NetStumbler v0.4.0 Release Notes

Marius Milner <mariusm@pacbell.net>

Thank you for your interest in NetStumbler. It is provided to you as a convenience, at no cost and without warranty. If you don't like it, or if you feel that it doesn't quite do what you want, you are free to delete it from your system. By installing or using it, you agree to be bound by the terms of the License Agreement.

NetStumbler is "beggarware". This means that you do not have to pay for a license to use it. However if you use it and like it, please consider making a donation at http://www.stumbler.net/donate to support future development, web hosting and other costs that I incur as a result of making this software available to you. Please bear in mind that I do this as a hobby in my spare time, not as a full time job.

Commercial and Government users are strongly encouraged to donate. The suggested donation is US$50 per copy. You may donate by visiting the web site http://www.stumbler.net/donate. You can pay in a variety of ways and may send a Purchase Order if needed.

What is NetStumbler?

NetStumbler is a tool for Windows that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It has many uses:

- Verify that your network is set up the way you intended.
- Find locations with poor coverage in your WLAN.
- Detect other networks that may be causing interference on your network.
- Detect unauthorized "rogue" access points in your workplace.
- Help aim directional antennas for long-haul WLAN links.
- Use it recreationally for WarDriving.

Requirements

General Requirements

The requirements for NetStumbler are somewhat complex and depend on hardware, firmware versions, driver versions and operating system. The best way to see if it works on your system is to try it.

Some configurations have been extensively tested and are known to work. These are detailed at http://www.stumbler.net/compat. If your configuration works but is not listed, or is listed but does not work, please follow the instructions on the web site.

The following are rules of thumb that you can follow in case you cannot reach the web site for some reason.

- This version of NetStumbler requires Windows 2000, Windows XP, or better.
- The Proxim models 8410-WD and 8420-WD are known to work. The 8410-WD has also been sold as the Dell TrueMobile 1150, Compaq WL110, Avaya Wireless 802.11b PC Card, and others.
- Most cards based on the Intersil Prism/Prism2 chip set also work.
- Most 802.11b, 802.11a and 802.11g wireless LAN adapters should work on Windows XP. Some may work on Windows 2000 too. Many of them report inaccurate Signal strength, and if using the "NDIS 5.1" card access method then Noise level will not be reported. This includes cards based on Atheros, Atmel, Broadcom, Cisco and Centrino chip sets.
- I cannot help you figure out what chip set is in any given card.

Firmware Requirements

If you have an old WaveLAN/IEEE card then please note that the WaveLAN firmware (version 4.X and below) does not work with NetStumbler. If your card has this version, you are advised to

upgrade to the latest version available from Proxim's web site. This will also ensure compatibility with the 802.11b standard.

Other Requirements and Compatibility Issues

- Your card must be configured in such a way that it can be seen by the management software that came with the card.
- The Microsoft-provided Orinoco drivers that come with Windows 2000 do not work with NetStumbler. Please visit Windows Update or www.proxim.com and upgrade to the latest drivers.
- When NetStumbler is in "auto reconfigure" mode (the default), it will occasionally disconnect you from your network. This enables it to perform its scans accurately, and is not a bug.
- If you have the WLAN card configured to connect to a specific SSID, NetStumbler may not report any accees points other than those that have that SSID. Configure your card with a blank SSID or, if a blank one is not permitted, "ANY" (without quotes).

Legal Note

I am not a lawyer. However as a user of this software, you need to be aware of the following.

In most places, it is illegal to use a network without permission from the owner. The definition of "use" is not entirely clear, but it definitely includes using someone else's internet connection or gathering information about what is on the network. It may include getting an IP address via DHCP. It may even include associating with the network.

The IP address reporting functionality in NetStumbler is for you to check the settings of your own network, and for corporate users to identify rogue access points operating within their organization. If you are doing neither of these things, it is suggested that you disable TCP/IP on your wireless adapter. This will help you to avoid possible legal trouble.

Marius Milner, NetStumbler.com and stumbler.net accepts no liability for damages caused by use of this software. For further

information please consult the License Agreement that can be found both in the installer and in the online help.

Mini-FAQ

Q1: NetStumbler reports "No wireless card found". Why?

> **A1:** Please check the compatibility lists above. Perhaps your adapter is not supported.

Q2: Why doesn't NetStumbler see the access point right next to my machine?

> **A2a:** The access point is configured not to respond to broadcast probes. Most manufacturers call this "disable broadcast SSID" or "closed". NetStumbler cannot see these networks unless you know the SSID and have your machine configured to connect to it.
>
> **A2b:** Your wireless card is configured to connect to a specific SSID. Try setting it to connect to a blank SSID or to "ANY" (without quotes).

Q3: What 802.11 frames does NetStumbler send?

> **A3a:** It sends out a probe request about once a second, and reports the responses. This is known as Active Scanning.
>
> **A3b:** (ORiNOCO only and with "Query APs for names" enabled) When it is connected to a BSS network, it will attempt to get the name of the access point. When it is connected to an IBSS network, it will try to get the names of all locally visible peers. This is done via Proxim's proprietary WMP protocol.
>
> **A3c:** (Only when connected to a Cisco access point and with "Query APs for names" enabled and with a valid IP address) It

will attempt to use Cisco's IAPP protocol to get the name and IP address of the access point.

A3d: If you leave TCP/IP enabled, your adapter may attempt to get a DHCP lease or send other traffic. NetStumbler will record the fact that you were issued an IP address.

Q4: Does NetStumbler listen for beacons, or put my card into promiscuous or RFMON mode?

A4: This is called Passive Scanning and is not in this version.

Q5: I'm seeing access points appear briefly and then disappear for a long time. What's happening?

A5a: Some wireless networks can be configured not to respond to probes every time they hear a request.

A5b: If you see lots of networks that appear briefly and then disappear forever, you may have found a FakeAP installation.

Q6: Why does NetStumbler disconnect me from the network?

A6: If you have "Options->Reconfigure card automatically" checked, it will configure your card with a profile that uses a null SSID and BSS mode (It will not change your WEP settings). Also, when it sees another network that has a better signal than the one you're connected to, it may disconnect the current connection so that it can get the AP name on the other network.

Q7: Does NetStumbler detect ROR and COR installations?

A7: Not usually. They are not always fully compliant with 802.11b and therefore may not be visible to NetStumbler.

Q8: Should I allow Windows XP to manage my wireless settings?

> **A8:** Probably not. When you are not connected to a network, XP will cycle through your favorite network names attempting to connect to them. While this is happening, NetStumbler may not see all available networks. It is recommended that you stop the "Wireless Zero Configuration" service while NetStumbler is running. You can do this by switching on "Auto Reconfigure", from Control Panel, or by running the command "net stop wzcsvc".

Q9: When will you support wireless card X? When will you add new feature Y that I want?

> **A9:** I work on this in my spare time. I can make no commitment to dates for new features or bug fixes. If you would like to help me support a particular piece of hardware, please consider sending me a sample rather than complaining that it isn't supported.

Q10: What does "Auto Reconfigure" actually do?

> **A10a:** When using the ORiNOCO driver, it stops the Wireless Zero Configuration service and makes sure that the card is always set to a blank SSID and BSS mode.
>
> **A10b:** When using the Prism driver, it stops the Wireless Zero Configuration service and checks for a blank or "ANY" SSID. If necessary, it makes changes to the card's registry settings and prompts you to reinsert the card.
>
> **A10c:** On all other drivers, it stops the Wireless Zero Configuration service and then does nothing. Usually this is a good thing, but you should experiment with it.

Release History

Version 0.4.0 (April 21, 2004)

- Fixed bug (introduced in 0.3.30) that caused "Reconfigure" to put ORiNOCO cards into a state where they would report no access points.
- Support for Atheros, Atmel, Intersil Prism2 based wireless cards. Improved support for Cisco cards.
- Allow use of Serial Earthmate GPS. (USB Earthmate should already work using NMEA and serial driver)
- If you scroll all the way to the right of the graph view, it will auto-scroll new data.
- Fixed bug (introduced in 0.3.30) in graph view: corrupted display when scrolling.
- Fixed bug in graph view: improper scroll bar tracking with large data sets.
- If "Reconfigure" is on, the Windows XP Wireless Zero Configuration service will be stopped when you start scanning. It is restarted when the application exits.
- If you connect to a network that supports DHCP, the IP subnet is reported.
- If the access point is discovered in the ARP table, its IP address is reported.
- While you are scanning, the system will be prevented from going into standby unless power is critically low.
- Large files load several times faster than before (though the really large ones still don't load fast enough).
- A whole lot of new Scripting features.

Version 0.3.30 (August 18, 2002):

- Allow configuration of baud rate and other settings for GPS.
- Added "Default SSID" filter to tree view.
- Close connection to NIC when scanning is not happening.
- Moved much of the configuration to a dialog box.
- Support for user-provided scripts to be invoked when various events occur.
- Many errors are reported in a more meaningful way.
- Workaround for problem with driver version 7.62.
- GPS now supports Garmin proprietary protocols.

- (NetStumbler) MIDI output of signal strength(s).
- (NetStumbler) Proper installation package (thank you Nullsoft)
- (NetStumbler) Use NDIS 5.1 native 802.11 features for scanning on Cisco and some Prism cards on Windows XP.
- (NetStumbler) Support for 802.11a on Windows XP.
- (NetStumbler) Support for USB devices on 98/Me.

Version 0.3.23 (February 14, 2002):

- Count of filtered and all APs in bottom right corner.
- Handle "ASTRAL" on serial port so that Tripmate can be used.
- Autosave feature added.
- Popup menu allows deletion of APs from list.
- Complete rewrite of NIC access code in preparation for multiple chipset support.
- (MiniStumbler) First public release. No tree or graph view.

Version 0.3.22 (August 6, 2001):

- Fixed bug where system suspend or other long delays would stop the GPS from updating.
- Make AP name collection optional. Stop flooding LAN with WMP packets.
- Handle misreported WEP on some IBSS networks.
- Make card reconfiguration optional.
- Windows Me support.

Version 0.3.21 (July 16, 2001):

- Support for Dell Mini-PCI card.

Version 0.3.20 (July 13, 2001):

- Added Beggarware license agreement.

Version 0.3.10 (July 12, 2001):

- GPS code largely rewritten.
- GPS on ports up to COM8 instead of COM4.
- Adjustable scan speed.
- Export summary files.

Version 0.3.00 (June 19, 2001):

- Support for even more OEM cards (Now supported: Lucent, Dell 1150, Toshiba, Compaq, Enterasys/Cabletron, Elsa MC-11, ARtem Comcard, Buffalo Airstation WLI-PCM-L11)
- Currently connected AP appears in a bold font in the tree view, and has an asterisk by its channel number in list view
- This session's previously connected APs are marked with a '+' in list view
- Added Ctrl+B key shortcut to toggle scanning
- Filtering by channel number, ESSID, and capability flags
- Saves entire data log as well as AP summary data
- Graphical view of signal and noise over time if you select a single AP
- Automatic reconfiguration of card, if desired. This will take your card out of peer mode, and unset the desired SSID if you have one. It also disassociates from networks that are out of range.
- Creating a new document can be configured to automatically start scanning or not
- Get the name of an AP, where supported (it won't be unless the AP doesn't have WEP, or you have the WEP key configured). It looks like Aironet APs don't support this.
- Merge data files together
- Ability to drag and drop column headers
- Remembers view settings when switching views, and you can save the current settings as defaults
- Read and write Pete Shipley's log format, as well as an extended version
- Some APs respond to scan requests on multiple channels. These now appear as one item rather than multiple APs.
- Uses NS1 file extension
- Improved handling of invalid files
- GPS should no longer lock up and stop responding
- Removed non-functional toolbar buttons

Version 0.2.00 (May 16, 2001):

- Works only with Lucent, Dell, and Toshiba cards
- Doesn't crash the other PCMCIA devices that you have installed.
- Should now work with USB devices.

- Runs on Windows 2000, 95, 98 (and Me? – Untested).
- Saves the data instead of making a 0 byte file.
- Supports NMEA0183 GPS devices. It stores the location of the highest recorded SNR.
- Lists the brand of AP hardware (based on the MAC address)
- Shows current signal strength as well as the max, and has a dot that is colored to show the strength next to the AP name
- Tree view to the left shows Channels, and Names; this will do more in a future version.
- Makes a sound when it first sees an AP

Version 0.1.00 (May 5, 2001):

- Initial proof of concept version, first public release.
- Works only on Windows 2000.
- Works with most Hermes chipset cards, but not if any other PCMCIA devices are installed.
- Doesn't save data (creates a 0 byte file).