Re: panic in RELENG_5 UMA

Source: http://unix.derkeiler.com/Mailing−Lists/FreeBSD/stable/2005−06/0768.html

---

From: Gary Mu1der (*gmulder_at_infotechfl.com*)
Date: 06/24/05

```
Date: Fri, 24 Jun 2005 15:28:34 −0400
To: freebsd−stable@freebsd.org
```

All,

Can someone confirm that the following stack trace is showing the same problem, or not?

I can reproduce the problem with the custom kernel config included below (which is basically GENERIC stripped of devices I don't have or need and IPFILTER added), but not with a stock GENERIC kernel.

To cause the crash I'm running 20−30 instances of the following script:

```
d5# cat arping.sh
#!/bin/sh

while :
do
        arp −d 192.168.4.$1 >/dev/null 2>&1;
        ping −c 1 −t 1 192.168.4.$1 >/dev/null 2>&1;
done
```

```
d5# uname −a
FreeBSD d5.bidx.com 5.4−RELEASE FreeBSD 5.4−RELEASE #6: Thu Jun 23
13:45:20 EDT 2005
root@d5.bidx.com:/usr/obj/usr/src/sys/DB−DUAL−AMD64−RAID5 amd64

d5# kgdb /usr/obj/usr/src/sys/DB−DUAL−AMD64−RAID5/kernel.debug ./vmcore.5
[GDB will not be able to debug user−mode threads:
/usr/lib/libthread_db.so: Undefined symbol "ps_pglobal_lookup"]
GNU gdb 6.1.1 [FreeBSD]
Copyright 2004 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain
conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB. Type "show warranty" for details.
This GDB was configured as "amd64−marcel−freebsd".
#0 doadump () at pcpu.h:167
```

```
167 pcpu.h: No such file or directory.
        in pcpu.h
(kgdb) bt
#0 doadump () at pcpu.h:167
#1 0x0000000000000000 in ?? ()
#2 0xffffffff802557b7 in boot (howto=260) at
/usr/src/sys/kern/kern_shutdown.c:410
#3 0xffffffff80255fef in panic (fmt=0xffffff00b5907500 " ë6µ")
    at /usr/src/sys/kern/kern_shutdown.c:566
#4 0xffffffff8029ad2a in sbdrop_locked (sb=0xffffffffb6274860, len=1146)
    at /usr/src/sys/kern/uipc_socket2.c:1149
#5 0xffffffff8029afe2 in sbflush_locked (sb=0xffffffffb6274860)
    at /usr/src/sys/kern/uipc_socket2.c:1116
#6 0xffffffff8029b049 in sbrelease_locked (sb=0xffffffffb6274860,
so=0xffffff00a0a2a8a0)
    at /usr/src/sys/kern/uipc_socket2.c:564
#7 0xffffffff8029b0d5 in sbrelease (sb=0xffffffffb6274860,
so=0xffffff00a0a2a8a0)
    at /usr/src/sys/kern/uipc_socket2.c:577
#8 0xffffffff80297b03 in sorflush (so=0xffffff00a0a2a8a0)
    at /usr/src/sys/kern/uipc_socket.c:1483
#9 0xffffffff80297e42 in sofree (so=0xffffff00a0a2a8a0) at
/usr/src/sys/kern/uipc_socket.c:407
#10 0xffffffff80298467 in soclose (so=0xffffff00a0a2a8a0) at
/usr/src/sys/kern/uipc_socket.c:485
#11 0xffffffff802847b5 in soo_close (fp=0xffffff009ca95b60, td=0x0)
    at /usr/src/sys/kern/sys_socket.c:299
#12 0xffffffff8022c2c0 in fdrop_locked (fp=0xffffff009ca95b60,
td=0xffffff00b5907500)
    at file.h:288
#13 0xffffffff8022c40a in closef (fp=0xffffff009ca95b60,
td=0xffffff00b5907500)
    at /usr/src/sys/kern/kern_descrip.c:1920
#14 0xffffffff8022e5be in fdfree (td=0xffffff00b5907500)
    at /usr/src/sys/kern/kern_descrip.c:1624
#15 0xffffffff80238bd0 in exit1 (td=0xffffff00b5907500, rv=0)
    at /usr/src/sys/kern/kern_exit.c:236
#16 0xffffffff8023a04e in sys_exit (td=0x0, uap=0x0) at
/usr/src/sys/kern/kern_exit.c:93
#17 0xffffffff8035cd8c in syscall (frame=
      {tf_rdi = 0, tf_rsi = 5263360, tf_rdx = 0, tf_rcx = 34366596768,
tf_r8 = 0, tf_r9 = 140737488350136, tf_rax = 1, tf_rbx = 0, tf_rbp = 3,
tf_r10 = −1099499764224, tf_r11 = 515, tf_r12 = 140−−−Type <return> to
continue, or q <return> to quit−−−
737488350376, tf_r13 = 0, tf_r14 = 0, tf_r15 = 0, tf_trapno = 12,
tf_addr = 34368259080, tf_flags = 0, tf_err = 2, tf_rip = 34366590280,
tf_cs = 43, tf_rflags = 514, tf_rsp = 140737488350296, tf_ss = 35}) at
/usr/src/sys/amd64/amd64/trap.c:771
#18 0xffffffff80349f88 in Xfast_syscall () at
/usr/src/sys/amd64/amd64/exception.S:248
#19 0x0000000000000000 in ?? ()
```

```
#20 0x0000000000505000 in ?? ()
#21 0x0000000000000000 in ?? ()
#22 0x000000080068a6a0 in ?? ()
#23 0x0000000000000000 in ?? ()
#24 0x00007fffffffebb8 in ?? ()
#25 0x0000000000000001 in ?? ()
#26 0x0000000000000000 in ?? ()
#27 0x0000000000000003 in ?? ()
#28 0xffffff0000b50600 in ?? ()
#29 0x0000000000000203 in ?? ()
#30 0x00007fffffffeca8 in ?? ()
#31 0x0000000000000000 in ?? ()
#32 0x0000000000000000 in ?? ()
#33 0x0000000000000000 in ?? ()
#34 0x000000000000000c in ?? ()
#35 0x0000000800820408 in ?? ()
#36 0x0000000000000000 in ?? ()
#37 0x0000000000000002 in ?? ()
#38 0x0000000800688d48 in ?? ()
#39 0x000000000000002b in ?? ()
#40 0x0000000000000202 in ?? ()
#41 0x00007fffffffec58 in ?? ()
#42 0x0000000000000023 in ?? ()
#43 0x00007fffffffe968 in ?? ()
#44 0x0000000000000023 in ?? ()
#45 0x0000000000000000 in ?? ()
−−−Type <return> to continue, or q <return> to quit−−−
#46 0x0000000000000000 in ?? ()
#47 0x0000000000000000 in ?? ()
#48 0x0000000000000000 in ?? ()
#49 0x0000000000000000 in ?? ()
#50 0x0000000000000000 in ?? ()
#51 0x0000000000000000 in ?? ()
#52 0x0000000000000000 in ?? ()
#53 0x00000000a14b4000 in ?? ()
#54 0xffffffffb6274c40 in ?? ()
#55 0x0000000001010000 in ?? ()
#56 0x0000000000000000 in ?? ()
#57 0xffffff00b536eba0 in ?? ()
#58 0xffffff00ec19a780 in ?? ()
#59 0xffffffffb6274b58 in ?? ()
#60 0xffffff00b5907500 in ?? ()
#61 0xffffffff8026a26c in sched_switch (td=0x0, newtd=0x3, flags=0)
    at /usr/src/sys/kern/sched_4bsd.c:881
#62 0x0000000000000000 in ?? ()
#63 0x0000000000000000 in ?? ()
#64 0x0000000000000000 in ?? ()
#65 0x0000000000000000 in ?? ()
#66 0x0000000000000000 in ?? ()
#67 0x0000000000000000 in ?? ()
#68 0x000000000000037f in ?? ()
```

#69 0x0000000000000000 in ?? ()
#70 0x0000000000000000 in ?? ()
#71 0x0000ffff00001f80 in ?? ()
#72 0x0000000000000000 in ?? ()
#73 0x0000000000000000 in ?? ()
#74 0x0000000000000000 in ?? ()
#75 0x0000000000000000 in ?? ()
−−−Type <return> to continue, or q <return> to quit−−−
#76 0x0000000000000000 in ?? ()
#77 0x0000000000000000 in ?? ()
#78 0x0000000000000000 in ?? ()
#79 0x0000000000000000 in ?? ()
#80 0x0000000000000000 in ?? ()
#81 0x0000000000000000 in ?? ()
#82 0x0000000000000000 in ?? ()
#83 0x0000000000000000 in ?? ()
#84 0x0000000000000000 in ?? ()
#85 0x0000000000000000 in ?? ()
#86 0x0000000000000000 in ?? ()
#87 0x0000000000000000 in ?? ()
#88 0x0000000000000000 in ?? ()
#89 0x0000000000000000 in ?? ()
#90 0x0000000000000000 in ?? ()
#91 0x0000000000000000 in ?? ()
#92 0x0000000000000000 in ?? ()
#93 0x0000000000000000 in ?? ()
#94 0x0000000000000000 in ?? ()
#95 0x0000000000000000 in ?? ()
#96 0x0000000000000000 in ?? ()
#97 0x0000000000000000 in ?? ()
#98 0x0000000000000000 in ?? ()
#99 0x0000000000000000 in ?? ()
#100 0x0000000000000000 in ?? ()
#101 0x0000000000000000 in ?? ()
#102 0x0000000000000000 in ?? ()
#103 0x0000000000000000 in ?? ()
#104 0x0000000000000000 in ?? ()
#105 0x0000000000000000 in ?? ()
#106 0x0000000000000000 in ?? ()
−−−Type <return> to continue, or q <return> to quit−−−
#107 0x0000000000000000 in ?? ()
#108 0x0000000000000000 in ?? ()
#109 0x0000000000000000 in ?? ()
#110 0x0000000000000000 in ?? ()
#111 0x0000000000000000 in ?? ()
#112 0x0000000000000000 in ?? ()
#113 0x0000000000000000 in ?? ()
#114 0x0000000000000000 in ?? ()
#115 0x0000000000000000 in ?? ()
#116 0x0000000000000000 in ?? ()
#117 0x0000000000000000 in ?? ()

```
#118 0x0000000000000000 in ?? ()
#119 0x0000000000000000 in ?? ()
#120 0x0000000000000000 in ?? ()
#121 0x0000000000000000 in ?? ()
#122 0x0000000000000000 in ?? ()
#123 0x0000000000000000 in ?? ()
#124 0x0000000000000000 in ?? ()
#125 0x0000000000000000 in ?? ()
#126 0x0000000000000000 in ?? ()
#127 0x0000000000000000 in ?? ()
#128 0x0000000000000000 in ?? ()
#129 0x0000000000000000 in ?? ()
#130 0x0000000000000000 in ?? ()
#131 0x0000000000000000 in ?? ()
#132 0x0000000000000000 in ?? ()
#133 0x0000000000000000 in ?? ()
Cannot access memory at address 0xffffffffb6275000
(kgdb)

d5# cat DB−DUAL−AMD64−RAID5
#
# GENERIC −− Generic kernel configuration file for FreeBSD/amd64
#
# For more information on this file, please read the handbook section on
# Kernel Configuration Files:
#
#
http://www.FreeBSD.org/doc/en_US.ISO8859−1/books/handbook/kernelconfig−config.html
#
# The handbook is also available locally in /usr/share/doc/handbook
# if you've installed the doc distribution, otherwise always see the
# FreeBSD World Wide Web server (http://www.FreeBSD.org/) for the
# latest information.
#
# An exhaustive list of options and more detailed explanations of the
# device lines is also present in the ../../conf/NOTES and NOTES files.
# If you are in doubt as to the purpose or necessity of a line, check first
# in NOTES.
#
# $FreeBSD: src/sys/amd64/conf/GENERIC,v 1.421.2.8 2005/03/30 01:05:53
murray Exp $

machine amd64
cpu HAMMER
ident DB−DUAL−AMD64−RAID5

# Debug Options
makeoptions DEBUG=−g
options DDB
options KDB
options BREAK_TO_DEBUGGER
```

```
options INVARIANT_SUPPORT
options INVARIANTS
options WITNESS
options WITNESS_KDB
options WITNESS_SKIPSPIN

# To statically compile in device wiring instead of /boot/device.hints
#hints "GENERIC.hints" # Default places to look for
devices.

options SCHED_4BSD # 4BSD scheduler
#options SCHED_ULE # 4BSD experimental scheduler
options INET # InterNETworking
#options INET6 # IPv6 communications protocols
options FFS # Berkeley Fast Filesystem
options SOFTUPDATES # Enable FFS soft updates support
#options UFS_ACL # Support for access control lists
options UFS_DIRHASH # Improve performance on big
directories
#options MD_ROOT # MD is a potential root device
#options NFSCLIENT # Network Filesystem Client
#options NFSSERVER # Network Filesystem Server
#options NFS_ROOT # NFS usable as /, requires
NFSCLIENT
#options NTFS # NT File System
#options MSDOSFS # MSDOS Filesystem
options CD9660 # ISO 9660 Filesystem
options PROCFS # Process filesystem (requires
PSEUDOFS)
options PSEUDOFS # Pseudo−filesystem framework
options GEOM_GPT # GUID Partition Tables.
options COMPAT_43 # Needed by COMPAT_LINUX32
options COMPAT_IA32 # Compatible with i386 binaries
options COMPAT_FREEBSD4 # Compatible with FreeBSD4
options COMPAT_LINUX32 # Compatible with i386 linux
binaries
options SCSI_DELAY=5000 # Delay (in ms) before probing SCSI
options KTRACE # ktrace(1) support
options SYSVSHM # SYSV−style shared memory
options SYSVMSG # SYSV−style message queues
options SYSVSEM # SYSV−style semaphores
options _KPOSIX_PRIORITY_SCHEDULING # POSIX P1003_1B real−time
extensions
options KBD_INSTALL_CDEV # install a CDEV entry in /dev
options AHC_REG_PRETTY_PRINT # Print register bitfields in debug
                             # output. Adds ~128k to driver.
options AHD_REG_PRETTY_PRINT # Print register bitfields in debug
                             # output. Adds ~215k to driver.
options ADAPTIVE_GIANT # Giant mutex is adaptive.
```

```
# Workarounds for some known−to−be−broken chipsets (nVidia nForce3−Pro150)
device atpic # 8259A compatability
options NO_MIXED_MODE # Don't penalize working chipsets

# Linux 32−bit ABI support
options LINPROCFS # Cannot be a module yet.

# Bus support. Do not remove isa, even if you have no isa slots
device acpi
device isa
device pci

# Floppy drives
device fdc

# ATA and ATAPI devices
device ata
#device atadisk # ATA disk drives
#device ataraid # ATA RAID drives
device atapicd # ATAPI CDROM drives
device atapifd # ATAPI floppy drives
#device atapist # ATAPI tape drives
options ATA_STATIC_ID # Static device numbering

# SCSI Controllers
#device ahc # AHA2940 and onboard AIC7xxx devices
device ahd # AHA39320/29320 and onboard AIC79xx devices
#device amd # AMD 53C974 (Tekram DC−390(T))
#device isp # Qlogic family
#device ispfw # Firmware for QLogic HBAs− normally a
module
#device mpt # LSI−Logic MPT−Fusion
#device ncr # NCR/Symbios Logic
#device sym # NCR/Symbios Logic (newer chipsets +
those of `ncr')
#device trm # Tekram DC395U/UW/F DC315U adapters

#device adv # Advansys SCSI adapters
#device adw # Advansys wide SCSI adapters
#device aic # Adaptec 15[012]x SCSI adapters,
AIC−6[23]60.
#device bt # Buslogic/Mylex MultiMaster SCSI adapters

# SCSI peripherals
device scbus # SCSI bus (required for SCSI)
#device ch # SCSI media changers
device da # Direct Access (disks)
device sa # Sequential Access (tape etc)
device cd # CD
device pass # Passthrough device (direct SCSI access)
device ses # SCSI Environmental Services (and SAF−TE)
```

```
# RAID controllers interfaced to the SCSI subsystem
#device amr # AMI MegaRAID
#device ciss # Compaq Smart RAID 5*
#device dpt # DPT Smartcache III, IV − See NOTES for
options
#device iir # Intel Integrated RAID
#device ips # IBM (Adaptec) ServeRAID
#device mly # Mylex AcceleRAID/eXtremeRAID
#device twa # 3ware 9000 series PATA/SATA RAID

# RAID controllers
device aac # Adaptec FSA RAID
#device aacp # SCSI passthrough for aac (requires CAM)
#device ida # Compaq Smart RAID
#device mlx # Mylex DAC960 family
#XXX pointer/int warnings
#device pst # Promise Supertrak SX6000
#device twe # 3ware ATA RAID

# atkbdc0 controls both the keyboard and the PS/2 mouse
device atkbdc # AT keyboard controller
device atkbd # AT keyboard
device psm # PS/2 mouse

device vga # VGA video card driver

device splash # Splash screen and screen saver support

# syscons is the default console driver, resembling an SCO console
device sc

# PCCARD (PCMCIA) support
# PCMCIA and cardbus bridge support
#device cbb # cardbus (yenta) bridge
#device pccard # PC Card (16−bit) bus
#device cardbus # CardBus (32−bit) bus

# Serial (COM) ports
#device sio # 8250, 16[45]50 based serial ports

# Parallel port
#device ppc
#device ppbus # Parallel port bus (required)
#device lpt # Printer
#device plip # TCP/IP over parallel
#device ppi # Parallel port interface device
#device vpo # Requires scbus and da

# If you've got a "dumb" serial or parallel PCI card that is
# supported by the puc(4) glue driver, uncomment the following
# line to enable it (connects to the sio and/or ppc drivers):
```

```
#device puc

# PCI Ethernet NICs.
#device de # DEC/Intel DC21x4x (``Tulip'')
#device em # Intel PRO/1000 adapter Gigabit
Ethernet Card
#device ixgb # Intel PRO/10GbE Ethernet Card
#device txp # 3Com 3cR990 (``Typhoon'')
#device vx # 3Com 3c590, 3c595 (``Vortex'')

# PCI Ethernet NICs that use the common MII bus controller code.
# NOTE: Be sure to keep the 'device miibus' line in order to use these NICs!
device miibus # MII bus support
#device bfe # Broadcom BCM440x 10/100 Ethernet
device bge # Broadcom BCM570xx Gigabit Ethernet
#device dc # DEC/Intel 21143 and various workalikes
device fxp # Intel EtherExpress PRO/100B (82557, 82558)
#device lge # Level 1 LXT1001 gigabit Ethernet
#device nge # NatSemi DP83820 gigabit Ethernet
#device pcn # AMD Am79C97x PCI 10/100 (precedence
over 'lnc')
#device re # RealTek 8139C+/8169/8169S/8110S
#device rl # RealTek 8129/8139
#device sf # Adaptec AIC−6915 (``Starfire'')
#device sis # Silicon Integrated Systems SiS 900/SiS
7016
#device sk # SysKonnect SK−984x & SK−982x gigabit
Ethernet
#device ste # Sundance ST201 (D−Link DFE−550TX)
#device ti # Alteon Networks Tigon I/II gigabit
Ethernet
#device tl # Texas Instruments ThunderLAN
#device tx # SMC EtherPower II (83c170 ``EPIC'')
#device vge # VIA VT612x gigabit Ethernet
#device vr # VIA Rhine, Rhine II
#device wb # Winbond W89C840F
#device xl # 3Com 3c90x (``Boomerang'', ``Cyclone'')

# ISA Ethernet NICs. pccard NICs included.
#device cs # Crystal Semiconductor CS89x0 NIC
# 'device ed' requires 'device miibus'
# XXX kvtop brokenness, pointer/int warnings
#device ed # NE[12]000, SMC Ultra, 3c503, DS8390 cards
#device ex # Intel EtherExpress Pro/10 and Pro/10+
#device ep # Etherlink III based cards
#device fe # Fujitsu MB8696x based cards
# XXX kvtop brokenness, pointer/int warnings
#device lnc # NE2100, NE32−VL Lance Ethernet cards
#device sn # SMC's 9000 series of Ethernet chips
#device xe # Xircom pccard Ethernet
```

```
# Wireless NIC cards
#device wlan # 802.11 support
#device an # Aironet 4500/4800 802.11 wireless NICs.
#device awi # BayStack 660 and others
#device wi # WaveLAN/Intersil/Symbol 802.11
wireless NICs.

# Pseudo devices.
device loop # Network loopback
device mem # Memory and kernel memory devices
device io # I/O device
device random # Entropy device
device ether # Ethernet support
#device sl # Kernel SLIP
#device ppp # Kernel PPP
#device tun # Packet tunnel.
device pty # Pseudo−ttys (telnet etc)
device md # Memory "disks"
#device gif # IPv6 and IPv4 tunneling
#device faith # IPv6−to−IPv4 relaying (translation)

# The `bpf' device enables the Berkeley Packet Filter.
# Be aware of the administrative consequences of enabling this!
# Note that 'bpf' is required for DHCP.
#device bpf # Berkeley packet filter

# USB support
#device uhci # UHCI PCI−>USB interface
#device ohci # OHCI PCI−>USB interface
#device usb # USB Bus (required)
#device udbp # USB Double Bulk Pipe devices
#device ugen # Generic
#device uhid # "Human Interface Devices"
#device ukbd # Keyboard
#device ulpt # Printer
#device umass # Disks/Mass storage − Requires scbus and da
#device ums # Mouse
#device urio # Diamond Rio 500 MP3 player
#device uscanner # Scanners
# USB Ethernet, requires mii
#device aue # ADMtek USB Ethernet
#device axe # ASIX Electronics USB Ethernet
#device cue # CATC USB Ethernet
#device kue # Kawasaki LSI USB Ethernet
#device rue # RealTek RTL8150 USB Ethernet

# FireWire support
#device firewire # FireWire bus code
#device sbp # SCSI over FireWire (Requires scbus and da)
#device fwe # Ethernet over FireWire (non−standard!)
```

```
# SMP
#device apic # I/O APIC
options SMP # SMP support

# IPFilter
options IPFILTER
options IPFILTER_LOG
options IPFILTER_DEFAULT_BLOCK
```