

## Re: Filter Hook

---

*Source:*

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2006-08/msg00000.1>

---

- *From:* "Doron Holan [MS]" <[doronh@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:doronh@xxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sun, 6 Aug 2006 10:33:16 -0700
- 

you can't reduce IRQL inline, you can only raise it and then lower it. if you truly want to synchronously process something, then queue it to a work item. if you want your filter to not negatively affect performance, learn how to process the results in the completion routine asynchronously

d

---

Please do not send e-mail directly to this alias. this alias is for newsgroup purposes only.

This posting is provided "AS IS" with no warranties, and confers no rights.

<x856256@xxxxxxxx> wrote in message  
[news:1154873993.596484.241370@xx](mailto:news:1154873993.596484.241370@xx)

No,

The code is not taking any spinlocks.  
Anyone has an idea how can I reduce the IRQL level inside the filter hook function?

Thanks,  
Guy

Don Burn wrote:

You cannot call a lot of functions at DISPATCH\_LEVEL. I am not well versed in filter hooks, so you need to determine if the raising to DISPATCH is avoidable. For instance, if the code takes a spinlock, could it take an ERESOURCE instead.

---

Don Burn (MVP, Windows DDK)  
Windows 2k/XP/2k3 Filesystem and Driver Consulting  
<http://www.windrvr.com>

Re: Filter Hook

Remove StopSpam from the email to reply

<x856256@xxxxxxxx> wrote in message  
[news:1154861486.219608.122660@xx](mailto:news:1154861486.219608.122660@xx)

Hello and thanks Don for the answer.

It is running in IRQL\_DISPATCH, I will try to reduce it and see what happens.

Thanks,  
Guy

Don Burn wrote:

A filter hook driver should not have an interrupt handler it is only concerned with packets as they are presented to it. You should not try to use IoConnectInterrupt with a software interrupt.

What IRQL are you running at when you crash, a common problem here would be calling the functions you mentioned at IRQL\_DISPATCH or higher.

--  
Don Burn (MVP, Windows DDK)  
Windows 2k/XP/2k3 Filesystem and Driver Consulting  
<http://www.windrvr.com>  
Remove StopSpam from the email to reply

<x856256@xxxxxxxx> wrote in message  
[news:1154814887.364085.142850@xx](mailto:news:1154814887.364085.142850@xx)

Hi,

Drivers are very new to me,  
can someone help me with

## Re: Filter Hook

the next issue  
please:

I have tried to set up a Filter Hook driver.  
I took an example code from codeproject (DrvFltIp) and it works ok on my computer (Windows XP).

When I try to process the packets more thoroughly than in this example code, my computer crashed (freezes or restarts immediately).  
The crash happens when I do something that involves a KeWaitForSingleObject or a KeDelayExecutionThread call (but I am not sure these are the only scenarios that cause a crash).

I looked in the dump file with WinDbg after the crash and saw that one of the last actions of the kernel were sending an interrupt and afterwards an exception. So my guess was that the kernel is sending a trap that was sent to it by the hardware to my driver to handle, but since I didn't set up an interrupt call back function, an exception is raised.  
The next thing I did was to try and set up an interrupt call back function, but this also

## Re: Filter Hook

caused a similar crash to the system (when I tried to pull out the parameters that I have to pass to the function "IoConnectInterrupt" from the isrStack). I tried to call the function "IoConnectInterrupt" from the function "DriverObject->MajorFunction[IRP\_MJ\_CREATE]" when got "IRP\_MJ\_CREATE" in "irpStack->MajorFunction" or when I got "IRP\_MN\_START\_DEVICE IRP" in "irpStack->MinorFunction". When I tried even to access the parameter "irpStack->Parameters->StartDevice.AllocatedResourcesTranslated->Count" (even without calling "IoConnectInterrupt") it caused a crash.

If anyone can help me understand what I am doing wrong, and why I am getting all these crashes I would be grateful.

Thanks,  
Guy