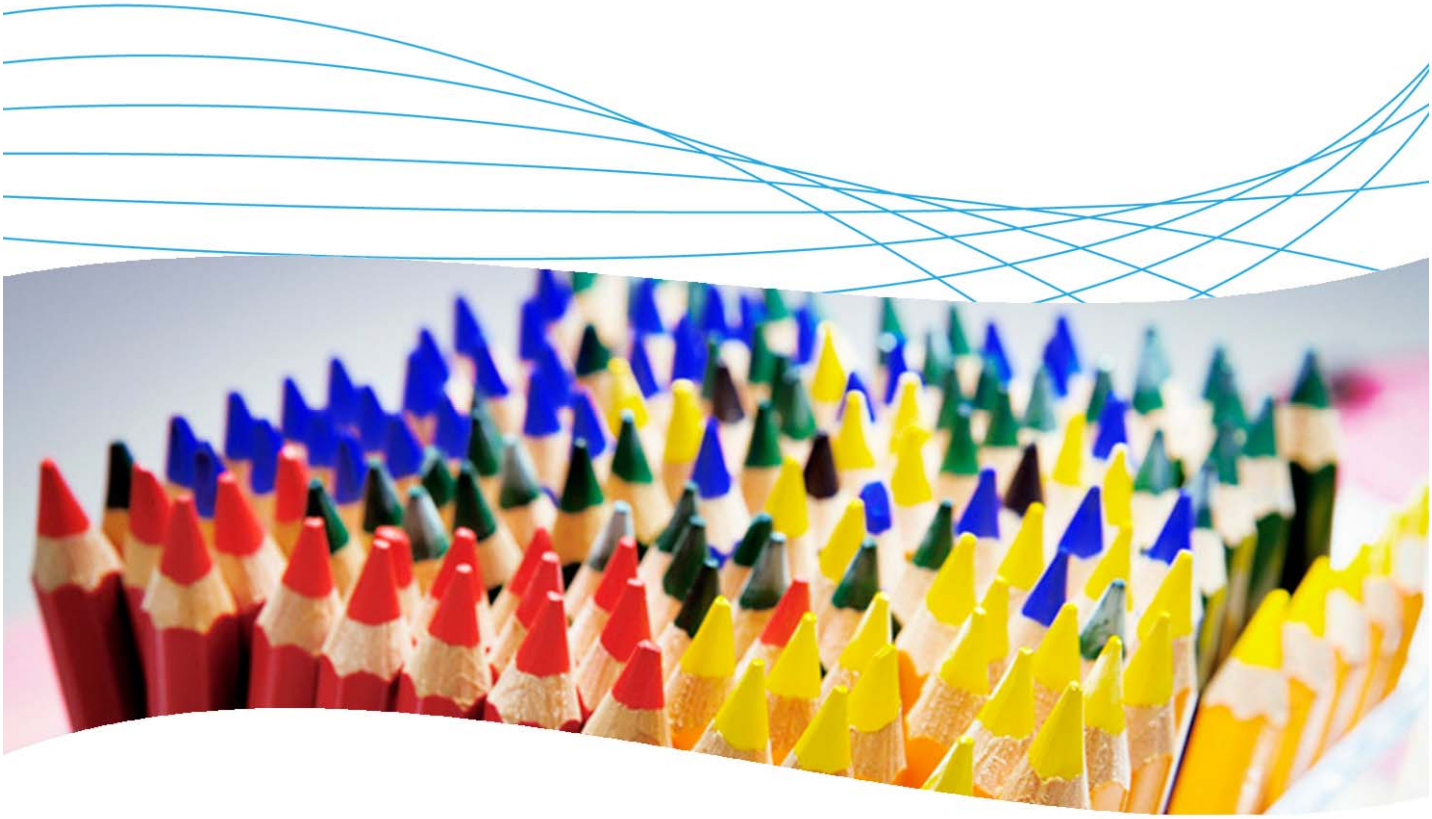
An HP ProCurve Networking Application Note

Traffic monitoring with sFlow and ProCurve Manager Plus



Contents

1. Introduction

This application note presents the advantages of the sFlow protocol and its implementation for traffic monitoring on ProCurve switches and ProCurve Manager Plus.

2. Prerequisites

This procedure assumes you have a network containing ProCurve switches and monitored by ProCurve Manager Plus.

3. Network diagram

Figure 1 details the hardware configuration referenced in this section.

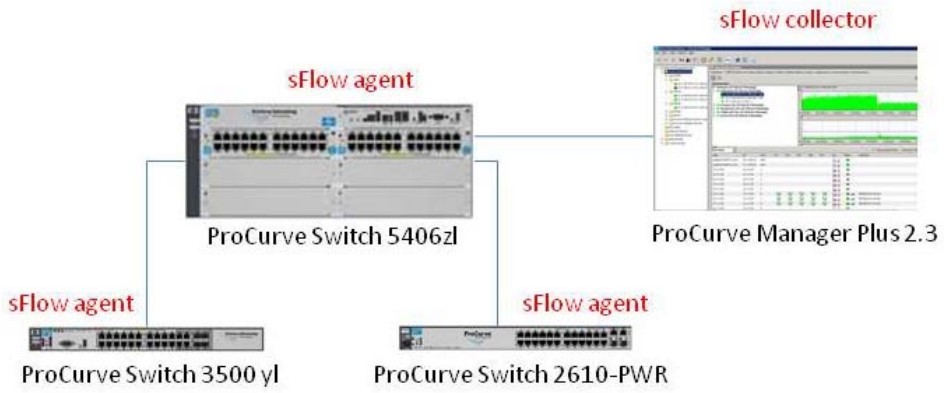


Figure 1. Setup for monitoring traffic flow with PCM+ and sFlow

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 Manager Plus, latest version. Version used here is PCM+ 2.3
- ProCurve switches: 5406zl, 3500yl, 2610-PWR

4. About the sFlow protocol

As defined in RFC 3176 written by InMon, sFlow is a technology for monitoring traffic in data networks containing switches and routers. In particular, it defines the sampling mechanisms implemented in an sFlow Agent for monitoring traffic, the sFlow MIB for controlling the sFlow Agent, and the format of sample data used by the sFlow Agent when forwarding data to a central data collector.

4.1 sFlow history

Packet sampling has been used to monitor network traffic for over 10 years. HP first demonstrated network-wide monitoring using packet sampling at the University of Geneva and CERN at Telecom 91. This was followed by the introduction of networking products with embedded packet sampling capability—HP Extended RMON—in 1993. Other vendors then either implemented sFlow or chose to develop proprietary packet sampling methods (e.g. Cisco Netflow). Today sFlow has been accepted as a standard in the network industry.

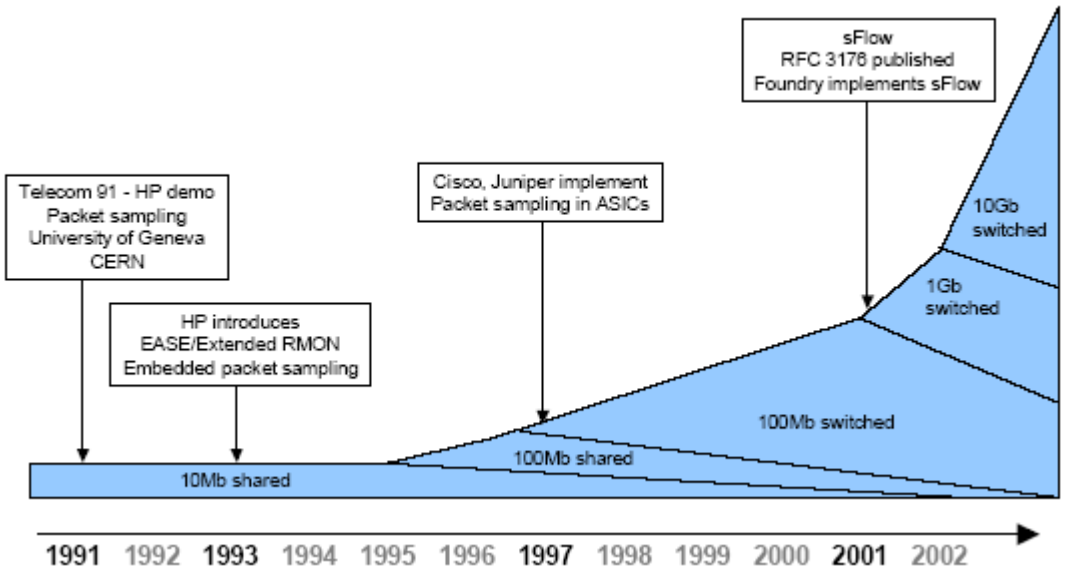


Figure 2. History of the sFlow protocol
Source: www.sFlow.org

4.2 Protocol description

sFlow operates as a combination of packet sampling and counter polling on the network equipment.

- **Sampling**: Each network switch contains an sFlow agent, which reports to an sFlow collector. A sampling rate, N, is defined, either for the complete agent or for a single interface. One packet out of N is captured and sent to the collector.
- **Polling**: A polling interval defines how often the sFlow counters for a specific interface are sent to the collector, but an sFlow agent is free to schedule polling in order maximize internal efficiency. If the regular schedule is chosen, each counter start time will be chosen differently to smooth performance.

The sampled data is sent as a UDP packet to the specified host and port on the sFlow collector. The default port is 6343. If counter samples are lost, new values will be sent when the next polling interval has passed. The loss of packet flow samples is a slight reduction in the effective sampling rate.

The UDP payload contains the sFlow datagram. Each datagram provides information about the sFlow version, its originating agent's IP address, a sequence number, how many samples it contains, and usually up to 10 flow samples or counter samples.

4.3 Benefits of using sFlow

The advantages of using sFlow include:

- **Accuracy**: sFlow can be implemented in hardware (ASICs) at wire speed. Users can obtain detailed analysis of information about layer 3 though layer 7.
- **Scalability**: sFlow can monitor all speeds of links, up to 10 Gbps and more. Thousands of devices can be monitored.
- **Low cost**: sFlow is already implemented in most switches and routers, and can be used easily in conjunction with management platforms such as ProCurve Manager Plus and InMon.
- **Minimal network load**: sFlow adds only a minimal amount to network overhead.

4.4 sFlow applications

Some typical sFlow applications include:

- **Traffic monitoring**: sFlow provides a minute-by-minute view of the traffic on the network: bandwidth used, protocols, connections, and more.
- **Intrusion detection**: sFlow can help recognize network-based attacks (for example, in conjunction with the NBAD engine in ProCurve Network Immunity Manager).
- **Route profiling**: sFlow can help to see the most active routes on the network.
- **Accounting and billing**: For billing purposes, sFlow can provide detailed information about applications in use on the network.

5. sFlow configuration on ProCurve switches

This section provides command syntax for configuring sFlow on a ProCurve switch.

5.1 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.

5.2 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
```

5.3 Activate sampling and polling

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

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

Where *1/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.

5.4 View sampling and polling statistics

To view sampling and polling statistics:

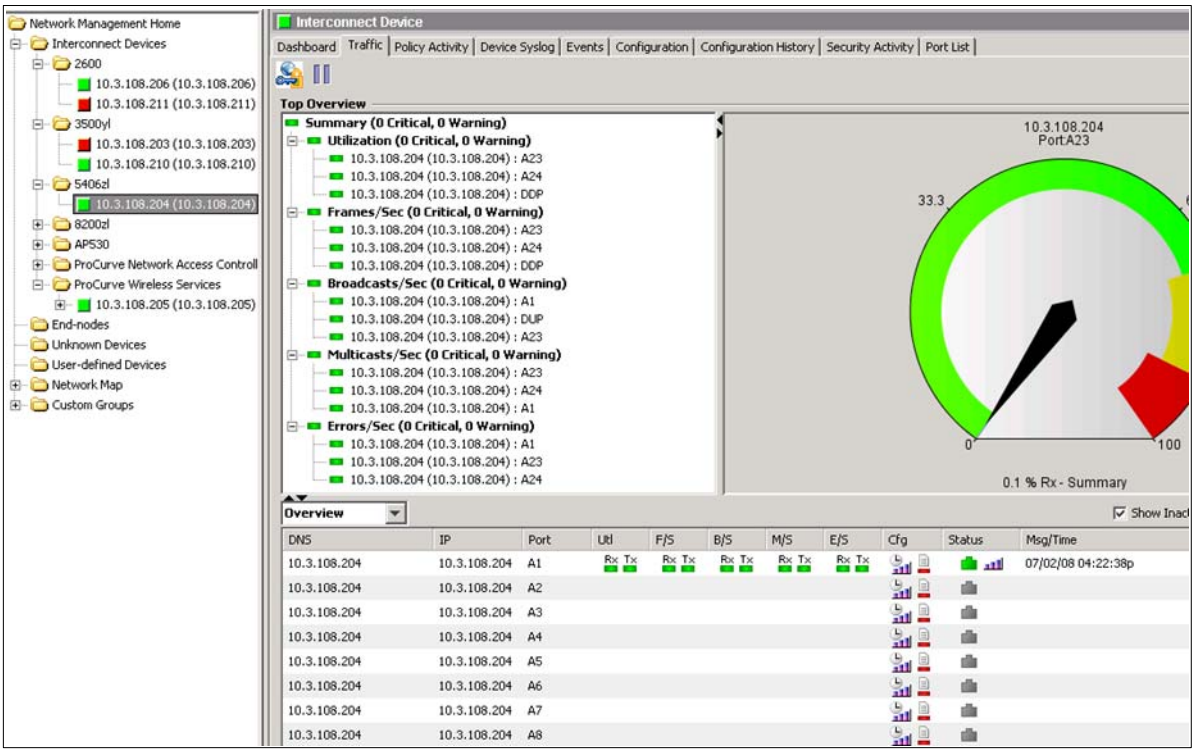
```
5406zl(config)# show sFlow 1 sampling

 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
```

6. Using the PCM+ Traffic Monitor

You can use the ProCurve Manager Plus Traffic Manager, with its built-in Traffic Monitor, to monitor network traffic. Traffic monitoring is set to run automatically, with the capability for simultaneously performing statistics polling and sFlow sampling.

6.1 View the Traffic Monitor

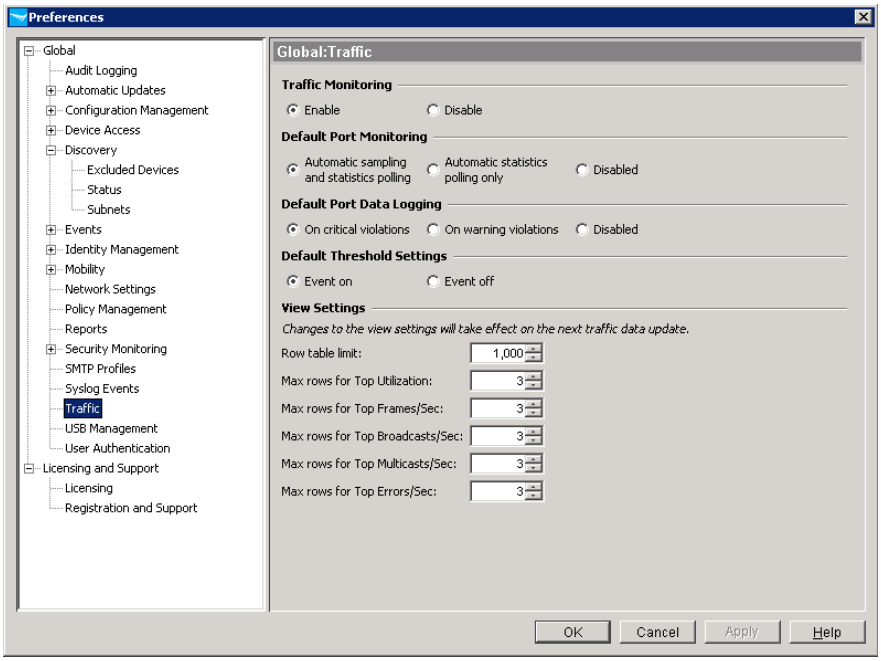
The ProCurve Manager Plus Traffic Monitor is accessed from the Traffic tab when clicking on a network equipment or on a group of network equipment:



In the Traffic tab on the left side, the top ports are listed for different categories: Utilization, Frames/Sec, Broadcasts/Sec, Multicasts/Sec, and Errors/Sec.

6.2 Specify the global port display

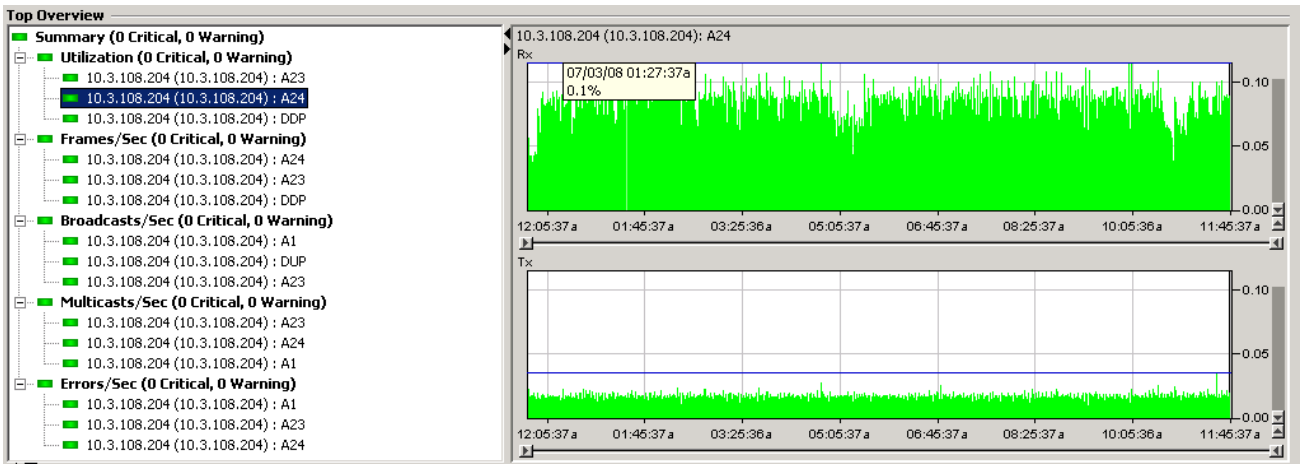
To set the number of top X ports you want to list for each category, go to Preferences > Traffic. You see the Global Traffic window:



This window lets you can also enable/disable traffic monitoring, choose the monitoring mode (sampling and polling, or polling only), and control logging (on critical or warning violations).

6.3 View port metrics

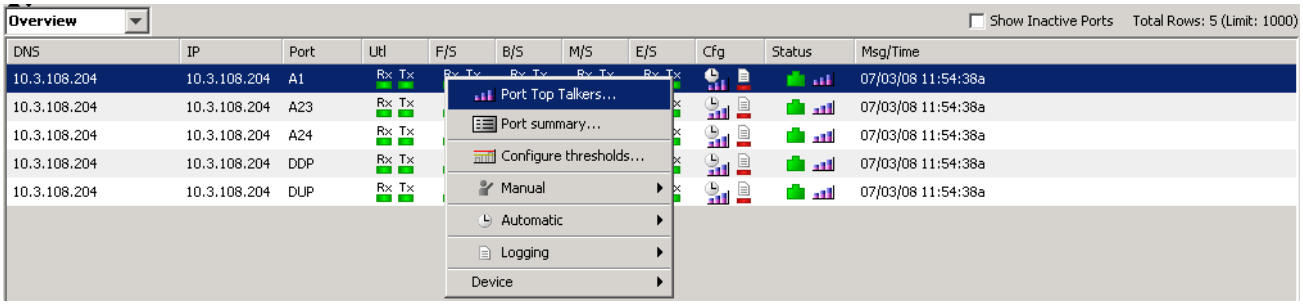
Clicking on a port in the traffic view displays metrics (for example, utilization) for that port on the right side of the window. You have two charts: Rx and Tx, indicating received and transmitted traffic on the port.



The bottom part of the traffic view lists all the ports of the chosen device or group, even the inactive ones. To view only active ports, click to disable Show Inactive Ports.

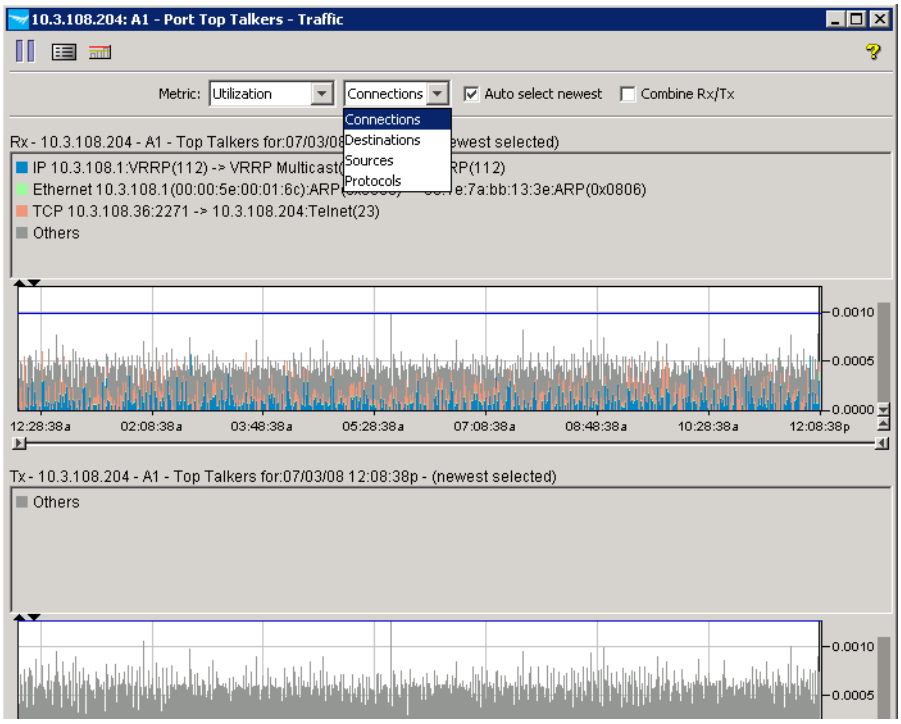
6.3 Other port views

If you right-click on a port in the left or bottom pane you can choose between several views:

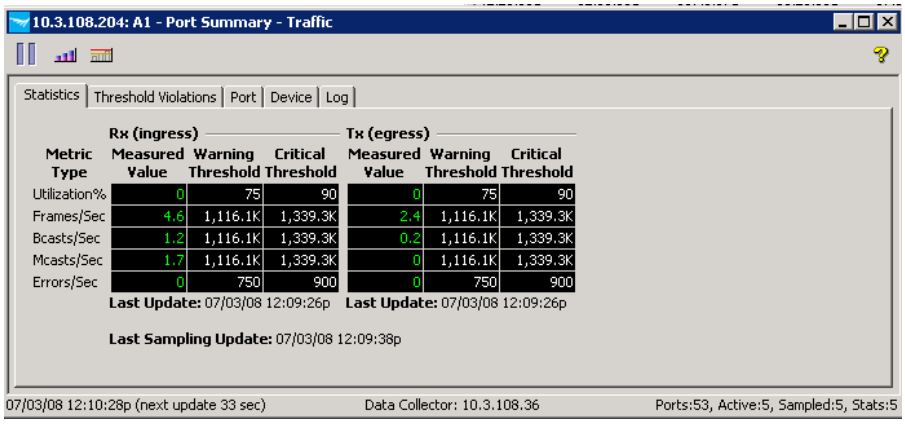


The views include:

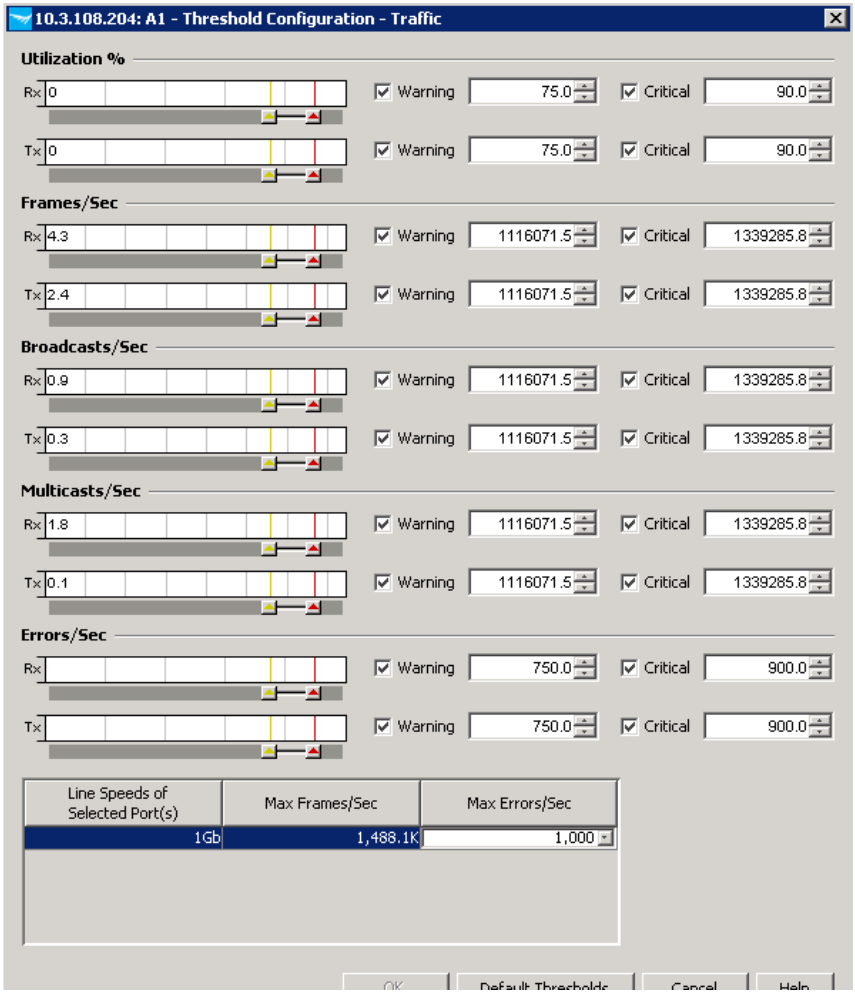
- **Port Top Talkers**: Gives a view of the protocols and connections that generate the most traffic on the port at a given time. You can obtain the view by connections, destinations, sources or protocols:



- **Port summary**: Gives more precise figures on port statistics, threshold violations, and other information about the port or device:



- **Configure thresholds**: Enables you to set the limits for warning and critical thresholds for the different metrics:



Other options allow you to:

- Manually or automatically enable/disable sampling or polling-only.
- Enable/disable automatic data logging for warning or critical data.
- Gain access to the Device menu.

6. Reference documents

This concludes the procedure for traffic flow monitoring using ProCurve Manager Plus and sFlow.

For further information about how to configure ProCurve switches and ProCurve Manager 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 on sFlow:
  http://sFlow.org/

For further information, please visit www.procurve.eu

4AA2-1626EEE, July 2008