



USER GUIDE

SNAP Sniffer

©2008-2016 Synapse, All Rights Reserved. All Synapse products are patent pending. Synapse, the Synapse logo, SNAP, and Portal are all registered trademarks of Synapse Wireless, Inc.

Doc# 116-061520-013-A000

6723 Odyssey Drive // Huntsville, AL 35806 // (877) 982-7888 // Synapse-Wireless.com

Disclaimers

Information contained in this Manual is provided in connection with Synapse products and services and is intended solely to assist its customers. Synapse reserves the right to make changes at any time and without notice. Synapse assumes no liability whatsoever for the contents of this Manual or the redistribution as permitted by the foregoing Limited License. The terms and conditions governing the sale or use of Synapse products is expressly contained in the Synapse's Terms and Condition for the sale of those respective products.

Synapse retains the right to make changes to any product specification at any time without notice or liability to prior users, contributors, or recipients of redistributed versions of this Manual. Errata should be checked on any product referenced.

Synapse and the Synapse logo are registered trademarks of Synapse. All other trademarks are the property of their owners. For further information on any Synapse product or service, contact us at:

Synapse Wireless, Inc.
6723 Odyssey Drive
Huntsville, Alabama 35806
256-852-7888
877-982-7888
256-924-7398 (fax)

www.synapse-wireless.com

License governing any code samples presented in this Manual

Redistribution of code and use in source and binary forms, with or without modification, are permitted provided that it retains the copyright notice, operates only on SNAP® networks, and the paragraphs below in the documentation and/or other materials are provided with the distribution:

Copyright 2008-2016, Synapse Wireless Inc., All rights Reserved.

Neither the name of Synapse nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. SYNAPSE AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THIS SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL SYNAPSE OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE, EVEN IF SYNAPSE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

1.	Introduction	1
2.	Installation	1
3.	Using the SNAP Sniffer	3
4.	Important Notes.....	6

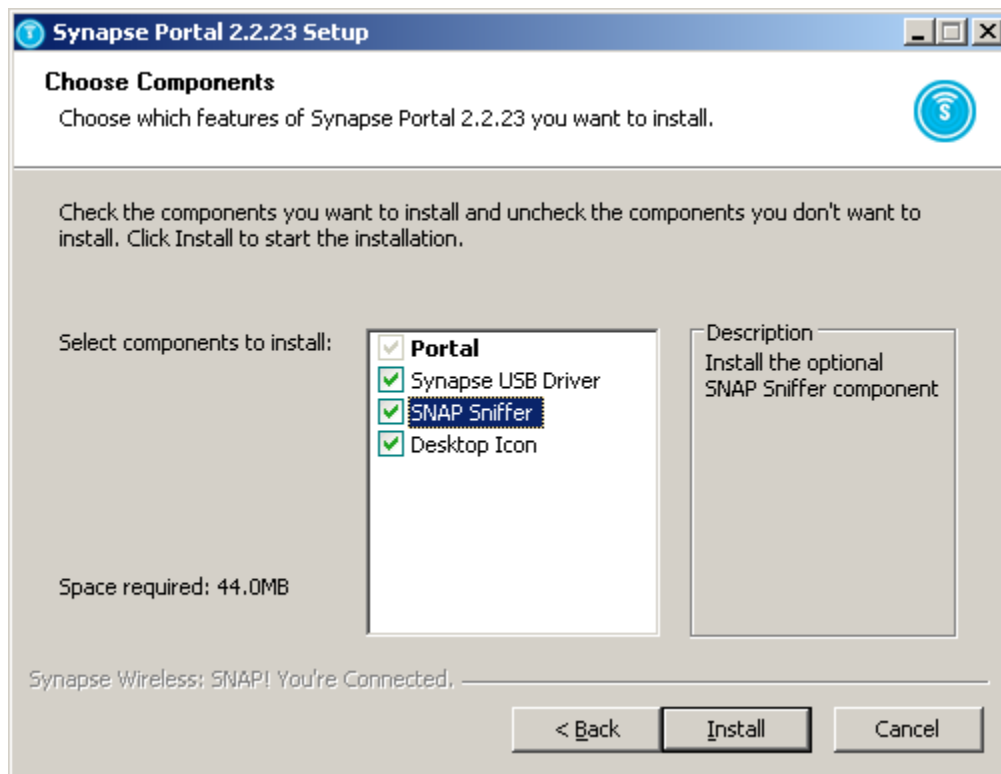
1. Introduction

The SNAP Sniffer provides developers more insight into how their SNAP network works and aids in the debugging of SNAPpy scripts. Specifically the SNAP Sniffer shows detailed information about packets being sent by the nodes in a SNAP network.

The SNAP Sniffer comprises two parts: the GUI, which displays packets; and a special firmware image for a SNAP node, which sends received packets to the GUI.

2. Installation

The files needed to run the SNAP Sniffer are included with Portal (starting with version 2.2.23). By default the SNAP Sniffer is selected to be installed:

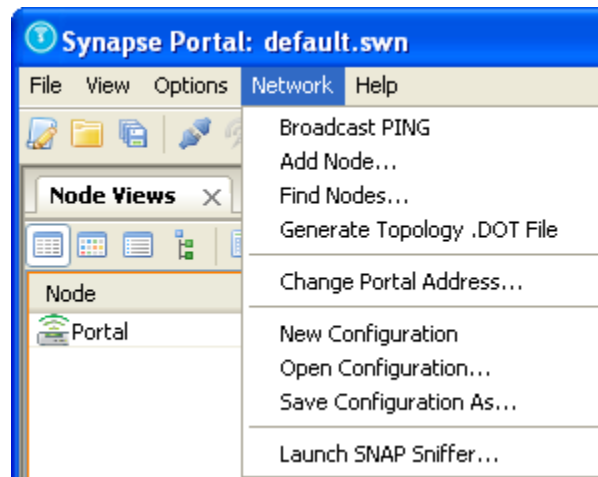


Once installed the SNAP Sniffer can be started from the Start Menu on Windows:



On OS X, the Sniffer and Portal are available from the /Applications/Synapse directory. On Linux, use the SnapSniffer application in the /usr/lib/portal directory.

Also the SNAP Sniffer can be started from the Network menu within Portal:



Before starting the SNAP Sniffer, you will need to convert one of your SNAP nodes to a sniffer node. This node must be directly connected to the PC's serial or USB port while sniffing. Portal can be used to load the special "SNAP Sniffer" firmware image onto the node.

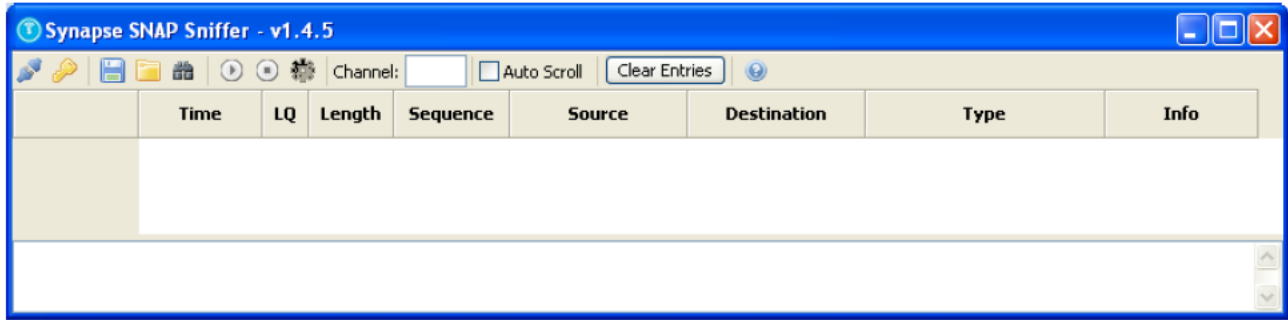
Portal includes a collection of current Synapse Firmware Image (.SFI) files in its installation. These firmware images allow you to refresh or upgrade the firmware in your network nodes, or to load the SNAP Sniffer image on to a node. The process for loading the .SFI onto a node is the same as upgrading the firmware on any SNAP node. Please see the "SNAP Reference Manual" or "Portal Users Guide" for detailed instructions on this process. The only SNAP node that needs to be running the Sniffer firmware image is the node directly connected to the PC that is running the SNAP Sniffer GUI.

While hardware variations between nodes often require different firmware files for running SNAP (e.g., the RF220UF1 requires different firmware than the RF220SU module), the Sniffer firmware is more generalized. Firmware for the ATmega128RFA1 is appropriate for any SNAP node based on this hardware, including all the RF200, RF220, RF266, SM200, SM220, SNAPstick 200, and SNAPstick 220 modules. (The RF200 Sniffer firmware delivered with Portal is actually just a copy of the ATmega128RFA1 firmware.)








NOTE: The SNAP Sniffer works regardless of what encryption is present. It detects traffic, which doesn't affect encryption. If you're working with encrypted nodes no special SNAP Sniffer settings are needed.

3. Using the SNAP Sniffer

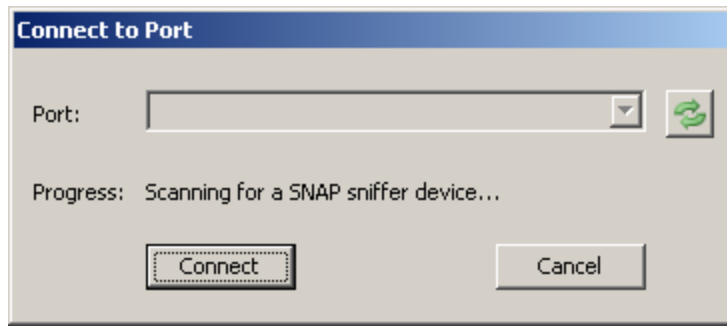
Once launched, the SNAP Sniffer's main GUI window should be displayed:



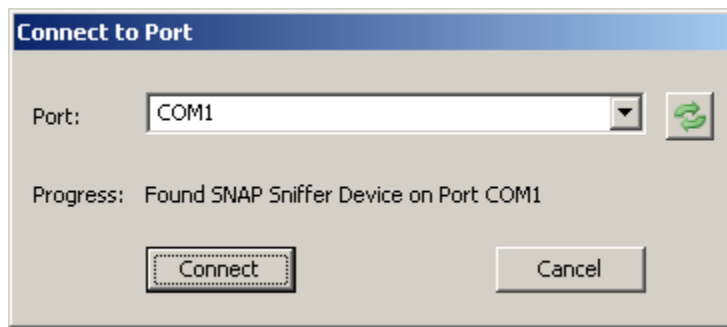
The toolbar allows quick access to the SNAP Sniffer's main functions:

Toolbar Option	Description
	Connect/disconnect from a SNAP Sniffer node
	Configure network encryption
	Save the currently captured packets to a Synapse SNAP Sniffer (.sss) file
	Opens an .sss file of previously captured packets. This option is only available when disconnected from a SNAP Sniffer node
	Instruct the SNAP Sniffer node to start capturing packets from the specified channel
	Instruct the SNAP Sniffer node to stop capturing packets
	Set the radio rate at which the node should monitor traffic. This requires a Sniffer node capable of receiving different radio rates, and uses the same rate enumerations that the SNAP nodes on that platform would use. See the <code>setRadioRate()</code> function in the SNAP Reference Manual for more information.
Channel: <input type="text"/>	Select the channel to have the SNAP Sniffer node to listen on
<input type="checkbox"/> Auto Scroll	Continuously scroll to display the last received packet
Clear Entries	Clear all received packets from the capture buffer


When connecting to a SNAP Sniffer node, the familiar connect dialog is displayed:



Once a SNAP sniffer device has been found¹ it will indicate which port the device is located on:



Click the “Connect” button if the correct sniffer was found, or the “Port” drop down can be used to select the correct COM port.

Now that the GUI is connected it is possible to start receiving packets from a channel. For example, to see the SNAP packets being sent on channel 13, type 13 in the channel box and press the  button. As packets are received they are displayed in the grid below the toolbar:

	Time	LQ	Length	Sequence	Source	Destination	Type	Info
1	0.000	63	21	bb	000002 (526f79)	0001 TTL=4	Multicast RPC	Method: vmStat(5, 2)
2	0.006	48	21	bb	000002 (546f62)	0001 TTL=3	Multicast RPC	Method: vmStat(5, 2)
3	0.012	63	21	bb	000002 (436f6b)	0001 TTL=3	Multicast RPC	Method: vmStat(5, 2)
4	0.018	83	21	bb	000002 (506570)	0001 TTL=3	Multicast RPC	Method: vmStat(5, 2)
5	0.019	72	21	bb	000002 (4a6f6c)	0001 TTL=3	Multicast RPC	Method: vmStat(5, 2)
6	0.190	48	22	51	546f62	0001	Mesh Broadcast	Type: RREQ - 546f62 is looking for 000002 (MAXHOPS=2)
7	0.204	83	25	c3	506570	0001	Mesh Broadcast	Type: RREQ - 546f62 is looking for 000002 (MAXHOPS=1)
8	0.205	63	25	e0	526f79	0001	Mesh Broadcast	Type: RREQ - 546f62 is looking for 000002 (MAXHOPS=1)
9	0.219	63	25	6c	436f6b	0001	Mesh Broadcast	Type: RREQ - 546f62 is looking for 000002 (MAXHOPS=1)
10	0.225	72	25	c2	4a6f6c	0001	Mesh Broadcast	Type: RREQ - 546f62 is looking for 000002 (MAXHOPS=1)
11	0.233	63	22	e1	526f79	546f62	Mesh PTP	Type: RREP - 000002 responding to 546f62
12	0.234	48	8	e1	546f62	526f79	ACK	
13	0.244	48	45	50	546f62	000002 (526f79)	RPC	Method: tellVmStat(20485, 'Tob')
14	0.245	63	8	50	526f79	546f62	ACK	
15	1.123	82	22	c5	506570	0001	Mesh Broadcast	Type: RREQ - 506570 is looking for 000002 (MAXHOPS=2)
16	1.129	63	25	6d	436f6b	0001	Mesh Broadcast	Type: RREQ - 506570 is looking for 000002 (MAXHOPS=1)

In this example, Portal was started which caused us to send a “broadcast ping” and discover the other nodes in this network.

The grid contains the following pieces of information per packet:

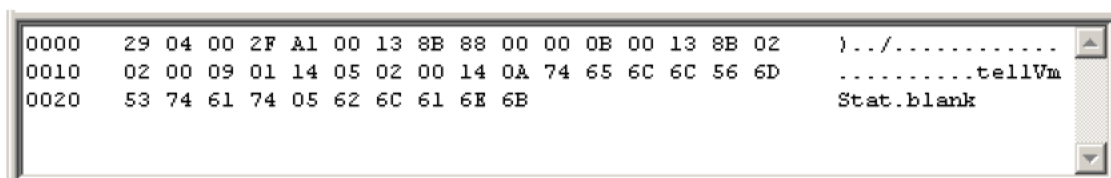
¹ On Linux, connecting a Sniffer node requires the same permissions adjustments necessary for connecting a SNAP node. See the readme file delivered with the Linux Portal application for more information.

Column Name	Description
Time	The time, in seconds, of packet receipt as calculated by the SNAP Sniffer node (relative to the first packet heard since the Sniffer was connected or cleared)
LQ	The link quality as received by the SNAP Sniffer node in negative dBm (lower is stronger)
Length	The total length in bytes of the received packet
Sequence	The sequence number, as specified by the sender, of the received packet
Source	The originating source address of the received packet. An address in parenthesis indicates the address of the node who forwarded the packet
Destination	The final destination address of the received packet. An address in parenthesis indicates the address of the node who forwarded the packet
Type	The packet type
Info	Information about the received packet, which varies by packet type

Taking a look again at the example capture from Portal starting up we can determine the following about each packet:

1. Portal at address 00.00.02 sends a multicast RPC vmStat with parameters 5 and 2 which are forwarded by the bridge node, 52.6f.79.
2. The vmStat(5, 2), which is the “broadcast ping”, was re-broadcasted by node 54.6f.62, 43.f6.6b, 50.65.70 and 4a.6f.6c.
3. Node 54.6f.62 sends a mesh broadcast route request (RREQ) message trying to determine a route to Portal at address 00.00.02. Note that the node waited 0.190 seconds to respond to the vmStat since Portal asked all nodes to randomize their response over a 2-second interval (specified on Portal’s preferences screen).
4. The other nodes in the network re-broadcasted the RREQ packet.
5. Portal responds back with a mesh point-to-point route reply (RREP) message to node 54.6f.62 via the bridge node, 52.6f.79.
6. Node 54.6f.62 acknowledges the RREP packet with an ACK packet. The sequence number on the ACK packet matches the sequence number of the message acknowledged by that packet.
7. Now that node 54.6f.62 knows the route to Portal, he sends an RPC call to Portal, invoking the tellVmStat function
8. Next the other nodes similarly try to determine a route to Portal, rebroadcasting their requests if they are not responded to the first time.

The SNAP Sniffer can also display a raw hexadecimal display of each packet received, by clicking on the packet in the grid:



4. Important Notes

Currently when the SNAP Sniffer encounters a packet it cannot decode, including a packet that is encrypted when the Sniffer is not configured to use the same encryption and encryption key, the GUI will include the packet in the list but will not be able to reliably display the Type or Info. If the Sniffer is configured to use encryption (either AES or Basic), it will decrypt encrypted packets and display them, marked with an asterisk in the Type column, and will continue to display unencrypted radio traffic without the asterisk.

Additionally, if a packet is not a valid SNAP packet it will not be decoded by the GUI.

A SNAP Sniffer node cannot be used for any function other than capturing received packets to the SNAP Sniffer GUI. This prevents the SNAP Sniffer node from acting as a repeater or bridge. However, it is possible to reload the regular SNAP firmware on the node using Portal. Once the regular SNAP firmware is reloaded on the node, it can resume running SNAPpy scripts, etc.

It is also important to note that the sniffer can only show packets that occurred within its wireless reception range. If you have a large (mutli-hop) network, there may be remote communications taking place that the SNAP sniffer cannot “hear”.