Intel® EP80579 Software for IP Telephony Applications on Intel® QuickAssist Technology

Package Version Telephony.L.1.0.1

Release Notes

June 2010

Order Number: 320413-009US

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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

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

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

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site.

Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.

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

Code Names are only for use by Intel to identify products, platforms, programs, services, etc. ("products") in development by Intel that have not been made commercially available to the public, i.e., announced, launched or shipped. They are never to be used as "commercial" names for products. Also, they are not intended to function as trademarks.

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

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

Copyright © 2010, Intel Corporation. All rights reserved.

Contents

1 Description of Release 5
- 1.1 New Features 5
- 1.2 Supported Operating Systems 5
- 1.3 Supported Component Versions 5
  - 1.3.1 Version Numbering Scheme 5
  - 1.3.2 Package Version 5
  - 1.3.3 BIOS/Firmware Version 6

2 Known Issues - Silicon 6

3 Known Issues - Embedded 6

4 Resolved Issues - Embedded 13

5 Known Issues - Security 14

6 Resolved Issues - Security 22

7 Known Issues - IP Telephony 22

8 Resolved Issues - IP Telephony 23

9 Related Documentation 24
- 9.1 Where to Find Current Software and Documentation 24
- 9.2 Embedded Documents 25
- 9.3 Security Documents 25
- 9.4 IP Telephony Documents 26

Tables

1 Intel® EP80579 Integrated Processor Product Line Errata 6
2 Summary of Embedded Software Open Issues 6
3 Summary of Embedded Software Resolved Issues 13
4 Summary of Security Software Open Issues 14
5 Summary of Security Software Resolved Issues 22
6 Summary of Telephony Software Open Issues 23
7 Summary of Telephony Software Resolved Issues 23
8 Embedded Documents 25
9 Security Documents 25
10 IP Telephony Documents 26

Revision History

Date	Revision	Description
04 June 2010	009	Added new errata "IXA00161211 - Security Vulnerability in Gigabit Ethernet Driver due to Ethernet frames that exceed MTU" on page 8
23 June 2009	008	Added new errata "IXA00343773 - Software lockup may occur in Embedded Gigabit Ethernet driver" on page 12
04 May 2009	007	Added Section 2, "Known Issues - Silicon" on page 6
28 April 2009	006	Updated BIOS version: TRXTG063.ROM
30 March 2009	005	Updated BIOS version: TRXTG061.ROM
05 February 2009	004	Updated BIOS version: TRXTG062.ROM
18 December 2008	003	Release Notes for 1.0.1 release. Updates include: • Updated BIOS version: TRXTG061.ROM • new asynchronous API of the SRTP Acceleration driver
2 October 2008	002	Updated BIOS version: TRXTG060.ROM
September 2008	001	Initial release. Package Version: Telephony.L.1.0.103

§ §

1 Description of Release

This document describes extensions to and deviations from the release functionality described in Intel® EP80579 Software for IP Telephony Applications on Intel® QuickAssist Technology Programmer's Guide.

For instructions on loading and running the release, see the Getting Started Guide for your operating system.

Note: Prior to installing the EP80579 software package, uninstall the previous installation of the software. Refer to the Getting Started Guide for instructions on uninstalling the software.

These release notes may also include known issues with third-party or reference platform components that affect the operation of the software.

Note: The "Intel® EP80579 Integrated Processor with Intel® QuickAssist Technology Development Board" is referred to as "development board" throughout this document.

1.1 New Features

- New asynchronous API of the SRTP Acceleration driver

See the Getting Started Guide for your operating system for detailed information about the features of this release.

1.2 Supported Operating Systems

This software release has been validated with the following operating systems:

- Red Hat* Enterprise Linux* 5.0 (RHEL 5.0) Client package, Kernel 2.6.18

1.3 Supported Component Versions

1.3.1 Version Numbering Scheme

The version numbering scheme used in this software release uses this naming convention:

package.os.major.minor.maintenance-build

where:

- package can be one of the following:
  - Embedded
  - Security
  - Telephony
- os can be one of the following:
  - L = Linux*

1.3.2 Package Version

Package Version Telephony.L.1.0.1-51

1.3.3 BIOS/Firmware Version

The term BIOS is used to refer to pre-boot firmware which could include legacy BIOS or Extensible Firmware Interface (EFI) compliant firmware.

BIOS Version: TRXTG063.ROM

2 Known Issues - Silicon

The Intel® EP80579 Integrated Processor Product Line Specification Update describes known silicon defects. Defects that are specific to Intel® EP80579 silicon are listed in the section called "Intel® EP80579 Integrated Processor Product Line Errata".

Table 1 lists defects identified with the Intel® EP80579 silicon that have software workarounds. If the workaround is implemented in the released software, it is indicated by **X** in the appropriate Operating System column in Table 1. For workaround details, see the Intel® EP80579 Integrated Processor Product Line Specification Update.

Table 1. Intel® EP80579 Integrated Processor Product Line Errata

No.[1]	Errata	Operating System		
		Linux*	FreeBSD*	Windows*
3	Gigabit Ethernet MAC Receive Timer interrupt problems	X	X	X
4	Gigabit Ethernet MAC Large Segment Offload (LSO) premature descriptor write back	X	N/A[2]	X
5	Gigabit Ethernet MAC XOFF from link partner can pause flow-control (XON/XOFF) transmission[3]	N/A	N/A	N/A
6	Gigabit Ethernet MAC transmit descriptor use of Report Status (RS) bit for non-data (Context & Null) descriptors	X	X	X
8	Gigabit Ethernet MAC legacy transmit descriptor write-back may occur before the packet data associated with the descriptor is fetched[4]		N/A[5]	
9	Gigabit Ethernet MAC may have EEPROM deadlock when using manual software EEPROM access	X	X	X

Notes:
1. This is the same defect number assigned in the Intel® EP80579 Integrated Processor Product Line Specification Update.
2. LSO is not supported by the FreeBSD driver.
3. This issue depends on the link partner flow control settings. The Flow Control thresholds have been tested extensively with no observed issues.
4. The software workaround defined in the Specification Update is not currently implemented in the Linux or Windows Ethernet driver.
5. TCP Segmentation Offload is not supported by the FreeBSD driver.

3 Known Issues - Embedded

For supplementary information relating to the Known Issues, please refer to Table 8, "Embedded Documents" on page 25.

Table 2. Summary of Embedded Software Open Issues

IXA00058263 - SATA port 1 not showing populated when CD/DVD ROM attached 7
IXA00160925 - Manual setting of duplex mode of Embedded Gigabit Ethernet driver fails on Microsoft Windows XP Embedded & Red Hat Enterprise Linux 5.0 7
IXA00161030 - Race condition in the GCU driver may result in deadlock in reboot scenarios 8

IXA00161211 - Security Vulnerability in Gigabit Ethernet Driver due to Ethernet frames that exceed MTU . 8
IXA00179772 - IDE mode within the BIOS setup menu should be set to "AHCI" for optimal performance on Red Hat Enterprise Linux 5.0 10
IXA00206755 - Driver displays install warnings with Red Hat Enterprise Linux 5.0 distribution - 2.6.18 kernel 10
IXA00216017 - CompactFlash cards are not supported with embedded software drivers 10
IXA00241849 - Installation issues observed on Red Hat Enterprise Linux 5 using DVD SATA drives with IDE mode set to AHCI 11
IXA00343773 - Software lockup may occur in Embedded Gigabit Ethernet driver 12

3.1 IXA00058263 - SATA port 1 not showing populated when CD/DVD ROM attached

Title	**SATA port 1 not showing populated when CD/DVD ROM attached**
Reference #	IXA00058263
Description	In the BIOS Setup Menu under the IDE selection screen the 2nd SATA port (SATA 1) shows "Not Present" when a CD/DVD ROM is plugged into SATA port 1 and the IDE mode is AHCI. Hard Drives will appear correctly. However, the CD/DVD ROM appears to be fully functional and can be selected in the boot order.
Implication	In the AHCI mode for IDE, CD/DVD ROMs may not show up when plugged into the SATA ports. This is viewed in the Advanced->IDE Configuration Screen in the BIOS setup menu. Functionality of the device is not impacted and will still be selectable in the boot order. The CD/DVD ROM devices tested were Plextor PX-72Sa and LG GSA-H62L.
Resolution	No work around available.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Driver-General

3.2 IXA00160925 - Manual setting of duplex mode of Embedded Gigabit Ethernet driver fails on Microsoft Windows XP Embedded & Red Hat Enterprise Linux 5.0

Title	**Manual setting of duplex mode of Embedded Gigabit Ethernet driver fails on Microsoft Windows XP Embedded & Red Hat Enterprise Linux 5.0**
Reference #	IXA00160925
Description	When Embedded Gigabit Ethernet driver is manually configured to run at 10Mbs or 100Mbs full duplex, the operation mode is set to half-duplex. This behavior has been observed under Microsoft Windows XP Embedded and Red Hat Enterprise Linux 5.0. Autonegotiation allows driver to run at 10Mbs and 100Mbs full duplex.
Implication	It is not possible to manually set the duplex mode to full duplex with the Embedded Gigabit Ethernet driver. Attempts to do this will result in duplex mode being set to half duplex. The system will still function, but will do so in half duplex mode.
Resolution	Use autonegotiation instead of manual configuration if full duplex is desired.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Gigabit Ethernet Controller Driver

3.3 IXA00161030 - Race condition in the GCU driver may result in deadlock in reboot scenarios

Title	**Race condition in the GCU driver may result in deadlock in reboot scenarios**
Reference #	IXA00161030
Description	A race condition exists in the GCU driver that can result in a deadlock of the system during various reboot scenarios. Additionally, there is also a possibility that this could be encountered at runtime as well when modifying the state of a network interface using ethtool.
Implication	This issue occurs during contention when accessing the global_adaptor_spinlock during gcu_read/gcu_write operations and when the iegbe_watchdog() is called within the softIRQ fired by a kernel timer. While the window of contention is extremely small (~50 microseconds), iteratively rebooting the system or changing interface state a large number of times (> 200) causes the system to hang.
Resolution	To resolve this issue, make the following modifications to the GCU driver: In file gcu_main.c: Change all occurrences of spin_lock(&global_adapter_spinlock); to spin_lock_bh(&global_adapter_spinlock). Change all occurrences of spin_unlock(&global_adapter_spinlock); to spin_unlock_bh(&global_adapter_spinlock); After these modifications are made, you need to recompile and install the gcu/igbe drivers.
Affected OS	CentOS 5.2 Linux Red Hat Enterprise Linux 5.0
Driver/Module	Gigabit Ethernet Controller Driver

3.4 IXA00161211 - Security Vulnerability in Gigabit Ethernet Driver due to Ethernet frames that exceed MTU

Title	**Security Vulnerability in Gigabit Ethernet Driver due to Ethernet frames that exceed MTU**
Reference #	IXA00161211
Description	A security vulnerability exists in the Gigabit Ethernet Driver. The driver allows remote DOS attack through careful selection of frame size in relation to interface MTU, which causes a denial of service (panic), via a crafted frame size.
Implication	Since the Intel® EP80579 Linux Gigabit Ethernet driver does not support receiving packets that span multiple Rx buffers, it checks the End of Packet bit of every frame, and discards it if it is not set. This creates a situation where the first part of a spanning packet is discarded, but the second part is not (since it is the end of packet and it passes the EOP bit test). If the second part of the frame is small (4 bytes or less), the driver subtracts 4 from it to remove its CRC, underflow the length, and winds up in skb_over_panic, when the driver tries to skb_put a huge number of bytes into the skb. This allows a remote DOS attack through careful selection of frame size in relation to interface MTU, which causes a denial of service (panic), via a crafted frame size. Additional information on this defect is available at: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4536

Title	**Security Vulnerability in Gigabit Ethernet Driver due to Ethernet frames that exceed MTU (Continued)**

Resolution	The following updates should be applied to the driver to address the security vulnerability.
	Corrective Action #1:
	Embedded/src/GbE/iegbe_main.c:
	In the function iegbe_clean_rx_irq() find the conditional code fragment:
	`if(unlikely(!(rx_desc->status & E1000_RXD_STAT_EOP))) {`
	`/* All receives must fit into a single buffer */`
	`E1000_DBG("%s: Receive packet consumed multiple"`
	`" buffers\n", netdev->name);`
	`dev_kfree_skb_irq(skb);`
	`goto next_desc;`
	`}`
	Replace it with:
	`/* !EOP means multiple descriptors were used to store a`
	`* single packet, if that is the case we need to toss it.`
	`* In fact, we need to toss every packet with the EOP bit`
	`* clear and the next frame that _does_ have the EOP bit set,`
	`* as it is by definition only a frame fragment */`
	`if (unlikely(!(rx_desc->status & E1000_RXD_STAT_EOP)))`
	`adapter->discarding = TRUE;`
	`if (adapter->discarding) {`
	`/* All receives must fit into a single buffer */`
	`E1000_DBG("%s: Receive packet consumed multiple"`
	`" buffers\n", netdev->name);`
	`if (rx_desc->status & E1000_RXD_STAT_EOP)`
	`adapter->discarding = FALSE;`
	`dev_kfree_skb_irq(skb);`
	`goto next_desc;`
	`}`
	Corrective Action #2:
	Embedded/src/GbE/iegbe.h:
	In the iegbe_adapter structure, add the discarding element to the end of the structure.
	Ensure that the element is not added within any of the conditional preprocessor statements:
	`struct iegbe_adapter {`
	`struct timer_list tx_fifo_stall_timer;`
	`struct timer_list watchdog_timer;`
	`.`
	`.`
	`.`
	`uint32_t pci_state[16];`
	`int msg_enable;`
	`#ifdef CONFIG_PCI_MSI`
	`boolean_t have_msi;`
	`#endif`
	`boolean_t discarding;`
	`}`

Affected OS	Red Hat Enterprise Linux 5.0 CentOS 5.2 Linux
Driver/Module	Gigabit Ethernet Controller Driver

3.5 IXA00179772 - IDE mode within the BIOS setup menu should be set to "AHCI" for optimal performance on Red Hat Enterprise Linux 5.0

Title	**IDE mode within the BIOS setup menu should be set to "AHCI" for optimal performance on Red Hat Enterprise Linux 5.0**
Reference #	IXA00179772
Description	The performance of the Embedded Gigabit driver is significantly lower when the IDE mode is set to "Legacy". AHCI inherently provides higher performance and setting the system to AHCI mode will result in superior performance results, provided the hard drive used in the system supports AHCI.
Implication	System performance is significantly lower when IDE mode is set to "Legacy" mode.
Resolution	AHCI inherently provides higher performance. Setting the system IDE mode to "AHCI" will result in superior performance results. Refer to the chapter titled Pre-boot (BIOS) Firmware within the Getting Started Guide for instructions to toggle the IDE mode to "AHCI" in the BIOS setup menu.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Gigabit Ethernet Controller Driver

3.6 IXA00206755 - Driver displays install warnings with Red Hat Enterprise Linux 5.0 distribution - 2.6.18 kernel

Title	**Driver displays install warnings with Red Hat Enterprise Linux 5.0 distribution - 2.6.18 kernel**
Reference #	IXA00206755
Description	When building the Intel® EP80579 Software Drivers for Embedded Applications using Red Hat Enterprise Linux 5.0, warnings are displayed as follows: Warning: vmlinux - Section mismatch: reference to .exit.text: from .smp_alternatives between '__smp_alt_begin' (at offset...) and '__smp_locks_end'
Implication	These warning messages are from the Red Hat Enterprise Linux 5.0 distribution. They are not from the embedded software drivers. These warnings will not interfere with the building and function of the embedded software drivers
Resolution	No work around is available. The building and function of the embedded software drivers are not impacted.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	All

3.7 IXA00216017 - CompactFlash cards are not supported with embedded software drivers

Title	**CompactFlash cards are not supported with embedded software drivers**
Reference #	IXA00216017
Description	Currently CompactFlash on the Lower Expansion Bus of the Intel EP80579 Development Board are not supported with drivers in any of the embedded software releases.
Implication	No CompactFlash driver support is available for use of the CompactFlash.
Resolution	No work around available.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Not Applicable

3.8 IXA00241849 - Installation issues observed on Red Hat Enterprise Linux 5 using DVD SATA drives with IDE mode set to AHCI

Title	**Installation issues observed on Red Hat Enterprise Linux 5 using DVD SATA drives with IDE mode set to AHCI**
Reference #	IXA00241849
Description	When IDE mode is set to AHCI, installation of Red Hat Enterprise Linux using some DVD SATA drives will fail. During the installation process the message "Loading AHCI driver" is displayed, and the installation hangs. This has been observed on some DVD SATA drives.
Implication	When IDE mode is set to AHCI, installation of Red Hat Enterprise Linux using some DVD SATA drives will fail.
Resolution	If DVD SATA drives exhibit this behavior, perform installation with IDE mode set to Legacy. If AHCI is desired, perform installation using USB DVD, USB CD drive, or other DVD SATA drive.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	SATA

3.9 IXA00343773 - Software lockup may occur in Embedded Gigabit Ethernet driver

Title	**Software lockup may occur in Embedded Gigabit Ethernet driver**
Reference #	IXA00343773
Description	The Embedded Gigabit Ethernet driver uses spin_lock_bh() to protect the MDIO registers. This can cause a soft-lockup issue. The lockup would look similar to: BUG: soft lockup - CPU#0 stuck for 10s! [netstat:4281] Pid: 4281, comm: netstat EIP: 0060:[<c0609590>] CPU: 0 EIP is at _spin_lock+0x7/0xf EFLAGS: 00000286 Tainted: PF (2.6.18-GA102_OCF #1) EAX: f48c2f00 EBX: 00000002 ECX: c072bf8e EDX: f152be40 ESI: 00000011 EDI: c072bf8e EBP: e604a7c0 DS: 007b ES: 007b CR0: 8005003b CR2: b7fa6000 CR3: 2582a000 CR4: 000006d0 [<f48c10b6>] gcu_get_adapter+0x16/0x20 [gcu] [<f48c14e3>] gcu_read_eth_phy+0x23/0x130 [gcu] [<f494c6c5>] iegbe_oem_phy_is_link_up+0x55/0x90 [iegbe] [<f49432a9>] iegbe_watchdog+0x419/0x5c0 [iegbe] [<f4942e90>] iegbe_watchdog+0x0/0x5c0 [iegbe] [<c042dc29>] run_timer_softirq+0xfb/0x151 [<c042a77a>] __do_softirq+0x5a/0xbb [<c0407461>] do_softirq+0x52/0x9d [<c0407406>] do_IRQ+0xa5/0xae [<c040592e>] common_interrupt+0x1a/0x20 [<c04e5edd>] delay_tsc+0x9/0x13 [<c04e5f10>] __delay+0x6/0x7 [<f48c1519>] gcu_read_eth_phy+0x59/0x130 [gcu] [<f4946f63>] iegbe_read_phy_reg+0x163/0x180 [iegbe] [<f493f325>] iegbe_update_stats+0x855/0x880 [iegbe] [<f4941a56>] iegbe_get_stats+0x16/0x20 [iegbe] [<c05adeed>] dev_seq_show+0x22/0x8e [<c048bdae>] seq_read+0x191/0x273 [<c048bc1d>] seq_read+0x0/0x273 [<c0471174>] vfs_read+0x9f/0x141 [<c04715c2>] sys_read+0x3c/0x63 [<c0404eff>] syscall_call+0x7/0xb
Implication	The Gigabit Ethernet driver's use of spin_lock_bh() to protect the MDIO registers can cause a soft-lockup issue.

Title	**Software lockup may occur in Embedded Gigabit Ethernet driver (Continued)**

Resolution	All changes for this workaround are located in the "gcu_main.c" file. Contents of the patch file are included below.
	These contents could be saved to a file and then applied using the patch command or they can be manually applied. After updating the source file, recompile the gcu and iegbe driver and install.
	---------- 	
	diff -Naur GbE-Orig/gcu_main.c GbE/gcu_main.c
	--- GbE-Orig/gcu_main.c 2009-06-23 12:21:48.000000000 -0700
	+++ GbE/gcu_main.c 2009-06-23 12:21:41.000000000 -0700
	@@ -94,6 +94,7 @@
	
	static struct gcu_adapter *global_adapter = 0;
	static spinlock_t global_adapter_spinlock = SPIN_LOCK_UNLOCKED;
	+static unsigned int g_flags = 0;
	
	MODULE_AUTHOR("Intel(R) Corporation");
	MODULE_DESCRIPTION("Global Configuration Unit Driver");
	@@ -412,7 +413,7 @@
	return NULL;
	}
	
	- spin_lock(&global_adapter_spinlock);
	+ spin_lock_irqsave(&global_adapter_spinlock, g_flags);
	
	return global_adapter;
	}
	@@ -437,7 +438,7 @@
	*adapter = 0;
	}
	
	- spin_unlock(&global_adapter_spinlock);
	+ spin_unlock_irqrestore(&global_adapter_spinlock, g_flags);
	
	return;
	}

Affected OS	CentOS 5.2 Linux Red Hat Enterprise Linux 5.0
Driver/Module	Gigabit Ethernet Controller Driver

4 Resolved Issues - Embedded

Issues that have been resolved in previous versions of the software are included here.

Table 3. Summary of Embedded Software Resolved Issues

IXA00058114 - Embedded Gigabit Ethernet driver Load/Unload memory leak on Red Hat Enterprise Linux v5.0 14

4.1 IXA00058114 - Embedded Gigabit Ethernet driver Load/Unload memory leak on Red Hat Enterprise Linux v5.0

Title	Embedded Gigabit Ethernet driver Load/Unload memory leak on Red Hat Enterprise Linux v5.0
Reference #	IXA00058114
Description	A memory leak has been found while loading/unloading the Gigabit Ethernet driver over 15000 times in a 20 hour period without a reboot of the development board.
Implication	Although any memory leak is a concern, this is an extreme situation that should not impact any known usage model with the embedded software Linux release.
Resolution	This issue was determined to be an Operating System feature. See IXA00320219 for details
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Gigabit Ethernet Controller Driver

5 Known Issues - Security

For supplementary information relating to the Known Issues, please refer to Table 9, “Security Documents” on page 25.

Note: Some open issues listed below require applying patches that are described in the Getting Started Guide. No additional action is required.

Table 4. Summary of Security Software Open Issues

IXA00239764 - OCF cannot use Look Aside Crypto Random number generator without a patch 15
IXA00239767 - Linux kernel will only invoke OCF once to generate a random number..... 15
IXA00239768 - Openswan patched with OCF uses the incorrect bottom half spinlock variant..... 15
IXA00241987 - High data rates expose a memory leak in the openswan-2.4.9-ocf-linux-20070727.patch file..... 16
IXA00277532 - IPSec performance improvement modifications to Gigabit Ethernet driver on Linux..... 16
IXA00281625 - Keygen: TLS PRF as documented in RFC 2246 for TLS v 1.0 17
IXA00283570 - Kernel panic when removing icp_ocf driver while passing traffic (>400Mbs)..... 18
IXA00298242 - Changes required to enable Security Acceleration on A0 Silicon 19
IXA00302585 - CpaCySymCbFunc: Symmetric callback function does not document CPA_STATUS_RETRY status 19
IXA00304731 - Synchronous symmetric operation timeout under extreme loads 20
IXA00320219 - Decreasing value of the metric 'MemFree' in /proc/meminfo may not imply a memory loss in Linux or the application..... 20
IXA00329534 - OpenSSL fails to generate Digital Certificates using RSA with 1024 bits key 21
IXA00331336 - Repeated start/stop of QuickAssist modules results in QuickAssist initialization failure..... 21
IXA00331338 - Intel® EP80579 Development Platform does not recover from soft lockup caused by a SSL stress test on Linux..... 22

5.1 IXA00239764 - OCF cannot use Look Aside Crypto Random number generator without a patch

Title	**OCF cannot use Look Aside Crypto Random number generator without a patch**
Reference #	IXA00239764
Description	OCF 20070727 uses a statically declared array of memory to store random data. This memory comes from the heap which is not physically contiguous. The Look-Aside Crypto component requires the data pointer to be physically contiguous.
Implication	The Look-Aside Crypto random number generator cannot be used with OCF unless a patch is applied to OCF to change the random number memory from a static array to kmalloc'd memory.
Resolution	AFTER the OCF patch (ocf-linux-26-20070727.patch) has been applied to the Linux kernel, the linux-ocf-20070727-backport.patch file needs to be applied to $KERNEL_SOURCE_ROOT with the command: patch -p0 < $ICP_ROOT/OpenSourcePatches/linux-ocf-20070727-backport.patch Also, see Errata item IXA00239767. The patch does not need to be applied more than once.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Opensource Software

5.2 IXA00239767 - Linux kernel will only invoke OCF once to generate a random number

Title	**Linux kernel will only invoke OCF once to generate a random number**
Reference #	IXA00239767
Description	The OCF 20070727 release patches the Linux kernel random.c file with changes that enable OCF to be called to create a random number and save this into the Linux entropy pool. The changes will result in OCF only getting invoked once to fill the Linux entropy pool with random data.
Implication	The Linux kernel patched with OCF will only invoke OCF once to fill the Linux entropy pool with data. When the random data left in the Linux entropy pool goes below a threshold, only the other devices in the system configured to fill the pool with random data will be invoked.
Resolution	AFTER the OCF patch (ocf-linux-26-20070727.patch) has been applied to the Linux kernel, the linux-ocf-20070727-backport.patch file needs to be applied to $KERNEL_SOURCE_ROOT with the command: patch -p0 < $ICP_ROOT/OpenSourcePatches/linux-ocf-20070727-backport.patch Also, see Errata item IXA00239764. The patch does not need to be applied more than once.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Opensource Software

5.3 IXA00239768 - Openswan patched with OCF uses the incorrect bottom half spinlock variant

Title	**Openswan patched with OCF uses the incorrect bottom half spinlock variant**
Reference #	IXA00239768
Description	Openswan 2.4.9 is patched with OCF 20070727 with the Openswan 2.4.9 is patched with OCF 20070727 with the ocf-openswan-2.4.9-20070727.patch file. This patch applies the incorrect type of spinlock to the Openswan code.
Implication	The system may crash when running high data rates through a VPN tunnel using Openswan 2.4.9 and OCF 20070727.

Title	**Openswan patched with OCF uses the incorrect bottom half spinlock variant**
Resolution	AFTER the OCF patch (ocf-openswan-2.4.9-20070727.patch) has been applied to the Openswan code, the ocf-openswan-2.4.9-20070727-session-migration-backport.patch file needs to be applied to the Openswan installation folder with the command: patch -p1 < $ICP_ROOT/OpenSourcePatches/ocf-openswan-2.4.9-20070727-session-migration-backport.patch Also, see Errata item IXA00241987. The patch does not need to be applied more than once.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Opensource Software

5.4 IXA00241987 - High data rates expose a memory leak in the openswan-2.4.9-ocf-linux-20070727.patch file

Title	**High data rates expose a memory leak in the openswan-2.4.9-ocf-linux-20070727.patch file**
Reference #	IXA00241987
Description	When passing traffic at very high data rates over an OCF accelerated Openswan IPsec VPN tunnel, a memory loss can be observed in the system. This is most acute with bi-directional traffic tests with very obvious packet loss.
Implication	All of the available memory in the system can be consumed in a relatively short period of time when running bi-directional tests at very high data rates when packet loss is obvious.
Resolution	AFTER the OCF patch (ocf-openswan-2.4.9-20070727.patch) has been applied to the Openswan code, the ocf-openswan-2.4.9-20070727-session-migrationbackport.patch file needs to be applied to the Openswan installation folder with the command: patch -p1 < $ICP_ROOT/OpenSourcePatches/ocf-openswan-2.4.9-20070727-session-migration-backport.patch. Also, see Errata item IXA00239768. The patch does not need to be applied more than once.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Opensource Software

5.5 IXA00277532 - IPSec performance improvement modifications to Gigabit Ethernet driver on Linux

Title	**IPSec performance improvement modifications to Gigabit Ethernet driver on Linux**
Reference #	IXA00277532
Description	For IPSec, the Openswan application requires additional memory for the IPSec headers and footers beyond what is originally allocated for the incoming packet. To do this, an additional alloc_skb() is called to create the new buffer and skb_copy_expand() is called to copy the original sk_buff to the new larger buffer.
Implication	These additional memory creation and copy buffer calls impact performance for IPSec.

Title	IPSec performance improvement modifications to Gigabit Ethernet driver on Linux
Resolution	By applying the following changes, the iegbe_main.c driver file is modified to create the original buffer to include sufficient space for the IPSec header and footer. This eliminates the additional memory functional call when processing IPSec. These changes must be applied and the driver rebuilt per instructions in the Getting Started Guide. Step 1: modify $ICP_ROOT/Embedded/src/iegbe.h, at the end of the file change to #define IEGBE_ADBUF 64 //Additional buffer space for IPsec #endif /* _IEGBE_H_ */ Step 2: modify $ICP_ROOT/Embedded/src/iegbe_main.c. The following shows the differences between the original and the new file. 4289c4290 < unsigned int bufsz = adapter->rx_buffer_len + NET_IP_ALIGN; --- > unsigned int bufsz = adapter->rx_buffer_len + NET_IP_ALIGN + IEGBE_ADBUF; 4336c4337 < skb_reserve(skb, NET_IP_ALIGN); --- > skb_reserve(skb, NET_IP_ALIGN + IEGBE_ADBUF); 4472c4473 < skb = dev_alloc_skb(adapter->rx_ps_bsize0 + NET_IP_ALIGN); --- > skb = dev_alloc_skb(adapter->rx_ps_bsize0 + NET_IP_ALIGN + IEGBE_ADBUF); 4481c4482 < skb_reserve(skb, NET_IP_ALIGN); --- > skb_reserve(skb, NET_IP_ALIGN + IEGBE_ADBUF);
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Gigabit Ethernet Controller Driver

5.6 IXA00281625 - Keygen: TLS PRF as documented in RFC 2246 for TLS v 1.0

Title	Keygen: TLS PRF as documented in RFC 2246 for TLS v 1.0
Reference #	IXA00281625
Description	The key generation API accelerates the TLS PRF, which is defined as part of RFC2246. One of the inputs to this function is a label. The API defines an enumerated type with values that correspond to some of the required labels. However, for some of the operations/labels required by RFC2246, no values are specified. The following are the operations/labels specified by RFC2246 and the corresponding enum values, where defined: +-------+----------+----------+----------+ :RFC2246: : : : :Section: Operation : Label : API Enum : +-------+----------+----------+----------+ : 6.3 : Derive the key material : "key expansion" : CPA_CY_KEY_TLS_OP_KEY_MATERIAL_DERIVE : : : Derive final client write key : "client write key" : : : : Derive final server write key : "server write key" : : : : Derive IV block : "IV block" : : : 7.4.9 : Client finished : "client finished" : CPA_CY_KEY_TLS_OP_CLIENT_FINISHED_DERIVE : : : Server finished : "server finished" : CPA_CY_KEY_TLS_OP_SERVER_FINISHED_DERIVE : : 8.1 : Computing the master secret : "master secret" : CPA_CY_KEY_TLS_OP_MASTER_SECRET_DERIVE : +-------+----------+----------+----------+
Implication	For some of the operations and labels required by RFC2246, no supported enum type is provided. A user-defined value must be provided.

Title	**Keygen: TLS PRF as documented in RFC 2246 for TLS v 1.0**
Resolution	For those operations/labels above for which no enum value is provided, the client should use the enum value CPA_CY_KEY_TLS_OP_USER_DEFINED, and pass the label using the userLabel field of the CpaCyKeyGenTlsOpData data structure.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Crypto Module

5.7 IXA00283570 - Kernel panic when removing icp_ocf driver while passing traffic (>400Mbs)

Title	**Kernel panic when removing icp_ocf driver while passing traffic (>400Mbs)**
Reference #	IXA00283570
Description	Removing icp_ocf driver while passing traffic of more than 400 Mbs generates a kernel panic. The log file shows the following: icp_ocfDrvSymProcess(): icp_LacSymOpPerform failed, lacStatus = 2 icp_ocfDrvSymProcess(): icp_LacSymOpPerform failed, lacStatus = 2 icp_ocfDrvSymProcess(): icp_LacSymOpPerform failed, lacStatus = 2 icp_ocfDrvSymProcess(): icp_LacSymOpPerform failed, lacStatus = 2 icp_ocfDrvSymProcess(): icp_LacSymOpPerform failed, lacStatus = 2 [error] LacSessionTableDescInvalidate() - : Session cannot be deregistered as there are 128 or more callbacks pending [error] LacSessionTableDescInvalidate() - : Session cannot be deregistered as there are 134 or more callbacks pending icp_ocfDrvExit(): 2 LAC sessions were not deregistered correctly. This is not a clean exit! slab error in kmem_cache_destroy(): cache `ICP Op Data': Can't free all objects [<c1062f7d>] kmem_cache_destroy+0x88/0x133 [<ecca82e6>] icp_ocfDrvFreeCaches+0x36/0xe0 [icp_ocf] [<ecca8558>] icp_ocfDrvExit+0x128/0x140 [icp_ocf] [<c103b677>] sys_delete_module+0x192/0x1bb [<c10464b8>] audit_syscall_entry+0x11c/0x144 [<c1003d0b>] syscall_call+0x7/0xb
Implication	There will be a kernel panic when the current OCF driver is removed while traffic is passing.
Resolution	AFTER the OCF patch (ocf-linux-26-20070727.patch) and linux-ocf-20070727-backport.patch has been applied to the Linux kernel, the linux-ocf-20070727-driver-removal.patch patch file needs to be applied to $KERNEL_SOURCE_ROOT with the command: patch -p0 < $ICP_ROOT/OpenSourcePatches/linux-ocf-20070727-driver-removal.patch
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Opensource Software

5.8 IXA00298242 - Changes required to enable Security Acceleration on A0 Silicon

Title	**Changes required to enable Security Acceleration on A0 Silicon**
Reference #	IXA00298242
Description	The current software release will not run correctly on A0 silicon due to a silicon change which corrects the interpretation of the setting of the 'interrupt disable' (INTD) bit for the Gigabit Ethernet driver. The GigE driver uses MSI interrupts; the software currently sets the interrupt disable bit to a 1, to disable INTx interrupts. However, on A0 silicon, setting this bit to a 1 incorrectly disables MSI interrupts too, so the bit needs to be set to 0.
Implication	The code changes detailed below are required to enable correct operation on earlier (A0) silicon revisions.

Resolution	If the software is required to run on A0 silicon, set the INTD bit to zero. The following code change needs to be made if running this software release on A0 silicon:
	In the file: $ICP_ROOT/Embedded/src/GbE/iegbe_main.c
	Modify this line of code:
	from:
	pci_write_config_word(adapter->pdev, PCI_COMMAND, pci_cmd | IEGBE_INTD_DISABLE);
	to:
	pci_write_config_word(adapter->pdev, PCI_COMMAND, pci_cmd & (~IEGBE_INTD_DISABLE));

Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	QuickAssist (R) Driver

5.9 IXA00302585 - CpaCySymCbFunc: Symmetric callback function does not document CPA_STATUS_RETRY status

Title	**CpaCySymCbFunc: Symmetric callback function does not document CPA_STATUS_RETRY status**
Reference #	IXA00302585
Description	In some cases, the callback function from cpaCySymPerformOp() may return with a status of CPA_STATUS_RETRY, even though only CPA_STATUS_SUCCESS and CPA_STATUS_FAIL are specified by the documentation. This behavior has been observed for symmetric operations that requires a pre-compute (HMAC, GCM, XCBC).
Implication	This may be visible when stressing the system, for example when performing several hundred random number generations in succession, whilst initializing normal priority sessions and performing operations before the pre-compute has completed. The reason for this is that the random operations fill the request rings resulting in a retry.
Resolution	The client can invoke the operation again for that session and the system will recover. To reduce the likelihood of seeing this behavior, minimize the number of requests to generate random numbers while simultaneously initializing sessions requiring pre-computes.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Crypto Module

5.10 IXA00304731 - Synchronous symmetric operation timeout under extreme loads

Title	Synchronous symmetric operation timeout under extreme loads
Reference #	IXA00304731
Description	In some cases, under heavy loads / high data rates, for example running several hundred large random number generations, a synchronous symmetric operation may timeout and report a failure when run simultaneously. This is a rare occurrence and is caused by a synchronous operation's wait-queue timing out. The current wait-queue time limit is set to 1 second for synchronous symmetric operations. The symmetric operation wait-queue timeout period is defined in LAC_SYM_SYNC_CALLBACK_TIMEOUT in the file lac_sync.h. Under 'normal' random number usage this should not be an issue. This may only be evident when flooding the system with large random number requests and synchronous symmetric operations.
Implication	A synchronous symmetric operation may timeout and fail under heavy loads.
Resolution	If a synchronous timeout occurs while performing operations, then increase the timeout of LAC_SYM_SYNC_CALLBACK_TIMEOUT in the file lac_sync.h. Also reduce the number of simultaneous large random number requests and synchronous operations.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Crypto Module

5.11 IXA00320219 - Decreasing value of the metric 'MemFree' in /proc/meminfo may not imply a memory loss in Linux or the application

Title	Decreasing value of the metric 'MemFree' in /proc/meminfo may not imply a memory loss in Linux or the application
Reference #	IXA00320219
Description	When the performance sample code was run for several days, the metric 'MemFree' in /proc/meminfo indicated a non-trivial loss in free memory. When memory loss was ruled out in Intel drivers and sample code, the same metric was monitored on an idle Linux system over a similar period of time. Once again, the metric pointed to a memory loss. Further investigation on the web, indicated that the apparent loss in memory reported in /proc/meminfo is caused by the kernel not freeing memory released by applications. The kernel does not release memory to realize other optimizations. However, this unused memory can be released non-destructively by setting the tunable parameter as described in the Resolution section.
Implication	When memory loss is suspected or reported by memory tools while running applications, performance suites, or stress tests, the customer should use prescriptions in the Resolution section to rule out memory grabbed by kernel as described in this erratum.
Resolution	Writing to /proc/sys/vm/drop will cause the kernel to drop clean caches, dentries, and inodes from memory, causing that memory to become free. To free pagecache: echo 1 > /proc/sys/vm/drop_caches To free dentries and inodes: echo 2 > /proc/sys/vm/drop_caches To free pagecache, dentries and inodes: echo 3 > /proc/sys/vm/drop_caches As this is a non-destructive operation, and dirty objects are not freeable, the user should run "sync" first in order to make sure all cached objects are freed. This tunable field was added in kernel version 2.6.16.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Opensource Software

5.12 IXA00329534 - OpenSSL fails to generate Digital Certificates using RSA with 1024 bits key

Title	**OpenSSL fails to generate Digital Certificates using RSA with 1024 bits key**
Reference #	IXA00329534
Description	OpenSSL fails to generate RSA Digital Certificates when using OCF based kernel cryptographic operations. The failure has been observed both when using the cryptosoft software library and EP80579 OCF driver.
Implication	It is not possible to generate an OpenSSL certificate when an OCF driver is active (any driver, including cryptosoft).
Resolution	Remove icp_ocf and/or cryptosoft before generating an OpenSSL certificate: rrmod icp_ocf # The line below is needed to make sure cryptosoft is not loaded; this command should fail normally rmmod cryptosoft # run the OpenSSL certificate generation command openssl req -new -x509 -days 365 -newkey rsa:1024 -nodes â€"keyout server.key -out server.crt
Affected OS	CentOS 5.2 Linux Red Hat Enterprise Linux 5.0
Driver/Module	Opensource Software

5.13 IXA00331336 - Repeated start/stop of QuickAssist modules results in QuickAssist initialization failure

Title	**Repeated start/stop of QuickAssist modules results in QuickAssist initialization failure**
Reference #	IXA00331336
Description	The FreeBSD/Linux system was built, installed as per the instructions in the Security Getting Started Guide on a platform with 1GB RAM and an external PCIe NIC - Intel PRO/1000 NIC. FreeBSD: The QuickAssist modules were repeatedly started and stopped using the following commands for over 24 hours: >/etc/rc.d/qat_service_freeBSD start >/etc/rc.d/qat_service_freeBSD stop The QuickAssist modules eventually fail to install and logs an error in the syslog. Linux: The QuickAssist modules were repeatedly started and stopped about 100 times using the following commands: >/etc/init.d/qat_service start >/etc/init.d/qat_service stop The system eventually does a kernel panic due to page fault.
Implication	Starting and stopping the QuickAssist modules repeatedly might result in QuickAssist initialization failure on FreeBSD or a kernel panic on Linux.
Resolution	Reboot the system to restart QuickAssist. The issue is under investigation.
Affected OS	FreeBSD 6.2 Red Hat Enterprise Linux 5.0
Driver/Module	QuickAssist (R) Driver

5.14 IXA00331338 - Intel® EP80579 Development Platform does not recover from soft lockup caused by a SSL stress test on Linux

Title	Intel® EP80579 Development Platform does not recover from soft lockup caused by a SSL stress test on Linux
Reference #	IXA00331338
Description	Accelerated Secure web server (Apache & OpenSSL) soft locks up during a SSLSwamp stress test on Linux, and does not recover once traffic is stopped. The test consists of SSLSwamp sending heavy traffic towards a platform running Apache / OpenSSL. The two soft lock ups observed occur after 2 & 5 days of the test running. SSLSwamp command: sslswamp -connect IP:[ipaddress]:443 -update 10 -cipher EDH-RSA-DESCBC3-SHA-time 86400
Implication	High load of HTTPS traffic might trigger this problem.
Resolution	It is not recommended to use the CRB for applications requiring more than 20 secure (https) connections per second.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Multiple Drivers

6 Resolved Issues - Security

Issues that have been resolved in previous versions of the software are included here.

Table 5. Summary of Security Software Resolved Issues

IXA00309248 - Only ACPI mechanism should be used to retrieve [N]CDRAM info from BIOS..... 22

6.1 IXA00309248 - Only ACPI mechanism should be used to retrieve [N]CDRAM info from BIOS

Title	Only ACPI mechanism should be used to retrieve [N]CDRAM info from BIOS
Reference #	IXA00309248
Description	In the current release, if the retrieval of the [N]CDRAM information using ACPI mechanism fails, then the software calls the routine "asd_read_bios_registers" to compute [N]CDRAM information. The returned values are invalid because the routine makes incorrect assumptions about the BIOS settings. NOTE: Only ACPI mechanism should be used in the release package to retrieve [N]CDRAM info from BIOS.
Implication	When the ACPI retrieval of [N]CDRAM information does not succeed, the EP80579 Security Software will fail to load with the error message “Failed to initialize HAL” in Syslog.
Resolution	In the file .../Acceleration/drivers/icp_asd/src/kernel/linux/asd_dram.c, line 175: If the call to asd_get_acpi_vars fails, delete the call to asd_read_bios_registers, display an error instead of a warning, and return FAIL.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	Crypto Module

7 Known Issues - IP Telephony

For supplementary information relating to the Known Issues, please refer to Table 10, “IP Telephony Documents” on page 26.

Table 6. Summary of Telephony Software Open Issues

IXA00335397 - Error message related to tainting the kernel appears when loading sRTP driver 23

7.1 IXA00335397 - Error message related to tainting the kernel appears when loading sRTP driver

Title	**Error message related to tainting the kernel appears when loading sRTP driver**
Reference #	IXA00335397
Description	When the ./load_sRTP_driver install command is executed to load the sRTP driver, the following message is seen: [root@ Install]# ./load_sRTP_driver loading /voice_1.1_ga/build_latest/srtp_acc_driver.ko srtp_acc_driver: module license 'dual BSD/GPL' taints kernel. [info] srtp_acc_init_module() - srtp acc driver loaded successfully Install Successful The installation of the sRTP driver is successful.
Implication	Loading the SRTP Access Driver flags the kernel as tainted by a proprietary module. No impacts ensue on the functionality of the SRTP Access Driver.
Resolution	In the source file srtp_acc_driver.c, replace the line containing MODULE_LICENSE ("dual BSD/GPL"); with the line MODULE_LICENSE("Dual BSD/GPL"); Once this is updated, recompile the driver. The kernel taint message will no longer occur after this update.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	SRTP Driver

8 Resolved Issues - IP Telephony

Issues that have been resolved in previous versions of the software are included here.

Table 7. Summary of Telephony Software Resolved Issues

IXA00161025 - BIOS sets Local Expansion Bus LEBBAR size to 128 Mbytes 23
IXA00253246 - SRTP acceleration is not faster than non-accelerated SRTP for small packets..... 24

8.1 IXA00161025 - BIOS sets Local Expansion Bus LEBBAR size to 128 Mbytes

Title	**BIOS sets Local Expansion Bus LEBBAR size to 128 Mbytes**
Reference #	IXA00161025
Description	The BIOS for the Intel® EP80579 development board sets the Local Expansion Bus LEBBAR to 128 Mbytes of MMIO address space.
Implication	If application software sets bit 9 (CNFG4_0) of any of the EXP_TIMING_CS[7 - 0] registers, then only EX_CS[3 - 0] are accessible via the IA-32 core. In this mode, the IA-32 core will not be able to access any of the EX_CS[6 - 4] connected to the mezzanine connectors.
Resolution	This issue was resolved with TRXTG062.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	HSS Voice Driver

8.2 IXA00253246 - SRTP acceleration is not faster than non-accelerated SRTP for small packets

Title	SRTP acceleration is not faster than non-accelerated SRTP for small packets
Reference #	IXA00253246
Description	Current implementation of SRTP acceleration is slower than the non-accelerated SRTP for small packets. CPU cycle consumption is higher on 64 byte packets in the accelerated scenario compared to the non-accelerated scenario. However, on a voice packet of 96 bytes, CPU cycle consumption is less in the accelerated scenario as compared to the non-accelerated scenario. Performance figures are listed below. Performance was measured through the modified LibSRTP. An SRTP Session with a single stream was established. RTP packets were sent through the SRTP stream via the LibSRTP library call "srtp_protect()". The time for a certain number of packets was recorded with the CPU usage. To simulate a voice call, two streams were created in the session and the same performance tests were run. Accelerated LibSRTP CPU Usage (1200 MHz Fab C) Packet Size (bytes) Call throughput (kbits/s) Call throughput packets/s 96 307.2 200 176 281.6 100 256 273.0666639 66.666666 336 1075.2 200 1024 -- -- Accelerated LibSRTP GA1.0 Unmodified LibSRTP CPU Usage (1200MHz Fab C) 0.25 0.99 Packet Size (bytes) Throughput Mbps throughput packets/s Throughput Mbps throughput packets/s 96 46.08 60000 94.04 122447.9167 176 84.48 60000 111.15 78941.76136 256 120.47 58823.24219 126.68 61855.46875 336 155.08 57693.45238 136.677 50847.09821 1024 402.89 49180.9082 155.05 18927.00195 Accelerated LibSRTP GA1.0 Unmodified LibSRTP Packet Size (bytes) MHz per call MHz per call 96 1 1.940416844 176 0.5 1.504906883 256 0.340001657 1.280404155 336 1.039979365 4.67283303
Implication	Throughput will be slower in the accelerated LibSRTP scenario.
Resolution	The customer should use the non-accelerated libSRTP when high throughput rates are required with smaller packet sizes.
Affected OS	Red Hat Enterprise Linux 5.0
Driver/Module	General

9 Related Documentation

9.1 Where to Find Current Software and Documentation

The software release and associated collateral can be found on the Hardware Design resource center.

1. In a web browser, go to http://www.intel.com/go/soc
2. For Software and pre-boot firmware: Click on “Tools & Software” tab.
3. For Documentation: Click on “Technical Documents” tab.

The EP80579 security software release package contains encryption software and is subject to export requirements defined by the U.S Department of Commerce. To satisfy these requirements, the End User Certification Form must be filled out and submitted for review/approval. Instructions on this process are included during the download process. Please note that this process may take up to two business days to complete.

9.2 Embedded Documents

The documents in Table 8 provide more information about the Embedded software provided in this release.

Table 8. Embedded Documents

Document Name	Number
Intel® EP80579 Software Drivers for Embedded Applications Programmer's Guide and API Reference Manual	320154
Intel® EP80579 Software Drivers for Embedded Applications on Linux* Getting Started Guide	320151
Software for Intel® EP80579 Integrated Processor Product Line PHY Porting Guide	320203
Ethernet PHY Selection Criteria for the Intel® EP80579 Integrated Processor Product Line Application Note	320254
Intel® EP80579 Integrated Processor Product Line Datasheet	320066
Intel® EP80579 Integrated Processor Product Line Specification Update	320176

9.3 Security Documents

The documents in Table 9 provide more information about the Security software provided in this release.

Table 9. Security Documents

Document Name	Number
Intel® EP80579 Software for Security Applications on Intel® QuickAssist Technology for Linux* Getting Started Guide	320182
Intel® EP80579 Software for Security Applications on Intel® QuickAssist Technology Programmer's Guide	320183
Intel® EP80579 Software for Security Applications on Intel® QuickAssist Technology Cryptographic API Reference Manual	320184
Intel® EP80579 Software on Intel® QuickAssist Technology Debug Services API Reference Manual	320185
Installing and Using OpenVPN* on Linux* Application Note	321165

9.4 IP Telephony Documents

The documents in Table 10 provide more information about the IP Telephony software provided in this release.

Table 10. IP Telephony Documents

Document Name	Reference Number
Integrating a Voice Application with the TDM Infrastructure of the Intel® EP80579 Integrated Processor with Intel® QuickAssist Technology White Paper	320053
Intel® EP80579 Software for IP Telephony Applications on Intel® QuickAssist Technology for Linux* Getting Started Guide	320414
Intel® EP80579 Software for IP Telephony Applications on Intel® QuickAssist Technology Programmer's Guide	320415
Intel® EP80579 Software for IP Telephony Applications on Intel® QuickAssist Technology Linux* Device Driver API Reference Manual	320416
Intel® EP80579 Software for IP Telephony Applications on Intel® QuickAssist Technology TDM I/O Access API Reference Manual	320417
Intel® EP80579 Software for IP Telephony Applications on Intel® QuickAssist Technology for Linux* SRTP Acceleration Driver Application Note	320517
Intel® EP80579 Software for IP Telephony Applications on Intel® QuickAssist Technology Linux* Tuning Guide	320524

§ §