

# Using filters with the Daintree Networks Sensor Network Analyzer

Application Note AN028



Copyright © 2003-2009, Daintree Networks Inc  
All rights reserved

## Trademarks and acknowledgements

- ZigBee® is a registered trademark of the ZigBee Alliance.
- 802.15.4™ is a trademark of the Institute of Electrical and Electronics Engineers (IEEE).
- SimpliciTI™ is a trademark of Texas Instruments.

These trademarks are registered by their respective owners in certain countries only. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

## Disclaimer

This note and any examples it contains are provided as-is and are subject to change without notice. Except to the extent prohibited by law, Daintree Networks makes no express or implied warranty of any kind with regard to this guide, and specifically disclaims the implied warranties and conditions of merchantability and fitness for a particular purpose. Daintree Networks shall not be liable for any errors or incidental or consequential damage in connection with the furnishing, performance or use of this guide and the examples included.

The software described in this guide is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording, for any purpose other than the purchaser's personal use, without the written permission of Daintree Networks.

Sensor Network Analyzer Release 3.0 (2009-02-19)

## About Daintree's Sensor Network Analyzer

Daintree's Sensor Network Analyzer (SNA) provides the industry's most comprehensive solution for developing, decoding, debugging and deploying wireless embedded networks. Well known as an expert tool for IEEE 802.15.4 and ZigBee, the SNA has recently extended its support to include additional standards-based and proprietary network protocols including 6LoWPAN, SimpliciTI (from Texas Instruments) and Synkro (from Freescale Semiconductor), with the ability to easily add more protocols. (See [www.daintree.net/technology](http://www.daintree.net/technology) for an up-to-date list of supported protocols.)

The SNA's features include the following:

- A powerful protocol decoder that allows you to drill down to the packet, field, and byte level
- Unique visualization capabilities that allow you to view all 15.4 network devices and interactions simultaneously
- Customization options including filtering, labeling and color-coding to make it easy to locate packets of interest
- Performance measurements for 802.15.4 and ZigBee
- Intuitive tools that make it easy to perform complex functions such as multi-node and multi-channel capture and ZigBee commissioning

The SNA also supports a wide range of third-party semiconductor and development boards as capture devices: both USB and Ethernet. (See [www.daintree.net/products/hardware.php](http://www.daintree.net/products/hardware.php) for an up-to-date list of supported hardware.)

Available in three different editions – Professional, Standard and Basic – you can pay for the functionality you need today, and upgrade in future as your needs increase.

Visit [www.daintree.net](http://www.daintree.net) to find out more about Daintree's wireless embedded analysis products.

## About packet filters

Have you ever wondered what was going on in a wireless embedded network, but couldn't figure it out? You looked, but all you saw was a confusing collection of packets being sent between many different devices, all communicating different things.

Wouldn't it be helpful to know which devices were sending and receiving packets, when, and how often? Don't you wish there was an easy way to check the performance of routers, and see whether they were forwarding or dropping packets?

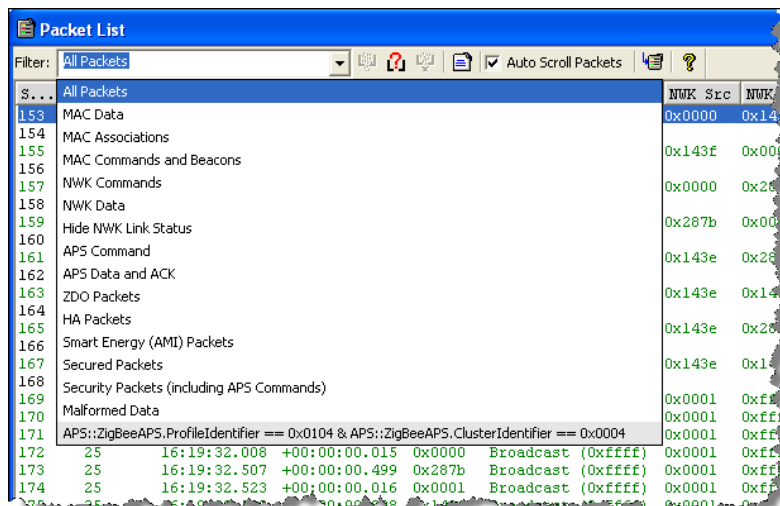
One of the key benefits of wireless embedded protocols such as ZigBee is the ability to create a network of many devices that can communicate independently with each other over a wireless meshed network. Unfortunately, this independence creates challenges when it comes to troubleshooting what is going on.

The simplest solution to this is to filter for packets of interest. Basic filtering by packet type or protocol layer will help narrow the search very quickly. This application note provides examples of how you can filter using the SNA.

Note that from release 3.0, the SNA supports multiple network protocols (not just ZigBee and IEEE 802.15.4). You use the SNA's **Protocols** menu to select which network protocol and layers you want to decode, and the selected protocol determines which filters are available. The examples in this application note show ZigBee PRO, with instructions that are valid for ALL network protocols.

## Filtering packets

The **Filter** menu in the Packet List window provides a range of filters that can be used to quickly reduce many thousands or tens of thousands of packets to just the application-layer communication. This hides all of the other network maintenance and lower-layer acknowledgement exchanges, which can be a distraction.



At the bottom of the Filter list, you'll see a much more complex filter command – in fact, virtually any filter can be constructed to narrow your search down to very specific combinations of packet header values.

In this application note, we'll start by exploring the simplest way to create filters (using context sensitivity), before moving on to manually creating filters using the SNA's Define Filter tool.

## Context sensitivity

Very often, it is much easier to look at the network visually rather than a list of packets. The SNA's visual windows (which support all network protocols that use IEEE 802.15.4 MAC Associations) provide a good starting point. When you then want to drill down into a bit more detail, you can – for example by requesting all packets transmitted by a particular device.

The example below shows a device selected from the visual display, with a filter selected to show all packets transmitted by this device (at the Network layer). The Packet List window beneath the visual display shows only the filtered packets.

The screenshot shows the 'Visual Device Tree' window with a network diagram. A context menu is open over a device, with the 'Filter' option selected. The 'Filter' submenu is open, showing 'MAC' and 'NWK' options. The 'NWK' option is selected, and the 'Source Device' sub-option is also selected. Below the diagram is the 'Packet List (NWK)' window, which displays a table of filtered packets. The filter applied is '(NWK::ZigBeeNWK) && (IEEE802.15.4::IEEE802.15.4.SourcePANIdentifier==0x12ef | IEEE802.15.4::IEEE802.15.4.SourcePANIdentifier==0x0001) && (IEEE802.15.4::IEEE802.15.4.SourcePANIdentifier==0x12ef | IEEE802.15.4::IEEE802.15.4.SourcePANIdentifier==0x0001)'. The table shows columns for Seq No, Channel, Time, Time Delta, MAC Src, MAC Dest, NWK Src, NWK Dest, Protocol, Packet Type, Security, and FCS.

Seq No	Channel	Time	Time Delta	MAC Src	MAC Dest	NWK Src	NWK Dest	Protocol	Packet Type	Security	FCS
151	25	16:18:59.603		0x0001	0x0000	0x0001	0x0000	ZigBee ZDP	ZDP: BindResp		
169	25	16:19:31.977	+00:00:32.373	0x0001	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
170	25	16:19:31.983	+00:00:00.007	0x287b	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
171	25	16:19:31.993	+00:00:00.010	0x143f	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
172	25	16:19:32.008	+00:00:00.015	0x0000	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
173	25	16:19:32.507	+00:00:00.499	0x287b	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
174	25	16:19:32.523	+00:00:00.016	0x0001	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
175	25	16:19:32.532	+00:00:00.008	0x143e	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
176	25	16:19:32.676	+00:00:00.144	0x0000	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
177	25	16:19:33.294	+00:00:00.618	0x0001	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
178	25	16:19:33.300	+00:00:00.006	0x143e	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
179	25	16:19:33.302	+00:00:00.002	0x287b	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
180	25	16:19:33.304	+00:00:00.003	0x143e	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
181	25	16:19:33.331	+00:00:00.026	0x0000	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
182	25	16:19:33.378	+00:00:00.048	0x0000	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
183	25	16:19:34.010	+00:00:00.632	0x0000	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓
184	25	16:19:34.711	+00:00:00.701	0x0000	Broadcast (0xffff)	0x0001	0xffff	ZigBee ZCL	HA: On/off: Toggle		✓

This simple right-click and menu selection provides a host of other interesting information. For example, in the example above, the fourth column of the Packet List window (titled "Time Delta") shows the interval between successive network packet transmission by this device.

The same filter is also applied to the Packet Timeline window below, which shows when packets were transmitted by this device. Since this is a network-layer packet, this view also shows how network layer communication by device 0001 also trigger multi-hop communication by other devices in assisting 0001 get its packets to its destination.

The screenshot shows the 'Packet Timeline' window. The 'View by:' dropdown is set to 'MAC Source'. The 'Channel Summary' section shows the PAN ID: 0x12ef and the MAC addresses of the devices: 0x0001 (cc:cc:cc:..), 0x0000 (00:50:c2:..), 0x143e (cc:cc:cc:..), 0x287b (cc:cc:cc:..), and 0x143f (cc:cc:cc:..). The timeline shows a series of green bars representing packet transmissions, with a significant cluster of activity between 150 and 200 on the x-axis.

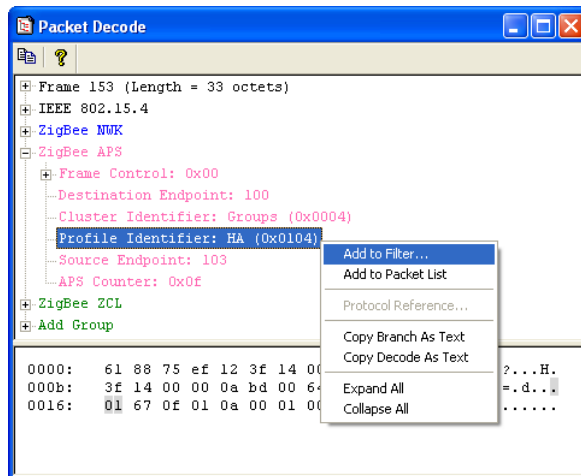
## Creating filters

The SNA provides a number of pre-defined filters for each network protocol it supports. You can edit any pre-defined filter to create a new filter, or else create new filters from scratch.

### Creating a simple filter

The Packet Decode window provides a quick and easy way to create a custom filter. This window shows a detailed decode (down to the field and byte level) of the packet currently selected in the Packet List window.

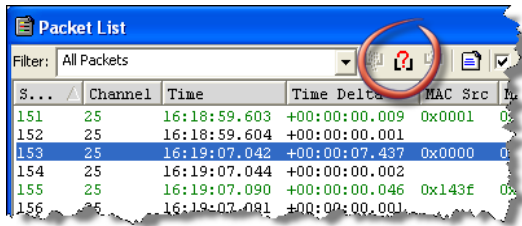
1. Select the packet of interest from either the Packet List or Packet Timeline window to display its details in the Packet Decode window.
2. In the Packet Decode window, drill-down to the field for which you want to create the filter. Then right-click that field and select **Add to Filter**.



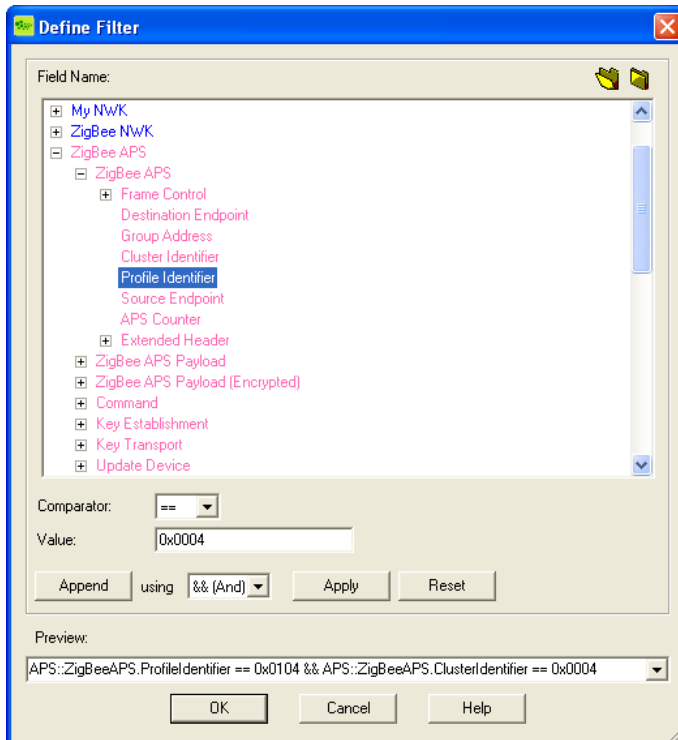
3. Use the Define Filter window to create the filter. The default is for the filter to match the selected field and value. You can change the field, comparator and value as required. The following comparators are available:
  - == (Equal to)
  - != (Not equal to)
  - < (Less than)
  - > (Greater than)
  - <= (Less than or equal to)
  - >= (Greater than or equal to)
  - ## (Contains, where the field is present, regardless of its value)
4. Click **Apply**. Details of the filter are shown in the **Preview** bar at the bottom of the Define Filter window.
5. Click **OK** to save and apply the filter.

## Creating complex, compound filters

1. Open the Define Filters window as described above, or by clicking the Define Filters icon from the Packet List window.




2. Drill down in the Define Filter window to find the first field you want to include in your filter. Then click that field to select it.
3. Select the comparator for the filter, and then specify the value.
4. Click **Apply** to add the specified details to the filter. Those details are shown in the **Preview** bar at the bottom of the Define Filter window.
5. Repeat steps 2 and 3 to add the next condition to the filter. Then click the **Append** button and select the conditional operator:
  - o &t&t (And)
  - o || (Or)
6. Click **Apply** to append the new condition to the existing filter. The Preview bar is updated to show the compound filter.



7. When you finish adding conditions to the filter, click **OK** to save and apply the compound filter.

## Editing existing filters

You can also edit existing filters: both pre-defined and custom.

1. Select the filter you want to edit from the Packet List **Filter** drop-down list.
2. Click the  Define Filters icon. The Define Filter window opens, showing the selected filter in its Preview bar.
3. Manually edit the filter either by typing in the **Preview** bar, or else by adding conditions to the filter as described previously (for *Creating Complex, Compound Filters*).
4. Click **OK** to save and apply the updated filter.

## Predefined filters

Note that the available filters will vary depending on which protocol stack is currently selected.

The following pre-defined filters are available:

Filter	Definition
All Packets	No Filter is defined and all packets are shown.
MAC Data	MAC Frame Type == Data. Will include all higher layer packets e.g. NWK Data and Commands.
MAC Associations	MAC Association Request and Association Response Command Frames
MAC Commands and Beacons	MAC Frame Type == Command    Beacon
NWK Commands	NWK Frame Type == Command
NWK Data	NWK Frame Type == Data. Will include all higher layer packets e.g. APS Data and Commands.
Hide NWK Link Status	In ZigBee PRO, each route periodically (~15 seconds) sends a Link Status message. Select to filter out the link status message from the packet list but show all other packets. The filter used is <code>!(nwkPayCmdFrmID == 8)</code>
APS Command	APS Frame Type == Command
APS Data and Ack	APS Frame Type == Data    Acknowledgement
ZDO Packets	APS Profile ID == 0x0000 (ZDO)
HA Packets	APS Profile ID == 0x0104 (Home Automation)
Smart Energy (AMI) Packets	APS Profile ID == 0x0109 (Smart Energy)
Secured Packets	Any MAC, NWK, or APS packets with the Security flag enabled indicating the presence of a AUX Security Header.
Security Packets (including APS Commands)	Any MAC, NWK, or APS packets with the Security flag enabled indicating the presence of a AUX Security Header PLUS all APS command packets.
Malformed Data	Packets that contain either too much or not enough data (extra or missing bytes).