendix — Flash Configurations

This chapter covers only the basic information needed for clock control parameter programming. For a more detailed treatment of Ibex Peak clocks, see *Ibex Peak Platform Clocks and Intel® Management Engine — Platform Compliancy Guide for ME Hardware, Intel*.

Figure B-1. Configuration "A" — Desktop or Mobile

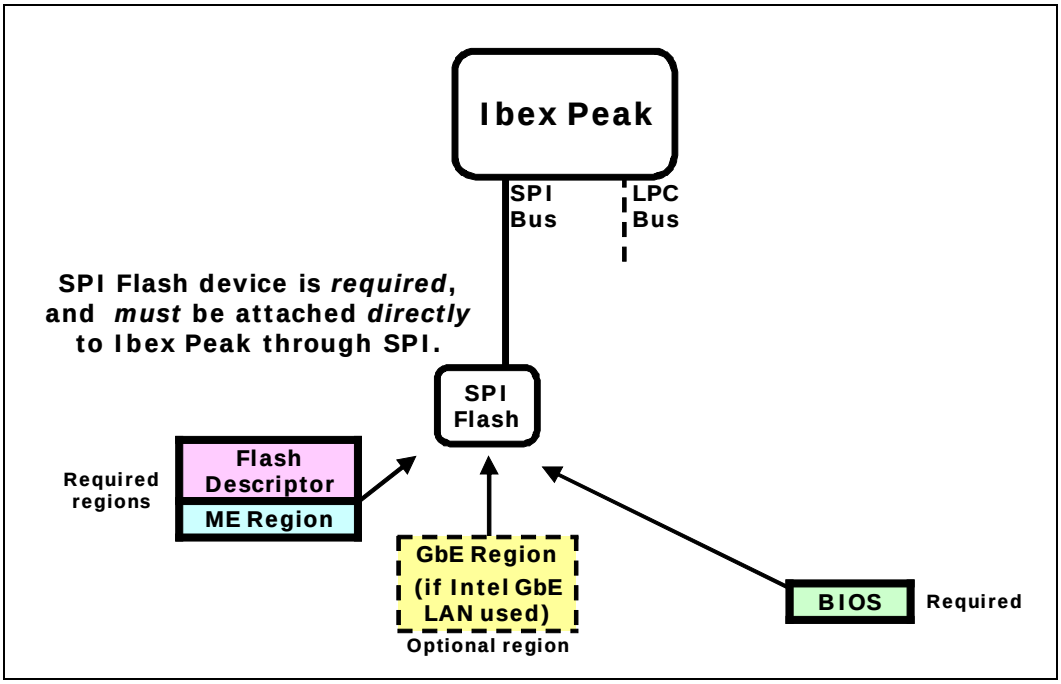


Figure B-2. Configuration "B" — Mobile only

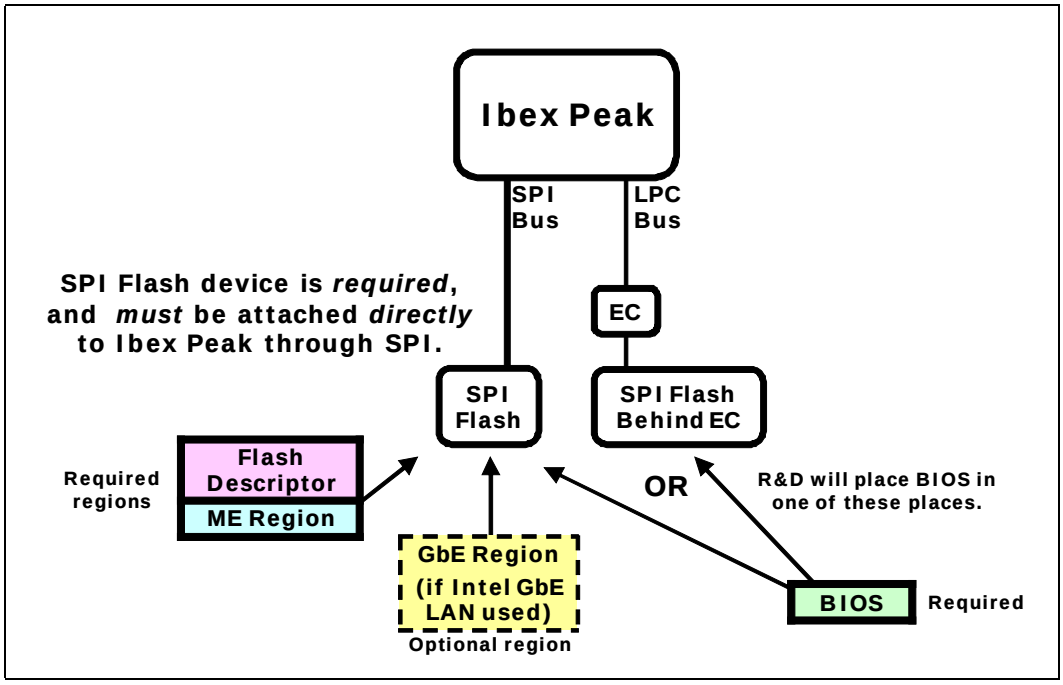


Figure B-3. Configuration "C" — Desktop only

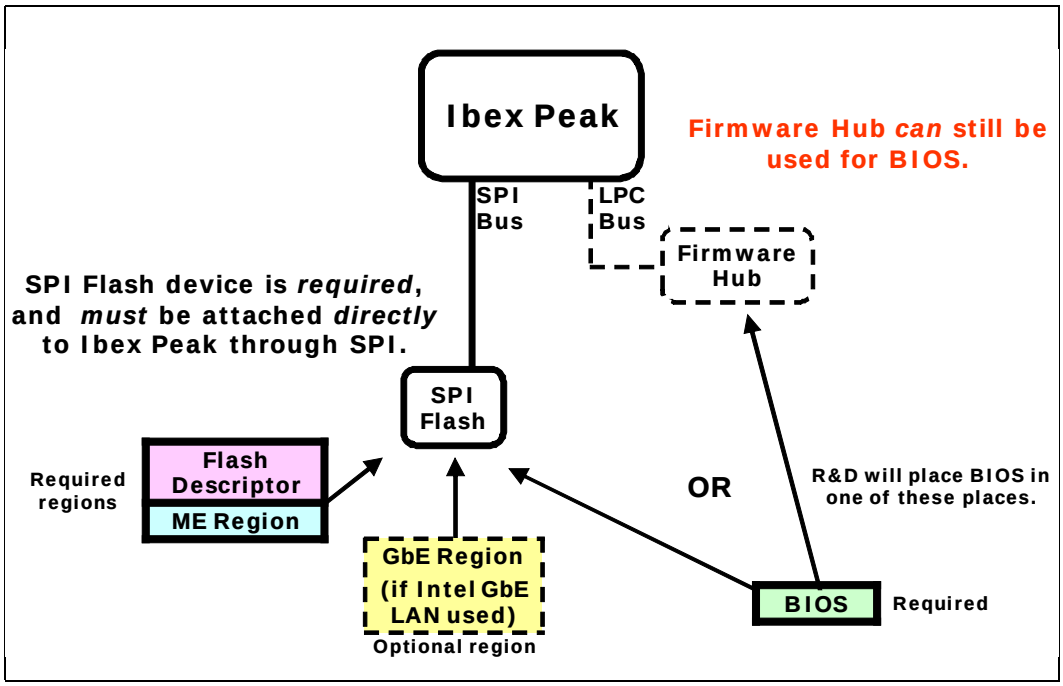
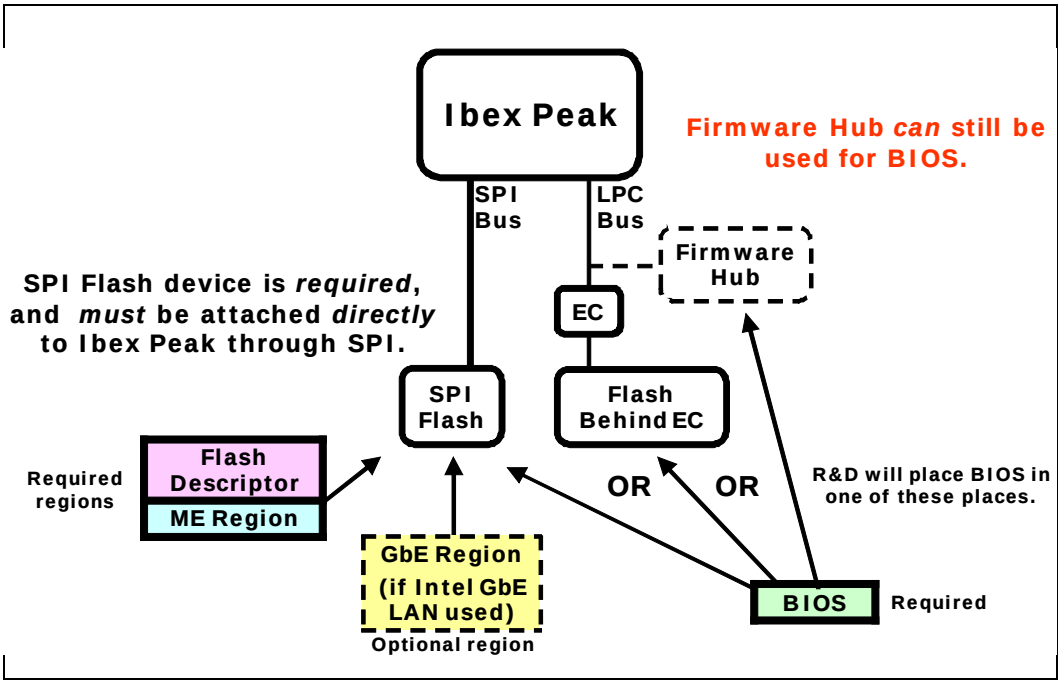


Figure B-4. Configuration "D" — Mobile only



§

1 Introduction 11
1.1 Prerequisites 11
1.2 ME FW Kit Contents 11
1.3 External Hardware Requirements for Bring Up 15

2 Image Creation: Config Wizard (FICW) 17
2.1 Flash Image Configuration Wizard (FICW) Requirements 17
2.1.1 OS Support 17
2.2 Installation Instructions 17
2.3 Use Configuration Wizard to Build SPI Flash Binary Image 19

3 Image Creation: Flash Image Tool (FITC) 37
3.1 Start FITC and Load the Default Settings XML File 37
3.2 Set Up The Build Environment 37
3.3 Configure PCH Silicon Stepping 39
3.4 Set Up Descriptor and SPI Flash Device(s) 39
3.4.1 Set Up Soft-Straps (Ibex Peak B-stepping Only) 44
3.5 Set Up SPI Flash Regions 49
3.6 Configure PCH Silicon SKU 52
3.7 ME FW Feature Configuration 52
3.7.1 Clock Control Parameters 52
3.7.2 Firmware Features and Capabilities 57
3.8 Build SPI Flash Binary Image 61
3.8.1 Build SPI Flash Binary Image 61
3.8.2 Save Your Settings 62
3.8.3 Protect Saved Configuration Files 62

4 Burn the SPI Flash Binary Image 65
4.1 Flash Burner/Programmer 65
4.2 Flash Programming Tool (DOS Version) 65
4.2.1 Flash Programming Tool (Windows* Version) 66

5 Intel® ME Firmware Feature Bring Up 67
5.1 Manufacturing Mode (GPIO33) 67
5.2 Intel Wired LAN Settings and Driver 69
5.3 Thermal Reporting 69

A Appendix — Ibex Peak Clock Configuration 75
A.1 Functional Blocks 76
A.2 ME FW Clock Control Parameters 77
A.2.1 FCSS – Flex Clock Source Select 77
A.2.2 PLLEN* – PLL Enable 78
A.2.3 OCKEN – Output Clock Enable 79
A.2.4 OBEN – Output Buffer Enable 81
A.2.5 IBEN – Input Buffer Enable 81
A.2.6 DIVEN* – Divider Enable 82
A.2.7 PM1 – Power Management 83
A.2.8 PM2 – Power Management 83
A.2.9 SEBP1 – Single Ended Buffer Parameters 84
A.2.10 SEBP2 – Single Ended Buffer Parameters 85
A.2.11 SSCCTL* – SSC Control 87
A.2.12 PMSRCCLK1 – SRC Power Management 87
A.2.13 PMSRCCLK2 – SRC Power Management 90

B Appendix — Flash Configurations 93

3-1 Build | Environment Variables… 38
3-2 Build | Build Settings… 38
3-3 PCH Silicon Stepping Combo Box 39
3-4 SKU Manager Combo Box 52
3-5 Build | Build Image 61
3-6 Protecting FITC Configuration XML and ConfigParams TXT Files 63
5-1 Desktop CRB Manufacturing Mode Jumper Location 68
5-2 Mobile CRB Manufacturing Mode Jumper Location 68
5-3 Flash Descriptor Security Override (GPIO33) Rework for Redfort 68
5-4 MPG BIOS: Enable TR (Step 1 of 3) 70
5-5 MPG BIOS: Enable TR (Step 2 of 3) 71
5-6 MPG BIOS: Enable TR (Step 3 of 3) 72
5-7 CCG BIOS: Enable TR (Step 1 of 2) 73
5-8 CCG BIOS: Enable TR (Step 2 of 2) 74
A-1 Ibex Peak Buffer Through Mode Architecture 75
A-2 Ibex Peak Display Clock Integration Architecture 76
B-1 Configuration “A” — Desktop or Mobile 93
B-2 Configuration “B” — Mobile only 94
B-3 Configuration “C” — Desktop only 94
B-4 Configuration “D” — Mobile only 95

1-1 ME FW Kit Contents 11
1-2 ME FW Kit Tools 13
2-1 FICW In FITC Directory 17
2-2 Configuration Wizard: Choose Configuration File 19
2-3 Configuration Wizard: Choose Configuration File 20
2-4 Configuration Wizard: Image Source Files (1 of 2) 21
2-5 Configuration Wizard: Image Source Files (2 of 2) 22
2-6 Configuration Wizard: Intel ME VSCC Table Configuration 23
2-7 Configuration Wizard: Intel ME Configuration Parameters Screen 24
2-8 Configuration Wizard: Intel Integrated Wired LAN Configuration 25
2-9 Configuration Wizard: DMI/PCIe* configuration 26
2-10 Configuration Wizard: Thermal Reporting Configuration 27
2-11 Configuration Wizard: Boot Configuration options 28
2-12 Configuration Wizard: Production/nonproduction configuration 29
2-13 Configuration Wizard: Integrated Clocking Configuration 30
2-14 Configuration Wizard: OEM Request Record — Single-Ended Clocks (1 of 2) 31
2-15 Configuration Wizard: OEM Request Record — Single-Ended Clocks (2 of 2) 32
2-16 Configuration Wizard: OEM Request Record — Differential Clocks 33
2-17 Configuration Wizard: Braidwood Configuration 34
2-18 Configuration Wizard: Save and Build 35
3-1 Flash Image | Descriptor Region 39
3-2 Flash Image | Descriptor Region | Descriptor Map 39
3-3 Flash Image | Descriptor Region | Component Section 40
3-4 Flash Image | Descriptor Region | Master Access Section | CPU/BIOS 41
3-5 Flash Image | Descriptor Region | Master Access Section | Manageability Engine (ME) 41
3-6 Flash Image | Descriptor Region | Master Access Section | GbE LAN 42
3-7 Flash Image |Descriptor Region | ME VSCC Table | Add Table Entry 42
3-8 Flash Image | Descriptor Region | ME VSCC Table | AT26DF321 43
3-9 Flash Image | Descriptor Region | OEM Section 43
3-10 Flash Image | Descriptor Region | PCH Straps | PCH Strap 0 44
3-11 Flash Image | Descriptor Region | PCH Straps | PCH Strap 2 45
3-12 Flash Image | Descriptor Region | PCH Straps | PCH Strap 4 45
3-13 Flash Image | Descriptor Region | PCH Straps | PCH Strap 7 46
3-14 Flash Image | Descriptor Region | PCH Straps | PCH Strap 9 46
3-15 Flash Image | Descriptor Region | PCH Straps | PCH Strap 10 47
3-16 Flash Image | Descriptor Region | PCH Straps | PCH Strap 11 48
3-17 Flash Image | Descriptor Region | PCH Straps | PCH Strap 14 48
3-18 Flash Image | Descriptor Region | PCH Straps | PCH Strap 15 49
3-19 Flash Image | PDR Region 49
3-20 Flash Image | GbE Region 50
3-21 Flash Image | ME Region 51
3-22 Flash Image | BIOS Region 51
3-23 Flash Image | Configuration | ICC Data 53
3-24 Flash Image | Configuration | ICC Data | OEM Request Record 0 | Static Registers Section 54
3-25 Flash Image | Configuration | ICC Data | OEM Request Record 0 | Dynamic Registers Section 55
3-26 High Impact Clock Control Parameters 56
3-27 Flash Image | Configuration | ME 58
3-28 Flash Image | Configuration | Power Packages 59
3-29 Flash Image | Configuration | Features Supported 59
3-30 Flash Image | Configuration | Features Supported (HM57) 60

3-31 Flash Image | Configuration | Features Supported (HM55) 61
5-1 Thermal Reporting Options in MPG BIOS 72
A-1 SSC Blocks 76
A-2 Clock Dividers 76
A-3 Flex Clock Source Select Parameters 77
A-4 PLL Enable Parameters 78
A-5 Output Clock Enable Parameters 80
A-6 Input Buffer Enable Parameters 82
A-7 Divider Enable Parameters 82
A-8 Power Management Parameters 83
A-9 Power Management Parameters 84
A-10 Single Ended Buffer Parameters 84
A-11 Single Ended Buffer Parameters 86
A-12 SSC Control Parameters 87
A-13 SRC Power Management 88
A-14 SRC Power Management 91