

Re: Trying to monitor wireless traffic

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.networking/2007-12/msg00365.html>

- *From:* Syren Baran <syren@xxxxxx>
 - *Date:* Mon, 31 Dec 2007 02:15:07 +0100
-

Philippe Perrin schrieb:

Hello all

I would like to monitor the network traffic on my home wireless network. I would like to monitor which computers are connected, what they are doing, etc. Actually the same as I could do if I were using Ethereal from a router. My wireless network is protected with a WPA key, which I know of course.

I tried using Ethereal, but it sees only the packets issued by the computer it's running on, not the packets exchanged between the access point and other computers of the network.

Is there any way I can see/capture packets on a WPA-protected network, knowing the key???

You dont need the key to capture the packets.

You need to change the mode of your wireless card to monitor mode.

You'll obviously still need some tool to decrypt the captured packets with your key. If youre using ndiswrapper youre probably out of luck, as most (to my knowledge) windows drivers dont support monitor mode.

If you can set the mode via iwconfig <device> mode monitor Ethereal/Wireshark will display the raw packets from other devices as you cant send in monitor mode.

Thanks,
Philippe