

3rd Gen Intel® Xeon® Scalable Processor, Codename Ice Lake

Datasheet, Volume Two: Registers

August 2022

Reference Number:735086-001US



Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at Intel.com, or from the OEM or retailer.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document. The products described 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.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps. Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, Xeon, Intel® Xeon Phi[™], and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as the property of others.

Copyright © 2022, Intel Corporation. All Rights Reserved.



Contents

1	Intro	Introduction		
	1.1	.Regist	ers Overview and Configuration Process	. 8
	1.2	Related	Publications	.8
		1.2.1	Terminology	.9
		1.2.2	State of Data	13
2	Regis	sters Ov	verview	15
	2.1	Registe	er Structure	16
	2.2	Configu	Iration Register Rules	15
	2.3	Notatio	nal Conventions	18
3	DMI I	Port Re	gisters (Bus: B(0), Device: 3, Function: 0)	21
-	3.1	The DM	II Port is controlled through a set of configuration registers	
		and reg	gisters located in memory mapped space at DMIRCBAR.Bus:	
		B(0), D	Device: 3, Function: 0 (DMI Registers)	21
		3.1.1 3 1 2	DMIRCDAR (DMIRCDAR) (DMIRCDAR_MODE_DMI_U_U_U_U_CFG) — ONSEL SUN	21
		5.1.2	(PXPCAPID 0 0 0 CFG) — Offset 90h	22
		3.1.3	PCI Express Capability Register (PXPCAP) (PXPCAP_0_0_0_CFG)	~~
		314	- Offset 92h	22
		5.1.4	(PERFCTRLSTS_0_0_0_0_CFG) — Offset 180h23	
		3.1.5	CPUBUS NO (CPUBUSNO) — Offset 104h	25
		3.1.6	CPUBUS NO 1 (CPUBUSNO1) — Offset 108h	25
		3.1.7	$CPOBOS NO 2 (CPOBOSNO2) - Offset 10Cn \dots$	26
4	Intel	UPI Re	gisters	27
		4.0.1	KTI misc stat (KTIMISCSTAT) — Offset D4h	27
		4.0.2	KTI IpU (KTILPU) — Offset 94h	27
		4.0.5	as PCIE RSVD0_0, offset 44h.KTI pcsts (KTIPCSTS) — Offset 120h	28
		4.0.4	Vendor ID (VID_1) — Offset 0h	29
		4.0.5	Device ID (DID_1) - Offset 2h	29
5	Integ	rated M	lemory Controller (IMC) Registers	31
	5.1	TADWA	YNESS_0 — Offset 20DD4h	31
		5.1.1	TADWAYNESS_1 — Offset 20DD8h	32
		5.1.2 5 1 3	TADWAYNESS_2 — Offset 20DECh	32 22
		5.1.4	TADWATNESS_S — Offset 20DE01	32
		5.1.5	TADWAYNESS_5 — Offset 20DE8h	32
		5.1.6	TADWAYNESS_6 — Offset 20DECh	32
		5.1.7	TADWAYNESS_7 — Offset 20DF0h	32
		5.1.8	RCOMP_TIMER — Offset 20DFCh	33
		5.1.9	SPAREADDRESSLO — Offset 20E24n	33 ⊃⊿
		5 1 11	SCRUBADDRESSIO – Offset 20E2Ch	34
		5.1.12	SCRUBADDRESSHI — Offset 20E30h	35
		5.1.13	RASENABLES — Offset 20E3Ch	36
		5.1.14	SMISPARECTL — Offset 20E40h	37
		5.1.15	LEAKY_BUCKET_CFG — Offset 20E44h	38
		5.1.16	LEAKY_BUCKET_CNTR_HI — Offset 20E4Ch	40
		5.1.1/ 5 1 10	SPAKING_PAIKUL_STATE C Offert 20EE8b	4U // 1
		2.1.10	TIC_INIT_STATL_G - UTSEL ZULLOT	+1



	5.1.19	SPAREINTERVAL – Offset 20EF0h	2
	5.1.20	MCMTR — Offset 20EF8h	3
	5.1.21	PXPENHCAP — Offset 2180Ch	1
	5.1.22	CHN TEMP CFG – Offset 22404h45	5
	5.1.23	CHN TEMP STAT – Offset 22408h	5
	5.1.24	DIMM TEMP THRT LMT 0 – Offset 2241Ch	5
	5.1.25	DIMM TEMP EV OFST 0 – Offset 22424h47	7
	5.1.26	DIMMTEMPSTAT 1 – Offset 22430h48	3
	5.1.27	DIMMTEMPSTAT 0 – Offset 224D4h	3
	5.1.28	DIMM TEMP TH 1 – Offset 224E4h)
	5.1.29	DIMM TEMP EV OFST 1 – Offset 22510h49)
	5.1.30	CORRERRCNT 0 – Offset 22C18h)
	5.1.31	$CORRERRCNT^{-1} - Offset 22C1Ch \dots 51$	L
	5.1.32	CORRERRCNT ² – Offset 22C20h52	2
	5.1.33	CORRERRCNT ⁻³ – Offset 22C24h52	2
	5.1.34	CORRERRTHRSHLD 0 – Offset 22C30h	3
	5.1.35	CORRERRTHRSHLD 1 – Offset 22C34h	3
	5.1.36	CORRERRTHRSHLD ² – Offset 22C38h	1
	5.1.37	CORRERRTHRSHLD ⁻ 3 – Offset 22C3Ch54	1
	5.1.38	CORRERRORSTATUS – Offset 22C50h	5
	5.1.39	PLUS1_RANK0 — Offset 22D28h55	5
	5.1.40	PLUS1_RANK1 — Offset 22D2Ch	5
	5.1.41	PLUS1 RANK2 – Offset 22D30h	5
	5.1.42	PLUS1_RANK3 — Offset 22D34h56	5
	5.1.43	PLUS1_RANK4 — Offset 22D38h56	5
	5.1.44	PLUS1_RANK5 — Offset 22D3Ch56	5
	5.1.45	PLUS1_RANK6 — Offset 22D40h	5
	5.1.46	PLUS1_RANK7 — Offset 22D44h	5
			-
	5.1.47	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56	5
Powe	5.1.47 r Contr	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h	5
Powe	5.1.47 er Contr	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h	5))
Powe 6.1	5.1.47 r Contr PCU Re	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h	5
Powe 6.1	5.1.47 r Contr PCU Re 6.1.1 6.1.2	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h	5 9 9 9 9
Powe 6.1	5.1.47 r Contr PCU Re 6.1.1 6.1.2 6.1.3	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h 56 ol Unit (PCU) Registers 59 gisters 59 Vendor ID (VID_0_11_0_CFG) — Offset 0h 59 Device ID (DID_0_11_0_CFG) — Offset 2h 59 SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h 59	5 9 9 9 9 9
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h 56 ol Unit (PCU) Registers 59 gisters 59 Vendor ID (VID_0_11_0_CFG) — Offset 0h 59 Device ID (DID_0_11_0_CFG) — Offset 2h 59 SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h 59 SMB STATUS CFG (SMB_STATUS CFG) — Offset 84h 61	$\overline{\mathbf{b}}$
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h 56 ol Unit (PCU) Registers 59 gisters 59 Vendor ID (VID_0_11_0_CFG) — Offset 0h 59 Device ID (DID_0_11_0_CFG) — Offset 2h 59 SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h 59 SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h 61 SMB DATA CFG (SMB_DATA CFG) — Offset 88h 63	
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h 56 ol Unit (PCU) Registers 59 gisters 59 Vendor ID (VID_0_11_0_CFG) — Offset 0h 59 Device ID (DID_0_11_0_CFG) — Offset 2h 59 SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h 59 SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h 61 SMB DATA CFG (SMB_DATA_CFG) — Offset 88h 63 SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h 63	
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h 56 ol Unit (PCU) Registers 59 gisters 59 Vendor ID (VID_0_11_0_CFG) — Offset 0h 59 Device ID (DID_0_11_0_CFG) — Offset 2h 59 SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h 59 SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h 61 SMB DATA CFG (SMB_DATA_CFG) — Offset 88h 63 SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h 63 SMB TSOD POLL RATE CFG (SMB_TSOD_POLL RATE CFG) — Offset 98h 64	599991331
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h 56 ol Unit (PCU) Registers 59 gisters 59 Vendor ID (VID_0_11_0_CFG) — Offset 0h 59 Device ID (DID_0_11_0_CFG) — Offset 2h 59 SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h 59 SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h 61 SMB DATA CFG (SMB_DATA_CFG) — Offset 88h 63 SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h 64 Vendor ID (VID_0_11_2_CFG) — Offset 0h 64	5 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h 56 ol Unit (PCU) Registers 59 gisters 59 Vendor ID (VID_0_11_0_CFG) — Offset 0h 59 Device ID (DID_0_11_0_CFG) — Offset 2h 59 SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h 59 SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h 61 SMB DATA CFG (SMB_DATA_CFG) — Offset 88h 63 SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h 63 SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h 64 Vendor ID (VID_0_11_2_CFG) — Offset 0h 64 Device ID (DID_0_11_2_CFG) — Offset 2h 65	5 9 9 9 9 9 1 3 3 4 4 5
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 80h63SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Vendor ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD 0 11 2 CFG) — Offset 4h65	5 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 80h63SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Vendor ID (DID_0_11_2_CFG) — Offset 2h64PCI Command (PCICMD_0_11_2_CFG) — Offset 4h65PCI Status (PCISTS 0 11 2 CFG) — Offset 6h66	
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB TATUS CFG (SMB_TATUS_CFG) — Offset 80h59SMB STATUS CFG (SMB_TATUS_CFG) — Offset 80h59SMB STATUS CFG (SMB_TATUS_CFG) — Offset 80h59SMB TATUS CFG (SMB_TATUS_CFG) — Offset 80h59SMB TATUS CFG (SMB_TATUS_CFG) — Offset 80h60SMB DATA CFG (SMB_TALCFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Vendor ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 4h66PCI Status (PCISTS_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h66	5 9 9 9 9 9 1 8 8 1 1 5 5 5 7
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h61SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 4h65PCI Status (PCISTS_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h67Cache Line Size Register (CLSR 0 11 2 CFG) — Offset Ch68	5 9 9 9 9 9 1 8 8 4 4 5 5 5 7 8
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.14	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_TATUS_CFG) — Offset 84h61SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 6h65PCI Status (PCISTS_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h67Cache Line Size Register (CLSR_0_11_2_CFG) — Offset Ch68PCI Latency Timer (PLAT 0 11 2 CFG) — Offset Dh68	5 9 9 9 9 9 1 3 3 4 4 5 5 5 7 3 3
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.14 6.1.13 6.1.14 6.1.15	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_TATUS_CFG) — Offset 84h61SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 6h65PCI Status (PCISTS_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h67Cache Line Size Register (CLSR_0_11_2_CFG) — Offset Dh68PCI Latency Timer (PLAT_0_11_2_CFG) — Offset Eh68Header Type (HDR 0 11 2 CFG) — Offset Eh69	5 9 9 9 9 9 1 3 3 1 1 5 5 5 7 3 3 9
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.14 6.1.15 6.1.13 6.1.14 6.1.15 6.1.14 6.1.15 6.1.16	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h61SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 6h65PCI Status (PCISTS_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h66PCI Latency Timer (PLAT_0_11_2_CFG) — Offset Dh68Header Type (HDR_0_11_2_CFG) — Offset Fh69Built In Self Test (BIST 0 11 2 CFG) — Offset Fh69	
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.12 6.1.13 6.1.14 6.1.15 6.1.15 6.1.16 6.1.17	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h61SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h66PCI Latency Timer (PLAT_0_11_2_CFG) — Offset Ph66PCI Latency Timer (PLAT_0_11_2_CFG) — Offset Fh65Built In Self Test (BIST_0_11_2_CFG) — Offset Fh69Subsystem Vendor ID (SVID 0 11 2 CFG) — Offset 2ch70	5 9 9 9 9 9 1 3 3 4 4 5 5 5 7 3 3 9 9 0
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.12 6.1.13 6.1.14 6.1.15 6.1.14 6.1.15 6.1.17 6.1.16	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 80h61SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h67Cache Line Size Register (CLSR_0_11_2_CFG) — Offset Dh68PCI Latency Timer (PLAT_0_11_2_CFG) — Offset Dh68Header Type (HDR_0_11_2_CFG) — Offset Fh69Built In Self Test (BIST_0_11_2_CFG) — Offset Fh69Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset 2Ch70Subsystem ID (SDID 0 11 2 CFG) — Offset 2Eh70	
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.14 6.1.15 6.1.14 6.1.15 6.1.15 6.1.16 6.1.17 6.1.18 6.1.17 6.1.18 6.1.17 6.1.18 6.1.17 6.1.18 6.1.11 6.1.12	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_DATA_CFG) — Offset 84h61SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 4h65PCI Status (PCISTS_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h67Cache Line Size Register (CLSR_0_11_2_CFG) — Offset Ch68PCI Latency Timer (PLAT_0_11_2_CFG) — Offset Eh69Built In Self Test (BIST_0_11_2_CFG) — Offset Fh69Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset 2h69Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset 2h69Subsystem ID (SDID_0_11_2_CFG) — Offset 2h70Subsystem ID (SDID_0_11_2_CFG) — Offset 2h70Subsystem ID (SDID_0_11_2_CFG) — Offset 2h70Capability Pointer (CAPPTR 0 11 2 CFG) — Offset 34h70	
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.14 6.1.15 6.1.14 6.1.15 6.1.16 6.1.17 6.1.15 6.1.16 6.1.17 6.1.18 6.1.17 6.1.18 6.1.17 6.1.18 6.1.12	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h61SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h67Cache Line Size Register (CLSR_0_11_2_CFG) — Offset Ch66PCI Latency Timer (PLAT_0_11_2_CFG) — Offset Fh65Built In Self Test (BIST_0_11_2_CFG) — Offset Fh65Built In Self Test (BIST_0_11_2_CFG) — Offset 2h70Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset 2h70Subsystem ID (SDID_0_11_2_CFG) — Offset 2h70Capability Pointer (CAPPTR_0_11_2_CFG) — Offset 34h70Interrupt Line (INTL_0_11_2_CFG) — Offset 3Ch71	
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.14 6.1.15 6.1.16 6.1.17 6.1.15 6.1.16 6.1.17 6.1.18 6.1.17 6.1.18 6.1.17 6.1.18 6.1.19 6.1.10 6.1.11 6.1.21 6.1.12 6.1.11 6.1.21 6.1.12 6.1.10 6.1.11 6.1.21	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h61SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h67Cache Line Size Register (CLSR_0_11_2_CFG) — Offset Ch68PCI Latency Timer (PLAT_0_11_2_CFG) — Offset Eh69Built In Self Test (BIST_0_11_2_CFG) — Offset Fh69Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset 2ch70Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset 34h70Capability Pointer (CAPPTR_0_11_2_CFG) — Offset 34h70Interrupt Line (INTL_0_11_2_CFG) — Offset 3Ch71Interrupt Pin (INTPIN_0_11_2_CFG) — Offset 3Dh71	5 9 9 9 9 1 3 3 4 4 5 5 5 7 3 3 9 9 0 0 1 1
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.14 6.1.15 6.1.16 6.1.17 6.1.18 6.1.17 6.1.18 6.1.19 6.1.11 6.1.12 6.1.13 6.1.14 6.1.12 6.1.13 6.1.14 6.1.12 6.1.11 6.1.22	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 80h59SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h67Cache Line Size Register (CLSR_0_11_2_CFG) — Offset Dh68Header Type (HDR_0_11_2_CFG) — Offset Fh69Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset Fh69Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset 2ch70Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset 34h70Interrupt Line (INTL_0_11_2_CFG) — Offset 3Ch71Interrupt Line (INTL_0_11_2_CFG) — Offset 3Ch71Minimum Grant (MINGNT_0_11_2_CFG) — Offset 3Ch71Minimum Grant (MINGNT_0_11_2_CFG) — Offset 3Eh72	5 9 9 9 9 9 1 3 3 1 1 5 5 5 7 3 3 9 9 0 0 1 1 2
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.14 6.1.15 6.1.16 6.1.17 6.1.18 6.1.17 6.1.18 6.1.17 6.1.18 6.1.19 6.1.11 6.1.22 6.1.20 6.1.21 6.1.22 6.1.23	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 84h61SMB DATA CFG (SMB_DATA_CFG) — Offset 88h63SMB PERIOD CFG (SMB_DATA_CFG) — Offset 88h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h67Cache Line Size Register (CLSR_0_11_2_CFG) — Offset Ch68Header Type (HDR_0_11_2_CFG) — Offset Fh69Built In Self Test (BIST_0_11_2_CFG) — Offset Fh69Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset 2ch70Subsystem ID (SDID_0_11_2_CFG) — Offset 34h70Interrupt Line (INTL_0_11_2_CFG) — Offset 30h71Interrupt Line (INTL_0_11_2_CFG) — Offset 30h71Minimum Grant (MINGNT_0_11_2_CFG) — Offset 3Fh72Maximum Latency (MAXLAT_0_11_2_CFG) — Offset 3Fh72	
Powe 6.1	5.1.47 PCU Re 6.1.1 6.1.2 6.1.3 6.1.4 6.1.5 6.1.6 6.1.7 6.1.8 6.1.9 6.1.10 6.1.11 6.1.12 6.1.13 6.1.14 6.1.15 6.1.16 6.1.17 6.1.18 6.1.17 6.1.18 6.1.19 6.1.11 6.1.12 6.1.13 6.1.14 6.1.15 6.1.16 6.1.17 6.1.12 6.1.13 6.1.14 6.1.12 6.1.21 6.1.12 6.1.13 6.1.14 6.1.12 6.1.21 6.1.22 6.1.23 6.1.21 6.1.22 6.1.23 6.1.21 6.1.22 6.1.23 6.1.24	EAKY_BKT_2ND_CNTR_REG — Offset 22E78h56ol Unit (PCU) Registers59gisters59Vendor ID (VID_0_11_0_CFG) — Offset 0h59Device ID (DID_0_11_0_CFG) — Offset 2h59SMB COMMAND CFG (SMB_CMD_CFG) — Offset 80h59SMB STATUS CFG (SMB_STATUS_CFG) — Offset 80h59SMB STATUS CFG (SMB_DATA_CFG) — Offset 88h61SMB PERIOD CFG (SMB_PERIOD_CFG) — Offset 90h63SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) — Offset 98h64Vendor ID (VID_0_11_2_CFG) — Offset 0h64Device ID (DID_0_11_2_CFG) — Offset 2h65PCI Command (PCICMD_0_11_2_CFG) — Offset 4h65PCI Status (PCISTS_0_11_2_CFG) — Offset 6h66Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h67Cache Line Size Register (CLSR_0_11_2_CFG) — Offset Ch68Header Type (HDR_0_11_2_CFG) — Offset Fh69Subsystem Vendor ID (SVID_0_11_2_CFG) — Offset Fh69Subsystem ID (SDID_0_11_2_CFG) — Offset 2ch70Subsystem ID (SDID_0_11_2_CFG) — Offset 3ch71Interrupt Line (INTL_0_11_2_CFG) — Offset 3ch71Interrupt Pin (INTPIN_0_11_2_CFG) — Offset 3ch71Minimum Grant (MINGNT_0_11_2_CFG) — Offset 3ch72PACKAGE ENERGY STATUS (PACKAGE_ENERGY_STATUS_CFG) — Offset 90h.72	5 9 9 9 9 9 9 9 9 9 9 9 9 9

6



6.1.26	PACKAGE TEMPERATURE (PACKAGE_TEMPERATURE_CFG) — Offset C8h 74
6.1.27	BIOS MAILBOX DATA (BIOS MAILBOX DATA CFG) — Offset 8Ch
6 1 28	BIOS MAILBOX INTERFACE (BIOS MAILBOX INTERFACE CEG) - Offset 90b 75
0.1.20	DIGS MALEDOX INTEL ACCOUNTER ACCOUNT AND A STATE OF A S
6.1.29	US MAILBOX DATA (US_MAILBOX_DATA_CFG) — Offset AUT
6.1.30	OS MAILBOX INTERFACE (OS_MAILBOX_INTERFACE_CFG) — Offset A4h 76
6.1.31	DRAM ENERGY STATUS (DRAM ENERGY STATUS CFG) - Offset 80h
6 1 32	PACKAGE OVERELOW STATUS (PACKAGE PARI PERE STATUS) - Official 88h 77
0.1.52	ACKAGE WER NEGOMATION (FRAM DOWER LIFE STATION) - Office tool 70
6.1.33	DRAM POWER INFORMATION (DRAM_POWER_INFO_CFG) — Offset Ash
6.1.34	MEM TRML TEMPERATURE REPORT
	(MEM_TRML_TEMPERATURE_REPORT[0]) — Offset C8h78
6 1 35	MEM TRMI TEMPERATURE REPORT
0.1.55	(MEM TDML TEMPEDATURE DEPORT[1]) Officit CCh 70
6 1 26	
6.1.36	MEM TRML TEMPERATURE REPORT
	(MEM_TRML_TEMPERATURE_REPORT[2]) — Offset D0h79
6.1.37	MEM TRML TEMPERATURE REPORT
	(MEM_TRML_TEMPERATURE_REPORT[3]) — Offset D4h
6 1 38	DRAM PLANE OVERELOW STATUS
0.1.50	(DDAM DADI DEDE STATUS (CC) Officiat DSh 70
	(DRAM_RAPL_PERF_STATUS_CFG) - Offset Dollard and a second se
6.1.39	THERMIRIP CONFIGURATION (THERMIRIP_CONFIG_CFG) — Offset F8h80
6.1.40	MEMHOT EXTERNAL STATUS (MH_EXT_STAT_CFG) — Offset 84h 80
6.1.41	
6 1 12	POP ASSOC REGISTER (POP ASSOCIOI) - Officet 44b 81
0.1.42	
6.1.43	$PQR ASSOC REGISTER (PQR_ASSOC[10]) = Offset 48h \dots 81$
6.1.44	PQR ASSOC REGISTER (PQR_ASSOC[11]) — Offset 4Ch 81
6.1.45	POR ASSOC REGISTER (POR ASSOC[12]) — Offset 50h
6146	POR ASSOC REGISTER $(POR ASSOC[13]) - Offset 54h$ 81
6 1 47	
0.1.47	PQR ASSOC REGISTER (PQR ASSOC[14]) = 0 mset 501
6.1.48	PQR ASSOC REGISTER (PQR_ASSOC[15]) — Offset 5Ch
6.1.49	PQR ASSOC REGISTER (PQR_ASSOC[16]) — Offset 60h 82
6.1.50	POR ASSOC REGISTER (POR ASSOC[17]) — Offset 64h
6 1 51	POR ASSOC REGISTER (POR ASSOC[18]) - Offset 68h 82
6 1 5 2	
0.1.52	PQR ASSOC REGISTER (PQR_ASSOC[19]) - Oliset ocli
6.1.53	PQR ASSOC REGISTER (PQR_ASSOC[20]) — Offset 70h
6.1.54	PQR ASSOC REGISTER (PQR_ASSOC[21]) — Offset 74h 82
6.1.55	POR ASSOC REGISTER (POR ASSOC[22]) — Offset 78h
6 1 56	POP ASSOC REGISTER (POP ASSOC[23]) — Offset 7Ch 82
6 1 57	
6.1.5/	POR ASSOC REGISTER (POR_ASSOC[24]) — Oliset 8011
6.1.58	PQR ASSOC REGISTER (PQR_ASSOC[25]) — Offset 84h
6.1.59	PQR ASSOC REGISTER (PQR_ASSOC[26]) — Offset 88h 82
6.1.60	POR ASSOC REGISTER (POR ASSOC[27]) — Offset 8Ch
6 1 6 1	POR ASSOC REGISTER (POR ASSOC[28]) - Offset 90h 83
6 1 6 2	
0.1.02	PQR ASSOC REGISTER (PQR_ASSOC[29]) — Oliset 9411
6.1.63	PQR ASSOC REGISTER (PQR_ASSOC[30]) — Offset 98h
6.1.64	PQR ASSOC REGISTER (PQR_ASSOC[31]) — Offset 9Ch
6.1.65	POR ASSOC REGISTER (POR ASSOC[32]) — Offset A0h
6 1 66	POP ASSOC REGISTER (POR ASSOC[33]) - Offset Adh 83
6 1 67	
0.1.0/	PQR ASSOC REGISTER (PQR_ASSOC[34]) — Oliset A8183
6.1.68	PQR ASSOC REGISTER (PQR_ASSOC[35]) — Offset ACh83
6.1.69	PQR ASSOC REGISTER (PQR ASSOC[36]) — Offset B0h
6.1.70	POR ASSOC REGISTER (POR ASSOC[37]) — Offset B4h
6 1 71	POP ASSOC DECISTED (DOP ASSOC[33]) - Official B8h 83
0.1.71	POR ASSOC REGISTER (POR ASSOC[S0]) = Offset Bolt
0.1./2	PQK ASSOC REGISTER (PQK_ASSOC[39]) - Offset BCn
6.1.73	PQR ASSOC REGISTER (PQR_ASSOC[40]) — Offset C0h
6.1.74	PQR ASSOC REGISTER (PQR_ASSOC[41]) — Offset C4h
6.1.75	POR ASSOC REGISTER (POR ASSOC[42]) - Offset C8h 84
6 1 76	POR ASSOC REGISTER (POR ASSOC[43]) $-$ Offset CCh 84
6 1 77	$\frac{1}{2} O(1) = O(1) =$
0.1.//	ruk about kegistek (ruk_about[44]) - Umset Dun



Tables

1-1	Public Publications
2-1	Register Attributes Definitions
4-1	State Tracker Encoding



Revision History

§

Document Number	Revision Number	Description	Date
735086- 001US	001	Initial Release	July 2022

intel¹ Introduction

ALL INFORMATION IN THIS DOCUMENT IS PRELIMINARY AND SUBJECT TO CHANGE.

3rd Gen Intel® Xeon® Scalable processor datasheet Volume 2 provides Configuration Space Registers (CSRs).

- **Note:** Features within this document may not be available on all platform segments, processor types, or processor SKUs.
- **Note:** Unless specified otherwise, the term "processor" will represent the following processors throughout the rest of the document.

The 3rd Gen Intel Xeon Scalable processor is the next generation of 64-bit, multi-core server processor built on 10-nm process technology. The processor supports up to 52 bits of physical address space and 57 bits of virtual address space. The processor is designed for a platform consisting of at least one 3rd Gen Intel Xeon Scalable processor and the Platform Controller Hub (PCH). Included in this family of processors are integrated memory controller (IMC) and an Integrated I/O (IIO) on a single silicon die.

All processor types support up to 64 lanes of PCI Express* 4.0 links capable of 16.0 GT/s, and 4 lanes of DMI3/PCI Express* 3.0. It features four Integrated Memory Controllers (IMC), each IMC supports up to two DDR4 channels with up to two DIMMs per channel.

For more supported processor configurations, see the 3rd Gen Intel® Xeon® Scalable Processor, Codename Ice Lake Datasheet, Volume One: Electrical, document number 732800.

1.1 Registers Overview and Configuration Process

This is volume two (Vol 2) of the processor public document, which provides uncore register and core MSR information for the processor. This volume documents the Configuration Space Registers (CSRs) of each individual functional block in the uncore logic, MMIO Registers for the IIO, and core MSRs. The processor contains one or more PCI devices within each functional block. The configuration registers for these devices are mapped as devices residing on the PCI Bus assigned to the processor socket. CSRs are the basic hardware elements that configure the uncore logic to support various system topologies, memory configuration and densities, and hardware hooks required for RAS operations.

- **Note:** The content contained in this volume comprehends the different processor types. Some register and field descriptions will apply only to the specific processor types. Not all features specific for each processor type have been explicitly identified in this volume, and not all features documented are available for all SKUs.
- **Note:** Some Default values will vary based on processor type and SKU, and in most cases these are the read only register fields which provide processor support visibility to firmware. Firmware should not rely on these Default values provided in this document, and instead verify these values by reading them with firmware.

1.2 Related Publications

Refer to the following documents for additional information.



Table 1-1. Public Publications

Document	Document Number/Location
3rd Gen Intel® Xeon® Scalable Processor, Codename Ice Lake Datasheet, Volume One: Electrical	
Advanced Configuration and Power Interface Specification 4.0	http://www.acpi.info/
PCI Local Bus Specification 3.0	http://www.pcisig.com/
PCI Express Base Specification, Revision 3.0	http://www.pcisig.com/
PCI Express Base Specification, Revision 2.1	
PCI Express Base Specification, Revision 1.1	
PCIe* Gen 3 Connector High Speed Electrical Test Procedure	325028-001 / http://www.intel.com/content/ www/us/en/io/pci-express/pci- express-architecture-devnet- resources.html
DDR4 SDRAM Specification and Register Specification	http://www.jedec.org/
Intel [®] 64 and IA-32 Architectures Software Developer's Manuals Volume 1: Basic Architecture Volume 2A: Instruction Set Reference, A-M Volume 2B: Instruction Set Reference, N-Z Volume 3A: System Programming Guide Volume 3B: System Programming Guide Intel [®] 64 and IA-32 Architectures Optimization Reference Manual	325462 / http://www.intel.com/products/ processor/manuals/index.htm
Intel [®] Virtualization Technology Specification for Directed I/O Architecture Specification	http://www.intel.com/ content/ www/us/en/intelligent- systems/ intel-technology/vt- directed-io- spec.html
Intel [®] Trusted Execution Technology Software Development Guide	http://www.intel.com/technology/ security/

1.2.1 Terminology

Term	Description
AC	Read and Write Access Control
ASPM	Active State Power Management
AVX	Intel Advanced Vector Extensions (AVX) promotes legacy 128-bit SIMD instruction sets that operate on XMM register set to use a "vector extension" (VEX) prefix and operates on 256-bit vector registers (YMM).
AVX512	The base of the 512-bit SIMD instruction extensions are referred to as Intel [®] AVX-512 foundation instructions. They include extensions of the AVX family of SIMD instructions but are encoded using a new encoding scheme with support for 512-bit vector registers, up to 32 vector registers in 64-bit mode, and conditional processing using opmask registers.
BMC	Baseboard Management Controller
CA	Coherency Agent. In some cases this is referred to as a Caching Agent though a CA is not actually required to have a cache. It is a term used for the internal logic providing mesh interface to LLC and Core. The CA is a functional unit in the CHA.
СНА	The functional module that includes the CA (Coherency Agent) and HA (Home Agent).



Term	Description
СР	Control Policy
DDR4	Fourth generation Double Data Rate SDRAM memory technology.
DMA	Direct Memory Access
DMI3	Direct Media Interface Gen3 operating at PCI Express 3.0 speed.
DTLB	Data Translation Look-aside Buffer. Part of the processor core architecture.
DTS	Digital Thermal Sensor
ECC	Error Correction Code
Enhanced Intel SpeedStep® Technology	Allows the operating system to reduce power consumption when performance is not needed.
Execute Disable Bit	The Execute Disable bit allows memory to be marked as executable or non-executable, when combined with a supporting operating system. If code attempts to run in non-executable memory the processor raises an error to the operating system. This feature can prevent some classes of viruses or worms that exploit buffer overrun vulnerabilities and can thus help improve the overall security of the system. See the Intel [®] 64 and IA-32 Architectures Software Developer's Manuals for more detailed information.
FLIT	Flow Control Unit. The Intel UPI Link layer's unit of transfer. A FLIT is made of multiple PHITS. A Flit is always a fixed amount of information (192 bits).
Functional Operation	Refers to the normal operating conditions in which all processor specifications, including DC, AC, system bus, signal quality, mechanical, and thermal, are satisfied.
GSSE	Extension of the SSE/SSE2 (Streaming SIMD Extensions) floating point instruction set to 256b operands.
НА	A Home Agent (HA) orders read and write requests to a piece of coherent memory. The HA is implemented in the CHA logic.
ICU	Instruction Cache Unit. Part of the processor core architecture.
IDI	Intra-Die Interconnect. The protocol used by Intel cores
IFU	Instruction Fetch Unit. Part of the processor core.
ΙΙΟ	Integrated I/O Controller. An I/O controller that is integrated in the processor die. The IIO consists of the DMI3 module, PCIe modules, and MCP (Ice Lake Server with Fabric SKUs only) modules.
IMC	Integrated Memory Controller. A Memory Controller that is integrated in the processor die.
Intel [®] ME	${\rm Intel}^{\circledast}$ Management Engine. The processor uses ${\rm Intel}^{\circledast}$ ME 11 for Ice Lake Workstation 1S, Ice Lake Workstation 2S and Ice Lake HEDT.
Intel [®] QuickData Technology	Intel QuickData Technology is a platform solution designed to maximize the throughput of server data traffic across a broader range of configurations and server environments to achieve faster, scalable, and more reliable I/O.
Intel $^{\mathbb{R}}$ Ultra Path Interconnect (Intel $^{\mathbb{R}}$ UPI)	A cache-coherent, link-based Interconnect specification for Intel processors. Also known as Intel UPI.
Intel [®] 64 Technology	64-bit memory extensions to the IA-32 architecture. Further details on Intel 64 architecture and programming model can be found at http://developer.intel.com/technology/intel64/
Intel [®] Turbo Boost Technology	A feature that opportunistically enables the processor to run a faster frequency. This results in increased performance of both single and multi-threaded applications.
Intel [®] TXT	Intel [®] Trusted Execution Technology
Intel [®] Virtualization Technology (Intel [®] VT)	Processor Virtualization which when used in conjunction with Virtual Machine Monitor software enables multiple, robust independent software environments inside a single platform.



Term	Description
Intel [®] VT-d	Intel [®] Virtualization Technology (Intel [®] VT) for Directed I/O. Intel VT-d is a hardware assist, under system software (Virtual Machine Manager or OS) control, for enabling I/O device Virtualization. Intel VT-d also brings robust security by providing protection from errant DMAs by using DMA remapping, a key feature of Intel VT-d.
Integrated Heat Spreader (IHS)	A component of the processor package used to enhance the thermal performance of the package. Component thermal solutions interface with the processor at the IHS surface.
IOV	I/O Virtualization
IVR	Integrated Voltage Regulation (IVR): The processor supports several integrated voltage regulators.
Intel UPI	Intel $^{(B)}$ Ultra Path Interconnect (Intel $^{(B)}$ UPI) Agent. An internal logic block providing interface between internal mesh and external Intel UPI.
LLC	Last Level Cache
LRDIMM	Load Reduced Dual In-line Memory Module
LRU	Least Recently Used. A term used in conjunction with cache allocation policy.
M2M	Mesh to Memory. Logic in the IMC which interfaces the IMC to the mesh.
M2PCIe	a.k.a MS2IOSF && M2IOSF - The logic in the IIO modules which interface the modules to the mesh.
МСР	A module in the IIO enabled in Ice Lake Server with Fabric which is used to interface to the on package ${\rm Intel}^{\textcircled{R}}$ Omni-Path.
MESH	The on die interconnect which connects modules in the processor.
MESI	Modified/Exclusive/Shared/Invalid. States used in conjunction with cache coherency
MS2IDI	Mesh to IDI. An internal logic block providing interface between internal Mesh and Core
MLC	Mid Level Cache
NCTF	Non-Critical to Function: NCTF locations are typically redundant ground or non-critical reserved, so the loss of the solder joint continuity at end of life conditions will not affect the overall product functionality.
NID \ NodeID	Node ID (NID) or NodeID (NID). The processor implements up to 4- bits of NodeID (NID).
Pcode	Pcode is microcode which is run on the dedicated microcontroller within the PCU.
РСН	Platform Controller Hub. The next generation chipset with centralized platform capabilities including the main I/O interfaces along with display connectivity, audio features, power management, manageability, security and storage features.
PCU	Power Control Unit.
PCIe*	PCI Express*
PCI Express 3.0	The third generation PCI Express specification that operates at twice the speed of PCI Express 2.0 (8 Gb/s); PCI Express 3.0 is completely backward compatible with PCI Express 1.0 and 2.0.
PCI Express 2.0	PCI Express Generation 2.0
PECI	Platform Environment Control Interface
Phit	The data transfer unit on Intel UPI at the Physical layer is called a phit (physical unit). A Phit will be either 20 bits, or 8 bits depending on the number of active lanes.
Processor	Includes the 64-bit cores, uncore, I/Os and package



Term	Description
Processor Core	The term "processor core" refers to Si die itself which can contain multiple execution cores. Each execution core has an instruction cache and data cache and MLC cache. All execution cores share the L3 cache.
RAC	Read Access Control
Rank	A unit of DRAM corresponding four to eight devices in parallel, ignoring ECC. These devices are usually, but not always, mounted on a single side of a DDR4 DIMM.
RDIMM \ LRDIMM	Registered Dual In-line Memory Module \ Load Reduced DIMM
RTID	Request Transaction IDs are credits issued by the CHA to track outstanding transaction, and the RTIDs allocated to a CHA are topology dependent.
SCI	System Control Interrupt. Used in ACPI protocol.
SKU	Stock Keeping Unit (SKU) is a subset of a processor type with specific features, electrical, power and thermal specifications. Not all features are supported on all SKUs. A SKU is based on specific use condition assumption.
SSE	Intel [®] Streaming SIMD Extensions (Intel [®] SSE)
SMBus	System Management Bus. A two-wire interface through which simple system and power management related devices can communicate with the rest of the system.
Storage Conditions	A non-operational state. The processor may be installed in a platform, in a tray, or loose. Processors may be sealed in packaging or exposed to free air. Under these conditions, processor landings should not be connected to any supply voltages, have any I/Os biased or receive any clocks. Upon exposure to "free air" (that is, unsealed packaging or a device removed from packaging material) the processor must be handled in accordance with moisture sensitivity labeling (MSL) as indicated on the packaging material.
Intel [®] Omni-Path	The HPC fabric enabled on the Ice lake Server with Fabric. This is provided through a primary side connector on the package.
TAC	Thermal Averaging Constant
TC	Traffic Controller block is in charge of verifying that inbound and outbound traffic coming from mesh to PCIe ports don't have errors.
TDP	Thermal Design Power
TSOD	Temperature Sensor On DIMM
Wolf River	The on package component included on Ice Lake Server with Fabric which provide ${\rm Intel}^{\rm (I\!R)}$ Omni-Path fabric.
UDIMM	Unbuffered Dual In-line Memory Module
Uncore	The portion of the processor comprising the shared LLC cache, CHA, IMC, PCU, Ubox, IIO and Intel UPI modules.
Unit Interval	Signaling convention that is binary and unidirectional. In this binary signaling, one bit is sent for every edge of the forwarded clock, whether it be a rising edge or a falling edge. If a number of edges are collected at instances t 1, t 2, t n,, t k then the UI at instance "n" is defined as: UI n = t n - t n - 1
Volume Management Device (VMD)	Volume Management Device (VMD) is a new technology used to improve PCIe management. VMD maps the PCIe configuration space for child devices/adapters for a particular PCIe x16 module into its own address space, controlled by a VMD driver.
VCCIN	Primary voltage input to the voltage regulators integrated into the processor.
VSS	Processor ground
VSSA	System agent supply for Intel UPI and PCIe
VCCIO	IO voltage supply input



Term	Description
VCCD	DDR power rail
WAC	Write Access Control
x1, x4, x8, x16	Refers to a Link or Port with one, two, four or eight Physical Lane(s)

1.2.2 State of Data

The data contained within this document is preliminary. It is the most accurate information available by the publication date of this document. The information in this revision of the document is based on early development data. Information may change prior to production.

§





2 Registers Overview

This document is the volume two (Vol 2) of the processor datasheet document which provides the Configuration Space Registers (CSRs) of each individual functional block in the uncore logic, MMIO Registers for the IIO, and core MSR information for the processor.

The processor supports the following configuration register types:

- PCI Configuration Registers (CSRs): CSRs are chipset specific registers that are located at PCI defined address space. The processor contains PCI devices within each functional block. The configuration registers for these devices are mapped as devices residing on the PCI Bus assigned to the processor socket. CSRs are the basic hardware elements that configure the uncore logic to support various system topologies, memory configuration and densities, and hardware hooks required for RAS operations.
 - When the Volume Management Device (VMD) is enabled for a particular root bus in the IIO, the VMD exposes the configuration space of its child devices through CFGBAR and the MMIO space of child devices through MEMBAR. CfgRd\Wr accesses to the child device will be dropped. A VMD driver can resurfaces VMD as an additional PCI segment, allowing child devices behind VMD to be visible via standard methods.
- Memory-mapped I/O registers: These registers are mapped into the system memory map as MMIO low or MMIO high. They are accessed by any code, typically an OS driver running on the platform. This register space is introduced with the integration of some of the chipset functionality. These MMIO registers are located in the IIO module for the PCIe segments.
- Machine Specific Registers (MSRs) are architectural and only accessed by using specific ReadMSR/WriteMSR instructions are located in the core.
- **Note:** The content contained in this volume comprehends multiple product types and SKUs. Some register and field descriptions will apply only to the specific product types and SKUs. Not all features specific for each processor type have been explicitly identified in this volume, and not all features documented are available for all SKUs. Some Default values will vary based on processor type and SKU, and in most cases these are the read only register fields which provide processor support visibility to firmware. Firmware should not rely on these Default values provided in this document, and instead verify these values by reading them with firmware.
- **Note:** There are 2 bus ranges supported for the uncore [1-0]. The Bus Number is configurable in the Ubox, CSR CPUBUSNO_CFG (B(30); Device: 0; Function: 2, Offset: 0xD0).
- **Note:** This document uses the notation: B(30) is the uncore Bus 0, andB(31) is the uncore Bus 1. By default the Bus Number for CPUBUSNO0 is 0 and CPUBUSNO1 is 1.



2.1 Register Structure

This section covers the register structure for Configuration Space Registers (CSR), Memory Mapped IO (MMIO) Registers, and Machine Specific Registers (MSRs).

Configuration Space Registers (CSR)

Configuration space registers are accessed via the configuration transaction mechanism defined in the PCI specification and uses the Bus, Device, and Function number concept to address a specific device's configuration space. If initiated by a remote CPU, accesses to PCI configuration registers are achieved via configuration transactions on Intel UPI. All configuration register accesses are accessed over Message Channel through the Ubox but can come from various sources:

- Local cores
- Remote cores (over Intel UPI)
- PECI or JTAG

Configuration registers can be read or written in Byte, WORD (16-bit), or DWORD (32bit) quantities. Accesses larger than a DWORD to PCI Express configuration space will result in unexpected behavior. All multi-byte numeric fields use "little-endian" ordering (lower addresses contain the least significant parts of the field).

Memory-Mapped I/O Registers

The PCI standard provides configuration space registers as well as registers which reside in memory-mapped space. For PCI devices, this is typically where the majority of the driver programming occurs and the specific register definitions and characteristics are provided by the device manufacturer. Access to these registers are typically accomplished via CPU reads and writes to non-coherent (UC) or write combining (WC) space. Reads and writes to memory-mapped registers can be accomplished with 1, 2, 4 or 8 byte transactions.

Prior to 10nm, the server Ubox provided sideband access to uCR and CSR registers within the coherent fabric and memory subsystem IPs. In particular, the CSRs that were accessed by BIOS were all mapped within PCIe CFG space. However, client and device have supported MMIO space within their IP blocks. To facilitate convergence across 10 nm, this feature adds support to the Ubox to allow IPs to contain MMIO registers that are accessible via the GPSB interface. This will allow these IPs containing MMIO registers to be directly connected (without change) to the GPSB fabric accessed by proxy through the Ubox.

2.2 Configuration Register Rules

Unimplemented Devices/Functions and Registers

- Configuration reads to unimplemented functions and devices will return all ones emulating a master abort response. Note that there is no asynchronous error reporting that happens when a configuration read master aborts. Configuration writes to unimplemented functions and devices will return a normal response.
- Software should not attempt or rely on reads or writes to unimplemented registers or register bits. Unimplemented registers should return all zeroes when read. Writes to unimplemented registers are ignored. For configuration writes to these register (require a completion), the completion is returned with a normal completion status (not master-aborted).



2.3 Register Terminology

The bits in configuration register descriptions will have an assigned attribute from the following table. Bits without a Sticky attribute are set to their default value by a hard reset.

Table 2-1. Register Attributes Definitions (Sheet 1 of 2)

Attribute	Description	
RO	Read Only: These bits can only be read by software, writes have no effect. The value of the bits is determined by the hardware only.	
RW	Read / Write: These bits can be read and written by software.	
RC	Read Clear Variant: These bits can be read by software, and the act of reading them automatically clears them. HW is responsible for writing these bits, and therefore the -V modifier is implied.	
W1S	Write 1 to Set: Writing a 1 to these bits will set them to 1. Writing 0 will have no effect. Reading will return indeterminate values.	
WO	Write Only: These bits can only be written by microcode, reads return indeterminate values. Microcode that wants to ensure this bit was written must read wherever the side- effect takes place.	
RW-O	Read / Write Once: These bits can be read by software. After reset, these bits can only be written by software once, after which the bits becomes 'Read Only'.	
RW-L	Read / Write Lock: These bits can be read and written by software. The bits can be made to be 'Read Only' via a separate configuration bit or other logic.	
RW/L	/L means the field is lockable When locked, SW cannot write to it. When unlocked, SW can write to it.	
RW1C	Read / Write 1 to Clear: These bits can be read and cleared by software. Writing a '1' to a bit clears it, while writing a '0' to a bit has no effect.	
RW0C	Read / Write 0 to Clear: These bits can be read and cleared by software. Writing a '0' to a bit clears it while writing a '1' has no effect.	
RW/V	/V means writeable by hardware at any time - SW could write something and then read it back and should not necessarily expect to see the value previously written.	
RW/P	/P means it is reset by powergood reset instead of normal reset - that is, it is a "sticky" reset.	
ROS	RO Sticky: These bits can only be read by software, writes have no effect. The value of the bits is determined by the hardware only. These bits are only re-initialized to their default value by a PWRGOOD reset.	
RW1S	Read, Write 1 to Set: These bits can be read. Writing a 1 to a given bit will set it to 1. Writing a 0 to a given bit will have no effect. It is not possible for software to set a bit to "0". The 1->0 transition can only be performed by hardware. These registers are implicitly - V.	
RWS	R / W Sticky: These bits can be read and written by software. These bits are only re- initialized to their default value by a PWRGOOD reset.	
RW1CS	$\sf R$ / W1C Sticky: These bits can be read and cleared by software. Writing a '1' to a bit clears it, while writing a '0' to a bit has no effect. These bits are only re-initialized to their default value by a PWRGOOD reset.	



Table 2-1. Register Attributes Definitions (Sheet 2 of 2)

Attribute	Description
RW-LB	Read/Write Lock Bypass: Similar to RWL, these bits can be read and written by software. HW can make these bits "Read Only" via a separate configuration bit or other logic. However, RW-LB is a special case where the locking is controlled by the lock-bypass capability that is controlled by the lock-bypass enable bits. Each lock-bypass enable bit enables a set of config request sources that can bypass the lock. The requests sourced from the corresponding bypass enable bits will be lock-bypassed (i.e. RW) while requests sourced from other sources are under lock control (RO). The lock bit and bypass enable bit are generally defined with RWO attributes. Sticky can be used with this attribute (RW-SWB). These bits are only reinitialized to their default values after PWRGOOD. Note that the lock bits may not be sticky, and it is important that they are written to after reset to guarantee that software will not be able to change their values after a reset.
RO-FW	Read Only Forced Write: These bits are read only from the perspective of the cores.
RWS-O	If a register is both sticky and "once" then the sticky value applies to both the register value and the "once" characteristic. Only a PWRGOOD reset will reset both the value and the "once" so that the register can be written to again.
RW-V / RO-V	These bits may be modified by hardware. Software cannot expect the values to stay unchanged. This is similar to "volatile" in software land.
RWS-V	These bits can be read or written by software and may be modified by hardware. Software cannot expect the values to stay unchanged. These bits are re-initialized to their default values by a PWRGOOD reset.
RWS-L	If a register is both sticky and locked, then the sticky behavior only applies to the value. The sticky behavior of the lock is determined by the register that controls the lock.
RWS-LV	These bits can be read or written by software and may be modified by hardware. Software cannot expect the values to stay unchanged. These bits are re-initialized to their default values by a PWRGOOD reset. If a register is both sticky and locked, then the sticky behavior only applies to the value. The sticky behavior of the lock is determined by the register that controls the lock.
SMM-RO	Read Only in SMM: These bits can only be read by software while in SMM. Writes in SMM have no effect. Attempting to read or write these bits outside of SMM will cause a #GP exception to be raised.
R/SMM-W	Read / Write Only in SMM: These bits can be read by software inside or outside of SMM but can only be written by software while in SMM. Attempting to write these bits outside of SMM will cause a $\#$ GP exception to be raised.
SMM-RW	Read Only in SMM / Write Only in SMM: These bits can only be read and written by software while in SMM. Attempting to write these bits outside of SMM will cause a $\#$ GP exception to be raised.
SMM-RW1C	Read / Write 1 to Clear in SMM: These bits can be read and cleared by software only while in SMM. Writing a '1' to a bit clears it, while writing a '0' to a bit has no effect.
RSVD-P	Reserved - These bits are reserved for future expansion and their value must not be modified by software. When writing these bits, software must preserve the value read.

2.4 Notational Conventions

Hexadecimal and Binary Numbers

Base 16 numbers are represented by a string of hexadecimal digits followed by the character H (for example, F82EH). A hexadecimal digit is a character from the following set: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F. Hexadecimal numbers can also be shown using an "x" character (for example 0x2A).

Base 2 (binary) numbers are represented by a string of 1s and 0s, sometimes followed by the character B (for example, 101B). The "B" designation is only used in situations where confusion as to the type of the number might arise.



Base 10 numbers are represented by a string of decimal digits followed by the character D (for example, 23D). The "D" designation is only used in situations where confusion as to the type of the number might arise.





3 DMI Port Registers (Bus: B(0), Device: 3, Function: 0)

3.1 The DMI Port is controlled through a set of configuration registers and registers located in memory mapped space at DMIRCBAR.Bus: B(0), Device: 3, Function: 0 (DMI Registers)

This chapter documents the DMI registers in Bus: B(0), Device 3, Function 0.

Note: The DMI Port's Configuration space is not accessible to the Operating System and the DMI port should not be enumerated by the OS.

3.1.1 DMIRCBAR (DMIRCBAR) (DMIRCBAR_MODE_DMI_0_0_CFG) - Offset 50h

Туре	Size	Offset	Default
PCI	32 bit	[B:0, D:3, F:0] + 50h	0000000h

BIOS Access	SMM Access	OS Access
RW	RW	R

Bit Range	Default & Access	Field Name (ID): Description	
31:12	00000h RW/O	DMIRCBAR: This field corresponds to bits 32 to 12 of the base address for the DMI Root Complex register space. BIOS will program this register with a 4KB block of contiguous memory address space. This register ensures that a naturally aligned 4KB space is allocated within the first 4GB of addressable memory space. System Software uses this base address to program the DMI Root Complex register set. All the Bits in this register are locked in Intel TXT mode.	
11:1	0h RO	Reserved	
0	0h RW	 DMIRCBAREN: 0: DMIRCBAR is disabled and does not claim any memory 1: DMIRCBAR memory mapped accesses are claimed and decoded Notes: Accesses to registers pointed to by the DMIRCBAR, via message channel or JTAG mini-port are not gated by this enable bit i.e. accesses these registers are honored regardless of the setting of this bit. BIOS sets this bit only when it wishes to update the registers in the DMIRCBAR. It must clear this bit when it has finished changing values. This is required to ensure that the registers cannot be changed during an Intel TXT lock. This bit is protected by Intel TXT mode, but the registers in DMIRCBAR are not protected except by this bit. 	



3.1.2 PCI Express Capability Identity (PXPCAPID) (PXPCAPID_0_0_0_CFG) — Offset 90h

Туре	Size	Offset	Default
PCI	8 bit	[B:0, D:3, F:0] + 90h	10h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	10h RO	CAPABILITY_ID: Assigned by PCI-SIG for PCI Express capability ID.

3.1.3 PCI Express Capability Register (PXPCAP) (PXPCAP_0_0_0_CFG) - Offset 92h

Туре	Size	Offset	Default
PCI	16 bit	[B:0, D:3, F:0] + 92h	0092h

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description	
15:14	0h RO	Reserved	
13:9	00h RO	INTERRUPT_MESSAGE_NUMBER: Applies to Root Ports. This field indicates the interrupt message number that is generated for Power Management/Hot Plug/Bandwidth-change events. When there are more than one MSI interrupt Number allocated for the root port MSI interrupts, this register field is required to contain the offset between the base Message Data and the MSI Message that is generated when there are these change interrupts. IIO assigns the first vector for these change events and so this field is set to 0.	
8	0h RW/O	SLOT_IMPLEMENTED: 1: Indicates that the PCI Express link associated with the port is connected to a slot. 0: Indicates no slot is connected to this port. Notes: This bit is set by BIOS.	
7:4	9h RO/V	DEVICE_PORT_TYPE: Device type is Root Complex Integrated Endpoint for DMI.	
3:0	2h RW/O	CAPABILITY_VERSION: PCI Express Capability is Compliant with Version 2.0 of the PCI Express Spec.	



3.1.4 Performance Control and Status 0 (PERFCTRLSTS_0) (PERFCTRLSTS_0_0_0_0_CFG) - Offset 180h

Туре	Size	Offset	Default
PCI	32 bit	[B:0, D:3, F:0] + 180h	00183011h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
31:21	0h RO	Reserved	
20:16	18h RW	OUTSTANDING_REQUESTS_GEN1: Number of outstanding RFOs and non-posted requests from a given PCIe port. This register controls the number of outstanding inbound non-posted requests - I/O, Config, Memory - (maximum length of these requests is a single 64B cacheline) that a Gen1 PCI Express downstream port can have. This register provides the value for the port when it is operating in Gen1 mode and for a link width of x4. BIOS programs this register also specifies the number of RFOs that can be kept outstanding on IDI for a given port. The link speed of the port can change during a PCI Express Hot-Plug event and the port must use the appropriate multiplier. A value of 1 indicates one outstanding pre-allocated request, 2 indicates two outstanding pre-allocated requests, and so on. If software programs a value greater than the buffer size the DMA engine supports, then the maximum hardware supported value is used. Current BIOS recommendation is to leave this field at it's default value.	
15:14	0h RO	Reserved	
13:8	30h RW	OUTSTANDING_REQUESTS_GEN2: Number of outstanding RFOs and non-posted requests from a given PCIe port. This register controls the number of outstanding inbound non-posted requests - I/O, Config, Memory - (maximum length of these requests is a single 64B cacheline) that a Gen2 PCI Express downstream port can have. This register provides the value for the port when it is operating in Gen2 mode and for a link width of x4. BIOS programs this register based on the read latency to main memory. This register also specifies the number of RFOs that can be kept outstanding on IDI for a given port. The link speed of the port can change during a PCI Express Hot-Plug event and the port must use the appropriate multiplier. A value of 1 indicates one outstanding pre-allocated request, 2 indicates two outstanding pre-allocated requests, and so on. If software programs a value greater than the buffer size the DMA engine supports, then the maximum hardware supported value is used. Current BIOS recommendation is to leave this field at it's default value.	
7:6	0h RO	Reserved	
5	0h RW	FORCENOSNOOP:	
4	1h RW	READ_STREAM_INTERLEAVE_SIZE:	



Bit Range	Default & Access	Field Name (ID): Description
3	0h RW	NOSNOOPOPWREN:
2	0h RW	NOSNOOPOPRDEN:
1	0h RW	READ_PASSING_READ_DISABLE: Disable reads bypassing other reads
0	1h RW	READ_STREAM_POLICY:



3.1.5 CPUBUS NO (CPUBUSNO) – Offset 104h

Configs the PECI services to be able correctly access devices on the fabric post enumeration for PCIConfig and EndPointCOnfig Commands. The set of registers maps the pre-enumerated value used internally by the PECI Service to the allocated bus number. These register mimic the configuration done in Mesh and UBOX.

Туре	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 104h	03020100h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	03h RW	ROOTBUSS3: Base Root bus for Physical Mesh2IOSF Stack 3
23:16	02h RW	ROOTBUSS2: Base Root bus for Physical Mesh2IOSF Stack 2
15:8	01h RW	ROOTBUSS1: Base Root bus for Physical Mesh2IOSF Stack 1
7:0	00h RW	ROOTBUSSO: Base Root bus for Physical Mesh2IOSF Stack 0

3.1.6 CPUBUS NO 1 (CPUBUSNO1) – Offset 108h

Configs the PECI services to be able correctly access devices on the fabric post enumeration for PCIConfig and EndPointCOnfig Commands. The set of registers maps the pre-enumerated value used internally by the PECI Service to the allocated bus number. These register mimic the configuration done in Mesh and UBOX.

Туре	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 108h	07060504h

BIOS Access	SMM Access	OS Access	
RW	R	R	

Bit Range	Default & Access	Field Name (ID): Description
31:24	07h RW	ROOTBUSS7: Base Root bus for Physical Mesh2IOSF Stack 7
23:16	06h RW	ROOTBUSS6: Base Root bus for Physical Mesh2IOSF Stack 6
15:8	05h RW	ROOTBUSS5: Base Root bus for Physical Mesh2IOSF Stack 5
7:0	04h RW	ROOTBUSS4: Base Root bus for Physical Mesh2IOSF Stack 4



3.1.7 CPUBUS NO 2 (CPUBUSNO2) – Offset 10Ch

Configs the PECI services to be able correctly access devices on the fabric post enumeration for PCIConfig and EndPointCOnfig Commands. The set of registers maps the pre-enumerated value used internally by the PECI Service to the allocated bus number. These register mimic the configuration done in Mesh and UBOX.

Туре	Size	Offset	Default
PCI	32 bit	[B:0, D:2, F:0] + 10Ch	0E0D0908h

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	0Eh RW	ROOTBUSU1: UBOX U1
23:16	0Dh RW	ROOTBUSU0: UBOX U0
15:8	09h RW	ROOTBUSS9: Base Root bus for Physical Mesh2IOSF Stack 9
7:0	08h RW	ROOTBUSS8: Base Root bus for Physical Mesh2IOSF Stack 8



4 Intel UPI Registers

The Intel UPI module is the coherent communication interface between processors. The Ice Lake processor implements either 2 or 3 Intel UPI links based on processor type.

4.0.1 KTI misc stat (KTIMISCSTAT) – Offset D4h

Туре	Size	Offset	Default
PCI	32 bit	[B:30, D:2, F:0] + D4h	0000003h

Register Level Access:

BIOS Access	SMM Access	OS Access	Policy Group ID
R	R	R	1

Bit Range	Default & Access	Field Name (ID): Description
31:3	0h RO	Reserved
2:0	3h RO/V	KTI_RATE: This reflects the supported current Intel UPI rate setting into the PLL. 100 - 9.6 GT/s 101 - 10.4 GT/s 110 - 11.2 GT/s other - Reserved

4.0.2 KTI lp0 (KTILP0) – Offset 94h

ktilp0



T

T

T

1

T

Туре	Size	Offset	Default
PCI	32 bit	[B:30, D:2, F:1] + 94h	0900000h

Register Level Access:

BIOS Access	SMM Access	OS Access	Policy Group ID
R	R	R	1

Bit Range	Default & Access	Field Name (ID): Description
31:24	09h RO/V	Reserved
23:20	0h RO	Reserved
19:16	0h RO/V	BASE_NODEID: Parameter bits from peer agent. Cleared on any LL initialization. The NodeID of the sending socket.
15	0h RO/V	Reserved
14	0h RO/V	Reserved
13	0h RO	Reserved
12:8	00h RO/V	SENDING_PORT: Parameter bits from peer agent. Cleared on any LL initialization. The processor die port number of the sending port. Legal values are 0-2.
7:4	0h RO/V	Reserved
3:0	0h RO/V	. <u>Reserved</u>

4.0.3 KTI lp1 (KTILP1) — Offset 98hBit definitions are the same as PCIE_RSVD0_0, offset 44h.KTI pcsts (KTIPCSTS) — Offset 120h



Туре	Size	Offset	Default
PCI	32 bit	[B:30, D:2, F:1] + 120h	00000000h

Register Level Access:

T

T

BIOS Access	SMM Access	OS Access
RW	RW	R

Bit Range	Default & Access	Field Name (ID): Description
31:5	0000000h RW	Reserved
4	0h RW	LL_STATUS_VALID: Bit indicates valid training status logged from PCode to BIOS.
3:0	0h RW	Reserved

4.0.4 Vendor ID (VID_1) - Offset 0h

PCI Vendor ID Register

Туре	Size	Offset	Default
PCI	16 bit	[B:30, D:2, F:2] + 0h	8086h

Register Level Access:

BIOS Access	SMM Access	OS Access	Policy Group ID
R	R	R	1

Bit Range	Default & Access	Field Name (ID): Description
15:0	8086h RO	VENDOR_IDENTIFICATION_NUMBER: The value is assigned by PCI-SIG to Intel.

4.0.5 Device ID (DID_1) - Offset 2h

PCI Device Identification Number



Туре	Size	Offset	Default
PCI	16 bit	[B:30, D:2, F:2] + 2h	3442h

Register Level Access:

BIOS Access	SMM Access	OS Access	Policy Group ID
R	R	R	1

Bit Range	Default & Access	Field Name (ID): Description
15:0	3442h RO	DEVICE_IDENTIFICATION_NUMBER:

Table 4-1. State Tracker Encoding

Bits	Stae Name	Bits	State Name
5′b0_0000	RestP	5'b1_0010	Loopback.Marker Master
5′b0_0001	RestS	5'b1_0011	Loopback.Marker Slave
5′b0_0010	RestC	5'b1_0000	Loopback.Pattern Master
5′b0_0011	RxDtect	5'b1_0001	Loopback.Pattern Slave
5′b0_0100	TxClib	5′b1_1111	Compliance
5′b0_0101	TxDtect		
5′b0_0110	Poling		
5′b0_1000	Conig.LinkWidth		
5′b0_1001	Conig.FlitLock		
5′b0_1010	L1 / (eserved if L1 not suppored)		
5′b0_1100	L0e		
5′b0_1101	LOp		
5′b0_1110	Lc		
5′b0_1111	L		
Others	Rserved	Others	Reserved



Integrated Memory Controller (IMC) Registers

The Ice Lake Server implements four Integrated Memory Controllers (IMC). Each IMC is capable of controlling two DDR4 memory channels, 2 DIMMs per channel.

The IMC Host Configuration Space Registers are implemented in Bus: B(30), Device: 12-13-14-15, Function: 0

Device 12 applies to IMC 0

5

- Device 13 applies to IMC 1
- Device 14 applies to IMC 2
- Device 15 applies to IMC 3

5.1 TADWAYNESS_0 – Offset 20DD4h

There are total of 8 TAD ranges

Note for mirroring configuration:

For 1-way interleave, channel 0-2 mirror pair: target list = $\langle 0, 2, x, x \rangle$, TAD ways = 00

For 1-way interleave, channel 1-3 mirror pair: target list = <1,3,x,x>, TAD ways = 00

For 2-way interleave, 0-2 mirror pair and 1-3 mirror pair: target list = <0,1,2,3>, TAD ways = 01

For 1-way interleave, lockstep + mirroring, target list = <0,2,x,x>, TAD ways = 00



Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20DD4h	0000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
31:6	0000000h RW	TAD_LIMIT: highest address of the range in system address space, 64MB granularity, i.e. TADRANGLIMIT[51:26]. In case of 3 channel interleave, exclude the address not accessed by the system, even if the address is valid in memory.	
5:3	0h RW	CHN_LID: ChnLID: channel logical ID. logical channel for channel interleave.	
2:0	0h RW	TARGET_LID:TargetLID: target logical ID, a.k.a., base_offsetThe position of the MC in the socket interleave list in the SAD rule that maps to thisTAD rule.If 1-way interleaved to one MC, base_offset is 0.If 2-way interleaved across two MCs, base_offset is either 0 or 1.4-way, 0 through 3. 8-way, 0 through 7.	

5.1.1 TADWAYNESS_1 – Offset 20DD8h

Note: Bit definitions are the same as TADWAYNESS_0, offset 20DD4h.

5.1.2 TADWAYNESS_2 – Offset 20DDCh

Note: Bit definitions are the same as TADWAYNESS_0, offset 20DD4h.

5.1.3 TADWAYNESS_3 – Offset 20DE0h

Note: Bit definitions are the same as TADWAYNESS_0, offset 20DD4h.

5.1.4 TADWAYNESS_4 – Offset 20DE4h

Note: Bit definitions are the same as TADWAYNESS_0, offset 20DD4h.

5.1.5 TADWAYNESS_5 – Offset 20DE8h

- *Note:* Bit definitions are the same as TADWAYNESS_0, offset 20DD4h.
- 5.1.6 TADWAYNESS_6 Offset 20DECh
- *Note:* Bit definitions are the same as TADWAYNESS_0, offset 20DD4h.

5.1.7 TADWAYNESS_7 – Offset 20DF0h

Note: Bit definitions are the same as TADWAYNESS_0, offset 20DD4h.



5.1.8 RCOMP_TIMER – Offset 20DFCh

Defines the time from IO starting to run RCOMP evaluation until RCOMP results are definitely ready. This counter is added in order to keep determinism of the process if operated in different modes

The register also indicates that first RCOMP has been done - required by BIOS

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20DFCh	0B000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/V	RCOMP_IN_PROGRESS: rcomp is in progress.
30	0h RW	UNUSED: Unused. Intel reserved
29:22	2Ch RW	Reserved
21	0h RW	IGNORE_MDLL_LOCKED_BIT: ignore mdll locked bit.
20	0h RW	NO_MDLL_FSM_OVERRIDE: no mdll fsm override.
19:18	0h RO	Reserved
17	0h RW	Reserved
16	0h RW/V	FIRST_RCOMP_DONE: This is a status bit that indicates the first RCOMP has been completed. It is cleared on reset, and set by MC HW when the first RCOMP is completed. Bios should wait until this bit is set before executing any DDR command
15:0	0000h RW	COUNT: Unused spare bits. There is no logic behind this field

5.1.9 SPAREADDRESSLO – Offset 20E24h

Always points to the lower address for the next sparing operation. This register will not be affected by the M2M access to the spare source rank during the M2M window.



Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20E24h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000 h RW/V	RANKADD: Always points to the lower address for the next sparing operation. This register will not be affected by the M2M access to the spare source rank during the M2M window.

5.1.10 SCRUBCTL – Offset 20E28h

This register contains the Scrub control parameters and status.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20E28h	0000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW	SCRUB_EN: Scrub Enable when set.
30	0h RW	STOP_ON_CMPL: Stop patrol scrub at end of memory range. This mode is meant to be used as part of memory migration flow. SMI is signaled by default.
29	0h RW/V	PTL_CMPL: When stop_on_cmpl is enabled, patrol will stop at the end of the address range and set this bit. Patrol will resume from beginning of address range when this bit or stop_on_cmpl is cleared by BIOS and patrol scrub is still enabled by scrub_en.
28	0h RW	STOP_ON_ERR: Reserved
27	0h RW/V	PTL_STOPPED: Reserved
26	0h RW/V	SCRUBISSUED: When Set, the scrub address registers contain the last scrub address issued
25	0h RW	ISSUEONCE: When Set, the patrol scrub engine will issue the address in the scrub address registers only once and stop. Software is responsible to turn off periodic patrol before issuing patrol once. The patrol interval in PMA should be set to 0 in issue once mode. No cross product of patrol once with PkgC is allowed.



Bit Range	Default & Access	Field Name (ID): Description
24	0h RW/V	STARTSCRUB: When Set, the Patrol scrub engine will start from the address in the scrub address registers. Once the scrub is issued this bit is reset.
23	0h RW	STOP_ON_RANK: Reserved
22:0	0h RO	Reserved

5.1.11 SCRUBADDRESSLO – Offset 20E2Ch

This register contains part of the address of the last patrol scrub request issued. When running memtest, the failing address is logged in this register on memtest errors. Software can write the next address to be scrubbed into this register. The STARTSCRUB bit will then trigger the specified address to be scrubbed. Patrol scrubs must be disabled to reliably write this register.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20E2Ch	0000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:0	0000000 h RW/V	RANKADD: Contains the rank address or bits 37:6 of the system address of the last scrub issued. Can be written to specify the next scrub address with STARTSCRUB. Base system address in scrubaddress2lo/hi also need to be programmed in system address mode for the programmed address to work properly. In system address mode, scrubaddresshi.ptl_sa_mode must be cleared to 0 and then set back to 1 after STARTSCRUB is set for address written to take effect. RESTRICTIONS: Patrol Scrubs must be disabled when writing to this field. Bit 0 of this register maps to bit 6 of address. When target or channel XOR is enabled, address in this register wouldn't or shouldn't be the true system address, the system address with XOR applied. Error logging on patrol scrub error will reflect the true system address though.

5.1.12 SCRUBADDRESSHI – Offset 20E30h

This register pair contains part of the address of the last patrol scrub request issued. Software can write the next address into this register. Scrubbing must be disabled to reliably read and write this register. The STARTSCRUB bit will then trigger the specified address to be scrubbed.

(intel)

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20E30h	80008000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	Reserved
30:28	0h RW	Reserved
27:25	0h RW	Reserved
24:22	0h RW/V	Reserved
21:19	0h RW/V	CHNL: Can be written to specify the next scrub address with STARTSCRUB. This register is updated with channel address of the last scrub address issued. RESTRICTIONS: Patrol Scrubs must be disabled when writing to this field. Only used for legacy (non system address) patrol mode.
18:16	0h RW/V	RANK: Contains the physical rank ID of the last scrub issued. Can be written to specify the next scrub address with STARTSCRUB. RESTRICTION: Patrol Scrubs must be disabled when writing to this field. Only used for legacy (non system address) patrol mode.
15	1h RW/V	MIRR_PRI: Contains the primary indication when mirroring is enabled. Can be written to specify the next scrub address. RESTRICTION: Patrol Scrubs must be disabled when writing to this field. Only used for system address patrol mode.
14:0	0000h RW/V	RANKADDHI: Contains bits 52:38 of the system address of the last scrub issued. Can be written to specify the next scrub address with STARTSCRUB. Base system address in scrubaddress2lo/hi also need to be programmed in system address mode for the programmed address to work properly. scrubaddresshi.ptl_sa_mode must be cleared to 0 and then set back to 1 after STARTSCRUB is set for address written to take effect. RESTRICTIONS: Patrol Scrubs must be disabled when writing to this field. Only used system address patrol mode.

5.1.13 RASENABLES – Offset 20E3Ch

RAS Enables Register


Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20E3Ch	00000090h

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description	
31:10	0h RO	Reserved	
9:8	0h RW	Reserved: Keep default value.	
7:6	2h RW	CH1_MIRROR: The secondary channel number when the primary channel is channel 1 for mirroring. This is used by patrol logic.	
5:4	1h RW	CH0_MIRROR: The secondary channel number when the primary channel is channel 0 for mirroring. This is used by patrol logic.	
3:1	0h RO	Reserved	
0	0h RW	MIRROREN: Mirror mode enable. The channel mapping must be set up before this bit will have an effect on IMC operation. This changes the error policy.	

5.1.14 SMISPARECTL – Offset 20E40h

System Management Interrupt and Spare control register.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20E40h	0000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
31:18	0h RO	Reserved	
17	0h RW	INTRPT_SEL_PIN: Enable pin signaling. When set the interrupt is signaled via the err[0] pin to get the attention of a BMC.	



Bit Range	Default & Access	Field Name (ID): Description
16	0h RW	INTRPT_SEL_CMCI: (CMCI used as a proxy for NMI signaling). Set to enable NMI signaling. Clear to disable NMI signaling. If both NMI and SMI enable bits are set then only SMI is sent.
15	0h RW	INTRPT_SEL_SMI: SMI enable. Set to enable SMi signaling. Clear to disable SMI signaling.
14:0	0h RO	Reserved

5.1.15 LEAKY_BUCKET_CFG - Offset 20E44h

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20E44h	00000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW



Bit Range	Default & Access	Field Name (ID): Description	
31:12	0h RO	Reserved	
11:6	00h RW	LEAKY_BKT_CFG_HI: This is the higher order bit select mask of the two hot encoding threshold. The value of this field specify the bit position of the mask: 00h: reserved 01h: LEAKY_BUCKET_CNTR_LO bit 1, i.e. bit 12 of the full 53b counter 1Fh: LEAKY_BUCKET_CNTR_LO bit 31, i.e. bit 42 of the full 53b counter 20h: LEAKY_BUCKET_CNTR_HI bit 0, i.e. bit 43 of the full 53b counter 29h: LEAKY_BUCKET_CNTR_HI bit 9, i.e. bit 52 of the full 53b counter 2Ah - 3F: reserved When both counter bits selected by the LEAKY_BKT_CFG_HI and LEAKY_BKT_CFG_LO are set, the 53b leaky bucket counter will be reset and the logic will generate a LEAK pulse to decrement the correctable error counter by 1. MRC BIOS must program this register to any non-zero value before switching to NORMAL mode.	
5:0	00h RW	LEAKY_BKT_CFG_LO: This is the lower order bit select mask of the two hot encoding threshold. The value of this field specify the bit position of the mask: 00h: reserved 01h: LEAKY_BUCKET_CNTR_LO bit 1, i.e. bit 12 of the full 53b counter 1Fh: LEAKY_BUCKET_CNTR_LO bit 31, i.e. bit 42 of the full 53b counter 20h: LEAKY_BUCKET_CNTR_HI bit 0, i.e. bit 43 of the full 53b counter 29h: LEAKY_BUCKET_CNTR_HI bit 9, i.e. bit 52 of the full 53b counter 2Ah - 3F: reserved When both counter bits selected by the LEAKY_BKT_CFG_HI and LEAKY_BKT_CFG_LO are set, the 53b leaky bucket counter will be reset and the logic will generate a LEAK pulse to decrement the correctable error counter by 1. MRC BIOS must program this register to any non-zero value before switching to NORMAL mode.	

LEAKY_BUCKET_CNTR_LO — Offset 20E48h

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20E48h	0000000h

Register Level Access:

BIOS Access	SMM Access	OS Access	
RW	RW	RW	

Bit Range	Default & Access	Field Name (ID): Description	
		LEAKY_BKT_CNTR_LO:	
31:0	00000000h RW/V	This is the lower half of the leaky bucket counter. The full counter is actually a 53b HCLK counter. There is a least significant 11b of the 53b counter is not captured in CSR. The carry strobe from the not-shown least significant 11b counter will trigger this 42b counter pair to count. The 42b counter-pair is compared with the two-hot encoding threshold specified by the LEAKY_BUCKET_CFG_HI and LEAKY_BUCKET_CFG_LO pair. When the counter bits specified by the LEAKY_BUCKET_CFG_HI and LEAKY_BUCKET_CFG_HI and LEAKY_BUCKET_CFG_HI and LEAKY_BUCKET_CFG_HI and LEAKY_BUCKET_CFG_IO are both set, the 53b counter is reset and the leaky bucket logic will generate a LEAK strobe last for 1 HCLK.	

I

T



I

I

5.1.16 LEAKY_BUCKET_CNTR_HI - Offset 20E4Ch

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20E4Ch	0000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:10	0h RO	Reserved
9:0	000h RW/V	LEAKY_BKT_CNTR_HI: This is the upper half of the leaky bucket counter. The full counter is actually a 53b HCLK counter. There is a least significant 11b of the 53b counter is not captured in CSR. The carry strobe from the not-shown least significant 11b counter will trigger this 42b counter pair to count. The 42b counter-pair is compared with the two-hot encoding threshold specified by the LEAKY_BUCKET_CFG_HI and LEAKY_BUCKET_CFG_LO pair. When the counter bits specified by the LEAKY_BUCKET_CFG_LO are both set, the 53b counter is reset and the leaky bucket logic will generate a LEAK strobe last for 1 HCLK.

5.1.17 SPARING_PATROL_STATUS - Offset 20E7Ch

Formerly ssrstatus.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20E7Ch	0000000h

BIOS Access	SMM Access	OS Access	
RW	RW	RW	

Bit Range	Default & Access	Field Name (ID): Description
31:3	0h RO	Reserved



Bit Range	Default & Access	Field Name (ID): Description
2	0h RW/1C/V	PATROL_COMPLETE: All memory has been scrubbed. Hardware sets this bit each time the patrol engine steps through all memory locations. If software wants to monitor 0 to 1 transition after the bit has been set, the software will need to clear the bit by writing a one to clear this bit in order to distinguish the next patrol scrub completion. Clearing the bit will not affect the patrol scrub operation. Note, when mirroring is enabled, this bit will be set to 1 after either primary or secondary address scrubbing is done. If software clears this bit to observe 0 to 1 transition, the transition will happen twice to get full address scrubbed.
1	0h RW/V	COPY_COMPLETE: Sparing copy operation complete. Set by hardware once operation is complete. This bit is cleared by hardware when a new operation is enabled.
0	0h RW/V	COPY_IN_PROGRESS: This bit indicates that the sparing copy operation is in progress. This bit is set by hardware once the sparing copy has started. It is cleared by hardware once the copy operation is complete or fails.

5.1.18 MC_INIT_STATE_G — Offset 20EE8h

This register defines the DDR reset pin value, DCLK enable, refresh enable and bits indicating the MRC status

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20EE8h	00000122h

BIOS Access	SMM Access	OS Access	
RW	RW	RW	

Bit Range	Default & Access	Field Name (ID): Description	
31:10	0h RO	Reserved	
9	0h RW/P	CS_OE_EN: Reserved	
8	1h RW/P	SAFE_SR: This bit indicates if it is safe to keep the MC in SR during MC-reset. If it is clear when reset occurs, it means that the reset is without warning and the DDR-reset should be asserted. If set when reset occurs, it indicates that DDR is already in SR and it can keep it this way. This bit can also indicate MRC if reset without warning has occurred, and if it has, cold-reset flow should be selected Note to MRC BIOS: clear this bit at MRC entry.	
7	0h RW	MRC_DONE: MRC done.	
6	0h RO	Reserved	
5	1h RW	RESET_IO: DDR IO reset In order to reset the IO this bit has to be set for 20 DCLKs and then cleared. Setting this bit will reset the DDRIO receive FIFO registers only. It is required in some of the training steps.	
4:3	0h RO	Reserved	



Bit Range	Default & Access	Field Name (ID): Description
2	0h RW	DCLK_ENABLE: Reserved
1	1h RW	DDR_RESET: Reserved
0	0h RW/P	PU_MRC_DONE: This bit should be set to 1 by BIOS as soon as the MRC has successfully completed and all required information (for example, - training) is in the Bios flash. It indicates that first MRC has been completed

5.1.19 SPAREINTERVAL – Offset 20EF0h

Defines the interval between normal and sparing operations. Interval is defined in dclk.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20EF0h	03200C80h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:29	0h RO	Reserved
28:16	0320h RW	NUMSPARE: Sparing operation duration. System requests will be blocked during this interval and only sparing copy operations will be serviced. This needs to be an even number is ADDDC sparing mode. The value needs to be 32 or less in rank sparing mode.
15:0	0C80h RW	NORMOPDUR: Normal operation duration. System requests will be serviced during this interval.



5.1.20 MCMTR – Offset 20EF8h

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 20EF8h	0000010h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
31:30	0h RO	Reserved	
29	0h RO/V	HBM_MC_MODE: This bit specifies which kind of MC this is, HBM or DDR. When 1, the MC is an HBM MC. When 0, it is a DDR MC (this includes both DDR4 and DDRT).	
28:26	0h RO	Reserved	
25	0h RW	Reserved	
24:23	0h RO	Reserved	
22	0h RW/P	Reserved	
21	0h RW	Reserved	
20	0h RW	Reserved	
19	0h RW	Reserved	
18	0h RW/P	CHN_DISABLE: Channel disable control. When set, the channel is disabled. Note: Message Channel may not work if all channels are set to disable in this field.	
17:12	0h RO	Reserved	
11:10	0h RW	Reserved	
9	0h RW/P	Reserved	
8	0h RW	NORMAL: 0: Training mode 1: Normal Mode	
7	0h RW	Reserved	
6	0h RW	Reserved	
5	0h RW	Reserved	
4	1h RW	Reserved	



Bit Range	Default & Access	Field Name (ID): Description
3	0h RW/V/P	DIR_EN: Directory Enable. Read-Only (RO) with 0 value if not supported. This bit is not used by the design. M2M controls directory enable behavior.
2	0h RW/V/P	ECC_EN: ECC enable.
1	0h RO	Reserved
0	0h RW/P	CLOSE_PG: Use close page address mapping if set; otherwise, open page.

PXPCAP – Offset 21808h

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 21808h	00910010h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
31:30	0h RO	Reserved	
29:25	00h RO	INTERRUPT_MESSAGE_NUMBER: N/A for this device	
24	0h RO	SLOT_IMPLEMENTED: N/A for integrated endpoints	
23:20	9h RO	DEVICE_PORT_TYPE: Device type is Root Complex Integrated Endpoint	
19:16	1h RO	CAPABILITY_VERSION: PCI Express Capability is Compliant with Version 1.0 of the PCI Express Spec. Note: This capability structure is not compliant with Versions beyond 1.0, since they require additional capability registers to be reserved. The only purpose for this capability structure is to make enhanced configuration space available. Minimizing the size of this structure is accomplished by reporting version 1.0 compliancy and reporting that this is an integrated root port device. As such, only three Dwords of configuration space are required for this structure.	
15:8	00h RO	NEXT_PTR: Pointer to the next capability. Set to 0 to indicate there are no more capability structures.	
7:0	10h RO	CAPABILITY_ID: Provides the PCI Express capability ID assigned by PCI-SIG.	

5.1.21 PXPENHCAP – Offset 2180Ch

This field points to the next Capability in extended configuration space.



Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 2180Ch	00000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
31:20	000h RO	NEXT_CAPABILITY_OFFSET: Next capability offset.	
19:16	0h RO	CAPABILITY_VERSION: Indicates there are no capability structures in the enhanced configuration space.	
15:0	0000h RO	CAPABILITY_ID: Indicates there are no capability structures in the enhanced configuration space.	

5.1.22 CHN_TEMP_CFG — Offset 22404h

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22404h	DB0003FFh

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	1h RW	OLTT_EN: Enable OLTT temperature tracking
30	1h RW	Reserved
29	0h RW	Reserved
28	1h RW	Reserved
27	1h RW	BW_LIMIT_THRT_EN: Bandwith limit throttle enable.
26	0h RO	Reserved
25:24	3h RW	Reserved
23:16	00h RW	THRT_EXT: Max number of throttled transactions to be issued during BWLIMITTF due to externally asserted MEMHOT#.



Bit Range	Default & Access	Field Name (ID): Description
15	0h RW	THRT_ALLOW_ISOCH: When this bit is zero, MC will lower CKE during Thermal Throttling, and ISOCH is blocked. When this bit is one, MC will NOT lower CKE during Thermal Throttling, and ISOCH will be allowed based on bandwidth throttling setting. However, setting this bit means more power is consumed due to CKE being asserted during thermal or power throttling.
14	0h RW	
13:11	0h RO	Reserved
10:0	3FFh RW	BW_LIMIT_TF: BW Throttle Window Size in DCLK/8 (a value of 1 results in 8 DCLKs)

5.1.23 CHN_TEMP_STAT – Offset 22408h

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22408h	0000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:2	0h RO	Reserved
1	0h RW/1C/V	EV_ASRT_DIMM1: Event Asserted on DIMM ID 1
0	0h RW/1C/V	EV_ASRT_DIMM0: Event Asserted on DIMM ID 0

5.1.24 DIMM_TEMP_THRT_LMT_0 - Offset 2241Ch

All three THRT_CRIT, THRT_HI and THRT_MID are per DIMM BW limit, i.e. all activities (ACT, READ, WRITE) from all ranks within a DIMM are tracked together in one DIMM activity counter.

These throttle limits for hi and crit are also used during scalable memory buffer thermal throttling.



Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 2241Ch	00000FFFh

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:24	0h RO	Reserved
23:16	00h RW	THRT_CRIT: Max number of throttled transactions (ACT, READ, WRITE) to be issued during BWLIMITTF.
15:8	0Fh RW	THRT_HI: Max number of throttled transactions (ACT, READ, WRITE) to be issued during BWLIMITTF.
7:0	FFh RW	THRT_MID: Max number of throttled transactions (ACT, READ, WRITE) to be issued during BWLIMITTF.

Note: DIMM_TEMP_THRT_LMT_1 — Offset 22420hBit definitions are the same as DIMM_TEMP_THRT_LMT_0, offset 2241Ch.

5.1.25 DIMM_TEMP_EV_OFST_0 - Offset 22424h

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22424h	00000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:20	0h RO	Reserved
19	0h RW	Reserved
18	0h RW	Reserved
17	0h RW	Reserved
16	0h RW	Reserved
15	0h RW	Reserved



Bit Range	Default & Access	Field Name (ID): Description
14	0h RW	EV_THRTMID_TEMPLO: Initiate THRTMID on TEMPLO
13	0h RW	EV_2X_REF_EN: Enable 2X refresh when memory temperature is above TEMP_TWOXREF
12	0h RW	EV_MH_TEMPHI_EN: Assert MEMHOT# Event on TEMPHI
11	0h RW	EV_MH_TEMPMID_EN: Assert MEMHOT# Event on TEMPMID
10	0h RW	EV_MH_TEMPLO_EN: Assert MEMHOT# Event on TEMPLO
9:4	0h RO	Reserved
3:0	0h RW	DIMM_TEMP_OFFSET: Bit 3-0 - Temperature Offset Register

5.1.26 DIMMTEMPSTAT_1 - Offset 22430h

т	уре	Size	Offset	Default
М	IMIO	32 bit	MEM0_BAR + 22430h	0000055h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	Reserved
7:0	55h RW/V	DIMM_TEMP: Current DIMM Temperature for thermal throttling

5.1.27 DIMMTEMPSTAT_0 - Offset 224D4h

Note: Bit definitions are the same as DIMMTEMPSTAT_1, offset 22430h.

DIMM_TEMP_TH_0 — Offset 224E0h



Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 224E0h	005F5A55h

I.

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:27	0h RO	Reserved
26:24	0h RW	TEMP_THRT_HYST: Positive going Threshold Hysteresis Value. Set to 00h if sensor does not support positive-going threshold hysteresis. This value is subtracted from TEMP_THRT_XX to determine the point where the asserted status for that threshold will clear.
23:16	5Fh RW	TEMP_HI: TCase threshold at which to Initiate THRTCRIT and assert THERMTRIP# valid range: 32 - 127 in degree C. Note: the default value is listed in decimal. FF: Disabled Others: reserved. TEMP_HI should be programmed so it is greater than TEMP_MID
15:8	5Ah RW	TEMP_MID: TCase threshold at which to Initiate THRTHI and assert valid range: 32 - 127 in degree C. Note: the default value is listed in decimal. FF: Disabled Others: reserved. TEMP_MID should be programmed so it is less than TEMP_HI
7:0	55h RW	TEMP_LO: TCase threshold at which to initiate THRTMID and initiate Interrupt (MEMHOT#). Note: the default value is listed in decimal.valid range: 32 - 127 in degree C. FF: Disabled Others: reserved. TEMP_LO should be programmed so it is less than TEMP_MID

5.1.28 DIMM_TEMP_TH_1 - Offset 224E4h

Note: Bit definitions are the same as DIMM_TEMP_TH_0, offset 224E0h.

5.1.29 DIMM_TEMP_EV_OFST_1 - Offset 22510h

generated by critter 20_0_0x144



Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22510h	00000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:17	0h RO	Reserved
16	0h RW	Reserved
15	0h RW	Reserved
14	0h RW	EV_THRTMID_TEMPLO: Initiate THRTMID on TEMPLO
13	0h RW	EV_2X_REF_EN: Enable 2X refresh when memory temperature is above TEMP_TWOXREF
12	0h RW	EV_MH_TEMPHI_EN: Assert MEMHOT# Event on TEMPHI
11	0h RW	EV_MH_TEMPMID_EN: Assert MEMHOT# Event on TEMPMID
10	0h RW	EV_MH_TEMPLO_EN: Assert MEMHOT# Event on TEMPLO
9:4	0h RO	Reserved
3:0	0h RW	DIMM_TEMP_OFFSET: Bit 3-0 - Temperature Offset Register

5.1.30 CORRERRCNT_0 - Offset 22C18h

Per Rank corrected error counters.



Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22C18h	00000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/1C/V/ P	OVERFLOW_1: The corrected error count for this rank has been overflowed. Once set it can only be cleared via a write from BIOS.
30:16	0000h RW/V	COR_ERR_CNT_1: The corrected error count for this rank. Hardware automatically clear this field when the corresponding OVERFLOW_x bit is changing from 0 to 1. This counter increments in number of cacheline accesses - not by codewords. On a read access, if either of the codewords or both codewords have a corrected error, this counter increments by 1.
15	0h RW/1C/V/ P	OVERFLOW_0: The corrected error count for this rank has been overflowed. Once set it can only be cleared via a write from BIOS.
14:0	0000h RW/V	COR_ERR_CNT_0: The corrected error count for this rank. Hardware automatically clear this field when the corresponding OVERFLOW_x bit is changing from 0 to 1. This counter increments in number of cacheline accesses - not by codewords. On a read access, if either of the codewords or both codewords have a corrected error, this counter increments by 1.

5.1.31 CORRERRCNT_1 - Offset 22C1Ch

Per Rank corrected error counters.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22C1Ch	00000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/1C/V/ P	OVERFLOW_3: The corrected error count has crested over the limit for this rank. Once set it can only be cleared via a write from BIOS.
30:16	0000h RW/V	COR_ERR_CNT_3: The corrected error count for this rank.
15	0h RW/1C/V/ P	OVERFLOW_2: The corrected error count has crested over the limit for this rank. Once set it can only be cleared via a write from BIOS.
14:0	0000h RW/V	COR_ERR_CNT_2: The corrected error count for this rank.



5.1.32 CORRERRCNT_2 - Offset 22C20h

Per Rank corrected error counters.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22C20h	0000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/1C/V/ P	OVERFLOW_5: The corrected error count has crested over the limit for this rank. Once set it can only be cleared via a write from BIOS.
30:16	0000h RW/V	COR_ERR_CNT_5: The corrected error count for this rank.
15	0h RW/1C/V/ P	OVERFLOW_4: The corrected error count has crested over the limit for this rank. Once set it can only be cleared via a write from BIOS.
14:0	0000h RW/V	COR_ERR_CNT_4: The corrected error count for this rank.

5.1.33 CORRERRCNT_3 - Offset 22C24h

Per Rank corrected error counters.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22C24h	0000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RW/1C/V/ P	OVERFLOW_7: The corrected error count has crested over the limit for this rank. Once set it can only be cleared via a write from BIOS.
30:16	0000h RW/V	COR_ERR_CNT_7: The corrected error count for this rank.
15	0h RW/1C/V/ P	OVERFLOW_6: The corrected error count has crested over the limit for this rank. Once set it can only be cleared via a write from BIOS.
14:0	0000h RW/V	COR_ERR_CNT_6: The corrected error count for this rank.



5.1.34 CORRERRTHRSHLD_0 – Offset 22C30h

This register holds the per rank corrected error thresholding value.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22C30h	7FFF7FFFh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	Reserved
30:16	7FFFh RW	COR_ERR_TH_1: The corrected error threshold for this rank that will be compared to the per rank corrected error counter.
15	0h RO	Reserved
14:0	7FFFh RW	COR_ERR_TH_0: The corrected error threshold for this rank that will be compared to the per rank corrected error counter.

5.1.35 CORRERRTHRSHLD_1 - Offset 22C34h

This register holds the per rank corrected error thresholding value.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22C34h	7FFF7FFFh

BIOS Access	SMM Access	OS Access	
RW	RW	RW	

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	Reserved
30:16	7FFFh RW	COR_ERR_TH_3: The corrected error threshold for this rank that will be compared to the per rank corrected error counter.
15	0h RO	Reserved
14:0	7FFFh RW	COR_ERR_TH_2: The corrected error threshold for this rank that will be compared to the per rank corrected error counter.



5.1.36 CORRERRTHRSHLD_2 – Offset 22C38h

This register holds the per rank corrected error thresholding value.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22C38h	7FFF7FFFh

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	Reserved
30:16	7FFFh RW	COR_ERR_TH_5: The corrected error threshold for this rank that will be compared to the per rank corrected error counter.
15	0h RO	Reserved
14:0	7FFFh RW	COR_ERR_TH_4: The corrected error threshold for this rank that will be compared to the per rank corrected error counter.

5.1.37 CORRERRTHRSHLD_3 – Offset 22C3Ch

This register holds the per rank corrected error thresholding value.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22C3Ch	7FFF7FFFh

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31	0h RO	Reserved
30:16	7FFFh RW	COR_ERR_TH_7: The corrected error threshold for this rank that will be compared to the per rank corrected error counter.
15	0h RO	Reserved
14:0	7FFFh RW	COR_ERR_TH_6: The corrected error threshold for this rank that will be compared to the per rank corrected error counter.



5.1.38 CORRERRORSTATUS – Offset 22C50h

Per rank corrected error status. These bits are reset by BIOS.

Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22C50h	00003000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	Reserved
7:0	00h RW/1C/V	ERR_OVERFLOW_STAT: This 8 bit field is the per rank error over-threshold status bits. The organization is as follows: Bit 0 : Rank 0 Bit 1 : Rank 1 Bit 2 : Rank 2 Bit 3 : Rank 3 Bit 4 : Rank 4 Bit 5 : Rank 5 Bit 6 : Rank 6 Bit 7 : Rank 7 Note: The register tracks which rank has reached or exceeded the corresponding CORRERRTHRSHLD threshold settings.

5.1.39 PLUS1_RANK0 – Offset 22D28h

This register specifies the current ECC configuration for each rank, including portions of the rank that participates in an ADDDC region and its buddy.

Туре	Size	Offset	Default
MMIO	8 bit	MEM0_BAR + 22D28h	00h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
7:6	0h RO	Reserved	
5:0	00h RW	FAILDEVICE: This field specifies the failed device to be mapped out for this rank in +1 mode, including portion of the rank (and its buddy) that is participating in an ADDDC region. Set by BIOS at the beginning of a SDDC sparing flow. Valid Range is decimal 0-17 to indicate which device has failed.	



5.1.40	PLUS1_RANK1 — Offset 22D2Ch
Note:	Bit definitions are the same as PLUS1_RANK0, offset 22D28h.
5.1.41	PLUS1_RANK2 — Offset 22D30h
Note:	Bit definitions are the same as PLUS1_RANK0, offset 22D28h.
5.1.42	PLUS1_RANK3 — Offset 22D34h
Note:	Bit definitions are the same as PLUS1_RANK0, offset 22D28h.
5.1.43	PLUS1_RANK4 — Offset 22D38h
Note:	Bit definitions are the same as PLUS1_RANK0, offset 22D28h.
5.1.44	PLUS1_RANK5 — Offset 22D3Ch
Note:	Bit definitions are the same as PLUS1_RANK0, offset 22D28h.
5.1.45	PLUS1_RANK6 — Offset 22D40h
Note:	Bit definitions are the same as PLUS1_RANK0, offset 22D28h.
5.1.46	PLUS1_RANK7 — Offset 22D44h

- *Note:* Bit definitions are the same as PLUS1_RANK0, offset 22D28h.
- 5.1.47 EAKY_BKT_2ND_CNTR_REG Offset 22E78h

Secondary Leaky Bucket Counter Limit



Туре	Size	Offset	Default
MMIO	32 bit	MEM0_BAR + 22E78h	0000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
31:16	0000h RW	LEAKY_BKT_2ND_CNTR_LIMIT: Secondary Leaky Bucket Counter Limit (2b per DIMM). This register defines secondary leaky bucket counter limit for all 8 logical ranks within channel. The counter logic will generate the secondary LEAK pulse to decrement the ranks correctable error counter by 1 when the corresponding rank leaky bucket rank counter roll over at the predefined counter limit. The counter increment at the primary leak pulse from the LEAKY_BUCKET_CNTR_LO and LEAKY_BUCKET_CNTR_HI logic. Bit[31:30]: Rank 7 Secondary Leaky Bucket Counter Limit Bit[29:28]: Rank 6 Secondary Leaky Bucket Counter Limit Bit[27:26]: Rank 5 Secondary Leaky Bucket Counter Limit Bit[25:24]: Rank 4 Secondary Leaky Bucket Counter Limit Bit[21:20]: Rank 2 Secondary Leaky Bucket Counter Limit Bit[19:18]: Rank 1 Secondary Leaky Bucket Counter Limit Bit[19:18]: Rank 1 Secondary Leaky Bucket Counter Limit Bit[17:16]: Rank 0 Secondary Leaky Bucket Counter Limit The value of the limit is defined as the following: 0: the LEAK pulse is generated one DCLK after the primary LEAK pulse is asserted. 1: the LEAK pulse is generated one DCLK after the counter roll over at 1. 2: the LEAK pulse is generated one DCLK after the counter roll over at 2. 3: the LEAK pulse is generated one DCLK after the counter roll over at 3.	
15:0	0000h RW/V	LEAKY_BKT_2ND_CNTR: Per rank secondary leaky bucket counter (2b per rank) bit 15:14: rank 7 secondary leaky bucket counter bit 13:12: rank 6 secondary leaky bucket counter bit 11:10: rank 5 secondary leaky bucket counter bit 9:8: rank 4 secondary leaky bucket counter bit 7:6: rank 3 secondary leaky bucket counter bit 5:4: rank 2 secondary leaky bucket counter bit 3:2: rank 1 secondary leaky bucket counter bit 1:0: rank 0 secondary leaky bucket counter	

§





6 Power Control Unit (PCU) Registers

The Power Control Unit (PCU) is a dedicated controller that provides power and thermal management for the processor. The PCU implements a PECI interface for out-of-band management.

6.1 PCU Registers

6.1.1 Vendor ID (VID_0_11_0_CFG) - Offset 0h

PCI Vendor ID Register

Туре	Size	Offset	Default
PCI	16 bit	[B:30, D:11, F:0] + 0h	8086h

Register Level Access:

BIOS Access	SMM Access	OS Access	
R	R	R	

Bit Range	Default & Access	Field Name (ID): Description	
15.0	8086h	VENDOR_IDENTIFICATION_NUMBER:	
15:0	RO	The value is assigned by PCI-SIG to Intel.	

6.1.2 Device ID (DID_0_11_0_CFG) - Offset 2h

PCI Device Identification Number

Туре	Size	Offset	Default
PCI	16 bit	[B:30, D:11, F:0] + 2h	3448h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description	
15:0	3448h RO/V	DEVICE_IDENTIFICATION_NUMBER: The value is assigned by each IP/function owner as a unique identifier.	

6.1.3 SMB COMMAND CFG (SMB_CMD_CFG) - Offset 80h

This register contains the fields used by SW to configure SMBus command.

(intel)

Туре	Size	Offset	Default
PCI	32 bit	[B:30, D:11, F:0] + 80h	20005000h

BIOS Access	SMM Access	OS Access
RW	RW	R

Bit Range	Default & Access	Field Name (ID): Description	
31:30	0h RO	Reserved	
29	1h RW/V/P	DIF CAUVED: 0 = Overrides Clock signal to low. 1 = Clock signal is released high, allowing normal operation of CMD. Toggling this bit can be used to budge the port out of a stuck state. Software can write this bit to 0 and the SMB_SOFT_RST to 1 to force hung SMBus controller and the SMB slaves to idle state without using power good reset or warm reset. Note: software needs to set the SMB_CKOVRD back to 1 after 35ms in order to force slave devices to time-out in case there is any pending transaction. The corresponding SMB_STATUS_CFG.SMB_SBE error status bit may be set if there was such pending transaction time-out (non-graceful termination). If the pending transaction was a write operation, the slave device content may be corrupted by this clock override operation. A subsequent SMB command will automatically clear the SMB_SBE. Alternatively, if SMBUS error recovery is enabled, the SMBus time-out control timer will start when ckovrd is pulled low. When the time-out control timer expires, the SMB_CKOVRD# will de-assert, i.e. return to 1 value and clear the SMB_SBE=0.	
28	0h RW	SMB_DIS_WRT: Disables SMBus Write. Writing a 0 to this bit enables CMD write bit to be set to 1; Writing a 1 forces SMB_WRT[0] bit to be always 0, i.e. disabling SMBus write. SMBus Read is not affected. SMBus Write Pointer Update Command is not affected. Either SMB_DIS_WRT=1 or the FUSE_DIS_SMBUS_WRT=1 will disable the SMBus Write Capability. Note: SMBus write commands are silently converted to SMBus read commands. No error is logged or signaled.	
27	0h RW	Reserved	
26	0h RW	Reserved	
25	0h RW	Reserved	
24	0h RW	SMB_SOFT_RST: SMBus software reset strobe to gracefully terminate the pending transaction (after ACK) and keep the SMB controller from issuing any transaction until this bit is cleared. If the slave device is hung, software can write this bit to 1 and the SMB_CKOVRD to 0 (for more than 35ms) to force the hung SMB slaves to time-out and put the controller in idle state without using power good reset or warm reset. Note: software needs to set the SMB_CKOVRD back to 1 after 35ms in order to force slave devices to time-out in case there is any pending transaction. The corresponding SMB_STATUS_CFG.SMB_SBE error status bit may be set if there was such pending transaction time-out (non-graceful termination). If the pending transaction was a write operation, the slave device content may be corrupted by this clock override operation. A subsequent SMBus command will automatically clear the SMB_SBE. The IMC H/W will perform SMBus time-out (if the SMB_SBE_EN=1). Software should simply clear the SMB_SDE and SMB_SOFT_RST sequentially after writing the SMB_CKOVRD=0 and SMB_SOFT_RST=1 (asserting clock override and perform graceful txn termination). Hardware will automatically de-assert the SMB_CKOVRD (update to 1) after the pre-configured 35ms/65ms time-out period.	
23:21	0h RO	Reserved	



Bit Range	Default & Access	Field Name (ID): Description	
20	0h RW	SMB_TSOD_POLL_EN: Enables hardware-based TSOD Polling. This field does not affect the current SMBus transaction in flight. A change takes effect once the bus is no longer busy. If BIOS/ BMC would like to use SMBus, it must first suspend TSOD polling by setting this field to 0 and wait for the bus to become free. When BIOS/BMC is done with the bus, it must resume TSOD polling by setting this field to 1.	
19	0h RW/V	SMB_CMD_TRIGGER: CMD trigger. After setting this bit to 1, the SMBus master will issue the SMBus command using the other fields written in SMB_CMD_CFG. Note: Hardware will reset this bit when the SMBus command is being started.	
18	0h RW/P	SMB_PNTR_SEL: When set, enables SMBus pointer based access; otherwise, the random access protocol is used. Hardware based TSOD polling will also use this bit to enable the pointer word read. Important Note: Hardware based TSOD polling can be configured with pointer based access. If software manually issue SMBus transaction to other address, i.e. changing the pointer in the slave device, it is software's responsibility to restore the pointer in each TSOD before returning to hardware based TSOD polling while keeping the SMB_PNTR_SEL=1.	
17	0h RW/P	SMB_WORD_ACCESS: Enables Word Access. The SMBus controller performs SMBus word (2 bytes) access when set; otherwise, it performs a byte access.	
16:15	0h RW/P	SMB_WRT: These bits select SMBus Read/Write operation. Bit[16:15]=00 for SMBus Read, Bit[16:15]=01 for SMBus Write, Bit[16:15]=11 for writing to the pointer register. Bit[16:15]=10 is an illegal combination. Note 1: smb_pntr_sel and smb_word_access are ignored when writing to the pointer register. Note 2: smb_dis_wrt will NOT disable WrtPntr update command.	
14:11	Ah RW/P	SMB_DTI: This field specifies the device type identifier. Only devices with these device-type wi respond to commands: 0011 specifies TSOD. 1010 specifies EEPROMs. 0110 specifie a write-protect operation for an EEPROM. 1110 specifies a 4-channel I2C-bus multiplexer. Other identifiers can be specified to target non-EEPROM devices on the SMBus. Note: IMC based hardware TSOD polling uses hard coded DTI. Changing thi field has no effect on the hardware based TSOD polling.	
10:8	0h RW/P	SMB_SA: SMBus Slave Address. This field identifies the DIMM SPD/TSOD to be accessed.	
7:0	00h RW/P	SMB_BA: This field identifies the bus transaction address to be accessed. Note: in WORD access, 23:16 specifies 2B access address. In Byte access, 23:16 specified 1B access address. Also known as the command code in SMBus terms.	

6.1.4 SMB STATUS CFG (SMB_STATUS_CFG) - Offset 84h

This register contains the fields to monitor the status

(intel)

Туре	Size	Offset	Default
PCI	32 bit	[B:30, D:11, F:0] + 84h	0000000h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description	
31:21	0h RO	Reserved	
20	0h RO/V	TSOD_POLL_EN: Indicates if TSOD Polling is enabled on SMBus.	
19	0h RO	Reserved	
18:16	0h RO/V	LAST_BRANCH_CFG: Captures the SMBus mux branch configuration in the last issued BIOS/BMC or HW command to SMBUS mux. BMC can use this information to determine which DIMM on which branch has caused an error on SMBus. Bit 2 is defined as the mux enable bit. Bits [1:0] are defined as the branch to be selected.	
15	0h RO	Reserved	
14:11	0h RO/V	LAST_DTI: Captures the Device Type Identified code specified in the last issued BIOS/BMC or HW command. BMC can use this information to determine if an error on SMBus is caused by SMBus mux or by a DIMM.	
10:8	0h RO/V	TSOD_SA: Captures the slave address of the last TSOD device polled.	
7:4	0h RO	Reserved	
3	0h RO/V	SMB_WOD: Write Operation Done. This bit is set by iMC when a SMBus Write command has been completed on the SMBus. It is cleared by iMC when a subsequent SMBus Write command is issued	
2	0h RO/V	SMB_RDO: Read Data Valid. This bit is set by iMC when the Data field of this register receives read data from the SPD/TSOD after completion of an SMBus read command. It is cleared by iMC when a subsequent SMBus read command is issued.	
1	0h RO/V	SMB_SBE: SMBus Error. This bit is set by H/W if an SMBus transaction (including the TSOD polling or message channel initiated SMBus access) that does not complete successfully (non-Ack has been received from slave at expected Ack slot of the transferNote: Once SMB_SBE bit is set, H/W stops issuing hardware initiated TSOD polling SMBUS transactions until the SMB_SBE is cleared. H/W will not increment the SMB_STATUS_CFG.TSOD_SA or update SMB_STATUS_CFG.last_dti or SMB_STATUS_CFG.last_branch_config until the SMB_SBE is cleared. Manual SMBus command interface is not affected, i.e. new command issue will clear the SMB_SBE.	
0	0h RO/V/P	SMB_BUSY: SMBus Busy state. This bit is set by iMC while an SMBus/I2C command (including TSOD command issued from IMC hardware) is executing. Any transaction that is completed normally or gracefully will clear this bit automatically. By setting the SMB_SOFT_RST will also clear this bit. This register bit is sticky across reset so any surprise reset during pending SMBus operation will sustain the bit assertion across surprised warm-reset. BIOS reset handler can read this bit before issuing any SMBus transaction to determine whether a slave device may need special care to force the slave to idle state (e.g. via clock override toggling (SMB_CKOVRD) and/or via induced time-out by asserting SMB_CKOVRD for 25-35ms).	



6.1.5 SMB DATA CFG (SMB_DATA_CFG) - Offset 88h

This register contains read and write data from SMBUS

Туре	Size	Offset	Default
PCI	32 bit	[B:30, D:11, F:0] + 88h	00000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	R

Bit Range	Default & Access	Field Name (ID): Description	
31:16	0000h RW/P	SMB_WDATA: Write Data: Holds data to be written by SPDW commands. Since TSOD/EEPROM are I2C devices and the byte order is MSByte first in a word write, writing of I2C using word write should use SMB_WDATA[15:8]=12C_MSB and SMB_WDATA[7:0]=I2C_LSB. If writing of I2C using byte write, the SMB_WDATA[15:8]=don't care; SMB_WDATA[7:0]=write_byte. If we have a SMB slave connected on the bus, writing of the SMBus slave using word write should use SMB_WDATA[15:8]=SMB_LSB and SMB_WDATA[7:0]=SMB_MSB. It is software responsibility to figure out the byte order of the slave access.	
15:0	0000h RO/V	SMB_RDATA: Read Data. Holds data read from SMBus Read commands. Since TSOD/EEPROM are I2C devices and the byte order is MSByte first in a word read, reading of I2C using word read should return SMB_RDATA[15:8]=I2C_MSB and SMB_RDATA[7:0]=I2C_LSB. If reading of I2C using byte read, the SMB_RDATA[15:8]=don`t care; SMB_RDATA[7:0]=read_byte. If we have a SMB slave connected on the bus, reading of the SMBus slave using word read should return SMB_RDATA[15:8]=SMB_LSB and SMB_RDATA[7:0]=SMB_MSB. If the software is not sure whether the target is I2C or SMBus slave, please use byte access.	

6.1.6 SMB PERIOD CFG (SMB_PERIOD_CFG) - Offset 90h



Туре	Size	Offset	Default
PCI	32 bit	[B:30, D:11, F:0] + 90h	000003E8h

BIOS Access	SMM Access	OS Access
RW	RW	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	0h RO	Reserved
23:16	00h RW/P	Reserved
15:0	03E8h RW/P	SMB_CLK_PRD: This field specifies SMBUS Clock period in number of FXCLK. It is recommend to program an even value in this field since the hardware is simply doing a right shift for the divided by 2 operation. The value of this field must be less than or equal to 0x2710 (i.e. 10KHz or faster). Note the 100KHz SMB_CLK_PRD default value is calculated based on 100 MHz FXCLK. Time high and time low of SMBUS clock is defined as: TIME_HIGH = SMB_CLK_PRD/2 - SMB_CLK_OFFSET + SMB_CLK_RISE_OFFSET, TIME_LOW = SMB_CLK_PRD/2 + SMB_CLK_OFFSET - SMB_CLK_RISE_OFFSET

6.1.7 SMB TSOD POLL RATE CFG (SMB_TSOD_POLL_RATE_CFG) - Offset 98h

Configuration for SMBUS TSOD poll rate between consecutive TSOD accesses to the TSOD devices on the same SMBus segment

Туре	Size	Offset	Default
PCI	32 bit	[B:30, D:11, F:0] + 98h	0003E800h

Register Level Access:

BIOS Access	SMM Access	OS Access	
RW	RW	R	

Bit Range	Default & Access	Field Name (ID): Description
31:18	0h RO	Reserved
17:0	3E800h RW/P	SMB_TSOD_POLL_RATE: TSOD poll rate configuration between consecutive TSOD accesses to the TSOD devices on the same SMBUS port. This field specifies the TSOD poll rate in number of 500ns per CNFG_500_NANOSEC register field definition. The value of this field must be greater than 0x2400 (poll rate is less than ~217 TSODs polled per second). Instance 0 is shared between SMBUS ports 0 and 1, and instance 1 is used for SMBUS port 2 (MCP).

6.1.8 Vendor ID (VID_0_11_2_CFG) - Offset 0h

PCI Vendor ID Register



Туре	Size	Offset	Default
PCI	16 bit	[B:30, D:11, F:2] + 0h	8086h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	8086h RO	VENDOR_IDENTIFICATION_NUMBER: The value is assigned by PCI-SIG to Intel.

6.1.9 Device ID (DID_0_11_2_CFG) - Offset 2h

PCI Device Identification Number

Туре	Size	Offset	Default
PCI	16 bit	[B:30, D:11, F:2] + 2h	344Bh

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15:0	344Bh RO	DEVICE_IDENTIFICATION_NUMBER:

6.1.10 PCI Command (PCICMD_0_11_2_CFG) — Offset 4h

PCI Command Register



Туре	Size	Offset	Default
PCI	16 bit	[B:30, D:11, F:2] + 4h	0000h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description	
15:11	0h RO	Reserved	
10	0h RO	INTX_DISABLE: N/A for these devices	
9	0h RO	FAST_BACK_TO_BACK_ENABLE: Not applicable to PCI Express and is hardwired to 0	
8	0h RO	SERR_ENABLE: This bit has no impact on error reporting from these devices	
7	0h RO	IDSEL_STEPPING_WAIT_CYCLE_CONTROL: Not applicable to internal devices. Hardwired to 0.	
6	0h RO	PARITY_ERROR_RESPONSE: This bit has no impact on error reporting from these devices	
5	0h RO	VGA_PALETTE_SNOOP_ENABLE: Not applicable to internal devices. Hardwired to 0.	
4	0h RO	MEMORY_WRITE_AND_INVALIDATE_ENABLE: Not applicable to internal devices. Hardwired to 0.	
3	0h RO	SPECIAL_CYCLE_ENABLE: Not applicable. Hardwired to 0.	
2	0h RO	BUS_MASTER_ENABLE: Hardwired to 0 since these devices do not generate any transactions	
1	0h RO	MEMORY_SPACE_ENABLE: Hardwired to 0 since these devices do not decode any memory BARs	
0	0h RO	IO_SPACE_ENABLE: Hardwired to 0 since these devices do not decode any IO BARs	

6.1.11 PCI Status (PCISTS_0_11_2_CFG) - Offset 6h

PCI Status Register



Туре	Size	Offset	Default
PCI	16 bit	[B:30, D:11, F:2] + 6h	0000h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
15	0h RO	DETECTED_PARITY_ERROR: This bit is set when the device receives a packet on the primary side with an uncorrectable data error (including a packet with poison bit set) or an uncorrectable address/control parity error. The setting of this bit is regardless of the Parity Error Response bit (PERRE) in the PCICMD register.
14	0h RO	SIGNALED_SYSTEM_ERROR: Hardwired to 0
13	0h RO	RECEIVED_MASTER_ABORT: Hardwired to 0
12	0h RO	RECEIVED_TARGET_ABORT: Hardwired to 0
11	0h RO	SIGNALED_TARGET_ABORT: Hardwired to 0
10:9	0h RO	DEVSEL_TIMING: Not applicable to PCI Express. Hardwired to 0.
8	0h RO	MASTER_DATA_PARITY_ERROR: Hardwired to 0
7	0h RO	FAST_BACK_TO_BACK: Not applicable to PCI Express. Hardwired to 0.
6	0h RO	Reserved
5	0h RO	X66MHZ_CAPABLE: Not applicable to PCI Express. Hardwired to 0.
4	0h RO	CAPABILITIES_LIST: This bit indicates the presence of a capabilities list structure. When set to 1, indicates the register at 34h provides an offset into the function.
3	0h RO	INTX_STATUS: Reflects the state of the INTA# signal at the input of the enable/disable circuit. This bit is set by HW to 1 when the INTA# is asserted. This bit is reset by HW to 0 after the interrupt is cleared (independent of the state of the Interrupt Disable bit in the PCICMD register). Hardwired to 0 on the processor
2:0	0h RO	Reserved

6.1.12 Revision ID and Class Code Register (RID_CCR_0_11_2_CFG) — Offset 8h

PCIe header Revision ID register and Class Code register



Туре	Size	Offset	Default
PCI	32 bit	[B:30, D:11, F:2] + 8h	08800000h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	08h RO	BASE_CLASS: Base class code
23:16	80h RO	SUB_CLASS: Sub class code
15:8	00h RO	REGISTER_LEVEL_PROGRAMMING_INTERFACE: Register Level Programming Interface
7:0	00h RO/V	REVISION_ID: Reflects the Uncore Revision ID after reset. Reflects the Compatibility Revision ID if BIOS updates.

6.1.13 Cache Line Size Register (CLSR_0_11_2_CFG) – Offset Ch

PCI Cache Line Size Register

Туре	Size	Offset	Default
PCI	8 bit	[B:30, D:11, F:2] + Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	CACHELINE_SIZE: Size of Cacheline

6.1.14 PCI Latency Timer (PLAT_0_11_2_CFG) — Offset Dh

PCI Latency Timer



Туре	Size	Offset	Default
PCI	8 bit	[B:30, D:11, F:2] + Dh	00h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	PRIMARY_LATENCY_TIMER: Not applicable to PCI Express. Hardwired to 00h.

6.1.15 Header Type (HDR_0_11_2_CFG) — Offset Eh

PCI Header Type

Туре	Size	Offset	Default
PCI	8 bit	[B:30, D:11, F:2] + Eh	80h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7	1h RO	MULTI_FUNCTION_DEVICE: This bit defaults to 1b since all these devices are multi-function
6:0	00h RO	CONFIGURATION_LAYOUT: Type 0 header

6.1.16 Built In Self Test (BIST_0_11_2_CFG) - Offset Fh

PCI BIST Register

Туре	Size	Offset	Default
PCI	8 bit	[B:30, D:11, F:2] + Fh	00h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	BIST_TESTS: Not supported. Hardwired to 00h



6.1.17 Subsystem Vendor ID (SVID_0_11_2_CFG) - Offset 2Ch

Subsystem Vendor ID Register

Туре	Size	Offset	Default
PCI	16 bit	[B:30, D:11, F:2] + 2Ch	8086h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
15:0	8086h RW/O	SUBSYSTEM_VENDOR_IDENTIFICATION_NUMBER: The default value specifies Intel but can be set to any value once after reset.	

6.1.18 Subsystem ID (SDID_0_11_2_CFG) - Offset 2Eh

Subsystem ID Register

Туре	Size	Offset	Default
PCI	16 bit	[B:30, D:11, F:2] + 2Eh	0000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
15:0	0000h RW/O	SUBSYSTEM_IDENTIFICATION_NUMBER: Assigned by the subsystem vendor to uniquely identify the subsystem	

6.1.19 Capability Pointer (CAPPTR_0_11_2_CFG) - Offset 34h

PCI Capability Pointer Register



Туре	Size	Offset	Default
PCI	8 bit	[B:30, D:11, F:2] + 34h	00h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
7:0	00h RO	CAPABILITY_POINTER: Points to the first capability structure for the device which is the PCIe capability.

6.1.20 Interrupt Line (INTL_0_11_2_CFG) - Offset 3Ch

PCI Interrupt Line Register

Туре	Size	Offset	Default
PCI	8 bit	[B:30, D:11, F:2] + 3Ch	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description	
7.0	00h	INTERRUPT_LINE:	
7.0	RO	N/A for these devices	

6.1.21 Interrupt Pin (INTPIN_0_11_2_CFG) — Offset 3Dh

PCI Interrupt Pin Register

Туре	Size	Offset	Default
PCI	8 bit	[B:30, D:11, F:2] + 3Dh	00h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description	
7:0	00h RO	INTERRUPT_PIN: N/A since these devices do not generate any interrupt on their own	



6.1.22 Minimum Grant (MINGNT_0_11_2_CFG) — Offset 3Eh

PCI Min Grant Register

Туре	Size	Offset	Default
PCI	8 bit	[B:30, D:11, F:2] + 3Eh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description	
7:0	00h RO	MGV: The device does not burst as a PCI compliant master.	

6.1.23 Maximum Latency (MAXLAT_0_11_2_CFG) — Offset 3Fh

PCI Max Latency Register

Туре	Size	Offset	Default
PCI	8 bit	[B:30, D:11, F:2] + 3Fh	00h

Register Level Access:

BIOS Access	SMM Access	OS Access	
R	R	R	

Bit Range	Default & Access	Field Name (ID): Description	
7:0	00h RO	MLV: The device has no specific requirements for how often it needs to access the PCI bus.	

6.1.24 PACKAGE ENERGY STATUS (PACKAGE_ENERGY_STATUS_CFG) — Offset 90h

Package energy consumed by the entire CPU (including IA, Uncore). The counter will wrap around and continue counting when it reaches its limit.

Туре	Size	Scope	Default
MSR	<u>32 bit</u>	Package	<u>00000000h</u>

<u>Bit</u> Range	Default & Access	Field Name (ID): Description	
<u>31:0</u>	00000000 h RO_V	Energy Value (DATA): Energy Value	


6.1.25 PLATFORM INFO (PLATFORM_INFO_CFG) - Offset A8h

Platform Info Register contains read-only package-level ratio information.

Туре	Size	Offset	Default
PCI	64 bit	[B:31, D:30, F:0] + A8h	00080000F0010000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
63	0h RO/V/P	Reserved
62:61	0h RO	Reserved
60	0h RO/V	TIO_EN: Not used on servers. Reserved.
59	0h RO/V	SMM_SUPOVR_STATE_LOCK_ENABLE: Indicates to BIOS that the SMM_SUPOVR_STATE_LOCK MSR can be setup
58	0h RO/V	SXP_2LM_EN: Not used on servers. Reserved.
57	0h RO/V	EDRAM_EN: Not used on servers. Reserved.
56	0h RO/V	PUSHPATCHEN: Not used on servers. Reserved.
55:48	08h RO/V	MIN_OPERATING_RATIO: Indicates the minimum ratio supported by the processor (in units of 100MHz)
47:40	00h RO/V/P	MAX_EFFICIENCY_RATIO: Contains the maximum efficiency ratio in units of 100 MHz. System BIOS must use this as the minimum ratio in the _PSS table.
39	0h RO	Reserved
38	0h RO/V/P	ASA_ENABLE: 1 indicates ASA is enabled
37	0h RO/V/P	TIMED_MWAIT_ENABLE: 0 indicates that Timed MWAIT feature is not available, 1 indicates that Timed MWAIT feature is available.
36	0h RO/V	PEG2DMIDIS_EN: Not used on servers. Reserved.
35	0h RO/V/P	PFAT_ENABLE: 0 indicates that the Platform Firmware Armoring Technology (PFAT) feature is not available, 1 indicates that the PFAT feature is available.
34:33	0h RO/V/P	Reserved
32	0h RO/V/P	LPM_SUPPORT: When set to 1, indicates that BIOS may program IA32_PERF_CTL to levels below the max efficiency ratio down to Minimum Ratio bits [55:48]. 0 - Low Power mode not supported 1 - Low Power mode supported



Bit Range	Default & Access	Field Name (ID): Description	
		CPUID FAULTING EN:	
31	1h RO/V/P	When set to 1, indicates that the processor supports raising a #GP if CPUID is executed when not in SMM and the CPL > 0. When this bit is set, it indicates that (140h) MISC_FEATURE_ENABLES bit 0 can be written by a VMM.	
		PRG_TJ_OFFSET_EN:	
	415	Programmable TJ Offset Enable.	
30 Ih RO/V/P		When set to 1, indicates that the TCC Activation Offset field in IA32_TEMPERATURE_TARGET MSR is valid and programmable. When set to 0, indicates its not programmable. When this bit is 0, an attempt to write to MSR_TEMPERATURE_TARGET bits [27:24] will result in a GP fault.	
		PRG TDP LIM_EN:	
29	1h RO/V/P	Programmable TDP Limits for Turbo Mode. When set to 1, indicates that TDP Limits for Turbo mode are programmable, and when set to 0, indicates TDP Limits for Turbo mode are not programmable. When this bit is 0, an attempt to write to PP0_POWER_LIMIT, PP1_POWER_LIMIT and PACKAGE_POWER_LIMIT MSR will result in a GP fault.	
28	1h RO/V	PRG_TURBO_RATIO_EN: Programmable Turbo Ratios per number of Active Cores	
	Λh	SAMPLE PART:	
27	RO/V/P	Indicates if this part is a sample	
26:25	0h RO	Reserved	
	<u>A</u> L	OCVOLT_OVRD_AVAIL:	
24		0b Indicates that the part does not support Voltage override overclocking.	
	KU/ V	1b Indicates that the part supports Voltage override overclocking.	
	0h	PPIN_CAP:	
23	RO/V	When set to 1, indicates that this part supports the Protected Processor Inventory Number (PPIN) feature.	
22:18	0h RO	Reserved	
	0h	TAPUNLOCK:	
1/	RO/V	Reserved	
	1h	SMM SAVE CAP:	
16	RO/V	When set to 1 indicates this feature exists and is configured by SMM_SAVE_CONTROL	
		MAX_NON_TURBO_LIM_RATIO:	
		Contains the max non-turbo ratio.	
	00h	Contains the max non-turbo ratio. This is the ratio of the frequency that invariant TSC runs at. Frequency = ratio $*$ 100 MHz.	
15:8	RO/V/P	Note: The Maximum Non-Turbo Ratio is adjusted to the flexible limit ratio (as specified in the FLEX_RATIO MSR 194h FLEX_RATIO field bits [15:8]) if flexible limit is enabled (by setting the FLEX_RATIO MSR 194h FLEX_EN field bit[16]=1.	
		is reported in this field.	
7:0	0h RO	Reserved	

6.1.26 PACKAGE TEMPERATURE (PACKAGE_TEMPERATURE_CFG) - Offset C8h

Package temperature in degrees (C). This field is updated by FW.



Туре	Size	Offset	Default
PCI	32 bit	[B:31, D:30, F:0] + C8h	00000000h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	Reserved
7:0	00h RO/V	DATA: Package temperature in degrees (C).

6.1.27 BIOS MAILBOX DATA (BIOS_MAILBOX_DATA_CFG) — Offset 8Ch

Data register for the BIOS-to-PCODE mailbox. This mailbox is implemented as a means for accessing statistics and implementing PCODE patches.

This register is used in conjunction with BIOS_MAILBOX_INTERFACE.

Туре	Size	Offset	Default
PCI	32 bit	[B:31, D:30, F:1] + 8Ch	0000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000 h RW/V	DATA: This field contains the data associated with specific commands.

6.1.28 BIOS MAILBOX INTERFACE (BIOS_MAILBOX_INTERFACE_CFG) — Offset 90h

Control and Status register for the BIOS-to-PCODE mailbox. This mailbox is implemented as a means for accessing statistics and implementing PCODE patches.

This register is used in conjunction with BIOS_MAILBOX_DATA.



Туре	Size	Offset	Default
PCI	32 bit	[B:31, D:30, F:1] + 90h	0000000h

BIOS Access	SMM Access	OS Access	
RW	RW	R	

Bit Range	Default & Access	Field Name (ID): Description	
31	0h RW/1S/V	RUN_BUSY: SW may write to the two mailbox registers only when RUN_BUSY is cleared (0b). Setting RUN_BUSY to 1b will create a Fast Path event. After setting this bit, SW will poll this bit until it is cleared. PCODE will clear RUN_BUSY after updating the mailbox registers with the result and error code.	
30:29	0h RO	Reserved	
28:8	000000h RW/V	ADDR: This field contains the address associated with specific commands.	
7:0	00h RW/V	COMMAND: This field contains the SW request command or the PCODE response code, depend on the setting of RUN_BUSY.	

6.1.29 OS MAILBOX DATA (OS_MAILBOX_DATA_CFG) - Offset A0h

Data register for the OS-to-PCODE mailbox. This mailbox is implemented as a means for accessing statistics and implementing PCODE patches. This register is used in conjunction with OS_MAILBOX_INTERFACE_CFG.

Note: Bit definitions are the same as BIOS_MAILBOX_DATA_CFG, offset 8Ch.

6.1.30 OS MAILBOX INTERFACE (OS_MAILBOX_INTERFACE_CFG) — Offset A4h

Control and Status register for the OS-to-PCODE mailbox. This mailbox is implemented as a means for accessing statistics and implementing PCODE patches. This register is used in conjunction with OS_MAILBOX_DATA_CFG.



Туре	Size	Offset	Default
PCI	32 bit	[B:31, D:30, F:1] + A4h	00000000h

BIOS Access	SMM Access	OS Access
RW	RW	RW

Bit Range	Default & Access	Field Name (ID): Description	
31	0h RW/1S/V	RUN_BUSY: OS may write to the two mailbox registers only when RUN_BUSY is cleared (0b). Setting RUN_BUSY to 1b will create a Fast Path event. After setting this bit, OS will poll this bit until it is cleared. PCODE will clear RUN_BUSY after updating the mailbox registers with the result and error code.	
30:29	0h RO	Reserved	
28:8	000000h RW/V	ADDR: This field contains the address associated with specific commands.	
7:0	00h RW/V	COMMAND: This field contains the OS request command or the PCODE response code, depending on the setting of RUN_BUSY.	

6.1.31 DRAM ENERGY STATUS (DRAM_ENERGY_STATUS_CFG) - Offset 80h

DRAM energy consumed by all the DIMMS in all the Channels. The counter will wrap around and continue counting when it reaches its limit.

ENERGY_UNIT for DRAM domain is 15.3uJ.

The data is updated by PCODE and is Read Only for all SW.

6.1.32 PACKAGE OVERFLOW STATUS (PACKAGE_RAPL_PERF_STATUS) - Offset 88h

This register is used to report Package Power limit violations.

Туре	Size	Offset	Default
PCI	32 bit	[B:31, D:30, F:2] + 88h	0000000h

Register Level Access:

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000 h RO/V	PWR_LIMIT_THROTTLE_CTR:



6.1.33 DRAM POWER INFORMATION (DRAM_POWER_INFO_CFG) — Offset A8h

Power allowed for DRAM

Туре	Size	Offset	Default
PCI	64 bit	[B:31, D:30, F:2] + A8h	0028025800780118h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	R	R

Bit Range	Default & Access	Field Name (ID): Description	
63	0h RW/L	LOCK:	
62:55	0h RO	Reserved	
54:48	28h RW/L	DRAM_MAX_WIN:	
47	0h RO	Reserved	
46:32	0258h RW/L	DRAM_MAX_PWR: The maximal power setting allowed for DRAM.	
31	0h RO	Reserved	
30:16	0078h RW/L	DRAM_MIN_PWR: The minimal power setting allowed for DRAM.	
15	0h RO	Reserved	
14:0	0118h RW/L	DRAM_TDP: The Spec power allowed for DRAM. The TDP setting is typical (not guaranteed).	

6.1.34 MEM TRML TEMPERATURE REPORT (MEM_TRML_TEMPERATURE_REPORT[0]) - Offset C8h

This register is used to report the thermal status of the memory. The channel max temperature field is used to report the maximal temperature of all ranks.



Туре	Size	Offset	Default
PCI	32 bit	[B:31, D:30, F:2] + C8h	00000000h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:24	0h RO	Reserved
23:16	00h RO/V	CHANNEL2_MAX_TEMPERATURE: Temperature in Degrees (C).
15:8	00h RO/V	CHANNEL1_MAX_TEMPERATURE: Temperature in Degrees (C).
7:0	00h RO/V	CHANNELO_MAX_TEMPERATURE: Temperature in Degrees (C).

6.1.35 MEM TRML TEMPERATURE REPORT (MEM_TRML_TEMPERATURE_REPORT[1]) - Offset CCh

This register is used to report the thermal status of the memory. The channel max temperature field is used to report the maximal temperature of all ranks.

Note: Bit definitions are the same as MEM_TRML_TEMPERATURE_REPORT[0], offset C8h.

6.1.36 MEM TRML TEMPERATURE REPORT (MEM_TRML_TEMPERATURE_REPORT[2]) - Offset D0h

This register is used to report the thermal status of the memory. The channel max temperature field is used to report the maximal temperature of all ranks.

Note: Bit definitions are the same as MEM_TRML_TEMPERATURE_REPORT[0], offset C8h.

6.1.37 MEM TRML TEMPERATURE REPORT (MEM_TRML_TEMPERATURE_REPORT[3]) - Offset D4h

This register is used to report the thermal status of the memory. The channel max temperature field is used to report the maximal temperature of all ranks.

Note: Bit definitions are the same as MEM_TRML_TEMPERATURE_REPORT[0], offset C8h.

6.1.38 DRAM PLANE OVERFLOW STATUS (DRAM_RAPL_PERF_STATUS_CFG) - Offset D8h

This register is used by Pcode to report DRAM Plane Power limit violations in the Platform.



Туре	Size	Offset	Default
PCI	32 bit	[B:31, D:30, F:2] + D8h	00000000h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:0	00000000 h RO/V	PWR_LIMIT_THROTTLE_CTR:

6.1.39 THERMTRIP CONFIGURATION (THERMTRIP_CONFIG_CFG) — Offset F8h

This register is used to configure the source(s) of the Memtrip output signal from the CPU.

Туре	Size	Offset	Default
PCI	32 bit	[B:31, D:30, F:2] + F8h	000000C0h

Register Level Access:

BIOS Access	SMM Access	OS Access
RW	RW	R

Bit Range	Default & Access	Field Name (ID): Description
31:8	0h RO	Reserved
7	1h RW/P	OFFPKG_MEMTRIP_TO_MEMTRIP_EN: If set to 1, PCU will OR incoming Off package Memtrip information into the MemTrip Output Tree. If set to 0, MemTrip output pin will not have In package Memtrip information.
6	1h RW/P	INPKG_MEMTRIP_TO_MEMTRIP_EN: If set to 1, PCU will OR incoming In package Memtrip information into the MemTrip output Tree. If set to 0, MemTrip output pin will not have In package Memtrip information.
5:0	0h RO	Reserved

6.1.40 MEMHOT EXTERNAL STATUS (MH_EXT_STAT_CFG) - Offset 84h

Capture externally asserted MEM_HOT[1:0]# assertion detection.

Т



Туре	Size	Offset	Default
PCI	32 bit	[B:31, D:30, F:5] + 84h	00000000h

BIOS Access	SMM Access	OS Access
R	R	R

Bit Range	Default & Access	Field Name (ID): Description
31:3	0h RO	Reserved
2	0h RO/V	MH_EXT_STAT_2: MEM_HOT_IN[1]# assertion status for non-Purley platform. Set if MEM HOT pins are working in uni directional mode.
1	0h RO/V	MH_EXT_STAT_1: MEM_HOT[1]# assertion status at this sense period. Set if MEM_HOT[1]# is asserted externally for this sense period, this running status bit will automatically updated with the next sensed value in the next MEM_HOT input sense phase.
0	0h RO/V	MH_EXT_STAT_0: MEM_HOT[0]# assertion status at this sense period. Set if MEM_HOT[0]# is asserted externally for this sense period, this running status bit will automatically updated with the next sensed value in the next MEM_HOT input sense phase.

Power Control Unit Base Address Registers (PCU_BAR) Base address of these registers are defined in the 'PCU_BAR' register in Bus: (30), Device: 0, Function: 1, at offset FCh

Note:

6.1.41

Note: Bit definitions are the same as PQR_ASSOC[0], offset 20h.

6.1.42 PQR ASSOC REGISTER (PQR_ASSOC[9]) - Offset 44h

Note: Bit definitions are the same as PQR_ASSOC[0], offset 20h.

6.1.43 PQR ASSOC REGISTER (PQR_ASSOC[10]) - Offset 48h

Note: Bit definitions are the same as PQR_ASSOC[0], offset 20h.

6.1.44 PQR ASSOC REGISTER (PQR_ASSOC[11]) - Offset 4Ch

Note: Bit definitions are the same as PQR_ASSOC[0], offset 20h.

6.1.45 PQR ASSOC REGISTER (PQR_ASSOC[12]) - Offset 50h

Note: Bit definitions are the same as PQR_ASSOC[0], offset 20h.

6.1.46 PQR ASSOC REGISTER (PQR_ASSOC[13]) - Offset 54h

Note: Bit definitions are the same as PQR_ASSOC[0], offset 20h.



- 6.1.47 PQR ASSOC REGISTER (PQR_ASSOC[14]) Offset 58h
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.48 PQR ASSOC REGISTER (PQR_ASSOC[15]) Offset 5Ch
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.49 PQR ASSOC REGISTER (PQR_ASSOC[16]) Offset 60h
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.50 PQR ASSOC REGISTER (PQR_ASSOC[17]) Offset 64h
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.51 PQR ASSOC REGISTER (PQR_ASSOC[18]) Offset 68h
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.52 PQR ASSOC REGISTER (PQR_ASSOC[19]) Offset 6Ch
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.53 PQR ASSOC REGISTER (PQR_ASSOC[20]) Offset 70h
- *Note:* Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.54 PQR ASSOC REGISTER (PQR_ASSOC[21]) Offset 74h
- *Note:* Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.55 PQR ASSOC REGISTER (PQR_ASSOC[22]) Offset 78h
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.56 PQR ASSOC REGISTER (PQR_ASSOC[23]) Offset 7Ch
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.57 PQR ASSOC REGISTER (PQR_ASSOC[24]) Offset 80h
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.58 PQR ASSOC REGISTER (PQR_ASSOC[25]) Offset 84h
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.

6.1.59 PQR ASSOC REGISTER (PQR_ASSOC[26]) - Offset 88h

Note: Bit definitions are the same as PQR_ASSOC[0], offset 20h.



6.1.60	PQR ASSOC REGISTER (PQR_ASSOC[27]) - Offset 8Ch
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.61	PQR ASSOC REGISTER (PQR_ASSOC[28]) - Offset 90h
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.62	PQR ASSOC REGISTER (PQR_ASSOC[29]) - Offset 94h
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.63	PQR ASSOC REGISTER (PQR_ASSOC[30]) - Offset 98h
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.64	PQR ASSOC REGISTER (PQR_ASSOC[31]) - Offset 9Ch
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.65	PQR ASSOC REGISTER (PQR_ASSOC[32]) - Offset A0h
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.66	PQR ASSOC REGISTER (PQR_ASSOC[33]) - Offset A4h
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.67	PQR ASSOC REGISTER (PQR_ASSOC[34]) - Offset A8h
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.68	PQR ASSOC REGISTER (PQR_ASSOC[35]) - Offset ACh
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.69	PQR ASSOC REGISTER (PQR_ASSOC[36]) - Offset B0h
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.70	PQR ASSOC REGISTER (PQR_ASSOC[37]) - Offset B4h
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.71	PQR ASSOC REGISTER (PQR_ASSOC[38]) - Offset B8h
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.
6.1.72	PQR ASSOC REGISTER (PQR_ASSOC[39]) - Offset BCh
Note:	Bit definitions are the same as PQR_ASSOC[0], offset 20h.



- 6.1.73 PQR ASSOC REGISTER (PQR_ASSOC[40]) Offset C0h
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.74 PQR ASSOC REGISTER (PQR_ASSOC[41]) Offset C4h
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.75 PQR ASSOC REGISTER (PQR_ASSOC[42]) Offset C8h
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.
- 6.1.76 PQR ASSOC REGISTER (PQR_ASSOC[43]) Offset CCh
- **Note:** Bit definitions are the same as PQR_ASSOC[0], offset 20h.

6.1.77 PQR ASSOC REGISTER (PQR_ASSOC[44]) - Offset D0h

Note: Bit definitions are the same as PQR_ASSOC[0], offset 20h.