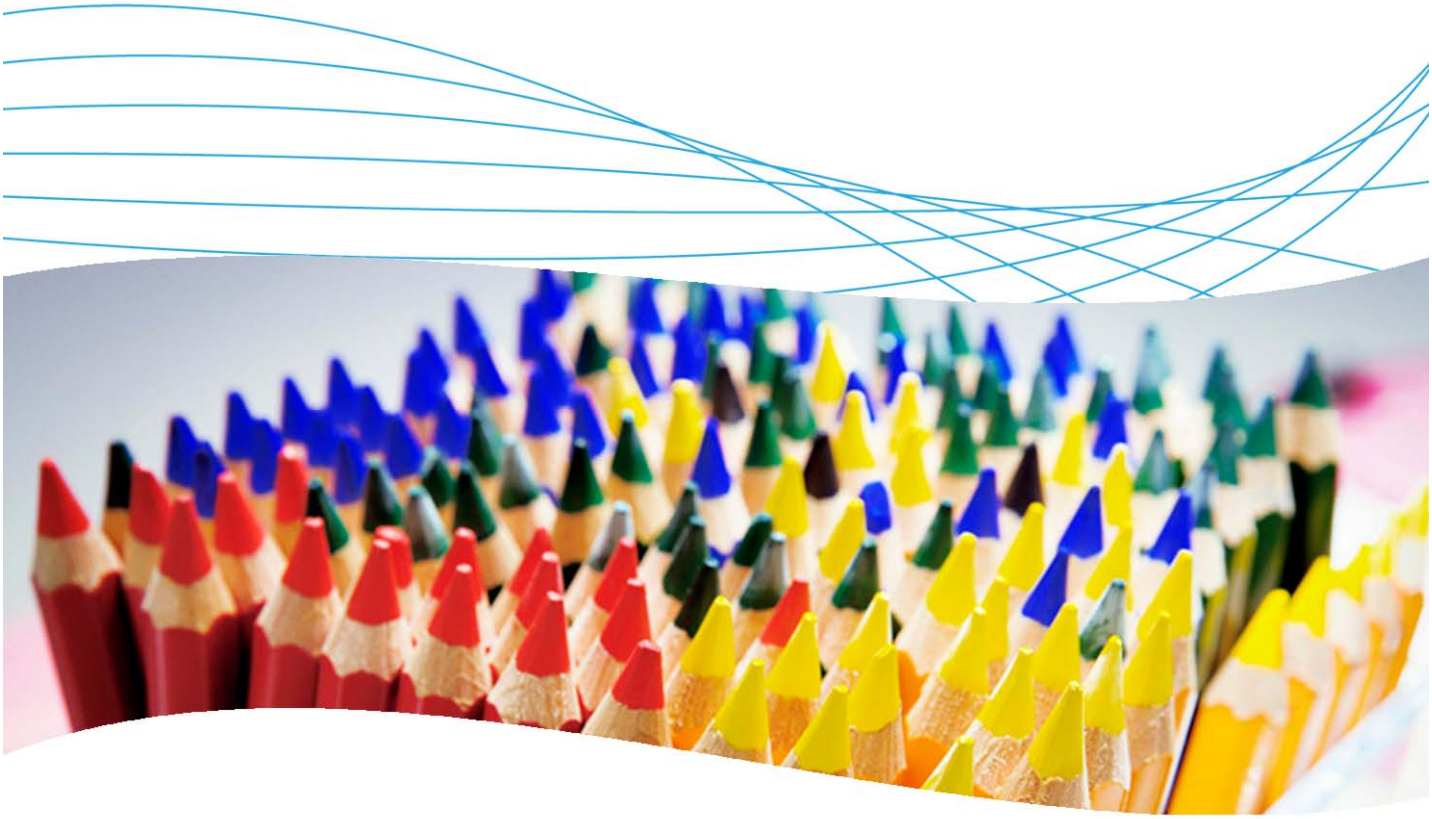
An HP ProCurve Networking Application Note

Traffic monitoring on ProCurve switches with sFlow and InMon Traffic Sentinel



Contents

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.

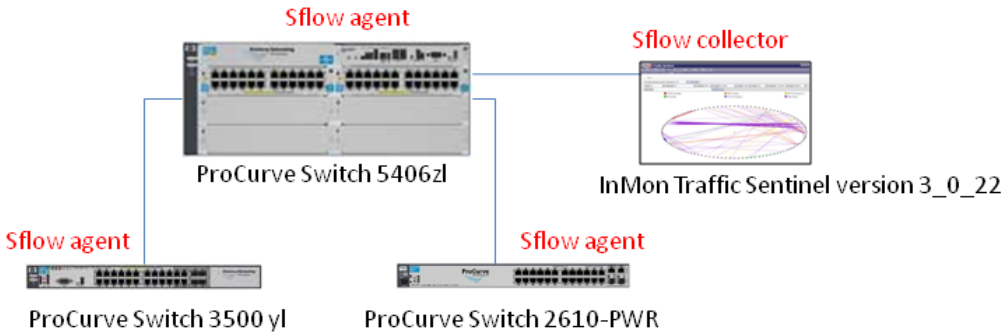


Figure 1. Setup for monitoring traffic flow with InMon Traffic Sentinel

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;procurve-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    | 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
```

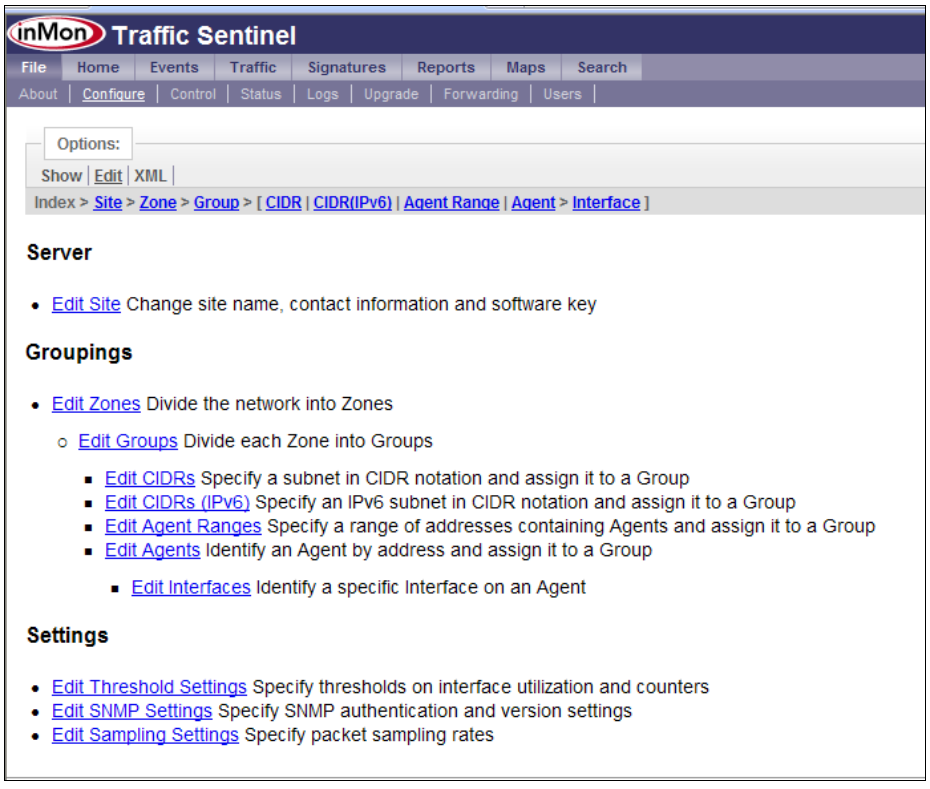
5. Traffic monitoring with InMon Traffic Sentinel

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

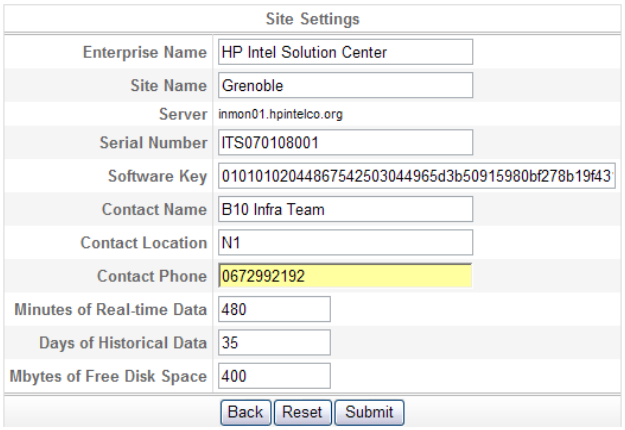
5.1 Configure basic settings

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:
   - The Show tab shows you the actual configuration.
   - The Edit tab allows you to modify the configuration.
   - 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:



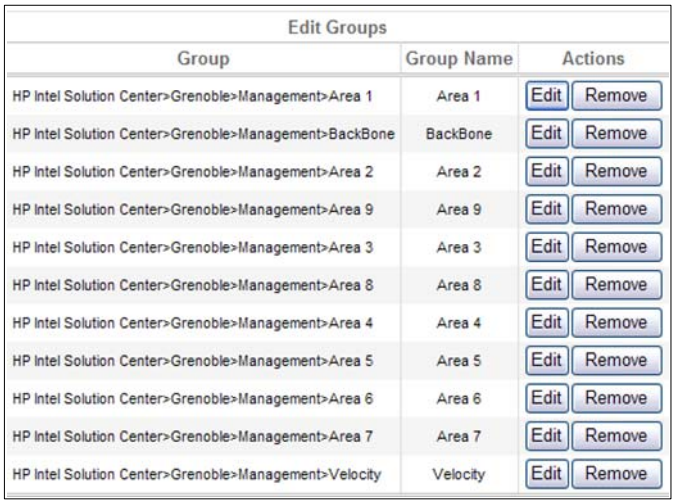
- Edit Site enables you to define the name and contact information, and also to input your license key:



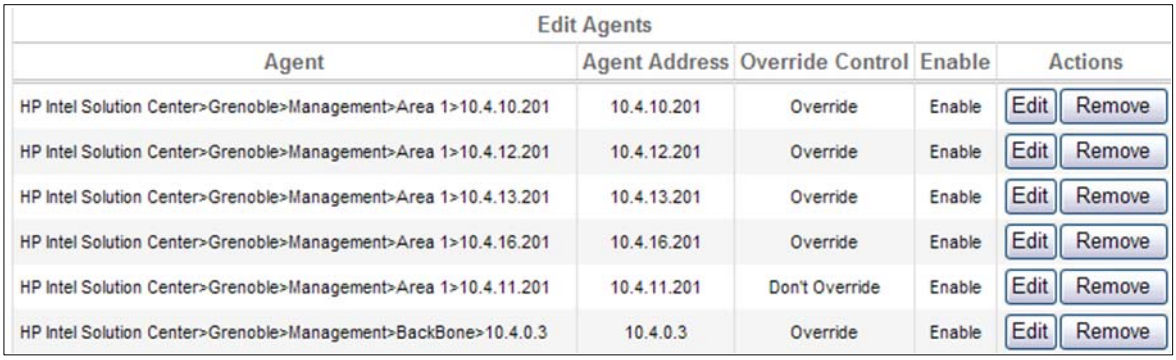
- Edit Zones allows you to divide your network into different logical zones, and within these zones to define groups of subnets, agents, interfaces.

  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:



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:



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

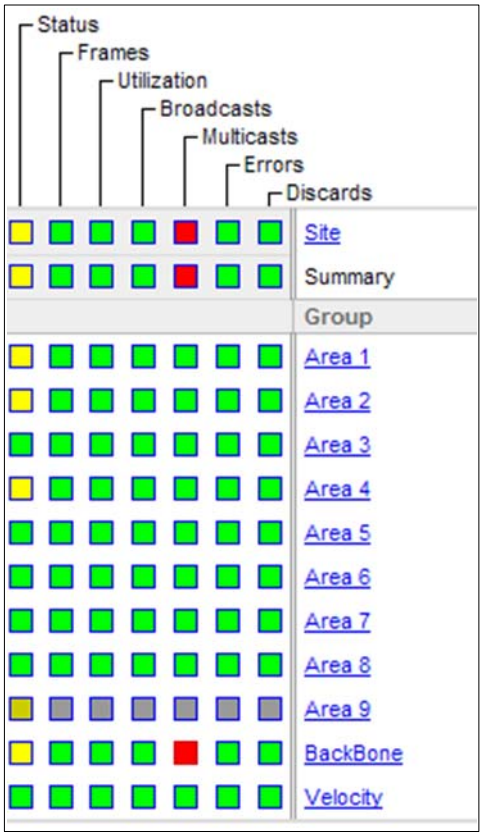
Path	Sampling Rate	Min. ifSpeed	Max. ifSpeed	Actions
HP Intel Solution Center>Grenoble	200	0Kb/sec	10Mb/sec	Edit Remove
HP Intel Solution Center>Grenoble	500	10Mb/sec	100Mb/sec	Edit Remove
HP Intel Solution Center>Grenoble	1000	100Mb/sec	1Gb/sec	Edit Remove
HP Intel Solution Center>Grenoble	2000	1Gb/sec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

Back New

5.2 Set up traffic monitoring

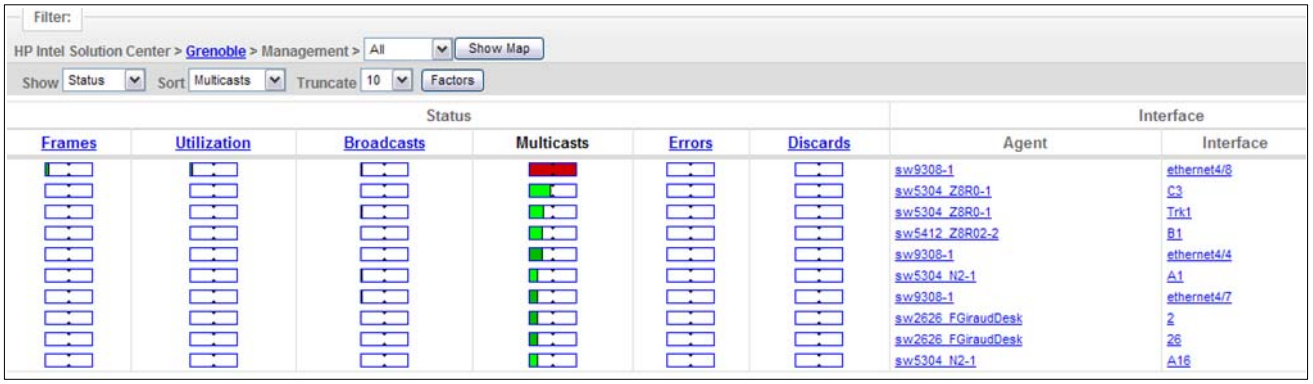
To set up traffic monitoring:

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

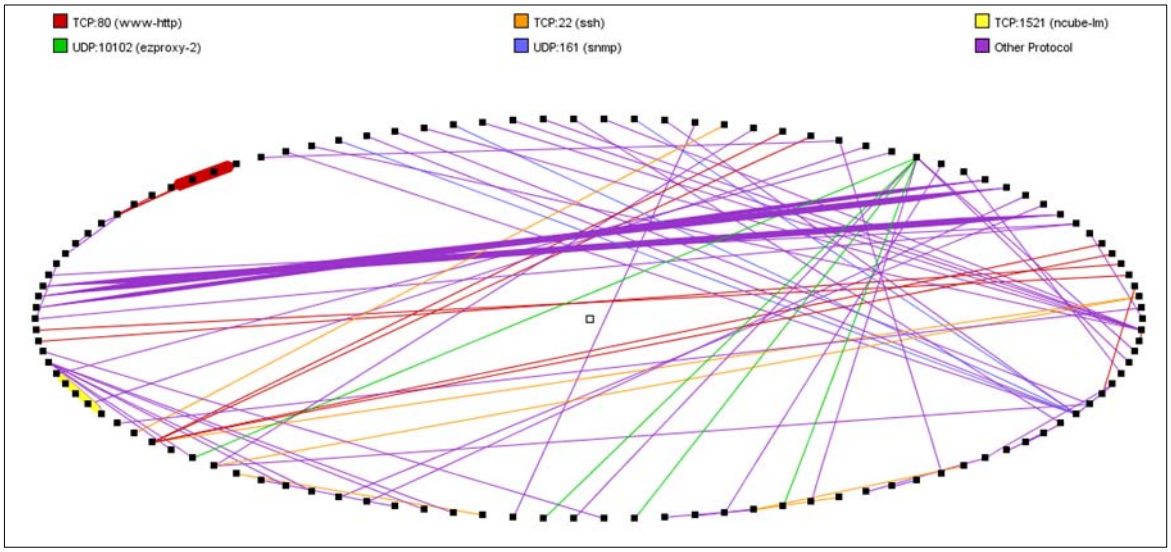


2. To view more details about a particular metric, click on one of the colored square indicators.

   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:

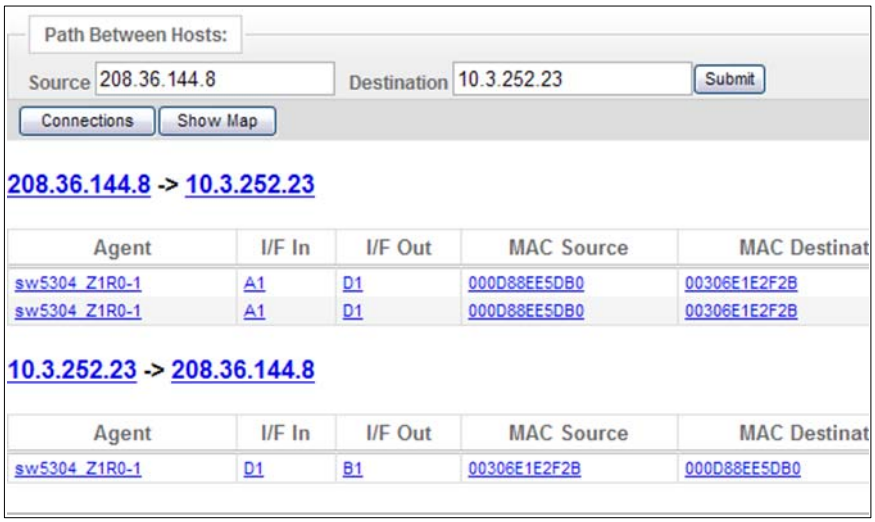


3. Another way to have a good overview of what is generating traffic on the network is to use the circles function (Traffic | Circles):



   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:

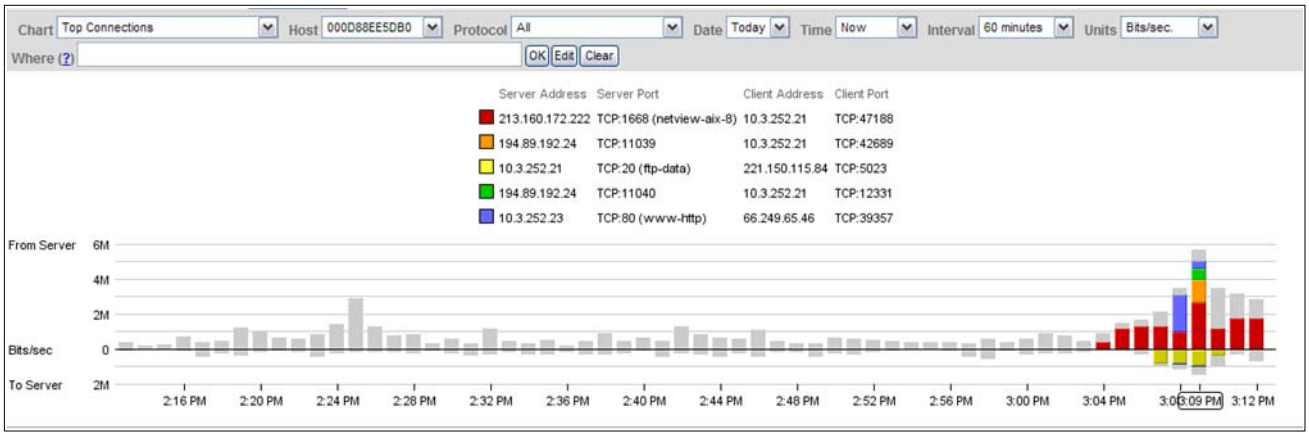


5. To obtain more information about a particular host, in the Path Between Hosts window click on one of the MAC Source or MAC Destination addresses. You then see a Find Host window, where you can choose between different views of the traffic:

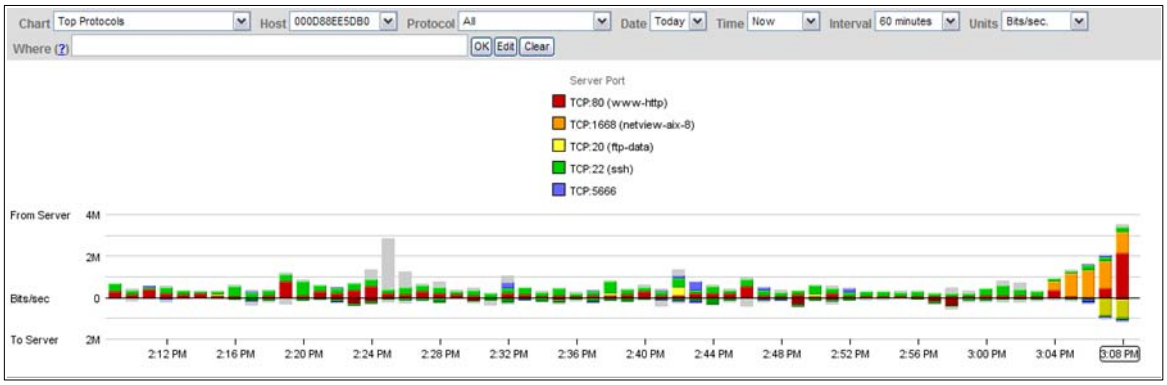
5.3 Traffic views

Here are some of the traffic views that are available.

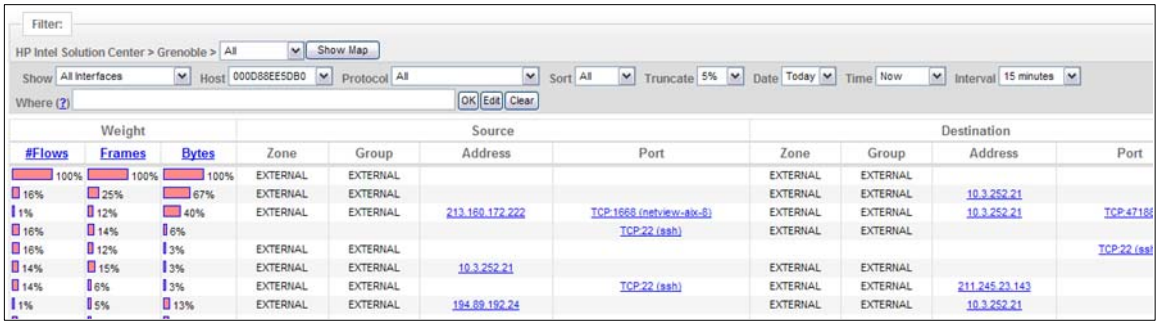
Clicking Connections gives top connections to and from this machine:



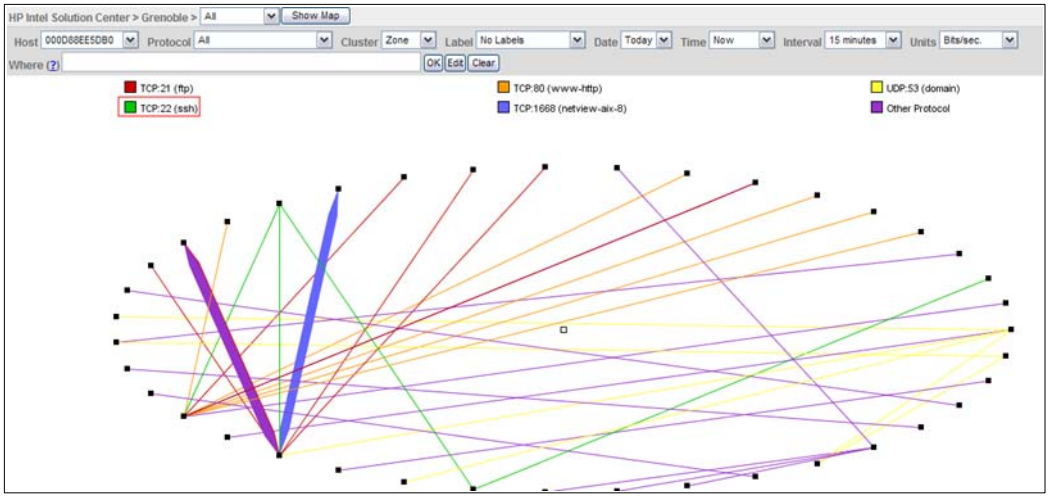
Clicking Protocols gives a view of the most used protocols for this MAC address over time:



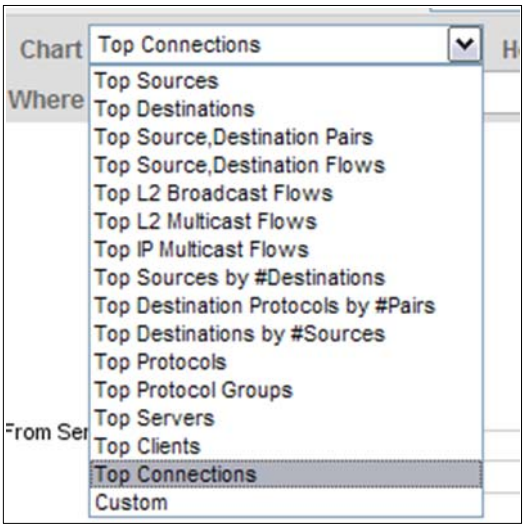
Factors view gives the proportion of each connection in percent of the flows, total frames and total bytes of the link to this machine:



A Circles view for this machine is also available:



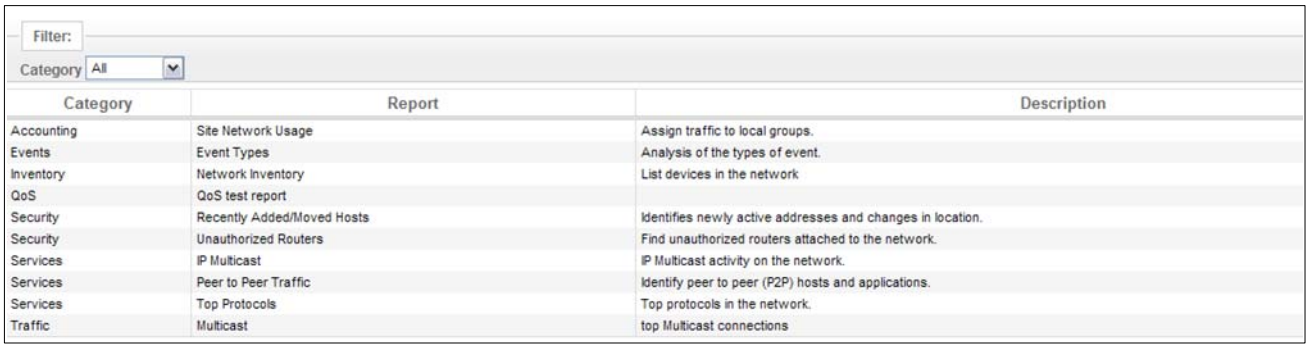
You have a wide variety of traffic types to display in charts:



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:



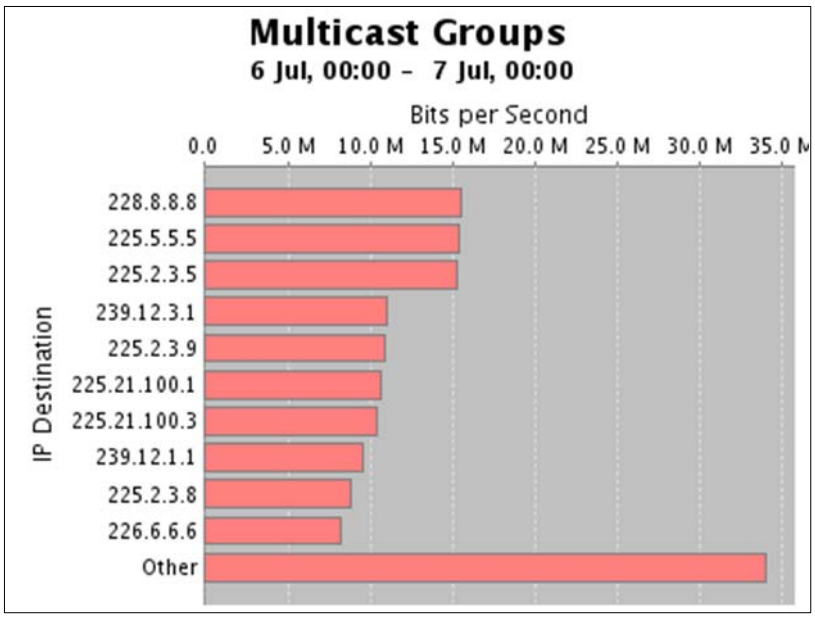
Category	Report	Description
Accounting	Site Network Usage	Assign traffic to local groups.
Events	Event Types	Analysis of the types of event.
Inventory	Network Inventory	List devices in the network
QoS	QoS test report	
Security	Recently Added/Moved Hosts	Identifies newly active addresses and changes in 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.

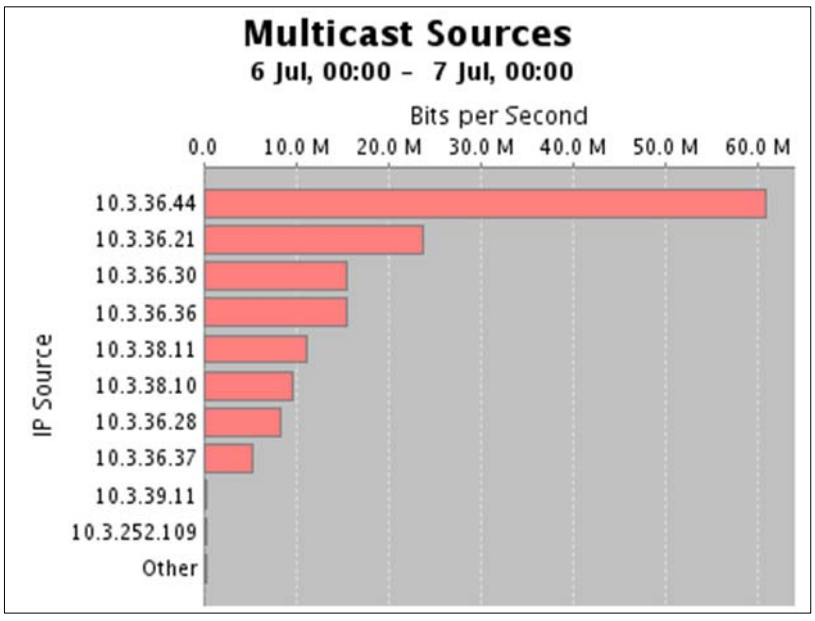
   For example if you select IP Multicast, you see a report that displays the IP Multicast activity on the network. You see activity reports for the top Multicast Groups, Multicast Sources, and Multicast Trends. This report can be exported as a .PDF or a .HTML file. For example:

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

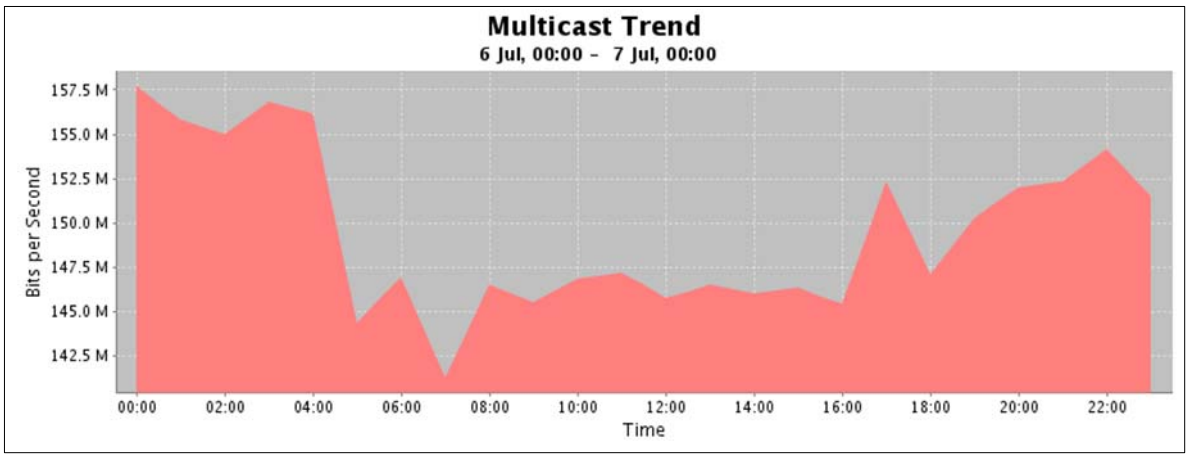
- **Top Multicast Groups**: Shows top IP multicast addresses by amount of traffic. For example:



- **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

4AA2-1719EEE, July 2008