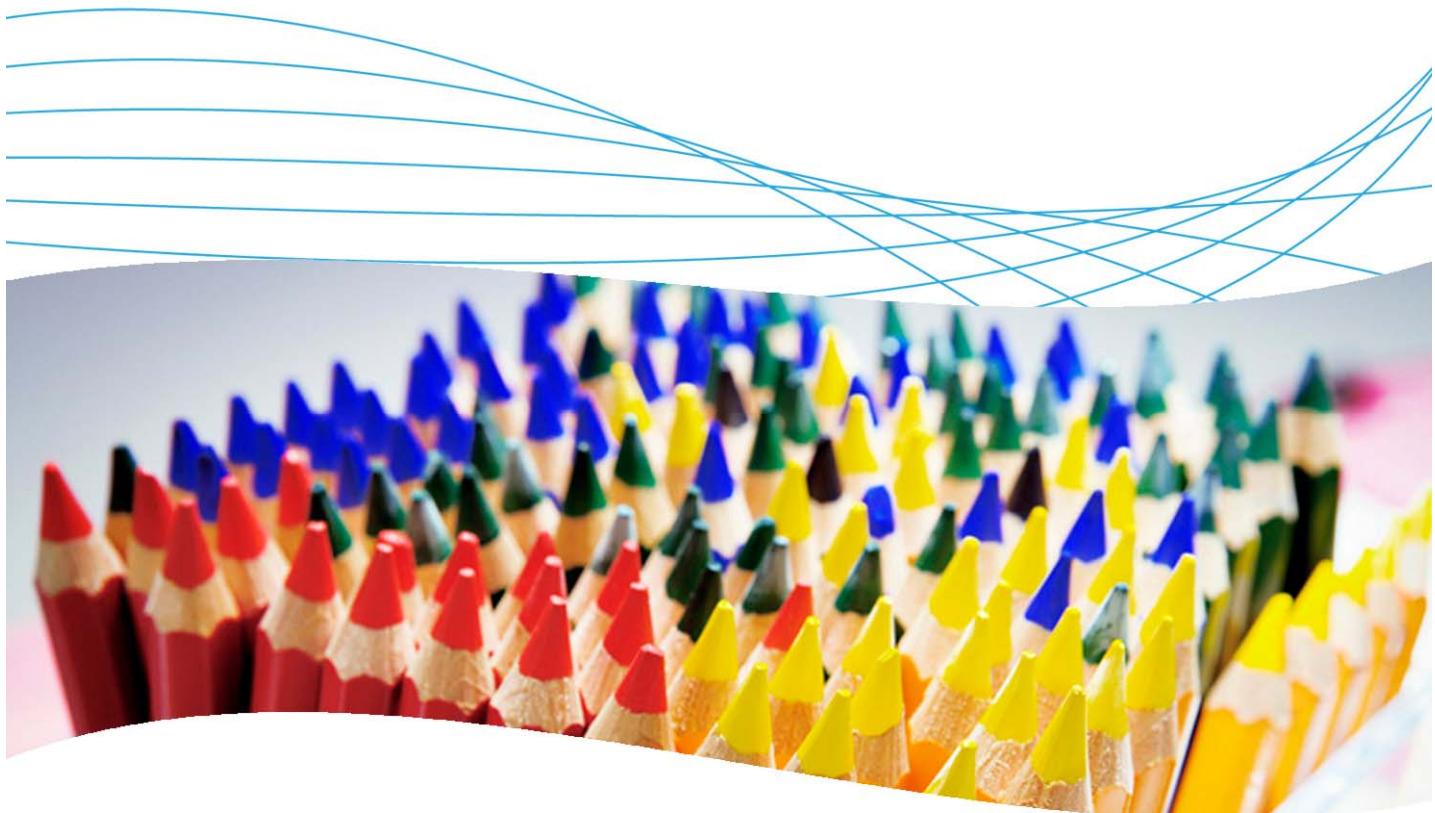


Traffic monitoring on ProCurve switches with sFlow and InMon Traffic Sentinel



Contents

| | |
|---|---|
| 1. Introduction | 3 |
| 2. Prerequisites | 3 |
| 3. Network diagram | 3 |
| 4. sFlow configuration on ProCurve switches | 3 |
| 4.1 Configure destination collectors | 3 |
| 4.2 View destination information | 4 |
| 4.3 Activate sampling and polling | 4 |
| 4.4 View sampling and polling statistics | 4 |

| | |
|--|-----------|
| 5. Traffic monitoring with InMon Traffic Sentinel | 5 |
| 5.1 Configure basic settings | 5 |
| 5.2 Set up traffic monitoring | 7 |
| 5.3 Traffic views..... | 9 |
| 5.4 Reporting | 11 |
| 6. Reference documents..... | 13 |

1. Introduction

This application note presents the monitoring and reporting capabilities of InMon Traffic Sentinel on ProCurve network equipment using the sFlow protocol.

The application note focuses on InMon Traffic Sentinel configuration. For more information on the sFlow protocol (history, protocol description, and benefits) and its implementation and configuration on ProCurve switches, please refer to ProCurve Application Note AN-S6, *Traffic Monitoring with sFlow and ProCurve Manager Plus*.

2. Prerequisites

This procedure assumes you have a network containing ProCurve switches, with traffic monitored by InMon Traffic Sentinel.

3. Network diagram

Figure 1 details the hardware configuration referenced in this section.

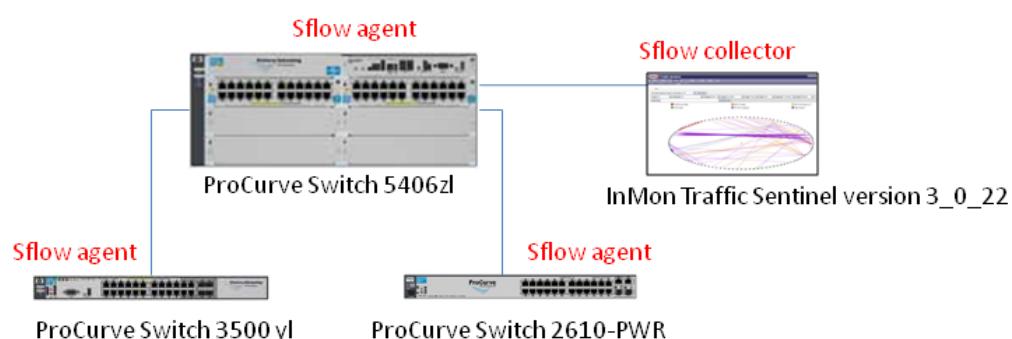


Figure 1. Setup for monitoring traffic flow with InMon Traffic Sentinel

The platform used to illustrate traffic monitoring consists of:

- One or more servers with the following services: Active Directory, DHCP, DNS, Certificate Authority, IAS
- ProCurve switches: 5406zl, 3500yl, 2610-PWR
- InMon Traffic Sentinel version 3_0_22

4. sFlow configuration on ProCurve switches

InMon Traffic Sentinel uses the sFlow protocol for traffic monitoring. This section provides the command syntax for configuring sFlow on a ProCurve switch.

4.1 Configure destination collectors

On each switch, three destinations (collectors) can be configured:

```
5406zl(config)# sFlow <1-3> destination <IP-addr> <udp-port-for-sFlow>
```

For example, to configure destination 1 to be 10.3.108.36:

```
5406zl(config)# sFlow 1 destination 10.3.108.36
```

The default UDP port used for sFlow is 6343.

4.2 View destination information

To view information about a destination:

```
5406zl(config)# show sFlow <1-3> destination
```

For example:

```
5406zl(config)# show sFlow 1 destination
Destination Instance      : 1
sFlow                      : Enabled
Datagrams Sent            : 557592
Destination Address       : 10.3.108.36
Receiver Port              : 6343
Owner                     : 10.3.108.36;procure-server.proact...
Timeout (seconds)         : 415
Max Datagram Size         : 1400
Datagram Version Support  : 5
```

4.3 Activate sampling and polling

To activate sampling on a set of switch ports, use:

```
5406zl(config)# sFlow <1-3> sampling <ports-list> N
```

Where *N* is the number of sampled packets. *N* can vary between 0 (sampling disabled) and 16441700.

For example:

```
5406zl(config)# sFlow 1 sampling all 500
```

To activate polling on a set of switch ports:

```
5406zl(config)# sFlow <1-3> sampling <ports-list> P
```

Where *P* is the interval in seconds between two polls of counters. *P* can vary between 0 (polling disabled) and 16777215.

4.4 View sampling and polling statistics

To view sampling and polling statistics:

```
5406zl(config)# show sFlow 1 sampling
```

| Port | Sampling | | | Dropped | | | Polling | |
|------|----------|------|----------------|---------|---------|----------|---------|--|
| | Enabled | Rate | Header Samples | Samples | Enabled | Interval | | |
| A1 | Yes(1) | 60 | 128 | 0 | Yes(1) | 20 | | |
| A23 | Yes(1) | 60 | 128 | 0 | Yes(1) | 20 | | |
| A24 | Yes(1) | 60 | 128 | 0 | Yes(1) | 20 | | |
| B24 | Yes(1) | 60 | 128 | 0 | Yes(1) | 20 | | |

```
5406zl(config)# show sFlow 1 sampling A1

Port | Sampling           Dropped | Polling
     | Enabled   Rate     Header Samples | Enabled Interval
-----+-----+-----+-----+
A1    Yes(1)      60     128          0   Yes(1)      20
```

5. Traffic monitoring with InMon Traffic Sentinel

This section uses a data center example to explain how to set up traffic monitoring using InMon Traffic Sentinel.

5.1 Configure basic settings

To configure basic settings for InMon Traffic sentinel:

1. Access Traffic Sentinel from its web interface.
2. Browse to the File | Configure menu. There you have three options:
 - o The Show tab shows you the actual configuration.
 - o The Edit tab allows you to modify the configuration.
 - o The XML tab enables you to import or export a configuration in XML format.
3. Select the Edit tab. In the Edit tab you have the following options:

The screenshot shows the InMon Traffic Sentinel web interface. At the top, there's a navigation bar with links for File, Home, Events, Traffic, Signatures, Reports, Maps, Search, About, Configure, Control, Status, Logs, Upgrade, Forwarding, and Users. Below the navigation bar, there's a toolbar with 'Options:' dropdown, 'Show', 'Edit', and 'XML' buttons, and a breadcrumb trail: Index > Site > Zone > Group > [CIDR | CIDR(IPv6) | Agent Range | Agent > Interface].

Server

- [Edit Site](#) Change site name, contact information and software key

Groupings

- [Edit Zones](#) Divide the network into Zones
 - o [Edit Groups](#) Divide each Zone into Groups
 - [Edit CIDRs](#) Specify a subnet in CIDR notation and assign it to a Group
 - [Edit CIDRs \(IPv6\)](#) Specify an IPv6 subnet in CIDR notation and assign it to a Group
 - [Edit Agent Ranges](#) Specify a range of addresses containing Agents and assign it to a Group
 - [Edit Agents](#) Identify an Agent by address and assign it to a Group
 - [Edit Interfaces](#) Identify a specific Interface on an Agent

Settings

- [Edit Threshold Settings](#) Specify thresholds on interface utilization and counters
- [Edit SNMP Settings](#) Specify SNMP authentication and version settings
- [Edit Sampling Settings](#) Specify packet sampling rates

- Edit Site enables you to define the name and contact information, and also to input your license key:

| Site Settings | |
|--|--|
| Enterprise Name | HP Intel Solution Center |
| Site Name | Grenoble |
| Server | inmon01.hpinelco.org |
| Serial Number | ITS070108001 |
| Software Key | 01010102044867542503044965d3b50915980bf278b19f43 |
| Contact Name | B10 Infra Team |
| Contact Location | N1 |
| Contact Phone | 0672992192 |
| Minutes of Real-time Data | 480 |
| Days of Historical Data | 35 |
| Mbytes of Free Disk Space | 400 |
| <input type="button" value="Back"/> <input type="button" value="Reset"/> <input type="button" value="Submit"/> | |

- Edit Zones allows you to divide your network into different logical zones, and within these zones to define groups of subnets, agents, interfaces.

For example, a zone can physically correspond to a site, and groups can correspond to different buildings within the site.

4. In this data center example, you create one zone, corresponding to the whole data center, and 10 groups (labeled Area 1, Area 2, etc.) corresponding to the different solution areas. You create a distinct group, called BackBone, for the network backbone:

| Edit Groups | | | |
|---|------------|-------------------------------------|---------------------------------------|
| Group | Group Name | Actions | |
| HP Intel Solution Center>Grenoble>Management>Area 1 | Area 1 | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>BackBone | BackBone | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 2 | Area 2 | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 9 | Area 9 | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 3 | Area 3 | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 8 | Area 8 | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 4 | Area 4 | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 5 | Area 5 | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 6 | Area 6 | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 7 | Area 7 | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Velocity | Velocity | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |

5. For each group you can define agent ranges. Then you go to Edit Agents to define the individual agents corresponding to the network equipment:

| Edit Agents | | | | | |
|---|---------------|------------------|--------|-------------------------------------|---------------------------------------|
| Agent | Agent Address | Override Control | Enable | Actions | |
| HP Intel Solution Center>Grenoble>Management>Area 1>10.4.10.201 | 10.4.10.201 | Override | Enable | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 1>10.4.12.201 | 10.4.12.201 | Override | Enable | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 1>10.4.13.201 | 10.4.13.201 | Override | Enable | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 1>10.4.16.201 | 10.4.16.201 | Override | Enable | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>Area 1>10.4.11.201 | 10.4.11.201 | Don't Override | Enable | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |
| HP Intel Solution Center>Grenoble>Management>BackBone>10.4.0.3 | 10.4.0.3 | Override | Enable | <input type="button" value="Edit"/> | <input type="button" value="Remove"/> |

6. Within the File | Configure | Edit view, you can define threshold settings and SNMP parameters.

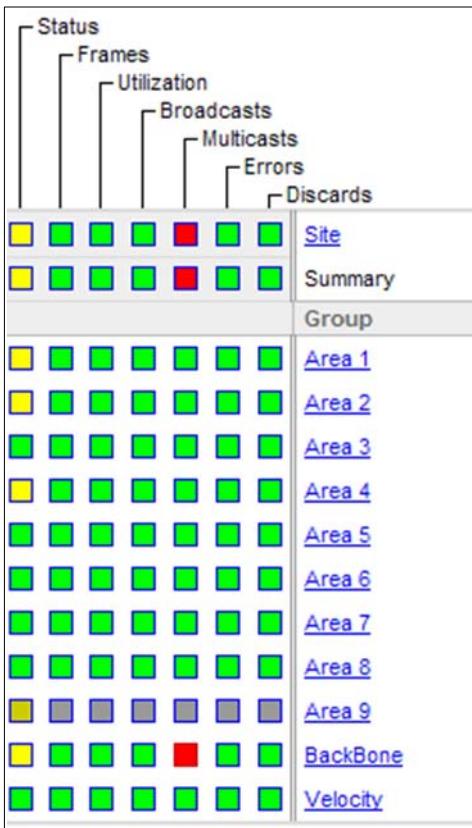
7. Finally, you can go to Edit Sampling Settings to define sampling rates for the different interface speeds:

| Edit Sampling Settings | | | | | |
|-----------------------------------|---------------|--------------|--------------|----------------------|------------------------|
| Path | Sampling Rate | Min. ifSpeed | Max. ifSpeed | Actions | |
| HP Intel Solution Center>Grenoble | 200 | 0Kb/sec | 10Mb/sec | Edit | Remove |
| HP Intel Solution Center>Grenoble | 500 | 10Mb/sec | 100Mb/sec | Edit | Remove |
| HP Intel Solution Center>Grenoble | 1000 | 100Mb/sec | 1Gb/sec | Edit | Remove |
| HP Intel Solution Center>Grenoble | 2000 | 1Gb/sec | 1000Gb/sec | Edit | Remove |

5.2 Set up traffic monitoring

To set up traffic monitoring:

1. Select Traffic | Status to see an overview of status of the different traffic metrics for each zone and group:

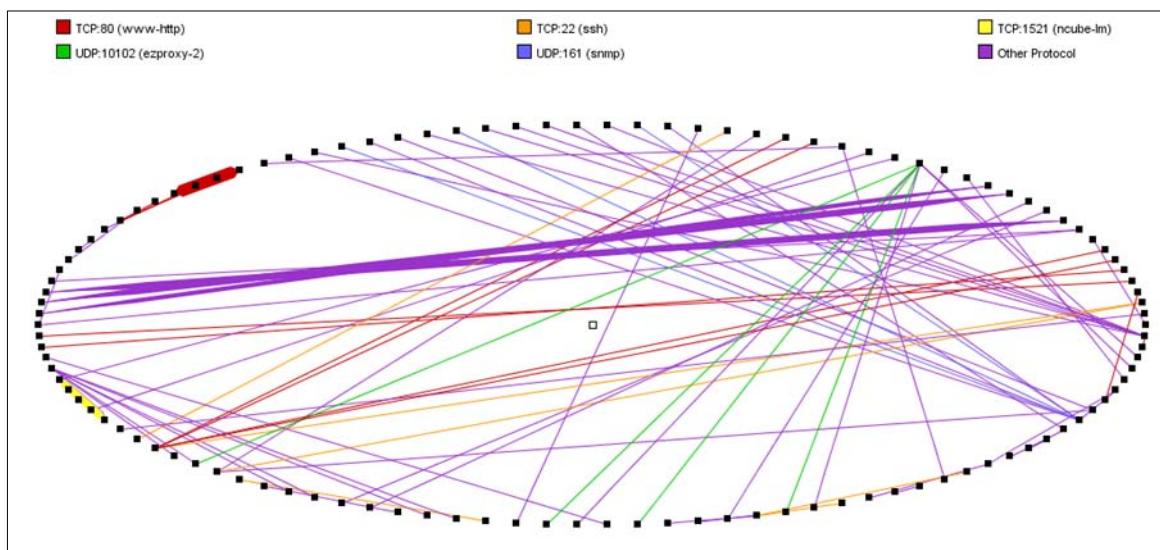


2. To view more details about a particular metric, click on one of the colored square indicators.

For example, you notice that the BackBone group is experiencing heavy multicast traffic (in red) and you want to determine which machines or applications are causing this multicast. Click on the square red BackBone indicator to display the list of sFlow agents, corresponding to the switches of the group. In this example, the top 10 interfaces with multicast traffic are listed:

| Status | | | | | | | Interface | |
|--------|-------------|------------|------------|--------|----------|-------------------|-------------|--|
| Frames | Utilization | Broadcasts | Multicasts | Errors | Discards | Agent | Interface | |
| █ | █ | █ | █ | █ | █ | sw9308-1 | ethernet4/8 | |
| █ | █ | █ | █ | █ | █ | sw5304_Z8R0-1 | C3 | |
| █ | █ | █ | █ | █ | █ | sw5304_Z8R0-1 | Trk1 | |
| █ | █ | █ | █ | █ | █ | sw5412_Z8R02-2 | B1 | |
| █ | █ | █ | █ | █ | █ | sw9308-1 | ethernet4/4 | |
| █ | █ | █ | █ | █ | █ | sw5304_N2-1 | A1 | |
| █ | █ | █ | █ | █ | █ | sw9308-1 | ethernet4/7 | |
| █ | █ | █ | █ | █ | █ | sw2626_FGraudDesk | 2 | |
| █ | █ | █ | █ | █ | █ | sw2626_FGraudDesk | 26 | |
| █ | █ | █ | █ | █ | █ | sw5304_N2-1 | A16 | |

3. Another way to have a good overview of what is generating traffic on the network is to use the circles function (Traffic | Circles):



This gives a graphical representation of the most important connections between machines on the network.

4. You can then click on a particular connection to display a Path Between Hosts screen with information about the corresponding flow:

The screenshot shows the "Path Between Hosts" interface. At the top, there are input fields for "Source" (208.36.144.8) and "Destination" (10.3.252.23), a "Submit" button, and two buttons: "Connections" and "Show Map". Below this, the text "208.36.144.8 -> 10.3.252.23" is displayed in blue. A table titled "Agent" lists connections from the source to the destination. Another table below it lists connections from the destination back to the source.

| Agent | I/F In | I/F Out | MAC Source | MAC Destination |
|---------------|--------|---------|--------------|-----------------|
| sw5304_Z1R0-1 | A1 | D1 | 000D88EE5DB0 | 00306E1E2F2B |
| sw5304_Z1R0-1 | A1 | D1 | 000D88EE5DB0 | 00306E1E2F2B |

| Agent | I/F In | I/F Out | MAC Source | MAC Destination |
|---------------|--------|---------|--------------|-----------------|
| sw5304_Z1R0-1 | D1 | B1 | 00306E1E2F2B | 000D88EE5DB0 |

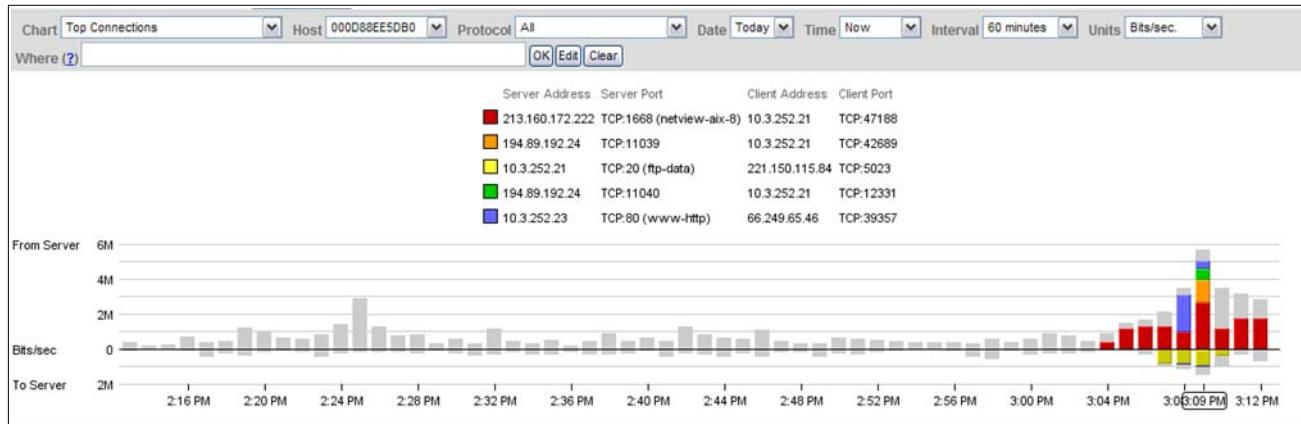
5. To obtain more information about a particular host, in the Path Between Hosts window click on one of the MAC Source or MAC Destination addresses. You then see a Find Host window, where you can choose between different views of the traffic:

The screenshot shows the "Find Host" interface. It has a search bar with "000D88EE5DB0" and a "Submit" button. Below the search bar is a placeholder text: "e.g. "www.inmon.com" or "10.1.4.2" or "001372CB6372"" and a row of buttons: "Connections", "Protocols", "Circles", "Explore", and "Interface". Below these are two rows of information: "Location" (HP Intel Solution Center>Grenoble>Management>BackBone>sw2824_BB1-1>2) and "MAC" (000D88EE5DB0). The "MAC Vendor" row shows "D-Link Corporation".

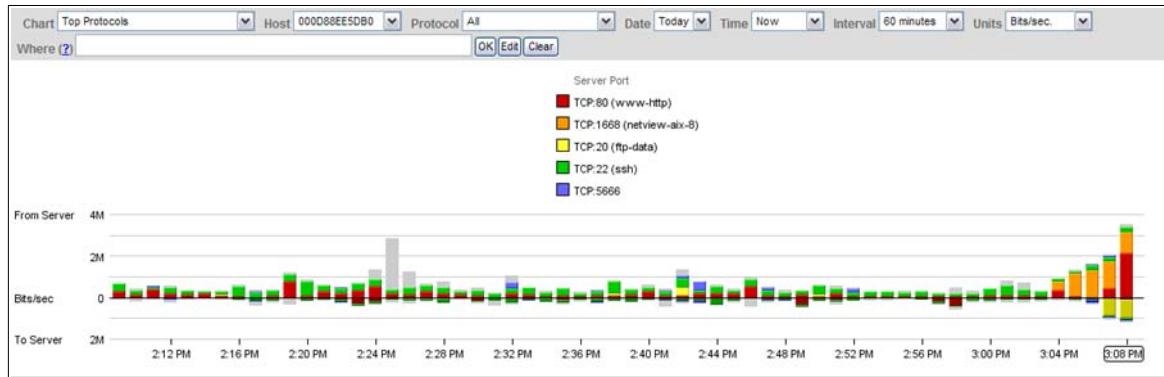
5.3 Traffic views

Here are some of the traffic views that are available.

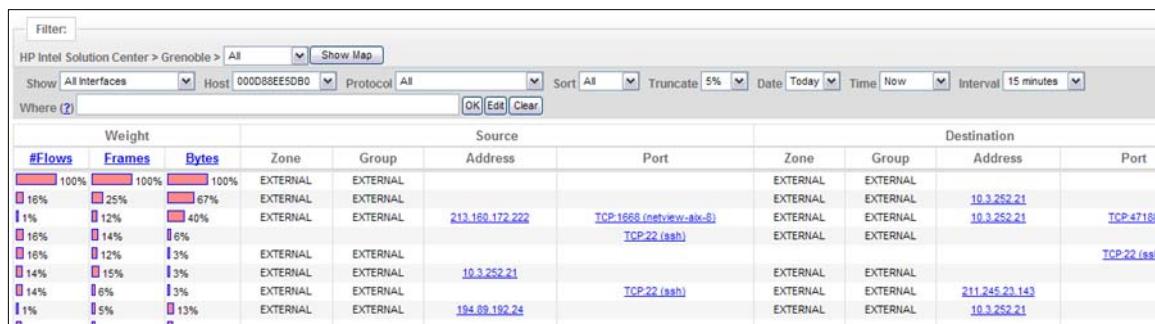
Clicking Connections gives top connections to and from this machine:



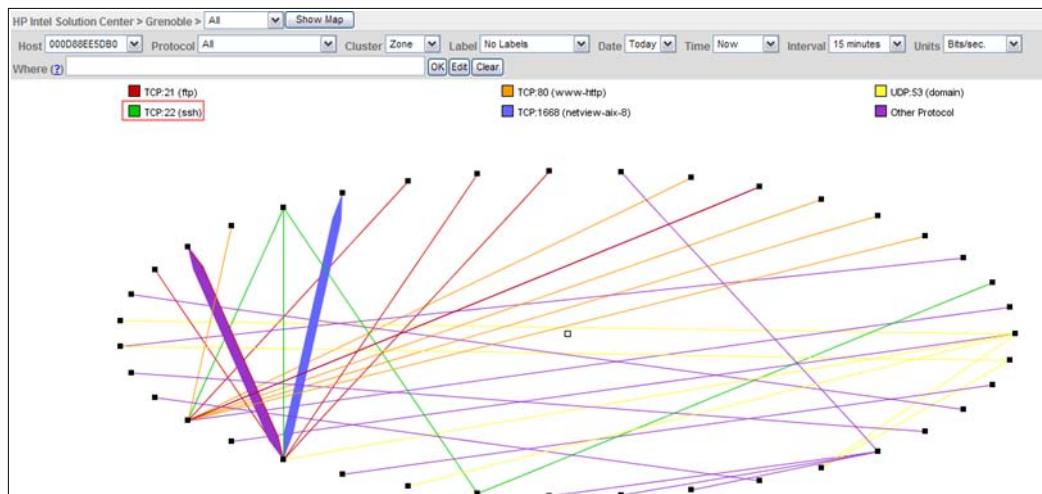
Clicking Protocols gives a view of the most used protocols for this MAC address over time:



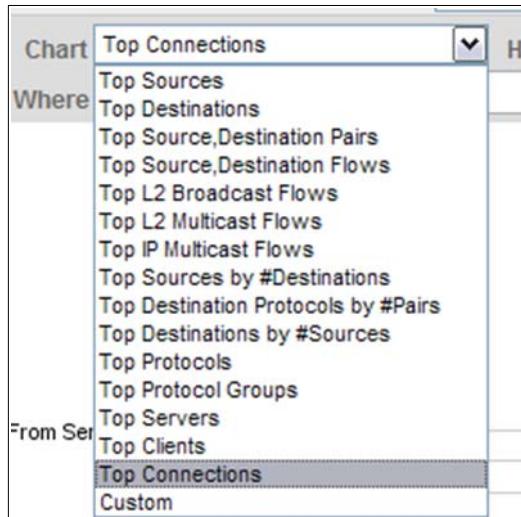
Factors view gives the proportion of each connection in percent of the flows, total frames and total bytes of the link to this machine:



A Circles view for this machine is also available:



You have a wide variety of traffic types to display in charts:



5.4 Reporting

To view the trends for a particular flow over a longer period, the reporting function is useful. To specify the type of reports:

1. On the Traffic Sentinel menu bar click on Reports. You see the available reports arranged by Category:

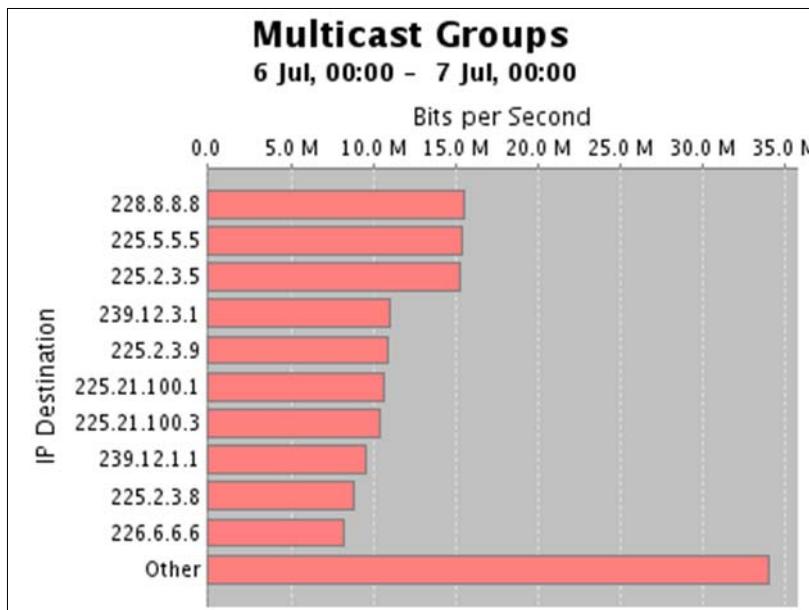
| Category | Report | Description |
|------------|----------------------------|--|
| Accounting | Site Network Usage | Assign traffic to local groups. |
| Events | Event Types | Analysis of the types of event. |
| Inventory | Network Inventory | List devices in the network. |
| QoS | QoS test report | |
| Security | Recently Added/Moved Hosts | Identifies newly active addresses and changes in location. |
| Security | Unauthorized Routers | Find unauthorized routers attached to the network. |
| Services | IP Multicast | IP Multicast activity on the network. |
| Services | Peer to Peer Traffic | Identify peer to peer (P2P) hosts and applications. |
| Services | Top Protocols | Top protocols in the network. |
| Traffic | Multicast | top Multicast connections |

2. Then you can choose a custom report.

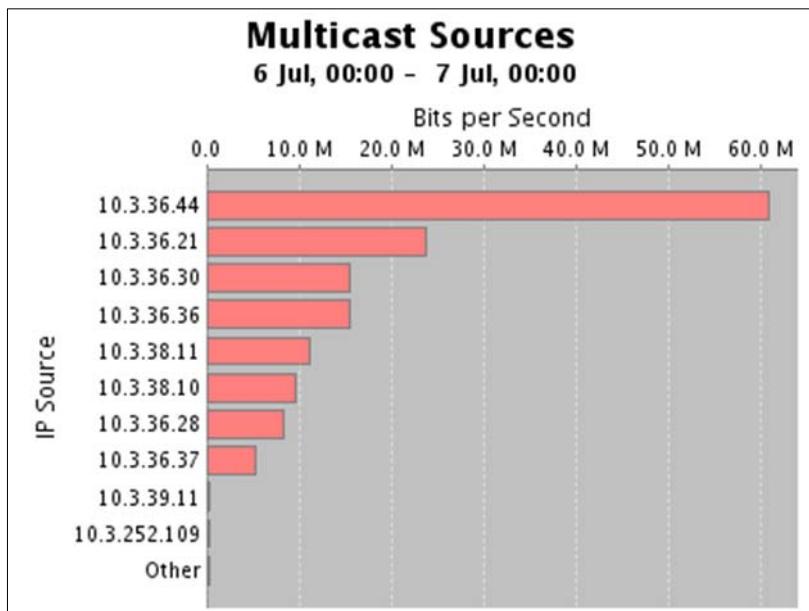
For example if you select IP Multicast, you see a report that displays the IP Multicast activity on the network. You see activity reports for the top Multicast Groups, Multicast Sources, and Multicast Trends. This report can be exported as a .PDF or a .HTML file. For example:

- **IP Multicast:** Shows IP multicast activity on the network.

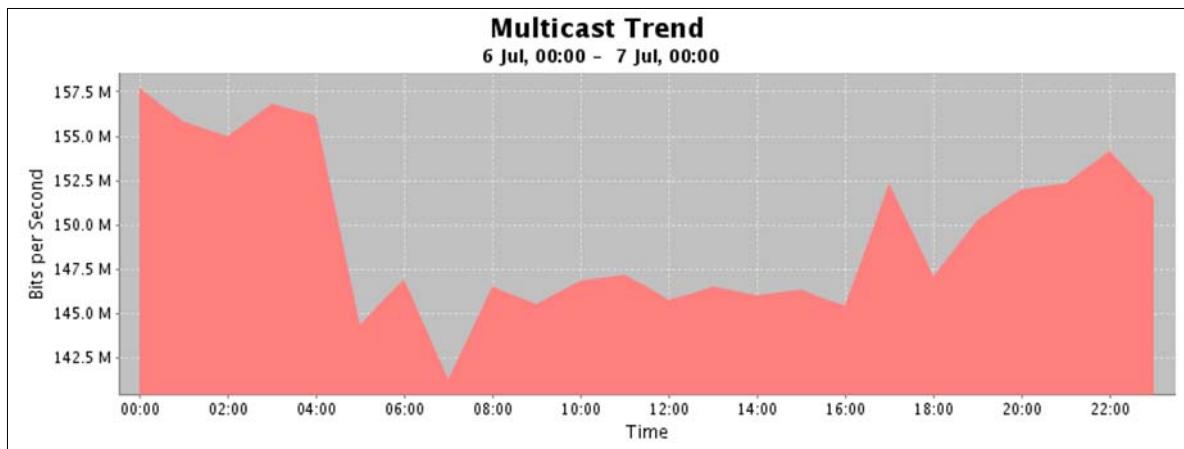
- **Top Multicast Groups:** Shows top IP multicast addresses by amount of traffic. For example:



- **Top Multicast Sources:** Shows Top IP multicast sources by amount of traffic. For example:



- **Multicast Trend:** Shows trends for total IP multicast activity over time:



6. Reference documents

This concludes the procedure for traffic flow monitoring on ProCurve switches using InMon Traffic Sentinel and sFlow.

For further information about how to configure ProCurve switches to support security, please refer to the following links:

- For PCM+ and IDM manuals:
<http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm>
<http://www.hp.com/rnd/support/manuals/IDM.htm>
- For user manuals for ProCurve 3500yl-5400zl-8212zl switches:
<http://www.hp.com/rnd/support/manuals/3500-6200-5400-ChapterFiles.htm>
- For ProCurve Switch 2610 series manuals:
<http://www.hp.com/rnd/support/manuals/2610.htm>
- For information, about InMon Traffic Sentinel, including documents and tutorials, see:
<http://www.inmon.com/products/trafficsentinel.php>

For further information, please visit www.procurve.eu



© 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

sFlow is a registered trademark of InMon Corp.

4AA2-1719EEE, July 2008