sFlowTrend-Pro

InMon Corp.
Table of Contents

1. Introduction .................................................................................................................. 1
   1.1. Introducing sFlowTrend-Pro ..................................................................................... 1
   1.2. About sFlow ........................................................................................................... 3
   1.3. Getting started ........................................................................................................ 3
   1.4. Navigating around sFlowTrend-Pro using the history navigator ......................... 5
      1.4.1. Bookmarking a tab and its settings ................................................................. 6
      1.4.2. Organising bookmarks .................................................................................... 6
      1.4.3. Going to a previously bookmarked tab ............................................................ 7
   1.5. Getting help ............................................................................................................ 7
      1.5.1. Using the on-line help window ........................................................................ 7
   2. The dashboard ............................................................................................................ 9
      2.1. Status .................................................................................................................. 9
      2.2. Thresholds .......................................................................................................... 10
      2.3. Top interfaces .................................................................................................... 10
   3. Network ..................................................................................................................... 12
      3.1. Interfaces ........................................................................................................... 12
      3.2. Counters ............................................................................................................. 13
         3.2.1. Counters charts ......................................................................................... 14
         3.2.2. Units ............................................................................................................ 15
         3.2.3. Using the legend to view one interface counter ......................................... 15
      3.3. Top N .................................................................................................................. 15
         3.3.1. Top N charts .............................................................................................. 16
            3.3.1.1. Custom Top N charts ....................................................................... 17
         3.3.2. Units ............................................................................................................ 18
         3.3.3. Understanding the Top N traffic chart ..................................................... 19
         3.3.4. Displaying end host information ............................................................... 19
         3.3.5. Using the legend to drilldown on specific traffic ....................................... 20
         3.3.6. Filtering for specific traffic ....................................................................... 20
      3.4. Circles ................................................................................................................. 20
         3.4.1. Clustering end hosts .................................................................................. 21
         3.4.2. Automatically labelling chart elements .................................................... 21
         3.4.3. Units ............................................................................................................ 22
            3.4.4. Changing the time selection .................................................................. 22
            3.4.5. Selectively labelling chart elements .................................................... 22
            3.4.6. Displaying end host information ............................................................. 23
            3.4.7. Pan and zoom ......................................................................................... 23
            3.4.8. Filtering for specific traffic .................................................................. 23
      3.5. Selecting a switch ............................................................................................... 23
      3.6. Selecting an interface ......................................................................................... 24
   4. Hosts .......................................................................................................................... 25
      4.1. Statistics .............................................................................................................. 25
      4.2. Charts ................................................................................................................. 26
         4.2.1. Physical host charts .................................................................................... 27
         4.2.2. Virtual host charts ..................................................................................... 28
         4.2.3. Using the legend to select one counter .................................................... 28
   5. Services ...................................................................................................................... 29
      5.1. Counters .............................................................................................................. 29
         5.1.1. Counters charts ......................................................................................... 30
         5.1.2. Using the legend to view one counter .................................................... 30
      5.2. Top N .................................................................................................................. 30
sFlowTrend-Pro

5.2.1. HTTP top N charts .................................................. 31
5.2.2. Units ........................................................................ 32
5.2.3. Understanding the Top N services chart ...................... 32
5.2.4. Displaying end host information ............................... 32
5.2.5. Using the legend to drilldown into service data .......... 33
6. Using and configuring thresholds .................................... 34
  6.1. Viewing thresholds .................................................... 34
  6.2. Threshold values and types ........................................ 35
  6.3. Defining thresholds .................................................... 36
  6.4. Root cause analysis ................................................... 37
7. Events ............................................................................ 38
8. Reports ............................................................................ 39
  8.1. Organising report definitions ...................................... 40
  8.2. Editing report definitions and sections ....................... 41
    8.2.1. Viewing report results ......................................... 41
    8.2.2. Editing a query section ......................................... 41
    8.2.2.1. Defining how query results are displayed .......... 42
    8.2.2.2. Editing a query using basic settings ................. 44
    8.2.2.3. Editing a query using advanced settings ........... 46
    8.2.2.4. Editing a query using scripted settings .......... 50
    8.2.3. Editing an HTML section ..................................... 51
  8.3. Running a report ......................................................... 52
9. Selecting a time period .................................................... 53
  9.1. Using the Time selector .............................................. 53
  9.1.1. Using custom time selection ................................... 54
  9.2. Making a time selection by dragging the mouse .......... 54
10. Filtering ......................................................................... 55
  10.1. Basic use of filters .................................................. 55
  10.2. Advanced use of filters .......................................... 56
  10.3. Terms available for use in filters ............................. 56
11. End host information ...................................................... 58
12. Running sFlowTrend-Pro as a service ............................ 60
  12.1. Introduction ........................................................... 60
  12.2. Installation ............................................................. 60
    12.2.1. Using the interactive installer ............................. 60
    12.2.2. Installing with a Debian or RPM package ............ 61
    12.2.3. Notes on installing sFlowTrend-Pro as a service under Linux ............................................. 61
    12.2.4. Memory configuration for the sFlowTrend-Pro service ......................................................... 62
    12.2.5. Configuring https certificates ......................... 62
  12.3. Connecting to a server .............................................. 63
  12.4. Connecting to a server using a web browser .............. 63
  12.5. Connecting to a server using Java Web Start .......... 63
13. Configuration ............................................................... 65
  13.1. Configuring the license ............................................. 65
  13.2. Configuring agents in sFlowTrend-Pro ..................... 65
    13.2.1. Adding a switch that is to be configured via SNMP ......................................................... 67
    13.2.2. Importing and exporting agent configuration .... 67
    13.2.3. Verifying the switch configuration and status .... 68
  13.3. Configuring subnets in sFlowTrend-Pro ..................... 68
13.4. Configuring action on events in sFlowTrend-Pro

13.5. Options

13.5.1. Setting the switch, interface, and host naming policy

13.5.1.1. Setting the switch naming policy

13.5.1.2. Setting the interface naming policy

13.5.1.3. Setting the host naming policy

13.5.2. Configuring global SNMP settings

13.5.3. Configuring advanced options

13.5.4. Proxy configuration

13.5.5. Email

13.5.6. Advanced sFlow

13.6. Configuring user authentication

13.6.1. Adding a user

14. Troubleshooting and frequently asked questions

14.1. Troubleshooting sFlowTrend-Pro

14.1.1. Installation problems

14.1.1.1. When I try to install sFlowTrend-Pro, my browser asks me what to do

14.1.1.2. When I try to install sFlowTrend-Pro, my browser displays a page of text instead of installing the program

14.1.1.3. sFlowTrend-Pro requires the Java Run-time Environment (JRE) v6.0, and Java Web Start

14.1.1.4. Java Web Start is not working correctly on Linux

14.1.2. No switches are listed in the Switch selector

14.1.3. When I select a switch in the Network, Top N tab, the chart is blank

14.1.4. When I select a switch in the Network Interfaces tab, the table is empty

14.1.5. When I select a switch in the Network Interfaces tab, the table rows have no counter values

14.1.6. sFlowTrend-Pro is not receiving sFlow from a switch or host

14.1.7. sFlowTrend-Pro cannot communicate with the switch using SNMP

14.1.8. On-line help or email is not working

14.2. Frequently asked questions

14.2.1. After I select a switch to monitor, why does nothing happen?

14.2.2. When I start sFlowTrend-Pro, why do I get an error message "Cannot open UDP port 6343"?

14.2.3. Why are most of the bars in a Top N chart coloured grey?

14.2.4. What firewall requirements does sFlowTrend-Pro have?

14.2.5. How do I change the time for which sFlowTrend-Pro stores data?

15. Advanced topics

15.1. Custom configuration

15.1.1. Client custom configuration settings

15.1.2. Server custom configuration settings

15.2. Customising protocol names

16. Reference

16.1. Menu reference

16.2. Database fields reference

16.2.1. Flows table fields

16.2.2. Counters table fields

16.2.3. Host counters table fields

16.2.4. Services table fields

16.2.5. Service counters table fields
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.2.6. Time fields</td>
<td>110</td>
</tr>
<tr>
<td>16.3. Filter functions reference</td>
<td>111</td>
</tr>
<tr>
<td>16.4. Database functions</td>
<td>111</td>
</tr>
<tr>
<td>16.4.1. Labels in database functions</td>
<td>111</td>
</tr>
<tr>
<td>16.4.2. Key functions</td>
<td>111</td>
</tr>
<tr>
<td>16.4.2.1. countryCode</td>
<td>111</td>
</tr>
<tr>
<td>16.4.2.2. countryName</td>
<td>112</td>
</tr>
<tr>
<td>16.4.2.3. hostname</td>
<td>112</td>
</tr>
<tr>
<td>16.4.2.4. ifAlias</td>
<td>112</td>
</tr>
<tr>
<td>16.4.2.5. ifAliasorVMName</td>
<td>113</td>
</tr>
<tr>
<td>16.4.2.6. ifName</td>
<td>113</td>
</tr>
<tr>
<td>16.4.2.7. ifOrVMName</td>
<td>113</td>
</tr>
<tr>
<td>16.4.2.8. locate</td>
<td>114</td>
</tr>
<tr>
<td>16.4.2.9. locateSwitch</td>
<td>114</td>
</tr>
<tr>
<td>16.4.2.10. mac</td>
<td>114</td>
</tr>
<tr>
<td>16.4.2.11. vendor</td>
<td>115</td>
</tr>
<tr>
<td>16.4.2.12. getParent</td>
<td>115</td>
</tr>
<tr>
<td>16.4.2.13. resolve</td>
<td>116</td>
</tr>
<tr>
<td>16.4.2.14. subnet</td>
<td>116</td>
</tr>
<tr>
<td>16.4.2.15. uuid</td>
<td>116</td>
</tr>
<tr>
<td>16.4.2.16. vmName</td>
<td>117</td>
</tr>
<tr>
<td>16.4.3. Value functions</td>
<td>117</td>
</tr>
<tr>
<td>16.4.3.1. count</td>
<td>117</td>
</tr>
<tr>
<td>16.4.3.2. max</td>
<td>117</td>
</tr>
<tr>
<td>16.4.3.3. min</td>
<td>118</td>
</tr>
<tr>
<td>16.4.3.4. rate</td>
<td>118</td>
</tr>
<tr>
<td>16.4.3.5. scale</td>
<td>118</td>
</tr>
<tr>
<td>16.4.3.6. sum</td>
<td>119</td>
</tr>
<tr>
<td>16.4.4. Time functions</td>
<td>119</td>
</tr>
<tr>
<td>16.4.4.1. format</td>
<td>119</td>
</tr>
<tr>
<td>16.4.4.2. timestamp</td>
<td>120</td>
</tr>
<tr>
<td>16.5. Classes and objects defined within scripted reports</td>
<td>120</td>
</tr>
<tr>
<td>16.5.1. Objects defined</td>
<td>120</td>
</tr>
<tr>
<td>16.5.1.1. report</td>
<td>120</td>
</tr>
<tr>
<td>16.5.1.2. reportVars</td>
<td>120</td>
</tr>
<tr>
<td>16.5.2. Classes defined</td>
<td>121</td>
</tr>
<tr>
<td>16.5.2.1. Chart</td>
<td>121</td>
</tr>
<tr>
<td>16.5.2.2. Query</td>
<td>121</td>
</tr>
<tr>
<td>16.5.2.3. Report</td>
<td>123</td>
</tr>
<tr>
<td>16.5.2.4. Table</td>
<td>125</td>
</tr>
<tr>
<td>A. Configuring switches to send sFlow</td>
<td>126</td>
</tr>
<tr>
<td>A.1. Using SNMP to configure the switch to send sFlow</td>
<td>126</td>
</tr>
<tr>
<td>A.1.1. Configuring ProCurve switches to allow sFlow configuration via SNMP</td>
<td>126</td>
</tr>
<tr>
<td>A.2. Using the switch CLI to configure sFlow</td>
<td>127</td>
</tr>
<tr>
<td>A.2.1. Alcatel-Lucent OmniSwitch</td>
<td>127</td>
</tr>
<tr>
<td>A.2.2. Brocade (Foundry Networks)</td>
<td>128</td>
</tr>
<tr>
<td>A.2.3. D-Link</td>
<td>128</td>
</tr>
<tr>
<td>A.2.4. Enterasys</td>
<td>128</td>
</tr>
<tr>
<td>A.2.5. Extreme Networks</td>
<td>128</td>
</tr>
<tr>
<td>A.2.6. Force10 Networks</td>
<td>129</td>
</tr>
<tr>
<td>A.2.7. H3C</td>
<td>129</td>
</tr>
<tr>
<td>A.2.8. Juniper Networks</td>
<td>129</td>
</tr>
<tr>
<td>A.2.9. Netgear</td>
<td>130</td>
</tr>
<tr>
<td>A.2.10. ProCurve Networking by HP</td>
<td>130</td>
</tr>
</tbody>
</table>

sFlowTrend-Pro
B. Configuring hosts to send sFlow ................................................................. 132
  B.1. Installing the host sFlow agent ................................................................. 132
  B.2. Configuring the host sFlow agent ............................................................... 132
    B.2.1. Linux configuration using DNS Service Discovery ................................. 132
    B.2.2. Linux configuration using the configuration file ................................. 133
C. Recommended sampling rates ................................................................. 134
D. Acknowledgements and copyright ......................................................... 135
List of Tables

15.1. Protocol definition sections .......................................................... 89
16.1. Database key fields available for flows ........................................... 94
16.2. Database value fields available for flows ........................................ 98
16.3. Database key fields available for counters ...................................... 99
16.4. Database value fields available for counters .................................... 99
16.5. Database key fields available for host counters ............................... 101
16.6. Database value fields available for host counters ........................... 102
16.7. Database key fields available for services ...................................... 107
16.8. Database value fields available for services ................................... 109
16.9. Database key fields available for service counters ......................... 109
16.10. Database value fields available for service counters .................... 110
16.11. Database time fields ................................................................. 110
16.12. JavaScript filter functions ......................................................... 111
C.1. Recommended sampling rates ......................................................... 134
Chapter 1. Introduction

1.1. Introducing sFlowTrend-Pro

sFlowTrend-Pro is a Java application, which monitors sFlow® enabled network switches, routers and hosts. It is designed to be easy to install and use, and to allow network and host problems to be understood and resolved quickly. Summaries and detail of network traffic can be displayed, on a per-switch or per-interface level, thresholds used to provide alerts to abnormal traffic conditions, and historical traffic patterns reviewed to determine when changes occurred. Host performance metrics can be monitored for an entire datacentre.

As its name implies, sFlowTrend-Pro only monitors sFlow enabled switches, routers and hosts. For the sake of clarity, in the remainder of this documentation network devices will be referred to as switches; if there is an instance where a router has different behaviour or requirements, this will be highlighted.

sFlowTrend is a limited functionality version of sFlowTrend-Pro. Throughout this documentation, sFlowTrend-Pro will be used to refer to sFlowTrend and sFlowTrend-Pro. Features that only apply to sFlowTrend-Pro will be highlighted with.

sFlowTrend-Pro can be deployed in two different ways, depending on the option that you chose when evaluating or purchasing it. The options are:

Run sFlowTrend-Pro as an application
This is the original version of sFlowTrend-Pro that was available, and remains the only one for sFlowTrend. When running as an application, data is collected when the application is running, and stops when the application is closed (or the user who launched it logs off).

Throughout this documentation, features that only apply to the application are highlighted with.

Run sFlowTrend-Pro as a service
When running sFlowTrend-Pro as a service, the system is split into a client half and a server half. The server runs continually in the background, collecting data even when no-one is logged in. The client is used to run the GUI, and view the data from the server. The client can be run on the same system as the server, or a different one, and multiple clients can connect to the same server at once.

Throughout this documentation, features that only apply to the service are highlighted with.

When running sFlowTrend-Pro as an application, it is run from Java Web Start. Java Web Start is a technology which allows Java applications to be installed and run easily. The easiest way to start sFlowTrend-Pro is to allow Java Web Start to create a desktop icon and menu items for sFlowTrend-Pro when first installing it. After that, just double click the desktop icon, or select the menu item as appropriate, and sFlowTrend-Pro will launch. Note that data is only collected while the application version of sFlowTrend-Pro is running.

The sFlowTrend-Pro service is installed via a traditional installer. The installation starts the service. After each reboot, the service is started automatically and data collection will resume. The installation also includes two shortcuts:

sFlowTrend-Pro local client
This allows you to start a client which connects to the local service.
sFlowTrend-Pro remote client

This allows you to start a client that you can use to connect to a server running on a different, remote system.

sFlowTrend-Pro has an optional user authentication feature (see Section 13.6, “Configuring user authentication”). If enabled, only users who are authenticated with a password can access the system and view data. Additionally, some functionality, for example adding new switches to monitor, is only available to administrators. If a particular part of sFlowTrend-Pro can only be used by an administrator, this is highlighted with [Admin] in this documentation. Note that if user authentication is not in use, then this does not apply and everyone can access all of the features.

sFlowTrend-Pro follows a familiar layout of many applications.

Menu
The main menu is available across the top of the window. A description of the menu items is given in Section 16.1, “Menu reference”.

History navigator
The history navigator allows you to move backwards and forwards through the recently viewed screens, in a similar way to a browser's history navigator, see Section 1.4, “Navigating around sFlowTrend-Pro using the history navigator”.

Tab bar
Immediately below the history navigator are a number of tabs. Clicking on a tab will take you to the view associated with that tab. Some parts of sFlowTrend-Pro are equipped with hotlinks, which take you to a different view or tab when clicked (the mouse cursor will change to a hand when this is possible).
Status bar
Along the bottom edge of the window is a status bar, which shows the overall status of the switches and hosts being monitoring, or the status of the currently selected switch if the Charts, Wireless, or Interfaces tab is being viewed.

Progress indicator
The progress indicator is present when sFlowTrend-Pro is configured to monitor at least one switch or host. It indicates when the charts and tables will be updated with the most recent traffic and host data. The outer ring in the progress indicator shows the progress through the current minute. The centre of the progress indicator indicates when the chart or table will next be updated. If the chart or table is updating every minute, or if the chart or table is not being automatically updated, the outer ring and centre will be synchronised.

Activity LED
In the bottom right corner, a green activity 'LED' shows incoming sFlow samples. This flashes when each sample is received, and so provides a very quick way to see if the network is correctly configured to send sFlow.

1.2. About sFlow
sFlow® is an industry standard technology for monitoring traffic in computer networks. The sFlow standard is designed and maintained by the industry group (http://www.sflow.org). Unlike other monitoring technologies, it is very efficient, and so can be used in modern high-speed networks. It also operates at layer two in the network, which means that switched as well as routed traffic can be monitored. Because the overhead of running sFlow on a network is low, it is recommended that sFlow is enabled on as many switch ports as possible in a network. This allows as complete a picture as possible of the traffic to be created. sFlowTrend-Pro helps you automatically configure sFlow on all interfaces, where possible.

sFlow is supported by most network switch manufacturers. An up-to-date list is maintained at http://www.sflow.org/products/network.php. Even if some of the switches in a network do not support sFlow, because most traffic transits several points in the network, good information on traffic can still be obtained.

With the release of host sFlow, the benefits of sFlow can also be realised for virtual switch, host and application monitoring. xSOver time, it is expected that system vendors will integrate host sFlow into their products. In the meantime, a host agent is available from http://host-sflow.sourceforge.net, the host sFlow SourceForge site, to allow sFlow to be added to any host.

1.3. Getting started
Please follow these steps to start monitoring your network traffic with sFlowTrend-Pro. It will also be useful to have the documentation available for your network switches.

1. Ensure that you have some switches or hosts that support sFlow. sFlowTrend-Pro can only monitor switches or hosts using sFlow.

2. If you are using the application version of sFlowTrend-Pro, then just run it from the Start menu, as with any other application.

If you are running sFlowTrend-Pro as a service, then the service should be started automatically after each reboot. To connect to the service to use the product, start the sFlowTrend-Pro client, using the Start menu. Two options are available: to connect to the server running on the local system, use the sFlowTrend-Pro local client menu item; to connect to a different remote server running the sFlowTrend-Pro service, use the sFlowTrend-Pro remote client menu item.
3. If you are running sFlowTrend-Pro as a service, then the license should be configured to allow sFlow to be collected. Refer to Section 13.1, “Configuring the license” for information on how to set the license.

4. Select the sFlowTrend-Pro Tools → Options (or, on an Apple Macintosh, sFlowTrend-Pro → Preferences) menu item and select the Advanced sFlow tab. Note the sFlow collector address and UDP port that sFlowTrend-Pro is using to receive sFlow. If your host has multiple IP addresses, they will be accessible through the sFlow collector address selector. Select the most appropriate IP address for sFlowTrend-Pro to use to receive sFlow.

5. Make sure that any host based firewalls, or external firewalls between the host running sFlowTrend-Pro and the switches being monitored allow:
   - UDP traffic from the switches being monitored to the sFlow port on the host running sFlowTrend-Pro.
   - UDP traffic to and from the host running sFlowTrend-Pro to the SNMP port (port 161) on the switches being monitored.

6. If you are using the remote client to connect to a remote sFlowTrend-Pro server, make sure that any host or external firewalls will allow communication between the client and the server. The client uses TCP port 8087 by default to connect to the server.

7. Select the Tools → Options (or, on an Apple Macintosh, sFlowTrend-Pro → Preferences) menu item and select the SNMP tab. Choose whether sFlowTrend-Pro should use SNMP v2c or SNMP v3 by default when communicating with the switches, and enter the appropriate settings for your network. In addition to these global settings, the SNMP settings can also be overridden per switch (see Section 13.2, “Configuring agents in sFlowTrend-Pro”). Note that the SNMP settings must allow write access if your switches are to be configured using SNMP (see below). If the switches are configured manually, then settings that allow read access can be used.

8. Next, sFlow should be enabled on the switches you wish to monitor. How this is done depends on the make and model of each switch. Some switches support sFlow configuration through SNMP, while others require that it is manually configured through the configuration interface for the switch (normally the web interface or command line interface (CLI)). In some cases, the switch can be configured either way. SNMP configuration is normally the easiest. Consult the switch vendor's documentation to determine how sFlow can be configured, and for any specific instructions. See Appendix A, Configuring switches to send sFlow for additional information on configuring switches.

   **SNMP configured sFlow**

   If a switch supports SNMP configuration of sFlow, then sFlowTrend-Pro can do most of the configuration work. To do this, select the Tools → Configure agents menu item. Click the Add button, and enter the IP address of the switch you wish to configure. The SNMP settings for the switch can also be changed from the default global settings here. Select OK on both dialogs to apply your changes. See Section 13.2.1, “Adding a switch that is to be configured via SNMP” for more information on configuring switches with SNMP.

   **Manually configured sFlow**

   To manually configure a switch to send sFlow, consult the switch documentation to determine the specific steps required. Normally, this is done through the web interface or the command line interface on the switch. Connect to the switch (say using a web browser, ssh or telnet). Follow the instructions for the switch to configure it to send sFlow to the IP address and UDP port that sFlowTrend-Pro is using to receive sFlow. You will also need to enable sFlow on one or more interfaces on the switch and set a sampling rate.
As soon as sFlow reaches sFlowTrend-Pro, the switch will automatically be added to sFlowTrend-Pro. Even though the switch is not configured through SNMP, configuring sFlowTrend-Pro with SNMP settings that allow read access to the switch will allow information about the switch to be displayed in a more useful way. For example the interfaces can be displayed by name, rather than number. See Section 13.2, “Configuring agents in sFlowTrend-Pro” for more information on this topic.

9. If you have any hosts that support sFlow, or you are installing the host sFlow agent, then enable these to send sFlow to sFlowTrend-Pro. See Appendix B, Configuring hosts to send sFlow for more information on configuring host sFlow.

10. When sFlowTrend-Pro starts to receive sFlow, the green 'LED' at the bottom right of the window should start flashing. This flashes for each sFlow sample received, so the more sFlow being received, the faster it will flash. Also, on the Dashboard tab, Status section, you can see the incoming sample rate.

11. Now that your switches are configured to send sFlow, they should be visible within sFlowTrend-Pro. In the Dashboard tab, the status bar will indicate how many switches are being monitored. The Dashboard tab highlights the busiest switch interfaces. See Chapter 2, The dashboard.

12. Go to the Nework tab, select the Flows sub-tab, and then use the Switch selector to view the traffic information for a specific switch. The default view shows top sources across all interfaces on the switch. You can change the chart displayed using the Chart selector, and view data for a specific interface using the Interface selector. See Section 3.3, “Top N” for more information on network traffic flows charts.

13. To find quickly the interfaces on a switch that are busiest, select the Interfaces sub-tab. This will show a table of all the interfaces on the selected switch. By clicking on the column headings, you can sort by Utilization, Unicasts per second, etc. Once you have found an interface of interest, click the chart button, at the left-hand end of each row, to go directly to the charts for that interface. See Section 3.1, “Interfaces” for more information on this tab.

1.4. Navigating around sFlowTrend-Pro using the history navigator

You can navigate around sFlowTrend-Pro by selecting tabs in the Tab bar to view and analyse the sFlow data. In addition, sFlowTrend-Pro includes a History navigator.

When you move to a different tab or you change the settings in the viewed tab (for example changing the selected switch, interface or chart in the Network > Flows tab), the History navigator automatically saves the tab and its settings changes in the history of viewed tabs and their settings. You can use the and buttons to move backwards and forwards through the history of viewed tabs and their settings, in much the same way as you would use the back and forward buttons in a web browser to navigate through the history of viewed web pages.
The History navigator also includes the ability to bookmark favourite tabs and their settings so that you can return to a tab configured with the saved settings at a later time. This is particularly useful if your favourite tabs include many special settings (eg filters).

**Note**

You can also access the functions of the History navigator using the Navigate menu. (see Section 16.1, “Menu reference”)

1.4.1. Bookmarking a tab and its settings

When you have configured a tab with useful settings and would like to save these settings so that you can return to the tab already configured with the settings, you can click the to save a bookmark. This will bring up the Add bookmark dialog which allows you to name the bookmark and choose a folder in which to save the bookmark.

1.4.2. Organising bookmarks

To view all the saved bookmarks click on the button. This will bring up the Show all bookmarks dialog. This dialog can also be accessed by selecting Navigate → Show all bookmarks

![Dialog displaying saved bookmarks](image)

The dialog displays the saved bookmarks in a hierarchical tree view of folders and bookmarks. You can use this dialog to add new folders, rename bookmarks and folders, delete bookmarks and folders and use drag and drop to rearrange bookmarks and folders.

In addition, in the dialog toolbar, you can click on the button to view the settings saved in the currently selected bookmark or click on the button to go to the tab configured with the settings saved in the currently selected bookmark.
1.4.3. Going to a previously bookmarked tab

To go to a previously bookmarked tab configured with the saved settings, you can select the bookmark from the Navigate → Go to bookmark menu. You can use the Show all bookmarks dialog, select the bookmark, then click the button.

1.5. Getting help

You can use the built-in help in sFlowTrend-Pro to get on-line and context-sensitive help. Three options are available from the Help menu:

Help → Contents
Shows the contents of the on-line help in a new window.

Help → Help on current view
Shows help for the current tab being viewed in sFlowTrend-Pro.

Help → Point and click help
Changes the mouse cursor to a help pointer , and then allows you to click anywhere within the sFlowTrend-Pro window. Instead of the mouse click having its usual effect, context sensitive help will be displayed for the part of the window that was clicked.

In addition, you can press the F1 key to get help on the current view, in most situations.

If you have trouble with getting sFlowTrend-Pro to work correctly, please refer to Chapter 14, Troubleshooting and frequently asked questions. If you still need help, please submit a support request at the InMon Corp. customer portal (http://www.myinmon.com).

For sales requests, please send an email to <sales@inmon.com>.

1.5.1. Using the on-line help window

The on-line help window is displayed when you request help. The window provides various ways to navigate the help system. On the left is the navigation panel, and on the right the content is displayed.

The navigation panel offers three ways to find the help that you are interested in. Select these by clicking on the tabs along the top of the panel. The options are:

Table of contents
Allows you to select the content displayed by finding the entry in the table of contents. The table of contents can be expanded and collapsed as needed by clicking the icon at the beginning of each entry, and the content displayed by clicking on the title of the entry.

Search
Allows you to search on text in the help. The results shown will be ordered based on relevance to the text you entered.
Favourites

Keeps a list of favourites or bookmarks that you can add to. When viewing a help entry, click the favourites toolbar button to add an entry to the favourites list. You can then quickly go back to that entry by clicking it in the favourites panel. Remove the entry by right clicking on it.
Chapter 2. The dashboard

The dashboard is the screen displayed when sFlowTrend-Pro is first launched. The purpose of the dashboard is to give a summary of the overall status of the network, to help you identify problems quickly. The dashboard contains three main types of information:

1. The overall status of sFlowTrend-Pro.
2. The status of the top-level thresholds.
3. Charts showing the interfaces in the network reporting the largest values of utilization, frames, and errors and discards.

2.1. Status

The status section of the dashboard shows a summary of the overall system, which can be useful for basic troubleshooting.

Some of the information shown:

- To the right of the InMon Corp. logo is the product name. This should be sFlowTrend-Pro if you are running sFlowTrend-Pro, or sFlowTrend if running basic sFlowTrend. Also, if you are running sFlowTrend-Pro, information about the current license is shown, including the expiry date, and the license ID number. If you have multiple copies of sFlowTrend-Pro, the license ID is useful if you need to refer to the license you are running when you are using the InMon customer portal (http://www.myinmon.com).

- If you are running the service version of sFlowTrend-Pro, then the server that you are currently connected to is shown. If the display area of any of the status items is not big enough to show the full text, then you can hover the mouse over the text to read it.

- If you have defined users to control access to sFlowTrend-Pro, the username of the currently logged in user is shown.

- The current rate of incoming samples is shown. This number includes only samples that actually reached sFlowTrend-Pro, and are coming from enabled switches and hosts. If you are seeing no data in sFlowTrend-Pro, this number can help you determine why (see Section 14.1, “Troubleshooting sFlowTrend-Pro”).
2.2. Thresholds

The thresholds section of the dashboard shows the current status of each of the top level thresholds.

<table>
<thead>
<tr>
<th>Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utilisation</td>
</tr>
<tr>
<td>Unicasts</td>
</tr>
<tr>
<td>Broadcasts</td>
</tr>
<tr>
<td>Multicasts</td>
</tr>
<tr>
<td>Errors</td>
</tr>
<tr>
<td>Discards</td>
</tr>
</tbody>
</table>

Each threshold category (Utilization, Unicasts, Broadcasts, Multicasts, Errors, Discards) indicates the most severely violated threshold across all the switches that you are monitoring. The colour of the bar indicates how severe the threshold violation is (green is normal, yellow is marginal and red critical). Further detail of the threshold value is indicated by how far to the right the threshold bar is within the indicator. For more information on how thresholds work, see Chapter 6, *Using and configuring thresholds*.

You can drill-down to the causes of any threshold violation by clicking on a threshold indicator on the dashboard. This will take you to the thresholds screen, showing the thresholds for all the switches being monitored, sorted by the threshold category that you clicked on. For example, if you click on the broadcast threshold indicator in the dashboard, you will be taken to the thresholds view for all switches, sorted by broadcasts (highest threshold value first). This shows you the detail of the broadcast thresholds across the whole network, and allows you to quickly find the switches contributing the most to threshold violations.

Note that if a switch is deleted from sFlowTrend-Pro, if it was contributing to any of the thresholds shown on the dashboard, then this contribution will not be removed until the end of the current minute.

2.3. Top interfaces

Three 'top interfaces' charts are provided on the dashboard.

<table>
<thead>
<tr>
<th>Top interfaces by total frames</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.244&gt;Tik1</td>
</tr>
<tr>
<td>10.0.0.244&gt;A13</td>
</tr>
<tr>
<td>10.0.0.244&gt;C1</td>
</tr>
<tr>
<td>10.0.0.244&gt;A11</td>
</tr>
<tr>
<td>10.0.0.244&gt;A3</td>
</tr>
<tr>
<td>10.1.4.253&gt;23</td>
</tr>
<tr>
<td>10.1.4.253&gt;24</td>
</tr>
<tr>
<td>10.0.0.244&gt;A1</td>
</tr>
<tr>
<td>10.0.0.244&gt;A5</td>
</tr>
<tr>
<td>10.0.0.244&gt;B2</td>
</tr>
</tbody>
</table>

These show, in bar chart format, the top 10 switch interfaces sorted by utilization, total frames (unicasts, multicasts and broadcasts), and errors and discards. The bar shows the average over the previous minute. These charts are designed to give you a summary view of the busiest interfaces, or interfaces which are...
experiencing the highest number of issues. Clicking on any of the bars allows you to quickly drill-down to the traffic charts for that specific interface.

Note that if a switch is deleted from sFlowTrend-Pro, if it was contributing to any of the top interface bar charts shown on the dashboard, then this contribution will not be removed until the end of the current minute.
Chapter 3. Network

The Network tab displays network performance statistics using sFlow data collected from switches (including virtual switches) and wireless access points. This tab includes a number of sub-tabs that allow you to view the data in different ways:

**Interfaces**
Sortable table showing the important interface counters (Utilization(%), Unicasts/s, Broadcasts/s, Multicasts/s, Errors/s, Discards/s) values for the most recent minute, for the for the currently selected switch. This tab is useful for comparing the usage of interfaces based on absolute values. See Section 3.1, “Interfaces”.

**Counters**
Trend charts showing how the overall network traffic load on an interface varies over time. See Section 3.2, “Counters”.

**Top N**
Trend charts showing the top N contributors to the network traffic and how the top N contributors change over time. See Section 3.3, “Top N”.

**Circles**
Charts that allow you to visualise the traffic flows between groups of addresses. See Section 3.4, “Circles”.

3.1. Interfaces

The Interfaces tab provides a tabular, sortable view of the values for the most recent minute, of the important interface counters (Utilisation(%), Unicasts/s, Broadcasts/s, Multicasts/s, Errors/s, Discards/s) for the currently selected switch.

![Switch selector](image)
This tab is useful for comparing the usage of interfaces based on absolute values. For example to compare the unicasts/s of all 100Mb/s interfaces on the selected switch (see Section 3.5, “Selecting a switch”), first click with the left mouse button on the Unicasts/scolumn heading, then click with the left mouse button on the ifSpeed column heading; this will cause the table to be sorted by ifSpeed and unicasts/s.

**Note**

When sorting on the Interface column, if the interface naming policy is ifIndex, then the interfaces will be sorted numerically, for all other interface naming policies, the interfaces will be sorted alpha-numerically (see Section 13.5.1, “Setting the switch, interface, and host naming policy”).

The Progress indicator shows when the counter values will next be updated. When sFlowTrend-Pro first starts collecting sFlow data from a switch, the first counter values will be available after 2 minutes. The counter values will then be updated every minute.

To investigate the cause of the usage values for an interface of interest, click on the chart button in the row for the interface. This will automatically make the Counters tab visible with the interface of interest selected.

### 3.2. Counters

Interface counter charts show how the overall network traffic load on an interface varies over time. These charts are generated from the interface counter data exported by sFlow. Interface counters charts are represented as stacked area charts.

![Interface counter chart](image.png)

This tab includes a control bar that allows you to select the switch (Section 3.5, “Selecting a switch”) and interface (Section 3.6, “Selecting an interface”) for which you would like to view trends in counter.
values, the counters charts to display and the specific time interval (see Chapter 9, Selecting a time period).

**Note**
When you have made changes to the selections for the chart, you can save these selections in a bookmark (see Section 1.4, “Navigating around sFlowTrend-Pro using the history navigator”) so that you can easily return to the same chart at a later date.

With sFlowTrend, or with sFlowTrend-Pro when the Time setting is relative to now (for example Last hour see Chapter 9, Selecting a time period), these charts are automatically updated when the next data point is available. The Progress indicator shows how long it will be before the chart is next updated.

### 3.2.1. Counters charts

The following charts are available:

**Utilization**
This chart shows the utilization trend for the selected interface. The utilization chart is useful for identifying any capacity problems with the interface. If utilization approaches 100% for sustained periods then action should be taken to increase the capacity of the link, reorganise the topology of the network, or limit the applications making use of the link. Change to the Top N tab and use the Top sources chart with Units selector set to Bits/s to start diagnosing the major sources of high utilization.

**Counters**
This chart shows basic interface counters. The counters chart is useful for examining the number of errors, broadcasts, multicasts or discards on an interface. High error rates can indicate a bad cable or interface card. High discard rates may indicate that the device cannot keep up with traffic. Change to the Top N tab and use the Top broadcasts or L2 multicast flows with Units selector set to Frames/s to help identify sources of high broadcast or multicast traffic.

**WAP frame counters**
This chart shows the trends of 802.11 wireless fragments and multicast frames.

**WAP control frame counters**
This chart shows the trends for 802.11 wireless control frames: Request To Send Success, Request To Send Failure, Acknowledgement Failure.

**WAP error counters**
This chart shows the trends for various different types of 802.11 wireless error frames.

**WAP associated stations**
This chart shows the trends in number of 802.11 wireless end hosts associated with the selected radio interface.

**WAP QoS counters**
This chart shows the trends for various different types of 802.11 wireless Quality of Service counters.

**Note**
The WAP counters charts will only display data if sFlowTrend-Pro is receiving sFlow from wireless devices that support the sFlow 802.11 Structures [http://www.sflow.org/sflow_80211.txt]
3.2.2. Units

When the Utilization chart is chosen, the Units selector automatically changes to Bits/s, and cannot be altered. The chart left y-axis indicates bits/s while the right y-axis indicates % utilization of the link bandwidth.

When the Counters chart or one of the 802.11 wireless counters charts is chosen, the Units selector automatically changes to Frames/s and cannot be altered.

3.2.3. Using the legend to view one interface counter

Sometimes the value for one interface counter can be much smaller than the values for other counters, making it hard to see the trend for the smaller counter. In this case, you can view the trend for only one interface counter, by clicking on the legend item corresponding to the counter of interest. For example, when viewing the Counters chart, clicking with the left mouse button on Errors will change the chart so that it displays only the trend for errors; an additional trend line for discards can be added to the chart using Shift+left mouse button on Discards; or clicking with the left mouse button on Errors or the background of the legend area will cause all trend lines to be displayed again.

3.3. Top N

The Top N tab displays charts that show the top N contributors to the network traffic and how the top N contributors change over time.

This tab includes a control bar that allows you to select the switch (Section 3.5, “Selecting a switch”) and interface (Section 3.6, “Selecting an interface”) for which you would like to analyse and view traffic data, and the type of chart to display. You can also select a specific time interval (Chapter 9, Selecting a time period) and filter on specific traffic (Chapter 10, Filtering)
Network

Note
When you have made changes to the selections for the chart, including creating a filter, you can save these selections in a bookmark (see Section 1.4, “Navigating around sFlowTrend-Pro using the history navigator”) so that you can easily return to the same chart at a later date.

With sFlowTrend, or with sFlowTrend-Pro when the Time setting is relative to now (for example Last hour see Chapter 9, Selecting a time period), these charts are automatically updated when the next data point is available. The Progress indicator shows how long it will be before the chart is next updated.

3.3.1. Top N charts
The Top N charts show the top N contributors to the network traffic and how the top N contributors change over time. These charts are generated from the sampled packets exported by sFlow. Top N traffic charts are shown using stacked bar charts.

The following network traffic top N charts are available:

Top sources
The top sources of traffic.

Top destinations
The top destinations of traffic.

Top input VLANs
The VLANs which are providing the most input traffic to the switch.

Top output VLANs
The VLANs which are receiving the most output traffic from the switch.

Top source-destination pairs
The top source address and destination address pairs.

Top source-destination flows
The top source address, source port, destination address and destination port flows.

Top inter-VLAN pairs
The VLANs between which most traffic is flowing.

Top connections
Top connections is similar to Top source-destination flows, but combines both directions of the traffic belonging to a client/server connection.

Top servers
The top servers.

Top clients
The top clients.

Top protocols
The top protocols.
Network

Top broadcast flows
The top flows of layer 2 broadcast traffic.

Top L2 multicast flows
The top flows of layer 2 multicast traffic.

Top IP multicast flows
The top flows of IP multicast traffic.

Most connected sources
The top sources ordered by the number of destinations that each has connected to. This is also referred to as 'fan-out'. This chart is useful for security analysis, to help identify hosts that are exhibiting address scanning behaviour.

Most connected destinations
The top destinations ordered by the number of sources that has connected to each. This is also referred to as 'fan-in'. This chart is useful for security analysis, to help identify hosts that might be victims of a distributed denial-of-service attack.

Most popular protocols
The top protocols ordered by the number of source/destination address pairs. This chart is also useful for security analysis, and shows the protocols that are most likely being used to perform scanning.

Top wireless versions
The wireless versions in use, for example 802.11a, 802.11g.

Top SSIDs
The top 802.11 wireless SSIDs in use.

Top channels
The top 802.11 wireless channels being used.

Top cipher suites
The top cipher suites being used to encrypt the 802.11 wireless traffic.

Note
In the VLAN charts, a VLAN of 0 indicates that no specific VLAN is being used, or the VLAN could not be determined.

Note
The 802.11 wireless charts will only display data if sFlowTrend-Pro is receiving sFlow from wireless devices that support the sFlow 802.11 Structures [http://www.sflow.org/sflow_80211.txt]

3.3.1.1. Custom Top N charts

In addition to the standard Top N charts, you can also define custom Top N charts. With a custom Top N chart you can choose the attributes (key fields) that are used to identify the top contributors. To define a custom Top N chart, click on the button next to the Chart selector. This will display the Edit custom Top N dialog. In the dialog, click on the Add custom Top N button to display a dialog that allows you to define the key fields for the custom Top N.
For example, if you would like to see the top source addresses before NAT has taken place and the associated addresses after NAT, select sourceNATAddress from the Available fields list and click Add -> to add this key field to the selected fields list, then select and add sourceAddress. See Table 16.1, “Database key fields available for flows” for descriptions of the available fields. You must enter a unique name for this custom Top N, before you click OK. After you click OK in the Edit custom Top N dialog, the custom Top N will be selected in the Chart selector and the corresponding custom Top N chart displayed. Custom Top N charts are listed after the standard Top N charts in the selector. You can use the Edit custom Top N dialog to edit or remove existing custom Top N definitions.

**Note**

The Available fields list includes a type-in text field that allows you to filter the available fields for fields whose names match the typed in text. For example, you can type addr into the type-in field to see only those fields which include addr in their names.

**Note**

Address translation data is available only if sFlowTrend-Pro is receiving sFlow from devices that support the extended_nat structure.

### 3.3.2. Units

You can use the Units selector to choose the measurement units used to calculate the top contributors. There are two types of Top N traffic charts:

**Rate-based charts**

These charts show the top N contributors based on their associated traffic rate in either bits/s or frames/s. Example rate-based charts are Top sources, Top source VLANs, Top broadcast flows. Use the Units selector to choose whether the top contributors should be sorted based on their traffic rate in either bits/s or frames/s.
If a specific interface is selected, then the rate-based charts will show ingress traffic (above the x-axis) and egress traffic (below the x-axis). This shows the top N contributors of traffic entering or exiting the selected interface. If the Units selector is set to Bits/s, the left y-axis will show the volume of traffic in bits/s, while the right y-axis will show the traffic volume in terms of % utilization of the interface bandwidth. If the Units selector is set to Frames/s, the traffic volume will be shown in frames/s.

If a specific wireless interface is selected, the Units selector includes an additional option, Air %. Air % is the percentage of the available bandwidth used by the traffic, taking into account the actual speed of transmission. Traffic transmitted at a low speed will have high air % utilization. This means that a host with poor signal strength may use a disproportionately large amount of wireless bandwidth and degrade performance for other users.

If the Interface selector is set to All, the charts will show the top contributors over the whole switch. If a connection oriented, client/server chart (Top connections, Top servers, Top clients, Top Protocols) is chosen, the chart will show traffic flowing to the server above the x-axis, while traffic flowing from the server will be shown below the x-axis. For the other rate-based charts, selecting All interfaces results in one overall rate for the switch. You can use the Units selector options of Bits/s and Frames/s to show top contributors based on the their traffic rate in terms of bits/s or frames/s respectively.

Count-based charts
These charts (Most connected sources, Most connected destinations, Most popular protocols) show an absolute count value for each of the top contributors. For example, the Most connected sources chart shows the count of destinations for each of the sources that talk to the most destination hosts. When these charts are selected, the Units selector automatically changes to Count and cannot be altered.

3.3.3. Understanding the Top N traffic chart

The legend in the Top N traffic chart shows the top contributors for the selected interval. The outlined time stamp, for example \( \text{4:10 PM} \), on the x-axis indicates the currently selected interval. You can select an interval and see the top contributors in that interval by clicking with the left mouse button on the bar corresponding to the interval of interest. Each other bar in the chart will then be recoloured to show how much traffic was generated, in the interval represented by the bar, by the top contributors from the currently selected interval. This allows you to see how the top contributors change over time.

If the latest (right most) bar is selected and the Time setting is relative to now (for example Last hour see Chapter 9, Selecting a time period, the charts will be updated automatically and always display the contributors for the most recent minute.

The grey part of each bar represents traffic not attributable to the top N shown in the legend (ie it represents the contribution from other sources, destinations etc. that are not in the top N).

If the whole of a bar is grey, the traffic in its interval is not attributable to any of the top contributors in the currently selected interval. You can click on this bar to make it the currently selected interval and see its top contributors.

3.3.4. Displaying end host information

You can find out more information about an end host by clicking on to the left of the host address in the legend. This will open the Lookup host dialog using the end host address. If the Lookup host dialog is already open, then the dialog will be changed to show information for the newly selected host. See Chapter 11, End host information for more information.
3.3.5. Using the legend to drilldown on specific traffic

You can use the legend in the network traffic top N charts to drilldown on traffic of interest. For example, if you are viewing a Top sources chart and you notice that one host is responsible for the majority of the traffic, you can investigate who this host is talking to and which application is generating the traffic by clicking with the left mouse button on legend item that corresponds to the host. The Top source-destination flows chart will then be displayed with a filter for the selected host applied. This will show you the top source-destination flows for which the host of interest is the source.

See Section 3.3.6, “Filtering for specific traffic” for more information of filtering on specific traffic.

3.3.6. Filtering for specific traffic

sFlowTrend-Pro allows the information displayed in a Top N traffic chart to be filtered. This allows you to focus on traffic that may be of interest. For example, if you only wanted to look at web traffic, you could set a filter for only TCP port 80 traffic. See Chapter 10, Filtering for details.

3.4. Circles

The Circles tab allows you to visualise the traffic flows between groups of addresses. For example, grouping end host addresses for each department allows you to view traffic between departments. Understanding network traffic in this way allows you to make accurate capacity planning decisions (eg, do I need to upgrade the link between the finance and the HR department?) and help enforce usage policies (are unauthorised hosts accessing the admin servers?).

A Circles chart shows the top 100 traffic flows, with the end hosts which are responsible for the top 100 flows displayed as black squares, and clustered together in circles. Lines, coloured according to the traffic
type, join the end hosts, of a flow. The width of a line is scaled according to the volume of traffic in the flow. The traffic type (or protocol) for each colour is shown in the chart legend. The legend entries are ordered left to right, ordered by the volume of each traffic type.

The Circles tab includes a control bar that allows you to select the switch (Section 3.5, “Selecting a switch”) and interface (Section 3.6, “Selecting an interface”) for which you would like to analyse and view traffic data, whether the top flows should be determined by frames or bytes, and whether the clusters and flows should be labelled automatically. You can also select specific time intervals and filter on specific traffic.

**Note**

When you have made changes to the selections for the circles chart, including creating a filter, you can save these selections in a bookmark (see Section 1.4, “Navigating around sFlowTrend-Pro using the history navigator”) so that you can easily return to the same chart at a later date.

### 3.4.1. Clustering end hosts

When end hosts are grouped in clusters, they are displayed as a circle of black squares. You can use the Cluster selector to choose how to cluster the end hosts. Currently, sFlowTrend-Pro supports end host clustering options:

**Subnets**

The end hosts, which are responsible for the top 100 flows, are grouped together according to their subnet. You must configure sFlowTrend-Pro with the subnets in your network for the end hosts to be clustered correctly (see Section 13.3, “Configuring subnets in sFlowTrend-Pro”). Any hosts with IP addresses that are not contained within the configured subnets will be displayed in a separate cluster named External. If the top flows are for L2 traffic (for example L2 broadcasts, ARPs or spanning tree) then the end hosts responsible for these flows will be grouped in a separate cluster named Non-IP.

**Country**

The end hosts, which are responsible for the top 100 flows, are grouped together according to the country in which the IP addresses of the end hosts are located. A host with an IP address, for which the country cannot be determined, will be displayed in a separate cluster named Unknown. If the top flows are for L2 traffic (for example L2 broadcasts, ARPs or spanning tree) then the end hosts responsible for these flows will be grouped in a separate cluster named Non-IP.

**Switch**

The end hosts, which are responsible for the top 100 flows, are grouped together according to the switch that they are most closely connected to. This allows you to understand traffic that stays within a switch and traffic that crosses multiple switches. A host which cannot be located to a switch, will be displayed in a separate cluster named Unknown.

### 3.4.2. Automatically labelling chart elements

The Label selector allows you to select how sFlowTrend-Pro should automatically label the elements in the chart. Elements that are automatically labelled will be labelled when the chart is loaded with the latest data. The following options are supported:

**No labels**

Labels will not be displayed automatically, however you can label selected end hosts or clusters by clicking on the corresponding element in the chart (see Section 3.4.2, “Automatically labelling chart elements”).

---

21
3.4.3. Units

You can select which traffic volume units are used to determine the top 100 flows that are displayed in the chart. If you change the Units selector to Bits/s then the flows which contributed the highest volume of traffic in bits/s are displayed. If you change the Units selector to Bits/s then the flows which contributed the highest volume of traffic in frames/s are displayed.

3.4.4. Changing the time selection

The Circles chart gives a graphical representation of the top 100 flows during the selected time period. The Time selector allows you to select the time period for which data is to be displayed.

For the Circles charts a time interval selection is defined by a start and end time. The Time selector includes the following, commonly used, time interval selections:

- Last 5 mins
- Last 10 mins
- Last 15 mins
- Last 30 mins
- Last hour
- Custom

The Custom option Gives full flexibility in accessing the stored historical data. Set the desired start and end times for the interval, then click the OK button to cause the chart for the selected interval to be displayed.

When a non-custom time period is selected, the displayed chart will be automatically updated when the next data point is available, thus displaying a rolling window of data.

The Time selector also includes back and forward buttons that can be used to view data for the previous or next time interval. For example if the time selection is Last 5 mins and the current time is Fri 21 Sep, 2012 11:44, clicking on the back arrow will cause the previous 5 minutes of data, ending at Fri 21 Sep 2012, 11:39, to be displayed (using the Custom time selection). The back and forward buttons will be inactive if the current time selection is at the beginning or the end of the stored data.

3.4.5. Selectively labelling chart elements

In addition to automatically labelling chart elements, you can selectively label chart elements by clicking on the element of interest. To show a label for an end host, click on the black square for the end host; to
show a label for a cluster, click on the white square in the centre of the circles, to label a flow click on a line. To remove a label, click on in the top right corner of the label.

3.4.6. Displaying end host information

You can find out more information about an end host by first clicking on the black square for the end host to display the label, then click on . This will open the Lookup host dialog using the end host address. If the Lookup host dialog is already open, then the dialog will be changed to show information for the newly selected host. See Chapter 11, End host information for more information.

3.4.7. Pan and zoom

The chart includes a view controller that allows you to zoom in and out; pan left, right, up, and down; and reset the chart to fit in the window. In addition you can zoom in and out using the mouse wheel and pan by dragging the mouse with the left button held down.

3.4.8. Filtering for specific traffic

sFlowTrend-Pro allows the information displayed in the chart to be filtered. This allows you to focus on traffic that may be of interest.

You can specify a filter using the Filter bar (see Section 10.1, “Basic use of filters”). In addition you can click on a label for an end host or a flow to automatically filter on traffic for the labelled end host or flow. You can also click on the legend entries to filter on traffic for specific protocols.

3.5. Selecting a switch

To view data for a specific switch, use the Switch selector in the control bar to select the switch you are interested in. The Switch selector lists the switches that have been included in the sFlowTrend-Pro configuration, or that sFlowTrend-Pro is receiving sFlow data from (see Section 13.2, “Configuring agents in sFlowTrend-Pro” for details on configuring switches in sFlowTrend-Pro). A switch is listed using its SNMP IP address, sFlow agent address, DNS Name, or sysName (see Section 13.5.1, “Setting the switch, interface, and host naming policy”).

In the Top N and Circles tabs, the Switch selector also includes an option All switches. When you select All switches, the resulting charts display the overall traffic through the network, such that, if traffic crosses multiple switches, the traffic is counted only once. If you would like to restrict the analysis to specific switches, you can do so by using a filter, for example: agent == "10.0.0.250" || agent == "10.0.0.248", where 10.0.0.250 and 10.0.0.248 are the sFlow agent addresses of the switches that you are interested in (see Section 3.3.6, “Filtering for specific traffic” for more information of filtering). The All switches option is not available in the Interfaces or Counters tabs, since interface counters are specific to a specific switch and interface.

Switches shown in italics in the selection list are disabled, meaning that data is not being stored for these switches. If the currently selected switch is enabled, click the button to disable this switch . If the currently selected switch is disabled, click the button to enable this switch .

Multiple switches can be enabled in sFlowTrend-Pro , whilst sFlowTrend allows five switches to be enabled at a time.
3.6. Selecting an interface

The Counters, Top N, and Circles tabs allow you to view data for a specific interface. Use the Interface selector in the control bar to select the interface that you are interested in. The Interface selector lists the interfaces for the currently selected switch, for which sFlow data is being received and stored. An interface is listed using its ifIndex, ifName, or ifAlias. (see Section 13.5.1, “Setting the switch, interface, and host naming policy”). Changing the interface selection causes a chart for the newly selected interface to be displayed.

In the Top N and Circles tabs, the Interface selector also contains an option All. Selecting this option allows you to view traffic flows through the whole switch (across all interfaces). This option is not available in the Counters tab, since counter charts can only display data for a single interface.
Chapter 4. Hosts

Network convergence, virtualization and cloud computing blur the line between network and system management. To understand performance in this environment you need to monitor both network and server resources. The Host sFlow standard, http://www.sflow.org/developers/specifications.php, defines the physical and virtual server performance metrics that a Host sFlow agent exports using the sFlow protocol. The Host sFlow agent provides scalable, multi-vendor, multi-OS performance monitoring with minimal impact on the systems being monitored.

For information on configuring host sFlow agent, see Appendix B, Configuring hosts to send sFlow.

The Hosts tab presents host performance statistics for hosts that are sending Host sFlow to sFlowTrend-Pro. This tab includes two sub-tabs providing different views of the host performance data:

Statistics
This sub-tab allows you to compare performance of all servers, virtual-machines and clusters across the whole network. See Section 4.1, “Statistics”.

Charts
This view allows you to trend performance metrics for any individual server or virtual-machine. See Section 4.2, “Charts”.

The ability to directly relate server performance to the corresponding network traffic is a key element in unifying network and system management.

4.1. Statistics

The Statistics sub-tab allows you to compare performance of all hosts over the last minute. Use the View selector to select the group of performance metrics (CPU, Memory, Disk, Network) of interest.
The selected performance metrics for the last minute are displayed in a sortable, hierarchical table, with one row for each host. Physical hosts are shown at the top level of the hierarchy. If the virtual-machines of a physical host are being monitored with sFlow, you can view the performance metrics for the virtual-machines by expanding the physical host.

This view is useful for comparing the current performance of hosts. For example, to compare the CPU utilization of all the hosts, click with the left mouse button on the % CPU column heading, to sort the hosts by CPU utilization.

To view the trend in performance for a host, click with the left mouse button on the row of data for that host. The tab will then change to the Charts sub-tab, showing a trend of the performance metrics for the selected host for the last hour.

### 4.2. Charts

The Charts sub-tab allows you to view a trend in performance for a host. Use the Host selector to select the host of interest and the Chart selector to select the performance metrics to trend. You can also select specific time interval (Chapter 9, Selecting a time period) over which to trend the data.
4.2.1. Physical host charts

If you select a physical host, the following charts are available:

CPU Utilization
The CPU utilization for each of the following categories: user, nice, system, IO wait, IRQ, Soft IRQ.

CPU load
1 minute, 5 minute, and 15 minute load averages.

Processes
Number of CPUs and number of processes running.

Interrupts
Number of interrupts/s and number of context switches/s.

Memory usage
Memory usage for each of the following categories: used, shared, buffers, cache, free.

Memory paging
Pages/s in and out.

Memory swapping
Pages/s swapped in and out.

Disk IO
Bytes/s read and written.
Disk usage
   Disk space used and free.

Network bytes
   Bytes/s received and sent over the network interfaces.

Network packets
   Packet/s received and sent for each of the following categories: packets, drops, errors.

4.2.2. Virtual host charts

If you select a virtual machine, the following charts are available:

vCPU utilization
   % time that the CPU is busy.

vMemory usage
   Memory used and free.

vDisk IO
   Bytes/s read and written.

vDisk usage
   Disk space allocated and available.

Network bytes
   Bytes/s received and sent over the network interfaces.

Network packets
   Packet/s received and sent for each of the following categories: packets, drops, errors.

4.2.3. Using the legend to select one counter

Sometimes one performance counter value can be much smaller than the other performance counters, making it hard to see the the smaller counter value trend. In this case, you can view the trend for only the smaller counter, by clicking on the legend item corresponding to the counter of interest. For example, when viewing the CPU Utilization chart, clicking with the left mouse button on I/O wait will change the chart to display only the trend for percent of CPU time spent waiting for IO; an additional trend line for the % of CPU time spent executing user processes can be added to the chart using Shift+left mouse button on User; or clicking with the left mouse button on I/O wait or the background of the legend area will cause all trend lines to be displayed again.
Chapter 5. Services

The Host sFlow standard, http://www.sflow.org/developers/specifications.php, defines application performance metrics that a Host sFlow agent exports using the sFlow protocol. A number of popular applications now include sFlow monitoring. For example, sFlow agents are now available for popular web servers, providing scalable performance monitoring of large web server clusters and load balancers.

The Services tab presents application performance statistics for services that are being monitored using sFlow. This tab includes two sub-tabs:

Counters
Trend charts showing how the overall volume of application transactions varies over time. See Section 5.1, “Counters”.

Top N
Trend charts showing the top contributors to application transaction volume and how the top contributors vary over time. See Section 5.2, “Top N”.

The ability to directly relate server and application performance to the corresponding network traffic is a key element in unifying management of cloud environments.

5.1. Counters

The counters tab shows how the overall volume of application transactions varies over time. It uses stacked area charts to display the application performance counters.

This tab includes a control bar which allows you to select the host and service for which you would like to view trends in transaction volumes, the application performance counters chart to display and the specific time interval (see Chapter 9, Selecting a time period ).
5.1.1. Counters charts

The following charts are available:

HTTP method
The trend in the number of operations per second for the various HTTP methods.

HTTP status
The trend in the number of operations per second with the various HTTP status codes.

5.1.2. Using the legend to view one counter

Sometimes one performance counter value can be much smaller than the other performance counters, making it hard to see the the smaller counter value trend. In this case, you can view the trend for only the smaller counter, by clicking on the legend item corresponding to the counter of interest. For example, when viewing the HTTP status chart, clicking with the left mouse button on Client error(4xx) will change the chart so that it displays only the trend for the number of operations per second that encountered client 400; an additional trend line for the number of successful operations/s can be added to the chart using Shift+left mouse button on Success(2xx); or clicking with the left mouse button on Client error(4xx) or the background of the legend area will cause all trend lines to be displayed again.

5.2. Top N

The top N tab displays trend charts showing the top contributors to application transaction volume and how the top contributors vary over time. For example, you can view the top URIs for a specific host or all hosts.
This tab includes a control bar which allows you to select the host and service for which you would like to view top n trend data, the type of chart to display. You can also select a the specific time interval (see Chapter 9, Selecting a time period), and filter on specific data (see Chapter 10, Filtering).

**Note**

When you have made changes to the selections for the chart, including creating a filter, you can save these selections in a bookmark (see Section 1.4, “Navigating around sFlowTrend-Pro using the history navigator”) so that you can easily return to the same chart at a later date.

### 5.2.1. HTTP top N charts

The following top n charts are available for understanding the top contributors to HTTP transaction volume.

- Top methods
- Top URIs
- Top URI paths
- Top URI files
- Top URI extensions
- Top URI hosts
- Top URI paths
- Top mime types
Top auth users
Top user agents
Top referrers
Top X-Forwarded-For
Top servers
Top clients
Top connections

5.2.2. Units

You can use the Units selector to choose the performance measurement used to calculate and display the top contributors. The following units are available:

Bytes/s
Calculates the top contributors based on the number of bytes/s in requests and responses.

Operations/s
Calculates the top contributors based on the number of operations per second.

Duration
Calculates the top contributors based on the mean duration of each transaction.

5.2.3. Understanding the Top N services chart

The legend in the Top N services chart shows the top contributors for the selected interval. The outlined time stamp, for example 4:10 PM, on the x-axis indicates the currently selected interval. You can select an interval and see the top contributors in that interval by clicking with the left mouse button on the bar corresponding to the interval of interest. Each other bar in the chart will then be recoloured so that it shows the transaction volume associated with the top contributors in the currently selected interval. This allows you to see how the top contributors change over time.

If the latest (right most) bar is selected and the Time setting is relative to now (for example Last hour see Chapter 9, Selecting a time period, the charts will be updated automatically and always display the contributors for the most recent minute.

The grey part of each bar represents transaction volume not attributable to the top N shown in the legend (ie it represents the contribution from other URIs, methods etc. that are not in the top N).

If the whole of a bar is grey, the transaction volume in its interval is not attributable to any of the top contributors in the currently selected interval. You can click on this bar to make it the currently selected interval and see its top contributors.

5.2.4. Displaying end host information

When Top servers, Top clients, or Top connections charts are displayed, you can find out more information about an end host by clicking on to the left of the host address in the legend. This will open the Lookup
host dialog using the end host address. If the Lookup host dialog is already open, then the dialog will be
drawn to show information for the newly selected host. See Chapter 11, End host information for more
information.

5.2.5. Using the legend to drilldown into service data

You can use the legend in the services top N charts to drill down into the service data. For example, if
you are viewing a Top URI hosts chart and you notice that most of the activity involves one URI host,
you can investigate which URIs for this host are being accessed by clicking with the left mouse button
on legend item that corresponds to the URI host. The Top URIs chart will then be displayed with a filter
for the selected URI host applied.

See Chapter 10, Filtering for more information of filtering.
Chapter 6. Using and configuring thresholds

Thresholds allow you to quickly identify specific problems in your network. When you set a threshold, you are identifying what is considered normal traffic levels for a switch or interface. If that traffic level is exceeded, then the threshold fires, and is highlighted for further investigation or action.

Thresholds are configured and monitored on the Thresholds tab in sFlowTrend-Pro.

The top half of the window allows you to view the current status (from the previous minute) of different thresholds (see Section 6.1, “Viewing thresholds”). The bottom half of the screen can help in determining the root cause of a threshold violation, for the thresholds currently being displayed (see Section 6.4, “Root cause analysis”).

6.1. Viewing thresholds

You can view and configure the thresholds for all switches, or for all interfaces on a specific switch. Use the View selector to select the view that you would like. The options are:

All Switches
   Displays a table of thresholds for each switch.

All Interfaces
   Displays a table of thresholds for every interface on each switch.
Customised thresholds

Displays only the thresholds for switches or interfaces that have been customised (see Section 6.3, “Defining thresholds”).

Switch name or address

If you select a specific switch (by name or IP address, depending on the switch naming policy configured in Tools → Options), the thresholds for each interface on that switch are displayed.

The current threshold values are shown in the table, in the top half of the window. Each column can be sorted by clicking on the header column. If you click on a column containing thresholds, then the column will be sorted by the current threshold values in the column. This provides an easy way to find the thresholds with the highest values (ie, those that are ‘most exceeded’).

6.2. Threshold values and types

Every threshold has a current value, which is displayed by the threshold indicator  . The value ranges from 0 - 100%, and the position of the bar in the indicator shows this value. In addition, as the threshold value exceeds predefined points, the colour of the indicator will change. If the threshold is normal, then the indicator is shown in green. As its value reaches 70%, then the threshold turns marginal, and is shown in yellow. At 90%, the threshold is critical, which is indicated by red.

The value of the threshold is defined by two factors: the trigger, and how long the threshold must have triggered for. For example, for the errors threshold, you might consider that the trigger is 5 errors per second. The duration might be 4 out of the previous 10 minutes. If the number of errors per second was 5 or more, in at least 4 out of the previous 10 minutes, then the threshold value would be 100%. The percent value is a combination of how long the trigger was exceeded for, relative to the configured setting, and how close the parameter being monitored was to the trigger.

To make it easier to find interfaces which have exceeded thresholds, the value of the threshold propagates up from a switch interface to the overall threshold value for the switch, and then from there to the overall threshold value for the network as a whole. The maximum threshold value propagates up, so that the overall value for a switch is the largest of the values for each of its interfaces.

Thresholds can be set on six different parameters:

Utilization

The percent utilization of an interface.

Unicasts

The number of unicast frames per second.

Broadcasts

The number of broadcast frames per second.

Multicasts

The number of layer 2 multicasts per second.

Errors

The number of errored frames per second.

Discards

The number of discarded frames per second.

When viewing the threshold table, you can click on any threshold indicator, to drill-down further and determine the cause of the threshold violation. If you click on a switch threshold, then the thresholds for all the interfaces in that switch will be displayed in the table. If you click on an interface threshold, then
sFlowTrend-Pro will jump to the charts for that interface, to give a view of the traffic seen on that interface. The traffic view selected is smart, so that the traffic highlighted will be related to the type of threshold clicked on (eg, if you click on the errors threshold for an interface, the Interface counters chart will be displayed with the errors/s trend selected).

6.3. Defining thresholds

Thresholds can be defined per interface, per switch, or globally. If a threshold is defined for a switch, then that threshold setting is used for each of the interfaces on the switch, unless specific thresholds for interfaces themselves are defined. Similarly, the global threshold setting is used for all switches and interfaces, unless overridden at the switch or interface level.

A threshold is configured using the edit threshold dialog. This can opened in a number of ways:

• Click the Configure global thresholds button on the threshold tab, to set the global thresholds. These will apply if a more specific threshold is not configured.

• When viewing a specific switch on the threshold tab, click the Configure switch thresholds button to configure the switch thresholds. These will apply if more specific interface thresholds are not configured.

• Similarly, when viewing all switches in the threshold tab, click the edit button to the left of the switch name to configure that switch’s thresholds.

• Finally, when viewing a table of interfaces (ie by selecting All interfaces, or a single switch), a specific interface's thresholds can be configured by clicking the edit button to the left of the interface number or name.

A useful way to see which thresholds have been customised is to select Customised thresholds to view. This will show all the switch and interface thresholds which have been customised; allowing their status to be observed, and their configuration changed.

When you open the edit threshold dialog, you can then enter the settings desired for each threshold parameter.
Using and configuring thresholds

See Section 6.2, “Threshold values and types” for a description of the settings for each threshold. By default, a switch threshold will be set to the global threshold setting, and an interface threshold will be set to the threshold setting for its switch. To customise the threshold, first uncheck the Use global thresholds (for a switch) or Use switch thresholds checkbox (for an interface), to allow the settings to be changed. If you want to remove the custom settings, and revert to the default, just re-check the checkbox.

6.4. Root cause analysis

The bottom half of the thresholds window allows you to analyse the cause of a threshold violation.

The pie chart on the left shows the root cause factors of threshold violations. These are the addresses and TCP/UDP ports that were seen most often across the interfaces with a threshold violation (marginal or critical). The chart shows the top ten factors. The scope of the interfaces being analysed is the same as the thresholds being viewed in the top half of the window. So, if All switches is selected in the View selector, then the chart will show the root cause factors for threshold violations on all interfaces. Similarly, if one specific switch is being viewed, the root cause factors will be for all interfaces on that switch.

From the set of interfaces being analysed, the specific threshold to determine the root cause factors for, is selected using the Analyse threshold selector. The thresholds for utilization, unicasts, broadcasts and multicasts can be analysed. Errors and discards cannot be analysed, as no traffic is recorded for an error or discard.

Assuming that at least one threshold has fired over the previous minute, in the set of interfaces and the threshold type you select, the root cause factors will be shown in the pie chart on the left. If you hover the mouse over a pie section, more detail about that factor will be shown, including the percentage of flows that the factor was present in, on all interfaces with a threshold violation. This helps you determine if a factor was a major contributor to the threshold violation, or if it was just one of many. If you then click on a pie section, the right-hand bar chart will be updated to show the percentage of flows that this factor was seen in, broken out by interface with a threshold violation. Only the top ten interfaces are shown. The colour of the bar represents the state of the threshold on that interface. If you click on a bar in the right-hand chart, then sFlowTrend-Pro will take you to the traffic chart for that interface, showing the top flows filtered by the root cause factor. Use this to get a full picture of the traffic that is causing the threshold violation on a specific interface.

The root cause analysis updates every minute, as new traffic is analysed. You can freeze the update to allow a more detailed analysis on the existing data by clicking the Freeze update button. The text of the button will change to indicate the time that update was frozen at. To resume normal minute updates, and ensure that you are analysing the latest data, click the button again.
Chapter 7. Events

sFlowTrend-Pro raises events when various conditions are detected. Traffic threshold events are raised when traffic levels cross the defined thresholds (see Chapter 6, Using and configuring thresholds). System events are raised when various conditions in the operation of sFlowTrend-Pro are detected (for example when users connect to or disconnect from sFlowTrend-Pro or if an error occurs). You can view these events in the Events tab.

The Events tab list the events and the summary information in the Events table. The tab allows you to view events for a selected time interval. It also allows you to view events of a selected Type (All, traffic Threshold, or sFlowTrend-Pro System), and Severity. You can filter viewed events further by entering a Search string which will match against the text displayed in the events table.

When you click on an event in the events table, the details of the event are displayed in the Event details pane. Where possible, the event details will include Follow up links. When you click on a follow up, sFlowTrend-Pro will display a view configured with the appropriate setting that gives you background information on the event. For example, for a traffic threshold event, clicking on the follow up takes you to a counters or utilization chart for the switch interface that crossed the threshold.

You can configure sFlowTrend-Pro to notify you when specific events are raised. See Section 13.4, “Configuring action on events in sFlowTrend-Pro".
Chapter 8. Reports

The Reports tab allows you to define custom reports, run reports and view and save the results of running a report.

A report definition consists of a description to describe the purpose of the report and a number of report sections. There are two types of report section:

Query section
A query section is used to define a query that will extract data from the sFlowTrend-Pro database and display results in tabular or graphical formats.

HTML section
An HTML section is used to embed text and other material in a report. For example an HTML section can be used to add a title and description for the data shown in a query section.

Running a report definition produces report results. These results can be saved so that they are available later and accessible to other users.

The Reports tab includes a reports browse pane that allows you to view existing report definitions, create and delete report definitions, and add and delete sections to report definitions. The Reports tab also includes a report settings pane that allows you to change the settings for a report and its sections, and run a report definition.

When you first install sFlowTrend-Pro a number of example report definitions will be installed in the System reports folder.
8.1. Organising report definitions

The reports browse pane allows you to organise report definitions in folders. A folder is shown using or The reports browse pane always shows the folders sorted alphabetically.

To add a new folder in an existing parent folder, select the parent folder and then click the new folder button .

A report definition is shown using The reports browse pane always shows the report definitions sorted alphabetically within a folder. To add a new report definition, select the folder in which to add the new report, then click the new report button . A new report definition with a query section will be created in the selected folder. You can also copy a report definition by selecting the report definition to copy, then clicking the copy report button . A copy of the report definition is created in the same folder.

A report section is shown using To add a new report section, select the folder in which to add the new report, then click the new section button and then select either HTML section, Query section, or Scripted query section. You can also copy a report section by selecting the section to copy, then clicking the copy section button . A copy of the section is created in the same report.

To delete a folder, report definition, or section, select the folder, report definition, or section to delete, then click the delete button You can also delete the selected folder, report definition, or section by clicking the right button and selecting Delete.

Administrators can add and delete report definitions. To load changes to report definitions that other administrators have made, click the Reload reports button in the reports browse pane.

You can change the name of a folder, report definition, or section by clicking on the folder, report definition, or section or by clicking the right button and selecting Rename. The reports browse pane will only allow you to rename folders, report definitions, and report sections if you choose a name which is unique among the siblings.

The reports browse pane supports drag and drop, so you can move a report definition to a another folder by dragging and dropping the report on the other folder. You can also use drag and drop to reorder sections within a report definition and move a section to a different report.

In addition, sFlowTrend-Pro allows you to import report definitions and export report definitions so that they can be imported into another sFlowTrend-Pro installation. See File → Import report and File → Export selected report .
8.2. Editing report definitions and sections

When you select a report definition or section in the reports browse pane, you can then edit its settings in the report settings pane.

The report settings pane also includes a number of controls:

- ![Save](image) Allows you to save any changes to the settings. This control is only active if you are an administrator and you have changed the settings.

- ![Undo](image) Allows you to undo any changes to the settings since the last save. This control is only active if you have changed the settings.

- ![Run](image) Allows you to run the report definition, including all the sections with the current (possibly unsaved) settings. The resulting report will be opened in a new window. Optionally if you are an administrator, you can save the results, by checking the Save results checkbox before you run the report definition, so that the results are available later and accessible to other users.

8.2.1. Viewing report results

When you select a report definition in the reports browse pane, the reports settings pane will show the description for the report definition and also a table of saved report results.

You can edit the report description so that it describes the purpose of the report. This description is not shown in the report results.

Each row in the report results table shows the time at which the report results were generated and also the following columns:

- ![View](image) View the report results in a new window.
- ![View](image) View the report results in a browser.
- ![View](image) View the report results in PDF format.
- ![Delete](image) delete the report results.

To refresh the report results table to load report results that have been generated by other users click the under the report results table.

8.2.2. Editing a query section

When you select a query section in the reports browse pane, the report settings pane will display the settings for the query section. In a query section you can define a query to specify the data that you want to extract from the database, and a display format for the data that is produced when the query is run.
A query specifies the data that you want to extract from the database. When a query is run it produces a table of results. When you define a query you are specifying the columns or fields that should be present in the table. A column can be a key field, for example sourceAddress, or a value field, for example bytesTotal. Each row in the table will represent a unique combination of the keys and values associated with that combination. For example, if a query is defined to have the fields sourceAddress and bytesTotal, then the query will produce a table of data where each row in the table includes a unique source address and the bytes sent by that address.

sFlowTrend-Pro supports commonly used, basic queries defined using Basic settings (see Section 8.2.2.2, “Editing a query using basic settings”), flexible, complex queries using Advanced settings (see Section 8.2.2.3, “Editing a query using advanced settings”), and flexible, complex queries with that ability to further process the results before display using Scripted settings (see Section 8.2.2.4, “Editing a query using scripted settings”).

When you add a new query section, a default query section will be created with Basic settings. You can edit these settings in the Basic settings tab, or if you are defining a more complex query, you can view the basic settings in the Advanced settings tab or the Scripted settings tab, and then edit the settings in one of these tabs. However, if you edit the settings in the Advanced settings tab, the settings will become incompatible with the Basic settings, so you will only be able to view and edit the query settings in the Advanced settings tab. Similarly, if you edit the settings in the Scripted settings tab, the settings will become incompatible with the Basic settings and Advanced settings so you will only be able to view and edit the query settings in the Scripted settings tab.

### 8.2.2.1. Defining how query results are displayed

The table of data produced when a query is run can be displayed in a number of different formats. You can select the most appropriate format for your use of the data. Displaying the data in a Table gives the raw data from the query; use this if you need the actual numbers. For example, you might want to check on the absolute utilisation of a link, or use the data in another application. Displaying the data in a Chart helps visualisation of the results; use this if you want to compare different items quickly, for example, easily see the largest contributors to the utilisation of a link. Another important difference between using a table and a chart is that a chart must have a value to plot. A table does not require a value, and so can be used to answer questions such as "which addresses were seen on a specific interface?".

In addition to choosing between a table and a chart, you can also decide whether to view the data as a total over the entire time period selected for the query, or as a trend of data over time. If you view the data as a total, then rows in the table represent data points for the whole time period. In this case, the interval from the time selector is ignored. If, however, you want to understand how a value changes over time, then you should select a trend. With a trend, each row in the table represents a data point for a period of time defined by the time selector interval.

If we use the Top Sources by frames query as an example, displaying the result of this query as a total will give the total frames sent by each of the top sources over the time period. Displaying the result as a trend will show how the number of frames sent by each of the top sources changed over time.

When a chart is used to display query results, the chart interprets results data using series, categories and values. sFlowTrend-Pro will choose the most appropriate fields to plot as categories and series based on the type of chart selected.

**Categories**

Categories are plotted on the x-axis of a chart. Charts that show data as totals have explicit categories, defined from the key fields that were used in the query. The categories are generated from all the unique combinations of the key fields found in the data. For example, if the key fields were sourceAddress and destinationAddress, then there will be a category for source-destination pair found in the data.
Charts that show data as a trend over time use time as categories. Each category corresponds to an interval in the overall time period of the query.

Values
Values are plotted on the y-axis of a chart. The value fields in the results form the values for the chart. Each category will be plotted against each of the values.

Series
Each series contains a set of related data. How a series is plotted depends on the type of chart. For example, a bar chart will show each series as a set of bars of the same colour, and each category will have a bar of each colour. A stacked bar chart shows only one bar per category, but each bar will contain several segments, with each segment representing a series.

For charts that show data as totals, a series is generated for each value field in the results. For example, if the value fields were framesTotal and bytesTotal, then one series is created for frames, and one for bytes. Recall that for a totals chart the categories are created from the key fields; this means that each series is formed from the associated value field plotted against each category.

For charts that show data as a trend, the series are generated from the key fields in the results. This is done in a similar way to the categories in a totals chart: each series will consist of the unique combinations of the key fields found in the results data. For example, if the key fields consisted of sourceAddress, then a series would be created for each source address found in the results. These series are then plotted against time.

The display format information panel (see Section 8.2.2.2, “Editing a query using basic settings”) is useful in understanding how a query will be plotted. When a query is created in the basic or advanced settings tabs, then the categories, series and values that will be produced are shown. For time trend charts, since the categories are always time, this is assumed and not shown in the information panel. Similarly, for a totals chart, since the series are always generated from the values, the series are not shown. In the case of a table, the columns that will form the table are shown.

The following formats can be used to display the data:

Bar chart (totals)
Displays the data in a bar chart, with bars used to show the values for each series in the data. Bar charts are used to display and compare data summarised over the query time period.

If one series is available (in the query one value is selected), then a single bar per category is shown. If multiple series are present, then a group of bars is plotted for each category, with the bars coloured to indicate the series.

Stacked bar chart (totals)
Displays the data in a stacked bar chart. This is similar to a normal bar chart, and when only one value field is selected in the query, produces the same result. However if multiple values are selected in the query, a series is generated for each value, and instead of plotting a separate bar for each series, a stacked bar is used. Each segment of the stacked bar represents a different series.

This type of chart is useful when two similar values are to be compared, for example framesIn and framesOut for an interface.

Line chart (trend)
Displays the data in a line chart trended over time. Each series in the data will be shown as a separate line in the chart, plotted against the categories. Use this chart to see how data changes over time.

A line in the chart is plotted for each series. With advanced charts, if more than one value is selected, a separate chart will be created for each value.
Area chart (trend)
Displays the data in an area chart trended over time. Each series in the data will be shown as an area in the chart. The areas for each item will overlap, which can make the results of this chart difficult to see. You could try a line chart or stacked area chart if this is the case.

As with the line chart, each area in the chart is formed from the series, and a separate chart will be created if multiple values are specified.

Stacked area chart (trend)
The stacked area chart is identical to the area chart, except the areas are stacked on top of each other, rather than overlapping. This can make the chart much easier to read.

Table
Use a table to view the raw results of your query. The table will include a column for each field specified in the query. It is not necessary for the query to include value fields, so a table is useful for inventory reports, where you want to understand what is present, rather than how much traffic is being generated.

All the columns for the query will be displayed in the table.

Table (trend)
The trend table also displays data in a tabular form, but includes time as the first column. Use this type of table to get the specific values from a query, instead of the visualisation provided by charts.

All the columns for the query will be displayed. Each row in the table will include the time, and associated data for that time. If there are multiple data points per time period, then there will be multiple rows with the same time. Also, if there are any data points which are the 'other' from a top-n query, then they will be shown with the non-value columns blank (the columns for value fields will show the value for 'other').

8.2.2.2. Editing a query using basic settings

The Basic settings tab helps you define and parameterise commonly used queries. These queries are very similar to those used in the Network tab (see Chapter 3, Network), Hosts tab (see Chapter 4, Hosts), and Services tab (see Chapter 5, Services).
To define a query using Basic settings, first decide whether you are interested in network traffic data (use the View selector to select Network), host performance data (use the View selector to select Host), or service performance data (use the View selector to select Service).

If the query is focused on network traffic data, you can select whether the query should extract data for the whole network or for an individual switch or interface. If the query should extract data for the whole network, use the Switch selector to select All switches. In this case, even if a traffic flow crossed multiple switches, the flow will only be counted once - i.e., the query de-duplicates the data. If the query should extract data about traffic crossing an individual switch and/or interface, use the Switch and Interface selectors to select the switch and interface of interest.

If the query is focused on host performance, you can select whether the query should extract data for all hosts physical hosts, all virtual hosts, or an individual host using the Host selector.

If the query is focused on service performance, you can select whether the query should extract data about all hosts or an individual host using the Host selector. You can use the Service selector to select the service of interest.

The next step is to use the Query selector to choose a predefined query; you can think of this as selecting the key fields for the columns in the query results. You can then use the Value selector to specify the value field column for the results. Note that the network Utilization and Counters predefined queries are only available when a single interface is selected using the Switch view and Interface view selectors.

The next step is to parameterise the query:

**Top N**

Specify how many rows there will be in the table. In general only a few contributors are responsible for the majority of the traffic or application transactions. Selecting a value for the top n results in data showing who those few contributors are. The Top N selector is not enabled when network Counters, or Utilization queries, host predefined queries, or service counters predefined queries are selected.
Time
Select the time period for which the query will extract data. The time selector is described at Chapter 9, 
Selecting a time period.

Filter
Further refine the query by filtering on specific attributes of the traffic. Filtering is described at 
Chapter 10, Filtering.

Once you have fully parameterised the query, you can select how you would like the results to be 
displayed using the Display results in selector to select a display format. When you select a display format, 
sFlowTrend-Pro helps you understand how the data produced by the query will be displayed. For example, 
if you select Bar chart (totals), the display format information panel will show which fields will be used 
for the categories (bars) and the value field used to determine the height of the bar.

8.2.2.3. Editing a query using advanced settings

The Advanced settings tab allows you to define your own queries by manually selecting the key fields and 
value fields that the query should extract data for.
To define a query using Advanced settings, first select the database table that query should access. sFlowTrend-Pro includes three database tables:

Counters
This database table includes data on the overall loading of each of the interfaces being monitored.

Traffic
This database table includes data on the end hosts using the network and which protocols they are using.

Host counters
This database table includes data on the performance of end hosts.

Service counters
This database table includes data on the overall application performance.
This database table includes data on application transactions and their attributes. It can be used to understand the top contributors to application transaction volume.

If you have selected Counters or Traffic database table, you can then decide whether the query should extract data for the whole network or for specific switches or a specific interface. If the query should extract data for the whole network, check the All switches check box. If the query is to extract data for specific switches, then make sure that the All switches check box is not checked, then select one or multiple switches from the list of switches being monitored. If the query should extract data about traffic crossing an individual interface, select the switch for the interface, then use the Interface selector to select the interface of interest. If the query is defined to have a view with multiple switches, if a traffic flow crossed multiple switches, the flow will only be counted once - ie the query de-duplicates the data.

If you have selected the Host counters database table, you can then decide whether the query should extract data for all hosts or for specific hosts. If the query should extract data for all hosts, check the All hosts check box. If the query is to extract data for specific hosts, then make sure that the All hosts check box is not checked, then select one or multiple hosts from the list of hosts being monitored.

If you have selected the Service counters or Services database table, you can then decide whether the query should extract data for all hosts or for specific hosts. If the query should extract data for all hosts, check the All hosts check box. If the query is to extract data for specific hosts, then make sure that the All hosts check box is not checked, then select one or multiple hosts from the list of hosts being monitored. If the query should extract data about a specific service, then use the Service selector to select the service of interest.

The next step is to specify the fields for which the query should extract data for. The Select query fields panel allows you to select fields from those available for the selected database. The available fields are shown in the Available fields list, with the value fields listed in italic. If you want to display the results of the query in a chart, you must select at least one value field. The Available fields list includes a type in text field that allows you to filter the available fields for fields whose names match the typed in text. For example, if you have selected the Traffic database, you can type addr into the type in field to see only those fields which include addr in their names.

You can also specify functions of fields. Functions are described at Section 16.4, “Database functions”. Click the Function button to show a dialog that helps you build a function. Some functions may not be relevant for the selected database.
If you have selected at least one value field, you will have the option of selecting whether the query results should be sorted and which value the results should be sorted on. You can also specify the Top N, which will cause the query results to show only the top n entries when sorting on the specified value. You can also choose to see all the results by checking the Include all checkbox, this is only sensible if you choose to display the query results in a table.

As with the Basic settings, you can parameterise the query further by selecting a time period for which data should be extracted (see Chapter 9, Selecting a time period) and a filter to select traffic that meets certain attributes (see Chapter 10, Filtering).

The final step is to select the output format for the query results using the Display results in selector. Select a table or chart appropriate to the report you are creating.

The Category or series format field can be used to improve the formatting of a chart. This can be set to a string, using the syntax of the Java Formatter [http://download.oracle.com/javase/6/docs/api/java/util/JavaFormatter.html].
Reports

Depending on the chart selected, a list of fields are used for the categories or series in the chart. The format string can combine the members of the list into a more human-readable form. Each item in the list of categories or series can be referenced in the format string using \texttt{%i$s} where \texttt{i} is the \textit{i}\textsuperscript{th} member of the list. For example, if the series list is \texttt{agent, ifIndex} (as in the example), and a format string \texttt{%1$s>%2$s} is used, then the series will be named \texttt{agent>ifIndex}. If a format is not specified, then the series will be named using a comma separated list (\texttt{agent, ifIndex} in the example).

It can be quite complicated to create a format string. The basic approach is to consider that each item in the series or category list will always be a string, and can be referenced using \texttt{%1$s}, \texttt{%2$s}, etc. Other characters can then be used to combine these together in a meaningful way (in the example above, the \texttt{>}' character is used to separate the agent from the ifIndex).

8.2.2.4. Editing a query using scripted settings

The Scripted settings tab allows you to define your own queries by manually specifying the key fields and value fields that the query should extract data for. Using a scripted query allows complete flexibility in the queries that can be run and charts generated. It is also possible to use the same set of data to create multiple output images in the report, for example a chart and a table of results. This technique can make reports faster to run with slow queries, since the query only has to be executed once. Scripted queries are written using the JavaScript language. This document does not describe the JavaScript language, however there are many good books and web sites on this topic. The user contributions area at the InMon Corp. customer portal (http://www.myinmon.com) can also be used for sharing example reports with other users.

The Scripted settings tab is divided into two areas: variable definitions and the script editor.

Variable definitions allow a query to be parameterised (run with different settings) without editing the script itself. Instead, a variable definition is changed. This mechanism is used by the basic and advanced
query editors to specify the various parameters of a query. If you view a basic query within the scripted query editor (by selecting the Scripted settings tab, you can see the variables used. Variables can be changed by editing the name of the variable, or the value, within the table. A variable can be deleted by clicking , and new variables added as required. Any variables defined here can be accessed from the report script as properties of the reportVars object.

The script editor is how the actual report script is entered. The script should be written in standard JavaScript, which can also include special classes defined by sFlowTrend-Pro. The normal flow of a report is to define the query required, to run the query to obtain a table of results, and finally to visualise the results using a chart or a table. A simple example of top sources is shown below:

```javascript
var query = new Query("flows", ",
    'timestamp("Timestamp", time), sourceAddress, 
    resolve("Source name", sourceAddress), rate(framesTotal)' ,
    ", "lastHour", 1, "rate(framesTotal)", true, false, 5);
var result = query.run();
report.timeChart("lineChart", result, "sourceAddress, resolve(sourceAddress)", 
    "%1$s(%2$s", "rate(framesTotal)");
```

Note that you have to take care with the use of single and double quotes, and use the line continuation character \ to concatenate long strings which cover multiple lines together. In particular, any quotes that appear within database functions must be double quotes (in the example above, we have used single quotes for the select string, to make it easier to then use double quotes within the functions).

You can refer to Section 16.5, “Classes and objects defined within scripted reports” for the reference of additional objects and classes defined within JavaScript to allow reports to be generated. Section 16.2, “Database fields reference” is the reference of fields available from the database, and Section 16.4, “Database functions” for the database functions that are available.

### 8.2.3. Editing an HTML section

When you select an HTML section in the reports browse pane, the report settings pane will display the settings for the HTML section. An HTML section can be used to provide formatted and unformatted content in the report. For example, if you would like to show a title and a description for a chart produced by a query section, you can insert an HTML section before the query section. You can then edit the settings for the HTML section as follows:

```html
<h1>Top sources</h1>
<p>This chart displays top sources for today</p>
```

You can enter text or HTML formatted text in an HTML section.
8.3. Running a report

To run a report definition, select the report definition or any of its sections in the reports browse pane, then click the Run reports button in the report settings pane. The results will be displayed in a separate window. If you are an administrator you can also select to save the results of running the report by checking the Save results checkbox. If you have chosen to save results, then the report results will be available in the report results table in the report settings pane when the report definition is selected in the reports browse pane.

When you run a report definition, the settings that are currently showing will be used and not the saved settings.
Chapter 9. Selecting a time period

sFlowTrend-Pro stores a history of network, host and application performance data (see Section 15.1, “Custom configuration” for information on configuring the length of history stored). The Time selector allows you to select the period in the history for which data is to be displayed. Since sFlowTrend stores one hour of data, the Time selector is not available and sFlowTrend always displays the last hour of data.

A time selection is defined by a start and end time, and, when data is displayed as a trend over time, an interval size. The interval size defines the granularity of the data displayed. For example Tue 10 Apr, 2007 01:00 - Tue 10 Apr, 2007 05:59, Interval = 2 mins, defines a 6 hour time period, with data points for each 2 minute interval in the time period. There are two ways to make a time selection:

- Using the Time selector (see Section 9.1, “Using the Time selector”)
- Dragging the mouse (see Section 9.2, “Making a time selection by dragging the mouse”)

9.1. Using the Time selector

The Time selector includes the following, commonly used, time selections:

Last hour
- Last hour, with a data point for each 1 minute interval.

Last 6 hours
- Last 6 hours, with a data point for each 2 minute interval.

Last 12 hours
- Last 12 hours, with a data point for each 5 minute interval.

Last 24 hours
- Last 24 hours, with a data point for each 15 minute interval.

Today
- Today, with a data point for each 15 minute interval.

Yesterday
- Yesterday, with a data point for each 15 minute interval.

This week
- This week, with a data point for each 1 day interval.

Last week
- Last week, with a data point for each 1 day interval.

Custom
- Custom time selections see Section 9.1.1, “Using custom time selection”

Note

If the start time of the time selection is earlier than the start of the stored history, the start time will be adjusted to the start of the stored history. For example if sFlowTrend-Pro is configured to store 7 days of data and today is Friday 15 Jun, 2007, then the earliest day for which there will be stored data will be Saturday 9 Jun, 2007. In this case, when Last
week is selected, the start time will be adjusted to Saturday 9 Jun, 2007 (rather than Sunday 3 Jun, 2007).

The Time selector also includes back and forward buttons that can be used to view data for the previous or next time period. For example if the time selection is Last 6 hours and the current time is Tue 10 Apr, 2007 12:53, clicking on the back arrow will cause the previous 6 hours of data, ending at Tue 10 Apr 2007, 06:53, to be displayed (using the Custom time selection). The back and forward buttons will be inactive if the current time selection is at the beginning or the end of the stored data.

When a non-custom time period is selected, the displayed chart will be automatically updated when the next data point is available, thus displaying a rolling window of data. The Progress indicator will show when the chart will next be updated.

When you choose a time selection which has an interval size greater than 1 minute, the Progress indicator will have two parts. The upper part will show progress through the current minute, whilst the lower part will show progress through the chosen interval (ie how long until the next data point will be available).

9.1.1. Using custom time selection

The Custom time selection gives full flexibility in accessing the stored historical data.

Use the date, hour, minute, and interval selectors to set the desired start and end times and interval size, then click the OK button. to cause the chart for the selected time period to be displayed.

Note

There is a maximum number of data points that can be displayed in a chart, so small interval size selections will not be available for long time period selections.

When the Custom time selection is used, the charts are static and are not updated as more data becomes available.

9.2. Making a time selection by dragging the mouse

You can select a time interval to view in more detail by dragging the mouse over the chart. As you drag the mouse the time selection is shown by highlighting in the region in the chart. When you release the mouse, a new chart will be displayed for the Custom period between the chosen start and end time sand using the smallest possible interval size (ie the most detailed data that can be displayed for the period). Since this new chart is using a Custom time selection, the new chart will be static and will not be updated as more data becomes available.
Chapter 10. Filtering

sFlowTrend-Pro allows the information displayed in a Top N network traffic or service chart (but not a counters chart) to be filtered. This allows you to focus on a subset of the data that may be of interest. For example, if you only wanted to look at web traffic, you could set a filter for only TCP port 80 traffic.

### 10.1. Basic use of filters

The filter is activated by clicking on the filter button (if you are currently viewing a counters chart, then the filter button is disabled). If the filter is active, then the button is shown without a red line, , and the filter bar is displayed. If it is inactive, the button is drawn with a red line though it, and the filter bar removed. The current filter can be activated and deactivated by repeatedly clicking the button. This does not remove the text of the filter in place, so you can quickly see the effect of filtering and not filtering your data.

Filters are created by entering the filter into the filter bar. The filter can be specified just by typing the appropriate expressions into the filter bar, or to make it easier you can use the filter builder.

To bring up the filter builder, click the Edit button at the right-hand end of the filter bar. The filter builder bar will appear below the filter bar.

<table>
<thead>
<tr>
<th>Filter</th>
<th>tcpServerPort</th>
<th>Operator</th>
<th>Equal</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the filter builder, you can select the term that you want to filter on, a relational operator (eg "==" for equality), and a value. For example, to filter on web traffic, you would select tcpServerPort for the filter term, the equality operator, and enter 80 for the value. Then, clicking on the Add button adds this expression to the filter.

You can combine many different expressions together, using logical operators ( | | for or, & & for and). For each expression you want to add to the filter, click the & & or | | button as appropriate (you can also use parenthesis to ensure the correct order of evaluation), then select the expression you want and click Add.

**Note**

How you type the value to compare against depends on what type of term you are comparing. For entries such as TCP ports, which are integers, just type the number. For MAC or IP addresses, the value must be surrounded by quotes: for example, ipServer == "10.0.0.1". Addresses and ports must be entered in their numeric form. It is not possible currently to use a DNS name in the filter.

When the filter is complete, apply it by clicking the OK button at the right of the filter bar. The chart will be redrawn, using only data that matches the filter. The current filter is displayed at the top of the chart, to remind you how the data was filtered. If there was an error in the filter, then instead of the chart an error message will be displayed. Sometimes, it can be difficult to understand the error messages. Common errors are omitting quotes around an address, or using & & or | | without matching expressions.
When using the filter builder, you will notice that as the filter is constructed, it is entered into the filter bar. It is also possible to directly type into the filter bar. See Section 10.2, “Advanced use of filters” for more information on the format of filters. For a list of the available items to filter on, and their meanings, see Section 10.3, “Terms available for use in filters”.

10.2. Advanced use of filters

This section contains information on using JavaScript to construct custom filters, which allows very specific filtering.

Section 10.1, “Basic use of filters” describes the basic use of filters. To use a filter, an expression is entered into the filter bar, which specifies what to filter on. The filter expression is actually interpreted in JavaScript, which allows the full power of JavaScript to be used to create a filter. The expression can take the form of a series of JavaScript statements, eg

```
statement-1;
statement-2;
...
statement-n
```

Each of these statements is evaluated for each network traffic datapoint found. The result used by the filter is the result of the final statement, `statement-n`, which must be a boolean. If the result is `true`, then the datapoint is passed by the filter, and added to the chart. If the result is `false`, then that datapoint is discarded. If the final expression is not a boolean, then an error is indicated. Note that the statements prior to the final one may have side effects, that affect the result of the final statement.

The terms that can be referenced from the filter are listed in Section 10.3, “Terms available for use in filters”. Any valid JavaScript boolean operator or function can be used to evaluate a term. This includes regular expressions, which allow more complex pattern matching than equality.

A common requirement, but one difficult to formulate in a filter, is testing if an IP address is a member of a specific subnet. To make this easier, a function is provided for this purpose: `inSubnet(address, subnet, maskBits)`. This will return `true` if `address` is a member of `subnet` with a mask of length `maskBits`. `address` can be any address field, or in fact any string representing an IP address.

For example, to create a filter to retain only traffic from subnet 10.1.2.0/24, use this filter:

```
inSubnet(ipSource, "10.1.2.0", 24)
```

More complex filters can be constructed; for example, if you wanted all traffic from the above subnet going to another subnet 192.168.0.0/16, then you could use:

```
inSubnet(ipSource, "10.1.2.0", 24) && inSubnet(ipDestination, "192.168.0.0", 16)
```

10.3. Terms available for use in filters

Section 16.2, “Database fields reference” describes the fields that can be used in filters. These fields must be formed into filter expressions, as described in Section 10.2, “Advanced use of filters”. The table also
Filtering

specifies the type of each field. You should be careful to only combine fields of the correct type together, using the normal rules for JavaScript.

As noted in Section 16.2, “Database fields reference”, only fields that are associated with the database table (flows or counters) that the query is being run over can be used.

In addition to constant fields, functions are also provided to help build filters. The functions available are described in Section 16.3, “Filter functions reference”
Chapter 11. End host information

sFlowTrend-Pro uses sFlow data to automatically discover the switch and interface that connects an end host to the network. You can access this location information, together with other useful information about an end host by selecting the Tools → Lookup host menu item. This opens the Lookup host dialog.

The Lookup host dialog includes the following fields:

Host
   Enter the IP address, MAC address or the DNS name of the end host for which information is required.

DNS name

MAC address
   The MAC address for an IP address is discovered from the traffic monitored over the last hour. If an IP address has not been seen in the last hour, then the MAC address will not be displayed.

MAC vendor
   If the MAC address is displayed, then the MAC vendor code in the MAC address is used to look up the MAC vendor.

Location
   The location (switch and interface connecting the end host to the network), is discovered from traffic monitored over the last hour. The location is given in the form Switch IP address>ifIndex. If the end host is not local then its location will be shown as the up link of the monitored switch or router closest to the border. If the end host has not been seen in the last hour, then the location will not be displayed.
Country

If the IP address for the end host is discovered, then it will be used to look up the country and indicate the country on the map. The country location for some IP address (for example local 10* addresses) are unknown.

Merit Network's Routing Assets Database (RADb)

Clicking on this link will open a browser to lookup the IP address in RADb. If the IP address is not shown, then this link will be inactive.

You can also access end host information directly from the Top N and Circles charts by clicking on the symbol shown next to end host addresses in the charts.

End host address mapping and location information can also be shown in reports by selecting the database key functions: countryCode, countryName, locate, mac, and vendor. See Section 16.4.2, “Key functions”
Chapter 12. Running sFlowTrend-Pro as a service

12.1. Introduction

sFlowTrend-Pro includes an option that allows it to be run as a service. When this option is chosen, data is collected continuously, regardless of whether you are logged in to the system or have the user interface active. When running as a service, sFlowTrend-Pro is split into two parts: the server, which is responsible for collecting and analysing sFlow data; and the client, which is used to view the data and create charts. By running sFlowTrend-Pro in this way, you can be sure of continuous data collection, and allow different people in your organisation to access the data easily.

Two clients are available, one which is used to access the server running on the same system as the client; and another optional client which can access data on a remote system.

When you purchase or request an evaluation of sFlowTrend-Pro you must choose the option of running sFlowTrend-Pro as a service. If you initially chose to run sFlowTrend-Pro as an application, but would now like to change to the service option, please submit a support request http://www.myinmon.com.

To allow the sFlowTrend-Pro server to receive sFlow from the devices that you are monitoring, the incoming sFlow data must be allowed to pass through any firewalls. When running as a service, host firewall configuration can be confusing, since the firewall configuration must correspond to the user that the service is running as. See Section 14.2.4, “What firewall requirements does sFlowTrend-Pro have?” if you are having difficulty in receiving sFlow.

12.2. Installation

Installation of sFlowTrend-Pro as a service is done through an installer, obtained from http://www.myinmon.com. Download the appropriate installation file for your system: either Windows, Linux or Mac. For Linux, you can download either an interactive installer, a Debian package (.deb file), or an RPM file, depending on your preference. If you are installing on Windows, Mac or using the interactive installer on Linux, follow the instructions in Section 12.2.1, “Using the interactive installer”. For more information on installing with a Debian or RPM package, see Section 12.2.2, “Installing with a Debian or RPM package”.

After sFlowTrend-Pro is installed, the license must be configured to allow it to be used. When the client first connects to the server, a dialog should automatically pop up to allow you to enter the license number. If it does not, or you would like to change the license, see Section 13.1, “Configuring the license” for more information. Note that normally sFlowTrend-Pro will use the Internet to download the license key, once the license number has been entered. If a proxy configuration is required for the server to connect to the Internet, please make sure that the proxy is correctly configured (see Section 13.5.4, “Proxy configuration”). If the system has no Internet connectivity at all, then the license key can be entered manually. First, request a manual license key using a support request at http://www.myinmon.com. Once you have the key, then enter it as described in Section 13.1, “Configuring the license”.

12.2.1. Using the interactive installer

On Windows, Mac, or if using the interactive installer on Linux, follow the instructions in this section after downloading the installer file.
Running sFlowTrend-Pro as a service

On Windows, just run the file by double-clicking it.

On Mac, mount the disk image by double clicking on it, then run the installer contained in the disk image by double clicking on it. Remember to unmount the disk image when finished.

On Linux, you will need to be root to install sFlowTrend-Pro. If you choose to use the interactive installer, run the installer by typing `#/bin/sh installer` where installer is the file you downloaded. Alternatively make the file executable and then run it.

When you launch the installer, you will be presented with a sequence of installation steps. After the initial welcome screen, you will need to accept the license agreement. Next, choose the directory where you would like to install sFlowTrend-Pro; it is recommended that you accept the default location. In the next screen, you can chose which components to install:

- **sFlowTrend-Pro service**
  - Select this option to install the service and the local client used to connect to the service on the same system.

- **sFlowTrend-Pro remote client**
  - Select this option to install the remote client, which you can use to connect to other systems running the service.

You can install both the service and the remote client on the same system, if desired. You must select at least one of the options to complete the installation.

If you selected the service installation, on the next screen you will be prompted for the sFlowTrend-Pro home directory. This is where the database, log files and custom configuration is stored. Using the default directory is recommended, although it can be changed if you would rather use a different location. In particular, please make sure that enough disk space is available to store the database. The disk space required will depend on the type of network traffic seen, and the number of switches being monitored. Several gigabytes will be enough for most installations. Once you have chosen a location, it cannot be changed without reinstalling sFlowTrend-Pro.

The remaining screens allow you to select the menu location to install the shortcuts for launching sFlowTrend-Pro, and then proceed with the installation. After completing the installation, the service is started automatically (if you chose to install it), and you will have the option of immediately launching the client.

### 12.2.2. Installing with a Debian or RPM package

If you chose to install sFlowTrend-Pro using a Debian or RPM package, then the normal method for installing these files should be followed for your operating system, after downloading them. Note that Java 6.0 must be installed prior to installing sFlowTrend-Pro. When installing sFlowTrend-Pro using a package file, the home directory cannot be changed.

### 12.2.3. Notes on installing sFlowTrend-Pro as a service under Linux

After completing the installation of sFlowTrend-Pro on Linux as a service, the sFlowTrend-Pro service will be automatically created (as `/etc/init.d/sflowtrend-server`) and started. The service will also be registered to automatically start when the system is booted, using `chkconfig`. This is only possible for Linux distributions that use the `chkconfig` command. Some distributions use other methods for automatically starting services. If the Linux that you are using does not use `chkconfig`, then you should enter the `/etc/init.d/sflowtrend-server` service manually as a service to be started at boot time.
If you are installing sFlowTrend-Pro on a system which does not have a graphical user interface, you can either install using a package (see Section 12.2.2, “Installing with a Debian or RPM package”), or using the interactive installer but with a terminal interface. To do this, add the command line option `-c` to the installer, eg: `#/bin/sh installer -c`. This will step through the same installation steps that are used for the graphical installer, just using a terminal interface. Please take care to enter the data correctly, as the command line interface is more difficult to use than the graphical interface.

### 12.2.4. Memory configuration for the sFlowTrend-Pro service

The amount of memory required by the sFlowTrend-Pro service varies considerably, depending on how many sFlow agents are monitored, and the quantity and type of network traffic. The default memory available to the service is generous and suitable for most installations. However, if memory runs low then events will appear in the event log warning of this, and performance of sFlowTrend-Pro may become poor.

To increase the memory available to the service, first go to the `bin` directory, in the directory on the server where sFlowTrend-Pro was installed. Here there should be a file named `sflowtrend-server.vmoptions`. Edit this file with a text editor, and add a line to the end with this format:

```
-Xmx1800m
```

This will change the memory available to be 1800 MB. The memory can also be reduced in a similar way. After making this change, the sFlowTrend-Pro service must be restarted for the change to take effect.

**Note**

It is very important to specify a valid memory configuration. If the directive is incorrectly typed, or has an invalid size of memory, then the sFlowTrend-Pro service will not start. Be aware that with a 32-bit JRE, the maximum memory that can be specified is approximately 1800 MB; if the size is greater than this, then the service will not start. If you are using a 64-bit OS and a 64-bit JRE, then a larger amount can be specified.

### 12.2.5. Configuring https certificates

To allow https to run on the sFlowTrend-Pro server, an https certificate is required. When the sFlowTrend-Pro service is first started, a default certificate will be installed. If possible, this will use the hostname of the server, or if this cannot be determined, then a generic `localhost` hostname.

It is possible to configure a different certificate to use for the server, if, for example, you wish to use a certificate signed by a local enterprise certificate authority. To do so, you will need to use the command `keytool`, which is included with the Java Development Kit (JDK), available from Oracle or the OpenJDK.

First stop the sFlowTrend-Pro service. Then create the keystore to use with `keytool`. The keystore must contain a trusted certificate entry (including a private key), and should be placed in the sFlowTrend-Pro home directory. You should then create the custom configuration options `server.webserver.https.keyStore`, `server.webserver.https.alias`, `server.webserver.https.password` and `server.webserver.https.keyPassword` (these are only required if the desired values are different from the defaults). When the sFlowTrend-Pro service is then restarted, the new certificate from the keystore will be used.

If, at any time a new default certificate is required (eg if the system name is changed), just stop the sFlowTrend-Pro service, delete the default keystore, and restart the service. A new default keystore will be automatically created.
12.3. Connecting to a server

If you installed the remote client, you can use this to connect to a remote server. Launch the client (using Start → Programs → sFlowTrend-Pro → sFlowTrend-Pro remote client). The Connection dialog will be shown:

![sFlowTrend-Pro: Choose server dialog]

Enter the name or IP address of the server, and if you have configured user authentication to control access (see Section 13.6, “Configuring user authentication”), the user and password for the connection. If user authentication is disabled on the server, then the user name and password can be left blank and will be ignored.

The client will use TCP port 8087, by default, to connect to the server. Please make sure that no firewalls are blocking this port on the client system, the server, or in the network. If the server that you would like to connect to has been configured to use a different port (see Section 15.1, “Custom configuration”), click the Advanced button, and enter the port used by the server.

If the connection is lost between the client and the server, the client will try to reconnect several times. If it cannot connect, then it will show an error message and exit. Even though the client has been disconnected, the server continues to collect data as before, unless of course the server was stopped.

12.4. Connecting to a server using a web browser

You can also connect to the server by pointing a web browser to http://server:8087/sflowtrend (or over https https://server:8443/sflowtrend). If the server that you would like to connect to has been configured to use a different webserver port (see Section 15.1, “Custom configuration”), you will need to use the configured port for http or https.

12.5. Connecting to a server using Java Web Start

As an alternative to manually running the remote client or using a web browser, it is also possible to launch the client using Java Web Start. This is a convenient way to run the client on an arbitrary host.
To connect using Java Web start, the client system must have Java (minimum 7.0) and Java Web start installed. Then, using a browser on that system, connect to the server with the TCP port that it is using - 8087 by default - eg http://server:8087. You should see the sFlowTrend-Pro server web page, which includes a link to start the client. Click this link, and the client should be downloaded from the server, launched, and connect to the server.
Chapter 13. Configuration

13.1. Configuring the license

If you are running sFlowTrend-Pro as a service, then the license must be configured before use. If you are running as an application, then the license cannot be configured (but the license dialog can still be used to view the expiry date, or any problems with the license).

Select the File → License menu item to launch the license dialog. The first time you run sFlowTrend-Pro as a service, this dialog should launch automatically.

Enter the license number for your sFlowTrend-Pro license (starts with "SFT...") in the License number field, then press the Set license button to configure the license on the server. If there is any problem with the license number you provided, this should be reported, allowing the correct number to be entered. Otherwise, if the license is accepted, the dialog will close and sFlowTrend-Pro will continue with the new license.

sFlowTrend-Pro will use the license number entered to download the actual license key from the Internet. If the server requires a proxy connection for Internet access, please ensure that this is correctly configured (see Section 13.5.4, “Proxy configuration”). If the system has no Internet connectivity at all, then the full license key can be entered manually. To get the key, please submit a support request at http://www.myinmon.com. Then click Advanced on the license dialog, and a field for the key will be shown. You can paste the key into the field using the Ctrl-v key. After pressing the Set license button, the new license from the key will be used.

13.2. Configuring agents in sFlowTrend-Pro

An sFlow agent is responsible for sending sFlow data to sFlowTrend-Pro from a switch (or router) or a host. In the case of a switch or router, one agent will be associated with the device, and the IP address of the agent will normally be the same (or one of the) IP address used for the switch. Switches can be configured to send sFlow from sFlowTrend-Pro using SNMP, or alternatively the switch can be manually configured. For hosts, normally the agent runs on a physical host. This agent can send data for both that host, and any virtual machines that are running on that host. Hosts are configured to send sFlow either through DNS or manually.

Select the Tools → Configure agents menu item to launch the Configure agents dialog. This dialog contains a table which lists all the agents that sFlowTrend-Pro is receiving sFlow from. For switches, it also allows you to change the SNMP settings for each switch, and to tell sFlowTrend-Pro about switches that it should configure via SNMP to send sFlow.

The table includes the following columns:

Status

This column uses colour coded symbols to indicate the overall status of the agent:

- The agent is enabled and sFlowTrend-Pro is receiving sFlow (and, if the agent is a switch or router, it can communicate with the switch using SNMP).

- The agent is disabled, but sFlowTrend-Pro is receiving sFlow from it. Or, if the agent is a switch, then either sFlowTrend-Pro is receiving CLI configured sFlow from it, and sFlowTrend-Pro is unable to communicate with the switch via SNMP to get the interface names, or sFlowTrend-Pro is...
still in the process of configuring sFlow on the switch. See Section 14.1.7, “sFlowTrend-Pro cannot communicate with the switch using SNMP”.

- The agent is enabled, but sFlowTrend-Pro is not receiving sFlow. If the agent is a switch, then this can also mean sFlowTrend-Pro cannot communicate with the switch using SNMP to enable it. See Section 14.1.6, “sFlowTrend-Pro is not receiving sFlow from a switch or host” and Section 14.1.7, “sFlowTrend-Pro cannot communicate with the switch using SNMP”.

- The agent is disabled and sFlowTrend-Pro is not receiving sFlow from it.

- A switch setting has been changed in the Configure agents dialog, but the change has not been deployed (operation pending). sFlowTrend-Pro will deploy the change when you click the OK button.

The tooltip for the status symbol gives more detail on the status of the agent.

**Type**

The type column displays the type of agent: whether it is a switch or a host:

- The agent is a switch or router.
- The agent is a host.
- The agent is both a switch/router and a host.

**DNS name**

The domain name obtained from the reverse DNS lookup of the SNMP IP address of the agent.

**SNMP IP address**

The IP address that sFlowTrend-Pro will use to communicate with the agent, if it is a switch, via SNMP to obtain the friendly system and interface names. This is also the IP address that sFlowTrend-Pro will use when using SNMP to configure the switch to send sFlow, if Configure via SNMP is selected.

**sFlow agent address**

The IP address that is used by the sFlow agent to uniquely identify itself. This address is learnt from the sFlow data and cannot be changed in sFlowTrend-Pro. For a switch, in many cases the sFlow agent address will be the same as the SNMP IP address. However if the switch is switching between multiple VLANs, the sFlow agent address may be in a VLAN that is not routable to the host that is running sFlowTrend-Pro. In which case you can edit the SNMP IP address field to tell sFlowTrend-Pro how to communicate with the switch.

**Use global SNMP settings**

For a switch, check this box if you would like sFlowTrend-Pro to use the global SNMP settings (see Section 13.5.2, “Configuring global SNMP settings”) when communicating with the switch using SNMP. If this box is not checked you can specify the SNMP settings for this switch by clicking on the button. sFlowTrend-Pro uses SNMP to query the switch for the systemGroup and ifTable, so that it can present friendly names for the switch and its interfaces. If sFlowTrend-Pro is to use SNMP to configure the switch to send sFlow, these settings must allow write access to the sFlow MIB.

**Configure sFlow via SNMP**

For a switch, check this checkbox if you would like sFlowTrend-Pro to use SNMP to configure the switch to send sFlow.
Enable
Check this checkbox if you would like sFlowTrend-Pro to receive and store data for this agent.

Edit
Although most of the commonly changed agent settings can be edited in the table, for a switch you can edit all the settings and view the detailed status of the switch by clicking on this button.

Delete
Delete the agent from the sFlowTrend-Pro and stop further data collection. If this agent has been configured by SNMP to send sFlow, sFlowTrend-Pro will disable sFlow before deleting the switch.

You can click with the left button on a column heading to sort the table by that column. You can also click with the Shift+left mouse button to add secondary sort columns.

Any changes made to agents and their settings will not be implemented until the OK button is clicked.

13.2.1. Adding a switch that is to be configured via SNMP

Clicking on the Add switch agent button launches a dialog that allows you to enter the details for a new switch. This should be used when you wish to tell sFlowTrend-Pro about a switch that should be configured via SNMP to send sFlow. Enter the following information:

SNMP IP address
The IP address that sFlowTrend-Pro should use when communicating with the switch via SNMP.

Use global SNMP settings
Check this box if you would like sFlowTrend-Pro to use the global SNMP settings (see Section 13.5.2, “Configuring global SNMP settings”). If this box is unchecked, you can click on Change SNMP settings to specify the SNMP settings specific to this switch. You can ask sFlowTrend-Pro to communicate with the switch using SNMP v2c or v3. Make sure that the SNMP settings that you enter will sFlowTrend-Pro write access to the sFlow MIB.

Enable
Check this box if you want sFlowTrend-Pro to enable and start collecting data from this switch. sFlowTrend allows data to be collected from only one switch, so if another switch is already enabled, the Enable checkbox will be inactive and you must disable the other switch before you can enable the new switch.

Configure sFlow via SNMP
Check this box if sFlowTrend-Pro is to use SNMP to configure the switch to send sFlow.

sFlowTrend-Pro will not configure the switch until the Configure agents dialog has been closed by clicking the OK button.

13.2.2. Importing and exporting agent configuration

The Configure agents dialog allows you to export configuration by selecting File → Export. The exported configuration is stored as XML.

You can import previously exported agent configuration, by selecting File → Import. If the imported configuration includes agents that are already present in the current configuration, then the imported configuration settings will overwrite the existing settings.
13.2.3. Verifying the switch configuration and status

Once you have submitted the changes that you have made in the Configure agents dialog, by clicking the OK button, when you go to the Charts, Interfaces, or Wireless tabs and select a switch, the sFlowTrend-Pro status bar (see Section 1.1, “Introducing sFlowTrend-Pro”) will show the status of the switch that is currently selected. The message in the status bar will give information on whether sFlowTrend-Pro can communicate with the selected switch using SNMP, has successfully used SNMP to configure the selected switch to send sFlow (if this option has been chosen), and whether sFlowTrend-Pro is receiving sFlow from the selected switch.

You can also view the status of a switch by selecting the Tools → Configure agents menu item to launch the Configure agents dialog and then viewing the tooltip for the colour coded switch status symbol or using the edit button to view the detailed status of a switch (see above).

The status message will also indicate if there is a problem with the configuration, for example:

No SNMP
sFlowTrend-Pro cannot communicate with the switch using SNMP. Verify that the sFlowTrend-Pro is using the correct SNMP settings and that there are no firewalls in the network or on the host that are blocking SNMP. See Section 14.1.7, “sFlowTrend-Pro cannot communicate with the switch using SNMP” for troubleshooting tips.

Cannot configure sFlow with SNMP - SNMP write access denied
sFlowTrend-Pro is not using the correct SNMP settings that allow write access to the sFlow MIB or the switch is not configured to allow SNMP set from the system running sFlowTrend-Pro.

Cannot configure sFlow with SNMP - no sFlow MIB
The switch cannot be configured via SNMP to send sFlow. Instead, you must use the switch CLI to configure sFlow (see Appendix A, Configuring switches to send sFlow).

Already in use
Another application has already configured this switch to send sFlow and there are no additional resources to send sFlow to sFlowTrend-Pro as well. Disable the other application so that the switch can be configured by sFlowTrend-Pro. You can identify the other applications which have already configured the switch by using the edit button. The Additional switch details section, under Other owners lists the IP addresses of the other systems which have configured the switch, together with a description of the application. Alternatively, you can configure sFlowTrend-Pro so that it removes the other application's claim on the switch and replaces it with its own (see Section 15.1, “Custom configuration”, sflowtrend.useForce).

13.3. Configuring subnets in sFlowTrend-Pro

Select the Tools → Configure subnets menu item to launch the Configure subnets dialog. This dialog allows you to tell sFlowTrend-Pro about how end host IP addresses should be grouped together. Grouping end host addresses allows you to understand traffic patterns better. For example, identifying end host addresses for each department, allows you to view traffic between departments; understanding network traffic in this way, allows you to make accurate capacity planning decisions and help enforce usage policies.

sFlowTrend-Pro uses Classless Inter-domain Routing (CIDR) as the method to define groups of addresses. In CIDR notation a group of IP addresses is defined using a network (IP) address and a number of mask
Configuration

bits indicating the number of significant bits from the address that will be shared by members of the group. For example, the CIDR 10.1.4.0/24 will group all the addresses that share the 10.1.4 prefix; ie all the addresses that exist on the 10.1.4.0/255.255.255.0 subnet. sFlowTrend-Pro supports the CIDR notation for grouping IPv4 and IPv6 addresses.

To illustrate CIDR priorities, consider the an IP address, 10.1.4.1. Suppose that two CIDRs are defined, 10.1.4.0/24 and 10.0.0.0/8. The IP address is contained in both of these CIDRs, but the CIDR 10.1.4.0/24 is a more specific group of addresses and so will have priority over the 10.0.0.0/8 CIDR.

CIDRs provide a very efficient means of specifying address groups. The goal is not to reflect every detailed subnet in the network, but to use CIDRs to describe the overall subnetting policy for the site.

The following example gives a typical subnet configuration:

<table>
<thead>
<tr>
<th>Subnet name</th>
<th>Address</th>
<th>Mask bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Centre</td>
<td>10.1.5.0</td>
<td>24</td>
</tr>
<tr>
<td>DMZ</td>
<td>10.1.4.0</td>
<td>24</td>
</tr>
<tr>
<td>Edinburgh</td>
<td>10.1.2.0</td>
<td>24</td>
</tr>
<tr>
<td>Multicast</td>
<td>224.0.0.0</td>
<td>4</td>
</tr>
<tr>
<td>Private</td>
<td>192.168.0.0</td>
<td>16</td>
</tr>
<tr>
<td>San Francisco</td>
<td>10.0.0.0</td>
<td>24</td>
</tr>
<tr>
<td>Unassigned</td>
<td>10.0.0.0</td>
<td>8</td>
</tr>
<tr>
<td>Web Servers</td>
<td>64.151.76.0</td>
<td>24</td>
</tr>
</tbody>
</table>

In this example we have added a special subnet for Multicast. We have also added a "catch all" subnet, called "Unassigned". Remember that an address will be assigned to the most specific CIDR, so the only addresses that will be shown in the Unassigned subnet will be local addresses that don't belong in any of the other subnets. Configuring a "catch all" subnet in this way, allows you to distinguish between internal and external addresses.

Configure subnets dialog allows you to add new subnets and edit and delete existing subnets. To edit an existing subnet, click on the edit symbol, for the row representing the subnet. To delete an existing subnet, click on the delete symbol, for the row representing the subnet. The dialog will prevent you from adding or editing subnets if the add or edit would result in duplicate names or CIDRs.

13.4. Configuring action on events in sFlowTrend-Pro

Select the Tools → Configure events menu item to launch the Configure action on events dialog. This dialog allows you to configure automatic actions when sFlowTrend-Pro raises an event.
The Configure action on events dialog allows you to add new actions by clicking on the Add action button and edit an existing action, by clicking on the edit symbol. When you add or edit an action the Edit action on event dialog is displayed. This dialog allows you to specify a specific action when certain event criteria are met.

To configure the event criteria, first select an event Type. You can select All, Threshold or System event types. Once you have selected an event type, you can then select other criteria specific to that type. For all event types, you can select the event Severity when an action will be performed. For the Threshold event type you can select additional event criteria, specific to threshold events.

To configure the action to be taken when event criteria are met, select an Action type. When you select the Email action, events meeting the criteria will be sent in an email to the Recipients that you specify. You can specify a number of email recipients by entering a comma separated list of email addresses. For sFlowTrend-Pro to be able to send events via email, you must first configure the email SMTP server (see Section 13.5.5, “Email”). When you select the Syslog action, events meeting the criteria will be exported to the specified syslog server using the specified UDP Port to connect to the syslog server and the specified Facility to indicate the source of the event. sFlowTrend-Pro uses the event severity as the syslog message priority severity level indicator. See http://tools.ietf.org/html/rfc3164 for more information on syslog.

If sFlowTrend-Pro generates a large number of events, this will cause a large number of actions with matching criteria to be run. This may be inconvenient: for example, if a network suddenly became very...
busy, and you have an email action enabled for threshold events on all interfaces, then you would receive a very large number of email messages (one per interface exceeding the threshold). To minimise this, it is recommended that you configure event actions carefully, only selecting event criteria that are important to you. sFlowTrend-Pro will also try to minimise event action storms. If more than a predefined number of actions are queued for processing (eg email messages queued to be sent), then further actions of that type will be suppressed. An additional event will be logged informing you that event action suppression has taken place. Once the pending actions are processed, then new ones will again be accepted. This suppression threshold can be configured (see server custom configuration settings event.threshold.email and event.threshold.syslog).

13.5. Options

Select the Tools → Options menu item to customise various aspects of sFlowTrend-Pro. On an Apple Macintosh, the customisation dialog is accessed from by selecting Preferences from the application menu.

13.5.1. Setting the switch, interface, and host naming policy

Use the Tools → Options menu item, View tab, to tell sFlowTrend-Pro how you would like your switches and their interfaces to be displayed and whether end hosts are identified using IP addresses or DNS names.

13.5.1.1. Setting the switch naming policy

Switches can be displayed using one of the following options:

SNMP IP address
The IP address that sFlowTrend-Pro uses to communicate with the switch via SNMP

sFlow agent address
The IP address that is used by the sFlow agent on the switch to uniquely identify the switch.

DNS name
The domain name obtained from the reverse DNS lookup of the SNMP IP address of the switch. If the reverse DNS lookup fails, the SNMP IP address will be used instead.

sysName
The SNMP sysName obtained from the SNMP MIB. If sFlowTrend-Pro cannot communicate with the switch using SNMP (see Section 14.1.7, “sFlowTrend-Pro cannot communicate with the switch using SNMP”), then SNMP IP address will be used instead.

If the SNMP IP address or the sFlow agent address option is chosen, the switches will be listed in numerical order in the Switch selector in the Charts and Interfaces tabs. For other options, the switches will be listed in alpha-numeric order, even if an IP address is shown because the name is not available.

13.5.1.2. Setting the interface naming policy

Interfaces can be displayed using one of the following options:

ifIndex
The integer that the switch uses to uniquely identify the interface.

ifName
The friendly name assigned to the interface, identifying the card/slot. For example A1, ethernet1/1. If sFlowTrend-Pro cannot communicate with the switch using SNMP (see Section 14.1.7, “sFlowTrend-Pro cannot communicate with the switch using SNMP”), then the ifIndex will be used instead.
ifAlias

A string administratively assigned to the interface often giving useful information about its purpose. For example "Connection to servers". If sFlowTrend-Pro cannot communicate with the switch using SNMP (see Section 14.1.7, “sFlowTrend-Pro cannot communicate with the switch using SNMP”), or the ifAlias is not assigned, then ifIndex will be used instead.

If the ifIndex option is chosen, the interfaces will be listed in numerical order in the Interface selector in the Charts tab. For other options, the interfaces will be listed in alpha-numeric order, even if the ifIndex is shown because the name is not available.

13.5.1.3. Setting the host naming policy

In the Charts and Thresholds tabs, end hosts can be identified using IP addresses or DNS names. Check the Resolve IP addresses to hostname in charts checkbox to tell sFlowTrend-Pro to use DNS names instead of IP addresses.

13.5.2. Configuring global SNMP settings

Select the Tools → Options menu item, SNMP tab to configure the SNMP settings which will be used for all switches. These settings will be used when querying switches for the friendly names for the switches and interfaces. You can ask sFlowTrend-Pro to communicate with the switches using SNMP v2c or SNMP v3. If sFlowTrend-Pro is to use SNMP to configure the switches to send sFlow, then the SNMP settings must allow write access to the sFlow MIB, and the switch must allow the system running sFlowTrend-Pro write access.

These global settings can be explicitly overridden for a specific switch (see Section 13.2, “Configuring agents in sFlowTrend-Pro”).

When these global settings are changed, sFlowTrend-Pro will start using the new settings to communicate with switches that use the global settings.

13.5.3. Configuring advanced options

Select the Tools → Options menu item, Advanced tab to view and configure some less commonly used settings:

Restore warnings
Checking this checkbox will cause sFlowTrend-Pro to display warnings asking you to confirm actions, for example when deleting switches or when exiting sFlowTrend-Pro. When these warnings are shown, you can ask sFlowTrend-Pro not to show these warnings again. This checkbox can be used to restore the behaviour of showing warnings.

Show alerts on this client
Leaving this checkbox checked will display alerts about sFlowTrend-Pro, such as notification of software updates, on this client. If you clear the checkbox, you will not receive any notifications on this client. This may be useful if, for example, you are using sFlowTrend-Pro to display network status in a public area.

Report problems with sFlowTrend-Pro to InMon
Leaving this checkbox checked will allow sFlowTrend-Pro to send reports of software problems to InMon. We appreciate this feedback, and it helps us improve sFlowTrend-Pro. If you do not want problem reports to be sent, then clear this checkbox.
sFlowTrend home directory
Allows you to change the directory used by sFlowTrend-Pro for storing information. The directory is configured differently, depending on whether you are running sFlowTrend-Pro as an application, or as a service.

*AP* If you are running as an application, then the home directory is used to store traffic and log data, and custom configuration information. If you have enabled user authentication (see Section 13.6, “Configuring user authentication”), then only Administrators can change the home directory. If you change the home directory, all currently saved traffic data and custom configuration information will be lost. sFlowTrend-Pro must be restarted for the change to take effect.

*Ser* If you are running sFlowTrend-Pro as a service, then two home directories are shown in advanced settings: one for the client, and one for the server:

sFlowTrend-Pro home directory
This allows the home directory for the current client to be changed. The client home directory is used for log files, and any custom configuration that is applicable to the client. The client needs to be restarted for changes to the home directory to take effect.

sFlowTrend-Pro server home directory
Displays the home directory used by the server. The server home directory is used to store traffic and log data, and custom configuration information. This directory cannot be changed from within sFlowTrend-Pro; it is entered when installing sFlowTrend-Pro. To change the directory, you can reinstall sFlowTrend-Pro.

13.5.4. Proxy configuration

If a proxy server is required for connectivity to the Internet, this is configured by selecting the Tools → Options menu item, Proxies tab. If you are running sFlowTrend-Pro as a service, the proxy can be set for both the client and the server. When you are running as an application, then just one proxy can be set.

It is important to set the proxies if required. The server uses Internet connectivity to download the initial license and any subsequent updates (for example, if you renew the license), and the client uses the Internet to display product alerts.

The configuration available for the proxies is as follows:

Default system proxy
Sets the proxy to be the same as the system default. Note that the system default settings are not necessarily those defined in the browser that you use: on Windows, the system default settings are those configured in Settings → ControlPanel → Internet Options. In Linux under Gnome, the system default settings are those configured in System → Preferences → Internet and Network → Network Proxy.

No proxy
No proxy will be used.

Manual proxy configuration
Allows configuration of a proxy server only for sFlowTrend-Pro. The address of the proxy server and the TCP port used to communicate with it should be entered into the Http proxy and port fields, respectively.

If there are any hosts that do not require a proxy, you can enter the address of these hosts into the Do not proxy for hosts field. Multiple hosts can be entered here, separated by semicolons or commas, and wildcards can be used to represent a range of hosts (for example, "*.inmon.com").
Note

If you change the proxy configuration from No Proxy or Manual proxy to Default system proxy, or vice-versa, then you must restart the sFlowTrend-Pro client or service (depending on which proxy was changed) to make the change effective.

13.5.5. Email

sFlowTrend-Pro uses a Simple Mail Transfer Protocol (SMTP) server to send email notification of events. The SMTP server receives messages from sFlowTrend-Pro and forwards them to their destination. The following SMTP server settings must be configured:

SMTP server
The hostname or IP address of the server that will receive messages from sFlowTrend-Pro for forwarding to their destinations (email recipients).

Port
The TCP port on the SMTP server that sFlowTrend-Pro connects to to send email for forwarding.

Sender
The full name of the user (for example sFlowTrend) that will be shown as the sender of emails sent by sFlowTrend-Pro

Address
The email address to be used as the From address in emails sent by sFlowTrend-Pro

Use authentication
Select authentication if your SMTP server will only receive and forward email from authenticated senders. If you select use authentication, then you must also enter the Username and Password that can be used to authenticate sFlowTrend-Pro as a valid sender.

Encryption
The email encryption method (None, TLS, SSL).

You can test the SMTP server configuration by clicking Test configuration. An email will be sent to the sender email address that you have entered. If the configuration fails, sFlowTrend-Pro will show an error message.

13.5.6. Advanced sFlow

Select the Tools → Options menu item, Advanced sFlow tab to view and configure some less commonly used sFlow related settings:

sFlow collector address
This selection list allows you to select the network interface and associated IP address on the system running sFlowTrend-Pro that will be used to receive sFlow. If you are using a CLI to configure sFlow on your switches, make sure that you use the selected IP address as the destination or collector address for sFlow when you configure the switch (see Appendix A, Configuring switches to send sFlow).

sFlow UDP port
This allows you to change the UDP port that sFlowTrend-Pro will listen on to receive sFlow. If you are using a CLI to configure sFlow on your switches, make sure that you configure the switch to send sFlow to this UDP port (see Appendix A, Configuring switches to send sFlow).
13.6. Configuring user authentication

You can control which users have access to sFlowTrend-Pro by using the user authentication feature of sFlowTrend-Pro. User authentication is configured via the Tools → Manage users menu item, which launches the Manage users dialog. This dialog contains a table which lists all the configured users and allows you to add users, change the password and role for a user, and delete users.

By default, there are no users configured in sFlowTrend-Pro and user authentication is disabled. This means that any user can use sFlowTrend-Pro and will have all the permissions associated with the Administrator role. If you are connecting to a remote server with user authentication disabled, the User name and Password fields in the Connection dialog (see Section 12.3, “Connecting to a server”) can be left blank and will be ignored.

Once you have added at least one user, user authentication is enabled and any user wishing to run sFlowTrend-Pro as an application or connect to the server, must login with a configured user login name and password.

13.6.1. Adding a user

Clicking on the Add user button, launches a dialog that allows you to enter the details for a new user:

User
The full name for the user.

Login
The user login name for the user.

Password
The password for the user. You must enter the same password in the Confirm password field.

Role
The role that the user should be assigned. sFlowTrend-Pro includes three roles:

Guest
Users with this role can access the traffic data.

User
Users with this role can access the traffic data and change their own password.

Administrator
Users with this role can access all the traffic data, configure switches in sFlowTrend-Pro (see Section 13.2, “Configuring agents in sFlowTrend-Pro”), manage users, playback saved sFlow data (see File → Start playback), and change sFlow related settings (see Section 13.5.6, “Advanced sFlow”).

Note
If you decide to enable user authentication, then you must always configure at least one user who is an Administrator. This means that the first user that you add, must be an Administrator.

In addition if you use the edit button to edit a user, or the delete button to delete a user, the user interface will enforce maintaining at least one Administrator. This means that you will be prevented from deleting the last user.
After having configured user authentication, if you decide to allow uncontrolled user access, you can do so by deleting the file `users.prp` in the sFlowTrend-Pro server home directory (or the sFlowTrend-Pro home directory).
Chapter 14. Troubleshooting and frequently asked questions

14.1. Troubleshooting sFlowTrend-Pro

14.1.1. Installation problems

14.1.1.1. When I try to install sFlowTrend-Pro, my browser asks me what to do

When everything is configured correctly, Java Web Start should automatically install sFlowTrend-Pro. However, sometimes the browser is not aware of Java Web Start. In this case, you have to tell it manually to run the Java Web Start program. This is called javaws. You may need to browse to the location of javaws - on Microsoft Windows, it should be installed in C:\Program Files\Java\jre1.6.0_06\bin (note the path may vary depending on the specific version of Java installed).

14.1.1.2. When I try to install sFlowTrend-Pro, my browser displays a page of text instead of installing the program

When Java Web Start is installed correctly, it should automatically be launched from the browser. If the browser displays a text (xml) file instead, then right-click on the link, select save link as or save target as, and save the file as sFlowTrend.jnlp.

Then, try double-clicking on the saved file. If this still doesn't work, then open a command prompt window, and run javaws sFlowTrend.jnlp (you will need to make sure that sFlowTrend.jnlp is in the current directory).

14.1.1.3. sFlowTrend-Pro requires the Java Run-time Environment (JRE) v6.0, and Java Web Start

sFlowTrend-Pro is written in Java, and needs a minimum of Java v6.0. Java must be installed before installing sFlowTrend-Pro. Also, in the case of other installation problems, it is often easiest just to re-install the Java JRE.

The JRE is available from www.java.com [http://www.java.com]

14.1.1.4. Java Web Start is not working correctly on Linux

There can be some problems with running Java Web Start on Linux. If you experience any problems, then these are some issues to be aware of:

• With Java 6.0, Java Web Start (and the Java Control Panel) require old C++ libraries to run. If, when trying to start sFlowTrend-Pro, you get an error message indicating that the application could not be started, try the "more details" button. If somewhere in the details it mentions that the system could not find the file libstdc++.so.5, or something similar, then this is likely to be the problem. To resolve this, you will need to install the older, compatibility C++ libraries. On Fedora, install the rpm compat-libstdc++-33; other Linux distributions should have a similar compatibility library available. Note that this issue does not exist with Java 5.0.
• Java for 64-bit Linux still does not include Java Web Start. Until this available, the best approach is to install an appropriate 32-bit JRE on the system, and then associating the file extension ".jnlp" in your browser with the javaws program located in the 32-bit JRE.

• GNU Java may be installed on your Linux system. Unfortunately, this does not currently include Java Web Start, and so you will need to install Oracle Java. This can be installed from [http://www.java.com](http://www.java.com). Similarly, there are problems with the OpenJDK Java Web Start, so you must install Oracle Java.

14.1.2. No switches are listed in the Switch selector

If there are no switches listed in the Switch selector in the Network and Threshold tabs, all the charts in the Dashboard tab show Waiting for first data point and the Activity LED is not flashing then sFlowTrend-Pro is not receiving sFlow data. The Status bar should also show Configure switches/routers to monitor.

You must first configure your switches to send sFlow, see Appendix A, Configuring switches to send sFlow. If there are still no switches listed see Section 14.1.6, “sFlowTrend-Pro is not receiving sFlow from a switch or host”.

14.1.3. When I select a switch in the Network, Top N tab, the chart is blank

If you select a switch using the Switch selector in the Network Top N tab and a blank screen is displayed, sFlowTrend-Pro has not received sFlow data that matches the criteria specified by the current settings in the Top N tab.

• If the Interface selector is also empty, sFlowTrend-Pro is not receiving sFlow data from the switch. First ensure that the selected switch is enabled (see Section 3.5, “Selecting a switch”. If the switch is enabled see Section 14.1.6, “sFlowTrend-Pro is not receiving sFlow from a switch or host”.

• If there are interfaces listed in the Interface selector, sFlowTrend-Pro has received sFlow data from the switch, but possibly not for the combination of the currently selected interface, chart, time, and filter. First make sure that the selected switch is enabled so that button is showing next to the Switch selector and that the Status bar indicates that the switch is not disabled. Then change the settings in the control bar as follows:

  • Charts: Top sources

  • Interfaces: All (this selection is only available if you are viewing a top N traffic trend chart).

  • Time: Last hour

  • Filter is disabled

For more information on settings in the Network tab see Chapter 3, Network.

Now wait for the Progress indicator to reach 100%.

If the Top sources chart is still not showing data, then sFlowTrend-Pro is not receiving sFlow from the switch, see Section 14.1.6, “sFlowTrend-Pro is not receiving sFlow from a switch or host”.

If you are now seeing data in the Top sources chart, sFlowTrend-Pro is receiving sFlow data from the switch. To understand which interfaces are reporting on traffic, change to the Interfaces tab and click on
the Unicasts/s column heading until the table is sorted so that rows are listed with the interface showing the highest unicasts/s listed first. If there are interfaces listed in table but there are no counter values, wait for the Progress indicator to reach 100% again (see Section 3.1, “Interfaces” for more information on the Interfaces tab). Then click on the chart button associated with first row. You will now be taken to the Counters tab with the interface with the most unicast/s selected.

14.1.4. When I select a switch in the Network Interfaces tab, the table is empty

If you select a switch using the Switch selector in the Network Interfaces tab and the table remains empty even after the Progress indicator has reached 100%, sFlowTrend-Pro is not receiving sFlow from that switch.

If Status bar message indicates that the switch is disabled, enable the switch by clicking on the click the button next to the Switch selector.

If the switch is enabled, then see Section 14.1.6, “sFlowTrend-Pro is not receiving sFlow from a switch or host”.

14.1.5. When I select a switch in the Network Interfaces tab, the table rows have no counter values.

If you select a switch using the Switch selector in the Network Interfaces tab and the table includes rows for the interfaces but the interface counter columns show ".-" even after the Progress indicator has reached 100%, twice, sFlowTrend-Pro is receiving sFlow from the switch but the sFlow data does not include interface counters. Check that the switch is configured to export interface counters (see Appendix A, Configuring switches to send sFlow).

14.1.6. sFlowTrend-Pro is not receiving sFlow from a switch or host

If the switch has been configured using the CLI to send sFlow, follow the steps below:

1. Ensure that the switch is using the correct IP address and UDP port used by the host running sFlowTrend-Pro. To view and configure the IP address and UDP port used by sFlowTrend-Pro see Section 13.5.3, “Configuring advanced options”.

2. Ensure that there are no host or network firewalls between the switch and sFlowTrend-Pro that are blocking the sFlow packets.

3. There may be insufficient traffic flowing through the switch for sFlow packets to be generated using the currently configured sampling rate. Try configuring the switch to sample more frequently. See Appendix C, Recommended sampling rates for recommended sampling rates.

If the host is running the sFlow agent, follow the steps below:

1. Ensure that the host is using the correct IP address and UDP port used by the host running sFlowTrend-Pro. To view and configure the IP address and UDP port used by sFlowTrend-Pro see Section 13.5.3, “Configuring advanced options”.

79
2. Ensure that there are no host or network firewalls between the host and sFlowTrend-Pro that are blocking the sFlow packets.

3. Check that the sFlow agent is running on the host. For more information on configuring the host agent, see Appendix B, Configuring hosts to send sFlow.

If sFlowTrend-Pro is to use SNMP to configure the switch to send sFlow, follow the steps below:

1. Make sure that the switch has been added to sFlowTrend-Pro, see Section 13.2.1, “Adding a switch that is to be configured via SNMP” and that the correct SNMP v2 or SNMP v3 settings, which allow write access to the sFlow MIB, have been specified. Some additional configuration of the switch may be necessary to allow it to accept SNMP sets from the host running sFlowTrend-Pro, for example, see Section A.1.1, “Configuring ProCurve switches to allow sFlow configuration via SNMP”.

2. Use Tools → Configure agents and view the status details for the switch either by moving the mouse over the status colour indicator to activate the tooltip or by clicking on the edit button. If the status indicates that the switch is not sending sFlow use the additional status message to identify the problem:

   No SNMP
   sFlowTrend-Pro cannot communicate with the switch using SNMP. Verify that the sFlowTrend-Pro is using the correct SNMP v2 or SNMP v3 settings and that there are no firewalls in the network or on the host that are blocking SNMP. See Section 14.1.7, “sFlowTrend-Pro cannot communicate with the switch using SNMP” for more diagnostics.

   Cannot configure sFlow with SNMP - SNMP write access denied
   sFlowTrend-Pro is not using the correct SNMP v2 read/write community or SNMP v3 settings or the switch is not configured to allow SNMP set from the system running sFlowTrend-Pro.

   Cannot configure sFlow with SNMP - no sFlow MIB
   The switch cannot be configured via SNMP to send sFlow. Instead, you must use the switch CLI to configure sFlow (see Appendix A, Configuring switches to send sFlow).

   Already in use
   Another application has already configured this switch to send sFlow and there are no additional resources to send sFlow to sFlowTrend-Pro as well. Disable the other application so that the switch can be configured by sFlowTrend-Pro. You can identify the other applications which have already configured the switch by using the edit button. The Additional switch details section, under Other owners lists the IP addresses of the other systems which have configured the switch, together with a description of the application. Alternatively, you can configure sFlowTrend-Pro so that it removes the other application’s claim on the switch and replaces it with its own (see Section 15.1, “Custom configuration”, sflowtrend.useForce).

3. If the status indicates that sFlow has been successfully configured, there may be insufficient traffic flowing through the switch for sFlow packets to be generated using the currently configured sampling rate. Try changing the sFlowTrend-Pro configuration so that the switch to is configured to sample more frequently (see Section 15.1, “Custom configuration”).

14.1.7. sFlowTrend-Pro cannot communicate with the switch using SNMP

If sFlowTrend-Pro cannot communicate with the switch using SNMP, the status bar shown when you go to the Network, sub-tabs and select a switch, will include No SNMP. In this case, sFlowTrend-Pro will be unable to display friendly names for the switch and its interfaces. It will also be unable to use SNMP
Troubleshooting and frequently asked questions

to configure the switch to send sFlow. Verify that the that the sFlowTrend-Pro is using the correct SNMP settings and that there are no firewalls in the network or on the host that are blocking SNMP.

More diagnostics are available by using Tools → Configure agents and viewing the status details for the switch either by moving the mouse over the status colour indicator to activate the tooltip or by clicking on the edit button. For example:

• Timed out indicates that the SNMP v2 community is incorrect or there are firewalls in the network or on the host blocking SNMP.

• Cannot decode response, Decryption failed, and User has no access privileges, indicate that the SNMP v3 settings being used by sFlowTrend-Pro do not match those configured on the switch. Check that the authentication and privacy passwords are correct, that the correct authentication protocol is being used and that the user has appropriate access privileges.

The sFlowTrend-Pro log file in the sFlowTrend-Pro server home directory (see Section 13.5.3, “Configuring advanced options”) may give additional details.

14.1.8. On-line help or email is not working

If on-line help isn't available in sFlowTrend-Pro (normally accessed from the Help menu item), then there is probably a problem with your Java installation. A similar issue can cause problems sending email on events, although other email configuration issues can also stop email being sent successfully.

The problem is caused by an obsolete version of the Java help or email system being installed outside of sFlowTrend-Pro. sFlowTrend-Pro includes its own version of the help and email system, but previously installed versions can override these, and if they are obsolete, then help and/or email will not work correctly.

The easiest way to resolve this is to uninstall the Java run-time environment, and then re-install it (obtainable from www.java.com [http://www.java.com]).

14.2. Frequently asked questions

This page contains answers to some frequently asked questions when running sFlowTrend-Pro.

14.2.1. After I select a switch to monitor, why does nothing happen?

sFlowTrend-Pro has an 'LED' at the bottom right of the window. This flashes green for every sFlow sample received. If it is not flashing, then no samples are being received. This can happen because no switch is configured to send sFlow, because there is insufficient network traffic on the switch to generate any sFlow, or because a firewall is blocking the sFlow data.

First, make sure that a switch is configured to send sFlow to sFlowTrend-Pro. With some switches, this can be done automatically, using sFlowTrend-Pro. Use the menu option Tools → Configure agents, and then Add switch agent. For other switches, sFlow must be configured through the switch's command line interface - refer to the manual for the switch. See also Section A.2, “Using the switch CLI to configure sFlow”.

If you think that sFlow is configured correctly, then try to ensure that sufficient network traffic is flowing through the switch. See Section 14.1.6, “sFlowTrend-Pro is not receiving sFlow from a switch or host”.

81
sFlow works by sending network packets to an sFlow collector, in this case sFlowTrend-Pro. The network packets are sent using UDP, on port 6343. If a firewall, either on the system running sFlowTrend-Pro or in the network, is blocking port 6343, then no sFlow data will reach sFlowTrend-Pro. Make sure that both the firewall on the system and all network firewall are allowing sFlow data through - see Section 14.2.4, “What firewall requirements does sFlowTrend-Pro have?” for more information.

14.2.2. When I start sFlowTrend-Pro, why do I get an error message "Cannot open UDP port 6343"?

This error message almost always means that another application is already using the default sFlow port, which is UDP 6343. A port can be used by only one application. If you try to run sFlowTrend-Pro more than once on the same system or another sFlow collector is already running on the same system, then you will see this error. Examples of other sFlow collectors are InMon Traffic Sentinel, a switch vendor's element manager, or one of the other sFlow applications available.

To find out which application is already using the sFlow port, follow these instructions:

- On Microsoft Windows, in a command prompt window, run the command:

  ```bash
  netstat -p udp -a -b
  ```

  This command takes a while to run. When it has completed, in the output look for a line like the following, containing 6343:

  ```
  UDP    PCNAME:6343         *:*                     2428
  [javaw.exe]
  ```

  This is saying that the program javaw.exe is using port 6343. Any Java application will appear as javaw.exe on Microsoft Windows, or if the application is not written in Java, then the name of the application will be shown. The number at the right (2428 in this case) is the process ID of the application.

- On Linux, from a terminal window, run the command:

  ```bash
  netstat -l -p -u | grep sflow
  ```

  This should produce a (long) line like:

  ```
  udp      0    0 *:sflow             *:*      26680/java
  ```

  The very last part of this line is telling us that the process with ID 26680 is running java, using port 6343. Again, if the application using the port is not written in Java, then the name of the program would be shown here.

  Once you have identified which application is using the sFlow port, you can decide which application to run at any one time, or you can change the port that sFlowTrend-Pro uses, by entering a new port number in the dialog.
Troubleshooting and frequently asked questions

Note

If you change the port that sFlowTrend-Pro uses and your switches are configured using SNMP to send sFlow; (see Section A.1, “Using SNMP to configure the switch to send sFlow”), sFlowTrend-Pro will automatically reconfigure your switches to send sFlow to the new port. However, if your switches are configured via the CLI to send sFlow and you change the port used by sFlowTrend-Pro, you must also manually reconfigure your switches to send sFlow to the new port (see Section A.2, “Using the switch CLI to configure sFlow”).

Occasionally, a host firewall can also cause this error message. If you could not find another program using the sFlow port, then refer to the section on firewalls: Section 14.2.4, “What firewall requirements does sFlowTrend-Pro have?”.

14.2.3. Why are most of the bars in a Top N chart coloured grey?

The grey part of a bar in a Top N chart indicates that the activity was from contributors not in the top N for the currently selected interval. See Section 3.3.3, “Understanding the Top N traffic chart” or Section 5.2.3, “Understanding the Top N services chart”.

14.2.4. What firewall requirements does sFlowTrend-Pro have?

sFlowTrend-Pro requires two network ports be available through all host or network firewalls between it and monitored switches, for the following purposes:

- Reception of sFlow data. Without sFlow connectivity, sFlowTrend-Pro will not show any data. By default, sFlow uses UDP port 6343 (this can be changed if required - see Section 13.5.6, “Advanced sFlow”). Only reception of sFlow traffic is required, sFlowTrend-Pro will never generate any sFlow traffic.

- SNMP connectivity between sFlowTrend-Pro and the monitored switches. This is strictly not required, but without it sFlowTrend-Pro will not be able to display friendly names for interfaces, and other similar features.

Also required is connectivity to a DNS server (to allow reverse IP address lookup), and http connectivity to the Internet (for license and product alert information; a proxy can be configured if required, and a license key manually entered if no Internet connectivity is available).

When running sFlowTrend-Pro as a service, the firewall configuration can be confusing. All of the requirements apply to the system which is running the service, and the client just requires http connectivity to allow it to receive product alerts. If the system running the service has a host firewall enabled, and the firewall can be configured differently for services or for specific users running a program, it is important that this configuration is correct. The firewall should allow the sFlowTrend-Pro service connectivity, and/or the configuration for the user that the sFlowTrend-Pro service is running under should allow the required connectivity. Under Windows, the service runs as user Administrator.
14.2.5. How do I change the time for which sFlowTrend-Pro stores data?

By default, sFlowTrend-Pro stores the last 7 days' of data. If required, this can be changed using the server custom configuration setting database.hoursPersistent.
Chapter 15. Advanced topics

This section contains information on advanced topics, which many users will not be concerned about.

15.1. Custom configuration

Some custom configuration is possible through the use of the sFlowTrend-Pro properties file. Modifying this is only recommended for advanced users. The file must be edited using a standard text editor, and sFlowTrend-Pro must be restarted before any of the changes will take effect.

If running sFlowTrend-Pro as a service, then both the client and the server have their own property files. Care must be taken to modify the appropriate one, depending on the desired outcome. The correct file to modify is indicated against each property, below. If the server property file needs to be modified, then this will affect all users using the server. The service must be restarted for the changes to take effect. If the client property file is modified, then this will only affect that client. In this case, the client must be closed and re-opened before the change will take effect.

The properties file is called `config.prp`, and it is located in the sFlowTrend-Pro home directory (which can be identified and changed through the sFlowTrend-Pro Tools → Options menu selection). If you are running sFlowTrend-Pro as a service, then take care to locate the correct client home directory, on the local system (the first shown via the Options menu), or the server home directory, on the remote server system (the second shown).

If the `config.prp` file does not exist in the directory, then it must first be created. The file is organised as a series of lines, where each line is of the form:

```
propertyName = value
```

For example,

```
chart.topn = 8
```

would change the number of entries in a top-n to 8. Note that all properties and values must be entered exactly as specified. Some of the properties that can be modified using the properties file are:

15.1.1. Client custom configuration settings

The settings in this section apply to the client. If you are running sFlowTrend-Pro as an application, then the client and server share the configuration file. If you are running as a service, then the file should be modified on the client only.

```
chart.font , chart.legend.font , chart.title.font , chart.subtitle.font
```

These settings control the fonts used for the charts displayed in the Charts tab. The format for these settings is one of:

```
fontname-style-pointsize
```
Advanced topics

fontname-pointsize
fontname-style
fontname

where style is case insensitive "PLAIN", "BOLD", "BOLDITALIC", or "ITALIC"; for example Arial-BOLD-11.

cart.topn
  Controls how many entries are displayed in each top-n chart (ie the value of n). The default value is 5.

circles.font , circles.legend.font , circles.title.font , circles.subtitle.font
  These settings control the fonts used for the Circles charts. The format for these settings is one of:

  fontname-style-pointsize
  fontname-pointsize
  fontname-style
  fontname

where style is case insensitive "PLAIN", "BOLD", "BOLDITALIC", or "ITALIC"; for example Arial-BOLD-11.

circles.maxFlows
  Controls the number of flows displayed in the Circles charts. The default value is 100.

client.lookAndFeel
  This setting controls the look and feel used for the sFlowTrend-Pro client. By default the Java system
  look and feel, which is most consistent with the operating system, look and feel is used. Alternative
  Java cross-platform look and feels are Nimbus and Metal (the look and feel used for earlier versions
  of sFlowTrend-Pro).

client.serverPort
  This setting controls the TCP port used by the client to connect to the server. It must match the
  server.webserver.port of the server you are connecting to (unless the port is changed in the
  connect dialog of the client - for more information, see Section 12.3, “Connecting to a server”). The
  default is 8087.

client.https.serverPort
  This setting controls the TCP port used by the client to connect to the server over https. It must match
  the server.webserver.https.port of the server you are connecting to. The default is 8443.

client.https.keyStore
  The Filename of client trusted certificate key store in sFlowTrend-Pro client home directory. The
  default is trustedCerts.

client.https.password
  The password for the client trusted certificate key store. The default is sflowtrend.

15.1.2. Server custom configuration settings

The settings in this section apply to the server. If you are running sFlowTrend-Pro as an application, then
the client and server share the configuration file. If you are running as a service, then the file should be
modified on the server only.
Advanced topics

**database.hoursPersistent**
- Controls how many hours of data will be stored in the database, before being flushed. This number can be reduced from the default of 168 (1 week), if the database is getting too large.

**event.threshold.email**
- Sets the number of queued email event actions when email suppression will be enabled. The default value is 3, and a value of 0 switches off suppression of event email messages.

**event.threshold.syslog**
- Sets the number of queued syslog event actions when syslog suppression will be enabled. The default value is 5, and a value of 0 switches off suppression of event syslog messages.

**sflowtrend.autoEnable**
- The default value for this setting is **true**. In this case, sFlowTrend-Pro will automatically enable and start collecting data from the first \( n \) switches that it receives unsolicited (command line configured) sFlow from, where \( n \) is the maximum number of switches allowed by the software license. To control manually which switches are enabled, set this value to **false**.

**sflowtrend.samplingRate.[ifSpeed.]medium**
- If sFlowTrend-Pro is using SNMP to configure the switches to send sFlow, sFlowTrend-Pro will use this value to configure the sampling rate for all interfaces of the given ifSpeed. The default values are:

  - `sflowtrend.samplingRate.medium = 512`
  - `sflowtrend.samplingRate.10.medium = 128`
  - `sflowtrend.samplingRate.100.medium = 256`
  - `sflowtrend.samplingRate.1000.medium = 512`
  - `sflowtrend.samplingRate.10000.medium = 1024`

  
  For example

  - `sflowtrend.samplingRate.100.medium = 256`

  tells sFlowTrend-Pro to configure all interfaces with an ifSpeed of 100 Mb/s with a sampling rate of 1 in 256. The value for `sflowtrend.samplingRate.medium` is used by sFlowTrend-Pro when configuring an interface with an ifSpeed for which a sampling rate has not been specified. For example, with the default sampling rate settings, a 4 Gb/s trunk would be configured with a sampling rate of 1 in 512.

  You can specify sampling rates for other ifSpeeds. For example

  - `sflowtrend.samplingRate.8000.medium = 1024`

  tells sFlowTrend-Pro to configure all interfaces, with an ifSpeed of 8 Gb/s, with a sampling rate of 1 in 1024.

**sflowtrend.useForce**
- The default value for this setting is **false**. In this case, if sFlowTrend-Pro is using SNMP to configure the switches to send sFlow, and finds that a switch has already been configured by another application and there are no unclaimed receiver entries on the switch, then sFlowTrend-Pro will not configure the switch. In this case sFlowTrend-Pro will show the switch status as **Already in use.** If the value for this
setting is true and there are no unclaimed receiver entries on the switch, then sFlowTrend-Pro will overwrite the first receiver entry forcibly claim it.

**server.webserver.port**

The TCP port that the server web server will listen on. This default value is 8087. If this is changed, then a client connecting to the server would also need to change to the same value (see client.serverPort).

**server.webserver.localonly**

By default, this setting is false, which means that the server web server can respond to requests from any client. If you want to disallow clients other than the system that is running the server from connecting to the server, then set this property to true.

**server.webserver.https.port**

The TCP port that the web server will use for https connections to clients. The default value is 8443. If this is changed, then a client connecting to the server would also need to change the corresponding setting (see client.https.serverPort).

**server.webserver.https.keyStore**

Filename of https key store in sFlowTrend home directory. The default value is httpsKeyStore.

**server.webserver.https.alias**

Alias of certificate for https in key store. The default value is sflowtrend.

**server.webserver.https.password**

Password for the key store. The default value is sflowtrend.

**server.webserver.https.keyPassword**

Password for the private key. If left blank or ommitted (default), then the password for the key store is used.

### 15.2. Customising protocol names

sFlowTrend-Pro comes with a built-in mapping from protocol numbers (eg TCP and UDP port) to names, to make charts and reports easier to understand. If you have any site-specific protocols that you would like to add, so that they show with the correct name for your network, then this can achieved by adding a protocol definitions file.

First, create a file called protocols.txt in the sFlowTrend-Pro server home directory (you can find this from the Tools → Options menu). Make sure that you create the file on the server, if you are running sFlowTrend-Pro as a service. Then add to the file the definitions required. The format of the file must be

```
[Section]
number, name
number, name
rangeStart-rangeEnd, name
number, name, longName
...

[Section]
number, name
number, name
...
```

Advanced topics
Each [Section] provides definitions for a specific type of protocol number. The sections that are currently allowed are show in Table 15.1, “Protocol definition sections”. Following the section definition, any number of definition lines can be entered. The definition lines start with the protocol number (in decimal), or optionally a range of numbers, followed by a comma then the name of the protocol. This can be optionally followed by an extended name, which is currently not used in sFlowTrend-Pro, but could be in the future.

Table 15.1, “Protocol definition sections” shows the sections than can be used, and provides an example of a definition line that might be in each section. Once you have created the file with the definitions that you require, or if you edit the file, the sFlowTrend-Pro service must be restarted for the change to take effect (or if you are running sFlowTrend-Pro as an application, just restart the application).

Table 15.1. Protocol definition sections

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Example definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ETHERNET]</td>
<td>Ethernet ethertype</td>
<td>2048, IPv4</td>
</tr>
<tr>
<td>[IEEE802]</td>
<td>IEEE 802.2 SAP</td>
<td>170, SNAP</td>
</tr>
<tr>
<td>[IP]</td>
<td>IP protocol number</td>
<td>17, UDP</td>
</tr>
<tr>
<td>[ICMP]</td>
<td>ICMP type</td>
<td>8, Echo</td>
</tr>
<tr>
<td>[TCP]</td>
<td>TCP port</td>
<td>80, http</td>
</tr>
<tr>
<td>[UDP]</td>
<td>The total of all non-error received frames</td>
<td>161, snmp</td>
</tr>
</tbody>
</table>

For example, this is an excerpt from the standard mapping that is included with sFlowTrend-Pro:

[IIEEE802]
2, Indiv LLC Sublayer Mgt
3, Group LLC Sublayer Mgt
4, SNA Path Control

[IP]
0, HOPOPT, IPv6 Hop-by-Hop Option
1, ICMP, Internet Control Message
2, IGMP, Internet Group Management
3, GGP, Gateway-to-Gateway
4, IP, IP in IP (encapsulation)
5, ST, Stream
6, TCP, Transmission Control

[TCP]
1, tcpmux, TCP Port Service Multiplexer
2, compressnet, Management Utility
3, compressnet, Compression Process
5, rje, Remote Job Entry
7, echo, Echo
9, discard, Discard
11, systat, Active Users
13, daytime, Daytime (RFC 867)
17, qotd, Quote of the Day
18, msp, Message Send Protocol
19, chargen, Character Generator
Advanced topics

20, ftp-data, File Transfer [Default Data]
21, ftp, File Transfer [Control]
22, ssh, SSH Remote Login Protocol
Chapter 16. Reference

16.1. Menu reference

This section contains a reference for each of the menu selections in sFlowTrend-Pro.

File → Start playback

sFlowTrend-Pro has the ability to read saved sFlow data from a file, as well as live from an sFlow switch. Start playback allows you to select the file and start playback. The main purpose for this feature is to allow demonstrations of the capability of sFlow. The file used for playback should contain sFlow datagrams in PCAP format (eg captured by wireshark or tcpdump). When the file is played back, the sFlow samples will be consumed by sFlowTrend-Pro in real time, not at the time the file was saved.

If you are running sFlowTrend-Pro remote client, sFlow data is sent to the remote server that you are connected to.

sFlowTrend-Pro can playback data from one file at a time, so this menu selection is only available if a playback has already been started. Use Stop playback to stop the current playback, before starting a playback from a different file.

File → Stop playback

Stop playback allows you to stop the currently running playback. This menu selection is not available if sFlowTrend-Pro is not currently playing back data from a file.

File → Import report

Brings up a file chooser dialog which allows you to select a previously saved report definition and import it into sFlowTrend-Pro The report definition will be imported into the Imported reports folder in the Reports tab.

File → Export selected report

This menu item will be active whenever a report is selected in the Reports tab. Export selected report brings up a dialog which allows you to select a directory and file in which to save the currently selected report. The exported report definition can then be transferred to another sFlowTrend-Pro installation or shared with other users.

File → Exit

Terminates sFlowTrend-Pro. If you are running sFlowTrend-Pro as an application, as well as closing the sFlowTrend-Pro window, this also stops collection of sFlow data; this includes attempting to disable the sending of sFlow from any switches that were configured via SNMP.

On an Apple Macintosh, select Quit sFlowTrend-Pro from the application menu, to terminate sFlowTrend-Pro

Tools → Configure agents

Brings up the Configure agents dialog, to allow switches to be added and removed from sFlowTrend-Pro, SNMP settings changed, etc. See Section 13.2, “Configuring agents in sFlowTrend-Pro”.

91
Tools → Configure subnets
Brings up the Configure subnets dialog, to allow end host IP addresses to be grouped together in subnets using CIDRs. Grouping IP addresses into subnets allows you to view traffic between groups of addresses easily. Section 13.3, “Configuring subnets in sFlowTrend-Pro”.

Tools → Configure events
Brings up the Configure action on events dialog, to allow action on events to be configured, example sending email notification of events. Section 13.4, “Configuring action on events in sFlowTrend-Pro”.

Tools → Change password
If you have logged in to sFlowTrend-Pro this menu item allows you to change your password.

Tools → Manage Users
Brings up the Manage users dialog which allows you to configure user authentication to control who can access sFlowTrend-Pro. Section 13.6, “Configuring user authentication”.

Tools → Options
Brings up the Options dialog, to allow sFlowTrend-Pro options to be changed. See Section 13.5, “Options”. On an Apple Macintosh the customisation dialog is accessed by selecting Preferences from the application menu.

Tools → Lookup host
Brings up the Lookup host dialog, which allows you to look up address, network location, and geographical location for end hosts. See Section 13.5, “Options”.

Navigate → Back
Allows you to navigate back through the history of previously viewed tabs in a similar way to the back button in a web browser. See Section 1.4, “Navigating around sFlowTrend-Pro using the history navigator”

Navigate → Forward
Allows you to navigate forward through the history of recently viewed tabs in a similar way to the forward button in a web browser. See Section 1.4, “Navigating around sFlowTrend-Pro using the history navigator”

Navigate → Add bookmark
Allows you to save a bookmark for the currently viewed tab and its settings, so that you can return to the same tab with these settings later. See also Section 1.4.1, “Bookmarking a tab and its settings”

Navigate → Show all bookmarks
Brings up a dialog which shows the currently saved bookmarks and allows you to view the settings saved in each bookmark, rename and rearrange bookmarks, and select a bookmarked tab and its settings that you now want to view. See also Section 1.4.2, “Organising bookmarks”

Navigate → Go to bookmark
Displays the currently saved bookmarks in a hierarchical menu. Select a bookmark from the menu to go to the bookmarked tab configured with the settings saved in the bookmark. See also Section 1.4.3, “Going to a previously bookmarked tab”

Help → Contents
Shows the contents of the on-line help in a new window.
Help on current view
Shows help for the current tab being viewed in sFlowTrend-Pro.

Point and click help
Changes the mouse cursor to a help pointer, and then allows you to click anywhere within the sFlowTrend-Pro window. Instead of the mouse click having its usual effect, context sensitive help will be displayed for the part of the window that was clicked.

About sFlowTrend-Pro
Shows information about sFlowTrend-Pro, including the version number. On an Apple Macintosh, About is located in the application menu.

Help on the web
Opens a web browser and views the sFlowTrend-Pro on-line help from the web.

sFlowTrend-Pro home page
Opens a web browser and views the sFlowTrend-Pro home page.

16.2. Database fields reference

This section contains a reference for each of the database fields. There are used in JavaScript filters, and in the select and sort statements in advanced reports.

Depending on which database table a query is being run over, different fields are available. The tables available are:

flows
contains flow data from network switches (both physical and virtual). Flow data contains details of traffic, such as source and destination addresses, ports, etc.

counters
contains counters data from network switches (both physical and virtual). Counters data contains volumetric data on traffic through interfaces, such as bytes, frames, errors, etc.

hostCounters
contains counters data from sFlow enabled hosts. This includes information such as CPU utilization, memory usage, etc, for each host.

services
contains detailed data from sFlow enabled services. This is analogous to flow data for network traffic. For example, if the apache web server has the sFlow monitoring module installed and enabled, then detail of HTTP transactions, such as URIs served, will be contained in this table.

serviceCounters
contains counter data for sFlow monitored services, such as http. This data is volumetric, such as the number of requests of each HTTP method.

The fields available are keys, values or time. Keys represent aspects of the traffic being analysed (eg a source address), while values are associated with that traffic (eg frames transmitted). Value fields can be used in a database sort statement, to sort the column in the resulting table (note that the same field must be in the select statement before it can be used in the sort statement). Additionally, there is one time field, which represents the time when traffic was observed.

The fields below are organised by database table, and by key, value and time.
16.2.1. Flows table fields

This section documents the fields available when a query is run over the flows table.

Table 16.1. Database key fields available for flows

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>A string representing the address of the sFlow agent where the traffic was observed</td>
<td></td>
</tr>
<tr>
<td>agent</td>
<td>sFlow agent IP address</td>
<td>string</td>
</tr>
<tr>
<td>IfIndex</td>
<td>An integer representing the ifIndex that the traffic was seen on</td>
<td>integer</td>
</tr>
<tr>
<td>inputIfIndex</td>
<td>switch input interface</td>
<td>integer</td>
</tr>
<tr>
<td>Qualified interface</td>
<td>A string representing the agent and ifIndex, separated by '&gt;'</td>
<td></td>
</tr>
<tr>
<td>inputInterface</td>
<td>qualified switch input interface</td>
<td>integer</td>
</tr>
<tr>
<td>outputInterface</td>
<td>qualified output interface</td>
<td>integer</td>
</tr>
<tr>
<td>clientInterface</td>
<td>qualified interface associated with the client</td>
<td>integer</td>
</tr>
<tr>
<td>serverInterface</td>
<td>interface associated with the server</td>
<td>integer</td>
</tr>
<tr>
<td>MAC address</td>
<td>A string representing a MAC address in hex</td>
<td></td>
</tr>
<tr>
<td>macSource</td>
<td>source MAC address</td>
<td>string</td>
</tr>
<tr>
<td>macDestination</td>
<td>destination MAC address</td>
<td>string</td>
</tr>
<tr>
<td>macClient</td>
<td>client MAC address</td>
<td>string</td>
</tr>
<tr>
<td>macServer</td>
<td>server MAC address</td>
<td>string</td>
</tr>
<tr>
<td>IP address</td>
<td>A string representing an IP address in numeric notation</td>
<td></td>
</tr>
<tr>
<td>ipSource</td>
<td>source IP address</td>
<td>string</td>
</tr>
<tr>
<td>ipDestination</td>
<td>destination IP address</td>
<td>string</td>
</tr>
<tr>
<td>ipClient</td>
<td>client IP address</td>
<td>string</td>
</tr>
<tr>
<td>ipServer</td>
<td>server IP address</td>
<td>string</td>
</tr>
<tr>
<td>Highest layer address available</td>
<td>A string representing the highest layer address available</td>
<td></td>
</tr>
<tr>
<td>sourceAddress</td>
<td>source address (IP if available, otherwise MAC)</td>
<td>string</td>
</tr>
<tr>
<td>destinationAddress</td>
<td>destination address (IP if available, otherwise MAC)</td>
<td>string</td>
</tr>
<tr>
<td>serverAddress</td>
<td>server address (IP if available, otherwise MAC)</td>
<td>string</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>clientAddress</td>
<td>client address (IP if available, otherwise MAC)</td>
<td>string</td>
</tr>
<tr>
<td>UDP port</td>
<td>An integer representing the UDP port, or 0 if not UDP</td>
<td></td>
</tr>
<tr>
<td>udpSourcePort</td>
<td>UDP source port</td>
<td>integer</td>
</tr>
<tr>
<td>udpDestinationPort</td>
<td>UDP destination port</td>
<td>integer</td>
</tr>
<tr>
<td>udpClientPort</td>
<td>UDP client port</td>
<td>integer</td>
</tr>
<tr>
<td>udpServerPort</td>
<td>UDP server port</td>
<td>integer</td>
</tr>
<tr>
<td>TCP port</td>
<td>An integer representing the TCP port, or 0 if not TCP</td>
<td></td>
</tr>
<tr>
<td>tcpSourcePort</td>
<td>TCP source port</td>
<td>integer</td>
</tr>
<tr>
<td>tcpDestinationPort</td>
<td>TCP destination port</td>
<td>integer</td>
</tr>
<tr>
<td>tcpClientPort</td>
<td>TCP client port</td>
<td>integer</td>
</tr>
<tr>
<td>tcpServerTCP</td>
<td>TCP server port</td>
<td>integer</td>
</tr>
<tr>
<td>Highest layer ‘port’ available</td>
<td>A string with the protocol and the highest layer port (including ethertype) available, separated by ‘:’</td>
<td></td>
</tr>
<tr>
<td>sourcePort</td>
<td>source port (L4 port, L3 protocol or L2 ethertype)</td>
<td>string</td>
</tr>
<tr>
<td>destinationPort</td>
<td>destination port (L4 port, L3 protocol or L2 ethertype)</td>
<td>string</td>
</tr>
<tr>
<td>clientPort</td>
<td>client port (L4 port, L3 protocol or L2 ethertype)</td>
<td>string</td>
</tr>
<tr>
<td>serverPort</td>
<td>server port (L4 port, L3 protocol or L2 ethertype)</td>
<td>string</td>
</tr>
<tr>
<td>VLAN</td>
<td>An integer representing the VLAN number (or 0, if no VLAN)</td>
<td></td>
</tr>
<tr>
<td>vlanSource</td>
<td>source VLAN</td>
<td>integer</td>
</tr>
<tr>
<td>vlanDestination</td>
<td>destination VLAN</td>
<td>integer</td>
</tr>
<tr>
<td>vlanClient</td>
<td>client VLAN</td>
<td>integer</td>
</tr>
<tr>
<td>vlanServer</td>
<td>server VLAN</td>
<td>integer</td>
</tr>
<tr>
<td>Priority</td>
<td>An integer representing the 802.1p priority</td>
<td></td>
</tr>
<tr>
<td>prioritySource</td>
<td>source (802.1p) priority</td>
<td>integer</td>
</tr>
<tr>
<td>priorityDestination</td>
<td>destination (802.1p) priority</td>
<td>integer</td>
</tr>
<tr>
<td>priorityClient</td>
<td>client (802.1p) priority</td>
<td>integer</td>
</tr>
<tr>
<td>priorityServer</td>
<td>server (802.1p) priority</td>
<td>integer</td>
</tr>
<tr>
<td>Other MAC attributes</td>
<td>Various other attributes of MAC traffic</td>
<td></td>
</tr>
<tr>
<td>ieee802SAP</td>
<td>IEEE 802 SAP</td>
<td>integer</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Other IP attributes</td>
<td>Various other attributes of IP (0 if non-IP traffic)</td>
<td></td>
</tr>
<tr>
<td>ipTOS</td>
<td>IP type of service (TOS)</td>
<td>integer</td>
</tr>
<tr>
<td>ipTTL</td>
<td>IP time to live (TTL)</td>
<td>integer</td>
</tr>
<tr>
<td>ipProtocol</td>
<td>layer 4 protocol (eg 6 for TCP, 17 for UDP)</td>
<td>integer</td>
</tr>
<tr>
<td>icmpType</td>
<td>ICMP type</td>
<td>integer</td>
</tr>
<tr>
<td>Frame type</td>
<td>Boolean tests for type of traffic</td>
<td></td>
</tr>
<tr>
<td>isUnicast</td>
<td>true if a unicast destination</td>
<td>boolean</td>
</tr>
<tr>
<td>isMulticast</td>
<td>true if a multicast destination</td>
<td>boolean</td>
</tr>
<tr>
<td>isL3Multicast</td>
<td>true if a layer 3 multicast destination</td>
<td>boolean</td>
</tr>
<tr>
<td>isBroadcast</td>
<td>true if a broadcast destination</td>
<td>boolean</td>
</tr>
<tr>
<td>Non-directional fields</td>
<td>Special non-directional fields for select statements only (these fields cannot be used in filters)</td>
<td></td>
</tr>
<tr>
<td>inputOrOutputIfIndex</td>
<td>the input or output ifIndex</td>
<td>integer</td>
</tr>
<tr>
<td>inputOrOutputInterface</td>
<td>the input or output qualified interface</td>
<td>string</td>
</tr>
<tr>
<td>Routing information (not supported by all sFlow implementations)</td>
<td>If isRouted == true, then the other values will be valid</td>
<td></td>
</tr>
<tr>
<td>isRouted</td>
<td>true if this packet was routed</td>
<td>boolean</td>
</tr>
<tr>
<td>ipNextHopRouter</td>
<td>next hop address if this packet was routed</td>
<td>string</td>
</tr>
<tr>
<td>sourceMaskLength</td>
<td>number of bits in the source mask if this packet was routed</td>
<td>integer</td>
</tr>
<tr>
<td>destinationMaskLength</td>
<td>number of bits in the destination mask if this packet was routed</td>
<td>integer</td>
</tr>
<tr>
<td>NAT information (not supported by all sFlow implementations)</td>
<td>NAT devices can provide information on addresses and ports that are rewritten using NAT</td>
<td></td>
</tr>
<tr>
<td>destinationNATAddress</td>
<td>Destination address before NAT</td>
<td>string</td>
</tr>
<tr>
<td>sourceNATAddress</td>
<td>Source address before NAT</td>
<td>string</td>
</tr>
<tr>
<td>destinationNATPort</td>
<td>Destination port before NAT</td>
<td>integer</td>
</tr>
<tr>
<td>sourceNATPort</td>
<td>Source port before NAT</td>
<td>integer</td>
</tr>
<tr>
<td>Tunnel information (not supported by all sFlow implementations)</td>
<td>Additional information on tunneled traffic</td>
<td></td>
</tr>
<tr>
<td>egressVNI</td>
<td>Virtual Network Identifier used to identify the traffic on egress from the switch</td>
<td>integer</td>
</tr>
<tr>
<td><strong>Term</strong></td>
<td><strong>Description</strong></td>
<td><strong>Type</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>ingressVNI</td>
<td>Virtual Network Identifier used to identify the traffic on ingress to the switch</td>
<td>integer</td>
</tr>
<tr>
<td>bgpAS</td>
<td>The local Autonomous System number</td>
<td>integer</td>
</tr>
<tr>
<td>bgpNextHop</td>
<td>Next-hop router from BGP routed traffic</td>
<td>string</td>
</tr>
<tr>
<td>bgpSourceAS</td>
<td>Source Autonomous System number from BGP routed traffic</td>
<td>integer</td>
</tr>
<tr>
<td>bgpSourcePeerAS</td>
<td>Source peer Autonomous System number from BGP routed traffic</td>
<td>integer</td>
</tr>
<tr>
<td>bgpDestinationAS</td>
<td>Destination Autonomous System number from BGP routed traffic</td>
<td>integer</td>
</tr>
<tr>
<td>bgpDestinationPeerAS</td>
<td>Destination peer Autonomous System number from BGP routed traffic</td>
<td>integer</td>
</tr>
<tr>
<td>bgpDestinationASPath</td>
<td>The destination Autonomous System path from BGP routed traffic</td>
<td>string</td>
</tr>
<tr>
<td>bgpCommunities</td>
<td>Communities from BGP routed traffic</td>
<td>string</td>
</tr>
<tr>
<td>bgpLocalPref</td>
<td>LocalPref from BGP routed traffic</td>
<td>integer</td>
</tr>
<tr>
<td>isWireless</td>
<td>true if this packet was send on a wireless network</td>
<td>boolean</td>
</tr>
<tr>
<td>wifiFrameControl</td>
<td>802.11 frame control</td>
<td>integer</td>
</tr>
<tr>
<td>wifiReceiverAddress</td>
<td>802.11 receiver address</td>
<td>string</td>
</tr>
<tr>
<td>wifiTransmitterAddress</td>
<td>802.11 transmitter address</td>
<td>string</td>
</tr>
<tr>
<td>wifiCipher</td>
<td>802.11 cipher suite</td>
<td>integer</td>
</tr>
<tr>
<td>wifiCipherFormatted</td>
<td>802.11 cipher suite, formatted into the convention hex string form (OUI-OUI-OUI-Suite)</td>
<td>string</td>
</tr>
<tr>
<td>wifiCipherName</td>
<td>The name of the 802.11 cipher suite</td>
<td>string</td>
</tr>
<tr>
<td>wifiTxSSID</td>
<td>802.11 transmit SSID</td>
<td>string</td>
</tr>
<tr>
<td>wifiTxBSSID</td>
<td>802.11 transmit BSSID</td>
<td>string</td>
</tr>
<tr>
<td>wifiTxVersion</td>
<td>802.11 protocol transmitted</td>
<td>string</td>
</tr>
<tr>
<td>wifiTransmissions</td>
<td>802.11 number of transmissions</td>
<td>integer</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>wifiTxDuration</td>
<td>802.11 transmitted packet duration</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRetransmitDuration</td>
<td>802.11 retransmit duration</td>
<td>integer</td>
</tr>
<tr>
<td>wifiTxChannel</td>
<td>802.11 transmit channel</td>
<td>integer</td>
</tr>
<tr>
<td>wifiTxSpeed</td>
<td>802.11 transmit speed</td>
<td>integer</td>
</tr>
<tr>
<td>wifiTxPower</td>
<td>802.11 transmit RSNI</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRxSSID</td>
<td>802.11 receive SSID</td>
<td>string</td>
</tr>
<tr>
<td>wifiRxBSSID</td>
<td>802.11 receive BSSID</td>
<td>string</td>
</tr>
<tr>
<td>wifiRxVersion</td>
<td>802.11 protocol received</td>
<td>string</td>
</tr>
<tr>
<td>wifiRxChannel</td>
<td>802.11 receive channel</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRxSpeed</td>
<td>802.11 receive speed</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRSNI</td>
<td>802.11 RSNI</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRCPI</td>
<td>802.11 RCPI</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRxDuration</td>
<td>802.11 received packet duration</td>
<td>integer</td>
</tr>
</tbody>
</table>

Non-directional wireless fields

Special non-directional fields for select statements only (these fields cannot be used in filters)

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>wifiVersion</td>
<td>802.11 protocol for transmit or receive</td>
<td>string</td>
</tr>
<tr>
<td>wifiSpeed</td>
<td>802.11 speed for transmit or receive</td>
<td>integer</td>
</tr>
<tr>
<td>wifiSSID</td>
<td>802.11 SSID for transmit or receive</td>
<td>string</td>
</tr>
<tr>
<td>wifiBSSID</td>
<td>802.11 BSSID for transmit or receive</td>
<td>string</td>
</tr>
<tr>
<td>wifiDuration</td>
<td>802.11 duration for transmit or receive</td>
<td>integer</td>
</tr>
<tr>
<td>wifiChannel</td>
<td>802.11 channel for transmit or receive</td>
<td>integer</td>
</tr>
</tbody>
</table>

**Table 16.2. Database value fields available for flows**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>Traffic byte count</td>
<td></td>
</tr>
<tr>
<td>bytesFromServer</td>
<td>Bytes sent from the server</td>
<td>integer</td>
</tr>
<tr>
<td>bytesToServer</td>
<td>Bytes sent to the server</td>
<td>integer</td>
</tr>
<tr>
<td>bytesIn</td>
<td>Bytes received.</td>
<td>integer</td>
</tr>
<tr>
<td>bytesOut</td>
<td>Bytes sent.</td>
<td>integer</td>
</tr>
<tr>
<td>bytesTotal</td>
<td>Total number of bytes</td>
<td>integer</td>
</tr>
<tr>
<td>Frames</td>
<td>Traffic byte count</td>
<td></td>
</tr>
</tbody>
</table>

98
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>framesFromServer</td>
<td>Frames sent from the server</td>
<td>integer</td>
</tr>
<tr>
<td>framesToServer</td>
<td>Frames sent to the server</td>
<td>integer</td>
</tr>
<tr>
<td>framesIn</td>
<td>Frames received.</td>
<td>integer</td>
</tr>
<tr>
<td>framesOut</td>
<td>Frames sent.</td>
<td>integer</td>
</tr>
<tr>
<td>framesTotal</td>
<td>Total number of frames</td>
<td>integer</td>
</tr>
</tbody>
</table>

**TCP/IP flags**

Various statistics from TCP/IP flags

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>synCount</td>
<td>The number of TCP/IP packets with SYN set</td>
<td>integer</td>
</tr>
<tr>
<td>synAckCount</td>
<td>The number of TCP/IP packets with both SYN and ACK set</td>
<td>integer</td>
</tr>
</tbody>
</table>

**802.11 channel utilization**

Usage of the 802.11 channel by percent utilization

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>wifiAirUtilizationIn</td>
<td>Percent utilization of the receive channel</td>
<td>integer</td>
</tr>
<tr>
<td>wifiAirUtilizationOut</td>
<td>Percent utilization of the transmit channel</td>
<td>integer</td>
</tr>
<tr>
<td>wifiAirUtilizationTotal</td>
<td>Total utilization of the channel</td>
<td>integer</td>
</tr>
</tbody>
</table>

### 16.2.2. Counters table fields

This section documents the fields available when a query is run over the `counters` table.

**Table 16.3. Database key fields available for counters**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>A string representing the address of the sFlow agent where the traffic was observed</td>
<td></td>
</tr>
<tr>
<td>agent</td>
<td>sFlow agent IP address</td>
<td>string</td>
</tr>
<tr>
<td>IfIndex</td>
<td>An integer representing the ifIndex that the traffic was seen on</td>
<td></td>
</tr>
<tr>
<td>ifIndex</td>
<td>switch interface associated with the counters</td>
<td>integer</td>
</tr>
<tr>
<td>Qualified interface</td>
<td>A string representing the agent and ifIndex, separated by '&gt;'</td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>qualified switch interface associated with the counters</td>
<td>integer</td>
</tr>
</tbody>
</table>

**Table 16.4. Database value fields available for counters**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface counters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard interface counters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>framesIn</td>
<td>The total of all non-error received frames</td>
<td>integer</td>
</tr>
<tr>
<td>framesOut</td>
<td>The total of all non-error transmitted frames</td>
<td>integer</td>
</tr>
<tr>
<td>ifInBroadcasts</td>
<td>Number of received broadcast frames</td>
<td>integer</td>
</tr>
<tr>
<td>ifOutBroadcasts</td>
<td>Number of transmitted broadcast frames</td>
<td>integer</td>
</tr>
<tr>
<td>ifInMulticasts</td>
<td>Number of received multicast frames</td>
<td>integer</td>
</tr>
<tr>
<td>ifOutMulticasts</td>
<td>Number of transmitted multicast frames</td>
<td>integer</td>
</tr>
<tr>
<td>ifInUcasts</td>
<td>Number of received unicast frames</td>
<td>integer</td>
</tr>
<tr>
<td>ifOutUcasts</td>
<td>Number of transmitted unicast frames</td>
<td>integer</td>
</tr>
<tr>
<td>ifInOctets</td>
<td>Number of received bytes</td>
<td>integer</td>
</tr>
<tr>
<td>ifOutOctets</td>
<td>Number of transmitted bytes</td>
<td>integer</td>
</tr>
<tr>
<td>ifInErrors</td>
<td>Number of received errors</td>
<td>integer</td>
</tr>
<tr>
<td>ifOutErrors</td>
<td>Number of transmitted errors</td>
<td>integer</td>
</tr>
<tr>
<td>ifInDiscards</td>
<td>Number of received discards</td>
<td>integer</td>
</tr>
<tr>
<td>ifOutDiscards</td>
<td>Number of transmitted discards</td>
<td>integer</td>
</tr>
<tr>
<td>ifInErrorsAndDiscards</td>
<td>The total of received errors and discards</td>
<td>integer</td>
</tr>
<tr>
<td>ifOutErrorsAndDiscards</td>
<td>The total of transmitted errors and discards</td>
<td>integer</td>
</tr>
<tr>
<td>utilizationIn</td>
<td>The ingress utilization</td>
<td>integer</td>
</tr>
<tr>
<td>utilizationOut</td>
<td>The egress utilization</td>
<td>integer</td>
</tr>
</tbody>
</table>

Interface status

Standard interface status

<table>
<thead>
<tr>
<th>ifStatus</th>
<th>Bit 0: ifAdminStatus, bit 1: ifOperStatus</th>
<th>integer</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifType</td>
<td>The ifType (see IANAIfType)</td>
<td>integer</td>
</tr>
<tr>
<td>ifSpeed</td>
<td>The interface speed in bits/second</td>
<td>integer</td>
</tr>
<tr>
<td>ifDirection</td>
<td>0 = unknown, 1 = full-duplex, 2 = half-duplex, 3 = in, 4 = out</td>
<td>integer</td>
</tr>
<tr>
<td>ifPromiscuousMode</td>
<td>Interface promiscuous mode</td>
<td>integer</td>
</tr>
<tr>
<td>ifUnknownProtos</td>
<td>Count of unknown protocols</td>
<td>integer</td>
</tr>
</tbody>
</table>

Basic wireless counters

Basic wireless counters (not supported by all sFlow implementations)
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>wifiAssociated</td>
<td>Number of associated stations</td>
<td>integer</td>
</tr>
<tr>
<td>wifiTxFragments</td>
<td>Number of transmitted fragments</td>
<td>integer</td>
</tr>
<tr>
<td>wifiTxFrames</td>
<td>Number of transmitted frames</td>
<td>integer</td>
</tr>
<tr>
<td>wifiTxMulticasts</td>
<td>Number of transmitted multicast frames</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRxFragments</td>
<td>Number of received fragments</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRxMulticasts</td>
<td>Number of received multicast frames</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRetries</td>
<td>Number of retried frames</td>
<td>integer</td>
</tr>
<tr>
<td>wifiMultiRetries</td>
<td>Number of multiple retries</td>
<td>integer</td>
</tr>
<tr>
<td>wifiFailures</td>
<td>Number of failed frames</td>
<td>integer</td>
</tr>
<tr>
<td>wifiAckFailures</td>
<td>Number of acknowledgement failures</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRTSFailures</td>
<td>Number of RTS failures</td>
<td>integer</td>
</tr>
<tr>
<td>wifiRTSSuccesses</td>
<td>Number of RTS successes</td>
<td>integer</td>
</tr>
<tr>
<td>wifiFCSErrors</td>
<td>Number of FCS errors</td>
<td>integer</td>
</tr>
<tr>
<td>wifiDuplicates</td>
<td>Number of duplicate frames</td>
<td>integer</td>
</tr>
<tr>
<td>wifiWEPUndecryptable</td>
<td>Number of undecryptable frames</td>
<td>integer</td>
</tr>
</tbody>
</table>

**Time-based wireless counters**

Channel time wireless counters (not supported by all sFlow implementations)

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>wifiElapsedTime</td>
<td>Total elapsed time in ms</td>
<td>integer</td>
</tr>
<tr>
<td>wifiOnChannelTime</td>
<td>Total time spent on channel in ms</td>
<td>integer</td>
</tr>
<tr>
<td>wifiOnChannelBusyTime</td>
<td>Busy time spent on channel in ms</td>
<td>integer</td>
</tr>
</tbody>
</table>

**QoS wireless counters**

Quality of service wireless counters (not supported by all sFlow implementations)

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>wifiQoSCFRx</td>
<td>Number of CF frames received</td>
<td>integer</td>
</tr>
<tr>
<td>wifiQoSCFLost</td>
<td>Number of CF frames lost</td>
<td>integer</td>
</tr>
<tr>
<td>wifiQoSCFUnusable</td>
<td>Number of CF frames unusable</td>
<td>integer</td>
</tr>
<tr>
<td>wifiQoSCFUnused</td>
<td>Number of CF frames unused</td>
<td>integer</td>
</tr>
<tr>
<td>wifiQoSDiscards</td>
<td>Number of discarded frames</td>
<td>integer</td>
</tr>
</tbody>
</table>

### 16.2.3. Host counters table fields

This section documents the fields available when a query is run over the hostCounters table.

**Table 16.5. Database key fields available for host counters**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>A string representing the address of the sFlow agent for the host</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>agent</td>
<td>sFlow agent IP address</td>
<td>string</td>
</tr>
<tr>
<td>Datasource</td>
<td>A String representing the sFlow datasource for the host</td>
<td></td>
</tr>
<tr>
<td>datasource</td>
<td>sFlow datasource for the host</td>
<td>string</td>
</tr>
<tr>
<td>parent</td>
<td>The sFlow datasource for the parent of this host</td>
<td>string</td>
</tr>
<tr>
<td>System identity</td>
<td>Information on the identity of the host</td>
<td></td>
</tr>
<tr>
<td>hostname</td>
<td>The host's hostname</td>
<td>string</td>
</tr>
<tr>
<td>System information</td>
<td>Information about the system and OS</td>
<td></td>
</tr>
<tr>
<td>machineType</td>
<td>The architecture of the system</td>
<td>string</td>
</tr>
<tr>
<td>osName</td>
<td>The name of the OS running on the host</td>
<td>string</td>
</tr>
<tr>
<td>osRelease</td>
<td>The release version string of the OS running on the host</td>
<td>string</td>
</tr>
<tr>
<td>Virtual information</td>
<td>Boolean test for virtual hosts</td>
<td></td>
</tr>
<tr>
<td>isVirtual</td>
<td>true if the host is a virtual host</td>
<td>boolean</td>
</tr>
</tbody>
</table>

### Table 16.6. Database value fields available for host counters

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host CPU counters</td>
<td>Host CPU performance counters expressed as an absolute value</td>
<td></td>
</tr>
<tr>
<td>cpuIdle</td>
<td>Idle CPU time in ms</td>
<td>integer</td>
</tr>
<tr>
<td>cpuIntr</td>
<td>Time in ms servicing interrupts</td>
<td>integer</td>
</tr>
<tr>
<td>cpuNice</td>
<td>Nice CPU time in ms</td>
<td>integer</td>
</tr>
<tr>
<td>cpuSoftIntr</td>
<td>Time in ms servicing soft interrupts</td>
<td>integer</td>
</tr>
<tr>
<td>cpuSystem</td>
<td>System CPU time in ms</td>
<td>integer</td>
</tr>
<tr>
<td>cpuTotal</td>
<td>Total CPU time available in ms (the sum of all of the other CPU time fields, including idle)</td>
<td>integer</td>
</tr>
<tr>
<td>cpuUser</td>
<td>User CPU time in ms</td>
<td>integer</td>
</tr>
<tr>
<td>cpuWIO</td>
<td>Time in ms waiting for I/O to complete</td>
<td>integer</td>
</tr>
<tr>
<td>vCpuTime</td>
<td>Virtual CPU time in ms</td>
<td>integer</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>cpuNum</td>
<td>Number of CPUs in the system</td>
<td>integer</td>
</tr>
<tr>
<td>vCpuNum</td>
<td>Number of virtual CPUs assigned to system</td>
<td>integer</td>
</tr>
<tr>
<td>cpuSpeed</td>
<td>Speed in MHz of the CPU</td>
<td>integer</td>
</tr>
<tr>
<td>loadOne</td>
<td>One-minute load average</td>
<td>integer</td>
</tr>
<tr>
<td>loadFive</td>
<td>Five-minute load average</td>
<td>integer</td>
</tr>
<tr>
<td>loadFifteen</td>
<td>Fifteen-minute load average</td>
<td>integer</td>
</tr>
<tr>
<td>procRun</td>
<td>Total number of runnable processes</td>
<td>integer</td>
</tr>
<tr>
<td>procTotal</td>
<td>Total number of processes</td>
<td>integer</td>
</tr>
<tr>
<td>contexts</td>
<td>Count of context switches</td>
<td>integer</td>
</tr>
<tr>
<td>interrupts</td>
<td>Count of interrupts</td>
<td>integer</td>
</tr>
<tr>
<td>uptime</td>
<td>Seconds since the last reboot</td>
<td>integer</td>
</tr>
<tr>
<td>vNodeCpuNum</td>
<td>Number of physical CPUs in a virtualized host</td>
<td>integer</td>
</tr>
<tr>
<td>vNodeCpuSpeed</td>
<td>Expected speed of the physical CPUs in a virtualized host</td>
<td>integer</td>
</tr>
</tbody>
</table>

### Host CPU percentage counters

Host CPU performance counters expressed as a percentage of total CPU time

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpuIdleUtil</td>
<td>Percentage of idle CPU time</td>
<td>integer</td>
</tr>
<tr>
<td>cpuIntrUtil</td>
<td>Percentage of CPU time servicing interrupts</td>
<td>integer</td>
</tr>
<tr>
<td>cpuNiceUtil</td>
<td>Percentage of nice CPU time</td>
<td>integer</td>
</tr>
<tr>
<td>cpuSoftIntrUtil</td>
<td>Percentage of CPU time servicing soft interrupts</td>
<td>integer</td>
</tr>
<tr>
<td>cpuSystemUtil</td>
<td>Percentage of system CPU time</td>
<td>integer</td>
</tr>
<tr>
<td>cpuUserUtil</td>
<td>Percentage of user CPU time</td>
<td>integer</td>
</tr>
<tr>
<td>cpuUtil</td>
<td>Percentage of non-idle CPU time</td>
<td>integer</td>
</tr>
<tr>
<td>cpuWIOUtil</td>
<td>Percentage of CPU time waiting for I/O to complete</td>
<td>integer</td>
</tr>
<tr>
<td>vCpuTimeUtil</td>
<td>Percentage utilization of virtual CPU time</td>
<td>integer</td>
</tr>
</tbody>
</table>

### Host disk counters

Host disk counters expressed as an absolute value

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>diskFree</td>
<td>Free disk space in bytes</td>
<td>integer</td>
</tr>
<tr>
<td>diskTotal</td>
<td>Total disk size in bytes</td>
<td>integer</td>
</tr>
<tr>
<td>diskUsed</td>
<td>Total space used on disk</td>
<td>integer</td>
</tr>
<tr>
<td>diskReads</td>
<td>Number of read operations from disk</td>
<td>integer</td>
</tr>
<tr>
<td>bytesRead</td>
<td>Number of bytes read from disk</td>
<td>integer</td>
</tr>
<tr>
<td><strong>Term</strong></td>
<td><strong>Description</strong></td>
<td><strong>Type</strong></td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>readTime</td>
<td>Time in ms reading from disk</td>
<td>integer</td>
</tr>
<tr>
<td>diskWrites</td>
<td>Number of write operations completed to disk</td>
<td>integer</td>
</tr>
<tr>
<td>bytesWritten</td>
<td>Number of bytes written to disk</td>
<td>integer</td>
</tr>
<tr>
<td>writeTime</td>
<td>Time in ms writing to disk</td>
<td>integer</td>
</tr>
<tr>
<td>vDiskAlloc</td>
<td>Disk space allocated to virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vDiskAvail</td>
<td>Disk space available to virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vDiskCapacity</td>
<td>Capacity of disk for virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vDiskErrors</td>
<td>Number of virtual disk errors</td>
<td>integer</td>
</tr>
<tr>
<td>vDiskReadBytes</td>
<td>Number of bytes read by virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vDiskReadReqs</td>
<td>Number of read requests by virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vDiskWriteBytes</td>
<td>Number of bytes written by virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vDiskWriteReqs</td>
<td>Number of write requests by virtual system</td>
<td>integer</td>
</tr>
</tbody>
</table>

**Host disk percentage counters**
Host disk counters expressed as a percentage

<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Description</strong></th>
<th><strong>Type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>diskFreeUtil</td>
<td>Free disk space expressed as a percentage of total space</td>
<td>integer</td>
</tr>
<tr>
<td>diskUsedUtil</td>
<td>Used disk space expressed as a percentage of total space</td>
<td>integer</td>
</tr>
<tr>
<td>partitionMaxUsed</td>
<td>Utilization of the highest utilized partition expressed as a percentage</td>
<td>integer</td>
</tr>
<tr>
<td>vDiskAllocUtil</td>
<td>Disk space allocated to virtual system expressed as a percentage of capacity</td>
<td>integer</td>
</tr>
<tr>
<td>vDiskAvailUtil</td>
<td>Disk space available to virtual system expressed as a percentage of capacity</td>
<td>integer</td>
</tr>
</tbody>
</table>

**Host memory counters**
Host memory performance counters expressed as an absolute value

<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Description</strong></th>
<th><strong>Type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>memoryBuffers</td>
<td>Bytes of memory used for buffers</td>
<td>integer</td>
</tr>
<tr>
<td>memoryCache</td>
<td>Bytes of memory used for cache</td>
<td>integer</td>
</tr>
<tr>
<td>memoryFree</td>
<td>Free bytes of memory</td>
<td>integer</td>
</tr>
<tr>
<td>memoryShared</td>
<td>Shared bytes of memory</td>
<td>integer</td>
</tr>
<tr>
<td>memoryTotal</td>
<td>Total bytes of memory</td>
<td>integer</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>memoryUsed</td>
<td>Bytes of memory used (= memoryTotal-memoryFree-memoryShared-memoryBuffers-memoryCache)</td>
<td>integer</td>
</tr>
<tr>
<td>memoryUsedTotal</td>
<td>Total bytes of memory used (= memoryTotal-memoryFree)</td>
<td>integer</td>
</tr>
<tr>
<td>swapFree</td>
<td>Free bytes of swap space</td>
<td>integer</td>
</tr>
<tr>
<td>swapTotal</td>
<td>Total bytes of swap space</td>
<td>integer</td>
</tr>
<tr>
<td>swapUsed</td>
<td>Bytes of swap space used</td>
<td>integer</td>
</tr>
<tr>
<td>pageIn</td>
<td>Page in count</td>
<td>integer</td>
</tr>
<tr>
<td>pageOut</td>
<td>Page out count</td>
<td>integer</td>
</tr>
<tr>
<td>swapIn</td>
<td>Swap in count</td>
<td>integer</td>
</tr>
<tr>
<td>swapOut</td>
<td>Swap out count</td>
<td>integer</td>
</tr>
<tr>
<td>vMemory</td>
<td>Memory in bytes used by virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vMemoryFree</td>
<td>Free memory in bytes available to virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vMemoryMax</td>
<td>Maximum memory in bytes available to virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vNodeMemTotal</td>
<td>Total size of physical memory in bytes in a virtualized host</td>
<td>integer</td>
</tr>
<tr>
<td>vNodeMemUsed</td>
<td>Used physical memory in bytes in a virtualized host</td>
<td>integer</td>
</tr>
<tr>
<td>vNodeMemFree</td>
<td>Free physical memory in bytes in a virtualized host</td>
<td>integer</td>
</tr>
</tbody>
</table>

Host memory percentage counters
Host memory performance counters expressed as a percentage of total memory

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>memoryBuffersUtil</td>
<td>Percentage of memory used for buffers</td>
<td>integer</td>
</tr>
<tr>
<td>memoryCacheUtil</td>
<td>Percentage of memory used for cache</td>
<td>integer</td>
</tr>
<tr>
<td>memoryFreeUtil</td>
<td>Percentage of memory free</td>
<td>integer</td>
</tr>
<tr>
<td>memorySharedUtil</td>
<td>Percentage of memory shared</td>
<td>integer</td>
</tr>
<tr>
<td>memoryUsedUtil</td>
<td>Percentage of memory used (see memoryUsed)</td>
<td>integer</td>
</tr>
<tr>
<td>memoryUsedTotalUtil</td>
<td>Percentage of used total memory (see memoryUsedTotal)</td>
<td>integer</td>
</tr>
<tr>
<td>swapFreeUtil</td>
<td>Percentage of swap space free</td>
<td>integer</td>
</tr>
<tr>
<td>swapUsedUtil</td>
<td>Percentage of swap space used</td>
<td>integer</td>
</tr>
<tr>
<td>vMemoryUtil</td>
<td>Memory used by virtual system expressed as a percentage of the total available</td>
<td>integer</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>vMemoryFreeUtil</td>
<td>Free memory available to virtual system expressed as a percentage of the total available</td>
<td>integer</td>
</tr>
<tr>
<td>vNodeMemUsedUtil</td>
<td>Used physical memory in a virtualized host, expressed as a percentage of the total available</td>
<td>integer</td>
</tr>
<tr>
<td>vNodeMemFreeUtil</td>
<td>Free physical memory in a virtualized host, expressed as a percentage of the total available</td>
<td>integer</td>
</tr>
</tbody>
</table>

Host network counters

Host network performance counters

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostBytesIn</td>
<td>Bytes received by the host</td>
<td>integer</td>
</tr>
<tr>
<td>hostBytesOut</td>
<td>Bytes sent by the host</td>
<td>integer</td>
</tr>
<tr>
<td>hostPacketsIn</td>
<td>Packets received by the host</td>
<td>integer</td>
</tr>
<tr>
<td>hostPacketsOut</td>
<td>Packets sent by the host</td>
<td>integer</td>
</tr>
<tr>
<td>hostErrorsIn</td>
<td>Error packets received by the host</td>
<td>integer</td>
</tr>
<tr>
<td>hostErrorsOut</td>
<td>Error packets sent by the host</td>
<td>integer</td>
</tr>
<tr>
<td>hostDropsIn</td>
<td>Dropped packets received by the host</td>
<td>integer</td>
</tr>
<tr>
<td>hostDropsOut</td>
<td>Dropped packets sent by the host</td>
<td>integer</td>
</tr>
<tr>
<td>vNetRxBytes</td>
<td>Bytes received by a virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vNetTxBytes</td>
<td>Bytes transmitted by a virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vNetRxPackets</td>
<td>Packets received by a virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vNetTxPackets</td>
<td>Packets transmitted by a virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vNetRxErrors</td>
<td>Error packets received by a virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vNetTxErrors</td>
<td>Error packets transmitted by a virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vNetRxDrops</td>
<td>Dropped packets received by a virtual system</td>
<td>integer</td>
</tr>
<tr>
<td>vNetTxDrops</td>
<td>Dropped packets transmitted by a virtual system</td>
<td>integer</td>
</tr>
</tbody>
</table>

Other virtualization counters

Other host counters for virtualized systems

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vState</td>
<td>The state of a virtualized host (see the libvirt documentation [<a href="http://libvirt.org/html/libvirt-libvirt.html#virDomainState">http://libvirt.org/html/libvirt-libvirt.html#virDomainState</a>])</td>
<td>integer</td>
</tr>
</tbody>
</table>
virtualDomains
The number of active domains in a virtualized host
integer

16.2.4. Services table fields
This section documents the fields available when a query is run over the services table.

Table 16.7. Database key fields available for services

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>A string representing the address of the sFlow agent for the service</td>
<td>string</td>
</tr>
<tr>
<td>agent</td>
<td>sFlow agent IP address</td>
<td></td>
</tr>
<tr>
<td>Datasource</td>
<td>A String representing the sFlow datasource for the service</td>
<td>string</td>
</tr>
<tr>
<td>datasource</td>
<td>sFlow datasource for the service</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Information on the type of service</td>
<td></td>
</tr>
<tr>
<td>service</td>
<td>The name of the service (eg http)</td>
<td>string</td>
</tr>
<tr>
<td>IfIndex</td>
<td>An integer representing the ifIndex that the request was seen on, if known</td>
<td>integer</td>
</tr>
<tr>
<td>inputIfIndex</td>
<td>the input interface for the request</td>
<td></td>
</tr>
<tr>
<td>outputIfIndex</td>
<td>the output interface for the request</td>
<td></td>
</tr>
<tr>
<td>Qualified interface</td>
<td>A string representing the agent and ifIndex that the request was seen on, separated by ‘&gt;’, if known</td>
<td>integer</td>
</tr>
<tr>
<td>inputInterface</td>
<td>qualified input interface for the request</td>
<td></td>
</tr>
<tr>
<td>outputInterface</td>
<td>qualified output interface for the request</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>A string representing an IP address in numeric notation</td>
<td>string</td>
</tr>
<tr>
<td>ipLocal</td>
<td>the local IP address associated with the request</td>
<td></td>
</tr>
<tr>
<td>ipRemote</td>
<td>the remote IP address associated with the request</td>
<td>string</td>
</tr>
<tr>
<td>ipClient</td>
<td>client IP address</td>
<td>string</td>
</tr>
<tr>
<td>ipServer</td>
<td>server IP address</td>
<td>string</td>
</tr>
<tr>
<td>UDP port</td>
<td>An integer representing the UDP port, or 0 if not UDP</td>
<td>integer</td>
</tr>
<tr>
<td>udpLocalPort</td>
<td>the local UDP port associated with the request</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>udpRemotePort</td>
<td>the remote UDP port associated with the request</td>
<td>integer</td>
</tr>
<tr>
<td>udpClientPort</td>
<td>UDP client port</td>
<td>integer</td>
</tr>
<tr>
<td>udpServerPort</td>
<td>UDP server port</td>
<td>integer</td>
</tr>
<tr>
<td>TCP port</td>
<td>An integer representing the TCP port, or 0 if not TCP</td>
<td></td>
</tr>
<tr>
<td>tcpLocalPort</td>
<td>the local TCP port associated with the request</td>
<td>integer</td>
</tr>
<tr>
<td>tcpRemotePort</td>
<td>the remote TCP port associated with the request</td>
<td>integer</td>
</tr>
<tr>
<td>tcpClientPort</td>
<td>TCP client port</td>
<td>integer</td>
</tr>
<tr>
<td>tcpServerTCP</td>
<td>TCP server port</td>
<td>integer</td>
</tr>
<tr>
<td>Highest layer 'port' available</td>
<td>A string with the protocol and port, separated by ':'</td>
<td></td>
</tr>
<tr>
<td>localPort</td>
<td>The local port associated with the request</td>
<td>string</td>
</tr>
<tr>
<td>remotePort</td>
<td>The remote port associated with the request</td>
<td>string</td>
</tr>
<tr>
<td>clientPort</td>
<td>The client port associated with the request</td>
<td>string</td>
</tr>
<tr>
<td>serverPort</td>
<td>The server port associated with the request</td>
<td>string</td>
</tr>
<tr>
<td>Other IP attributes</td>
<td>Other attributes of IP</td>
<td></td>
</tr>
<tr>
<td>ipProtocol</td>
<td>layer 4 protocol (eg 6 for TCP, 17 for UDP)</td>
<td>integer</td>
</tr>
<tr>
<td>HTTP fields</td>
<td>HTTP fields, available if the service is HTTP</td>
<td></td>
</tr>
<tr>
<td>httpHost</td>
<td>The host from the HTTP request</td>
<td>string</td>
</tr>
<tr>
<td>httpMethod</td>
<td>The method from the HTTP request</td>
<td>string</td>
</tr>
<tr>
<td>httpProtocol</td>
<td>The HTTP protocol version, encoded as major_number*1000+minor_number, eg HTTP1.1 is encoded as 1001</td>
<td>string</td>
</tr>
<tr>
<td>httpReferrer</td>
<td>The referrer from the HTTP request</td>
<td>string</td>
</tr>
<tr>
<td>httpURI</td>
<td>The full URI from the HTTP request</td>
<td>string</td>
</tr>
<tr>
<td>httpURIPath</td>
<td>The path from the URI. The path starts after the protocol, and ends at the start of the query</td>
<td>string</td>
</tr>
</tbody>
</table>
### Table 16.8. Database value fields available for services

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic values</td>
<td>Generic information on traffic</td>
<td></td>
</tr>
<tr>
<td>framesTotal</td>
<td>Number of frames or transactions</td>
<td>integer</td>
</tr>
<tr>
<td>numSamples</td>
<td>Number of samples seen</td>
<td>integer</td>
</tr>
<tr>
<td>HTTP values</td>
<td>Values associated with HTTP transactions</td>
<td></td>
</tr>
<tr>
<td>httpDuration</td>
<td>The mean duration of HTTP transactions, from start of request to end of response</td>
<td>integer</td>
</tr>
<tr>
<td>httpDuration</td>
<td>The mean duration of HTTP transactions, from start of request to end of response</td>
<td>integer</td>
</tr>
<tr>
<td>httpRequestBytes</td>
<td>The number of bytes in an HTTP request</td>
<td>integer</td>
</tr>
<tr>
<td>httpResponseBytes</td>
<td>The number of bytes in an HTTP response</td>
<td>integer</td>
</tr>
<tr>
<td>httpTotalBytes</td>
<td>The total number of bytes in a combined HTTP request and response</td>
<td>integer</td>
</tr>
</tbody>
</table>

### 16.2.5. Service counters table fields

This section documents the fields available when a query is run over the `serviceCounters` table.

### Table 16.9. Database key fields available for service counters

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Reference

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>A string representing the address of the sFlow agent for the service</td>
<td>agent sFlow agent IP address</td>
<td>string</td>
</tr>
<tr>
<td>Datasource</td>
<td>A String representing the sFlow datasource for the service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>datasource sFlow datasource for the service</td>
<td>string</td>
</tr>
<tr>
<td></td>
<td>parent The sFlow datasource for the parent of this service</td>
<td>string</td>
</tr>
<tr>
<td>Service Information on the type of service</td>
<td>service The name of the service (eg http)</td>
<td>string</td>
</tr>
</tbody>
</table>

**Table 16.10. Database value fields available for service counters**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP counters</td>
<td>Counters for HTTP operations counters</td>
<td></td>
</tr>
<tr>
<td>httpMethodConnectCount</td>
<td>Count of http CONNECT methods</td>
<td>integer</td>
</tr>
<tr>
<td>httpMethodDeleteCount</td>
<td>Count of http DELETE methods</td>
<td>integer</td>
</tr>
<tr>
<td>httpMethodGetCount</td>
<td>Count of http GET methods</td>
<td>integer</td>
</tr>
<tr>
<td>httpMethodHeadCount</td>
<td>Count of http HEAD methods</td>
<td>integer</td>
</tr>
<tr>
<td>httpMethodOptionCount</td>
<td>Count of http OPTION methods</td>
<td>integer</td>
</tr>
<tr>
<td>httpMethodPostCount</td>
<td>Count of http POST methods</td>
<td>integer</td>
</tr>
<tr>
<td>httpMethodPutCount</td>
<td>Count of http PUT methods</td>
<td>integer</td>
</tr>
<tr>
<td>httpMethodTraceCount</td>
<td>Count of http TRACE methods</td>
<td>integer</td>
</tr>
<tr>
<td>httpMethodOtherCount</td>
<td>Count of other http methods</td>
<td>integer</td>
</tr>
<tr>
<td>httpStatus1xxCount</td>
<td>Count of http status 1xx</td>
<td>integer</td>
</tr>
<tr>
<td>httpStatus2xxCount</td>
<td>Count of http status 3xx</td>
<td>integer</td>
</tr>
<tr>
<td>httpStatus3xxCount</td>
<td>Count of http status 3xx</td>
<td>integer</td>
</tr>
<tr>
<td>httpStatus4xxCount</td>
<td>Count of http status 4xx</td>
<td>integer</td>
</tr>
<tr>
<td>httpStatus5xxCount</td>
<td>Count of http status 5xx</td>
<td>integer</td>
</tr>
<tr>
<td>httpStatusOtherCount</td>
<td>Count of other http status</td>
<td>integer</td>
</tr>
</tbody>
</table>

**16.2.6. Time fields**

This section documents the time fields available. Time fields are common for all of the tables.

**Table 16.11. Database time fields**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>The time when traffic was observed</td>
<td>string</td>
</tr>
</tbody>
</table>
16.3. Filter functions reference

This section contains a reference for each of functions that can be used in JavaScript filters.

Table 16.12. JavaScript filter functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet membership</td>
<td>Tests if an address is in a subnet</td>
<td></td>
</tr>
<tr>
<td>inSubnet(address, subnet,</td>
<td>returns true if address is in subnet with maskBits</td>
<td>boolean</td>
</tr>
<tr>
<td>maskBits)</td>
<td></td>
<td>-------</td>
</tr>
<tr>
<td>Output ifIndex</td>
<td>Tests output interfaces</td>
<td></td>
</tr>
<tr>
<td>outputIfIndexIncludes(ifIndex)</td>
<td>returns true if the output interfaces includes ifIndex</td>
<td>boolean</td>
</tr>
</tbody>
</table>

16.4. Database functions

This section contains the reference information for database functions. Database functions are used within the `select` and `sort` (for value functions) statements in advanced reports, and take either database fields or other database functions as arguments. They allow the values from database fields to be modified before they are added to the result of running a query.

Database functions are divided into three types: `key functions`, which return a database key, `value functions`, which return a database value, and `time functions`, which operate on time. Each function can be used wherever the corresponding field can be used. They can each be used in a database select, to add a column to the resulting table. Value functions only can also be used in a sort statement, to sort the resulting table on that column.

16.4.1. Labels in database functions

Each function takes an optional string argument as the first parameter. If provided, this string is called the function label, and is used within charts and tables within the report, to display the name of the function. For example, to resolve the source address within a chart, you might use `resolve("Source name", sourceAddress)`. This specifies that when the name of the function is to be displayed, for example within the legend of a chart or the heading of a table, then the label "Source name" should be used. If this first parameter is not specified, then the function itself will be displayed (`resolve(sourceAddress)` in the example).

Using labels for functions is a way to make charts and tables more legible and understandable.

16.4.2. Key functions

16.4.2.1. countryCode

Synopsis

`countryCode([label,] ipAddress)`
Description

In addition to the optional label argument, described in Section 16.4.1, “Labels in database functions”, countryCode takes a single argument which must be an IPv4 address. The address can either be an address field (eg sourceAddress), or a literal address (eg "64.151.76.40"). It returns the ISO 3166 country code of the country in which the address is located, if known. If the country is not known, or the parameter is not an IPv4 address, then the empty string is returned.

Example

To select the sourceAddress and country code, use these fields in the select statement: sourceAddress, countryCode(sourceAddress)

16.4.2.2. countryName

Synopsis

countryName([label], ipAddress)

Description

countryName takes a single argument in addition to the optional label, which must be an IPv4 address. The address can either be an address field (eg sourceAddress), or a literal address (eg "64.151.76.40"). It returns the name of the country in which the address is located, if known. If the country is not known, or the parameter is not an IPv4 address, then the empty string is returned.

Example

To select the country of the clientAddress, use this field in the select statement: countryCode("Country", clientAddress) This will also use the label Country in a table heading or chart legend.

16.4.2.3. hostname

Synopsis

hostname([label], uuid) hostname([label], macAddress)

Description

hostname takes a single argument, in addition to the optional label, which can be a UUID or a MAC address. The argument can either be a key field (eg macSource or uuid), or a literal address or UUID (eg "00248C70AB58" or "6ba7b811-9dad-11d1-80b4-00c04fd430c8"). It returns the hostname associated with the UUID or MAC address, if known through host sFlow. If the address is not a UUID or MAC address, or the hostname cannot be determined, then the empty string is returned.

Example

To select the hostname of the hosts in a host counters query, use this field in the select statement: hostname(uuid)

16.4.2.4. ifAlias

Synopsis

ifAlias([label], interface)
Description

ifAlias takes a single argument, in addition to the optional label, which must be an interface field (note that ifAlias does not take an ifIndex parameter). It returns the ifAlias of the interface, if known. If the ifAlias is not known, or the parameter is not an interface, then the empty string is returned.

Example

To select the inputInterface and ifAlias from a switch, use these fields in the select statement:
inputInterface, ifAlias(inputInterface)

16.4.2.5. ifAliasOrVMName

Synopsis

ifAliasOrVMName([label,] interface)

Description

ifAliasOrVMName takes a single argument, in addition to the optional label, which must be an interface field (note that ifAliasOrVMName does not take an ifIndex parameter). It returns the ifAlias of the interface, if known. If the ifAlias is not known, then it returns the name of the virtual machine attached to the interface. If there is no ifAlias, and no VM attached to the interface, or the parameter is not an interface, then the empty string is returned.

Example

To select the inputInterface and ifAlias or VM name from a switch, use these fields in the select statement: inputInterface, ifAliasOrVMName(inputInterface)

16.4.2.6. ifName

Synopsis

ifName([label,] interface)

Description

ifName takes a single argument, in addition to the optional label, which must be an interface field (note that ifName does not take an ifIndex parameter). It returns the ifName of the interface, if known. If the ifName is not known, or the parameter is not an interface, then the empty string is returned.

Example

To select the ifName of the outputInterface from a switch, use this field in the select statement:
ifName(outputInterface)

16.4.2.7. ifOrVMName

Synopsis

ifOrVMName([label,] interface)

Description

ifOrVMName takes a single argument, in addition to the optional label, which must be an interface field (note that ifOrVMName does not take an ifIndex parameter). It returns the ifName of the interface, if
known. If the ifName is not known, then it returns the name of the virtual machine attached to the interface. If there is no ifName, and no VM attached to the interface, or the parameter is not an interface, then the empty string is returned.

Example

To select the ifOrVMName of the outputInterface from a switch, use this field in the select statement:  ifOrVMName(outputInterface)

16.4.2.8. locate

Synopsis

locate([label,] address)

Description

locate takes a single argument, in addition to the optional label, which must be an address. The address can either be an address field (eg sourceAddress), or a literal address (eg "64.151.76.40"). It returns the interface where the address is most likely to be located in the monitored network, if it can be determined. If the location cannot be determined, then the empty string is returned. Note that the address of an external system would most likely be located on a router interface. The location of an address can only be determined if network traffic from that address has been observed.

Example

To select the sourceAddress and location of the source address, use these fields in the select statement: sourceAddress, locate(sourceAddress)

16.4.2.9. locateSwitch

Synopsis

locateSwitch([label,] address)

Description

locateSwitch takes a single argument, in addition to the optional label, which must be an address. The address can either be an address field (eg sourceAddress), or a literal address (eg "64.151.76.40"). It works in the same way as Section 16.4.2.8, “locate”, but returns only the switch where the address is most likely to be located, rather than the complete interface. If the location cannot be determined, then the empty string is returned.

Example

To select the sourceAddress and switch where the source address is located, use these fields in the select statement: sourceAddress, locateSwitch(sourceAddress)

16.4.2.10. mac

Synopsis

mac([label,] address)
**Description**

`mac` takes a single argument, in addition to the optional label, which must be an `address`. The address can either be an address field (eg `sourceAddress`), or a literal address (eg "64.151.76.40"). It returns the most likely MAC address associated with the address if can be determined. If the address is already a MAC address, then it will be returned. If the MAC cannot be determined, then the empty string is returned. The MAC address associated with a layer 3 address can only be determined if network traffic from that address has been observed.

**Example**

To select the `sourceAddress` and MAC address associated with the source address, use these fields in the select statement: `sourceAddress, mac(sourceAddress)`

**16.4.2.11. vendor**

**Synopsis**

`vendor([label,] macAddress)`

**Description**

`vendor` takes a single argument, in addition to the optional label, which must be a `MAC address`. The address can either be an address field (eg `sourceAddress`), or a literal address (eg "00248C70AB58"). It returns the vendor associated with the address. If the address is not a MAC address or the vendor cannot be determined, then the empty string is returned.

**Example**

To select the source MAC address and vendor, use these fields in the select statement: `macSource, vendor(macSource)`

**16.4.2.12. getParent**

**Synopsis**

`getParent([label,] hostname)`

- `getParent([label,] macAddress)`
- `getParent([label,] uuid)`

**Description**

`getParent` takes a single argument, in addition to the optional label, which can be a `hostname`, a `MAC address` or a `UUID`. The argument can either be a key field (eg `hostname`, `macSource`, or `uuid`), or a literal hostname, address or UUID (eg "google.com", "00248C70AB58" or "6ba7b811-9dad-11d1-80b4-00c04fd430c8"). It returns the hostname, MAC address or UUID (respectively) associated with the parent of the host identified by the hostname, MAC address or UUID specified.

`getParent` is used to find system containment. For example, the parent of a virtual host is the physical host that is running the virtual one.

**Example**

To select the hostname of parent, of the host with hostname `server.inmon.com` in a host counters query, use this field in the select statement: `getParent("server.inmon.com")`
To select the UUID of the parent, of the host with UUID 6ba7b811-9dad-11d1-80b4-00c04fd430c8 in a host counters query, use this field in the select statement:
getParent("6ba7b811-9dad-11d1-80b4-00c04fd430c8")

### 16.4.2.13. resolve

**Synopsis**

resolve([label,] address)

resolve([label,] port)

**Description**

resolve takes a single argument, in addition to the optional label, which must be an address or port field. It returns the resolved name of the address or port, if known. If the resolved name is not known, or the parameter is not an address or port, then the empty string is returned. Note that resolve only works with the highest layer port fields (eg `sourcePort`), not with the numeric ports (such as `tcpSourcePort`).

**Example**

To select the `sourceAddress`, resolved name of the source address, and the resolved name of the `sourcePort`, use these fields in the select statement: `sourceAddress, resolve(sourceAddress), resolve(sourcePort)`

### 16.4.2.14. subnet

**Synopsis**

subnet([label,] ipAddress)

**Description**

subnet takes a single argument, in addition to the optional label, which must be an IP address field. It returns the name of the smallest defined subnet that the address belongs to. If the address does not belong to a subnet, then the name of the external subnet is returned. If the parameter is not an IP address, then the empty string is returned. For this function to be useful, subnets must have first been defined in sFlowTrend-Pro; see Section 13.3, “Configuring subnets in sFlowTrend-Pro” for more information.

**Example**

To select the `sourceAddress` and the subnet that `sourceAddress` belongs to, use these fields in the select statement: `sourceAddress, subnet(sourceAddress)`

### 16.4.2.15. uuid

**Synopsis**

uuid([label,] hostname) uuid([label,] macAddress)

**Description**

uuid takes a single argument, in addition to the optional label, which can be a hostname or a MAC address. The argument can either be a key field (eg `macSource` or `hostname`), or a literal address or hostname (eg
"00248C70AB58" or "google.com"). It returns the UUID associated with the MAC address or hostname, if know through host sFlow. If the hostname or address is not valid, or the UUID cannot be determined, then the empty string is returned.

Example

To select the uuid of the host server.inmon.com in a host counters query, use this field in the select statement: `uuid("server.inmon.com")`

16.4.2.16. vmName

Synopsis

```
vmName([label,] interface)
```

Description

`vmName` takes a single argument, in addition to the optional label, which must be an `interface` field (note that `vmName` does not take an `ifIndex` parameter). It returns the name of the virtual machine attached to the interface, if there is one. If there is no VM attached to the interface, or if the parameter is not an interface, then the empty string is returned.

Example

To select the virtual machine name for a VM attached to virtual switch interface `inputInterface`, use this field in the select statement: `vmName(inputInterface)`

16.4.3. Value functions

16.4.3.1. count

Synopsis

```
count([label,] keyField [, keyField, ...])
```

Description

`count` is an unusual function, which takes any number of `key` fields as arguments, in addition to the optional label, and returns a `value` field. It counts the number of unique combinations of all the key fields observed. This is useful if you are trying to understand for example, how many different connections a host made, rather than the specifics of each connection.

Example

To select each source, and the total number of destinations that each source connected to, you could use the following fields in a select: `sourceAddress, count(sourceAddress, destinationAddress)`

16.4.3.2. max

Synopsis

```
max([label,] valueField1, valueField2)
```
Description

`max` returns the larger of the values of two value fields. Either or both of the fields can also be other value functions, in addition to constant fields, to allow more complex expressions to be created. `max` is most useful when both the arguments are of similar type - eg frames, or bytes, etc.

Example

To select the larger of ingress frames and egress frames, use this field in the select statement: `max(framesIn, framesOut)`

To select the larger of the ingress frames per second and egress frames per second, you would use a combination of the `max` function and the `rate` function (see Section 16.4.3.4, “rate”): `max("Frame rate", rate(framesIn), rate(framesOut))`. This example uses a label ("Frame rate") which means that the function will be displayed as *Frame rate* in table headings and chart legends.

16.4.3.3. `min`

Synopsis

`min([label,] valueField1, valueField2)`

Description

`min` returns the smaller of the values of two value fields. Either or both of the fields can also be other value functions, in addition to constant fields, to allow more complex expressions to be created. `min` is most useful when both the arguments are of similar type - eg frames, or bytes, etc.

Example

To select the smaller of ingress bytes and egress bytes, use this field in the select statement: `min(bytesIn, bytesOut)`

16.4.3.4. `rate`

Synopsis

`rate([label,] valueField)`

Description

`rate` takes a single value field as a parameter, in addition to the optional label, and converts it to a value per second (ie a rate). For example, it would convert a frames field into frames per second.

Example

To select the total frames per second, use this field in the select statement: `rate(framesTotal)`

16.4.3.5. `scale`

Synopsis

`scale([label,] valueField, factor)`
Description

scale takes a single value field as a parameter, in addition to the optional label, and scales it by a constant factor, given as the second argument. The factor can be a real number. This is very useful to convert a bytes field into bits - use a scale factor of 8.

Example

To select the total bits per second, first of all scale total bytes to get bits, then convert it into a rate:
rate(scale(bytesTotal, 8))

16.4.3.6. sum

Synopsis

sum([label,] valueField1, valueField2)

Description

sum adds the values of two values, and returns the result. Either or both of the fields can be other value functions, in addition to constant fields, to allow more complex expressions to be created.

Example

To select the sum of ingress multicasts and broadcasts, use this field in the select statement:
sum(ifInMulticasts, ifInBroadcasts)

16.4.4. Time functions

16.4.4.1. format

Synopsis

format([label,] time, [[todayFormat], otherDayFormat])

Description

format takes up to three arguments, in addition to the optional label: the first must be the time field (time). The second, optionally, is a Java time and date format string that will be used to format time which is in today. The third argument is a format string that will be used to format time that is not in today. If the second argument is missing, the same format string will be used to format all time, regardless of whether it is in today or not. If both the second and third arguments are missing, then default formats are used, which formats time in today with a short time (no date), and formats time in other days in with a short time and date.

For documentation on how to construct a format string, please see the Java data format documentation [http://java.sun.com/javase/6/docs/api/java/text/SimpleDateFormat.html]

Example

To select time formatted with the default formatter, use this field in the select statement: format(time)

To select time formatted as 24 hour time, without the date, for today, and including a short date for other days, use this field in the select statement: format(time, "HH:mm", "dd/MM/yy HH:mm")
16.4.4.2. timestamp

Synopsis

timestamp([label,] time)

Description

timestamp takes a single argument, in addition to the optional label, which must be the time field (time), and returns the timestamp corresponding to the time. The timestamp is the number of milliseconds since January 1st, 1970.

Example

To select the timestamp of data, use this field in the select statement: timestamp(time)

16.5. Classes and objects defined within scripted reports

Scripted reports use a standard JavaScript environment to execute a script. Additional classes and objects are available within the script to allow the report to be generated. This section is a reference of the classes and objects available.

16.5.1. Objects defined

The following objects can be referenced from a scripted report:

16.5.1.1. report

Synopsis

report

Description

report is the single instance of the Report class available. The report object represents the current report being generated. Invoking any of the methods defined for the Report class on it will have the appropriate result on the report generated (for example, adding a chart).

Example

To add a table of results to a report, use the code

report.table(data);

where data is the result of running a previous query.

16.5.1.2. reportVars

Synopsis

reportVars.variable
Description

`reportVars` is an object with a property defined for each of the report variables specified in the scripted report tab. The name of each property is the name of the variable, and the value of the property is the value defined for that variable. This allows the values of the defined variables to be used from within the report script.

Example

You might want to parameterise the timeframe for the report to run over. To do this, add a variable `timeframe`, and enter its value as "today". Then from within the report script, refer to this value by `reportVars.timeframe`; you would probably use this to specify the period for a query. When the report is run, it would generate data for today. If you then changed the variable value to `lastHour`, then the report would generate data for lastHour, without the script itself having to be changed.

16.5.2. Classes defined

The following classes are defined in the environment of a scripted report:

16.5.2.1. Chart

Synopsis

```java
Chart.setWidth(int width)
Chart.setHeight(int height)
```

Description

Chart is the class of a chart generated within a report. An instance of a chart is obtained as the return value of the `chart` and `timeChart` methods in `Report`. After a chart has been created, its size can be modified from the default using the `setWidth` and `setHeight` methods.

Example

To generate a chart (using the previous data from a query), and change its size, the code

```javascript
var newChart = report.timeChart("lineChart", data, "sourceAddress, resolve(sourceAddress), 
%1$s(%2$s", "rate(framesTotal)");
newChart.setWidth(1000);
newChart.setHeight(800);
```

16.5.2.2. Query

Synopsis

```java
Query(String table, String view,
    String select, String filter,
    String period, int interval, String sort,
```
boolean decreasingOrder,  
boolean sortPerInterval, int n)

Query.run()

Description

Query is the class which defines a query to run on the database. The methods are:

Query(table, view, select, filter, period, interval, sort, decreasingOrder, sortPerInterval, n). Creates a new Query. The parameters are:

- **table** the database table to run the query on. Current valid tables are "flows", "counters", "hostCounters", "serviceCounters", "services", or "events".

- **view** the view of the database table required. The view can be thought of as a specific perspective on the data. If the view is the empty string, then all data is included. If it is a list of IP addresses of switches/routers, then only data from these devices is included. If you only want data for one switch interface, then use a string of the form "switch>ifIndex", where switch is the IP address of the switch, and ifIndex the ifIndex of the interface. Finally, a set hosts can be specified. To do this, use a view of the form hosts(host1, host2,..). Each host can be specified by hostname or UUID.

- **select** is a string containing a list of the database fields and functions required to select from the database for the query.

- **filter** is a JavaScript filter for the query. if not required, leave as the empty string.

- **period** the time that the query should run over. This is a string parameter, with values one of "last5Mins", "last10Mins", "last15Mins", "last30Mins", "lastHour", "last6Hours", "last12Hours", "last24Hours", "today", "yesterday", "thisWeek", "lastWeek" Additionally, arbitrary periods can be specified using dates of the form "yyyy-MM-dd HH:mm to yyyy-MM-dd HH:mm". The month and day are specified using digits, and the time is specified using 24-hour clock, for example "2012-10-05 10:00 to 2012-10-05 14:00" would run the query from 10:00 on October 5th, 2012 to 14:00 on the same day. The time is in the local timezone on the client.

- **interval** the size of each bucket (in minutes) in the resulting data. If this is set to 0, then only one bucket will be created.

- **sort** the field or function which to sort the data by. This field or function must have previously been included in the select statement. If no sorting is required, leave as the empty string.

- **decreasingOrder** if true then the data will be sorted with the largest first, if false then the data is sorted smallest first.

- **sortPerInterval** if true then sorting will be performed independently per bucket generated in the results. If a value is specified for n, then each bucket will have the top-n for that interval. If false, then the sort will be applied across all of the data in the period. If a value for n is specified, then the top-n is generated over the entire period.

- **n** the number of entries to include in the results, before including everything else in an "other" entry. This is used to create top-n queries. If set to 0, then all data is returned. Note that including all data can make the query significantly slower, and use more memory.

Query.run(). Runs the query, returning a Table.
Example

To create a query on the flows table, for top 5 sources by total frames, over the last hour with 1 minute buckets, and then run it, use the code:

```javascript
var query = new Query("flows", ",",
    'timestamp("Timestamp", time), sourceAddress,
    resolve("Source name", sourceAddress), rate(framesTotal)',
    ",", "lastHour", 1, "rate(framesTotal)", true, false, 5);
var result = query.run();
```

16.5.2.3. Report

Synopsis

Report.chart(type, data, categoryFields, categoryFormat, seriesFields, seriesFormat, valueFields [, title])
Report.paragraph(text)
Report.table(data [, title])
Report.timeChart(type, data, seriesFields, seriesFormat, valueFields [, title])

Description

Report is the class of the current report object (see Section 16.5.1.1, “report”). The methods defined within Report allow data to be added to a report. The methods are:

chart(type, data, categoryFields, categoryFormat, seriesFields, seriesFormat, valueFields [, title]) creates a chart (note: not a time-based chart; for this, use a timeChart) in the report. The parameters are:

- type a string representing the type of chart to be generated in the report. Current valid options are: "barChart", "stackedBarChart", "areaChart", "stackedAreaChart", "lineChart".
- data a Table, which is obtained from running a query.
- categoryFields a string containing a list of database key fields and key functions, which should form the categories to be displayed in the chart (i.e., on the x-axis). Each of the fields must be present in the data by selecting them in the query. The categories formed will be the combination of all of the specified fields in each row of the data. Note that this parameter is of type string, and any embedded strings within it (e.g., strings within database functions) must be correctly escaped to avoid JavaScript errors.
- categoryFormat a format string which can be used to make the combination of the category fields more legible (see Section 8.2.2.3, “Editing a query using advanced settings”). If this parameter is empty, then the category fields will be presented as a comma-separated list.
- seriesFields a string containing a list of database key fields and key functions, which should form the series to be displayed in the chart. Each of the fields must be present in the data by selecting them in the query. The series formed will be the combination of all of the specified fields in each row of the data. Note that this parameter is of type string, and any embedded strings within it (e.g., strings within database functions) must be correctly escaped to avoid JavaScript errors.
• **seriesFormat** a format string which can be used to make the combination of the series fields more legible (see Section 8.2.2.3, “Editing a query using advanced settings”). If this parameter is empty, then the series fields will be presented as a comma-separated list.

• **valueFields** a string containing a list of database value fields and value functions, which should form the values to be displayed in the chart. Each of the fields must be present in the data by selecting them in the query. Note that this parameter is of type string, and any embedded strings within it (e.g., strings within database functions) must be correctly escaped to avoid JavaScript errors.

• **title** an optional title for the chart. If this parameter is not provided, then one will be generated automatically.

**Example**

To generate a bar chart (using the previous data from a query, assuming that this data includes the fields `sourceAddress` and `framesTotal`), use the code

```javascript
var newChart = report.chart("barChart", data,
    "sourceAddress", "", /* Category fields, no need for c */
```
Example

To generate a time based line chart (using the previous data from a query, assuming that this data includes the fields `timestamp(time), sourceAddress` and `framesTotal`), use the code

```javascript
var newChart = report.timeChart("lineChart", data,
    "sourceAddress", "/* No need for series format
    "framesTotal"); /* values */
```

16.5.2.4. Table

Synopsis

```javascript
Table.getStart()
Table.getEnd()
Table.getInteval()
```

Description

`Table` is the class of a database table created by running a query. After running a query, the instance of the `Table` returned is then used to create a chart or html table. The start and end times of the data contained within a `Table` can be obtained using the `getStart()` and `getEnd()` methods. `getInteval()` returns the time interval of the data, in milliseconds.

Example

To generate a table of data by running a query, use the code:

```javascript
var query = new Query("flows", ",",
    'timestamp("Timestamp", time), sourceAddress,
    resolve("Source name", sourceAddress), rate(framesTotal)',
    ",", "lastHour", 1, "rate(framesTotal)", true, false, 5);
var data = query.run();
report.paragraph("Start of data: "+data.getStart());
```
Appendix A. Configuring switches to send sFlow

Your switches must be configured to send sFlow to sFlowTrend-Pro. There are two methods for configuring sFlow: telling sFlowTrend-Pro to configure the switch using SNMP or using the command line interface (CLI) on the switch.

A.1. Using SNMP to configure the switch to send sFlow

sFlowTrend-Pro can use SNMP to configure a switch to send sFlow. You will need to make sure that the switch is configured to allow SNMP read/write access from sFlowTrend-Pro. You will also need to know the SNMP v2 read/write community string or the SNMP v3 settings that will allow write access. See Section 13.2.1, “Adding a switch that is to be configured via SNMP” for details on how to set up sFlowTrend-Pro so that it uses SNMP to configure a switch to send sFlow.

Alcatel-Lucent and ProCurve Networking by HP switches support SNMP configuration of sFlow.

A.1.1. Configuring ProCurve switches to allow sFlow configuration via SNMP

You can use SNMP to configure ProCurve switches (except the 9300 and 9400 series) to send sFlow. For this to be possible you must ensure that sFlowTrend-Pro uses an SNMP community that is configured on the switch with unrestricted write access and that the IP address of the host running sFlowTrend-Pro is included in the list of authorised managers configured on the switch.

Assuming that sFlowTrend-Pro is running on host with IP address 10.1.2.5 and is using the read/write SNMP community snmprw, access the command line interface on the ProCurve switch and take the following steps to set up the switch so that it will allow sFlowTrend-Pro to configure sFlow via SNMP:

1. Configure the SNMP community so that it will allow any MIB variable that has read/write access to be set:

   ```
   (config)# snmp-server community snmprw manager unrestricted
   ```

   Then verify this setting with:

   ```
   (config)# show snmp-server
   ```

   The result should be something like:

<table>
<thead>
<tr>
<th>SNMP Communities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Name</td>
</tr>
<tr>
<td>----------------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Community Name</th>
<th>MIB View</th>
<th>Write Access</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Community Name</th>
<th>MIB View</th>
<th>Write Access</th>
</tr>
</thead>
</table>

126
2. Configure the IP authorized managers to include the IP address of the host running sFlowTrend-Pro:

```
(config)# ip authorized-managers 10.1.2.5
```

Then verify this setting with:

```
(config)# show ip authorized-managers
```

The result should be something like:

<table>
<thead>
<tr>
<th>IP Managers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Manager IP</td>
</tr>
<tr>
<td>10.1.2.5</td>
</tr>
</tbody>
</table>

### A.2. Using the switch CLI to configure sFlow

Using this method you must access the switch using its web interface, ssh, or telnet and manually configure the switch to send sFlow to the IP address and UDP port that sFlowTrend-Pro is using to receive sFlow (see Section 13.5.3, “Configuring advanced options” for information on determining and configuring the IP address and UDP port). You should enable sFlow on 1 or more interfaces on the switch and set a sampling rate and configure a counter polling interval. The counter polling interval controls how frequently the interface counters will be exported as part of the sFlow data. We recommend a counter polling interval of 30 seconds. We recommend that you enable sFlow on all interfaces. You should also determine the SNMP read community string for the switch so that you can configure sFlowTrend-Pro with this community string. This will allow sFlowTrend-Pro to query the switch for interface and system names.

Some example CLI configurations for enabling sFlow globally are given in the following sections. The configurations are for sFlowTrend-Pro running on a system with IP address 10.1.2.5 and receiving sFlow data on UDP port 6343, with the sFlow agent address which uniquely identifies the switch explicitly set to 10.10.1.1 (where possible).

Many switches support a command to show the current sFlow configuration and to indicate whether data has been exported:

```
show sflow
```

See your switch documentation for more details.

#### A.2.1. Alcatel-Lucent OmniSwitch

```
-> ip interface loopback0 10.10.1.1
```
Configuring switches to send sFlow

- sflow receiver 1 name sFlowTrend address 10.1.2.5 udp-port 6343
- sflow sampler 1 1/1-24 receiver 1 rate 128
- sflow poller 1 1/1-24 receiver 1 interval 30

**Note**

The OmniSwitches also support the configuration of sFlow using SNMP.

### A.2.2. Brocade (Foundry Networks)

```
config> int e 1/1 to 4/48
interface> sflow forwarding
config> sflow destination 10.1.2.5 6343
config> sflow sample 128
config> sflow polling-interval 30
config> sflow enable
```

### A.2.3. D-Link

The following commands apply to the D-Link xStack® DGS-3600 series switch:

```
enable sflow
create sflow analyzer_server 1 owner analyzer1 timeout infinite collectoraddress 10.1.2.5
create sflow counter_poller ports all analyzer_server_id 1 interval 30
create sflow flow_sampler ports all analyzer_server_id 1 rate 128
```

### A.2.4. Enterasys

```
set sflow receiver 1 owner analyzer1 timeout 180000
set sflow receiver 1 ip 10.1.2.5

#configure packet sampling instances on ports 1 through 12
#assign to sFlow Collector 1
set sflow port ge.1.1-12 sampler 1
set sflow port ge.1.1-12 sampler maxheadersize 128
set sflow port ge.1.1-12 sampler rate 128

#configure counter poller instances on ports 1 through 12
#assign to sFlow Collector 1
set sflow port ge.1.1-12 poller 1
set sflow port ge.1.1-12 poller interval 30
```

### A.2.5. Extreme Networks
enable sflow
configure sflow-agent 10.10.10.1
configure sflow-collector 10.1.2.5 port 6343
configure sflow sample-rate 128
configure sflow poll-interval 30
configure sflow backoff-threshold 50
enable sflow backoff-threshold
enable sflow ports all

A.2.6. Force10 Networks

Force10(conf)# sflow enable
Force10(conf)# sflow collector 10.1.2.5 agent-addr 10.10.10.1 6343
Force10(conf)# sflow sample-rate 128
Force10(conf)# sflow polling-interval 30

A.2.7. H3C

<sysname> system-view
[Sysname] sflow agent ip 10.10.10.1
[Sysname] sflow collector ip 10.1.2.5 port 6343
[Sysname] sflow version 5
[Sysname] sflow interval 30

Then for each interface:

[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] sflow enable inbound
[Sysname-Ethernet1/0] sflow sampling-mode random
[Sysname-Etherent1/0] sflow sampling-rate 128

Note
Set the sampling-mode to random on all interfaces that support random sampling. Deterministic sampling is less accurate and should be avoided. The sampling direction should be set consistently across all interfaces, in this example enabling inbound sampling on all interfaces monitors all traffic paths through the switch and avoids double counting.

A.2.8. Juniper Networks

The best way to find the appropriate commands for sFlow on your Juniper switch is to search the Juniper web site. As a starting point, here is an example configuration:

sflow {
    polling-interval 30;
Configuring switches to send sFlow

```bash
sample-rate 128;
collector 10.1.2.5 {
  udp-port 6343;
}
interfaces ge-0/0/0.0;
interfaces ge-0/0/1.0;
interfaces ge-0/0/2.0;
interfaces ge-0/0/3.0;
interfaces ge-0/0/4.0;
interfaces ge-0/0/5.0;
interfaces ge-0/0/6.0;
interfaces ge-0/0/7.0;
interfaces ge-0/0/8.0;
interfaces ge-0/0/9.0;
interfaces ge-0/0/10.0;
interfaces ge-0/0/11.0;
interfaces ge-0/0/12.0;
interfaces ge-0/0/13.0;
interfaces ge-0/0/14.0;
interfaces ge-0/0/15.0;
interfaces ge-0/0/16.0;
interfaces ge-0/0/17.0;
interfaces ge-0/0/18.0;
interfaces ge-0/0/19.0;
interfaces ge-0/0/20.0;
interfaces ge-0/0/21.0;
interfaces ge-0/0/22.0;
interfaces ge-0/0/23.0 {
  polling-interval 30;
  sample-rate 128;
}
}
```

A.2.9. Netgear

```bash
sflow receiver 1 owner collector1 timeout 4294967295 ip 10.1.2.5
```

For each interface:

```bash
sflow sampler 1 rate 128
sflow poller 1 interval 30
```

A.2.10. ProCurve Networking by HP

All ProCurve switches that support sFlow (except the 9300 and 9400 series) can be configured using SNMP. In addition, the ProCurve 3500 and 5400 series switches can be configured to send sFlow using the CLI.
(config)# sflow 1 destination 10.1.2.5 6343
(config)# sflow 1 sampling ethernet A1-A24 128
(config)# sflow 1 polling ethernet A1-A24 30

Note

ProCurve 9300 and 9400 switches must be configured using the CLI using the syntax given for Foundry switches. All other ProCurve switches can also be configured using SNMP to send sFlow;
Appendix B. Configuring hosts to send sFlow

Your hosts must be configured to send sFlow to sFlowTrend-Pro. Eventually, it is expected that operating system vendors will integrate sFlow directly into their products. Until then, an add-on agent is available for host sFlow from SourceForge [http://host-sflow.sourceforge.net].

B.1. Installing the host sFlow agent

Currently, the host sFlow agent is available in RPM form for Linux, as a Windows installer, and as an RPM for XenServer. The source code is also available if you would prefer to build it from scratch, perhaps for a different operating system. Download the package appropriate for your systems, and install using the normal methods for each operating system.

B.2. Configuring the host sFlow agent

If you are installing the agent on Windows, then the installer will ask for the IP address of the sFlow collector as part of the installation. Just enter the IP address of your installation of sFlowTrend-Pro, and then when the installation is complete, host sFlow will be sent there.

When installing on Linux, a little more configuration is required. This can be done in two ways: either via DNS Service Discovery (DNS-SD) (see Section B.2.1, “Linux configuration using DNS Service Discovery”) or by editing a configuration file (Section B.2.2, “Linux configuration using the configuration file”). First, perform one of these configuration steps. Once complete, then start the service using the normal Linux service management command:

# service hsflowd start

B.2.1. Linux configuration using DNS Service Discovery

If you are able to configure your local DNS servers, then the recommended way to configure host sFlow on Linux is via DNS Service Discovery. The sFlow configuration is placed into DNS records, which are then read by each sFlow host agent. This allows a large network of hosts to be easily configured and reconfigured as required.

The default configuration file is set for DNS-SD, so no changes are required there. Just add the following records to your DNS servers (used by the hosts to be monitored), and the hosts will then pick up the configuration automatically.

The following is an example configuration for DNS-SD. One TXT record should be created, with the name field _sflow._udp. This defines the overall sampling parameters for the agent. Following this, add an SRV record to specify each collector (e.g., instance of sFlowTrend-Pro) to send sFlow to.

_sflow._udp TXT "txtvers=1" "sampling=400" "polling=20"
SRV 0 0 6343 sflowtrend.inmon.com
SRV 0 0 6343 10.1.2.5.
This specifies a sample rate of 1 in 400, a counter polling rate of every 20 seconds (recommended settings), and then two sFlow destinations: one host called sflowtrend.inmon.com, and another with the IP address of 10.1.2.5, both using the standard UDP 6343 sFlow port. Note that the period after an IP address is often required. For your configuration, replace the SRV entries with those appropriate to your installation.

**B.2.2. Linux configuration using the configuration file**

If you are unable to modify your DNS servers, or would prefer just to try out host sFlow by editing the configuration file on a few systems, then follow this example.

The configuration file is /etc/hsflowd.conf. Edit this file, and first change the line DNSSD to

```
DNSSD = off
```

This switches off DNS-SD; otherwise, the rest of the configuration file is ignored. Then, uncomment the collector section at the end of the file, and modify to suit your installation. To have the same effect as the example in Section B.2.1, “Linux configuration using DNS Service Discovery” use this for the configuration file:

```
sflow {
    packetSamplingRate=400
    counterPollingInterval=20
    collector {
        ip=sflowtrend.inmon.com
        udpport=6343
    }
    collector {
        ip = 10.1.2.5
        udpport = 6343
    }
}
```
Appendix C. Recommended sampling rates

Table C.1, “Recommended sampling rates” gives the recommended packet sampling rates for sFlow for different interface speeds and traffic levels.

### Table C.1. Recommended sampling rates

<table>
<thead>
<tr>
<th>Interface Speed</th>
<th>Traffic level</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>10Mb/s</td>
<td>Low</td>
<td>64</td>
<td>128</td>
<td>256</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>128</td>
<td>256</td>
<td>512</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>256</td>
<td>512</td>
<td>1024</td>
</tr>
<tr>
<td>100Mb/s</td>
<td>Low</td>
<td>128</td>
<td>256</td>
<td>512</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>256</td>
<td>512</td>
<td>1024</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>512</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td>1Gb/s</td>
<td>Low</td>
<td>256</td>
<td>512</td>
<td>1024</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>512</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>1024</td>
<td>2048</td>
<td></td>
</tr>
<tr>
<td>10Gb/s</td>
<td>Low</td>
<td>512</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>1024</td>
<td>2048</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>2048</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Low, medium and high traffic levels are usually found in the following situations:

**Low**
- administrative office environment.

**Medium**
- typical mixed use environment with file servers and web browsing.

**High**
- computing clusters, large ISP backbone/hosting.
Appendix D. Acknowledgements and copyright


Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.


(C)opyright 2000-2009 by Object Refinery Limited and Contributors.

jFreeChart is distributed under the terms of the GNU Lesser General Public License (LGPL). [http://
www.gnu.org/licenses/lgpl.html]

sFlowTrend-Pro includes software developed by the JDOM Project [http://www.jdom.org] .

Copyright (C) 2000-2012 Jason Hunter & Brett McLaughlin.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions, and the disclaimer that follows
these conditions in the documentation and/or other materials
provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products
derived from this software without prior written permission. For
written permission, please contact <request_AT_jdom_DOT_org>.

4. Products derived from this software may not be called "JDOM", nor
may "JDOM" appear in their name, without prior written permission
from the JDOM Project Management <request_AT_jdom_DOT_org>.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESSED OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter <jhunter_AT_jdom_DOT_org> and Brett McLaughlin <brett_AT_jdom_DOT_org>. For more information on the JDOM Project, please see www.jdom.org [http://www.jdom.org].

sFlowTrend-Pro uses the Flying Saucer xhtml renderer [http://xhtmlrenderer.dev.java.net].

Flying Saucer is distributed under the terms of the GNU Lesser General Public License (LGPL). [http://www.gnu.org/licenses/lgpl.html]


TagSoup is distributed under the terms of the Apache License version 2.0. [http://opensource.org/licenses/apache2.0.php]


Copyright (c) 2008 MaxMind, Inc. All Rights Reserved.

Redistribution and use with or without modification, are permitted provided that the following conditions are met:
1. Redistributions must retain the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
2. All advertising materials and documentation mentioning features or use of this database must display the following acknowledgement:
   "This product includes GeoLite data created by MaxMind, available from http://maxmind.com/"
3. "MaxMind" may not be used to endorse or promote products derived from this database without specific prior written permission.

THIS DATABASE IS PROVIDED BY MAXMIND, INC \"AS IS\" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL MAXMIND BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
Acknowledgements and copyright

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS DATABASE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

sFlowTrend-Pro uses Jetty [http://www.eclipse.org/jetty/].

Jetty is distributed under the terms of the Apache License version 2.0. [http://opensource.org/licenses/apache2.0.php]


Jackson is distributed under the terms of the Apache License version 2.0. [http://opensource.org/licenses/apache2.0.php]

FreeMarker subcomponents with different copyright owners
-----------------------------------------------

FreeMarker, both in its source code and binary form (freemarker.jar) includes a number of files that are licensed by the Apache Software Foundation under the Apache License, Version 2.0. This is the same license as the license of FreeMarker, but the copyright owner is the Apache Software Foundation. These files are:

- freemarker/ext/jsp/web-app_2_2.dtd
- freemarker/ext/jsp/web-app_2_3.dtd
- freemarker/ext/jsp/web-jsptaglibrary_1_1.dtd
- freemarker/ext/jsp/web-jsptaglibrary_1_2.dtd

sFlowTrend-Pro uses FreeMarker [http://freemarker.org].

Copyright 2014 Attila Szegedi, Daniel Dekany, Jonathan Revusky

FreeMarker is distributed under the terms of the Apache License v2.0 [http://www.apache.org/licenses/LICENSE-2.0]

sFlowTrend-Pro uses Rhino [https://developer.mozilla.org/en-US/docs/Mozilla/Projects/Rhino].

Rhino is distributed under the terms of the MPL 2.0. [http://www.mozilla.org/MPL/2.0]

sFlowTrend-Pro use jQuery and jQuery UI developed by jQuery Foundation [https://jquery.com/].

Copyright (c) jQuery Foundation and other contributors [https://jquery.org/]

This software consists of voluntary contributions made by many individuals. For exact contribution history, see the revision history available at https://github.com/jquery/jquery

jQuery and jQuery UI are distributed under the MIT license [https://tldrlegal.com/license/mit-license]

sFlowTrend-Pro uses jqPlot [https://www.jqplot.com].

Copyright (c) 2009-2011 Chris Leonello

jqPlot is distributed under the MIT license [https://tldrlegal.com/license/mit-license]

Copyright (c) 2009 Trent Richardson [http://trentrichardson.com/Impromptu/]

Timepicker Addon is distributed under the MIT license [https://tldrlegal.com/license/mit-license]


Copyright (c) 2014 Simon Hagström

jQuery Split Pane plugin is distributed under the MIT license [https://tldrlegal.com/license/mit-license]

sFlowTrend-Pro uses jQuery Mouse Wheel plugin [https://github.com/jquery/jquery-mousewheel] .

Copyright (c) jQuery Foundation and other contributors [https://jquery.org/]

This software consists of voluntary contributions made by many individuals. For exact contribution history, see the revision history available at https://github.com/jquery/jquery-mousewheel

jQuery Mouse Wheel plugin is distributed under the MIT license [https://tldrlegal.com/license/mit-license]