



Setup Caligare Netflow with PacketShaper

created by: Rainer Bemsel - Version 1.0 - Dated: Dec/11/2005

This documents describes the basic steps to install Caligare Netflow on Debian GNU/Linux to receive Netflow-5 Data from PacketShaper. Caligare provides a 30-daysTrial version, which is fully functional. At the end of this document, I've attached some reports.

Connect to Caligare Website <http://www.caligare.com/netflow/download.php> , where you can download the iso-image and request a trial key.

- A) Download iso-netflow-3.2.4.iso and burn it onto a CD.
- B) Request a License Key fro the Trial Version

Install	File Name	Description	Size	Date
	netflow-3.2.4.i386.deb	Debian (DEB) installer	8 MB	Dec 06 2005
	netflow-3.2.4-1.i386.rpm	RedHat, Fedora, SuSE (RPM) installer	8 MB	Dec 06 2005

Documentation	File Name	Description	Size	Date
	netflow-3.2.4.pdf	Full product documentation	1.9 MB	Dec 05 2005

ISO-CD Image	File Name	Description	Size	Date
	iso-netflow-3.2.4.iso	ISO-CD self installation (*)	180 MB	Dec 06 2005

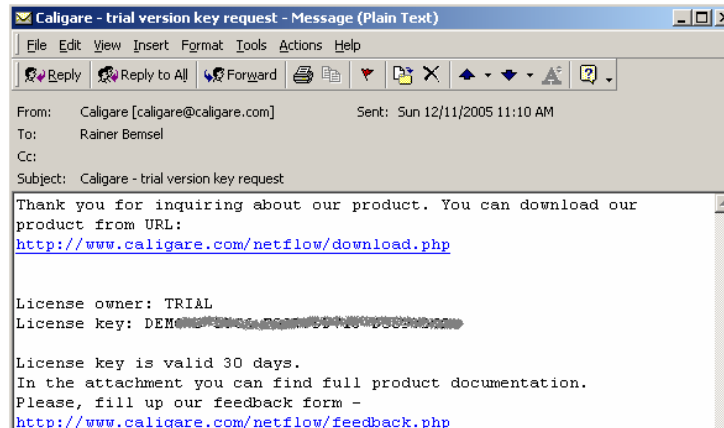


DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

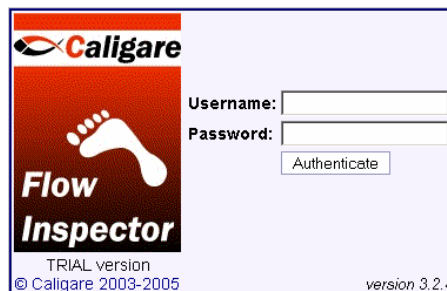
Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evolution by myself. All liability for use of the information presented here remains with the user.

C) Wait for the Email providing the License Key.



D) Start Installation

1. Boot from CD
2. The installation script will perform all necessary steps, and only a few inputs are required
 - It will create partitions
 - It will create EXT3 file-system
 - It will create a swap file system
 - It will mount target device
 - It will extract the image
 - It will copy the netflow software
 - It will set up the boot loader
 - It will ask for a hostname
 - It will set the time zone
 - It will ask to set a UNIX password (for root account)
3. Remove the CD and reboot the system
4. After rebooting, you have some more information to be put it
 - Choose of DHCP or Static -> I suggest to run a static address to make sure, that netflow data will be received throughout the whole trial period.
 - Now, you need the information from the email for License Owner, and the License Key itself
5. The Netflow daemon nfd will stop and restart.
6. Open a web browser from another PC and connect to the IP address of the Netflow Collector.



If you see the login screen - you are done with the first main step. Username: **admin**, Password **nfadmin**

E) Synchronize Time

In order to have Netflow Sender and Netflow Receiver in time sync, I recommend to synchronizing date and time first, before adding any collectors or enable Netflow-5 at the sender side.

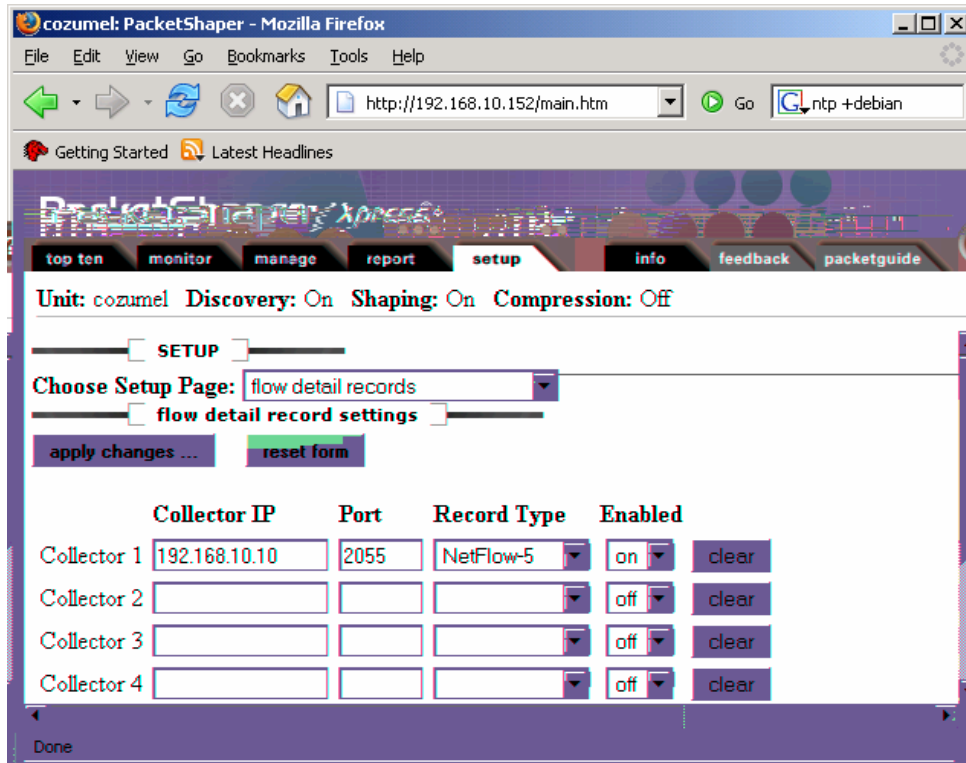
Note: 192.168.10.234 is hosting my local time server

```
Caligare-Server: ~#  
Caligare-Server: ~# ntpdate 192.168.10.234  
11 Dec 18:27:46 ntpdate [2816]: adjust time server 192.168.10.234 offset -0.131451 sec  
Caligare-Server: ~#
```

If you use Caligare Netflow as a permanent collector, it would make sense to install an NTP-Client, which does periodically time synchronization.

F) Configure PacketShaper for Netflow-5 Delivery

Connect to PacketShaper, click on SETUP Tab and choose FLOW DETAIL RECORDS page. Netflow will send packets by default on port 2055/UDP to the collector.



G) Set up Collector in Caligare

- Connect to Caligare with the Web User Interface
- Logon with admin (password: nfadmin)
- Click on Options - Collector - Add



Add new collector

Collector name:

Unit:

Enabled:

Port:

Number of hourly tables:

Number of daily tables:

Number of weekly tables:

Number of monthly tables:

Disable DoS protection: (not recommended)

Associated devices:

Forwarding list:

Comment:

Collector settings

Information
Collector PacketShaper created successfully ...

Unit	Name	Port	Comment	Command
<input type="checkbox"/>	primary	PacketShaper	2055	Edit Restart

Leave the advanced options for the collector on default. After Save, you should get a new unit.

Finally, wait a couple of minutes and verify statistics, if you get netflow data delivered.

Collectors status

Collector PacketShaper

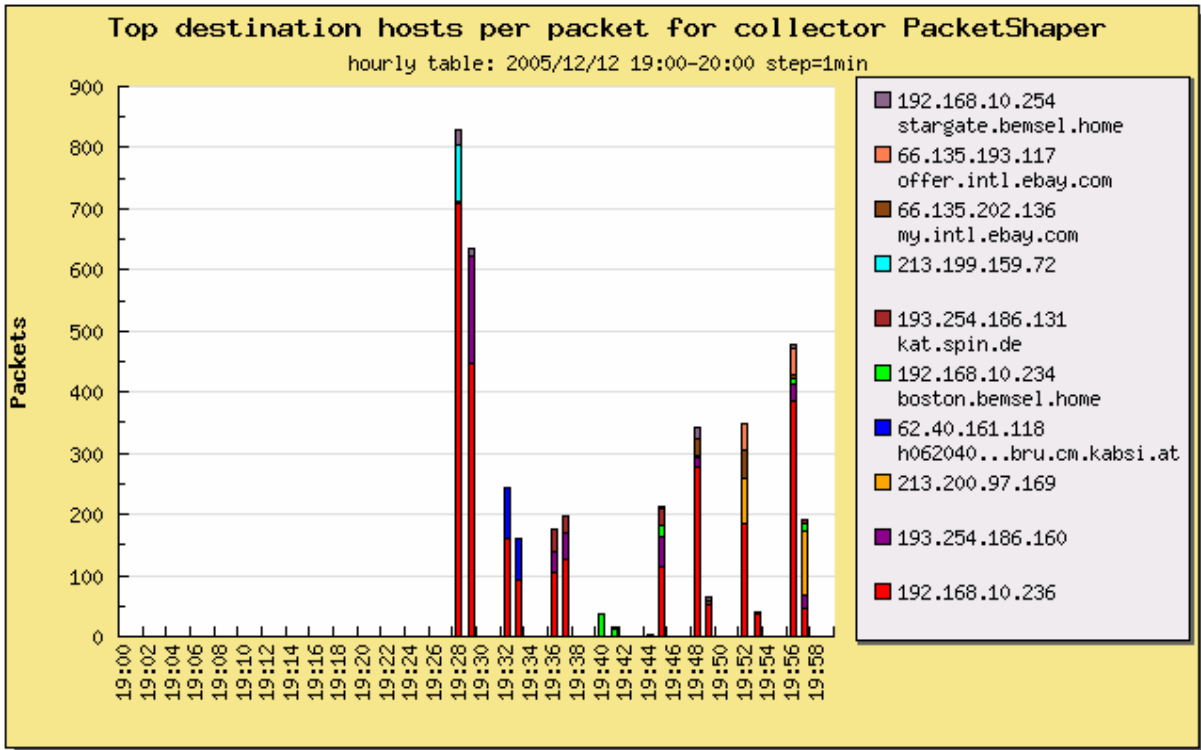
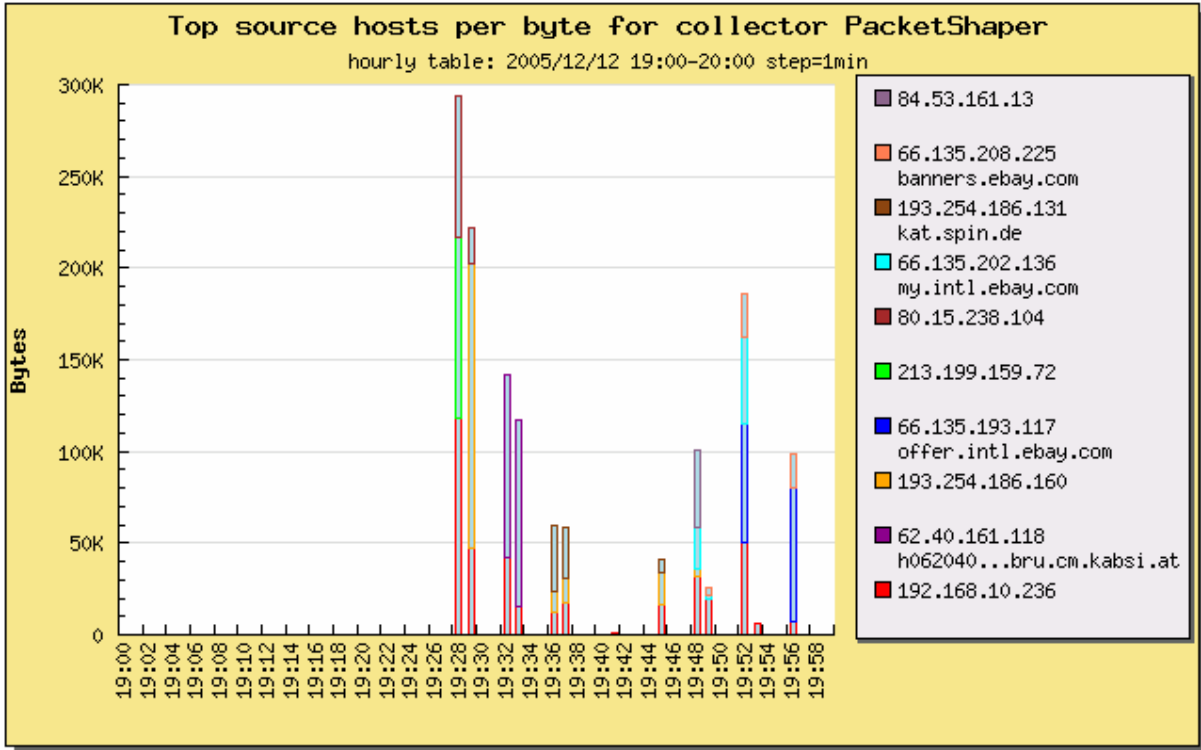
Start time: 2005-12-12 19:27:09
Uptime: 3 minutes and 13 seconds

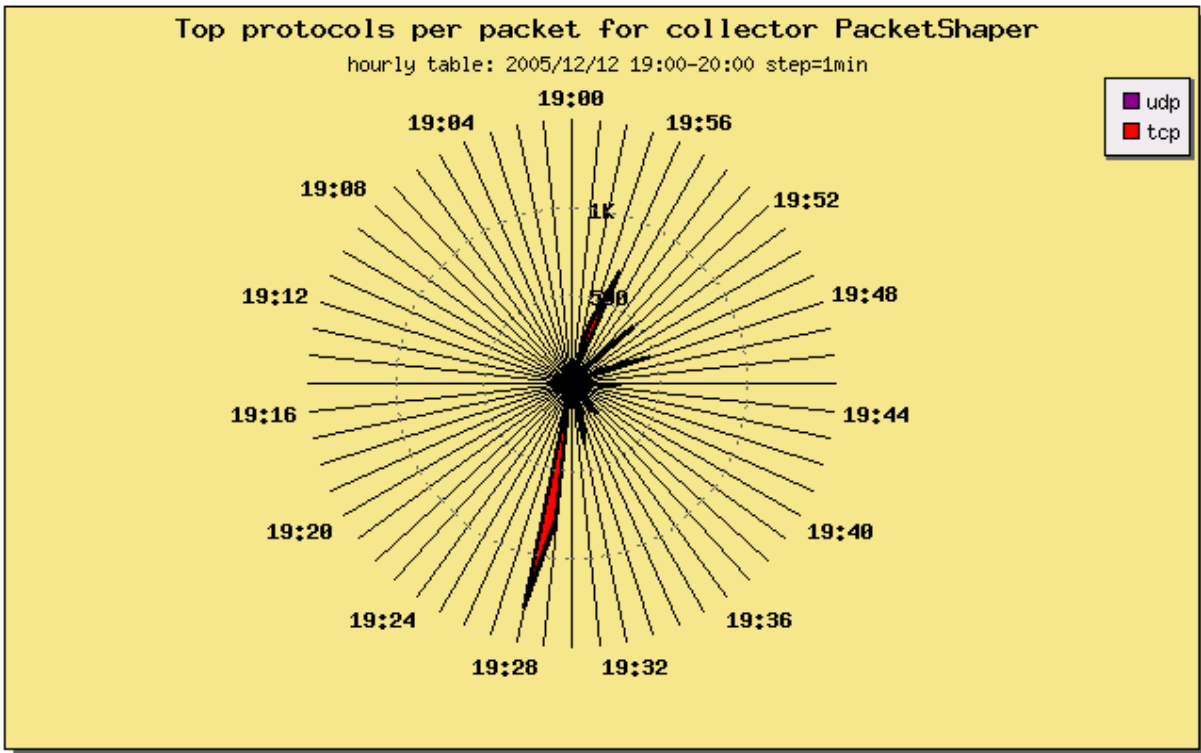
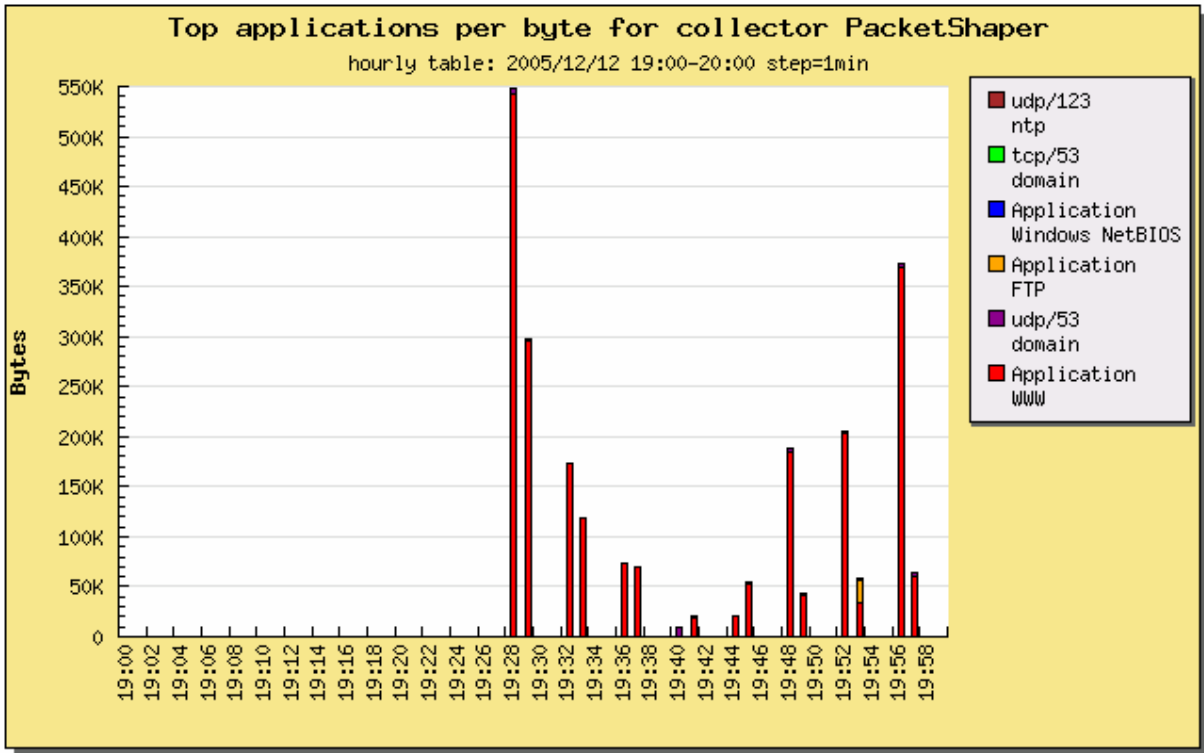
Collector PacketShaper (current hour)

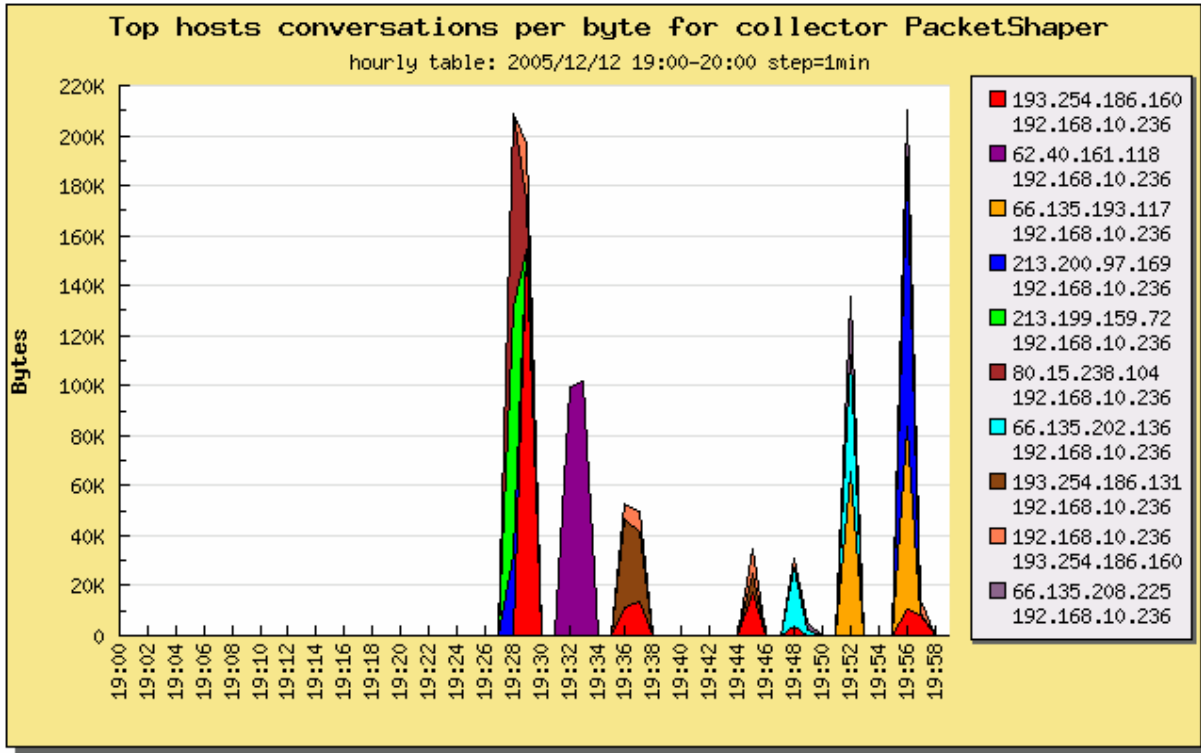
Number of packets:	42
Number of bytes:	19152
Number of flows:	378
Forwarded packets:	0
Dropped packets due to bad source IP:	0
Dropped packets due to unsupported netflow version:	0
Dropped flows due to corrupted time:	0

This is just the basic setup. There are a lot of tables, graphs and analysis possible. Some of them, are added on the next few pages.

Sample Graphs







All graphs can also be shown as table.

Top applications per byte for collector PacketShaper											
Time	Application WWW	Application FTP	Application E-mail	udp/53 domain	Application Windows NetBIOS	Application Direct Connect	udp/123 ntp	tcp/53 domain	Application Gnutella	icmp/0.0 echo pong	
Sun Dec 11 2005	0	0	0	0	0	0	0	0	0	0	0
Mon Dec 12 2005	9.1M (45.1%)	10.8M (53.42%)	71.2K (0.35%)	58.5K (0.29%)	23.3K (0.11%)	78.9K (0.39%)	20.3K (0.1%)	6.3K (0.03%)	40.5K (0.2%)	2.2K (0.01%)	
Tue Dec 13 2005	0	0	0	0	0	0	0	0	0	0	
Wed Dec 14 2005	0	0	0	0	0	0	0	0	0	0	
Thu Dec 15 2005	101.7M (86.27%)	15M (12.7%)	712.1K (0.6%)	299.5K (0.25%)	116.7K (0.1%)	0	41.1K (0.03%)	37.8K (0.03%)	0	8.9K (0.01%)	
Fri Dec 16 2005	16.5M (97.69%)	27.6K (0.16%)	222K (1.32%)	75.8K (0.45%)	35.4K (0.21%)	0	8.7K (0.05%)	8.5K (0.05%)	0	12.4K (0.07%)	
Sat Dec 17 2005	0	0	0	0	0	0	0	0	0	0	
Sum total	127.4M	25.8M	1M	433.8K	175.3K	78.9K	70.1K	52.6K	40.5K	23.4K	

A complete Feature List of Caligare could be found on their website

http://www.caligare.com/document/CFI_Brief.pdf

