Intel Massachusetts, Inc.
77 Reed Road
Hudson, MA 01749-2895
http://www.intel.com

Digital Semiconductor 21143-PD and 21143-TD
Errata

Errata Revision 4.0
May 22, 1998

ERRATA CONTENTS:
==========

This document contains Errata for the Digital Semiconductor 21143-PD and 21143-TD PCI/CardBus 10/100Mbps Ethernet LAN Controllers. The 21143 device revision affected by this errata can be identified as order number 21143-PD or 21143-TD, or in software as CFRV<7:0>=41H and is also labeled as DC1096B.

This Errata sheet describes problems associated with these chips or their documentation and offers workarounds which allow system designers and driver developers to use the 21143-PD and 21143-TD successfully.

Throughout this document, the Digital Semiconductor 21143-PD and 21143-TD PCI Fast Ethernet LAN Controllers are referred to as the 21143; the 21143 Hardware Reference Manual (order number EC-QWC4F-TE) is referred to as the Hardware Reference Manual; and the Digital Semiconductor 21143 Data Sheet (order number EC-QWC3F-TE) is referred to as the Data Sheet.

Errata Revision History:

25/Nov/97 1.0 Documented Items 1-2.
04/Feb/98 2.0 Added Item 3.
Modified Implication Section of Item 1 regarding future versions of Novell Client driver. No buffer size change will be made to future versions of this

driver.
Item 2 was reworded to enhance clarity.
10/Mar/98 3.0 Added Item 4.
22/May/98 4.0 Added Item 5, 6, 7.

Digital Semiconductor, now known as Intel Massachusetts, Inc., became a wholly-owned subsidiary of Intel Corporation on May 17, 1998.

1. Receive Buffer Relationship to Use of Memory Write and Invalidate

Background

The 21143 supports the extended PCI command for Memory Write and Invalidate. The 21143 will use Memory Write and Invalidate (MWI) only if it has been enabled via CSR0 (see Section 3.2.2.1 of the 21143 HRM).

A detailed description of the 21143's receive operation is located in Section 4.3.5 of the 21143 Hardware Reference Manual.

Problem

When all of the following conditions are met, the 21143 will stop processing receive frames:

1. Memory Write Invalidate is enabled (CSR0<24>=1).
2. The receive buffer ends on a cache-aligned address.
3. The packet size is such that the last longword of the packet is written to the last longword of the receive buffer.

When these conditions are met, the receive machine will not close the last receive descriptor. This causes the receive process to stall in the "Wait for receive packet" state (CSR5<19:17>) and no more packets will be received. Further received packets will eventually result in the report of a receive overflow condition in CSR8.

Implication

This anomaly can be completely avoided by implementation of any of the suggested workarounds.

The following summarizes the status of the drivers developed by Digital Semiconductor:

Novell Server (32-bit ODI): Unaffected -- MWI cannot be enabled in the present version of this driver (v3.11).
Novell Client (16-bit ODI): MWI command is enabled by default in v2.60. The anomaly can only be triggered by an illegal packet that is exactly 1536 bytes. The MWI command can be disabled by including the "EXT_MWI 0" keyword in the driver's net.cfg file.
NDIS3/4 (Windows 95, Windows NT, WfW): Unaffected -- MWI cannot be enabled in the present version of this driver (v4.22).
SCO Unix: (LLI and MDI): MWI command is enabled by default in v3.33 and v3.34. These drivers could trigger the anomaly on legal-sized

packets. Driver releases beginning with v3.35 eliminate the possibility of the anomaly by guaranteeing that the buffer does not end on a 32-byte cache boundary. In v3.33 and v3.34, the MWI command can be disabled by inserting the keyword EXT_MWI=0 in the space.c file and relinking the kernel.

NDIS2 (DOS and OS2): MWI command is enabled by default beginning with v2.60, but this driver is unaffected by the anomaly because the receive buffer size used by this driver is 1520 bytes which does not align to a 32-byte cache boundary.

When MWI support is added to the Digital Semiconductor drivers that do not presently support this command, the drivers will avoid the anomaly by selecting buffer sizes that cannot fall on a cache boundary.

For applications using drivers not developed by Digital Semiconductor, it will be necessary to assure that one of the suggested workarounds has been implemented.

Workaround

There are three workarounds that are possible for this issue. Implementation of any single item is sufficient to avoid the anomaly.

1. Receive Buffer size is at least 8 bytes greater than the maximum packet that will be received.
2. Memory Write and Invalidate is not enabled.
3. Buffer does not end on cache-aligned address.

Note: the 1st workaround does not account for the possibility of an illegal packet size on the network. Only the 2nd and 3rd workaround suggestions completely avoid this situation, and therefore are more robust workarounds.

2. Clkrun Behavior in D1, D2, and D3 Power States

Background

The 21143 has support for Clkrun in a CardBus or PCI environment. The Clkrun signal (clkrun_l) is asserted by the host during periods of normal system clock operation. The host may deassert this signal as a request to stop, or slow down, the system clock to a peripheral device. If the peripheral device requires that the normal system clock continue, it reasserts the Clkrun signal.

The 21143-PD/TD also supports the Advanced Configuration Power Interface (ACPI) specification v1.0. The ACPI specification specified four possible power states for a network controller: D0 for normal operation; and D1-D3 for lower power states.

Problem

The following are pre-conditions to the anomaly:

1. The 21143 is operated in the D1, D2, or D3 power states.
2. The 21143 has been configured not to report a link-change event as a power-management event.
3. The 21143 has detected a link failure on the 10Base-T port.

After all of these conditions have been met, the 21143 will acknowledge the deassertion of the Clkrun signal by reasserting Clkrun, even though it no longer needs the system clock.

If there has been no loss of link while operating in the D1, D2, or D3 power states, the 21143 will allow the clkrun request.

There are no restrictions to the clkrun functionality in the D0 state.

Implication

When all of the pre-conditions for the anomaly have been met, the 21143 will not be operating in its lowest power-savings mode.

Workaround

In a non-ACPI system, no workaround is required because this issue does not exist.

In an ACPI system, this anomaly cannot be worked around. However, due to the necessary pre-conditions, Digital Semiconductor believes that the occurrence of this behavior will be limited.

3. Leakage of PCI pads during Tri-state

Background

The Digital Semiconductor 21143-PD and 21143-TD are PCI and CardBus 10/100Mb/s Ethernet Controllers (collectively referred to as the 21143-xD). The 21143-xD differs from prior versions of the 21143 because the 21143-xD contains dual-function PCI/CardBus output pads that permit the 21143-xD to have a direct connection to either the PCI Local Bus or the CardBus. The 21143-xD uses PCI output drivers unless the cb_pads_l (pin 88) is pulled-down at power-up.

As a PCI agent, the 21143-xD is required to comply with the timing and voltage parameters established by the PCI Local Bus Specification Revision 2.1. In the PCI specification, an output is considered to be tri-stated when the total current delivered through the component pin is less than or equal to the leakage current specification. Maximum leakage current is defined to be 70uA in a 5V PCI signaling environment and 10uA in a 3.3V PCI signaling environment. The 21143-xD Data Sheet has the more restrictive specification of 10uA of leakage regardless of signaling environment.

Problem

When using the 21143-xD in a PCI environment, there is a transient condition where a weak p-channel transistor in the PCI output drivers is not completely cut-off. This occurs during a period when the 21143 PCI outputs should be tri-stated. If a different agent on the PCI bus drives a PCI signal from high to low, the 21143-xD may temporarily exceed the specification for PCI leakage current (Ioh). The additional leakage is the result of AC coupling of the high-to-low signal transition to the gate of the weak p-channel pull-up transistor which derives its control (gate) voltage through an n-channel pass gate. The worst-case condition occurs when the 21143-xD had driven a 'one' on the PCI pad during the most-recent PCI bus cycle.

Simulation has indicated the worst-case dynamic leakage current to be 1mA, with typical measured values of 200-250uA. The amount of leakage will dissipate to static levels in a timeframe of microseconds.

All of the 21143-xD PCI pads are affected by this anomaly. Designs that make use of the CardBus I/O pads are unaffected by this issue. Static DC leakage currents of the 21143-xD still meet the 10uA limit defined in the 21143 Data Sheet.

Implication

A PCI pull down device of another agent on the PCI bus will be required to sink the additional transient leakage current of the 21143-xD.

The PCI specification requires that I/O buffers source/sink substantial AC switching currents as described in the PCI V/I driver curves (see PCI specification). While other agents are driving the PCI bus, the worst-case transient leakage of the 21143-xD (1mA) will contribute to a slight elevation of static output low (Vol) levels. In a 5V PCI environment, where the pull-down load 22 ohms (maximum), the 21143-xD will contribute up to 22mV to Vol; in a 3.3V PCI environment, with a 40-ohm load (maximum), the 21143-xD will contribute up to 40mV to Vol. These resistance values are based on PCI I/O buffer load-line characteristics with worst-case 21143 transistor characteristics. Actual resistance values may be considerably smaller, resulting in even smaller contributions to the Vol level of the system.

Workaround

Currently there is no workaround for this anomaly. Although this anomaly does allow PCI tri-state leakage specification to be exceeded under worst-case conditions, Digital Semiconductor does not expect this contribution to Vol to cause interoperability problems with other PCI devices.

4. Restriction on use of SNOOZE mode
==========

Background

SNOOZE mode is a dynamic and automatic power-saving feature of the 21143. This mode allows the device to internally disconnect clocks to areas of the device that are not active, thereby reducing device power consumption. These clocks are automatically restarted when the 21143 detects that an inactive area of the chip must become active again.

The 21143-PD/TD supports the Advanced Configuration Power Interface (ACPI) specification v1.0. The ACPI specification specified four possible power states for a network controller: D0 for normal operation; and D1-D3 for lower power states. The 21143 can assert the gep<2>/rcv_match/wake pin when a Wake-Up packet or a Magic Packet(TM) has been received from the LAN while in D1, D2, or D3.

Refer to Chapter 7 "Power Management and Power Saving Support" of of the 21143 PCI/CardBus 10/100-Mb/s Ethernet LAN Controller HRM (EC-QWC4F-TE) for more information on SNOOZE mode, ACPI, and other power management features.

Problem

There is a logic problem that can prevent reliable notification that a Wake-Up packet or a Magic Packet had been received under the following conditions:

SNOOZE mode enabled, in ACPI D1 state, and 100Mb link speed.

Implications

As a result of the problem stated above, the system may fail to wake up from the D1 state when a Wake-Up packet or Magic Packet is received.

Workaround

Do not use SNOOZE mode, ACPI D1 state, and 100Mb link at the same time.

SNOOZE mode can be used in the D0 state. Before moving from the D0 state to D1 state, the 21143 should be removed from SNOOZE mode.

System software (BIOS, drivers, OS, applications, etc.) should disable SNOOZE mode in ACPI state D1. Disabling SNOOZE mode may slightly increase the overall power consumption of the 21143.

Digital Semiconductor software drivers do not enable SNOOZE mode by default. If alternative software drivers are being used, they should be modified to disable SNOOZE mode in the ACPI D1 state.

Magic Packet(TM) is a trademark of Advanced Micro Devices, Inc.

5. Extraneous Word During Transmit

==========

Background

The 21143 calculates a CRC on every transmit data packet. The four-byte result is appended to the packet and transmitted along with the packet data. The receiving node calculates a CRC on the received packet data and compares the result to the four-byte received CRC. When a mismatch occurs, the receiving station drops the packet. A higher layer protocol may elect to retransmit the packet in error.

Problem

There may be an intermittent event during an extended transmit time (several hours typically) where two extra bytes may be inserted to the transmitted packet. The receiving station would calculate a receive CRC error as the CRC byte offset is increased by two. This problem is a result of a minor manufacturing change that was made to include ACPI functionality in the 21143xD.

Implications

CRC error is a normal, expected soft-error event on Ethernet LANs. Higher protocol layers typically choose to retransmit the packet in error. It is most likely that this will only be detected using LAN test software or other analysis tools where a number of CRC errors may accumulate over an extended period of time. Digital Semiconductor has observed that the error rate may be from 2 to 20 errors in 24 hours of continuously transmitting packets in a stress testing environment. Due to the infrequent occurrence of the error, there will not be any significant impact to system operation or performance.

Workaround

There is currently no workaround for this anomaly.

6. Error Summary bit in TDES0 after link fail

==========

Background

During the transmission, the 21143 reports the status of the transmission in the transmit descriptor,TDES0. It contains transmitted frame status and descriptor ownership information. Link Fail Report, TDES0<2>, indicates the link failed while the packet was transmitted; Error Summary, TDES0<15>, indicates the logical OR of the following bits:

TDES0<1> - Underflow error
TDES0<2> - Link Fail Report
TDES0<8> - Excessive collisions
TDES0<9> - Late collision
TDES0<10> - No carrier
TDES0<11> - Loss of carrier

TDES0<14> - Transmit jabber timeout summary

Problem

The 21143 can attempt to transmit packets when the link has failed. Under this condition, the 21143 reports a link-fail status in the transmit descriptor, and it sets the bit TDES0<2> and TDES0<15>. After the link returns, the Link Fail Report bit, TDES0<2>, is cleared, however the Error Summary bit, TDES0<15>, is still set.

Implications

The transmit descriptor might indicate an Error Summary bit set while all other error bits are cleared in the transmit descriptor, TDES0. All DC21x4 drivers, except ODI-32 driver, will ignore the Error Summary bit, and the transmit operation will be restarted when the link returns. The ODI-32 driver will detect the Error Summary bit set and signal a transmit error to the higher protocol layers which then may elect to retransmit.

Workaround

There is no workaround for this anomaly.

7. Receive Watchdog Timer in Snooze mode

Background

Snooze mode is a dynamic and automatic power-saving feature of the 21143. This mode allows the device to internally disconnect clocks to areas of the device that are not active, thereby reducing device power consumption. These clocks are automatically restarted when the 21143 detects that an inactive area of the chip must become active again.

The 21143 provides a receive watchdog timer which can be used to monitor receive packets from the network. The receive watchdog timer should expire when a packet with a length greater than 2048 and less than or equal to 2560 bytes. The packet descriptor should close with the receive watchdog status bit, RDES0<4>, set.

Problem

When the 21143 is in snooze mode, the receive watchdog timer may expire while it receives a packet with the length between 1792 and 2304 bytes, thus packets could be truncated to 1792 bytes.

Implications

This anomaly only affects the range of operation of the Receive Watchdog Timer in snooze mode. Digital Semiconductor does not expect this behavior affects the device's performance.

Workaround

There is no workaround for this anomaly.

Important Notice

As of May 17, 1998, Digital Equipment Corporation's StrongARM, PCI Bridge, and Networking component businesses, along with the chip fabrication facility in Hudson, Massachusetts, were transferred to Intel Corporation. As a result of this transaction certain references to documents, web sites, telephone, and fax numbers have changed. For infomation about these products refer to the following URL:

http://developer.intel.com

For technical support, product updates, and documentation, contact the Customer Technology Center:

United States and International
1-800-628-8686
