

Using WinPcap on a Dial-up Connection

Mark E. Donaldson

WinPcap is normally not able to work with dial-up connections. The cause is the Microsoft NdisWan intermediate network driver, that avoids the protocols (except the ones written by Microsoft itself) to receive packets from PPP links. A trick to bypass this problem is to create the MS Network Monitor system device: WinPcap will be able to see it and through this device it will work on dial-up links.

Remember, you will have to download and install WinPcap 2.3 since older versions don't have this feature.

Adding this devices is quite simple if your OS includes Network Monitor (this is the case for example of Windows NT Server or Microsoft Windows 2000). In this case on Windows 2000 you will have have to:

- Go to Settings --> Control Panel --> Network and Dialup Connections.
- Right click on your dialup connection.
- Select properties then Networking then Install.
- Install Network Monitor.
- Exit and reboot.
- At this point, applications using WinPcap should see a new device: `\Device\Packet_NdisWanBh`. Use this device to capture on the dial-up link.

If you don't have Network Monitor to install, creating the device is possible but more tricky. Under Windows 2000 follow these steps:

- Go to the inf directory in your Windows folder (for example `c:\winnt\inf`). open the file `netrasa.inf` with a text editor.
- At the beginning of the file, find the string "ExcludeFromSelect". It's followed by a list of drivers that cannot be installed by the user.
- Inside this list, go to the line containing "MS_NdisWanBh" and comment it with a semicolon at the beginning.
- Save and close the file
- Go to Settings --> Control Panel --> add/remove hardware, select "add/troubleshoot a device", then "add a new device".
- Request the list of new hardware and from there select "other devices" and then "have disk". Pick `netrasa.inf`.
- From the manufacturers list select Microsoft, from the Models list select "Wan Miniport (Network Monitor)"
- Complete the installation and reboot.
- At this point, applications using WinPcap should see a new device: `\Device\Packet_NdisWanBh`. Use this device to capture on the dial-up link.

Note: we don't provide any guarantee that this process will work on your machine. This process can cause damage to your system, use it at your own risk.