

Re: Packet Sniffer

Source:

<http://www.tech-archive.net/Archive/PocketPC/microsoft.public.pocketpc.developer.networking/2004-08/0071.html>

From: Jeff Kelley [MS] (jeffkel_at_online.microsoft.com)

Date: 08/24/04

Date: Mon, 23 Aug 2004 17:10:01 -0700

Netlog does not put an adapter into promiscuous mode. To get into promiscuous mode you would need to have an NDIS protocol driver bind to the adapter and set the current packet filter (OID_GEN_CURRENT_PACKET_FILTER) settings to include promiscuous mode (NDIS_PACKET_TYPE_PROMISCUOUS). The standard TCP/IP and TCP/IP6 protocol drivers released with the OS don't normally set the packet filter to promiscuous. You could use the NDISUIO driver to do this, but I would recommend against it as the high number of packets that would need to be forwarded from device.exe to the application using NDISUIO would probably exceed the system capacity.

So, I think that you would need to write your own NDIS protocol driver to configure the packet filter to see all the packets. You could still use Netlog to capture the data, or your driver could capture it in a manner of your choosing.

```
--
Jeff Kelley
Microsoft / Windows CE Networking
This posting is provided AS IS with no warranties, and confers no rights.
"John Spaith [MS]" <jspaith@ONLINE.microsoft.com> wrote in message
news:OSBzLyTiEHA.3016@tk2msftngp13.phx.gbl...
> If you have CE 4.2 Platform Builder, you can compile the source to a
netmon
> like capture routine that can run on CE devices. You can then tell this
to
> tool to capture packets and it will log it out in the desktop netmon .cap
> format. We don't have a packet viewer for CE, so you'll have to copy the
> generated .cap file to the desktop and look at it with desktop netmon.
>
> The core sniffer is in %_WINCEROOT%\public\COMMON\oak\utils\netlog and a
> command like app to stop/start/etc... the sniffer is in
> %_WINCEROOT%\public\COMMON\oak\utils\netlogctl. I don't know how great
the
> documentation is on all this, but in netlogctl the program isn't that
> complicated so you should be able to read the source yourself.
>
> I don't know whether this will put your card into promiscuous mode or not -
> that's another problem.
>
> --
> John Spaith
> Software Design Engineer, Windows CE
```

microsoft.public.pocketpc.developer.networking: Re: Packet Sniffer

> Microsoft Corporation
>
> Have an opinion on the effectiveness of Microsoft Embedded newsgroups?
Let
> us know!
> <https://www.windowembeddedeval.com/community/newsgroups>
>
> This posting is provided "AS IS" with no warranties, and confers no
rights.
> You assume all risk for your use. © 2003 Microsoft Corporation. All rights
> reserved.
>
> "YaQ" <yaq@chez.com> wrote in message
> news:9a27b912b7b5ccedc5fe8ee2d3fc0c15@localhost.talkaboutcomputing.com...
> > Hello,
> >
> > I would like to know how i can do an sniffer of frames. I try with the
RAW
> > socket, but it isn't implemented in Wince .NET 4.2.
> > I also read I need to pass my LAN card in promiscuous mode : I know my
> > card can do this with vxsniffer, and the OID to do this is define, but I
> > don't know how I can pass my card in this mode.
> >
> > Thx for your answer
> >
>
>