ETHEREAL-USERS: DECEMBER 2004

- *Subject*: Re: [Ethereal-users] What is "Linux cooked capture" and why does it add 2 bytes?
- *From*: Guy Harris <gharris@xxxxxxxxx>
- *Date*: Tue, 28 Dec 2004 11:49:45 -0800

Rutger Thomschitz wrote:

> However, just recently, as I was doing an experiment
> with VTun (an opensource VPN solution) I noticed Ethereal reporting
> "Linux cooked capture", which seems to add an additonal 2 bytes. What is
> "Linux cooked capture"?

On Linux, packet capturing is done by opening a socket. In systems with a 2.2 or later kernel, the socket is a PF_PACKET socket, either of type SOCK_RAW or SOCK_DGRAM.

A SOCK_RAW socket supplies the packet data including what the driver specified, when constructing the socket buffer (skbuff) holding the packet, to be the packet's link-layer header; a SOCK_DGRAM packet supplies only data above what was specified by the driver to be the link-layer header.

For the purposes of libpcap, which is the library used by programs such as tcpdump, Ethereal/Tethereal, snort, etc. to capture network traffic, a SOCK_RAW socket is usually the appropriate type of socket on which to capture, and is what's used.

Unfortunately, the purported link-layer header might be missing (as is the case for some PPP interfaces), or might contain random unpredictable amounts of data (as is the case for at least some interfaces using ISDN), or might not contain enough data to determine the type of the packet (as is the case with at least some ATM interfaces), so capturing with a SOCK_RAW socket doesn't always work well.

For interfaces of those types - and for interfaces of a type that libpcap currently doesn't have code to support - libpcap uses a SOCK_DGRAM socket, and constructs a fake link-layer header from the address supplied by a "recvfrom()" on that socket.

A "Linux cooked capture" is one done with libpcap using a SOCK_DGRAM socket.

- **References**:
  - **[Ethereal-users] What is "Linux cooked capture" and why does it add 2 bytes?**
    - *From:* Rutger Thomschitz
- Prev by Date: **RE: [Ethereal-users] Ethereal 0.10.8 crashes with page fault in msvcrt.dll**
- Next by Date: **Re: [Ethereal-users] Hidden text)**
- Previous by thread: **[Ethereal-users] What is "Linux cooked capture" and why does it add 2 bytes?**
- Next by thread: **[Ethereal-users] MSVCRT.DLL illegal operation on Windows 98**
- Index(es):
  - **Date**
  - **Thread**